**Module 3 Review**

1. What is an IP address? IP address is your device’s digital address or its unique identifier.
   1. What is the purpose? IP address is needed to communicate on a TCP/IP network.
   2. What is the structure? IP address usually contains 32-bit numbers formatted four 8-bit separated by periods and will contain two component of a network ID and the host ID. Each 8-bit field represent a byte of the IP address. It will usually be in a format such as xxx.xxx.xx.xx with the network ID always coming before the host ID.
   3. What is the difference between IPv4 and IPv6? IPv4 is 32-bit while IPv6 is 128-bit IP address. IPv6 will contain letters while IPv4 won’t. Ipv4 are separated by periods while IPv6 is separated by colons. IPv4 use ARP (address resolution protocol) to map MAC address when IPv6 uses NDP (neighbor discovery protocol) to map MAC address.
   4. What is the highest number used in IPv4? The highest number used in IPv4 is 255, with the lowest being 0.
   5. What are the classes of IP addresses? A, B, C, D? There different classes of IPv4 address based on the first three bits of the IP address. Classes differ in how many networks of each class can exist and the number of unique hosts that each can accommodate.

* Class A are within the first bit set as 0 (between 0 to 127) and is designed for large networks. Network uses 8 bits leaving 24 bits for host identification, meaning it could hold up to 16,777,214 hosts.
* Class B have the first two bits set at 10 (between 128 to 191) designed for medium sized network. They split 16/16 for network and host ID bits which allows 16,384 host with as many as 65,534 host per network.
* Class C have the first three bits set at 110 (between 192 to 223) for smaller networks. Network portion is 24 bits, only 8 bits for host ID. Allows for 2,097,152 networks but each network can only have a max of 254 host.

1. What is a MAC address? Every network interface card have their own unique MAC address, connected with switches, for use as a network access within a network segment.
   1. How is it assigned? It is assigned by the Network interface card
   2. What is the length? It is 48 bits long written in hexadecimal for example B6-15-53-8F-29-6B
   3. Can it be changed? They are hardcoded into the network card so they cannot be changed but there is tricks and ways you can still change it.
   4. What is the purpose? The purpose is to identify which device is which and allow the router to transfer data into the specified address.
2. Difference between TCP and UDP. TCP is connection-oriented while UDP is connection-less. TCP is guaranteed to be delivered while UDP might not provide guaranteed delivery. TCP also uses a flow control so that user will not be overwhelmed by data while UDP does not have flow control.
   1. How are TCP connections established? When the sending TCP wants to establish connections, TCP sends a segment that is called a SYN to the TCP protocol on the receiving host. The receiving TCP returns a segment that is called an ACK to acknowledge the successful receipt of the segment. The sending TCP sends another ACK segment, then proceeds to send the data.
   2. What are common types of TCP connections? HTTP and HTTP/2
   3. What are common types of UDP connections? NTP TFTP DHCP RTSP
3. What are the differences between these network devices.
   1. Gateway - If the host needs to communicate outside the local network, it also needs a default gateway, which is normally the internal address of the router.
   2. Bridge - Bridges operate in the Data Link layer (Layer 2) of the OSI model. They join similar topologies, and they are used to divide network segments into multiple collision domains. Bridges isolate network traffic, preventing unwanted traffic from entering a segment when there are no recipients on that segment.
   3. Router - Routers connect multiple network types and determine the best path for sending data. They can route packets across multiple networks and use routing tables to store network addresses to determine the best destination. Routers operate at the Network layer (Layer 3) of the OSI model. Because of this, they make their decisions on what to do with traffic based on logical addresses, such as an IP address.
   4. Switch - Switches work at Layer 2 and they provide centralized connectivity, just like hubs. Hubs pass along all traffic, but switches examine the Layer 2 header of the incoming packet and forward it properly to the right port and only that port. (sender to receiver)
   5. Repeater – a device that receives a signal, amplifies it, then sends it out, usually use for cable extension
   6. Hub – used to link several PC together, they repeat any signal that comes in 1 port and copy it to the other ports.
   7. VPN - a secure (private) network connection that occurs through a public network
   8. Firewall - a hardware or software solution that serves as your network’s security guard.
   9. DMZ - Some firewalls have a third network port for a second semi-internal network. This port is used to connect servers that can be considered both public and private, such as web and email servers, this is known as DMZ.
   10. SSL - cryptographic protocols designed to provide communications security over a computer network.
   11. TLS – successor to SSL, now more popular than SSL
4. What is a wireless network?
   1. Advantages
   2. Disadvantages
5. Define and describe the following.
   1. Phishing
   2. Pharming
   3. Whaling
   4. Wardriving
   5. Spoofing
   6. Virus
   7. Worm
   8. Trojan
   9. R.A.T.
6. Principles of Authentication- When giving a user permission on a computer, only give them the permissions they need to do their work and nothing else.
7. Principles of Password security- password should be unique to yourself, it should be very difficult to guess, should be too complex to memorize, should be well-managed, and some passwords should have a second password (aka F2A).
8. Incident response evidence collection- When an alerts happen and there is something suspicious on the networks, a person could come in to collect digital evidence that a breach has happened.
9. What is Personally Identifiable Information? PII is is anything that can be used to identify an individual person on its own or in context with other information.
   * 1. Risks – could causes millions of monetary damages if a security breach happen containing those information
     2. Types – linked and linkable information
     3. Examples – someone’s credit card, phone number address, other contact information.
10. What is TCP/IP? Is a model and set of communication protocol used by all computer on the internet.
    * 1. What does it do? It allows computer on the internet to interact with each other/ Specify how they transfer data from one device to another.
      2. When was it invented? It was invented in the 1960s.
      3. Who invented it? It was developed by the US department of Defense, or Defense Advanced Research Projects Agency to be exact.
      4. What are the layers? The four layers are Process/Application, Host2Host, Internet and Network access
      5. What protocols are associated with each layer? The most commons protocols are:

Telnet FTP LDAP SNMP DHCP SMTP HTTP HTTPS

TCP UDP

ICMP ARP RARP IP

Ethernet Fast Ethernet Gigabit Ethernet 802.11

Protocols – what are they and what is the standard port:

HTTP

HTTPS

HTMP

URL

FTP

SMTP

DHCP

P2P

VLAN

SSH

RDP

1053

7850

161

Commands: ipconfig

Nslookup

Ping Hostname

tracert