### C172 Study Guide – Updated 2/8/21\*\*\*\*

|  |
| --- |
| *Insights from my experience of taking the OA twice:*   * *The details about the specs of cables are not essential: if you know the basics of which cable is most likely to be used, you are in a good place. (T1, T3, Coaxial, UTP, Fiber Optic)* * *The specific details about 802.11 standards (frequency, ODFM vs DSSS, etc) were never asked on either OA I took.* * *Knowing the names of specific attack names was helpful on a few of the questions (smurf attack, teardrop, ping of death, bluejacking, etc.)—I would review these before the test.* * *Feel comfortable with the CIA triad and the AAA—there are about three question for each topic.* * *Know your OSI model—what physical components make up each layer, what protocols are used in each layer, and what each layer actually does.* * *Know your networks: PAN, LAN, MAN, WAN, WLAN, VLAN, etc.* * *There are roughly three questions about network commands (ipconfig, ping, etc.) and what they do.* * *Understand Firewalls and their uses.* * *Know the difference between switches, repeaters, hubs, routers, and modems*   *When in doubt, use the process of elimination—if you know what an option means, and it doesn’t make sense in the context, don’t consider it. Most questions I wasn’t sure about, I could wean down to two viable options because the other options didn’t even make sense. For example, for some OSI questions, a couple of the options weren’t actual layers on the OSI model.*  *\*\*\* Update 2: A reddit user created a flash card set and quiz that I think is beneficial so I’m adding the link here.* [*https://quizlet.com/401533092/c172-wgu-complete-v3-flash-cards/*](https://quizlet.com/401533092/c172-wgu-complete-v3-flash-cards/)    *\*\*\*\*Update 3 (FunAdministration334) I’ve formatted this to be shorter, for printing purposes. I’ve edited typos and misinformation, to the best of my ability. Notes are a very personal thing, so please make a copy and alter it in a way that suits your own learning needs. 1/21/2021*  *\*\*\*\*\*Update 4 (8 Feb 2021 geek-girls-r-fun) Updated study guide with info from the cohorts and updates about the OA from other Redditors. Studied this guide with an experienced IT friend for 12 hours, updated the study guide for an additional 6 hours and passed the first time. I used this quizlet:* [*OA&PA Study Guide by kamerasheree*](https://quizlet.com/445441958/wgu-c172-network-and-security-foundations-pa-and-oa-set-flash-cards/)*. I used the Match feature of quizlet to make the learning more interesting. I did not read the text aside from Unit 2 for details on Basic Network commands but I did work on a helpdesk about 25 years ago so I have an idea of how networking & security work. Watched videos by Messer on* [*OSI*](https://www.youtube.com/watch?v=G7aVKgGUe9c) *& Firewalls (links in guide below). I tried the quizzes recommended in the Course Tips and found OSI Layers, Command-Line Utilities & Networking Attacks to be relevant. I took the PA twice, once right before the OA.* ***NOTE: Immediately after taking the OA, I revised this study guide to REMOVE anything that I didn’t see on the test. Yellow highlights are things I remember being on the OA.*** |

# Introduction to Networking Concepts (38% of assessment)

## Network Devices

Recommended Video: [Understanding the OSI Model - CompTIA Network+ N10-007 - 1.2 - Professor Messer IT Certification Training Courses](https://www.professormesser.com/network-plus/n10-007/understanding-the-osi-model-2/)

Objectives:

* Identify wired networking devices based on function.
* Identify wireless networking devices based on function.
* Identify security networking devices based on function.

|  |
| --- |
| ***Examples***  a. The NIC functions at the data link by using a unique MAC address.  b. The router is a network device that is used to connect two or more network segments by performing OSI layer 3 functions like packet-forwarding.  c. The router is responsible for implementing NAT (network address translation)  d. The file server is used as a shared storage for all member nodes of a LAN. |

*Notes: There were at least 4 straightforward questions about various OSI Layers. I memorized this table and wrote it down on my whiteboard before starting the OA.*

***A****ll* ***P****eople* ***S****eem to* ***N****eed* ***D****ata* ***P****rocessing. Messer video on* [*OSI*](https://www.youtube.com/watch?v=G7aVKgGUe9c)*.*

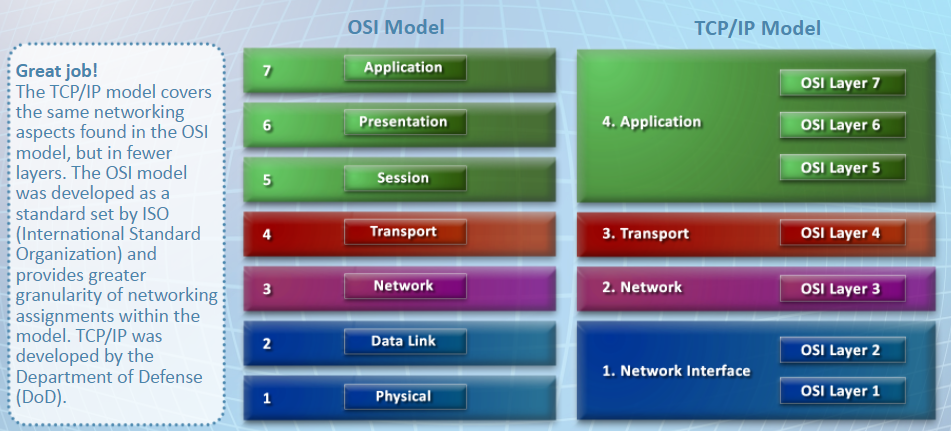
|  |  |  |  |
| --- | --- | --- | --- |
| ***OSI Layer*** | ***Unit*** | ***Physical Component & Function*** | ***Protocols*** |
| *7* ***A****pplication* |  | *Application software, network applications. Anything you can see with your eyeballs like web browsers and email.* | *HTTP, FTP, SMIP, IMAP, SMTP* |
| *6* ***P****resentation* |  | *Data conversion utilities. Protocol Conversion, data translation.* ***Data encryption/decryption.*** | ***SSL****, ASCII, JPEG, MIDI, MPEG, GIF, MP3, MP4* |
| *5* ***S****ession* |  | *Network Operating System. Establishes, manages & terminates sessions* | ***NFS****,* ***SQL****, PPTP, NetBIOS, PAP, SCP (tunneling)* |
| *4* ***T****ransport* | *segments* | *Network Operating System. Ensures Error Free Packets* | ***TCP*** *(segments so no missing packets),* ***UDP*** *(datagrams for streaming like games), SCTP* |
| *3* ***N****etwork* | *Packets* | ***Router****, Layer 3 switches. Provides routing decisions. NAT, PAT* | ***IP****, IPX, IPSec, RIP, IPv4, IPv6, ICMP* |
| *2* ***D****ata Link* | *Frames* | ***Switches****, NIC, Token Ring, Frame Relay, Bridge. Provides for flow of data. NIC FUNCTIONS at this layer. Bits pass over physical layer between devices on a LAN (collision domain).* | ***MAC addresses****, ARP, PPP, HDLC, LLC*  *Communication at MAC-address level - forwards packets on Layer 2 devices, like a bridge.* |
| *1* ***P****hysical* | *Bits* | ***802.11****, Repeater, Modem, Bluetooth, Ethernet, hubs, Network Cabling,* ***Wi-Fi****. Signals & Media.* | *DSL, ISDN, physical NICs, twisted pair cable, fiber. Questions about “medium” refer to cabling.* |

## TCP/IP and OSI Models

Objectives:

* Identify the OSI model.
* Identify the TCP/IP model.
* Identify protocols, data units, and devices to the given OSI layer.
* Identify the type of data that a networking device processes.

|  |
| --- |
| ***Examples***  a. The network is the OSI layer related to the function of the IP protocol suite.  b. The data link is the OSI layer responsible for organizing how bits are passed over the physical layer between devices within the same collision domain.  c. The transport layer makes sure packets of data are received correctly and resends them if they are not.  d. TCP and UDP perform functions of OSI layer 4. |

*Notes:*

*There were 2 questions about the function of the TCP/IP Layer functions. Such as which 3 OSI layers are in the TCP/IP Application layer?*

|  |  |  |
| --- | --- | --- |
| ***TCP/IP*** | ***OSI*** | ***Function*** |
| *(4) Application* | *(7) Application* | *Contains message, supports network applications.* |
| *(6) Presentation* | *Coding, compression, encryption. Protocol Conversion, data translation.* |
| *(5) Session* | *Aggregates connections for efficiency, synchronization, recovery. Establishes, maintains, terminates connection.* |
| *(3) Transport* | *(4) Transport* | *Ensures error-free packets. Transfers & re-sends messages. Responsible for breaking up data into segments.* |
| *(2) Network* | *(3) Network* | *Handles routing of datagrams, source to destination. IP addressing takes place. Provides routing decisions. NAT, PAT* |
| *(1) Network interface* | *(2) Data Link* | *Aggregates bits to frame and performs data transfer between neighboring network elements. Physical addressing takes place. Provides for flow of data. NIC FUNCTIONS at this layer.* |
| *(1) Physical* | *Deals with transmission of bits over copper, fiber, or radio. Physical NICs are here. Questions about “medium” refer to cabling.* |

## Network Commands

Objectives:

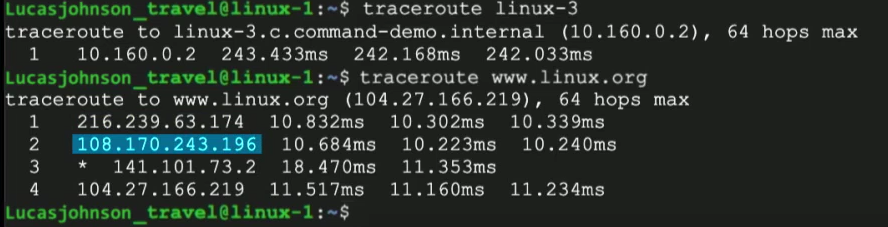
* Identify common networking commands.
* Identify common networking models.

|  |
| --- |
| ***Examples***  a. The ftp protocol allows a user to authenticate to a remote server, navigate the server’s file structure, and upload and download files.  b. Traceroute is a network diagnostic tool that displays the path packets take between two endpoints. |

*Notes:*

*I looked at Unit 2, watched the videos and ran each of these commands for myself, paying extra attention to nmap.* ***\*I removed notes for commands that I don’t remember on the OA\****

*Traceroute: Determine the number of hops required for a packet to reach its destination.*



*Nslookup: Determine IP address of domain name.*

*Ping: Determine IP address and latency in network.*

*Netstat -a: Display IP ports currently open on the Windows OS.*

*Whois: information about a webserver including contact information.*

*ARP: (Address Resolution Protocol) displays the IP to physical (MAC) address mappings for hosts that have been discovered in the ARP cache. ARP can be used to add, remove, or modify entries in the ARP cache. The hosts need to be on the local network, as these addresses are discovered by broadcasting to everyone on the network and noting the reply from the owner; broadcast traffic is not allowed through a router so that the system will maintain the MAC address of the router.* ***IP🡺MAC Address***

*Nmap: (Network Mapper) scans networks to see what it can find in terms of hosts and open ports (including well-known ones for many applications). It is commonly used to determine what is deployed on a network for vulnerability analysis, security scans, and related activities.*

## Network Media

Objectives:

* Identify the correct type of connector for the networking cable.
* Identify the correct type of network cables for a networking need.
* Identify 802.11 standards.
* Identify IEEE 802.3 standards.

|  |
| --- |
| ***Examples***  a. The CAT 6a is an ethernet cable that can maintain 10GBps transmission speeds through the course of its maximum 100-meter length.  b. The patch panel is a device used to organize network cables as they run between switches and other network devices.  c. The ethernet uses UTP cable and CSMA/CD to manage connected devices’ access to the wire. (802.11x uses CSMA/CA). |

*Notes:*

**\*I removed all network media that I do not remember being on the OA\***

*Fiber Optic: use light instead of electricity. Can* ***go longer distances, faster****. More durable and secure. Like transatlantic submarine cables.*

## Network Topologies

Objectives:

* Identify diagrams of various network topologies.
* Identify descriptions of various network topologies.
* Identify the standard or cable that corresponds to a network topology.

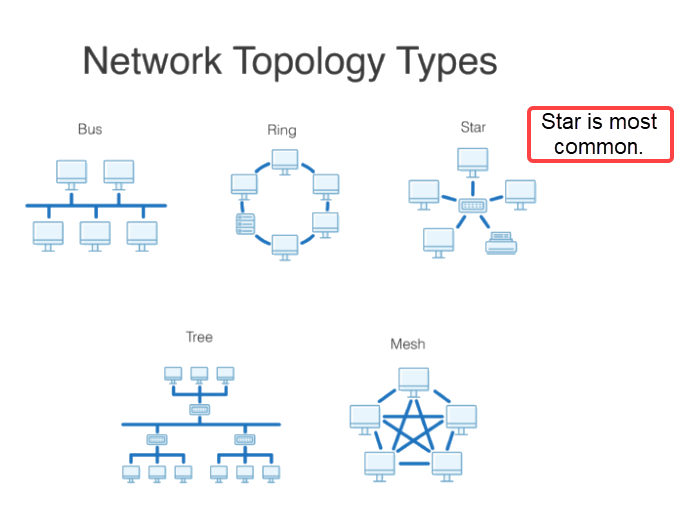
|  |
| --- |
| ***Examples***  a. In a ring topology, the nodes are connected to each other with a backbone cable that loops around and ends at the same point it started.  b. A mesh topology is where all nodes cooperate to distribute data amongst each other. |

*Notes: There were at least 3 topology questions. There were no pictures on the OA. Read the topologies section of the text as a refresher (I wish I had).*

*Bus topology: coaxial cable, Thinnet. A bus network topology is a single line of devices connected together by one shared network cable.*

*Ring topology: Each node connects to exactly two other nodes, forming a single continuous pathway for signals through each node. Nodes connected to each other with a backbone cable that loops around and ends at the same point it started.*

*Star topology: hub or switch in center. Each device is only connected to the central switch. All device-to-device communication is sent through the switch at the center of the network and then forwarded by the switch to the proper destination.*

*Mesh topology: Connects every node to every other node in the network.* *Mesh topologies are often drawn as a web of direct connections between computers or nodes in a network.* *Mesh networks are typically used where communication within a network must be highly available and* ***redundancy is needed****. The nodes within a mesh network can communicate with each other, and these connections can be changed dynamically if one node were to fail.*

## Network Types

Objective:

* Identify various network types based on a description or diagram.

|  |
| --- |
| ***Examples***  a. In a LAN network, you can wire multiple PCs to a home router.  b. A WLAN infrastructure connects network devices and printers through a central access point without the use of cabling.  c. The CAT 5e is commonly used within a 1000Mbps Ethernet network. |

*Notes:*

*There were 2 or 3 questions about these various network types:*

*PAN (personal area network) – any bluetooth/network device connected to your PC*

*LAN (local area network) – small network like home if not wireless.*

*WLAN (wireless LAN) – small network that is wireless like my home.*

*WAN (wide area network) – the world wide web*

*VLAN (Virtual LAN) – use a switch to create a virtual segment within a LAN. Ie; HR department might be on its own VLAN.*

## Hypervisors

* ***The two types of hypervisors***
  + ***Type 1 hypervisor****: Also called b****are- metal*** *hypervisors. This hypervisor is* ***loaded directly on the hardware*** *to abstract the hardware to the virtualization layer and is commonly used on servers.*
  + ***Type 2 hypervisor****: This hypervisor is an app loaded on an operating system and abstracts the virtualization layer through its host operating system and is commonly used on personal computers. Ie; Microsoft Virtual PC, Oracle Virtual Box, VMware Workstation,*

## Cloud Computing

* ***Cloud service/cloud computing*** *is an outsourced and hosted computing environment that delivers IT services via a network. Gmail, OneDrive, etc.*
* Cloud Computing Models
  + ***Infrastructure as a Service (IaaS):*** *Focuses on the facilities and infrastructure in the data center. Entire machines like private servers or VPS. AWS.*
  + ***Platform as a Service (PaaS):*** *focuses on application development on any desired platform utilizing cloud computing. Examples are Web Servers, database servers, MS Teams.*
  + ***Software as a Service (SaaS):*** *Focuses on application delivery. Examples are Gmail, google drive, MS OneDrive, Zoom*
* Cloud Infrastructures
  + ***Public cloud:*** *This cloud infrastructure is owned and operated by the cloud service company but made available for general public use. Gmail, google drive, MS OneDrive, Zoom*
  + ***Private cloud:*** *This cloud infrastructure is operated by the organization and made available only to members of the organization. For example, Gmail is installed on the internal server of a university. It’s an instance of Gmail that’s exclusively used by the university as a private cloud infrastructure.*
  + ***Community cloud:*** *This cloud infrastructure offers two or more organizations exclusive access to the infrastructure and computing resources. These organizations may share common policies that allow them to operate in a distributed mode. For example, police in different counties (organizations) can log into the state software. Another example: researchers at a university studying the environment can log into the environmental tracking software run by the state. The university researchers are an organization & the state researchers are an organization – they both access the cloud software as a community.*
  + ***Hybrid cloud:*** *This cloud infrastructure offers a combination of at least one private cloud and one public cloud. Most often used for retail companies who need to scale up quickly. A company has its own web servers but buys additional cloud servers to help with high volume traffic over the holidays.*

|  |
| --- |
| ***Examples***  a. Which cloud-hosting model provides exclusive cloud access for a single company?  b. Which type of hypervisor is loaded on an operating system and abstracts the virtualization layer through its host operating system and is commonly used on personal computers? |

# Introduction to Network Security (33% of assessment)

## Attacks, Threats, Risks, and Vulnerabilities

Objectives:

* Identify types of security attacks.
* Identify types of security threats.
* Identify types of attackers.
* Identify the cause of network vulnerabilities.
* Select the appropriate risk response to a network type of risk.
* Identify types of security mitigation.
* Identify types of attacks or attackers.
* Identify the seven steps of cyber-attacks.
* Identify how to prevent a cyber attack.

|  |
| --- |
| ***Examples***  a. Know the definitions for the following exploits: spoofing, ARP poisoning, Denial-of-Service, Smurf attack, port scanning, wiretapping, sniffing, buffer overflow, session hijacking, phishing, man-in-the-middle, zero-day, brute-force, bluesnarfing, etc.  b. Know the vulnerabilities (and remedies for the following): weak passwords, default passwords, BYOD, misconfigured firewall rules.  c. Know the purposes of/when to use: VPN, firewall, network filtering appliances, training for employees (education), patching. |

*Notes: I removed a bunch of the attacks because I don’t remember them on the OA. There were at least 4 attack related questions. If you are unsure, read the text about attacks.*

*Security Vulnerabilities*

*Not all attackers are malicious or bad actors; some hackers are actually good and help companies protect their networks. In fact, there is an entire branch of InfoSec jobs known as penetration testers who are tasked with attempting to compromise a network’s security.*

*Vulnerability Testers: scan servers & network devices for known vulnerabilities. Typically good guys. Outside consultants may scan the network and point out vulnerabilities & how to fix.*

*Insider Threats*

*Some of the most potent threats come from people within your organization. Because they have legitimate access to systems, they are in a position to hack from the inside of the network, often undetected. Furthermore, a disgruntled insider may have a motive. Whenever you combine motive and opportunity, you have a substantially increased risk of trouble.*

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Name** | **Description** | **Mitigation/OSI Layer** |
| Database Control | SQL Injection | Attackers take control of the database by entering SQL into the input boxes on a website instead of entering basic text. | Application (7)  Review source code & validate all user-entered data. Firewall: use reverse proxy system and scan incoming packets for malicious behavior. Use web-application firewall with rules to filter dangerous requests. Enable NX-bit (no-execute) functionality on physical computer. |
|  | Buffer Overflow | Buffer overflow is similar to SQL Injection but instead of SQL, they enter too much information into the form which causes the app to crash or other damage. | Application (7)  Coding to prevent too much input. Firewall to prevent suspicious data from being sent. Enable NX-bit (no-execute) functionality on physical computer. |
| Spoofing | Man in the Middle (MitM) | MitM impersonates both the sender & the receiver to intercept communication between two systems. A hacker hijacks a session between trusted client and network server. | MitM attacks occur in various OSI Layers  Although MITM uses IP spoofing at its base, it goes a mile beyond that in order to gain control, by choosing sessions from one or more layers to be hijacked.  Intrusion Prevention systems and IPSec can help. |
|  |  |  |  |
|  | VLAN Hopping | A method of attacking networked resources on a virtual LAN (VLAN). An attacking host on a VLAN gains access to traffic on other VLANs that would normally not be accessible. | Data Link (2)  Configure the switch Access Control File. |
| Denial of Service | Denial of Service (DoS)  Distributed Denial of Service (DDoS) | Denying service to a computer, network or network server by overwhelming the victim with large amounts of useless traffic. A computer is used to flood a server with TCP and UDP packets.  A DDoS attack is where multiple systems target a single system with a DoS attack. The targeted network is then bombarded with packets from multiple locations. | Transport (4) – [DoS in other OSI Layers](https://us-cert.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf)  DDoS attack blocking, commonly referred to as blackholing, is a method typically used by ISPs to stop a DDoS attack on one of its  customers. Basically, the site is taken down entirely so other sites on the network are not affected. |
|  | Ping of Death | Attacker pings the target & sends a ICMP packet over the max of 65,535 bytes and causes the victim’s system to crash or stop functioning. Causes buffer overflow and crashes. | Network (3)  Update operating systems. Configure Web Application firewall to drop malformed packets. |
|  | Ping Flood (Starts with Ping Sweep) | A Ping Sweep is an information gathering technique which is used to identify live hosts by pinging them. After the sweep, attacker overwhelms victim’s computer with a large amount of ICMP echo-request packets (pings). | Network (3)  Configure firewall to disallow pings (stops outside attacks not inside). Use intrusion prevention systems at network and host levels. |
|  | SMURF DDoS (distributed attack) | Rather than one computer sending ICMP packets, multiple computers are replying to the ICMP packet. It spoofs the source address for all ICMP packets | Network(3) & Transport (4)  Disable IP-directed broadcasts on your router. Reconfigure your operating system to disallow ICMP responses to IP broadcast requests. Reconfigure the perimeter firewall to disallow pings originating from outside your network. |
|  | Deauth Attack | Deauthentication (abbreviated deauth) is a denial-of-service (DoS) attack where the attacker can force any client (or even every client) off of the network. | Presentation (6)  The simplest defense is to use WPA3 security on your WAPs because in WPA3, the management packets are encrypted. If it is not possible to use WPA3, at least use WPA2 to make sure the data traffic is encrypted. |
| RPC Attack | RPC Exploit | A specially crafted RPC request is sent. Successful exploitation of this vulnerability could execute arbitrary code within the context of another user. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. | Session (5)  Mitigate with regular OS and application patching. Use of proxy  firewalls and intrusion detection devices can prevent many RPC and NetBIOS attacks. |
| Social Engineering | Phishing/Spear Phishing | User clicks on a link to a nefarious site which tricks them into entering their name/email address or other secure info. Ie; sending an email about your PayPal account which isn’t from PayPal.  Spear Phishing targets a person with extremely specific information – hacking a CEO’s phone with a specific calendar invite for their kid’s soccer practice. | Training on how to recognize & report phishing emails.  How to stop at the networking level? I don’t know, firewall?? but you should figure this out before taking the test. |

## Malware Attacks & Response

Objective:

* Identify appropriate mitigation responses for different types of malware.

|  |
| --- |
| ***Example***  a. A user notices that data seems to be missing or altered and computer settings are sometimes changed randomly. The user knows that no one else has physical access to the computer, and antivirus software scans do not detect any culprits. Which action should be taken to identify the problem? *(Install software to look for and remove rootkits.)* |

*Notes:*

How deal with rootkits, backdoor attacks, and Trojan horses. Run complete antivirus and anti-malware scans on your systems regularly and keep the virus definitions as up-to-date as possible to help you detect new and emerging threats.

*What helped me here was to go through the different malware threats/exploits/attacks, and go through each one and use google or the text to figure out how to combat/mitigate that attack.*

*For example: for rootkits, you need to make sure to have firewall, antivirus software, and make sure your patches are up-to-date.*

*Malware Attack*

*Viruses: Attaches itself to a file or host. (Many types!). Anti-virus software to mitigate.*

*Worms: Do not attach to a host file, they are self-contained programs. Don’t download attachments. Anti-virus software.*

*Trojans: Hides in a useful program. Use firewall software to mitigate.*

*Rootkits: Malware hidden in a host’s file system, quite hard to detect. Avoid opening suspicious emails & don’t download cracked software. Anti-malware w/rootkit detection. Keep OS updated.*

*Ransomware: Blocks victim’s data—threatens to publish it or delete it unless a ransom is paid. Scan all emails for known malware strains, and keep firewalls and endpoint protections up to date with the latest known malware signatures.*

*8) Zero day: Exploits a vulnerability in the OS software—requires a patch to be remedied. Zero day refers to the fact that the exploit was released before security vendors can issue protection against them. The public has no way to fix until a patch is released.*

## CIA Triad

Objective:

* Identify categories of the confidentiality, integrity, and availability (CIA) triad.

|  |
| --- |
| ***Examples***  a. An analyst has identified an active denial of service attack. Which category of the CIA triad is affected? (*availability)*  b. investigating a security incident, a technician discovers an unauthorized packet-capturing tool on the network. Which category of the CIA triad is being attacked? (*confidentiality)* |

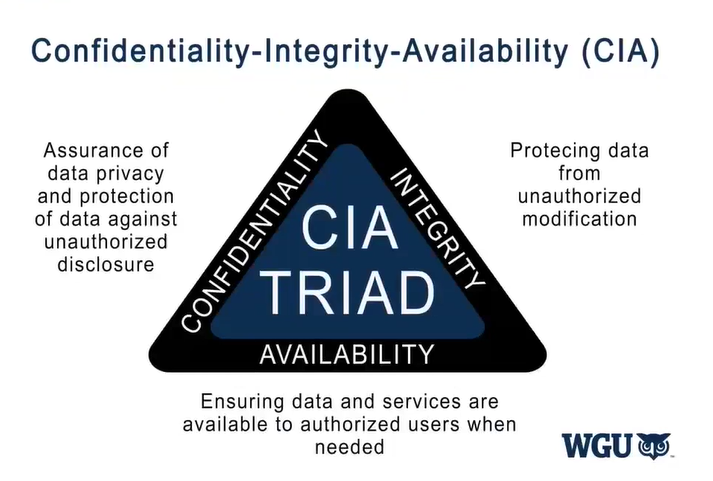
*Notes: There were at least 3 questions on this. Memorize the triangle and the examples I’ve listed here – they are from the cohort and were definitely on the test. Write this info on your whiteboard before starting the test and answering these questions will be easy.*

*Three most important components of security:*

***Confidentiality****: the access to information should be granted only on a need-to-know basis. A person in the customer support department should not have access to the HR database. Unencrypted info, Deleted files not completely purged, physical theft of a device, social engineering. Ie; User forgets to lock their screen and another person hops on and looks through email.*

***Integrity:***  *the information should not be tampered with from source to destination. Any time data is changed. Man in the Middle attacks, employee changes their salary $$ in the database.*

***Availability:*** *The services of an organization should be available. Denial of service Distributed Denial of Service attacks. Unable to access the system. User locked out after 3 tries of password. Changes to access list (intentional or accidental). Ie; email server crashes.*



## AAA

Objective:

* Identify categories of the AAA (authentication, authorization, and accounting)

|  |
| --- |
| ***Example***  A server is out of storage and fails to write to the log files. Administrators are still able to remotely log in and review logs. Which category of AAA is affected in this scenario? |

*Notes: There were 3 scenario based questions on the test. Memorize these and the examples and write them on your whiteboard before taking the test. When you get to these questions, they will be easy to answer. Look for more examples if you are unclear.*

***Authentication:*** *Who and what are you? (First step.) Username/password issues.*

***Authorization:*** *What are you allowed to do? (Second step.) Access rules. Administrative limitations.*

***Accounting:*** *Keeps track of what you do. (Final step.) Log files – anything with log files..*

***The order is important when answering scenario questions!!!***

# Network Security Operations (29% of assessment)

## Firewalls

Goals:

* Identify types of firewalls.
* Identify how firewall features will secure a network.

|  |
| --- |
| ***Examples***  a.Which network device is usually placed in-line between a trusted network and an untrusted network? *(Firewall)*  *b.* What are the different types of Firewalls? Which is considered most secure? Which one requires the most CPU? |

*Notes:*

*Messer –* [*Understanding Firewalls*](https://www.youtube.com/watch?v=roygo23ojEM) *(6minutes) & Messer –* [*Universal Security Control of Firewalls*](https://youtu.be/mDKKqPxMpb0) *(9mins)*

***Firewall:*** *A part of a computer system or network designed to block unauthorized access while permitting outward communication. Protection for one network from another. Network based firewalls filter traffic at OSI Layer 4 (TCP/UDP) (some can filter through Layer 7- application firewalls). Most firewalls are also Layer 3 routing devices that sit on the ingress/egress of a network – a central device that sits between you and the internet. Firewall rules are called Access control Lists – the ACLs allow or disallow traffic based on tuples (tuples = groups of variables like Source IP, Dest IP, Port Number, time, etc).*

*Types:*

* ***Packet Filtering Firewall:*** *A limit is placed on the packets that can enter the network. Compares traffic against pre-established criteria. Explicit ports must be opened to allow incoming and outgoing traffic Packet filtering can also limit information moving from one segment to another. Looks at data headers.*

*>>Operates at Layer 3 (the IP Layer) and Layer 4 ( the TCP and UDP port numbers)*

* ***Stateful Inspection Firewall:*** *EVERY packet is analyzed, categorized and a security decision is made. The inbound and outbound data packets are compared to determine if a connection should be allowed. This includes tracking the source and destination port numbers and sequence numbers as well as the source and destination IP addresses. Automatically creates rules to permit traffic based on communication type. Needs 1 rule to establish a session. Looks at data headers.*

*>>Operates at Layers 3, 4, 5.*

* ***Stateless Firewall:*** *Does NOT keep track of traffic flows (no sessions). Needs 2 rules (one to reach destination port, another to allow traffic to come back). Traffic sent outside an active session will be stateless.*
* ***Proxy Server:*** *Some firewalls are configured as proxies. You make a request to the firewall then the firewall makes its own request on your behalf to the internet. It then examines the response that it gets back for malware/danger and sends it to you if its safe. The client gets access to the network via the proxy server. This step is used to authenticate the user, establish the session, and set policies. The client must connect to the proxy server to connect to resources outside the network. Hides your IP address. Looks at actual data inside packets.*
* ***Application Level Firewall*** *(sometimes known as a proxy firewall). Blocks program-level traffic. Analyzes packet content. Modern firewalls are application-aware. They operate at Layer 7 (Application). Called application layer gateway, stateful multilayer inspection, deep packet inspection or next-gen. For example, you might be able to view Twitter but not post to Twitter because the application (stateful) firewall knows exactly what you should be allowed to do. Requires decode of the packets. Looks at actual data inside packets.*

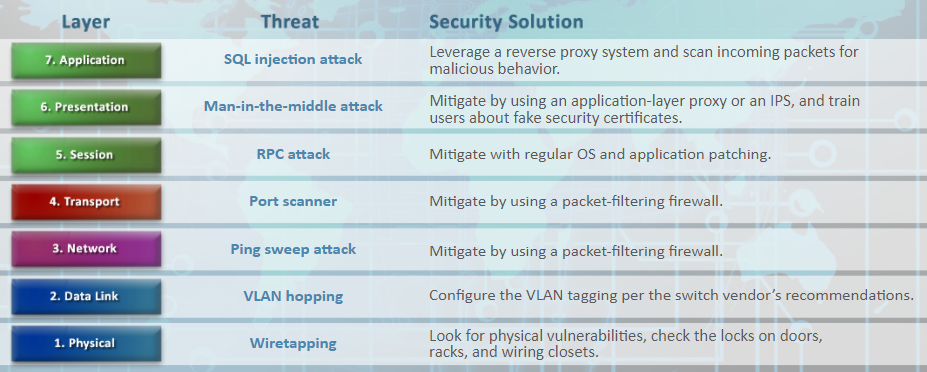
*>>Operates at Level 7 (and below)*

## Transport layer security

Objectives:

* Determine how to address a network risk at the transport layer.
* Apply network security protocols at the transport layer.
* Identify security protocols used to address network vulnerabilities at the transport layer.

