Study Guide

Network Security for Certified in Cybersecurity CCSM

# Checklist of Exam Objectives: Areas to Study

4.1 Understand computer networking

* Networks (e.g., Open System Interconnection (OSI) model, Transmission Control Protocol/Internet Protocol (TCP/IP) model, Internet Protocol version 4 (IPv4) Internet Protocol version 6 (IPv6), WiFi)
* Ports
* Applications

4.2 Understand network threats and attacks

* Types of threats (e.g., distributed denial of service (DDoS), virus, worm, Trojan, man-in-the-middle (MITM), side-channel)
* Identification (e.g., intrusion detection system (IDS), host-based intrusion detection system (HIDS), network intrusion detection system (NIDS))
* Prevention (e.g., anti-virus, scams, firewalls, intrusion prevention system (IPS))

4.3 Understand network security infrastructure

* On-premises (e.g., power, data center/closets, Heating, Ventilation, and Air Conditioning (HVAC), environmental, fire suppression, redundancy, memorandum of understanding (MOU)/memorandum of agreements (MOA))
* Design (e.g., network segmentation (demilitarized zone (DMZ), virtual local area network (VLAN), virtual private network (VPN), micro-segmentation), defense in depth, Network Access Control (NAC), segmentation for embedded systems, Internet of Things (IoT))
* Cloud (e.g., service level agreement (SLA), managed service provider (MSP), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), hybrid)

# Exam Essentials: What you need to know

#### Golden Keys:

##### Security and attacks at each layer of the OSI model

* Architecting Network segmentation
* Network monitoring and management

#### The network security challenge:

##### Confidentiality

##### Integrity

##### Availability

#### Network Components

* Firewalls
* IDS and IPS
* DMZ and Extranet

#### Wireless Networks

##### IEEE 802.11

* Cellular
* Satellite

# Important Terminology

#### Network — two or more devices that can communicate

#### IEEE 802.11 — standards for wireless local area networks (WLAN)

#### IPSec — Internet Protocol Security – a suite of protocols used to protect IP traffic

#### TLS — Transport Layer Security - the replacement for Secure Socket Layer (SSL) to protect traffic at the transport layer

#### Firewall — A device that acts as a gateway and regulates traffic between two network s

#### Egress Monitoring — Monitoring the traffic going out of a network

#### Botnet — Short for Robotically Controlled Network, a network of devices that is controlled remotely often through applications called Zombies and via a Command and Control (C2) server

#### VLAN — Virtual Local Area Network – a logical network as compared to a physical network. A VLAN may be configured as a series of ports on a physical switch or as ports located on different switches

#### Load Balancing— The distribution of workload across multiple devices or channels .

#### Router — a piece of electronic equipment that connects computer networks to each other, and sends information between networks (Cambridge dictionary)

#### Switch — a piece of equipment on the network that receives electronic data and sends it to the right place

#### MODEM — modulates and demodulates electrical signals. Transforms digital data into analog and visa versa

#### LAN — Local Area Network a network of devices connected [usually] within a local, limited area

#### WLAN — Wireless Local Area Network a network that connects devices over a wireless LAN

# Self-Assessment Questions: Test your Understanding

###### A bank wants to provide financial services to its clients. What type of network communication is most common?

###### Application layer encryption

###### Transport Layer Security (TLS)

###### Internet Protocol Security (IPSec)

###### Link Layer encryption

###### Which layer of the OSI stack is responsible for secure communications between two adjacent devices?

###### Data link layer

###### Application layer

###### Network layer

###### Transport layer

###### What type of attack can alter traffic between two hosts?

###### SMURF attack

###### Ping of Death attack

###### Man-in-the-middle attack

###### SYN Flood attack

###### An improperly configured router would be an example of a:

###### Threat event

###### Threat agent

###### Compensating control

###### Vulnerability

###### What type of attack would send malicious traffic over port 53?

###### Mail relay

###### DNS tunneling

###### IP spoofing

###### Wannacry

###### Where is a web application commonly located on a network?

###### LAN

###### WAN

###### Extranet

###### DMZ

###### Which protocol assigns an IP address to a device that wants to connect to a network?

###### DHCP

###### HTTP

###### ARP

###### MAC

1. Which layer of the OSI stack relies on data provided by the application at the source?
   1. Intermediate Network
   2. Destination Transport
   3. Destination Application
   4. Source Physical
2. Which technology can be used to securely connect an employee working remotely to corporate systems?
   1. Virtual LAN (VLAN)
   2. IEEE 802.11 Wireless
   3. Remote Procedure Call
   4. Virtual Private Network (VPN)
3. What does a botnet use to control infected machines?
   1. Email
   2. Zombies
   3. SPAM
   4. DNS Poisoning
4. Which of the following is a type of amplification attack – that amplifies the size of the attack?
   1. DNS Reflection
   2. Ping of Death
   3. Man-in-the-Middle
   4. ARP Poisoning
5. Which type of transmission is most reliant on line-of-sight?
   1. Ethernet
   2. WLAN
   3. Satellite
   4. IEEE 802.15
6. Which transmission media is the hardest to intercept?
   1. Optical fiber
   2. IEEE 802.11
   3. WEP
   4. Coaxial
7. What is an advantage of using SaaS instead of a locally managed application?
   1. Centralized management
   2. Faster response time
   3. Lower operating costs
   4. Better security
8. Which technology is designed to protect one network from another??
   1. Encryption
   2. DNS
   3. Firewall
   4. LAN

