Module - 7
# Sniffing

Types of Tapping :

1. Active :
- Man in the middle
- Monitor/Record Traffic
- Able to Change Data

2. Passive :
- Eavesdropping / Snooping
- Monitor / Record Traffic
- No Changing of data

# Sniffing Dangers :

1. DNS Traffic 2. Telnet Password 3. FTP passwords 4. Router Configs 5. Email Traffic 6. Web Traffic 7. Chat Session. 8. Syslog Traffic

# Switch Port Stealing : This is extremely useful to sniffed in the switched environment when the ARP Poisioning can't be done , it floods the lan with ARP packets. The Destination MAC address of each stealing packet is the same as the attacker while the source Mac address is one of the victim's MAC address.
It steals the port from the victim then attacker send it to the destinated port.

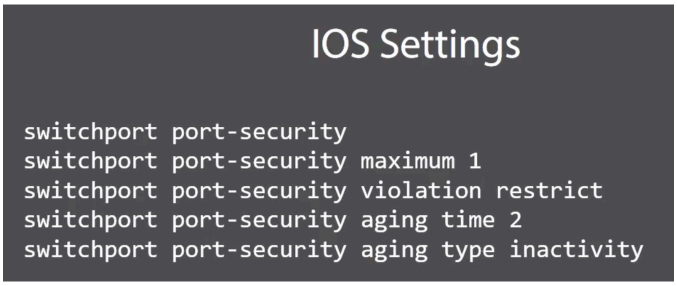
# Software for Sniffing :

1. Wireshark
2. Omnipeak
3. SoftPerfect NPA
4. Microsoft Network Monitor

# DHCP Assualt Concept :
1. A Refresher on DHCP
2. The Starvation
   - Yersinia
3. Going Rogue

# Countermeasure :

Stopping DHCP Starvation & Rogue Attacks
- Enable Port Security
  - Set Max number of MAC address
  -



IOS Settings

```
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

Absolute or inactivity :

Absolute Aging all the secured address on this port go out exactly after the minutes we descibe and are remove from the secured address list.

For Inactivity : The Secure address on this port go out only if there'no data traffic from the secured source for a specific time.

To stop Rogue attacks :
1. DHCP Snooping : Stop ports from responding DHCPOffer
2. Windows "World" : Authorized DHCP in AD (Active Directory)

# Big Mac Attack :

1. What's a MAC ?
2. Flooding : MAC Table reaches to Full then it start flooding out packets, another ways to sniff is SPANs Port (Port Mirroring)

# Countermeasures :

1. Port Security
2. Use AAA Security

# ARP Spoofing :

1. Forge your way : malformed arp reply
2. Overload the Switch
3. Overload results in a new mode
4. Flood the target

# Tools :

1. Dsniff : Password Sniffing and network analysing tool
2. Arpspoof
3. Ettercap
4. Cain & Abel

# IRDP Spoofing :

ICMP Router Discovery Protocol : It is a routing protocol that allow a host to discover the IP address of the active router and get out to the Internet.

IRDP doesn't require any authentication so the target host will prefer the default route defined by the Attacker and update their table

# Dangers of ARP Attacks :

1. DoS
2. Packet Sniffing
3. VoIP Tapping
4. Man in the Middle
5. Session Hijacking
6. Data Interception
7. Connection Hijacking
8. Manipulating data
9. Steal Passwords
10. Connection Resetting

# Countermeasures :

1. Dynamic Arp Inspection :

It intercept all the ARP requests and responses that go across the network
Each IP address will then be analysed

2. DHCP Snooping :

DHCP server records all the IP address and MAC address so by combining these two features we bind the Mac to ip

3. Static ARP Tables :

4. ARPWatch : Looks at ARP Traffic on a network and logs a pairing of IP addresses and MAC addresses along with a time stamp and alert the Administrator if someone try to spoof the those paired IP and MAC address.

# DNS Poisioning :

-> Intranet Poisioning
-> Internet Poisioning
-> Proxy Server Poisioning
-> Poisioning the Cache

# Intranet Poisioning :

This is going to be poisioning within the inside. Attacker sits between the connection and listens to all the DNS query
Tools used : arpspoof, dnsspoof, Cain and Abel

# Internet Poisioning :

When we search any site :
1. First it check its site
2. Then it check for the “Hosts” file
3. Then it check its ip address settings
4. Local DNS Server is also an Option

# Proxy Server Poisioning :

Procy Server just catches the website

# Poisoning the Cache :

Cache is used for faster name resolution but the problem is cache can be updated and edited. So the attacker can poison the cache on that server and make modification to the database and redirects everybody to their own site.

# Countermeasures for Sniffing :

# Detecting Sniffing Methods :

- Find the Device which is working in **promiscuous mode**
- Detect Sniffing via **Ping** :
  When the device is not in promiscous mode then it will discard the ping but if the device is in promiscous mode then it will reply back even if the MAC address is wronge.
- Detect Sniffing via **ARP** :
- Detect Sniffing via **DNS**

# Protection from Sniffing :

1. Encryption
2. Static MAC for Gateways
3. Physical Access Level Protection (Closed Unused Port)
4. Upgrade to IPv6
5. Switch off network ID Broadcast
6. Static Ips
7. Static ARP Entries
8. HTTPS
9. SFTP
10. VPNs/IPSec
11. SSL/TLS
12. Wireless Security
13. Direct MAC Retrieval
14. Tools

# Nmap to Find Sniffer :

```
nmap —script=sniffer-detect <ip_address>
```