|  |
| --- |
| ***Examples***  a. Which protocol is affected when a malicious user is targeting weaknesses in HTTPS? *(The secure sockets layer, or SSL)*  b. Which attack tricks a client into mapping an IP address to a spoofed MAC address? *(ARP spoofing)*  c c. Which type of port has access to all VLANs by default in a traditional layer 2 switch? *(Trunk)* |

*Notes: This table comes from the cohort. Pay close attention to VLAN hopping.*  

Another Layer 2 attack targets Ethernet switches that separate traffic into multiple logical networks called virtual local area networks (VLAN). When configuring a switch with VLANs, the network administrator typically configures each switch port to operate in one of two modes: access mode (also called untagged mode) or trunk mode (also called tagging mode).

When a computer is attached to an access port, it may only send and receive traffic on the VLAN assigned by the switch; the computer has no control over the VLAN selection. On the other hand, if a network administrator **mistakenly configures a computer's switch port as trunk mode**, the computer may be able to send and receive traffic on any VLAN on the switch.

## Wireless security

Objectives:

* Identify Wi-Fi vulnerabilities.
* Identify Wi-Fi security protocols.
* Identify wireless security standards.

|  |
| --- |
| ***Examples***  **Which type of wireless security protocol is the most secure?** (WPA2+AES)  **What is AES encryption?** Advanced Encryption Standard. A modern block cipher that supports three key lengths of 128, 192, and 256-bit encryption. It provides excellent long-term security against brute-force attacks.  **What is 3DES encryption?** In cryptography, Triple DES, officially the Triple Data Encryption Algorithm, is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block. The Data Encryption Standard's 56-bit key is no longer considered adequate in the face of modern cryptanalytic techniques and supercomputing power |

*Notes: I don’t remember anything about WEP v WPA2 or WPA3 specifically. However, there was at least one Ad-hoc v Infrastructure question.*

*WEP uses PSK (pre-shared key) and RC4 algorithm. It is weak.*

*WPA uses RC4 algorithm and TKIP (Temporary Integrity protocol) which rekeys after every 10,000 packets. (Better than WEP)*

*WPA2 uses AES and CCMP. (Most Used.)*

*WPA3 – strongest but newer so not used as much yet. When asked a question about which is best, always look at the WP# - the higher, the better.*

*Wireless Network Infrastructure Modes*

*Ad-hoc*

*In ad-hoc mode, all wireless communication is performed in a peer-to-peer fashion and does not require or involve a WAP. Ad-hoc wireless networks are rarely used in homes or offices, but they can be helpful in setting up a new device, such as a printer by connecting them directly, much as one would do with a physical cable. Ad-hoc networks are also occasionally used to transfer files between devices, such as between a camera and a laptop.*

*Infrastructure*

*In almost all cases, a WAP or wireless router is used to connect wireless devices to the network. The WAP acts like an Ethernet switch in wired networking and often has a physical cable that connects it to the rest of the network. A wireless router is a WAP and a router combined into a single device and is most often used in home and small business environments to connect to the internet while also providing wireless connectivity for nearby devices.*

## Encryption Techniques

Objectives:

* Determine the correct encryption type or technique to use to protect an OSI layer.
* Identify different types of cryptography.
* Distinguish between symmetric and asymmetric encryption.
* Apply encryption techniques to the OSI layer.
* Identify encryption types that can be used to protect the OSI layer.
* Determine how encryption techniques can be used to protect the OSI layer.

|  |
| --- |
| ***Example***   1. What is end-to-end encryption?   *Data is encrypted on the sender’s system and only the recipient is able to decrypt it.* |

*Notes: There were 2 questions on keys.*

*Symmetric encryption: have same key.*

*Asymmetric encryption: one public and one private key.*

*SSL: Secure Socket Layer uses an asymmetric key pair. Offers end-to-end encryption.*

*TLS: Transport Layer Security: It is the successor to SSL (basically the improved version.)*

## IDS/IPS

Objective:

* Identify types of intrusion detection systems (IDS) or intrusion prevention systems (IPS).

|  |
| --- |
| ***Example***  Which feature of a network intrusion prevention system (NIPS)  uses a list of known bad IP addresses to protect the network? (*Reputation-based prevention)* |

*Notes:* ***IDS/IPS:*** *Systems that identify misuse and anomalies on a network.*

* ***IDS:*** *An Intrusion Detection System is designed to monitor both inbound and outbound data traffic and report on any suspicious activity that could indicate an attack.*
* ***IPS:*** *An Intrusion Prevention System has the capability to stop or prevent malicious attacks that it detects in real time by interacting with the firewall. Firewalls can detect application-specific vulnerability signatures.*
* ***Packet Shaper:*** *A device that sits between a campus network and an outside network and is configured with a set of rules that are used to prioritize data traffic for shaping the bandwidth*

