Day-12

.....

Today I completed two more networking courses from the platform “Infosys Springboard” related to Network Attacks and how to be precautious towards these types of attacks and another course on Solving Network related issues by monitoring and analyzing the network using the platforms like wireshark and how to use command prompts to recognize and solve the issue. This both courses help me in securing cloud infra. The details are given as follow:

The course on “CompTIA Network+: Common Network Attack Types” help me understand different types of Network attacks like DoS, DDoS, Social Engineering, DNS Spoofing, VLAN hopping attacks, MAC flooding attacks, ARP poisoning attacks, etc. I also learned how to be precautious from these types of attacks by regular monitoring your network, having antivirus and anti-malware software and if the attack happens then learning from it. Some of the attacks I have explained below:

1) **DoS:** DoS stands for Denial of Service. It throws more network traffic to slow down or corrupt your service. It is done from a single device.

2) **DDoS:** DDoS works same as DoS but the attack is done from different devices or bots.

3) **Social Engineering:** This attack is done to an individual by falsely letting him believe that the attacker or its attack source is legitimate and then exploits its vulnerability by gaining personal/important information of the individual.

4) **DNS Spoofing:** It is done by changing DNS record to malicious site and gaining crucial information of the user and its device.

The second course I learnt was “CompTIA Network+: Solving Networking Issues”. I learned about the various tools used to analyze and monitor network. I also saw software tools like Wireshark which are used to monitor network. I also got a lot of information about command prompts like ipconfig, ipconfig /?, ipconfig /all, ipconfig /release, ipconfig /renew, arp –a, netstat –ano, power inline, etc.

These commands provide lots of information about the network and with the help of that we can solve the network related issue. Some of the CLI prompts and their working are written below:

1) **ipconfig:** Shows basic network information like IP address, subnet mask, etc.
2) **ipconfig /?:** Shows every ipconfig commands information.
3) **ipconfig /all:** Shows detailed network info like MAC address, DNS server etc.
4) **ipconfig /release:** Remove the current IP address.
5) **ipconfig /renew:** Requests a new IP address from the DHCP server.
6) **ipconfig /flushdns:** Clears the DNS resolver cache.
7) **ping 127.0.0.1:** Tests the lookback to check local network adapter (is okay or not).
8) **arp -a:** Shows the ARP (Address Resolution Protocol) table, which shows relation of IP addresses to MAC addresses**.**
9) **netstat -ano:** Shows active network connections.
10) **power inline:** Shows the power consumption and total power capacity of a PoE (Power over Ethernet) switch.

PoE: Power over Ethernet (PoE) is used to transfer power through the Ethernet cable by using the spare pairs that were available in an UTP cable. It is very useful as we can connect very crucial Data Center EMS devices like Temperature monitor, Humidity monitor, Dust levels monitor, CO2 levels monitor, I/O control, with PoE as it helps in managing Power consumption, is quite scalable and also helps in preventing overloads.

I have attached completion certificate of both courses for authentication: