**Module 8: Sniffing**

**Packet Sniffing**

* Turn the NIC of a system to promiscuous mode.
* Two types of Ethernet environments, sniffers work differently in each
  + **Shared Ethnernet**
  + **Switched Ethernet**
* Sniffing is possible using the following methods
  + **ARP Spoofing:** ARP is stateless, a machine can send an ARP reply even without asking for it and it can accept such a reply.
  + **MAC Flooding:** Siwtches have limited memory, once the memory is fully consumed, the switch will enter **fail-open** mode, it starts acting as a hub by broadcasting packets to all the ports on the switch.
* Passive Sniffing:
* Sniffing through a hub, wherein the traffic is sent to all ports.
  + It involves moniroting packets sent by others without sending any additional data packets in the network traffic
  + All hosts on the network can see all the traffic in a network that uses hub.
  + Hub is mostly replaced with switches
* Active Sniffing:
  + Sniff a switch-based networkf
  + Inject ARP into the network to flood the switch’s CAM table
  + Techniques:
    - **MAC flooding,**
    - **DHCP attacks,**
    - **DNS poisoning,**
    - **Switch port stealing**
    - **ARP poisoning,**
    - **Spoofing attack**
* Hack the network using sniffer
  + Connect laptop to a switch port
  + Run discovery tool to learn about network topology
  + Identify a victim’s machine
  + Poison the victim’s machine by using ARP spoofing
  + Destine for the victim’s machine is redirected of the attacker
  + Extract passwords and…
* Protocols vulnerable to sniffing
  + **Telnet and Rlogin:** keystrokes including usernames and pass are in clear text
  + **IMAP (Internet Message Access Protocol):** clear text
  + **HTTP:** clear text
  + **SMTP** and **NNTP (Network News Transfer Protocol):** clear text
  + **POP:** clear text
  + **FTP:** clear text
* Sniffing in the **Data Link Layer** of the OSI model
  + Networking layer are designed to work independently of each other, if a sniffer sniffs data in the data link layer, the upper layers will not be aware of the sniffing

**Hardware Protocol Analyzers**

* A piece of equipment that **captures signals** without altering the traffic in a cable segment
* It can be used to monitor network usage and identify **malicious network traffic**
* It captures a data packet, decode it, and analyzes its content based on certain **predetermined rules**
* It allows the attacker to see individual **data bytes** of each packet passing through the cable

**SPAN (Switched Port Analyzer) Port**

* A port that is configured to receive a copy of every packet that passes through a switch
* **Cisco** switch feature, also known as **port mirroring**

**Wiretapping**

* The process of monitoring of **telephone** and **Internet** conversations by a third party
* Attackers connect a **listening device** to the circuit carrying info between two phones or hosts on the Internet
* It allow an attacker to **monitor, intercept, access**, and **record info** contained in a data flow in a communication system
* **Active Wiretapping:** Monitor, record, alter, and inject data into the …
* **Passive Wiretapping:** Only monitor and record the traffic and collects knowledge regarding the data it contains

**MAC address/CAM Table**

* Each switch has a fixed-size dynamic Content Addressable Memory (CAM) table
* MAC Address: **3 bytes OUI (Organizationally Unique Identifier)**+**3bytes NIC specific**
* When a CAM Table is full:
  + Additional APP request traffic floods every port on the switch
  + Change the behavior of the switch to reset to its learning mode, broadcasting on every port like a hub
  + This attack will also fill the CAM tables of adjacent switches
* **MAC Flooding:** Flooding of the CAM table with fake MAC address and IP pairs until it is full
* **macof:** A unix/linux tool that is a part of the dsniff collection. Send random source MAC and IP. Floow siwtch’s CAM table.

**Switch Port Stealing**

* Use MAC Flooding to sniff the packet
* Flood the switch with forged ARP packets with the target MAC as the source and his own MAC as destination
* A **race condition** of the attacker’s flooded packets and the target host’s packets occurs, thus the switch must change its MAC, binding constantly between two different ports
* If the attacker is faster, he will direct packets intended for the target toward his ports.
* The attacker now manages to steal the target’ switch port and sends ARP requests to the stolen switch port to discover the target host’s IP
* When the attacker gets an ARP reply, the target host’s switch port bindin has been restored, and the attacker can now sniff the packets sent toward targeted host.

**Defend against MAC Attacks**

* Configuring Post Security on Cisco Switch
* Only 1 MAC address allowed on the switch port
* Port security can be used to **restrict inbound traffic** from only a selected set of MAC addresses and limit MAC flooding attack

**DHCP**

* DHCP Server maintains TCP/IP configuration info
* DHCP Attack: An active sniffing technique used to steal and manipulate sensitive data.
* **DHCP Starvation Attack:** This is a **DoS** attack on the DHCP servers where the attacker broadcasts forget DHCP requests and tries to lease all the DHCP addresses available
* **DHCP Starvation Attack Tools:** Yersinia, Hyenae
* **Rogue DHCP Server Attack:** A rouge DHCP server responds to DHCP request with fake IP addresses resulting in compromised network access. Work in conjunction with the **DHCP starvation attack.**
* Defend against DHCP starvation and Rogue Server Attacks:
  + **Enable port security** to defend against DHCP starvation attacks
  + **Enable DHCP snooping**, allowing the switch accept a DHCP transaction directed from a trusted port

**ARP**

* A stateless protocol used for resolving IP to MAC address
* ARP Spoofing
* Threats of ARP Poisoning:
  + Packet sniffing
  + Session hijacking
  + VoIP call tapping
  + Manipulating data
  + MitM attack
  + Data interception
  + Connection hijacking
  + Connection Resetting
  + Stealing Password
  + DoS Attack
* ARP Poisoning Tools: **arpspoof, Ettercap,BetterCAP**
* Defend against ARP Poisoning: Implement **Dynamic ARP Inspection** using HDCP snooping binding table
* ARP Spoofing detection tool: XArp

**MAC Spoofing/Duplicating**

* MAC duplication attack is launched by sniffing a network for MAC of clients who are actively associated with a switch port and re-using one of those addresses
* MAC duplication can be used to bypass wireless access points’ MAC filtering
* Tools: Technitium MAC Address Changer, SMAC

**IRDP (ICMP Router Discovery Protocol) Spoofing**

* A routing protocol that allows a host to discover the IP of active routers on their subnet by listening to router advbertsement and soliciting messages on their network
* The attacker sends a spoofed IRDP router advertisement message to the host on the subnet, causing it to change its default router to whatever the attacker chooses.
* Allow attackers to sniff the traffic and collect valuabnle info from the packets
* Launch MiTM, DoS, and passive sniffing attacks

**VLAN Hopping**

* A technique used to target network resource present on a VLAN
* Can be performed by using two primary methods, **Switch Spoofing** and **Double Tagging**
* Attackers perform VLAN hopping attacks to steal sensitive info, install malicious codes or programs, spread virus….
* **Switch Spoofing:** Attackers connect a rouge switch onto the network by tricking a legitimate switch and thereby creating a trunk link between them.
* **Douvle Tagging:** Add and modify tags in the Ethernet frame, thereby allowing the flow of traffic through any VLAN in the network

**STP Attack**

* Attackers connect a **rouge switch** into the network to change the operations of the **STP protocol** and sniff all the network traffic
* Attackers configures the rouge switch such that its priority is less than that of any other switch in the network, which makes it the root bridge, thus allowing the attackers to sniff all the traffic flowing in the network
* **STP**: Spanning Tree protocol ensures that the traffic follows an optimized path to enhance network performance

**Defend Against MAC Spoofing**

* **DHCP Snooping Binding Table,**
* **Dynamic ARP inspection**
* **IP Source guard**
* **Encryption**
* **Retrieval of MAC Address**
* **Implementation of IEEE 802.1X Suites**
* **AAA (Authentication, Authorization, Accounting)**

**Defend Against VLAN Hopping**

* **Defend against Switch Spoofing**
  + Configure the ports as access ports and ensure all access ports are configured not to negotiate trunks
  + Ensure all trunks ports are configured not to negotiate trunks
* **Defend against Double Tagging**
  + Ensure that each access port is assigned with VLAN except the default VLAN (VLAN 1)
  + Ensure that the native VLANs on all trunk ports are changed to an unused VLAN ID
  + Ensure that the native VLANs on all trunk ports are explicitly tagged

**Defend against STP attacks**

* **BPDU (Bridge Protocol Data Protocol) Guard:** Avoid the transmission of BPDUs on PortFast-enabled ports. Help in preventing potential bridging loops in the network
* **Loop Guard:** Protect the root bridge and ensures that it remains as the root in the STP topology, prevent nearby switches from being root switches
* **Root Guard:** Prevent it against the bridging loops, used to protect against a malfunctioned switch.
* **UDLD (Unidirectional Link Detection):** Enable devices to detect the existence of unidirectional links and further disable the affected interfaces in the network. There unidirectional links in the network can cause STP topology loops

**DNS Poisoning**

* Result in the substitution of a false IP address at the DNS level
* Posible using **Intranet DNS spoofing, Internet DNS spoofing, Proxy Server DNS poisoning, DNS Cache poisoning**
* **Intranet DNS Spoofing:** Work well against switches with ARP Poison Routing.
* **Internet DNS Spoofing:** Infect victim’s machine with a trojan and changes his DNS ip address to that of the attacker’s
* **Proxy Server DNS Poisoning:** Change victim’s proxy server setting in IE to that…
* **DNS Cache Poisoning:** Altering or adding forged DNS records into the DNS resolver cache.
* **Tools:** DerpNSpoof, Ettercap, DNS Spoof
* **Countermeasure:**
  + Iplement **DNSSEC (Domain Name System Security Extension)**
  + Use a SSL for securing the traffic
  + Resolve all DNS queries to a local DNS server
  + Block DNS requests being sent to ecternal servers
  + Configure a firewall to restrict ecternal DNS lookups
  + Implement IDS
  + Configure the DNS resolver to use a new random source port for each outgoing query
  + Restrict the DNS recusing service, to authorized users
  + Use NXDOMAIN (DNS Non-existent Domain) the Limiting

**Sniffing Tools**

* **Wireshark**
* Filters in Wireshark
  + Display Filtering by Protocol Example: Type the protocol in the filter box: arp, http, tcp, udp, dns, ip
  + Monitoring the Specific Ports
    - tcp.port==23
    - ip.addr==192.168.1.100 machine
    - ip.addr==192.168.1.100 && tcp.port=23
  + Filtering by Multiple IP Addresses
    - ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5
  + Filtering by IP Address
    - ip.addr == 10.0.0.4
  + Other Filters
    - ip.dst == 10.0.1.50 && frame.pkt\_len > 400
    - ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30
    - ip.src==205.153.63.30 or ip.dst==205.153.63.30
* Additional Filters
* **OmniPeek:** Display a google map
* **SteelCentral Packet Analyzer:** Provide a graphical console for high-speed packet analysis

**Countermeasure against Sniffing**

* **Restrict physical access** to network media
* Use **end-to-end encryption**
* Permanently add the **MAC address of the gateway** to the ARP cache
* Use **static IP and ARP table**s to prevent attackers from adding spoofed ARP entries
* Turn of **network identification broadcasts**
* Use **IPv6**
* Use **encrypted sessions**, **SSH** instead of **Telnet**, **SCP (Secure Copy)** instead of **FTP**, SSL for email
* Https instead of HTTP
* Switch instead of a hub
* SFTP instead of FTP
* PGP, S/MIME, VPN, IPSec, SSL/TLS, SSH and OPTs
* WPA, WPA2
* Retrieve the MAC directly from NIC instead of OS
* Detect promiscuous mode
* Use ACL to allow access to only a fixed range of trusted IP

**Sniffing Detection Techniques**

* Check the devices running in promiscuous mode
* Run IDS
* Run Network Tools
* **Ping Method:** Send a ping request to the suspect machine with its IP and an incorrect MAC. If **do not reject**,…
* **DNS Method:** A machine generating **reverse DNS lookup** traffic is suspious. Increase in network traffic can be an indication of the presence of a sniffer on the network.
* **ARP Method:** Only the machine in the promiscuous mode **caches the ARP info**. A machine in the promiscuous mode responds to the **ping message** as it has the correct info about the host sending the ping request in its cache, the rest of the machines will send an ARP probe to identify the source of the ping request.
* **Promiscuous Detection Tools:** Nmap’s NSE script, NetScan Tools PRO