# Answers to Self-Assessment Questions:

###### B – TLS is most common for client to web-server communications. Application layer encryption is good for email and ftp. IPSec is used for remote working and LAN-to-LAN communications. Link layer encryption connect two adjacent devices such as a laptop connecting to a wireless access point using

###### A – Link layer encryption is used for wireless and for point-to-point connections using a stream-based algorithm installed on a chip. This is fast and secure

###### C – Am attacker in the middle of a communications session (MITM) may alter, delete or just listen to traffic between two parties. SMURF refers to a type of ICMP-based flooding at the network layer. The Ping of Death is a misconfigured ICMP packet. The SYN flood sends many TCP SYN requests to overwhelm a target. This is at the transport layer.

###### D – this is a vulnerability that may be exploited by a threat agent (or source) using a threat event. A compensating control is an additional control to address a weakness in other controls.

###### 

###### B – DNS usually uses port 53 – which is open on most systems to allow DNS to operate. Sending malicious traffic disguised as DNS traffic is DNS tunneling. Mail relay is based on misconfigured mail servers on port 25. IP spoofing takes advantage of no authentication of IPv4 headers. Wannacry was an attack (and still one of the most common types of malicious traffic seen in 2020) against a Windows Operating System.

###### D – A DMZ is a network commonly used for internet-facing services such as a web application. It is not recommended to place a web application on an internal LAN.A WAN (Wide Area Network) is used to transmit traffic between LANs. An extranet is also internet-facing in most cases, but it is a semi-trusted network that is used for employees working remotely or business partners and requires more authentication than a DMZ.

###### A – Dynamic Host Configuration Protocol assigns an IP address to a device that wants to connect to a network. HyperText Transfer Protocol is used at the application layer. ARP associates MAC addresses with IP addresses, The Media Access Control address is the address of the Network Interface Card that connects a device to a network.

###### C – the destination Application Layer reads the Application Header created by the source Application Layer to determine how to handle the incoming data. An intermediate network node will use Network and DataLink headers, The destination Transport Layer wil communicate back to the source transport layer in the case of TCP traffic. The Source Physical communicates over the physical medium with the Destination Physical Layer.

###### D – a VPN is a good solution to protect traffic to a remote employee. A VLAN is a type of logical network segmentation. Wireless may be used locally by either party to connect to a Wireless Access Point – preferably using encryption such as WPA2. RPC is a protocol used to communicate between systems.

###### B – Zombies are often used to control infected machines. Email and SPAM may be used to distribute infections but not to control the infected machines. DNS poisoning will send traffic to the wrong destination website.

###### A – a DNS reflection attack is often called a DNS Amplification attack. It allows the attacker to increase the size of the attack to cause a Denial of Service. The Ping of Death uses a very large ICMP packet to disable systems, but it does not amplify its attack size. The Man-in-the-Middle intercepts traffic either actively (altering traffic) or passively (monitoring traffic). ARP poisoning alters traffic routing but does not do amplificaiton.

###### 

###### C – a satellite signal needs line-of-sight between the satellite and the ground-based dish. This signal can be interrupted by obstructions such as buildings, snow, or heavy rain. Ethernet is used for wired LAN connections, and WLAN (IEEE 802.11) and IEEE802.15 (Wireless Personal Area Networks such as Bluetooth) do not require line-of-sight.

###### A – optical fiber is the hardest to intercept, not impossible but the hardest of the transmission medium provided in the answers. Wireless is easy to intercept and it is easier to intercept traffic on a coaxial cable than on fiber.

###### A – an advantage of a Software as a Service installed service as compared to a locally managed application is the centralization of management. This is better for access control, compliance, patching and support since those functions are managed together with the Cloud Service Provider instead of local staff who may not be present in remote offices. Since the SaaS requires internet access it may not be as fast to respond as a local application. There is no guarantee that either SaaS or a locally managed application is more secure than the other. SaaS is almost certain to have higher operating costs than a local application but a local application often has higher capital costs.

###### C – A firewall protects one network from another by examining and blocking undesirable traffic. It should monitor both incoming and outgoing (egress) traffic. DNS is concerned with routing of internet traffic to the correct location. A LAN is a local area network and is not concerned with traffic between networks. Encryption protects traffic from alteration or disclosure but may actually make the job of the firewall more difficult by hiding the traffic so that the firewall cannot examine it properly.