**Module 8: Sniffing**

* **Sniffing:**
* a process of monitoring and capturing all data packets passing through a network.
* Grabbing Information of Systems/machines without the web.
* Hijacking normal traffic through the network.
* **Types of Sniffing:**
* Passive Sniffing: only listening/monitoring the traffic.
* Active Sniffing: Sniffing traffic using tools and technique and manipulating the traffic.

* **MAC Flooding:**
* overwhelming a switch’s MAC address table by flooding it with a massive amount of spoofed Ethernet frames, each containing a unique source MAC address.
* **MAC Flooding Attack:**
* Attacker: kali linux
* Victim: Window 11
* Tool: macof (in kali)

**Steps:**

1. Turn on both kali linux & Window 11
2. In Kali os, goto terminal > run cmd “sudo apt install dsniff” to install macof tool
3. Open wireshark on both kali linux & window 11
4. In kali os, run cmd “sudo macof -h” for tool help command

(note: -s for source, -d for destination, -i for interface, -n for times)

1. Turn on wireshark and start capturing traffic in same interface in both sides.
2. Run cmd “ sudo macof -i eth0 -n 10” > enter
3. Check the traffic on each side and also check mac address flooding
4. The result is mac flooding.

* **DHCP Starvation:**
* flooding the DHCP server with DHCP requests to consume all available IP addresses that the DHCP server can allocate.
* Client sending continuous DHCP discover message to DHCP server without listening to DHCP offer from server.

* **DHCP Starvation Attack:**
* Attacker: kali linux
* Victim: DHCP Server
* Tool: Yersinia

**Steps:**

1. In kali os, goto terminal> run cmd “sudo apt install Yersinia” to install tool
2. Run cmd “ sudo Yersina -h “ for help
3. Run cmd “ sudo Yersina -I ” using yersina in interactive mode.
4. Press “F2” for Dhcp Starvation > press “x” for dhcp attack (x means dos attack)
5. Press “1” for dhcp starvation
6. Check dhcp discover status in wireshark.

* **ARP Spoofing:**
* An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices.

Machines: window 11 & Kali Linux

Victim : window 11

Man in the middle: kali os

Tool: arpspoof

**Steps:**

1. In kali os, goto terminal > run cmd “sudo arpspoof -h”
2. Open wireshark in both machines.
3. Run cmd “sudo arpspoof -i eth0 -t 10.10.10.11 10.10.10.100”

(arpspoof -i INTERFACE -t VICTIM\_IP GATEWAY\_IP)

(window 11 ko ip 10.10.10.11 haina 10.10.10.100 chai ho vanera bewakuf banauxa)

1. Check the status of arp in window 11, run cmd “arp -a”

* **ARP poisoning:**
* sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table

Sender: Window 11

Receiver: Win -Server 2019

Sniffer: Win -Server 2022

(Scenario: Window 11 Access server 2019 and window server 2022 grab/ sniff the traffic)

Tool: Cain & Abel (in window server 2022)

**Steps:**

1. In Server 2022, Goto backup drive > CEH Tools > Sniffing > Arp Poisoning tools > Cain & Abel tool > Install
2. Goto cain & abelo tool > goto configuration tab > verify the ip address (checking interface for grabbing)
3. Goto left panel and select the icon next to file icon for starting grabbing > select sniffer tab
4. Select (+) icon and assign ip range > check All Tesk > ok
5. Select ‘ARP’ for Arp Poisoning
6. Click inside white box then select server 2019 and window 11

(one on left side and one on right side) > ok

1. Select “ARP” icon
2. Run cmd “arp -a” command in both machine server 2019 & window 11
3. Then in window 11, goto cmd and run cmd “ ftp 10.10.10.19” to access ftp server from windows 11.
4. Again goto window server 2022 > Cain & Abel tool > goto password tab > check the sniffed data.

* **MAC Changing:**
* Changing original mac address of the machine
* **MAC Changing in Windows 11: TMAC Tool**

**Steps:**

* Install tool > goto cmd prompt > run cmd ‘ipconfig /all’ > check the mac address
* Run ‘ tmac tool’ & check the details of nic card and mac
* Select ‘Random MAC Address’ > Change now

* **MAC Changing in Kali linux: Macchanger tool**

**Steps:**

* Goto terminal > run cmd ‘ macchanger -h’
* For MAC Lookup “ Sudo macchanger -s eth0” (eth0 is interface)
* For New MAC “Sudo macchanger -a eth0”
* For reverting back to original mac “Sudo macchanger -p eth0”