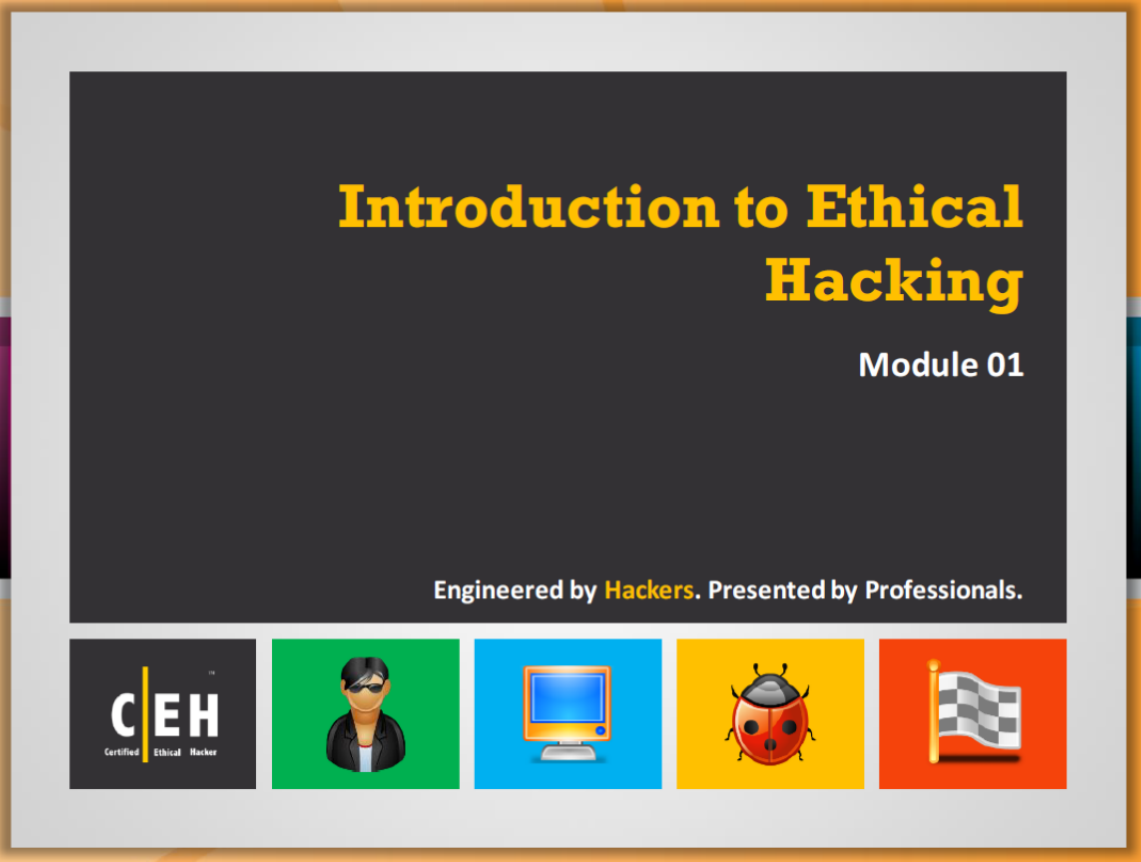
Introduction to Ethical Hacking

Module 01



Ethical Hacking and Countermeasures v8

Module 01: Introduction to Ethical Hacking

Exam 312-50

News

Zero-day Attacks are Meaner, more Rampant than we ever thought

Source: http://arstechnica.com

Computer attacks that target undisclosed **vulnerabilities** are more common and last longer than many **security researchers** previously thought. The finding comes from a new study that tracked the number and duration of **so-called zero-day** exploits over three years.

The typical zero-day attack, by definition, exploits software flaws before they are publicly disclosed. It lasts on average **312 days**, with some lasting as long as two and a half years, according to the study by researchers from antivirus provider Symantec. Of the 18 zero-day attacks the researchers found between 2008 and 2011, 11 of them previously went undetected. Recent revelations that the **Stuxnet malware** that sabotaged Iranian nuclear facilities relied on five zero days already underscored the threat posed by such attacks. But the researchers said their findings suggest the menace may be even greater.

"Zero-day attacks are difficult to prevent because they exploit unknown vulnerabilities, for which there are no patches and no antivirus or **intrusion-detection signatures**," they wrote. "It seems that, as long as software will have bugs and the development of exploits for new

vulnerabilities will be a profitable activity, we will be exposed to zero-day attacks. In fact, 60 percent of the zero-day vulnerabilities we identify in our study were not known before, which suggests that there are many more zero-day attacks than previously thought—perhaps more than twice as many."

Researchers Leyla Bilge and **Tudor Dumitras** conducted a systematic study that analyzed executable files collected from **11 million** computers around the world from February 2008 to March 2012. Three of the zero-day exploits they found were disclosed in 2008, seven were disclosed in 2009, six were disclosed in 2010, and two were disclosed in 2011. (The binary reputation data the researchers relied on prevented them from identifying attacks in 2012.) An attack on many versions of Microsoft Windows, which appears to have gone undetected as a zero day until now, had the shortest duration: just 19 days. An exploit of a separate security bug in the Windows shell had the longest duration: 30 months.

Of the 18 attacks studied, 15 targeted 102 or fewer of the 11 million hosts that were monitored. Eight of the exploits were directed at three or fewer hosts. The data confirms conventional wisdom that zero-day attacks are typically reserved for high-value targets. Of the remaining three attacks, one was exploited by Stuxnet and another was exploited by Conficker, the virulent worm discovered in 2008 that has infected millions of computers (and reportedly continues to do so). The Stuxnet and Conficker exploit targeted **1.5 million** and **450,000** hosts respectively. The results, the researchers said, demonstrated the dividends returned by zero-day exploits, which can command prices as high as **$250,000**.

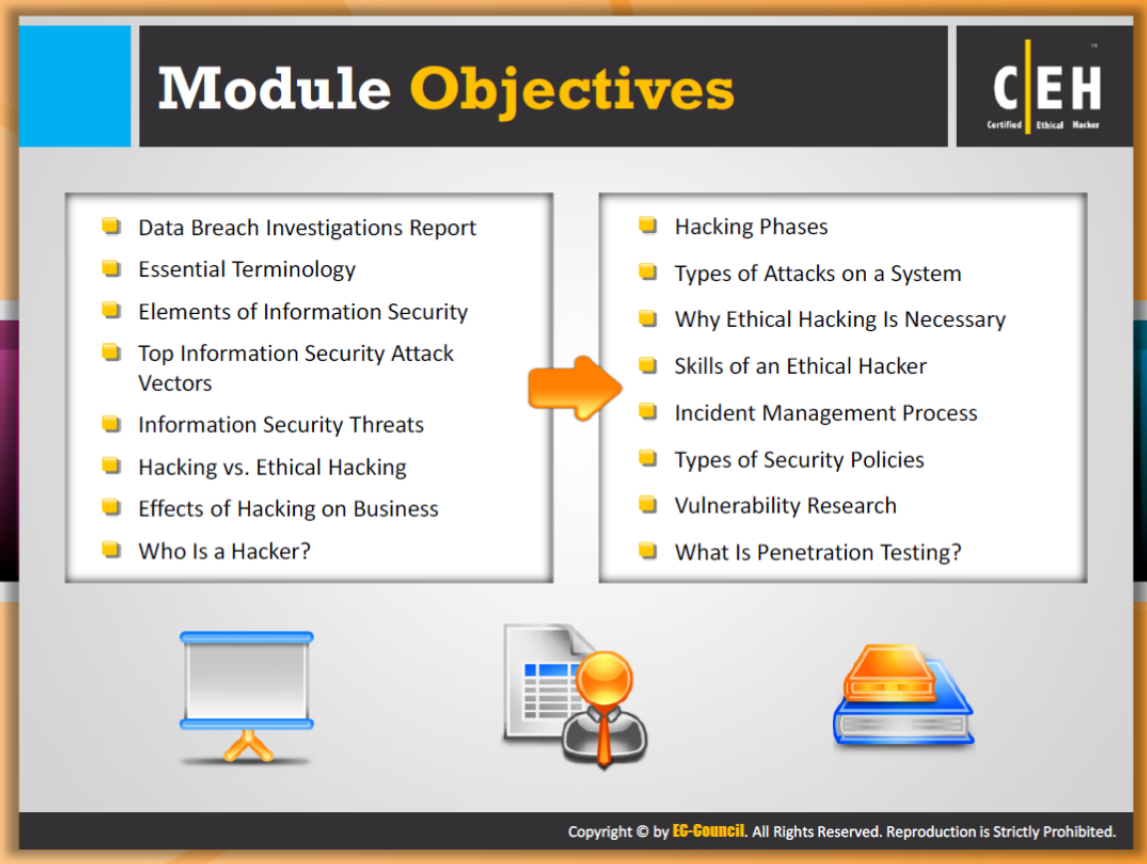
"For example, Conficker exploiting the vulnerability CVE-2008-4250 managed to infect approximately 370,000 machines without being detected over more than two months," they wrote. "This example illustrates the effectiveness of zero-day vulnerabilities for conducting stealth cyber-attacks."

The researchers cautioned that their method of collecting executable files had significant limitations, causing it to miss 24 zero-day attacks tracked by Symantec's own Internet Security Threats Report over the time period studied. Surprisingly, the number of attacks only grew once zero-day attacks became public knowledge—by margins of two- to 100,000-fold. The number of attack variants also rose, with 183 to 85,000 more variants detected each day. One possible cause of the surge in new files, the researchers said, is that the exploits may have been repackaged versions of the same attack.

"However, it is doubtful that repacking alone can account for an increase by up to five orders of magnitude," they wrote. "More likely, this increase is the result of the extensive re-use of field-proven exploits in other malware."

Author: Dan Goodin

http://arstechnica.com/security/2012/10/zero-day-attacks-are-meaner-and-more-plentiful-than-thought/



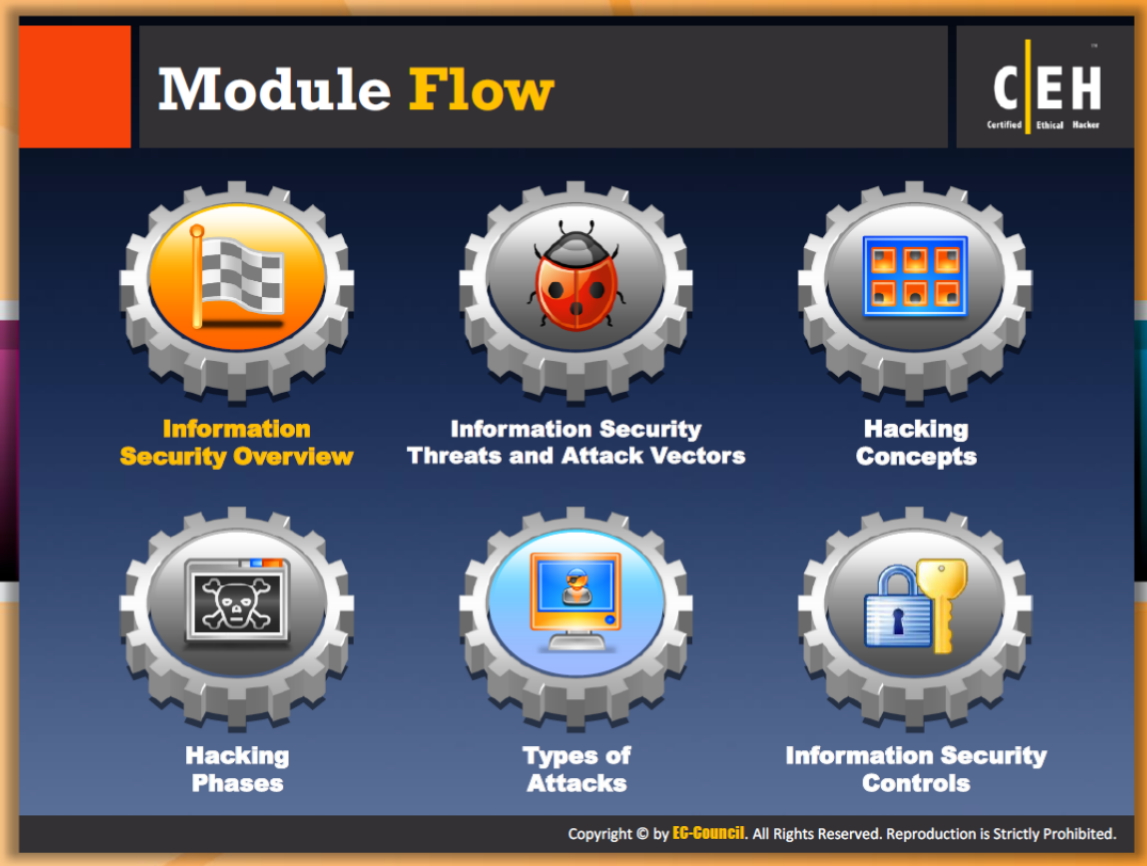
Module Objectives

It is important to bear in mind that attackers break into systems for various reasons and purposes. Therefore, it is important to comprehend how **malicious hackers** exploit systems and the probable reasons behind the attacks. As **Sun Tzu** put it in the Art of War, "If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat." It is the duty of **system administrators** and **network security professionals** to guard their infrastructure against exploits by knowing the enemy—the malicious hacker(s)—who seek to use the same infrastructure for illegal activities.

Ethical hacking is the process of checking and testing the organization network for the possible loopholes and vulnerabilities. The individuals or experts who perform ethical hacking are called **white hats**. They perform hacking in **ethical ways**, without causing any damage to the computer system, thereby **increasing** the **security perimeter** of an organization.

This module covers:

- Data Breach Investigations Report
- Essential Terminology
- Elements of Information Security
- Top Information Security Attack Vectors
- Information Security Threats
- Hacking vs. Ethical Hacking
- Effects of Hacking on Business
- Who Is a Hacker?
- Hacking Phases
- Types of Attacks on a System
- Why Ethical Hacking Is Necessary
- Skills of an Ethical Hacker
- Incident Management Process
- Types of Security Policies
- Vulnerability Research
- What Is Penetration Testing?

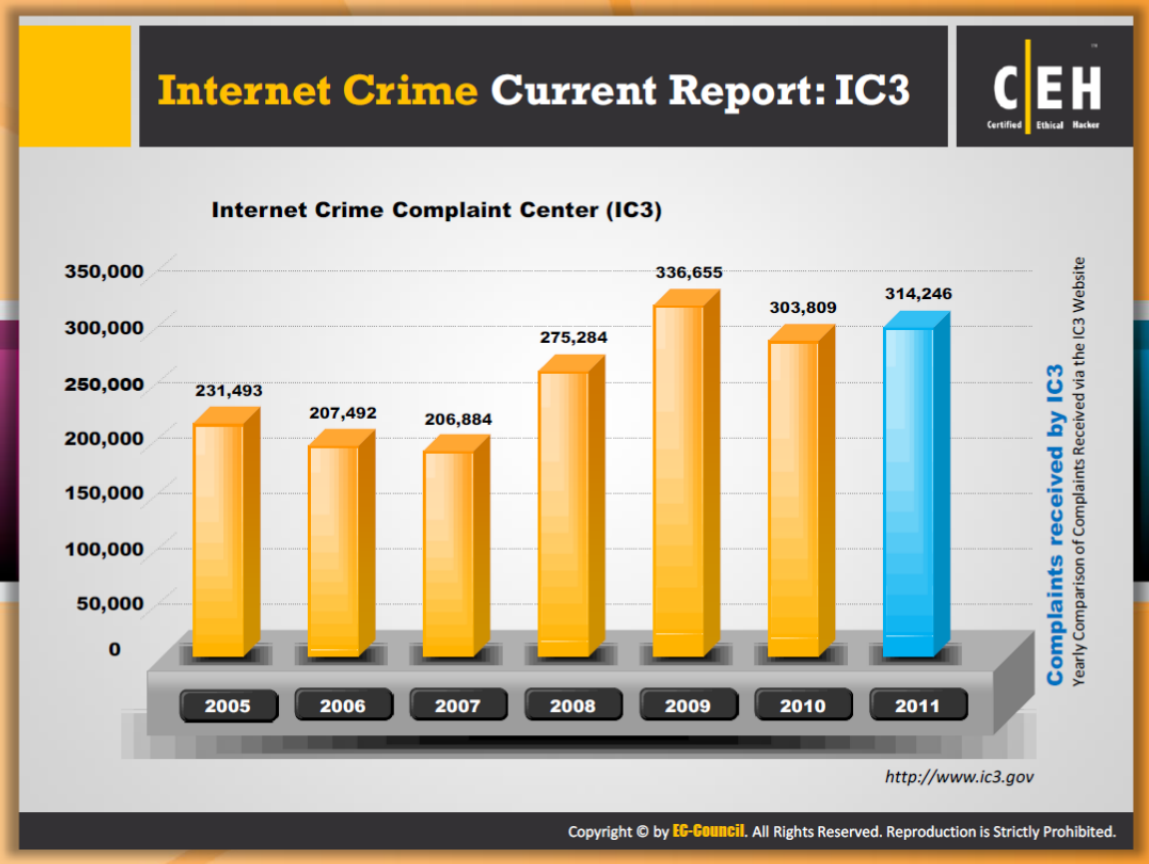


Module Flow

Information security refers to protecting or safeguarding any kind of sensitive information and information systems from unauthorized access, disclosure, alteration, disruption, and destruction. For most organizations, information is the critical resource to be secured. If sensitive information falls into wrong hands, then the respective organization may face a great threat. In an attempt to understand how to secure such critical information resources, first we will look at an **overview of information security**.

Information Security Overview	**Hacking Phases**
Information Security Threats and Attack Vectors	**Types of Attacks**
Hacking Concepts	**Information Security Controls**

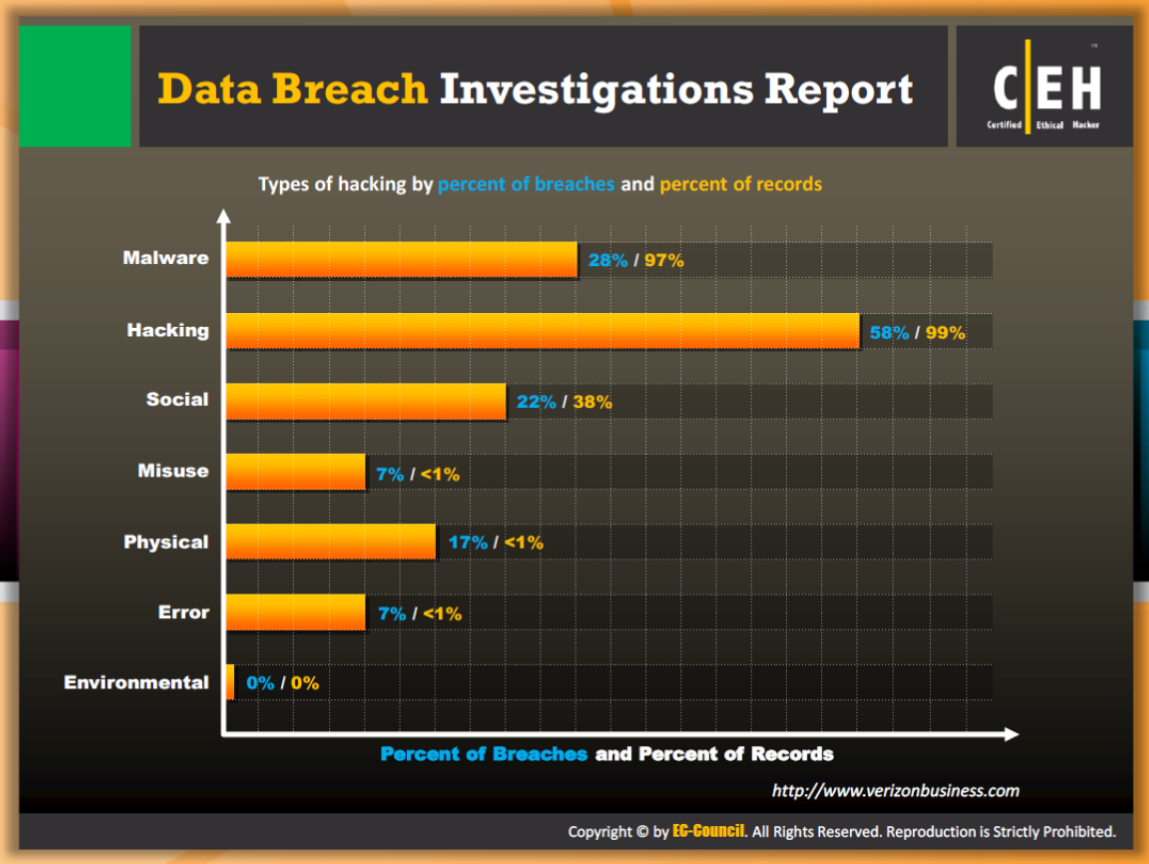
This section covers elements of information security, the strength of the component triangle (security, functionality, and usability), and essential terminology.



Internet Crime Current Report: IC3

Source: http://www.ic3.gov

The following is the crime report data from IC3; the **Internet Crime Complaint Center** (IC3) is a partnership among the Federal Bureau of Investigation (**FBI**), the National White Collar Crime Center (**NW3C**), and the Bureau of Justice Assistance (**BJA**). According to IC3, online Internet crime complaints are increasing daily. From the graph, you can observe that in the year **2005**, there were **231,493 crime complaints**, whereas in the year **2009**, complaints drastically increased to **336,655**. When compared to 2009, Internet crime complaints in the year **2011 decreased** to some extent.



Data Breach Investigations Report

Source: http://www.verizonbusiness.com

The data breach investigations report from **Verizon Business** shows the types of hacking by percent of breaches and percent of records. From the report, it is clear that most of the security breaches happening today are because of **hacking**. Therefore, in order to protect yourself from data or **security breaches**, you should test your network security against hacking.

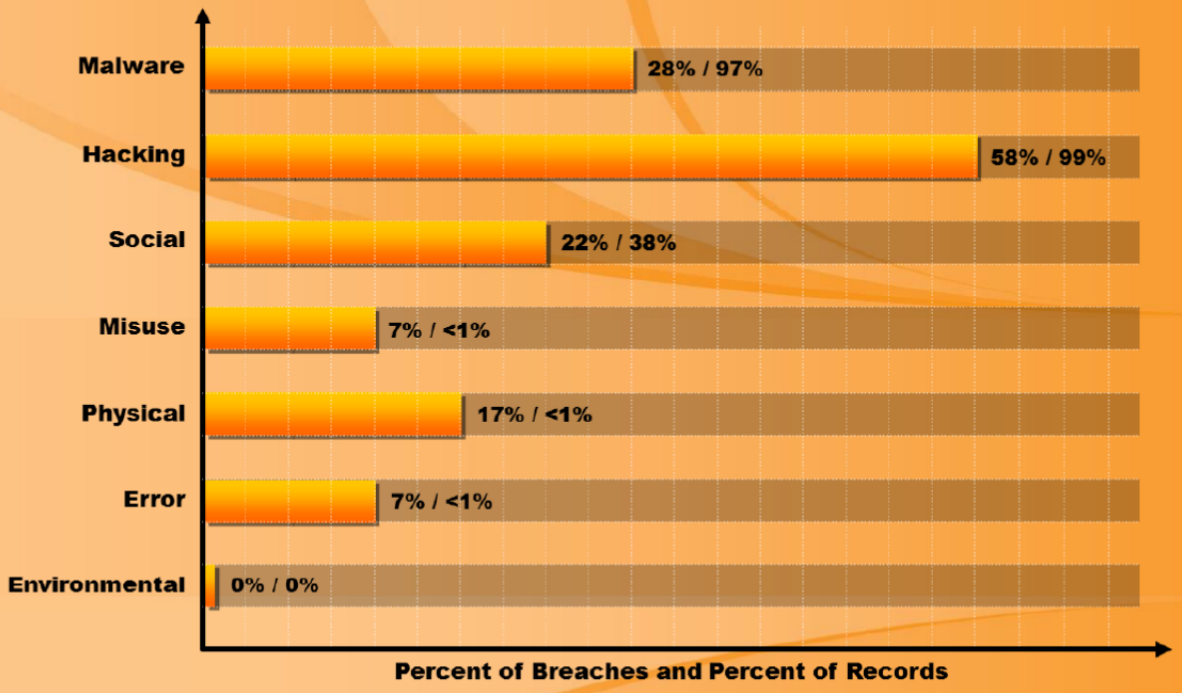


FIGURE 1.1: Data Breach Investigation Report

Essential Terminology

Hack Value

Hack value is the notion among hackers that something is worth doing or is interesting. Hackers might feel that **breaking down** the toughest network security might give them great satisfaction, and that it is something they accomplished that not everyone could do.

Exploit

An exploit is a defined way to **breach** the **security** of an IT system through vulnerability. The term exploit is used when any kind of attack has taken place on a system or network. An exploit can also be defined as **malicious software** or **commands** that can cause unanticipated behavior to occur on **legitimate software** or **hardware** by taking advantage of the vulnerabilities.

Vulnerability

Vulnerability is a **weakness in design** or an **implementation error** that can lead to an unexpected and undesirable event compromising the **security of the system**. In simple words, a vulnerability is **loop hole**, **limitation**, or **weakness** that becomes a source for an attacker to enter into the system by **bypassing** various user authentications.

Target of Evaluation

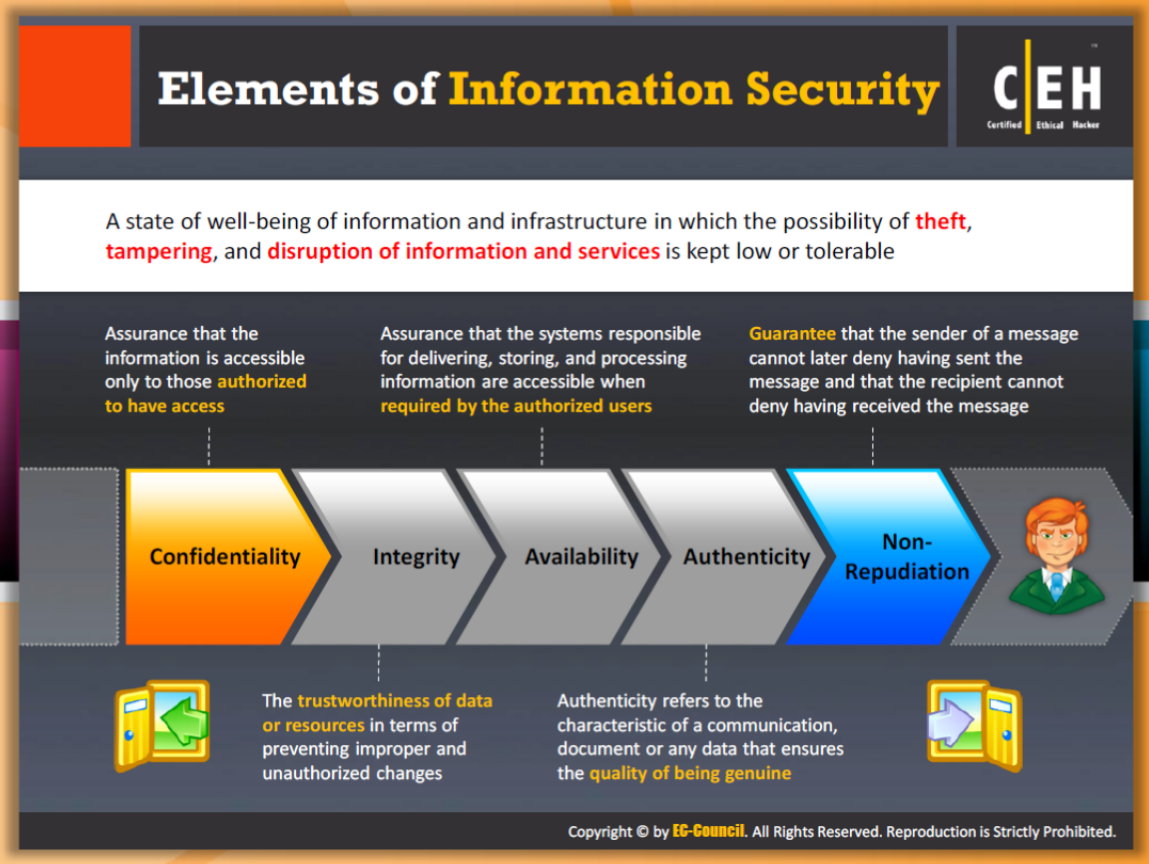
A target of evaluation is an IT system, product, or component that is identified / subjected to a required security evaluation. This kind of evaluation helps the evaluator understand the functioning, technology, and vulnerabilities of a particular system or product.

Zero-day Attack

In a zero-day attack, the **attacker exploits the vulnerabilities** in the computer application before the software developer releases a patch for them.

Daisy Chaining

Attackers who get away with **database theft** usually complete their task and then **backtrack** to cover their tracks by **destroying logs**, etc. The attackers gain control of other systems and use them for malicious activities. It becomes difficult to identify the attacker as they use others' systems to perform illegal activities.



Elements of Information Security

Information security is defined as: "A state of well-being of **information** and **infrastructure** in which the possibility of theft, tampering, and disruption of information and services is kept low or tolerable." It relies on the five major elements of: **confidentiality**, **integrity**, **availability**, **authenticity**, and **non-repudiation**.

Confidentiality

Confidentiality is the assurance that the information is accessible only to those authorized to have access. Confidentiality breaches may occur due to improper data handling or a **hacking attempt**.

Integrity

Integrity is the trustworthiness of data or resources in terms of preventing **improper** and **unauthorized changes**, the assurance that information can be relied upon to be sufficiently accurate for its purpose.

Availability

Availability is the assurance that the systems responsible for delivering, storing, and

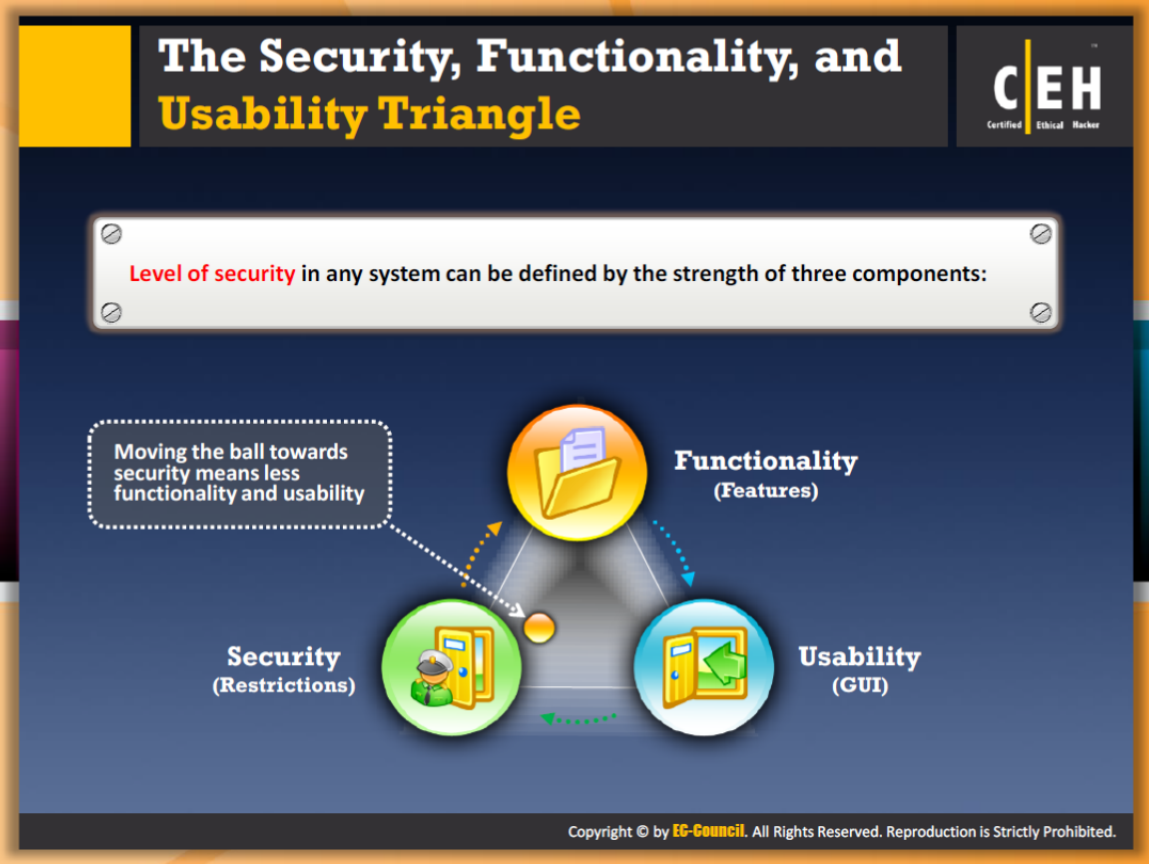
processing information are accessible when required by authorized users.

Authenticity

Authenticity refers to the characteristic of a communication, document, or any data that ensures the **quality** of being **genuine** or not corrupted from the original. The major roles of authentication include confirming that the user is who he or she claims to be and ensuring the message is **authentic** and **not altered** or **forged**. Biometrics, smart cards, and **digital certificates** are used to ensure authenticity of data, transactions, communications, or documents.

Non-repudiation

Non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the **authenticity** of their **signature** on a document or the sending of a message that they originated. It is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.



The Security, Functionality, and Usability Triangle

Technology is evolving at an unprecedented rate. As a result, new products that reach the market tend to be engineered for easy-to-use rather than secure computing. Technology, originally developed for "honest" **research** and **academic purposes**, has not evolved at the same pace as the user's profile. Moreover, during this evolution, system designers often overlook the vulnerabilities during the intended deployment of the system. However, increasing built-in default **security mechanisms** means users have to be more competent. As computers are used for more and more routine activities, it is becoming increasingly difficult for system administrators and other system professionals to allocate resources exclusively for securing systems. This includes time needed to **check log files**, **detect vulnerabilities**, and **apply security update patches**.

Routine activities consume system administrators' time, leaving less time for vigilant administration. There is little time to deploy measures and secure computing resources on a regular and innovative basis. This has increased the demand for dedicated security professionals to constantly monitor and defend **ICT (Information and Communication Technology)** resources.

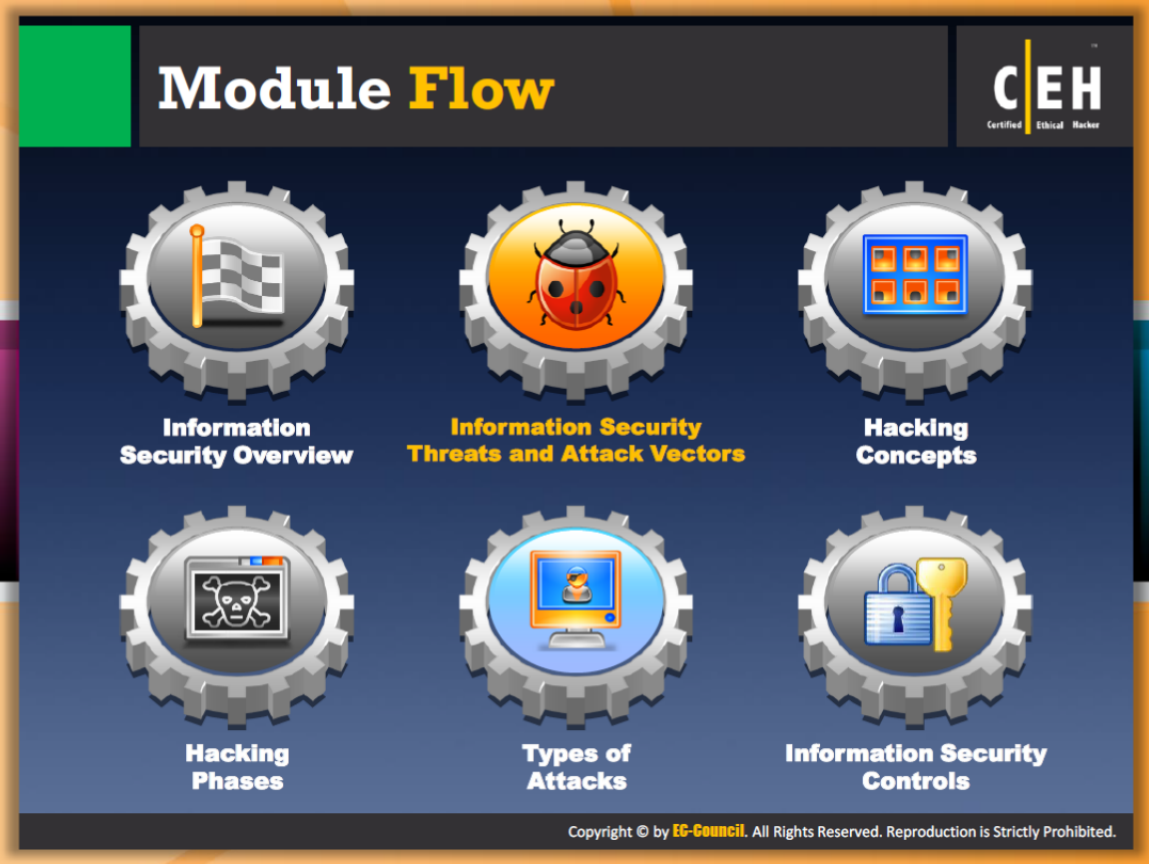
Originally, to "hack" meant to possess extraordinary computer skills to extend the limits of computer systems. Hacking required **great proficiency**. However, today there are automated

tools and codes available on the Internet that make it possible for anyone with a will and desire to hack and succeed.

Mere compromise of the security of a system does not denote success. There are websites that insist on "**taking back the net**" as well as people who believe that they are doing all a favor by posting exploit details. These can act as a detriment and can bring down the skill level required to become a successful attacker.

The ease with which system vulnerabilities can be exploited has increased while the knowledge curve required to perform such exploits has shortened. The concept of the elite/super attacker is an illusion. However, the fast-evolving genre of "**script kiddies**" is largely comprised of lesser-skilled individuals having **second-hand knowledge** of performing exploits. One of the main impediments contributing to the growth of **security infrastructure** lies in the unwillingness of exploited or compromised victims to report the incident for fear of losing the goodwill and faith of their employees, customers, partners, and/or of losing market share. The trend of information assets influencing the market has seen more companies thinking twice before **reporting incidents** to law enforcement for fear of bad press and negative publicity.

The increasingly networked environment, with companies often having their website as a single point of contact across geographical boundaries, makes it critical for administrators to take countermeasures to prevent **exploits** that can result in loss of an important reason why corporations need to invest in **security measures** to protect their information assets.



Module Flow

So far we discussed information security. Now we will discuss **threats** and **attack vectors** of information security.

Information Security Overview	Hacking Phases
Information Security Threats and Attack Vectors	Types of Attacks
Hacking Concepts	Information Security Controls

This section introduces you to top information security attack vectors, the possible **security threats** to valuable information, and the **goals of attackers** who perform attacks on information systems.

Top Information Security Attack Vectors

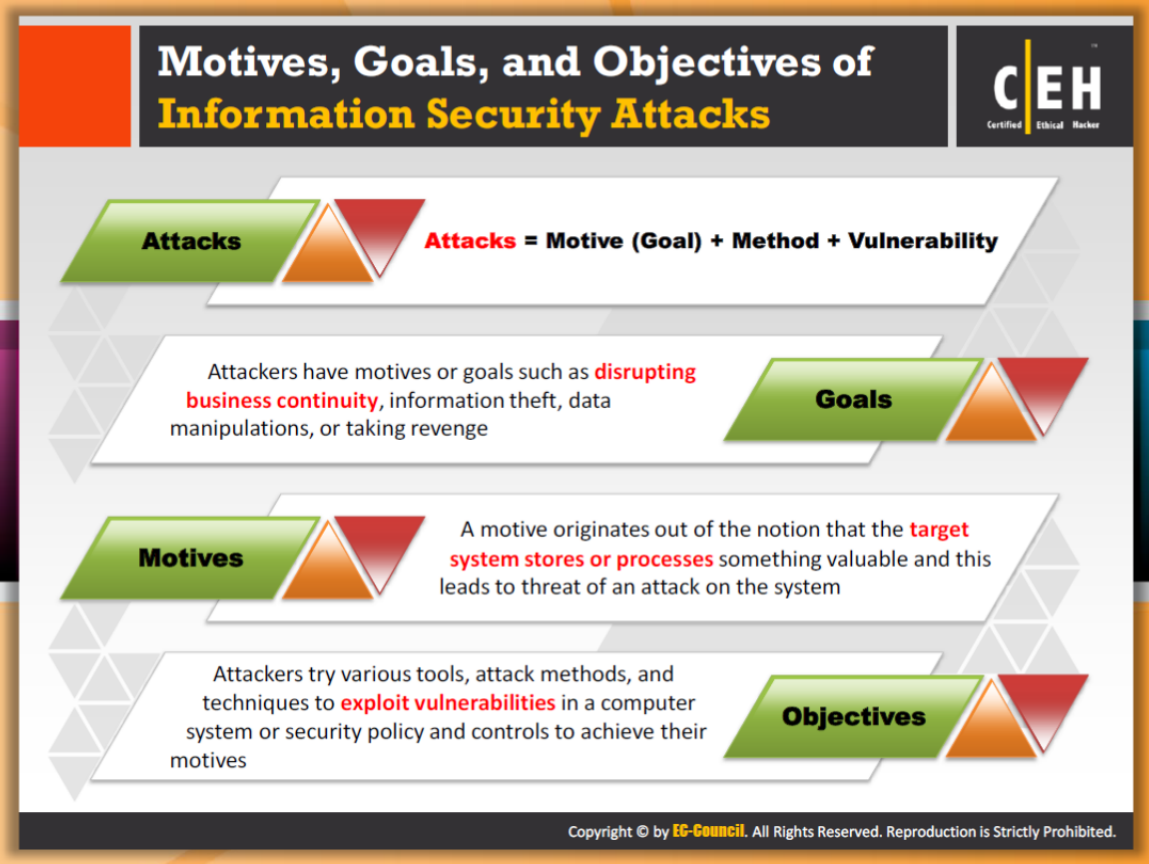
An attack vector is a path or means by which an attacker gains access to an information system to **perform malicious activities**. This attack vector enables an attacker to take advantage of the vulnerabilities present in the **information system** in order to carry out a particular attack.

Although there are some **traditional attacks vectors** from which attack can be performed, attack vectors come in many forms; one cannot predict in which form an attack vector can come.

The following are the **possible top attack vectors** through which attackers can attack information systems:

- Virtualization and Cloud Computing
- Organized Cyber Crime
- **Unpatched Software**
- Targeted Malware
- Social Networking
- Insider Threats

- **Botnets**
- Lack of Cyber Security Professionals
- Network Applications
- Inadequate Security Policies
- Mobile Device Security
- Compliance with Govt. Laws and Regulations
- Complexity of Computer Infrastructure
- **Hacktivism**



Motives, Goals, and Objectives of Information Security Attacks

Attackers generally have motives or **goals or objectives** behind performing information security attacks. It may be to disrupt the **business continuity** of the target organization, to **steal** valuable **information**, for the sake of **curiosity**, or even to take **revenge** on target organization. Therefore, these motives or goals depend on the attacker's state of mind, for what reason he or she is carrying out such an activity. Once, the attacker determines his/her **goal**, he or she can accomplish the goal by adopting various techniques to exploit vulnerabilities in an **information system** or **security policy** and controls.

Information Security Threats

Information security threats are broadly classified into **three** categories, as follows:

Natural Threats

Natural threats include **natural disasters** such as earthquakes, hurricanes, floods, or any **nature-created disaster** that cannot be stop. Information damage or lost due to natural threats cannot be prevented as no one knows in advance that these types of threats will occur. However, you can implement a few **safeguards** against natural disasters by adopting **disaster recovery plans** and **contingency plans**.

Physical Security Threats

Physical threats may include loss or damage of **system resources** through fire, water, theft, and **physical impact**. Physical impact on resources can be due to a **collision** or other damage, either intentionally or unintentionally. Sometimes, power may also damage hardware used to store information.

Human Threats

Human threats include threats of attacks performed by **both insiders and outsiders**.

Insider attacks refer to attacks performed by **disgruntled** or malicious **employees**. Outsider attacks refer to attacks performed by **malicious people** not within the organization. **Insider** attackers can be the **biggest threat** to information system as they may know the **security posture** of the information system, while **outsider** attackers apply many tricks such as **social engineering** to learn the security posture of the information system.

Information Security Threats (Cont'd)

Human threats can be further classified into **three types**, as follows:

Network Threats

A network is defined as the **collection of computers and other hardware** connected by communication channels to share resources and information. As the information travels from one computer to the other through the **communication channel**, a malicious person may break into the communication channel and **steal** the **information** traveling over the network. The attacker can impose various threats on a target network:

- Information gathering
- Sniffing and eavesdropping
- **Spoofing**
- Session hijacking and man-in-the-middle attacks
- SQL injection
- **ARP Poisoning**
- Password-based attacks

- Denial of service attack
- Compromised-key attack

Host Threats

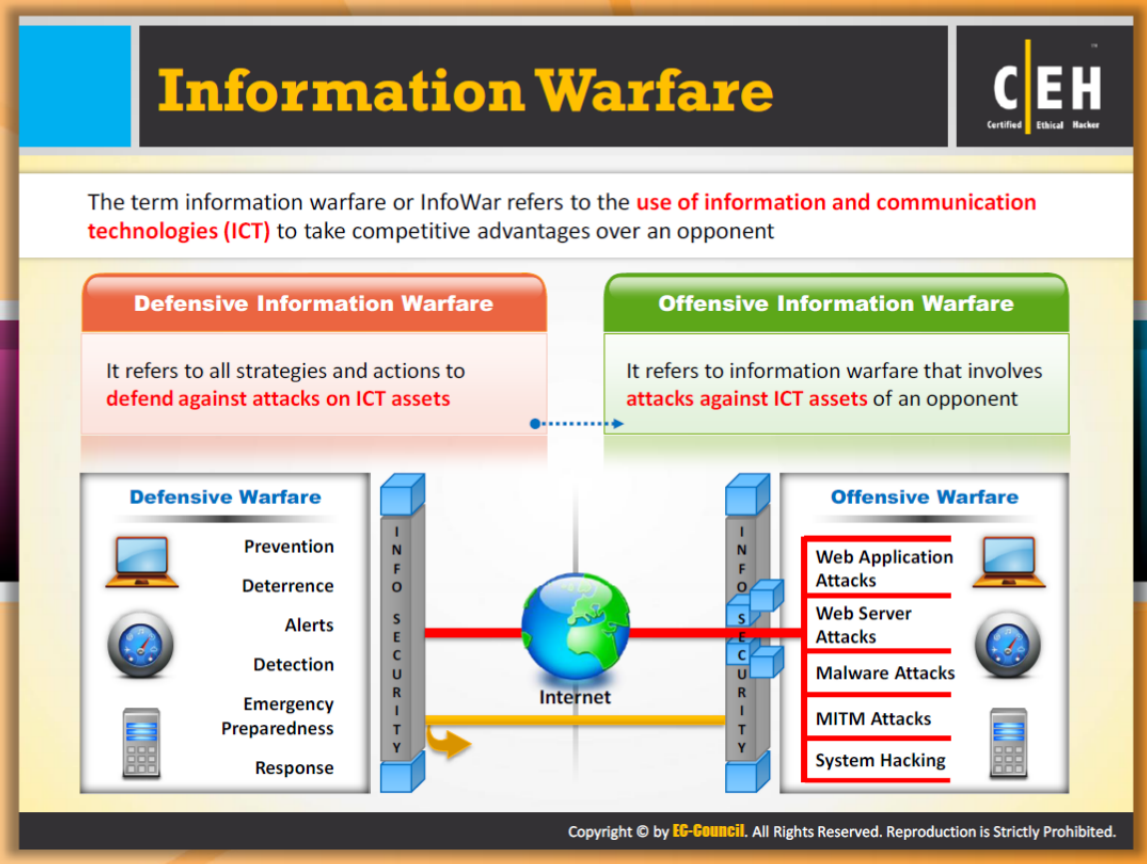
Host threats are directed at a particular system on which valuable information resides. Attackers try to breach the security of the information system resource. The following are possible threats to the host:

- Malware attacks
- Target Footprinting
- Password attacks
- Denial of service attacks
- Arbitrary code execution
- Unauthorized access
- Privilege escalation
- Back door Attacks
- Physical security threats

Application Threats

If the proper security measures are not considered during development of the particular application, the application might be vulnerable to different types of application attacks. Attackers take advantage of vulnerabilities present in the application to steal or damage the information. The following are possible threats to the application:

- Data/Input validation
- Authentication and Authorization attacks
- Configuration management
- Information disclosure
- Session management issues
- Buffer overflow issues
- Cryptography attacks
- Parameter manipulation
- Improper error handling and exception management
- Auditing and logging issues



Information Warfare

The term information warfare or **InfoWar** refers to the use of information and **communication technologies** (**ICT**) to take **competitive advantages** over an opponent.

Defensive Information Warfare: It refers to all strategies and actions to defend against attacks on ICT assets.

Offensive Information Warfare: It refers to information warfare that involves attacks against **ICT assets** of an opponent.

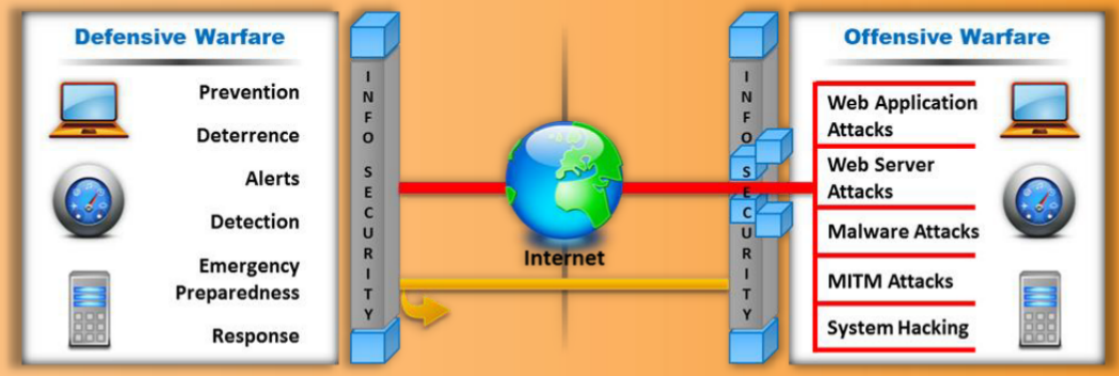
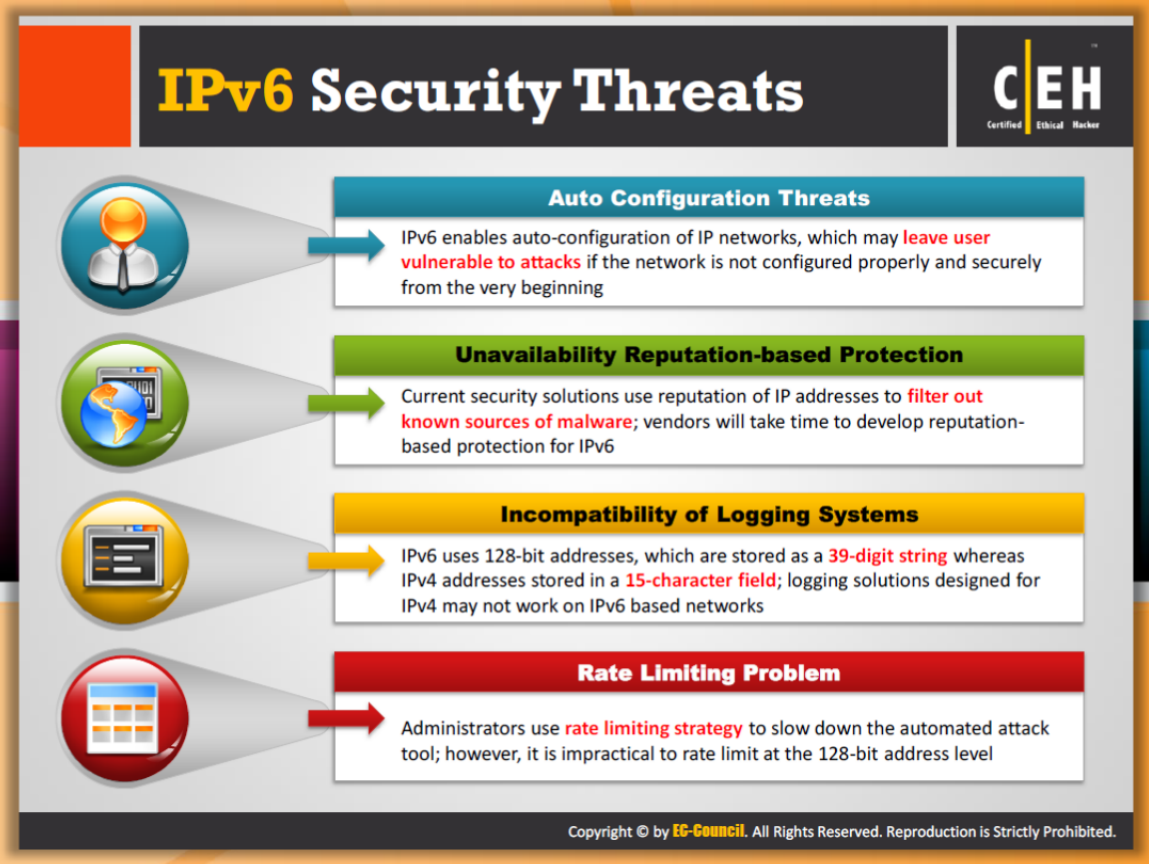


FIGURE 1.2: Defensive and Offensive Warfare Diagram



IPv6 Security Threats

Compared to IPv4, IPv6 has an **improved security** mechanism that assures a higher level of security and confidentiality for the information transferred over a network. However, IPv6 is still vulnerable. It still possesses information security threats that include:

Auto Configuration Threats

IPv6 enables auto-configuration of IP networks, which may leave user vulnerable to attacks if the network is not configured properly and securely from the beginning.

Unavailability Reputation-based Protection

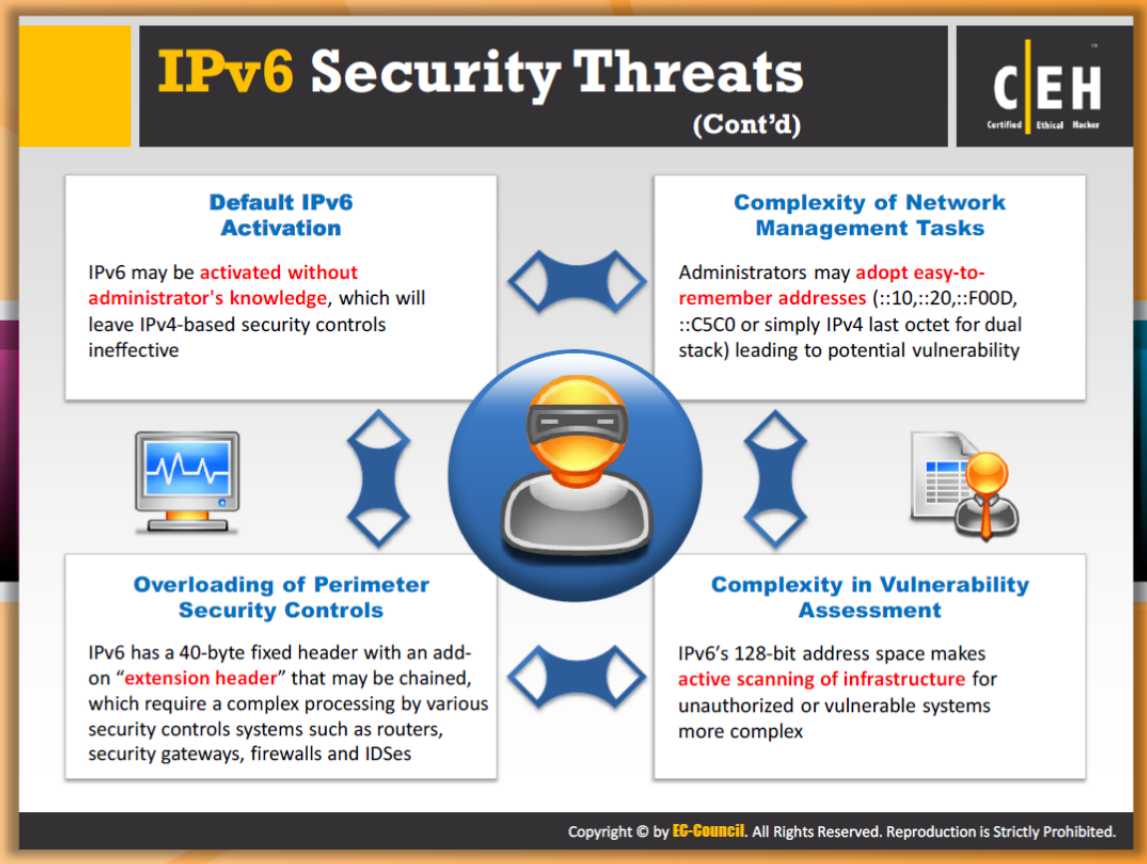
Current security solutions use the reputation of IP addresses to filter out known sources of malware; vendors will take time to develop **reputation-based protection** for IPv6.

Incompatibility of Logging Systems

IPv6 uses 128-bit addresses, which are stored as a **39-digit string**, whereas IPv4 addresses are stored in a **15-character** field; logging solutions designed for IPv4 may not work on IPv6-based networks.

Rate Limiting Problem

Administrators use a rate limiting strategy to slow down the automated attack tool; however, it is impractical to rate limit at the 128-bit address level.



IPv6 Security Threats (Cont'd)

You may also find the following threats when using IPv6:

Default IPv6 Activation

IPv6 may be activated without the administrator's knowledge, which will leave IPv4-based security controls ineffective.

Complexity of Network Management Tasks

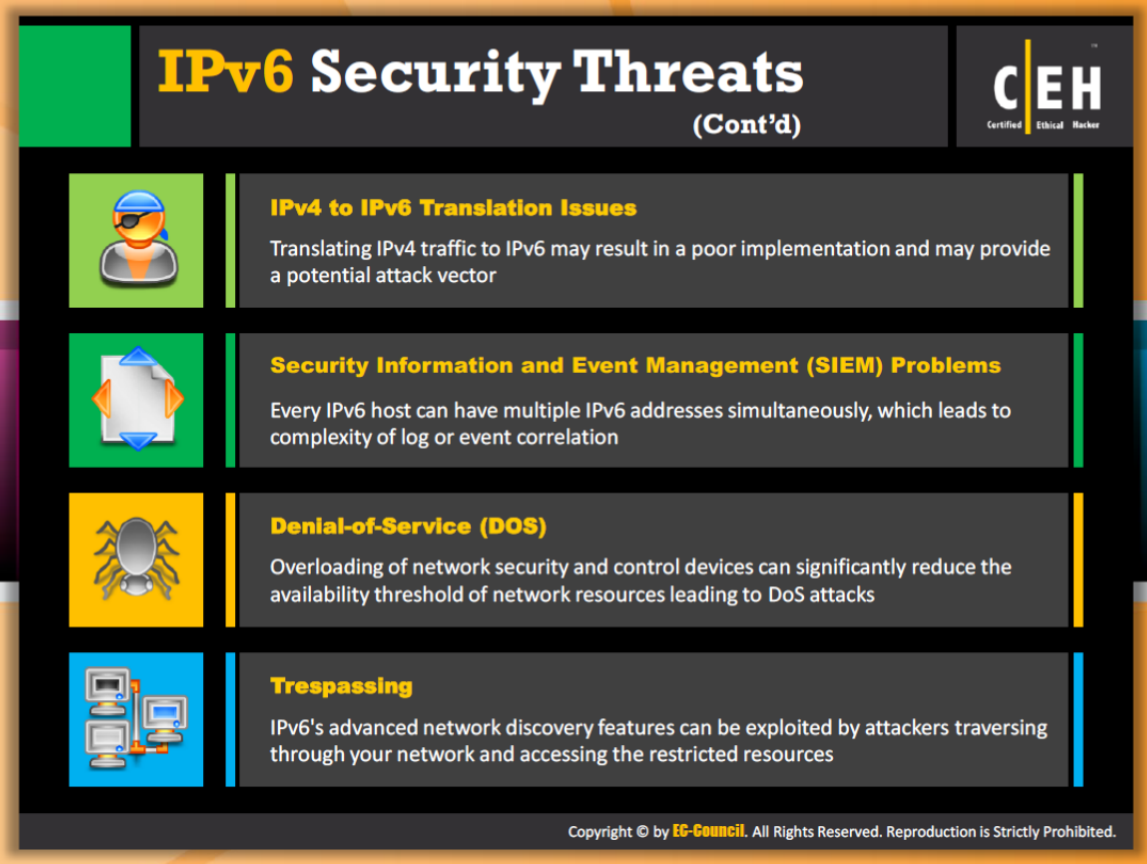
Administrators may adopt **easy-to-remember** addresses (`::10`,`::20`,`::F00D`, `::C5C0` or simply **IPv4 last octet** for dual stack) leading to a potential vulnerability.

Complexity in Vulnerability Assessment

IPv6's **128-bit address space** makes active scanning of infrastructure for unauthorized or vulnerable systems more complex.

Overloading of Perimeter Security Controls

IPv6 has a **40-byte** fixed header with an add-on "**extension headers**" that may be chained, which requires complex processing by various **security controls** systems such as **routers**, security **gateways**, firewalls, and **IDS**.



IPv6 Security Threats (Cont'd)

The following IPv6 security threats can also cause **serious damage** to your network:

IPv4 to IPv6 Translation Issues

Translating IPv4 traffic to IPv6 may result in **poor implementation** and may provide a potential attack vector.

Security Information and Event Management (SIEM) Problems

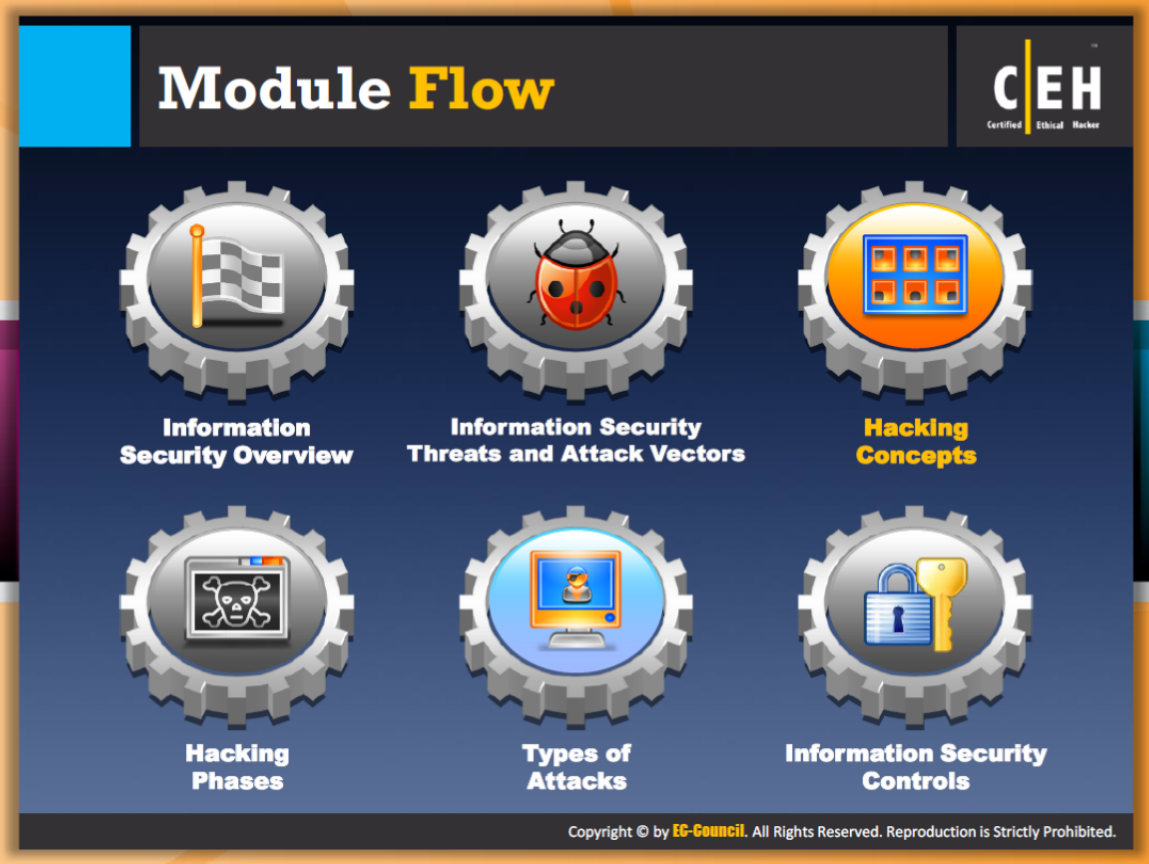
Every IPv6 host can have multiple IPv6 addresses simultaneously, which leads to **complexity** of **log** or **event correlation**.

Denial-of-service (DOS)

Overloading of network security and **control devices** can significantly reduce the availability threshold of network resources, leading to DoS attacks.

Trespassing

IPv6's advanced network discovery features can be exploited by attackers who can traverse through your network and access the **restricted resources**.

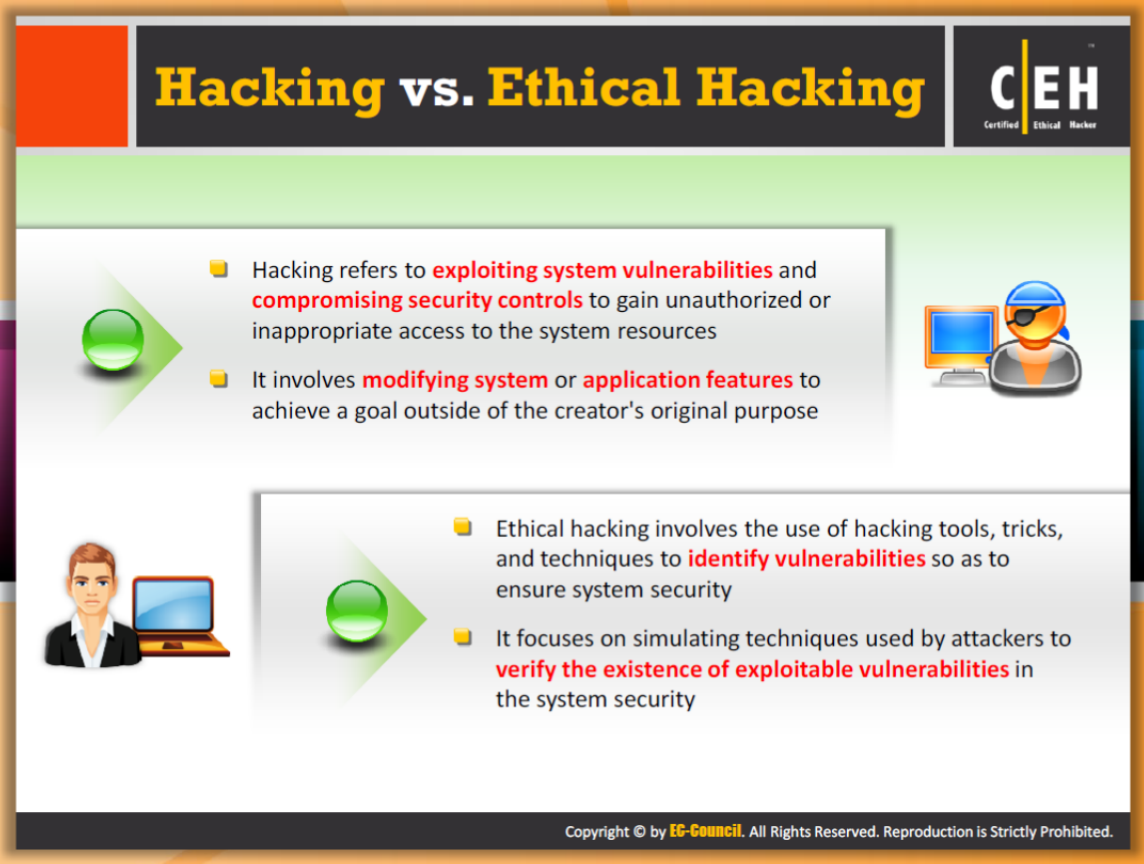


Module Flow

So far we have discussed **information security**, its **threats** and attack vectors. Now we will discuss how an attacker compromises information security with the help of **attack vectors**.

Information Security Overview	Hacking Phases
Information Security Threats and Attack Vectors	Types of Attacks
Hacking Concepts	Information Security Controls

This section will familiarize you with the **concept of ethical hacking**, how it differs from hacking, the **effects** of hacking activities on business, and different **classes of attackers**.



Hacking vs. Ethical Hacking

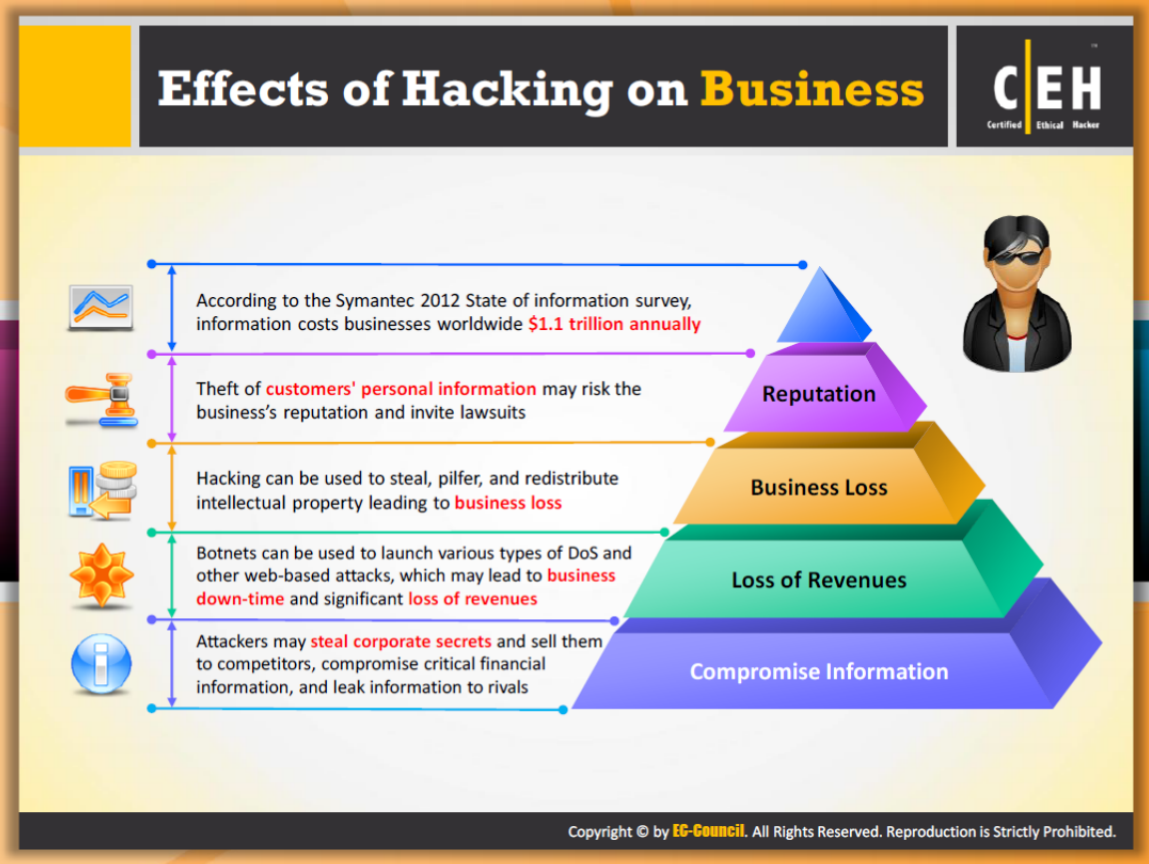
Most people do not understand the difference between hacking and ethical hacking. These two terms can be differentiated on the basis of the **intentions of** the **people** who are performing hacking activity. However, understanding the true intentions of hackers can be quite difficult.

Hacking

Hacking refers to exploiting system vulnerabilities and **compromising security controls** to gain **unauthorized** or inappropriate **access** to the system resources. It involves modifying system or application features to achieve a goal outside of the creator's original purpose.

Ethical Hacking

Ethical hacking involves the use of **hacking tools**, tricks, and techniques to identify **vulnerabilities** so as to ensure system security. It focuses on simulating techniques used by attackers to verify the existence of exploitable vulnerabilities in the **system security**.



Effects of Hacking on Business

According to the Symantec 2012 State of Information survey, information costs businesses worldwide **$1.1 trillion annually**. Every business must provide **strong security** for its customers; otherwise the business may put its reputation at stake and may even face lawsuits. Attackers use **hacking techniques** to steal, pilfer, and redistribute intellectual property of businesses and in turn to make financial gain. Attackers may profit, but the victim's business must face **huge financial losses** and may even lose its reputation.

Once an attacker gains control over the user's system, he or she can access all the files that are stored on the computer, including personal or corporate financial information, credit card numbers, and client or customer data stored on that system. If any such information falls into the wrong hands, it may create chaos in the normal functioning of an organization. Organizations must provide a strong security to its critical information sources containing customer data and its upcoming releases or ideas. If the data is altered or stolen, a company may lose credibility and the trust of its customers. In addition to the potential financial loss that may occur, the loss of information may cause a business to lose a crucial competitive advantage over its rivals. Sometimes attackers use **botnets** to launch various types of **DoS** and other **web-based attacks**. This causes the target business services to go down, which in turn may lead to loss of revenues.

There are many things that businesses can do to protect themselves and their assets. Knowledge is a key component in addressing this issue. Assessment of the risk prevalent in a business and how attacks could potentially affect that business is paramount from a security point of view. One does not have to be a security expert to recognize the damage that can occur when a company is victimized by an attacker. By understanding the problem and empowering employees to facilitate **protection** against attacks, the company would be able to deal with any **security issues** as they arise.

Who Is a Hacker?

A hacker is a person who **illegally breaks** into a **system** or **network** without any authorization to destroy, steal sensitive data, or perform malicious attacks. Hackers may be motivated by a multitude of **reasons**:

- Intelligent individuals with excellent computer skills, with the ability to create and explore the computer's software and hardware
- For some hackers, hacking is a **hobby** to see how many computers or networks they can compromise
- Their intention can either be to **gain knowledge** or to **poke** around doing illegal things
- Some hack with malicious intent, such as **stealing business data**, **credit card information**, **social security numbers**, email **passwords**, etc.

Hacker Classes

Hackers are mainly divided into eight classes:

Black Hats

Black hats are individuals with **extraordinary computing skills**, resorting to malicious or destructive activities and are also known as crackers. These individuals mostly use their skills for only destructive activities, causing huge losses for companies as well as individuals. They use their skills in finding vulnerabilities in the various networks including defense and government websites, banking and finance, etc. Some do it to cause damage, steal information, destroy data, or earn money easily by **hacking IDs** of bank customers.

White Hats

White hats are individuals who possess hacking skills and use them for defensive purposes; they are also known as **security analysts**. These days, almost every company has security analysts to defend their systems against the malicious attacks. White hats help companies secure their networks from outside intruders.

Gray Hats

Gray hats are the individuals who work both **offensively** and **defensively** at various times. Gray hats fall between white and black hats. Gray hats might help hackers by finding various vulnerabilities of a system or network and at the same time help vendors to improve products (software or hardware) by checking limitations and making them more secure, etc.

Suicide Hackers

Suicide hackers are individuals who aim to bring down critical infrastructure for a "**cause**" and are not worried about facing 30 years in jail for their actions. Suicide hackers are closely related to suicide bombers, who sacrifice their life for the attack and are not concerned with the consequences of their actions. There has been a rise in cyber terrorism in recent years.

Script Kiddies

Script kiddies are the **unskilled hackers** who compromise systems by running scripts, tools, and software developed by real hackers. They utilize small, **easy-to-use programs** or scripts as well as distinguished techniques to find and exploit the vulnerabilities of a machine. Script kiddies usually focus on the quantity of attacks rather than the quality of the attacks that they initiate.

Spy Hackers

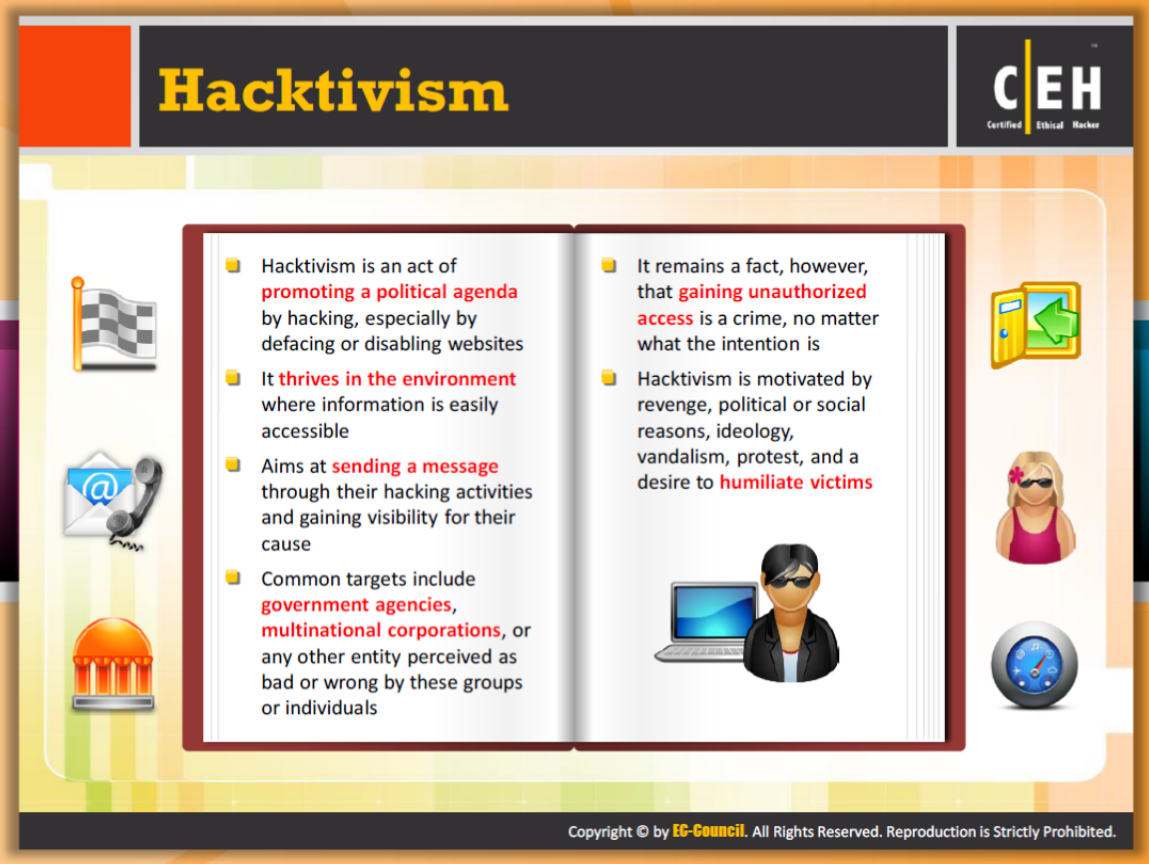
Spy hackers are individuals who are employed by an organization to penetrate and gain trade secrets of the competitor. These insiders can take advantage of the privileges they have to hack a **system or network**.

Cyber Terrorists

Cyber terrorists could be **people**, **organized groups** formed by terrorist organizations, that have a wide range of skills, motivated by religious or political beliefs, to create fear by **large-scale disruption of computer networks**. This type of hacker is more dangerous as they can hack not only a website but whole Internet zones.

State Sponsored Hackers

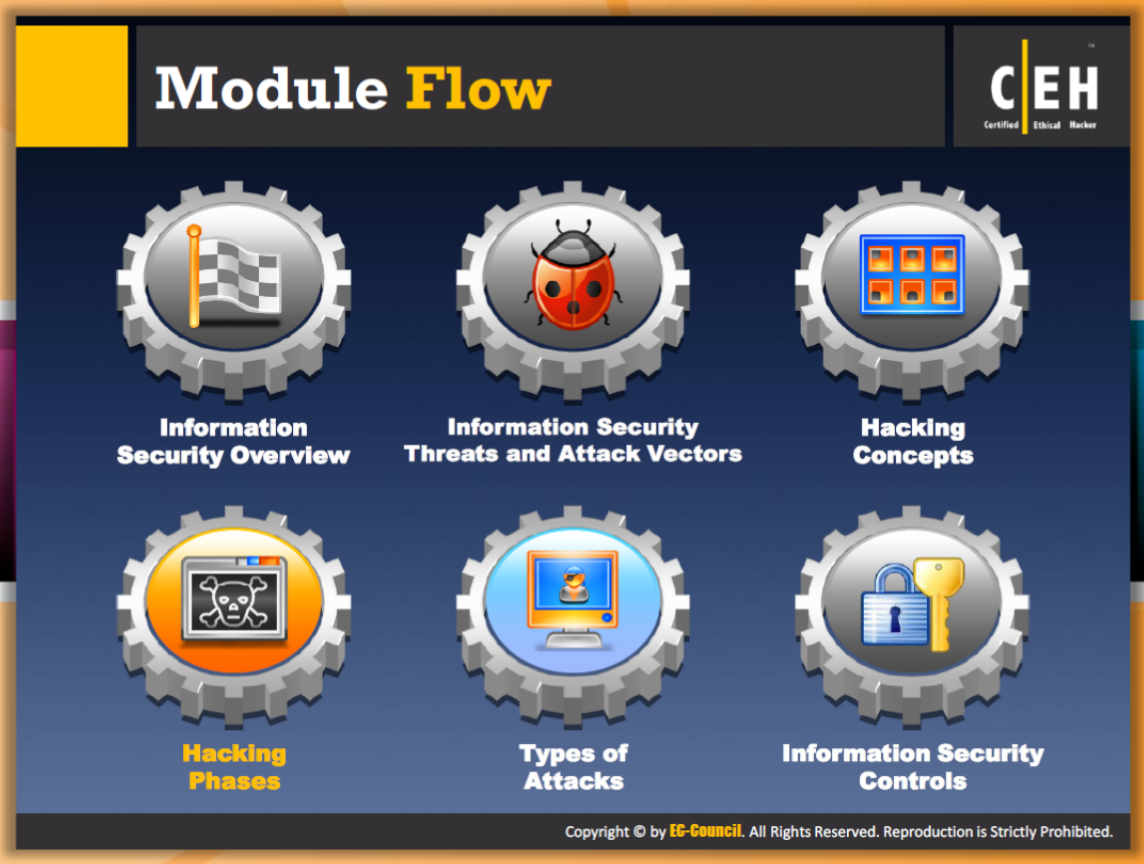
State sponsored hackers are individuals employed by the government to penetrate and gain top-secret information and to **damage information systems** of other governments.



Hacktivism

Hacktivism is an act of promoting a **political agenda** by **hacking**, especially by defacing or disabling websites. The person who does these things is known as a hacktivist.

- Hacktivism thrives in an environment where information is **easily accessible**
- It aims to send a message through hacking activities and gain visibility for a cause.
- Common targets include government agencies, multinational corporations, or any other entity perceived as "**bad**" or "**wrong**" by these groups or individuals.
- It remains a fact, however, that gaining **unauthorized access** is a crime, no matter what the intention is.
- **Hacktivism** is motivated by revenge, **political** or **social** reasons, **ideology**, **vandalism**, protest, and a desire to humiliate victims.

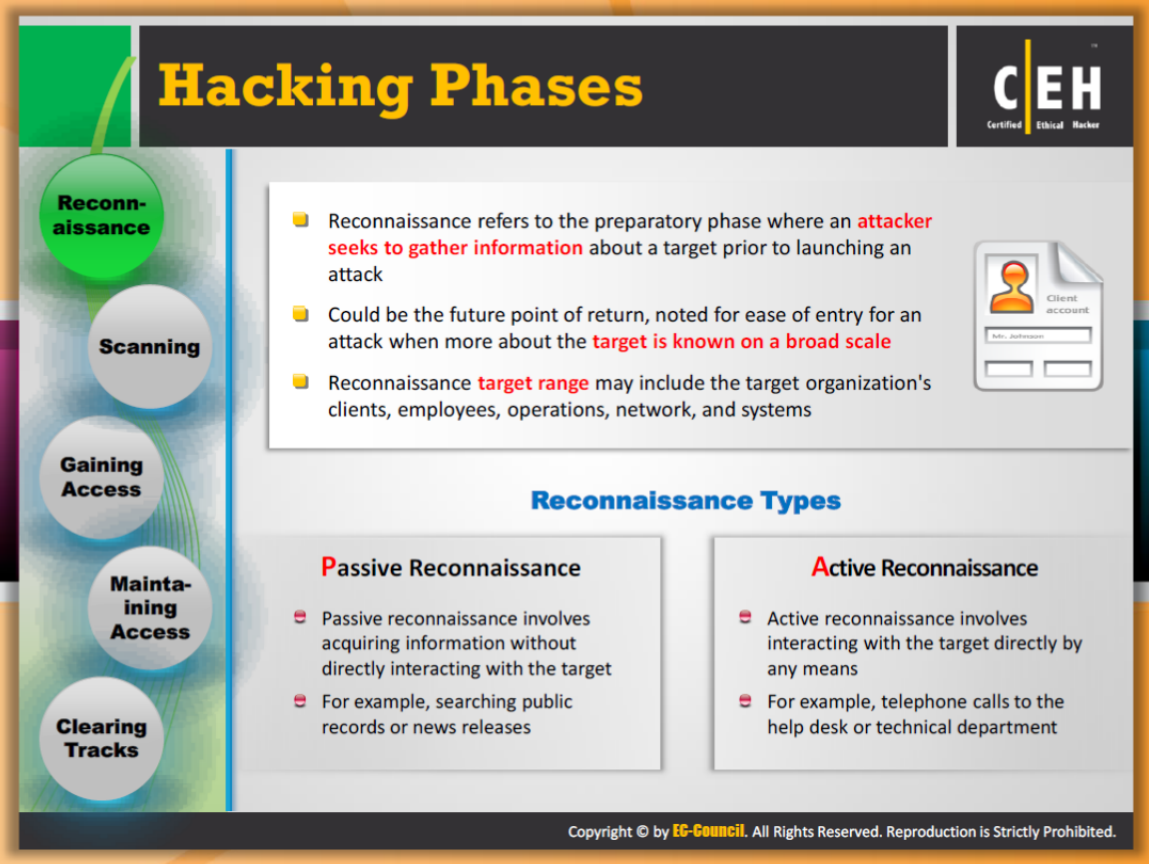


Module Flow

In the previous section, you learned about various hacking concepts. Now it's time to discuss the **hacking method**. Hacking cannot be accomplished in a single action. It needs to be done in phases. The information gathered or the privileges gained in one phase can be used in the next phase for advancing the process of hacking.

Information Security Overview	Hacking Phases
Information Security Threats and Attack Vectors	Types of Attacks
Hacking Concepts	Information Security Controls

This section lists and describes various phases involved in hacking.



Hacking Phases

The various phases involved in hacking are:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Reconnaissance

Reconnaissance refers to the preparatory phase where an attacker **gathers** as much **information** as possible about the target prior to launching the attack. Also in this phase, the attacker draws on competitive intelligence to learn more about the target. This phase may also involve network scanning, either external or internal, without authorization.

This is the phase that allows the **potential attacker** to strategize his or her attack. This may take some time as the attacker waits to unearth crucial information. Part of this reconnaissance may

involve "**social engineering**." A social engineer is a person who smooth-talks people into revealing information such as unlisted phone numbers, passwords, and other sensitive data.

Another reconnaissance technique is "**dumpster diving**." Dumpster diving is the process of looking through an organization's trash for discarded sensitive information. Attackers can use the Internet to obtain information such as employee's contact information, business partners, technologies in use, and other critical business knowledge, but "dumpster diving" may provide them with even more sensitive information such as usernames, passwords, credit card statements, bank statements, ATM slips, social security numbers, telephone numbers, and so on. The reconnaissance target range may include the target organization's clients, employees, operations, networks, and systems.

For example, a **Whois database** can provide information about Internet addresses, domain names, and contacts. If a potential attacker obtains **DNS information** from the registrar, and is able to access it, he or she can obtain useful information such as the mapping of domain names to IP addresses, mail servers, and host information records. It is important that a company has appropriate policies to protect its information assets, and also provide guidelines to its users of the same. Building user awareness of the precautions they must take in order to protect their information assets is a critical factor in this context.

Reconnaissance Types

Reconnaissance techniques can be categorized broadly into active and passive reconnaissance.

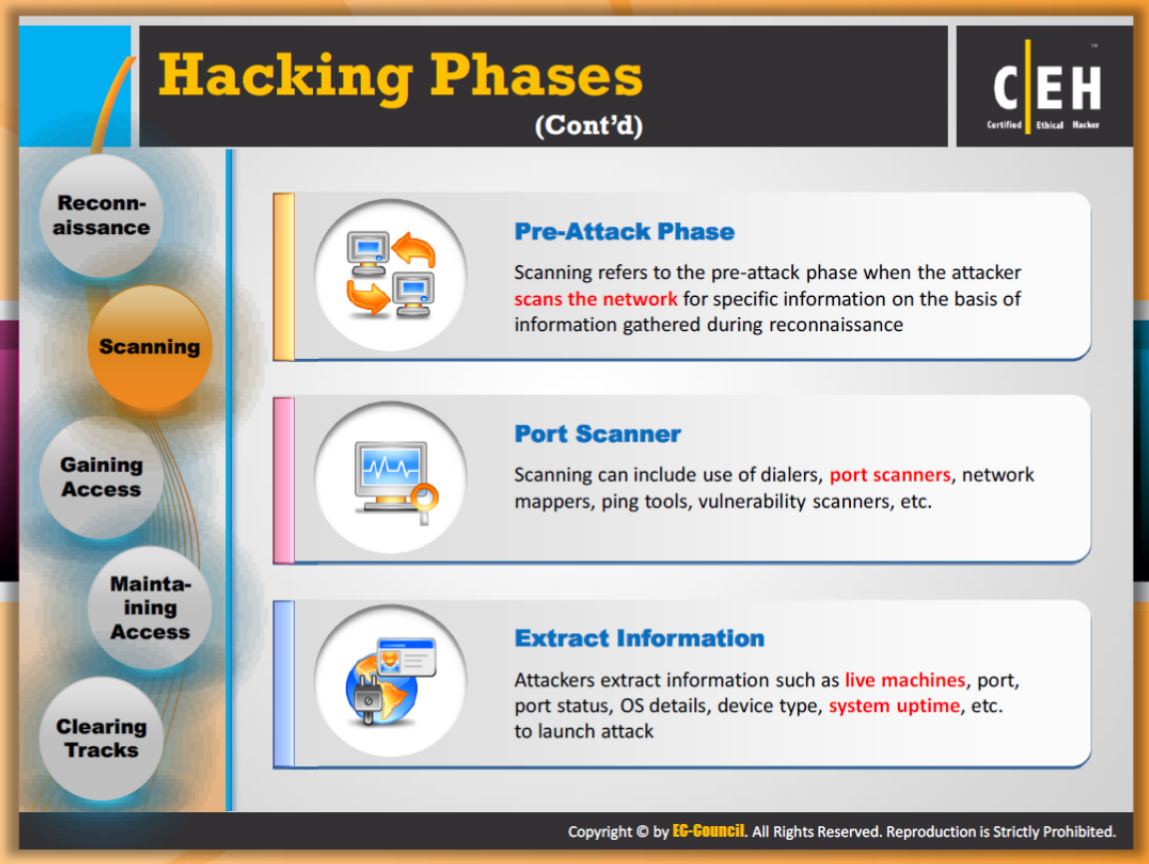
When an attacker approaches the attack using **passive reconnaissance** techniques, he or she does not interact with the system directly. The attacker uses publicly available information, social engineering, and dumpster diving as a means of gathering information.

When an attacker employs active reconnaissance techniques, he or she tries to interact with the system by using tools to detect open ports, accessible hosts, router locations, network mapping, details of operating systems, and applications.

The next phase of **attacking is scanning**, which is discussed in the following section. Some experts do not differentiate scanning from active reconnaissance. However, there is a slight difference as scanning involves more in-depth probing on the part of the attacker. Often reconnaissance and scanning phases overlap, and it is not always possible to demarcate these phases as watertight compartments.

Active reconnaissance is usually employed when the attacker discerns that there is a low probability that these reconnaissance activities will be detected. Newbies and script kiddies are often found attempting this to get faster, visible results, and sometimes just for the brag value they can obtain.

As an ethical hacker, you must be able to distinguish among the various reconnaissance methods, and be able to advocate preventive measures in the light of potential threats. Companies, for their part, must address security as an integral part of their business and/or operational strategy, and be equipped with **proper policies** and procedures to check for such activities.



Hacking Phases (Cont'd)

Scanning

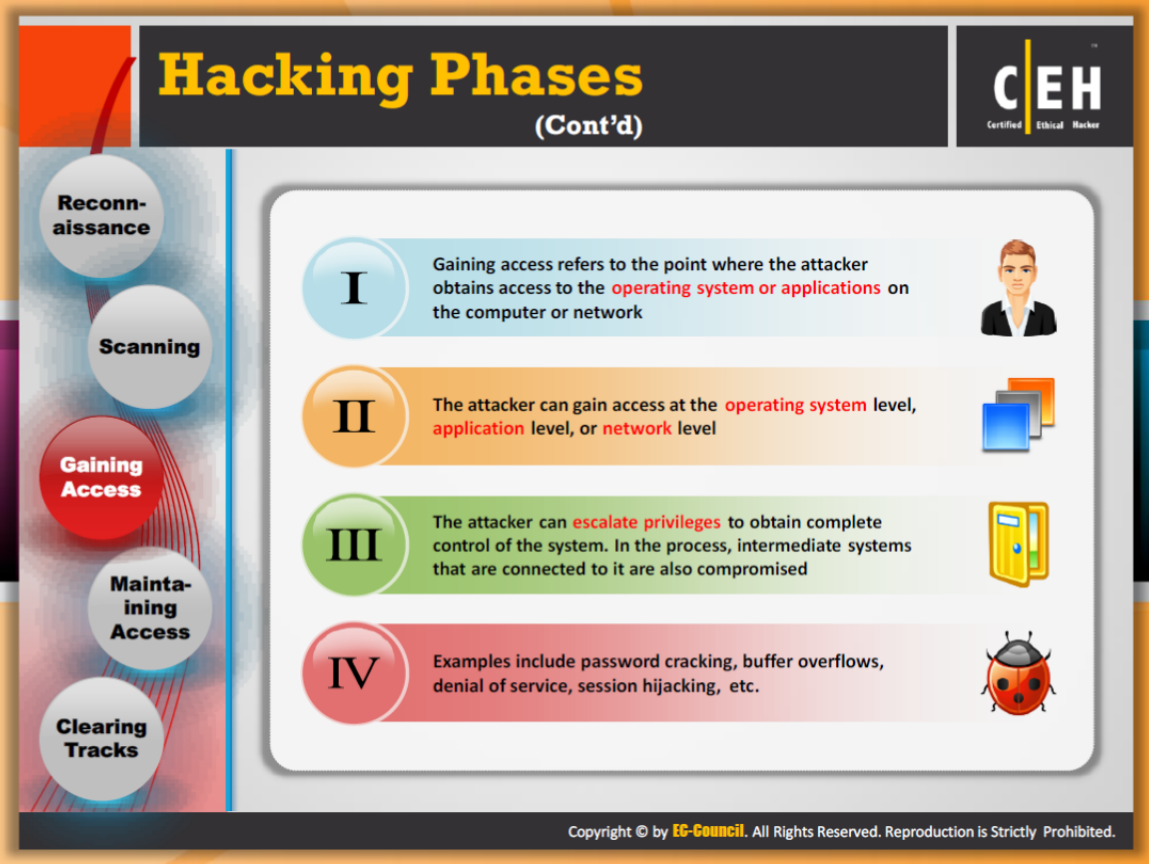
Scanning is what an attacker does prior **to attacking the network**. In scanning, the attacker uses the details gathered during reconnaissance to identify specific vulnerabilities. Scanning can be considered a logical extension (and overlap) of the active reconnaissance. Often attackers use automated tools such as **network/host scanners** and war dialers to locate systems and attempt to discover vulnerabilities.

An attacker can gather critical network information such as the mapping of systems, routers, and firewalls by using simple tools such as **Traceroute**. Alternatively, they can use tools such as Cheops to add sweeping functionality along with what Traceroute renders.

Port scanners can be used to detect listening ports to find information about the nature of services running on the target machine. The primary defense technique in this regard is to shut down services that are not required. Appropriate filtering may also be adopted as a defense mechanism. However, attackers can still use tools to determine the rules implemented for filtering.

The most commonly used tools are vulnerability scanners that can search for several known vulnerabilities on a target network, and can potentially detect thousands of vulnerabilities. This gives the attacker the advantage of time because he or she only has to find a single means of

entry while the systems professional has to secure many vulnerable areas by applying patches. Organizations that deploy **intrusion detection systems (IDSes)** still have reason to worry because attackers can use evasion techniques at both the application and network levels.



Hacking Phases (Cont'd)

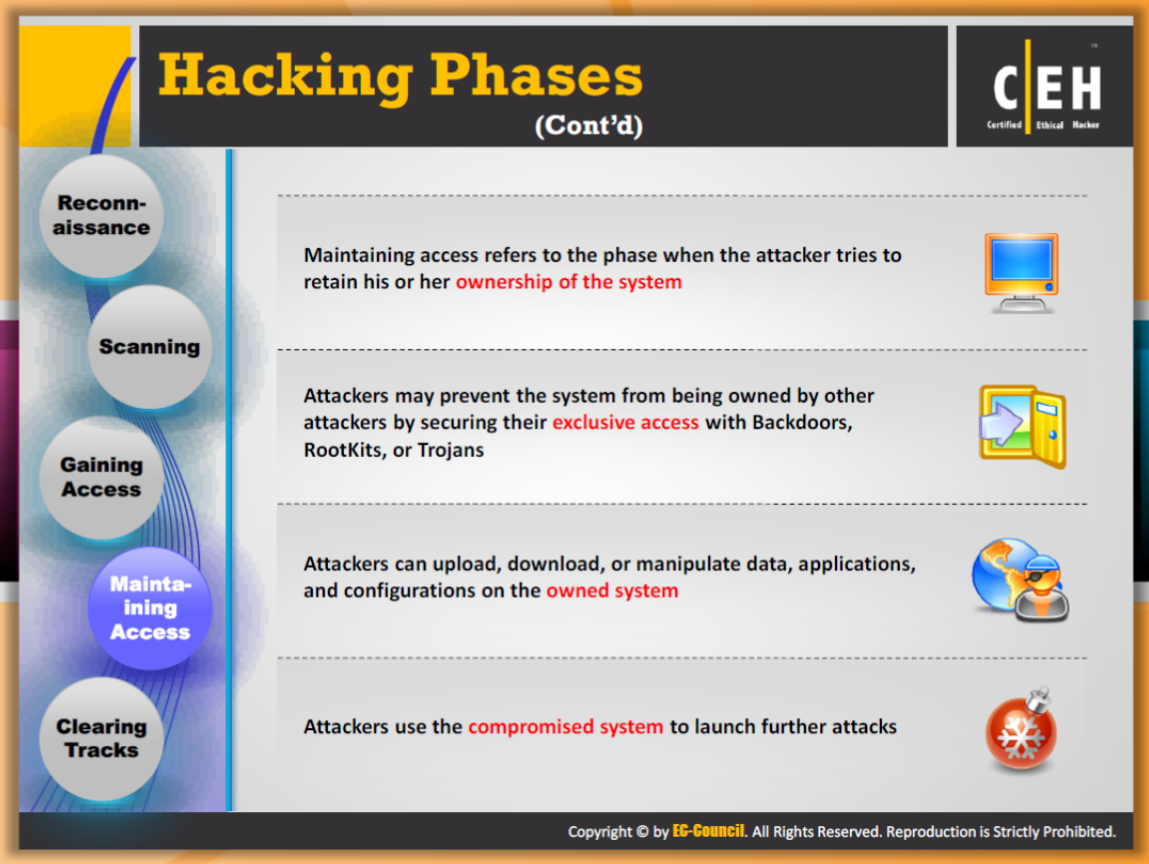
Gaining Access

Gaining access is the most important phase of an attack in terms of **potential damage**. Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network. The attacker can gain access at the operating system level, application level, or network level. Factors that influence the chances of an attacker gaining access into a target system include the **architecture** and **configuration** of the target system, the skill level of the perpetrator, and the initial level of access obtained. The attacker initially tries to gain minimal access to the target system or network. Once he or she gains the access, he or she tries to escalate privileges to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised.

Attackers need not always gain access to the system to cause damage. For instance, denial-of-service attacks can either exhaust resources or stop services from running on the target system. Stopping of service can be carried out by killing processes, using a **logic/time bomb**, or even reconfiguring and crashing the system. Resources can be exhausted locally by filling up outgoing communication links.

The exploit can occur locally, offline, over a **LAN** or the **Internet** as a deception or theft. Examples include stack-based buffer overflows, denial-of-service, and session hijacking.

Attackers use a technique called spoofing to exploit the system by pretending to be strangers or different systems. They can use this technique to send a malformed packet containing a bug to the target system in order to exploit vulnerability. Packet flooding may be used to remotely stop availability of the essential services. **Smurf attacks** try to elicit a response from the available users on a network and then use their legitimate address to flood the victim.



Hacking Phases (Cont'd)

Maintaining Access

Once an attacker gains access to the **target system**, the attacker can choose to use both the system and its resources and further use the system as a launch pad to scan and exploit other systems, or to keep a low profile and continue exploiting the system. Both these actions can damage the organization. For instance, the attacker can implement a sniffer to capture all network traffic, including telnet and ftp sessions with other systems.

Attackers, who choose to remain **undetected**, remove evidence of their entry and use a backdoor or a Trojan to gain repeat access. They can also install rootkits at the kernel level to gain super user access. The reason behind this is that rootkits gain access at the operating system level while a **Trojan horse** gains access at the application level. Both rootkits and Trojans depend on users to install them. Within **Windows systems**, most Trojans install themselves as a service and run as local system, which has administrative access.

Attackers can use **Trojan horses** to transfer **user names**, **passwords**, and even **credit card information** stored on the system. They can maintain control over their system for a long time by "**hardening**" the system against other attackers, and sometimes, in the process, do render some degree of protection to the system from other attacks. They can then use their access to steal data, consume CPU cycles, and trade sensitive information or even resort to extortion.

Organizations can use **intrusion detection systems** or deploy **honeypots** and **honeynets** to detect intruders. The latter though is not recommended unless the organization has the required security professional to leverage the concept for protection.

Hacking Phases (Cont'd)

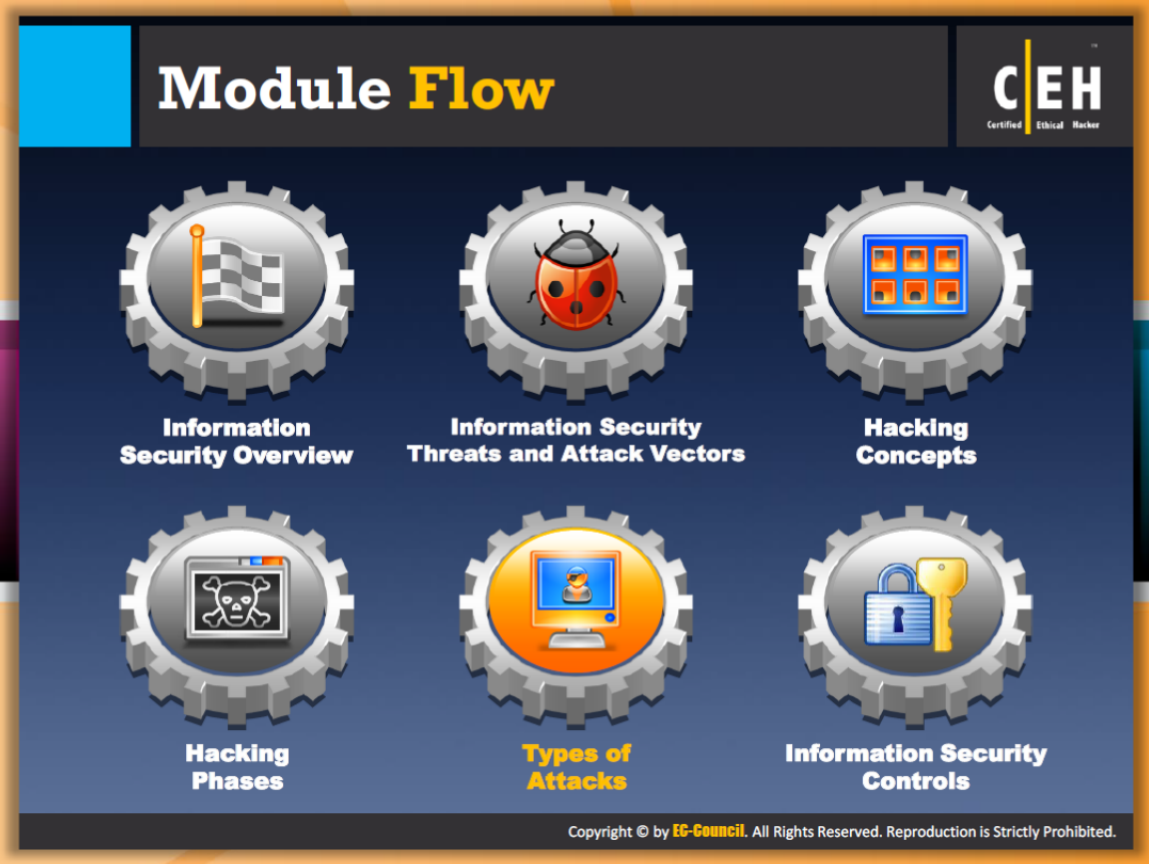
Clearing Tracks

An attacker would like to **destroy evidence** of his or her presence and activities for various reasons such as maintaining access and evading punitive action. **Trojans** such as **ps** or **netcat** come in handy for any attacker who wants to destroy the evidence from the log files or replace the system binaries with the same. Once the **Trojans** are in place, the attacker can be assumed to have gained total control of the system. Rootkits are automated tools that are designed to hide the presence of the attacker. By executing the script, a variety of critical files are replaced with Trojanned versions, **hiding** the **attacker** in seconds.

Other techniques include steganography and tunneling. **Steganography** is the process of hiding the data, for instance in images and sound files. Tunneling takes advantage of the transmission protocol by carrying one protocol over another. Even the extra space (e.g., unused bits) in the TCP and IP headers can be used for hiding information. An attacker can use the system as a cover to launch fresh attacks against other systems or use it as a means of reaching another system on the network **without** being detected. Thus, this phase of attack can turn into a new **cycle of attack** by using reconnaissance techniques all over again.

There have been instances where an attacker has lurked on a system even as system administrators have changed. The system administration can deploy **host-based IDSes** and anti-

virus tools that can detect Trojans and other seemingly benign files and directories. As an ethical hacker, you must be aware of the tools and techniques that attackers deploy, so that you are able to advocate and take **countermeasures** to ensure protection. These will be detailed in subsequent modules.

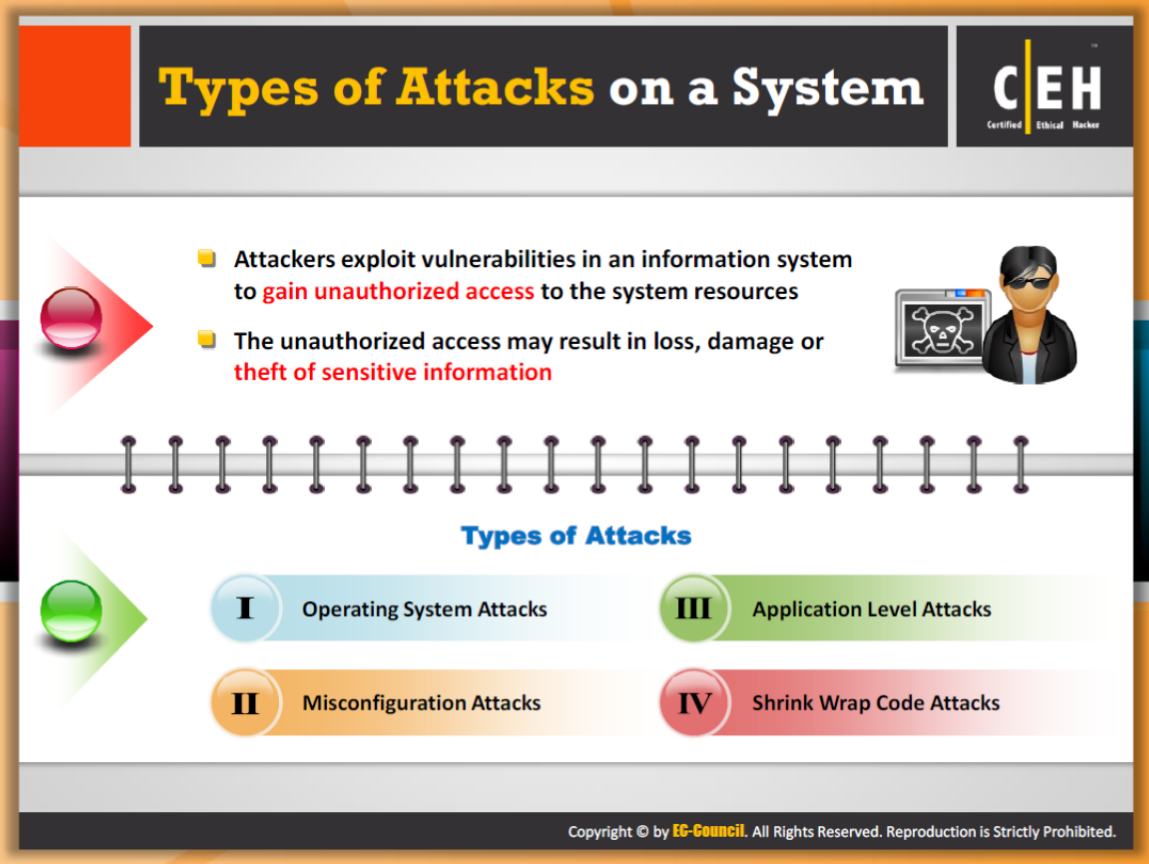


Module Flow

So far we discussed how important it is for an organization to keep their information resources secure, various security threats and attack vectors, hacking concepts, and the hacking phases. Now it's time to examine the **techniques** or the **type of attacks** the attacker adopts to hack a system or a network.

Information Security Overview	Hacking Phases
Information Security Threats and Attack Vectors	Types of Attacks
Hacking Concepts	Information Security Controls

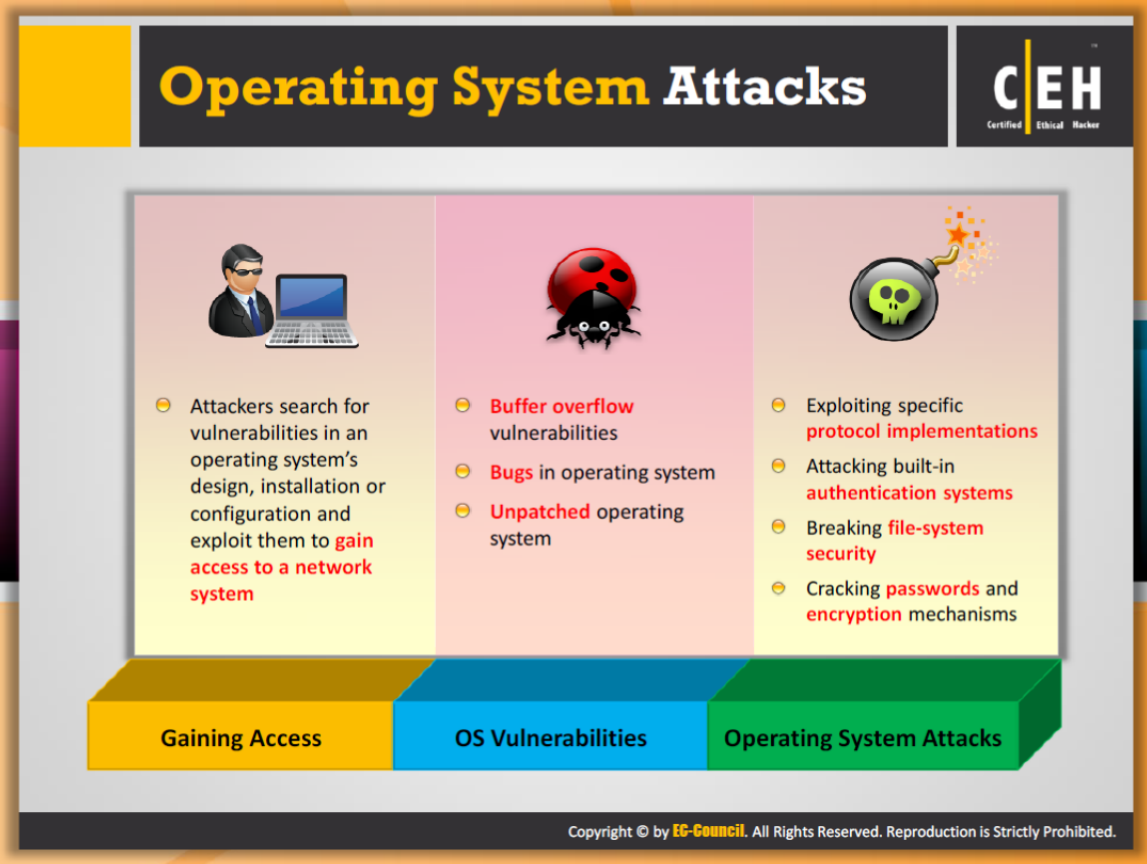
This section covers various types of attacks such as **operating system attacks** and **application-level attacks**.



Types of Attacks on a System

There are several ways an attacker can gain access to a system. The attacker must be able to exploit a **weakness** or **vulnerability** in a system:

- **Operating system attacks**: Attackers search for **OS vulnerabilities** and exploit them to gain access to a network system.
- **Application-level attacks**: Software applications come with **myriad functionalities** and features. There is a dearth of time to perform complete testing before releasing products. Those applications have various vulnerabilities and become a source of attack.
- **Misconfiguration attacks**: Most administrators don't have the necessary skills to maintain or fix issues, which may lead to **configuration errors**. Such configuration errors may become the sources for an attacker to enter into the target's network or system.
- **Shrink wrap code attacks**: Operating system applications come with numerous **sample scripts** to make the job of administrator easy, but the same scripts have various vulnerabilities, which can lead to shrink wrap code attacks.



Operating System Attacks

Today's operating systems, which are loaded with features, are **increasingly complex**. While users take advantage of these features, the system is prone to more vulnerabilities, thus enticing attackers. Operating systems run many services such as **graphical user interfaces (GUIs)**. These supports the use of ports and modes of access to the Internet, and extensive tweaking is required to lock them down. Attackers are constantly looking for **OS vulnerabilities** so that they can exploit and gain access to network systems. To stop attackers from entering their network, the system or network administrators must keep abreast of various new exploits and methods adopted by attackers and monitor their **networks continuously**.

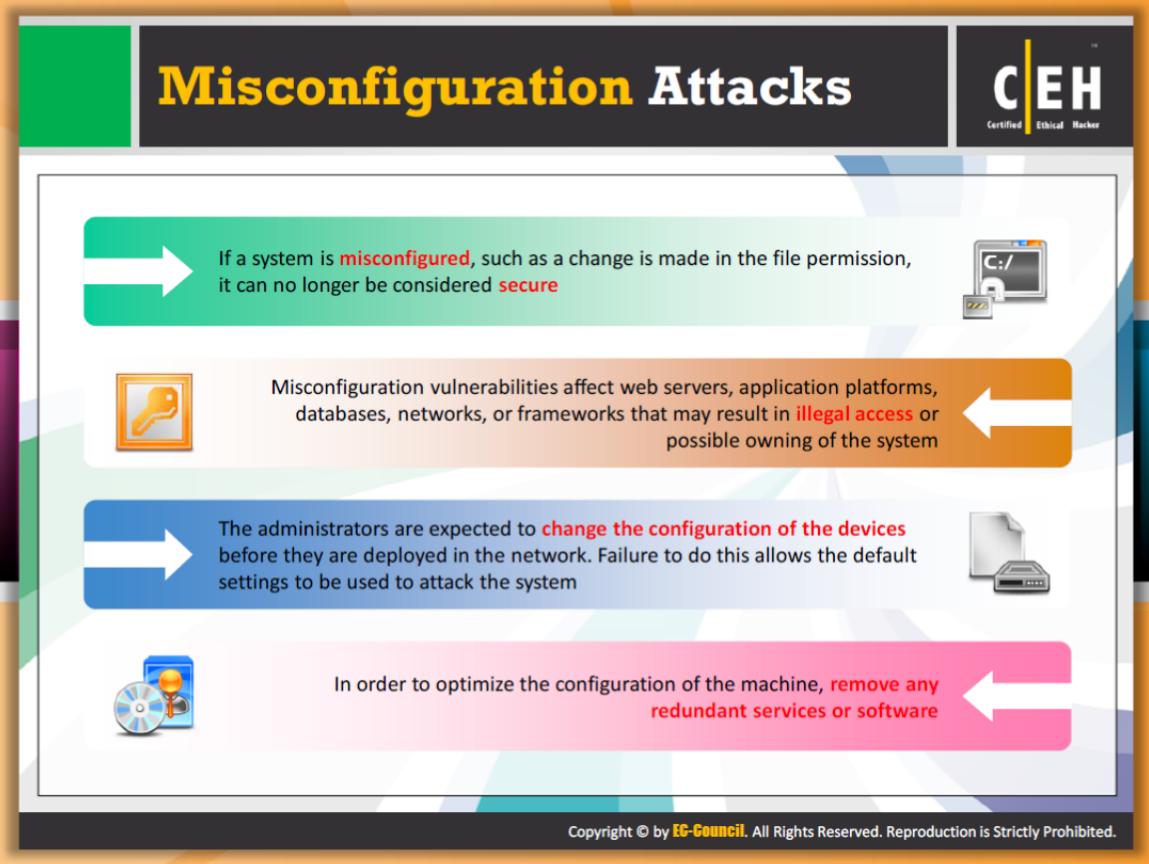
Most operating systems' installation programs install a large number of **services** and **open ports** by default. This situation leads attackers to search for various vulnerabilities. Applying **patches** and **hot fixes** is not easy with today's complex networks. Most patches and fixes tend to solve an immediate issue, but they cannot be considered a permanent solution.

Some OS vulnerabilities include:

- **Buffer overflow** vulnerabilities
- **Bugs** in the operating system
- Unpatched operating systems

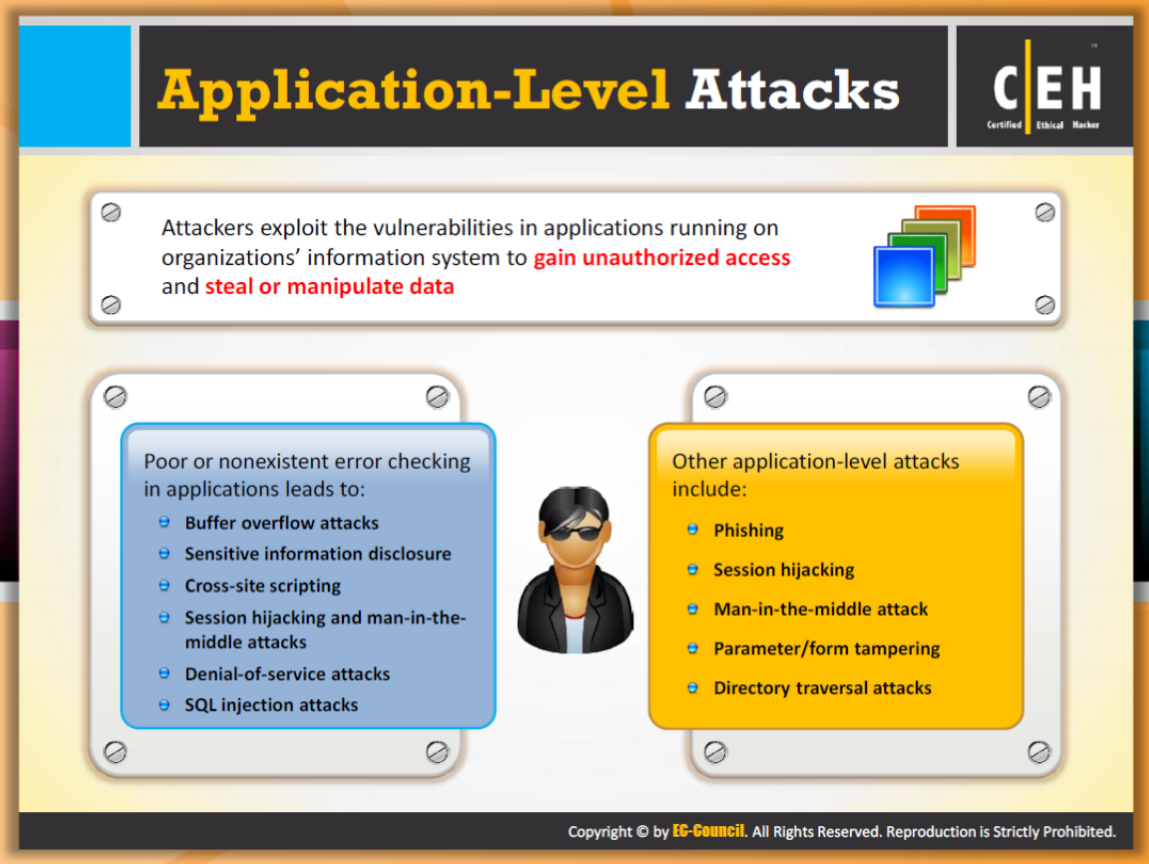
Attacks performed at the OS level include:

- Exploiting specific **network protocol implementations**
- Attacking built-in authentication systems
- Breaking file system security
- Cracking **passwords** and **encryption mechanisms**



Misconfiguration Attacks

Misconfiguration vulnerabilities affect **web servers**, **application** platforms, **databases**, **networks**, or **frameworks** that may result in **illegal access** or possible owning of the system. If a system is misconfigured, such as when a change is made in the file permission, it can no longer be considered secure. Administrators are expected to change the configuration of the devices before they are deployed in the network. Failure to do this allows the default settings to be used to attack the system. In order to optimize the configuration of the machine, remove any redundant services or software.



Application-level Attacks

Applications are being released with more features and more complex coding. With this increased demand in functionality and features, **developers generally overlook** the security of the application, which gives rise to vulnerabilities in applications. Attackers find and exploit these vulnerabilities in the applications using different tools and techniques. The applications are vulnerable to attack because of the following reasons:

- Software developers have **tight schedules to deliver** products on time
- Software applications come with a **multitude of features** and **functionalities**
- There is a **dearth of time to** perform complete **testing** before releasing products
- **Security** is often an afterthought, and frequently delivered as an "**add-on**" component

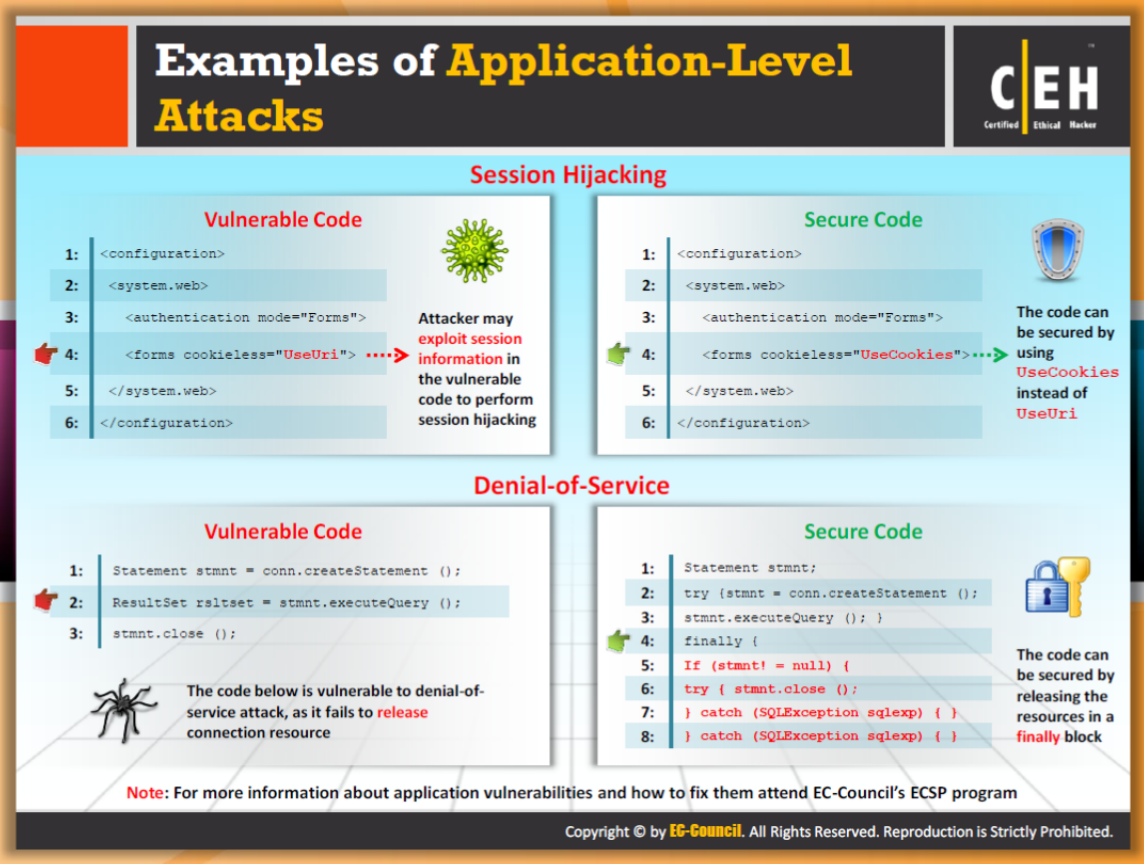
Poor or nonexistent error checking in applications leads to:

- Buffer overflow attacks
- Active content
- Cross-site scripting
- Denial-of-service and SYN attacks

- SQL injection attacks
- Malicious bots

Other application-level attacks include:

- Phishing
- Session hijacking
- Man-in-the-middle attacks
- Parameter/form **tampering**
- Directory traversal attacks



Examples of Application-Level Attacks

Session Hijacking

Attackers may exploit session information in the vulnerable code to perform session hijacking when you enable **cookieless authentication** in your application. When the target tries to browse through a URL, the session or authentication token appears in the request URL instead of the secure cookie, to give access to the **URL requested** by the target. Here, an attacker using his or her skills and monitoring tools can hijack the targets session and steal all sensitive information.

Vulnerable Code

Attackers may exploit session information in the vulnerable code to perform session hijacking.

```
1: <configuration>
2:  <system.web>
3:    <authentication mode="Forms">
4:    <forms cookieless="UseUri">
5:  </system.web>
6: </configuration>
```

TABLE 1.1: Session Hijacking Vulnerable Code

Secure Code

The code can be secured by using UseCookies instead of UseUri.

```
1: <configuration>
2:  <system.web>
3:    <authentication mode="Forms">
4:    <forms cookieless="UseCookies">
5:  </system.web>
6: </configuration>
```

TABLE 1.2: Session Hijacking Secure Code

Denial-of-Service

Vulnerable Code

The code that follows is vulnerable to a denial-of-service attack, as it fails to release a connection resource.

```
1: Statement stmnt = conn.createStatement ();
2: ResultSet rsltset = stmnt.executeQuery ();
3: stmnt.close ();
```

TABLE 1.3: Denial-of-Service Vulnerable Code

Secure Code

The code can be secured by releasing the resources in a finally block.

```
1:  Statement stmnt;
2:  try {stmnt = conn.createStatement ();
3:  stmnt.executeQuery (); }
4:  finally {
5:  If (stmnt! = null) {
6:  try { stmnt.close ();
7:  } catch (SQLException sqlexp) { }
8:  } catch (SQLException sqlexp) { }
```

TABLE 1.4: Denial-of-Service Secure Code

Shrink Wrap Code Attacks

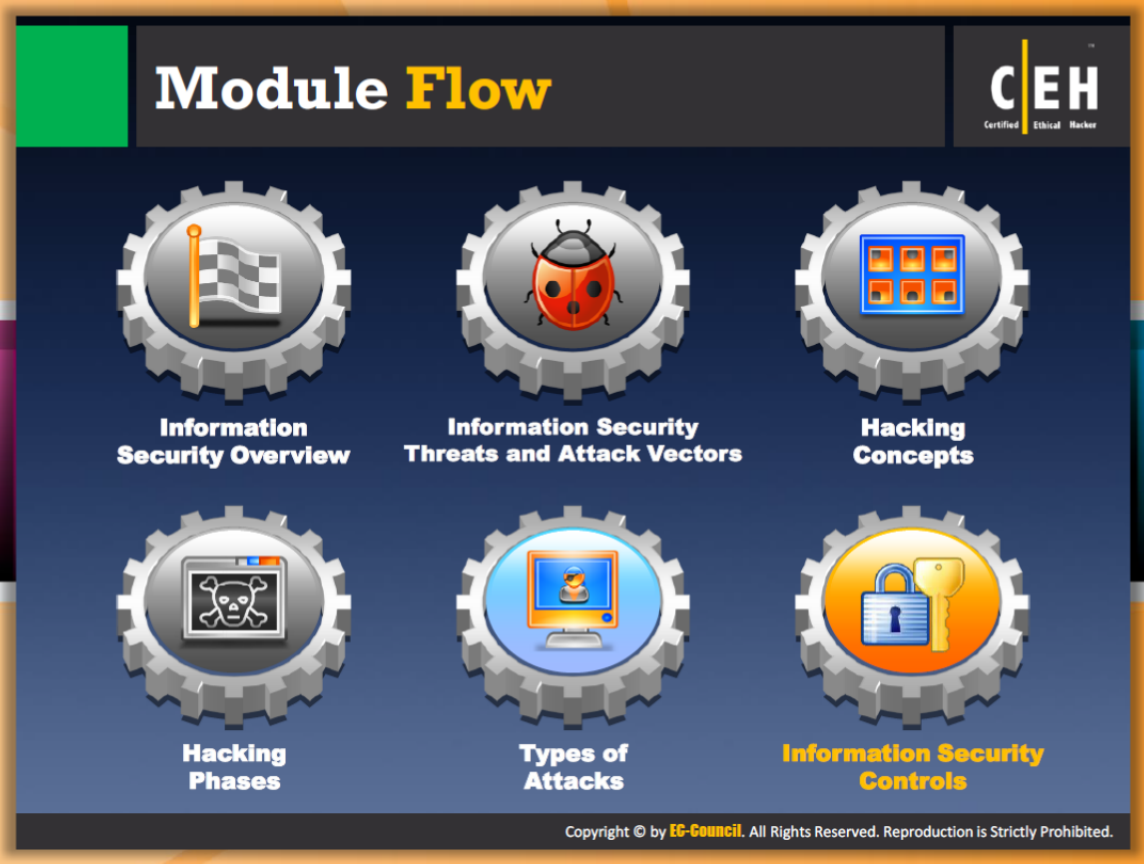
When you install an **OS/application**, it comes with many sample scripts to make the administrator's life easy.

- The problem is "**not fine tuning**" or customizing these scripts
- This will lead to **default code** or **shrink wrap code attacks**

Code for shrink wraps code attacks

```
01522  Private Function CleanUpLine(ByVal sLine As String) As String
01523      Dim lQuoteCount As Long
01524      Dim lcount      As Long
01525      Dim sChar       As String
01526      Dim sPrevChar   As String
01527
01528      ' Starts with Rem it is a comment
01529      sLine = Trim(sLine)
01530      If Left(sLine, 3) = "Rem" Then
01531          CleanUpLine = ""
01532          Exit Function
01533      End If
01534
01535      ' Starts with ' it is a comment
01536      If Left(sLine, 1) = "'" Then
01537          CleanUpLine = ""
01538          Exit Function
01539      End If
01540
01541      ' Contains ' may end in a comment, so test if it is a comment or in the
01542      ' body of a string
01543      If InStr(sLine, " '") > 0 Then
01544          sPrevChar = " "
01545          lQuoteCount = 0
01546
01547          For lcount = 1 To Len(sLine)
01548              sChar = Mid(sLine, lcount, 1)
01549
01550              ' If we found " ' then an even number of " characters in front
01551              ' means it is the start of a comment, and odd number means it is
01552              ' part of a string
01553              If sChar = "'" And sPrevChar = " " Then
01554                  If lQuoteCount Mod 2 = 0 Then
01555                      sLine = Trim(Left(sLine, lcount - 1))
01556                      Exit For
01557                  End If
01558              ElseIf sChar = """" Then
01559                  lQuoteCount = lQuoteCount + 1
01560              End If
01561              sPrevChar = sChar
01562          Next lcount
01563      End If
01564
01565      CleanUpLine = sLine
01566  End Function
```

FIGURE 1.3: Shrink Wraps Code

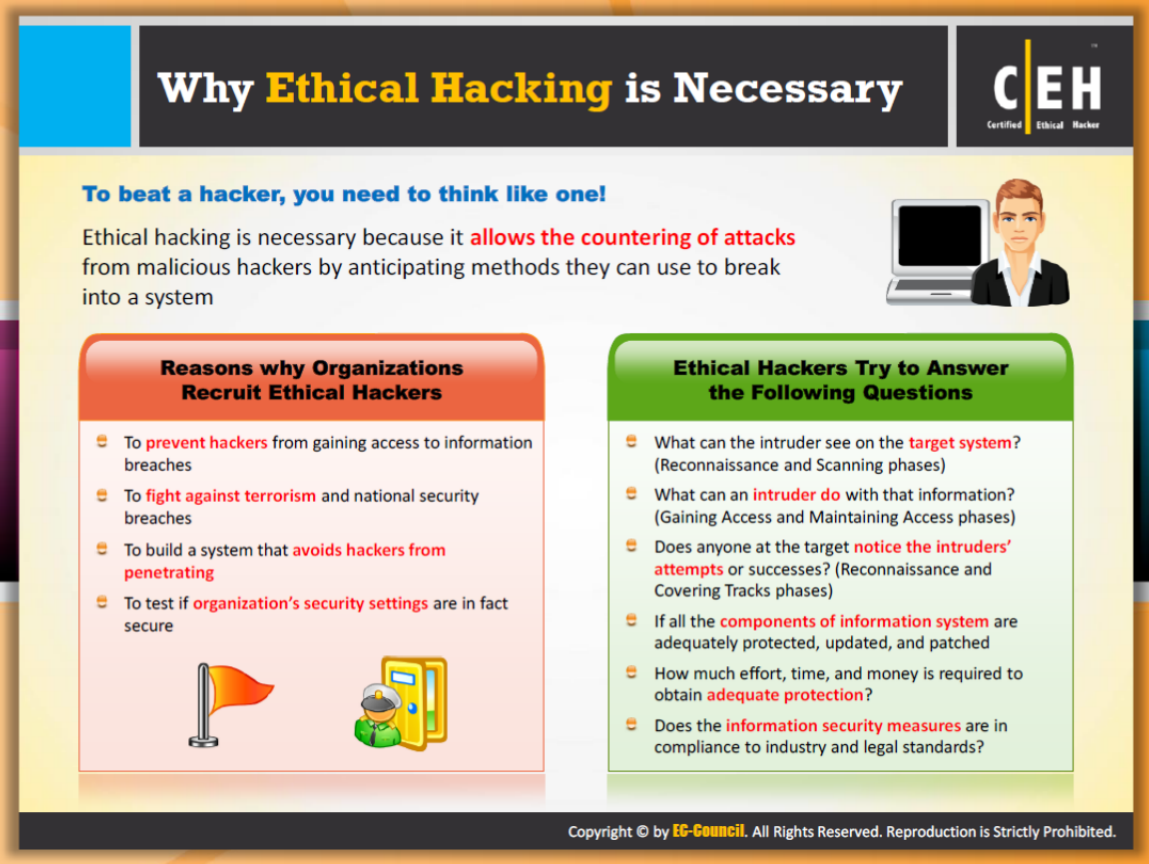


Module flow

In the previous section, we discussed how an attacker can compromise an information system and what type of attacks an attacker can perform. Now, we will discuss **information security controls**. Information security controls **prevent unwanted events** from occurring and **reduces** the **risk** to the information assets of the organization with **security policies**.

Information Security Overview	**Hacking Phases**
Information Security Threats and Attack Vectors	**Types of Attacks**
Hacking Concepts	**Information Security Controls**

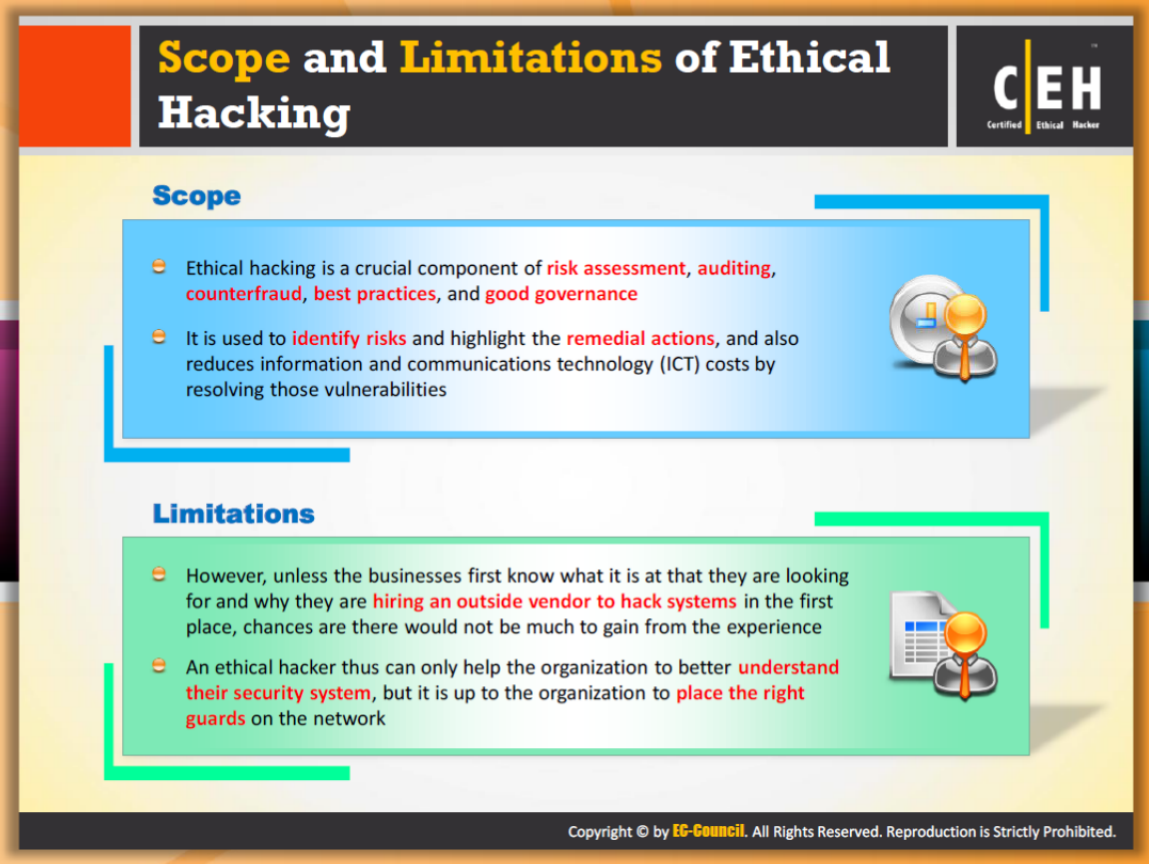
This section highlights the importance of ethical hacking and discusses various **security policies**.



Why Ethical Hacking Is Necessary

There is rapid growth in technology, so there is growth in the risks associated with the technology. **Ethical hacking** helps to **predict** the various possible **vulnerabilities** well in advance and rectify them without incurring any kind of attack from outsiders.

- **Ethical Hacking:** As hacking involves creative thinking, **vulnerability testing** and **security** audits cannot ensure that the network is secure.
- **Defense-in-Depth Strategy:** To achieve this, organizations need to implement a "**defense-in-depth**" strategy by penetrating their networks to **estimate vulnerabilities** and expose them.
- **Counter the Attacks:** Ethical hacking is necessary because it allows countering of attacks from malicious hackers by **anticipating methods** they can use to break into a system.



Scope and Limitations of Ethical Hacking

Ethical hacking has a scope, and there are various limitations of ethical hacking, as well.

Scope

The following is the scope of ethical hacking:

- Ethical hacking is a crucial component of **risk assessment**, **auditing**, **counter fraud**, best practices, and good governance.
- It is used to **identify risks** and highlight remedial actions, and it reduces **information and communications technology** (**ICT**) costs by resolving those vulnerabilities.

Limitations

The following are the limitations of ethical hacking:

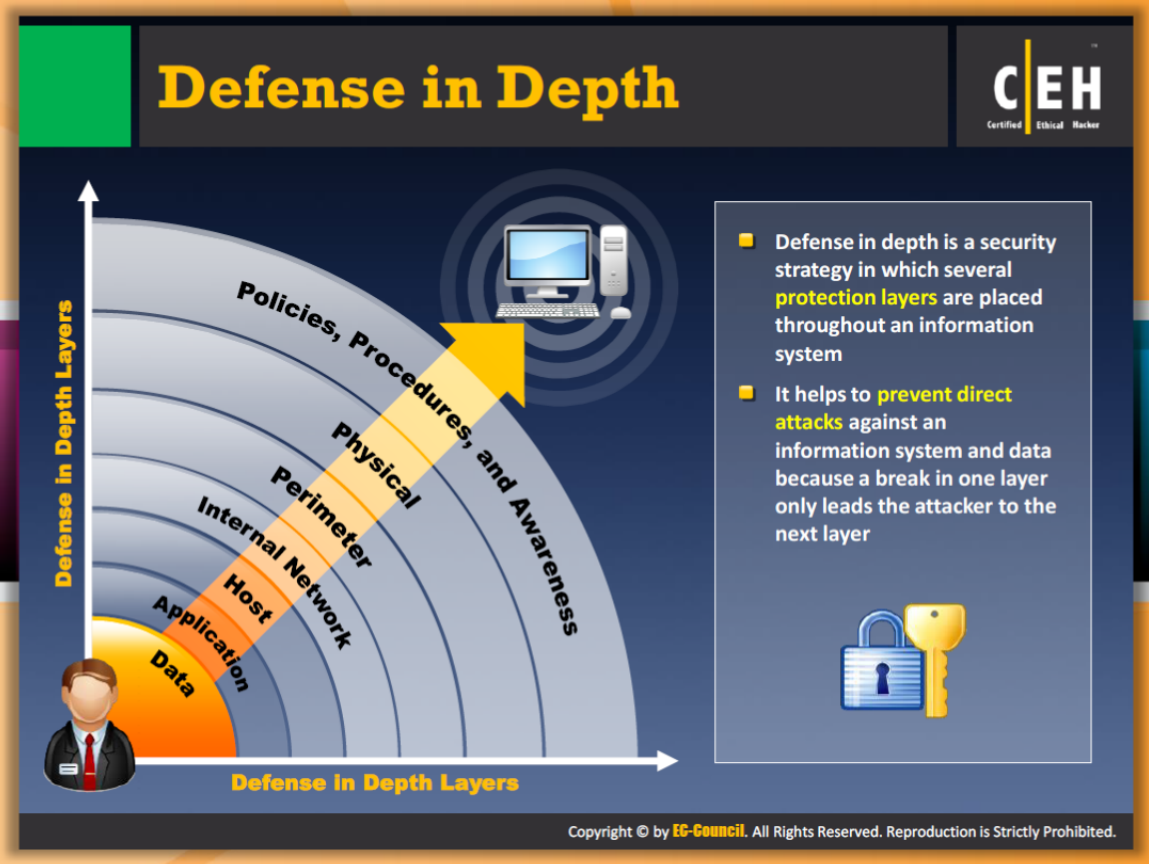
- Unless businesses first know what it is they are looking for and why they are hiring an outside vendor to hack systems in the first place; chances are that there will not be much to gain from the experience.
- An ethical hacker therefore can help the organization only to better understand their **security system**, but it is up to the organization to implement the right **safeguards** on the network.

Skills of an Ethical Hacker

Ethical hacking is the **legal hacking** performed by pen tester to **find vulnerabilities** in the information technology environment. In order to perform ethical hacking, the ethical hacker requires the skills of a computer expert. Ethical hackers should also have strong computer knowledge including **programming** and **networking**. They should be proficient at installing and maintaining systems using popular operating systems (e.g. UNIX, Windows, or Linux).

Detailed knowledge of **hardware** and **software** provided by popular computer and networking hardware vendors complement this basic knowledge. It is not always necessary that ethical hackers possess any additional specialization in security. However, it is an advantage to know how various systems maintain their security. **Management skills** pertaining to these systems are necessary for actual vulnerability testing and for preparing the report after the testing is carried out.

An ethical hacker should possess immense patience as the analysis stage consumes more time than the testing stage. The **time frame** for an evaluation may **vary** from a few days to several weeks, depending on the nature of the task. When an ethical hacker encounters a system with which he or she is not familiar, it is imperative the person takes the time to learn everything about the system and try to find its **vulnerable spots**.



Defense-in-Depth

Multiple defense-in-depth countermeasures are taken to **protect information** assets of a company. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and **multi-layered defense system** than to penetrate a single barrier. If a hacker gains access to a system, defense-in-depth minimizes the adverse impact and gives administrators and engineers time to deploy new or updated countermeasures to prevent a recurrence.

- Defense-in-depth is a security strategy in which **several protection layers** are placed throughout an information system.
- It helps to prevent direct attacks against an information system and data because a break in one layer only leads the attacker to the next layer.

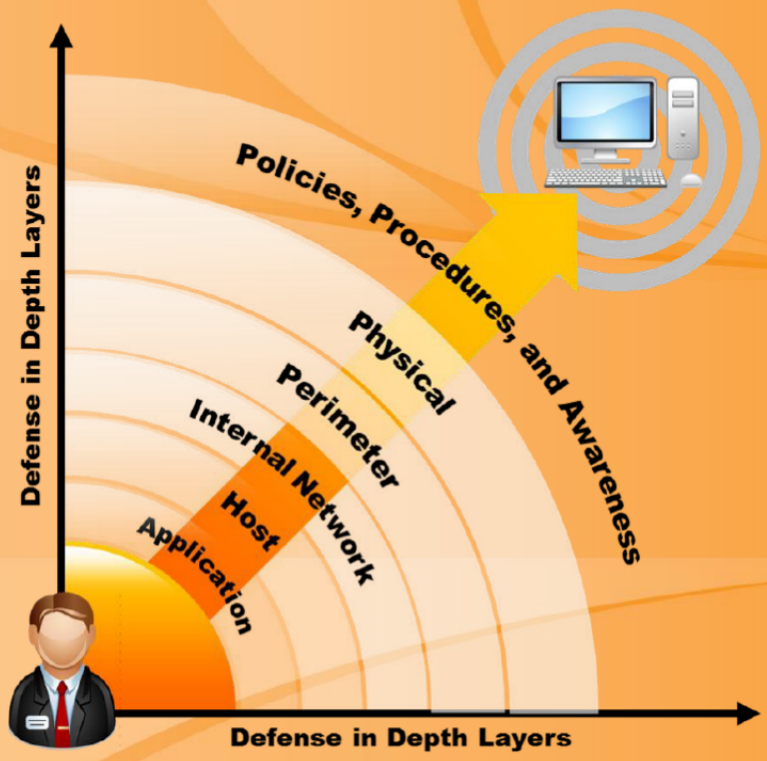
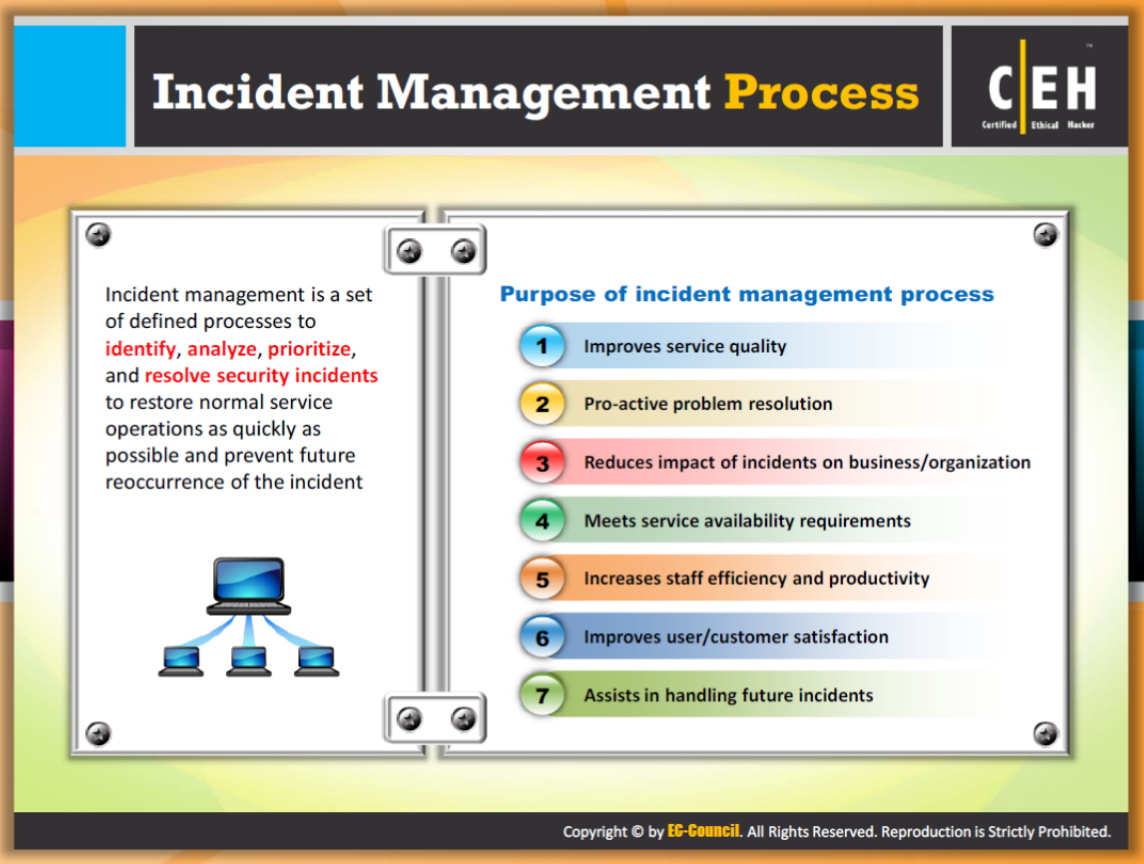


FIGURE 1.4: Defense in Depth Layers Diagram

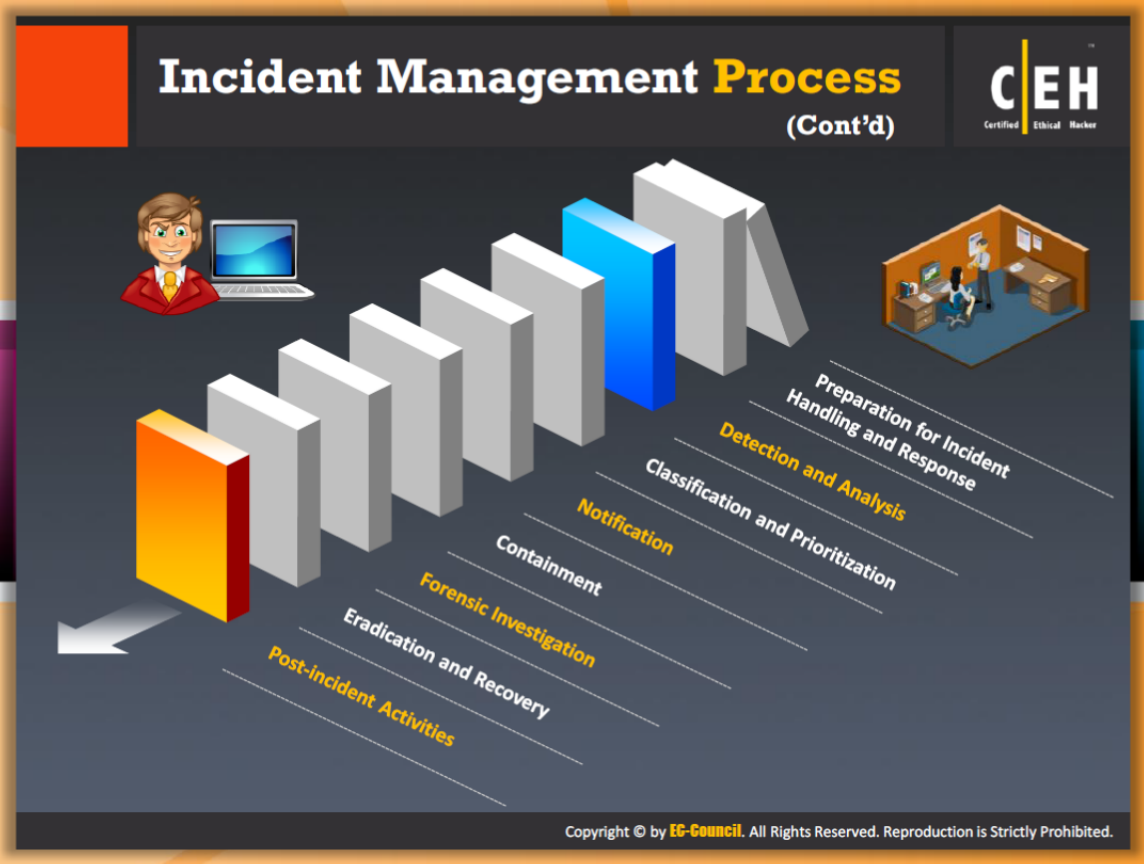


Incident Management Process

Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore the system to normal service operations as soon as possible and prevent the recurrence of the same incident.

The purpose of the incident management process:

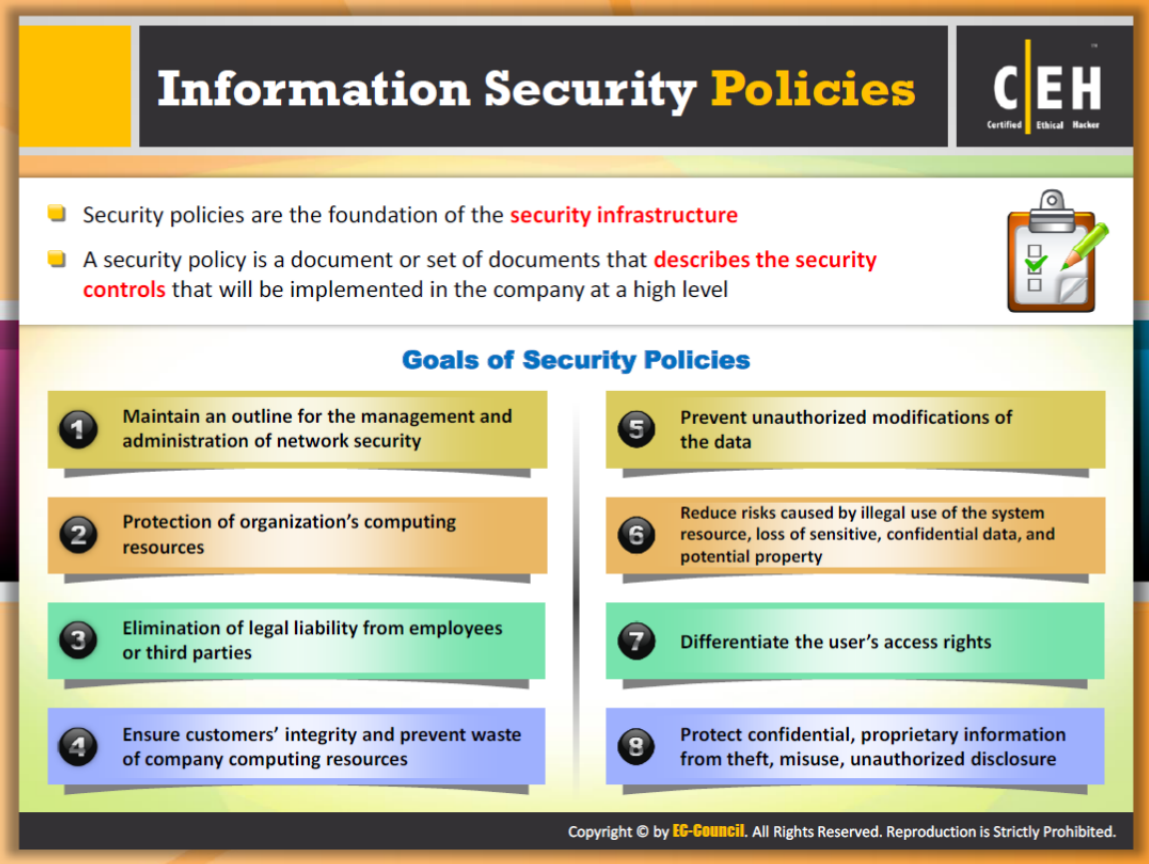
- Improves service quality
- Pro-active problem resolution
- Reduces impact of incidents on business/organization
- Meets service availability requirements
- Increases staff efficiency and productivity
- Improves user/customer satisfaction
- Assists in handling future incidents



Incident Management Process (Cont'd)

Incident management is the process of **logging**, **recording**, and **resolving** incidents that take place in the organization. The incident may occur due to fault, service degradation, error, etc. The incidents are reported by users, technical staff, or sometimes detected automatically by event **monitoring tools**. The main objective of the incident management process is to restore the service to a normal stage as early as possible to customers, while maintaining availability and quality of service. Any occurrence of the incident in an organization is handled and resolved by following these incident management steps:

- Preparation for Incident Handling and Response
- Detection and Analysis
- Classification and Prioritization
- Notification
- Containment
- Forensic Investigation
- Eradication and Recovery
- Post-incident Activities



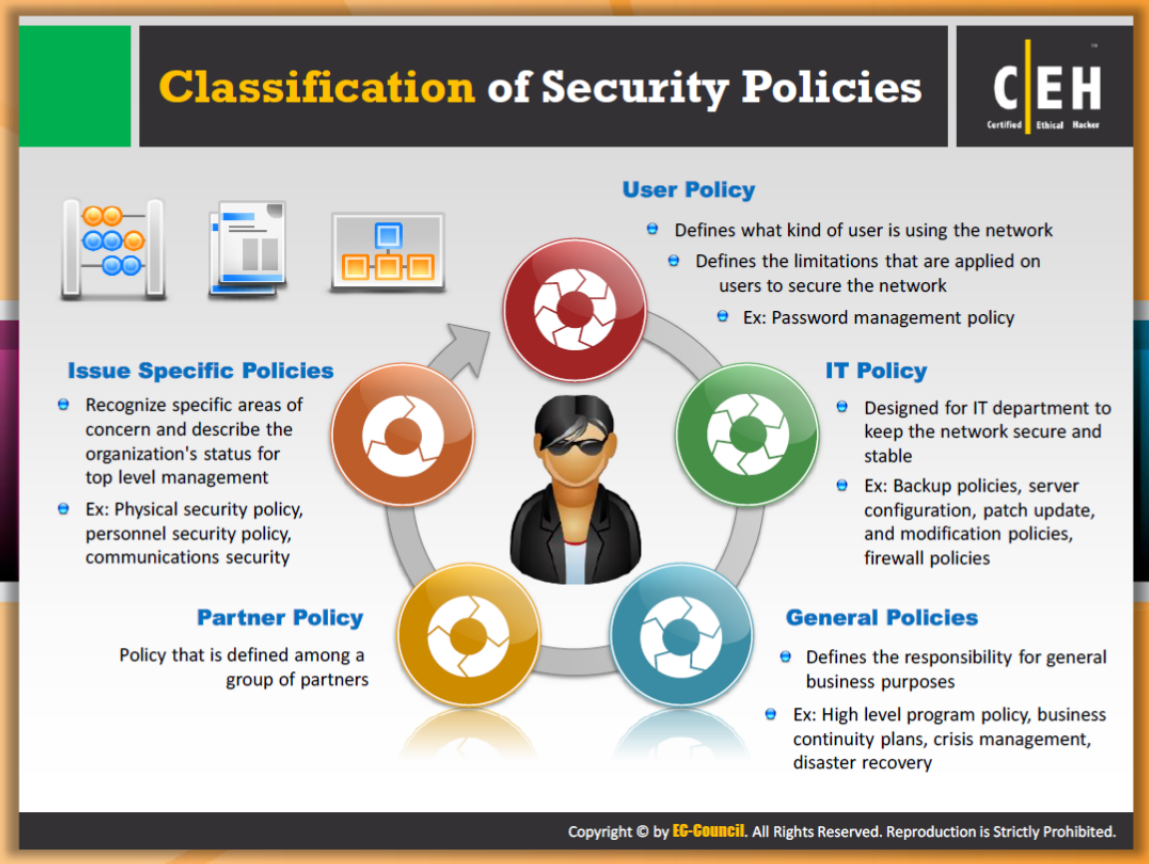
Information Security Policies

A security policy is a document or set of documents that describes the security controls that should be implemented in the company at a **high level for safeguarding** the organizational network from inside and outside attacks. This document defines the complete security architecture of an organization and the document includes clear objectives, goals, rules and regulations, formal procedures, and so on. It clearly mentions the assets to be protected and the person who can log in and access sites, who can view the selected data, as well as the people who are allowed to change the data, etc. Without these policies, it is impossible to protect the company from possible lawsuits, lost revenue, and so on.

Security policies are the foundation of the **security infrastructure**. These policies secure and safeguard the information resources of an organization and provide legal protection to the organization. These policies are beneficial since they help bring awareness of the staff working in the organization to work together to secure its communication, as well as minimizing the risks of security weaknesses through "**human-factor**" mistakes such as disclosing sensitive information to unauthorized or unknown sources, improper use of Internet, etc. In addition, these policies provide protection against cyber-attacks, malicious threats, foreign intelligence, and so on. They mainly address physical security, network security, access authorizations, virus protection, and disaster recovery.

The goals of security policies include:

- Maintain an **outline** for the management and administration of network security
- Protection of organization's computing resources
- **Elimination of legal liability** from employees or third parties
- Ensure customers' **integrity** and prevent wasting of company computing resources
- **Prevent unauthorized modifications** of data
- **Reduce risks** caused by illegal use of the system resources and loss of sensitive, confidential data and potential property
- Differentiate a user's access rights
- Protect confidential, proprietary information from theft, misuse, or **unauthorized disclosure**



Classification of Security Policies

Security policies are sets of policies that are developed to protect or safeguard a company's information assets, networks, etc. These policies are applicable to users, IT departments, organization, and so on. For effective security management, security policies are classified into five different areas:

User Policy

- Defines what kind of user is using the network
- Defines the limitations that are applied on users to secure the network
- Ex: Password Management Policy

IT Policy

Designed for an IT department to keep the network secure and stable

Ex: backup policies, server configuration, patch updates, modification policies, firewall policies

General Policies

Define the responsibility for general business purposes

Ex: high-level program policy, business continuity plans, crisis management, disaster recovery

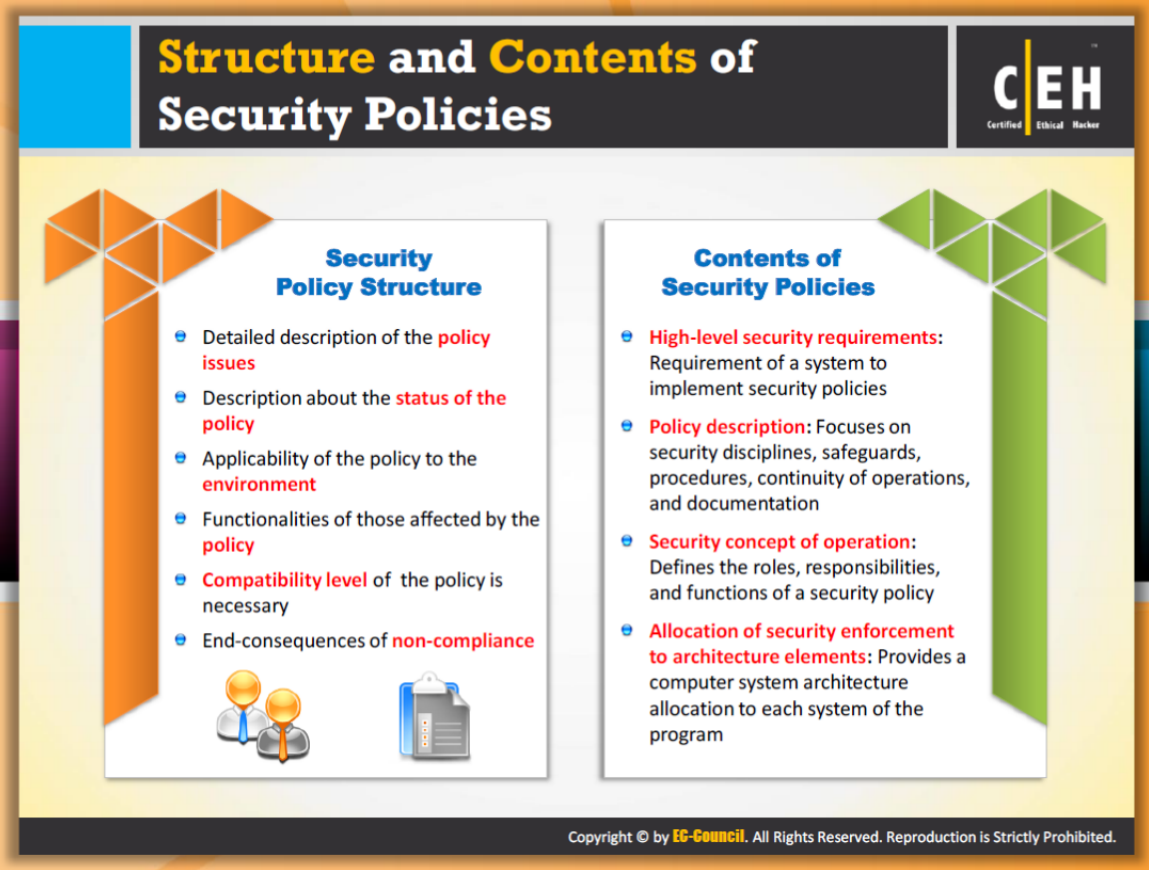
Partner Policy

Policy that is defined among a group of partners

Issue-specific Policies

Recognize specific areas of concern and describe the organization's status for top-level management

Ex: physical security policy, personnel security policy, communications security



Structure and Contents of Security Policies

Structure of Security Policies

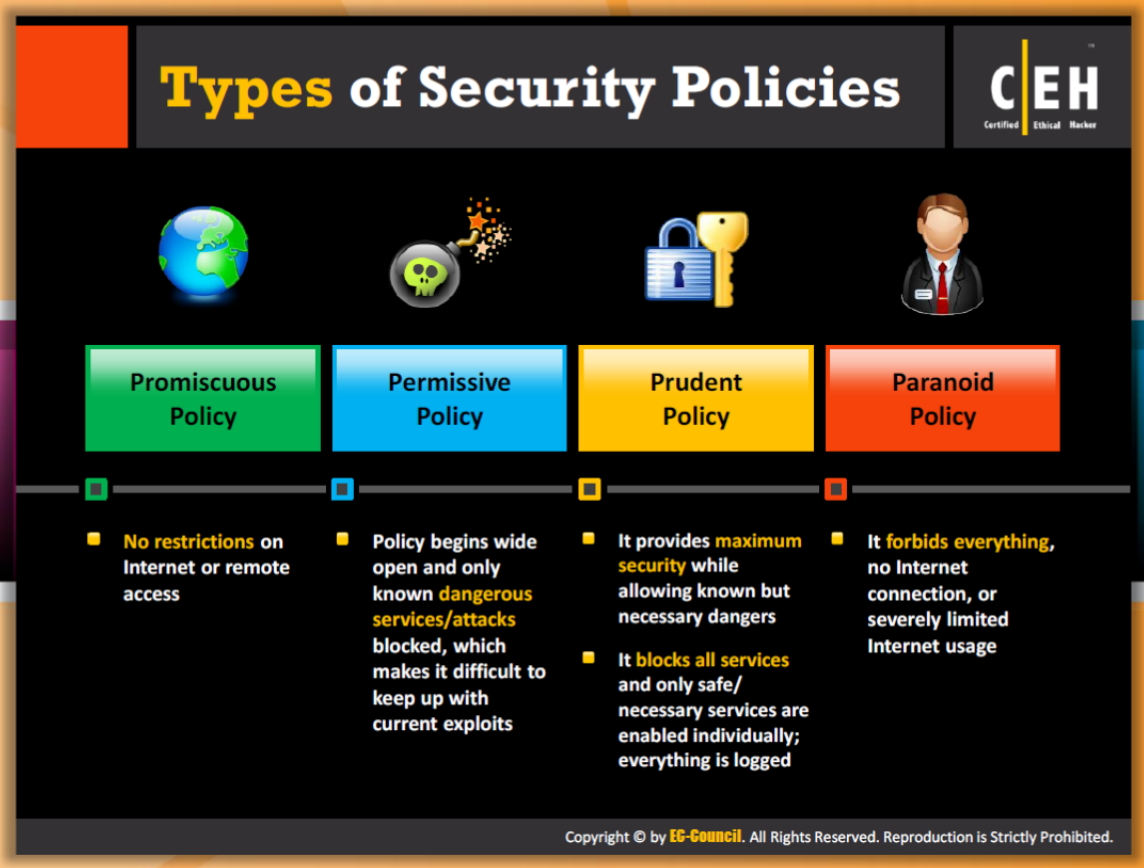
A security policy is the document that provides the way of **securing** the **company's physical personnel** and data from threats or **security breaches**. Security policies should be structured very carefully and should be reviewed properly to make sure that there is no wording that someone could take advantage of. The basic **structure** of security policies should include the following:

- **Detailed description** of the policy issues
- Description of the status of the policy
- Applicability of the policy to the environment
- Functionalities of those affected by the policy
- Specific **consequences** that will occur if the policy is not compatible with the organizational standards

Content of Security Policies

Security policies contain the following elements:

- **High-level Security Requirements:** Explains the **requirements** of a system for the security policies to be implemented. The four different types of requirements are **discipline**, **safeguard**, **procedural**, and **assurance**.
  - **Discipline Security Requirements:** This requirement includes various security policies such as **communications** security, **computer** security, **operations** security, **emanations** security, **network** security, **personnel** security, **information** security, and **physical security**.
  - **Safeguard Security Requirements:** This requirement mainly contains access control, archive, audit, authenticity, **availability**, **confidentiality**, cryptography, identification and authentication, integrity, interfaces, marking, **non-repudiation**, object reuse, recovery, and **virus protection**.
  - **Procedural Security Requirements:** This requirement mainly contains **access** policies, **accountability** rules, **continuity-of-operations** plans, and documentation.
  - **Assurance Security**: This includes **certification** and **accreditation reviews** and sustaining planning documents used in the assurance process**.**
- **Policy Description:** Focuses on security disciplines, **safeguards**, procedures, continuity of operations, and documentation. Each subset of this portion of the policy describes how the system's architecture will **enforce security**.
- **Security Concept of Operation:** Mainly defines the **roles**, **responsibilities**, and **functions** of a security policy. It focuses on mission, communications, encryption, user and maintenance rules, idle-time management, use of privately owned versus public-domain software, shareware software rules, and a virus protection policy.
- **Allocation of Security Enforcement to Architecture Elements:** Provides a computer system architecture allocation to each system of the program.



Types of Security Policies

A security policy is a **document** that **contains information** on the way the company plans to protect its **information assets** from **known** and **unknown threats**. These policies help to maintain the confidentially, availability, and integrity of information. The four major types of security policies are as follows:

Promiscuous Policy

With a promiscuous policy, there is **no restriction on Internet access**. A user can access any site, download any application, and access a computer or a network from a remote location. While this can be useful in corporate businesses where people who travel or work at branch offices need to access the organizational networks, many malware, virus, and Trojan threats are present on the Internet. Due to free Internet access, this malware can come as attachments without the knowledge of the user. **Network administrators** must be extremely alert if this type of policy is chosen.

Permissive Policy

In a permissive policy, the majority of Internet traffic is accepted, but several known **dangerous services** and attacks are blocked. Because only known attacks and exploits are

blocked, it is impossible for administrators to keep up with current exploits. Administrators are always playing catch-up with new attacks and exploits.

Prudent Policy

A prudent policy starts with all **services blocked**. The administrator enables safe and necessary services individually. This provides **maximum security**. Everything, such as system and network activities, is logged.

Paranoid Policy

In a paranoid policy, everything is forbidden. There is **strict restriction** on all usage of company computers, whether it is **system usage** or **network usage**. There is either no Internet connection or severely limited Internet usage. Due to these overly severe restrictions, users often try to find ways around them.

Steps to Create and Implement Security Policies

Implementing **security policies reduces** the **risk** of being attacked. Thus, every company must have its own security policies based on its business. The following are the steps to be followed by every organization in order to create and implement security policies:

1. Perform **risk assessment** to identify risks to the organization's assets
2. Learn from **standard guidelines** and other organizations
3. Include senior management and all other staff in policy development
4. **Set clear penalties** and enforce them and also review and update the security policy
5. Make the final version available to all staff in the organization
6. Ensure every member of your staff reads, signs, and understands the policy
7. Install the tools you need to **enforce** the **policy**
8. **Train** your **employees** and educate them about the policy

Examples of Security Policies

The following are some examples of security polies that are created, accepted, and used by organizations worldwide to secure their assets and important resources.

Acceptable-Use Policy

Defines the acceptable use of **system resources**

User-Account Policy

Defines the account creation process and **authority**, **rights**, and **responsibilities** of user accounts

Remote-Access Policy

Defines who can have remote access, and **defines access medium** and remote access security controls

Information-Protection Policy

Defines the **sensitivity levels** of information, who may have access, how is it stored and transmitted, and how should it be deleted from storage media

Firewall-Management Policy

Defines **access**, **management**, and **monitoring** of firewalls in the organization

Special-Access Policy

This policy defines the **terms and conditions** of granting special access to system resources

Network-Connection Policy

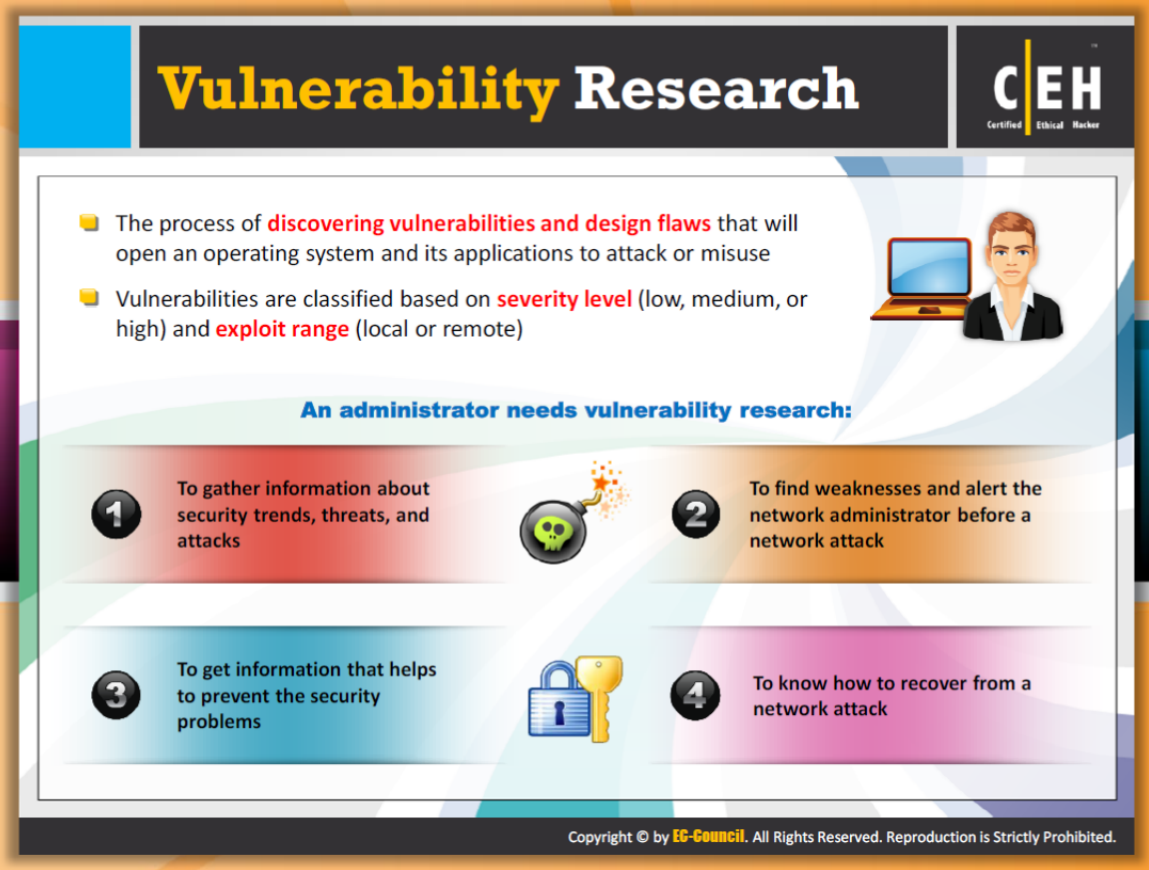
Defines who can install **new resources** on the network, approve the installation of new devices, document network changes, etc.

Email Security Policy

Created to govern the proper **usage of corporate email**

Password Policy

Provides guidelines for using **strong password protection** on organization's resources



Vulnerability Research

Vulnerability research means **discovering system design faults** and weaknesses that might help attackers compromise the system. Once the attacker finds out the vulnerability in the product or the application, he or she tries to **exploit** it.

Vulnerability research helps both security administrators and attackers:

- Discovering system design faults and **weaknesses** that might help attackers to compromise the system
- Keeping abreast of the latest **vendor-supported products** and other technologies in order to find news related to current exploits
- **Checking** newly released **alerts** regarding relevant innovations and product improvements for security systems
- Vulnerability research is based on the following classification:
  - **Severity level** (low, medium, or high)
  - **Exploit range** (local or remote)

An administrator needs vulnerability research:

- To gather information about security trends, threats, and attacks
- To find weaknesses and alert the network administrator before a network attack
- To get information that helps to prevent security problems
- To know how **to recover** from a network attack

Vulnerability Research Websites

The following are the some vulnerability research websites that you can use:

CodeRed Center

Source: http://www.eccouncil.org

The CodeRed Center is a comprehensive **security resource administrators** can turn to for daily, accurate, up-to-date information on the latest viruses, Trojans, malware, threats, security tools, risks, and vulnerabilities.

TechNet

Source: http://blogs.technet.com

TechNet is a project team from across **Microsoft Lync Server** teams and the community at large. It is led by the Lync Server documentation team; their writers and technical reviewers come from all disciplines, including product engineers, field engineers, support engineers, documentation engineers, and some of the most respected technology bloggers and authors in the Lync Server universe.

Security Magazine

Source: http://www.securitymagazine.com

Security Magazine is uniquely focused on solutions for enterprise security leaders. It is designed and written for business-minded executives who manage **enterprise risk and security**. Security Magazine provides management-focused features, opinions, and trends for leaders in business.

SecurityFocus

Source: http://www.securityfocus.com

The Security Focus website focuses on a few key areas that are of greatest importance to the security community.

- **BugTraq** is a high-volume, full-disclosure mailing list for the detailed discussion and announcement of computer security vulnerabilities. BugTraq serves as the cornerstone of the Internet-wide security community.
- The **SecurityFocus Vulnerability Database** provides security professionals with the most up-to-date information on vulnerabilities for all platforms and services.

Help Net Security

Source: http://www.net-security.org

Net Security is a daily security news site that has been covering the latest computer and network security news since its inception in 1998.

Besides covering news around the globe, HNS focuses on quality technical articles and papers, vulnerabilities, vendor advisories, malware, and hosts the largest security software download area with software for Windows, Linux, and Mac OS X.

HackerStorm

Source: http://www.hackerstorm.co.uk

HackerStorm is a security resource for **ethical hackers** and **penetration testers** to create better penetration testing plans and scopes, and conduct vulnerability research.

SC Magazine

Source: http://www.scmagazine.com

SC Magazine is published by Haymarket Media Inc. and is part of a global brand. There are three separate editions of the magazine:

- North America - U.S. and Canada
- International - U.K. and mainland Europe

- Asia Pacific Online - read by decision-makers in over **20 countries** in the Pacific Rim region

The magazine is published monthly, usually in the first week of each month. It is the longest running information security magazine in the world, with the widest distribution.

SC Magazine provides IT security professionals with in-depth and unbiased information in one incomparable publication. In each monthly issue it has timely news, comprehensive analysis, cutting-edge features, contributions from thought leaders and the best, most extensive collection of product reviews in the business. They been doing this since 1989, when it first began campaigning for organizations' information security leaders, making it the longest established IT security title in the United States.

Computerworld

Source: http://www.computerworld.com

For more than **40 years**, Computerworld has been the leading source of technology news and information for IT influencers worldwide. **Computerworld's website** (Computerworld.com), twice-monthly publication, focused conference series, and custom research form the hub of the world's largest global IT media network.

HackerJournals

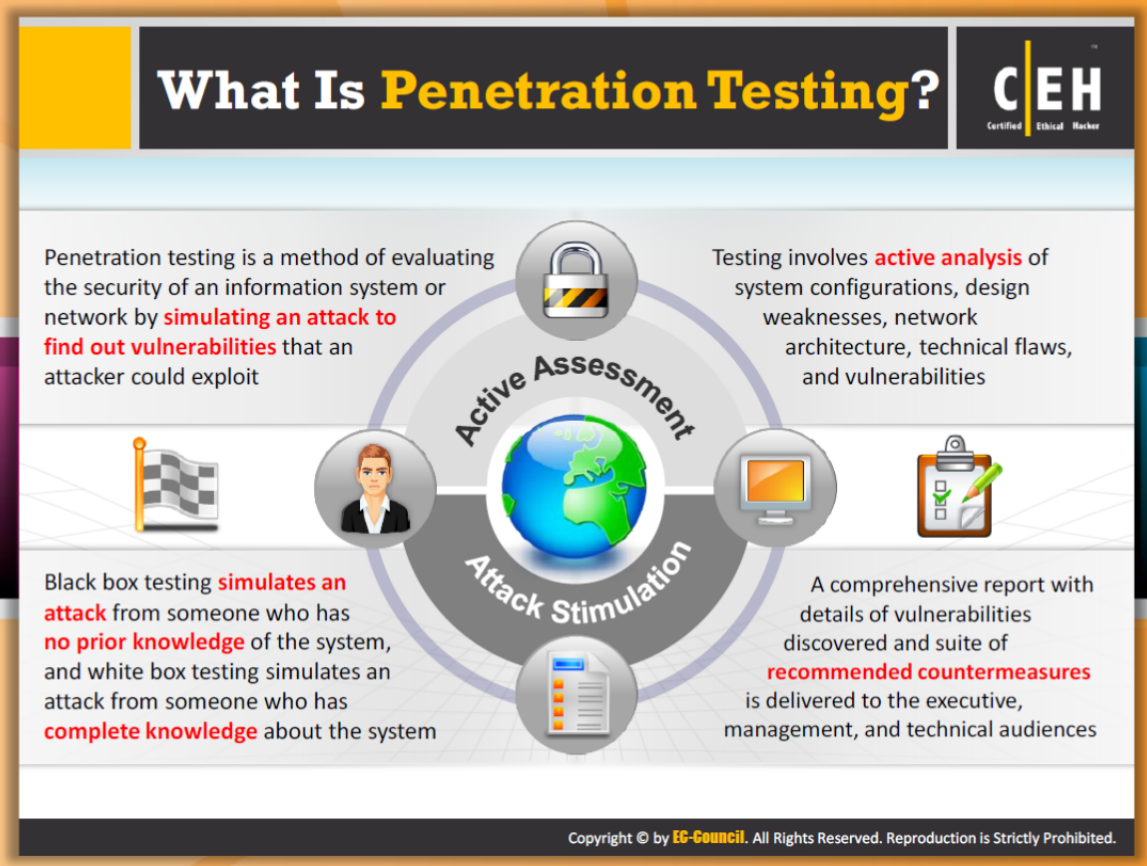
Source: http://www.hackerjournals.com

Hacker Journals is an online **Information Security Community**. It propagates news specifically related to information security threats and issues from all over the world. Its research teams search and compile news from tens of thousands of sites to bring you the most relevant Cyber Security titles in one location. In addition to news, it hosts blogs and discussions, education videos, as well as its World Famous Hack.ED column, providing education series in Ethical Hacking and Countermeasure Techniques and technologies.

WindowsSecurity Blogs

Source: http://blogs.windowsecurity.com

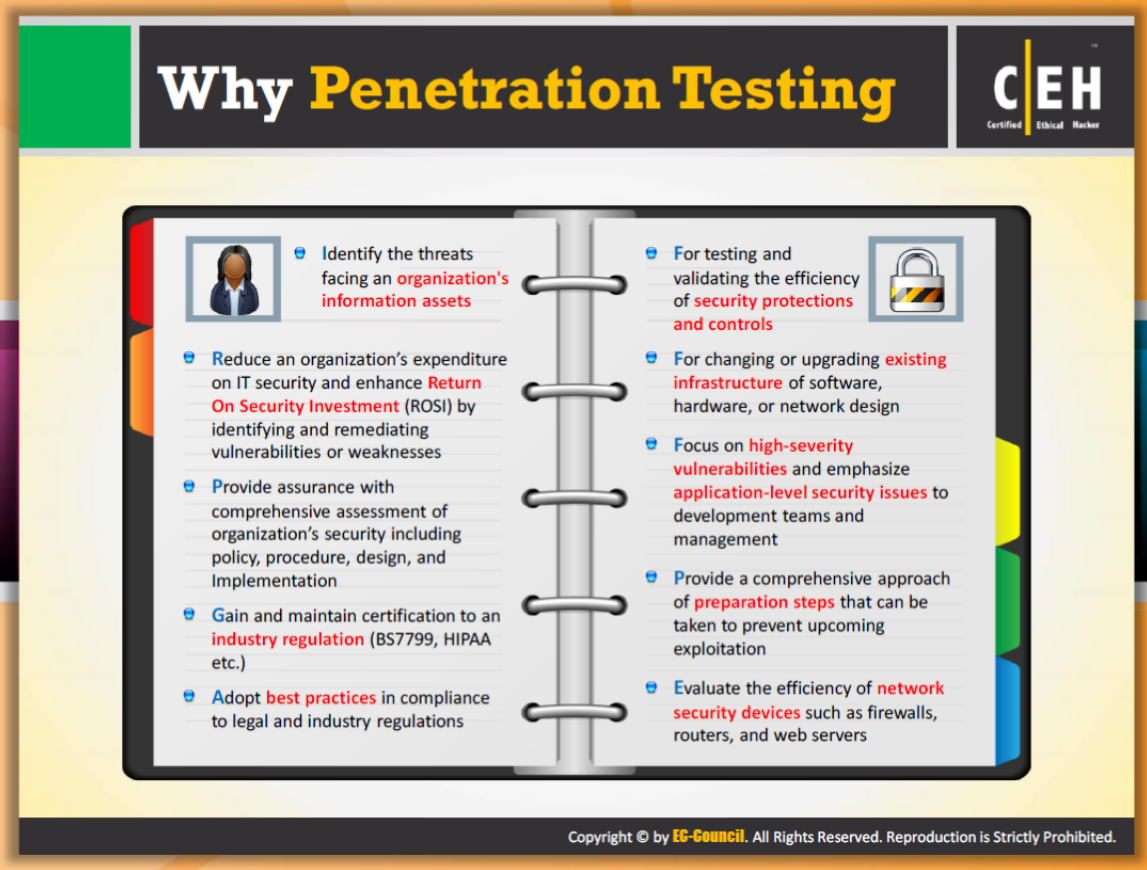
Windows security has blogs posted by **famous authors** who are leading industry experts. It has various features such as articles and tutorials, blogs, message boards, security tests, and white papers.



What Is Penetration Testing?

Penetration testing is a method of **evaluating security levels** of a particular system or network. This helps you determine the flaws related to **hardware** and **software**. The early identification helps **protect the network**. If the vulnerabilities aren't identified early, then they become an easy source for the attacker for the intrusion.

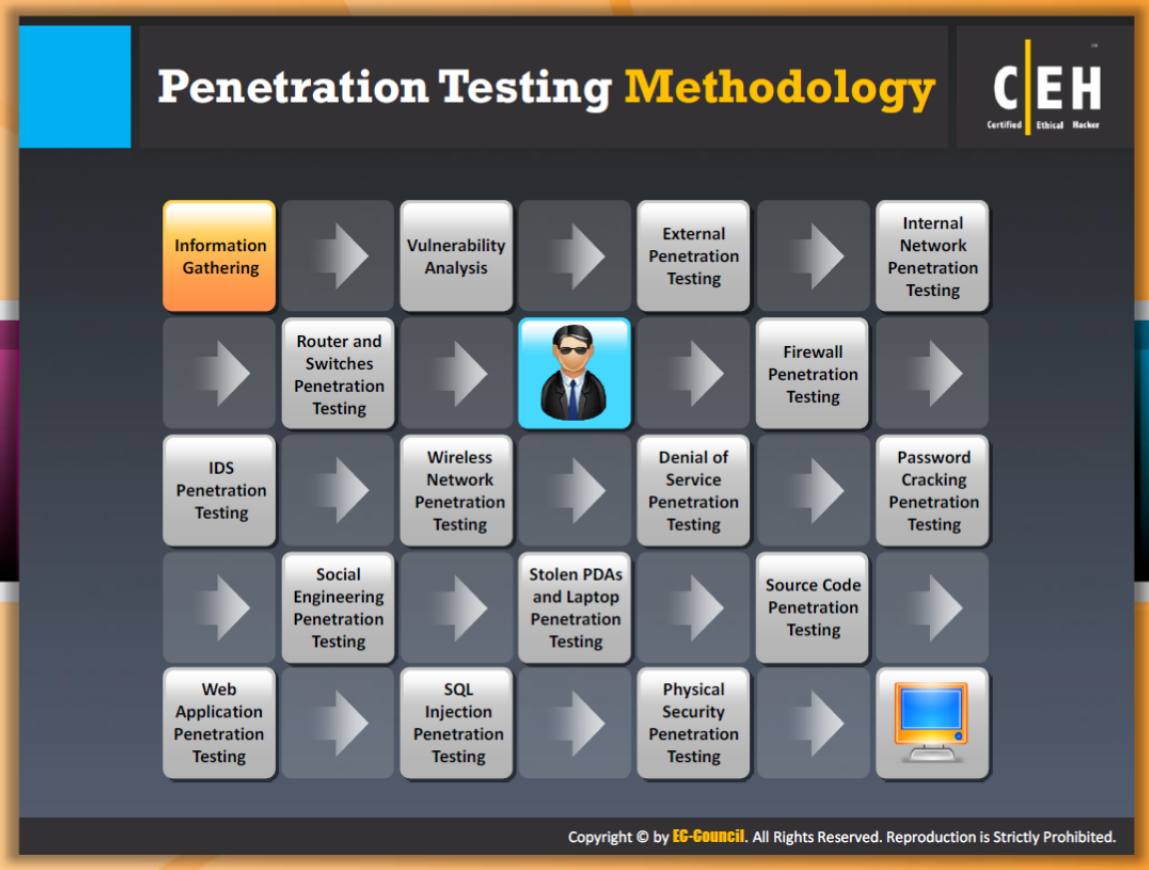
During penetration testing, a pen tester analyzes all the **security measures** employed by the organization for design weaknesses, technical flaws, and vulnerabilities. There are two types of testing; **black box testing** and **whitebox testing**. Black box testing simulates an attack from someone who is **unfamiliar** with the system, and white box testing simulates an attacker that has **knowledge** about the system. Once all the tests are conducted, the pen tester prepares a report and includes all the test results and the tests conducted along with the vulnerabilities found and the respective countermeasures that can be applied. Finally, the pen tester delivers the report to executive, management, and technical audiences.



Why Penetration Testing?

Penetration testing is required because it helps you to:

- Identify the threats facing an organization's information assets
- Reduce an organization's IT security **costs** and provide a better **Return On Security Investment (ROSI)** by identifying and resolving vulnerabilities and weaknesses
- Provide an organization with assurance: a thorough and comprehensive assessment of organizational security covering policy, procedure, design, and implementation
- Gain and maintain certification to an industry regulation (BS7799, HIPAA etc.)
- Adopt best practices by conforming to **legal** and **industry regulations**
- Test and validate the efficiency of **security protections** and **controls**
- Change or upgrade existing infrastructure of software, hardware, or network design
- Focus on **high-severity vulnerabilities** and emphasize **application-level security** issues to development teams and management
- Provide a comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation
- Evaluate the efficiency of network security devices such as firewalls, routers, and web servers



Penetration Testing Methodology

As a pen tester, you should never overlook any information resource. All possible information sources must be tested for vulnerabilities. Not just the information sources, but every **mechanism** and the **software** involved in your business must be tested because if the attacker is not able to compromise the information system, then he or she may try to gain access to the system and then to the **sensitive information**. A few attacks, such as denial-of-service attacks, don't even need access to the system. Therefore, to ensure that you check all possible ways of compromising a system or network, you should follow the penetration testing methodology. This ensures the full scope of the test.

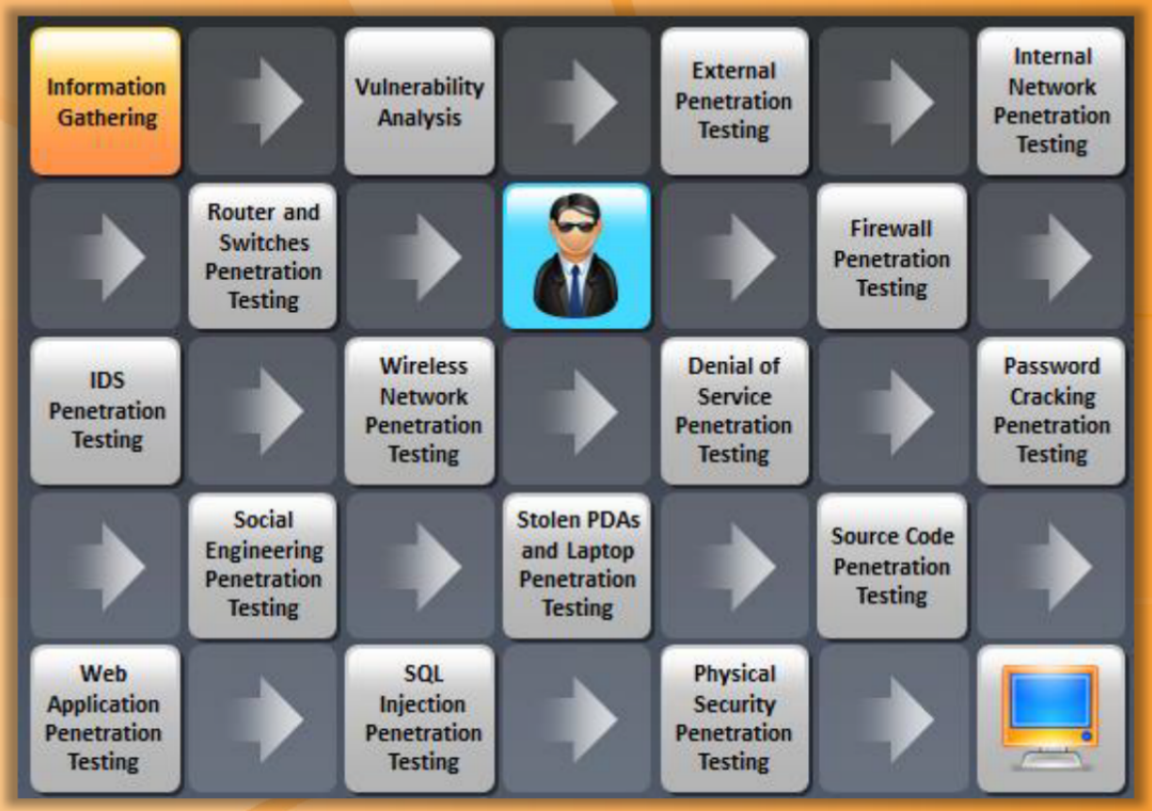
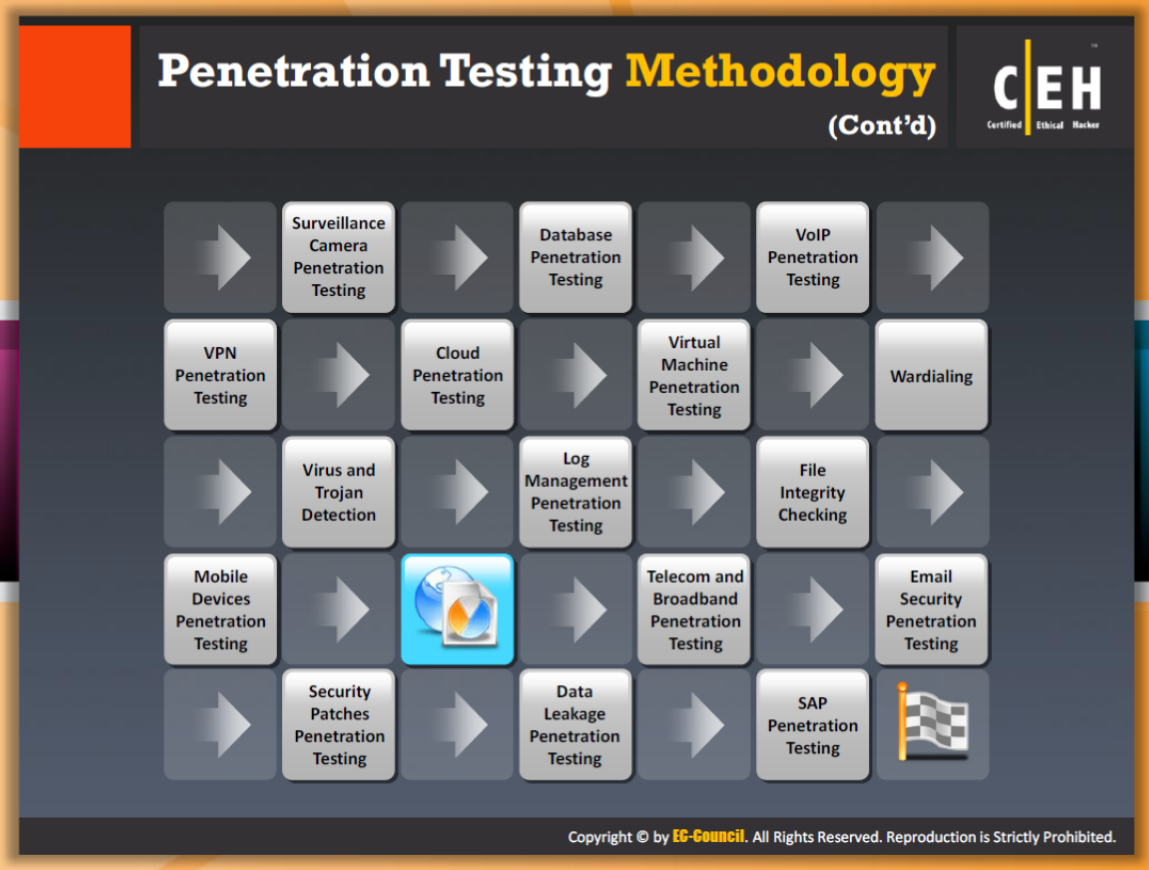


FIGURE 1.5: Penetration Testing Methodology Part -1



Penetration Testing Methodology (Cont'd)

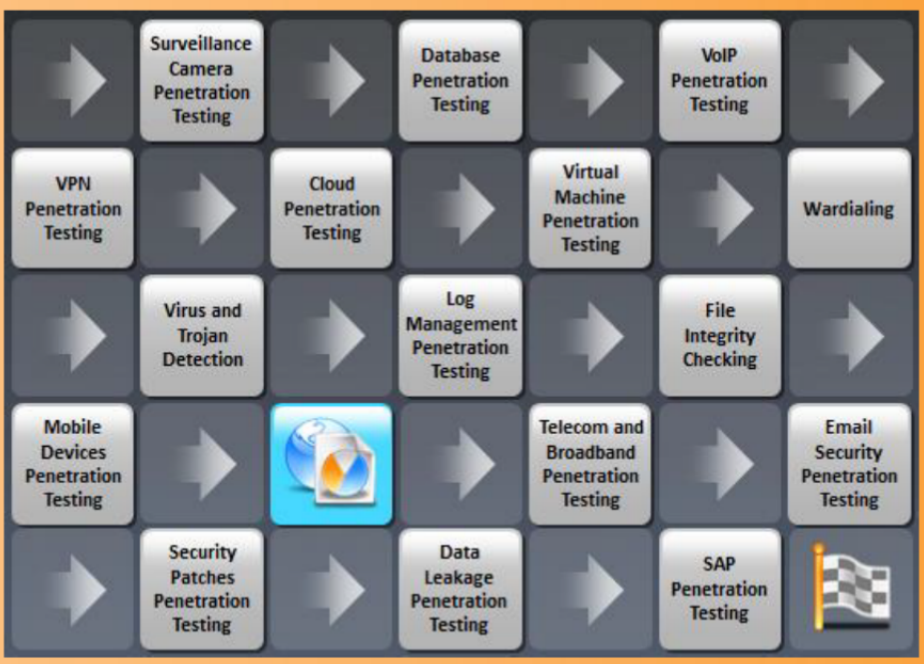
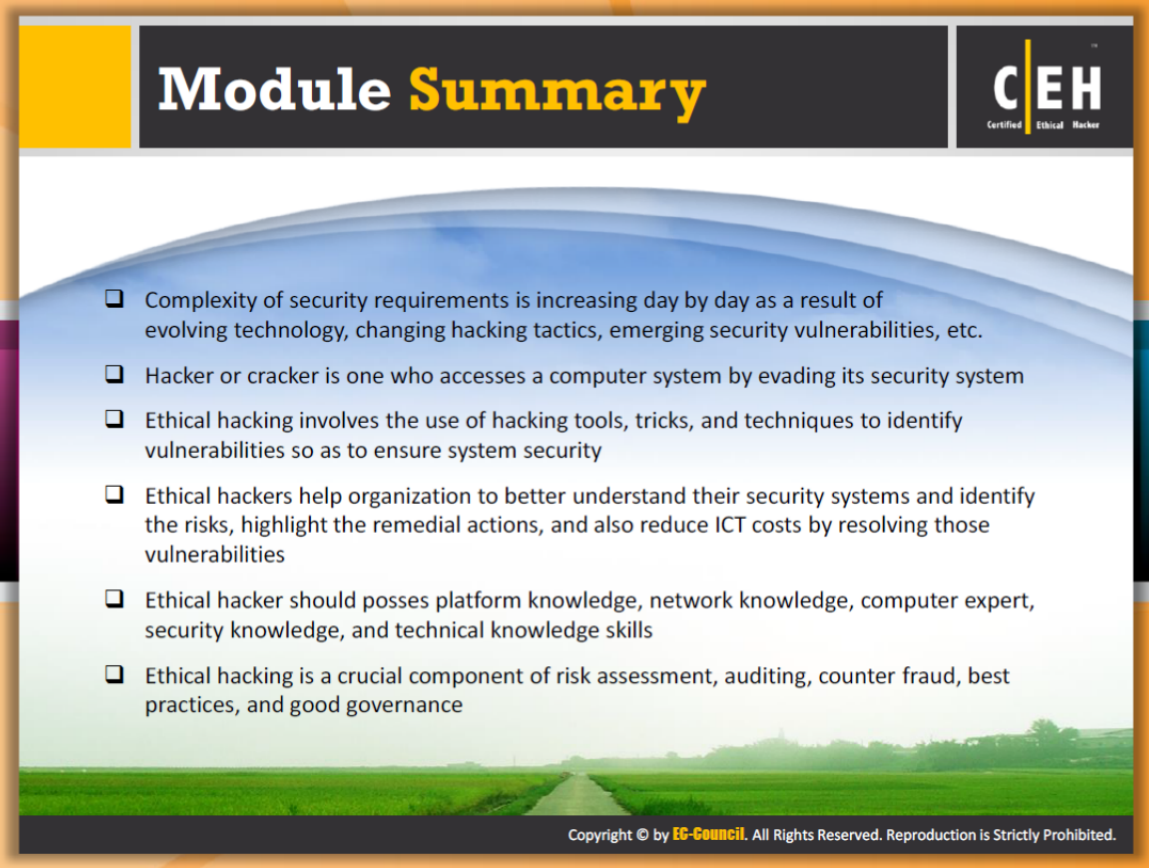


FIGURE 1.6: Penetration Testing Methodology Part -2



Module Summary

This module is summarized as follows:

- The complexity of **security requirements** is increasing day by day as a result of evolving technology, changing hacking tactics, emerging security vulnerabilities, etc.
- A hacker or cracker is someone who accesses a computer system by **evading** its **security** system.
- Ethical hacking involves the use of hacking tools, tricks, and techniques to identify **vulnerabilities** to ensure system security.
- Ethical hackers help organizations to better understand their security systems and **identify** the **risks**, highlight the **remedial actions**, and also reduce **ICT costs** by resolving those vulnerabilities.
- An ethical hacker possesses **platform** knowledge, **network** knowledge, **computer** expert, **security** knowledge, and **technical knowledge** skills.
- Ethical hacking is a crucial component of **risk assessment**, auditing, counter fraud, best practices, and good governance.