**Network Sniffing**

Packet sniffing is the process of monitoring and capturing all data packets passing through a given network using a software application or hardware device. Sniffing is straightforward in hub-based networks, as the traffic on a segment passes through all the hosts associated with that segment. However, most networks today work on switches. A switch is an advanced computer networking device. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network.

**//Working of Sniffer**

Packet sniffing is the process of monitoring and capturing all data packets passing through a given network using a software application or hardware device. Sniffing is straightforward in hub-based networks, as the traffic on a segment passes through all the hosts associated with that segment. However, most networks today work on switches. A switch is an advanced computer networking device. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network.

**There are two basic types of Ethernet environments:**

* **Shared Ethernet environment**, a single bus connects all the hosts that compete for bandwidth. In this environment, all the other machines receive packets meant for one machine. Thus, when machine 1 wants to talk to machine 2, it sends a packet out on the network with the destination MAC address of machine 2, along with its own source MAC address. Sniffing in a shared Ethernet environment is passive.
* **Switched Ethernet environment**, the hosts connect with a switch instead of a hub. The switch maintains a table that tracks each computer’s MAC address and the physical port on which that MAC address is connected, and then delivers packets destined for a particular machine. The switch is a device that sends packets to the destined computer only; furthermore, it does not broadcast them to all the computers on the network. switch is more secure than a hub

**Sniffing the network is possible using the following methods:**

* **ARP Spoofing:** ARP is stateless. A machine can send an ARP reply even without asking for it; furthermore, it can accept such a reply. When a machine wants to sniff the traffic originating from another system, it can ARP spoof the gateway of the network. The ARP cache of the target machine will have an incorrect entry for the gateway.
* **MAC Flooding:** Switches maintain a translation table that maps various MAC addresses to the physical ports on the switch. As a result, they can intelligently route packets from one host to another. However, switches have a limited memory. MAC flooding makes use of this limitation to bombard switches with fake MAC addresses until the switches can no longer keep up. If this happens then switch start behaving like hub. macof is a utility that comes with the dsniff suite and helps the attacker to perform MAC flooding.

Once a switch turns into a hub, it starts broadcasting all packets it receives to all the computers in the network. By default, promiscuous mode is turned off in network machines; therefore, the NICs accept only those packets that are addressed to a user’s machine and discard the packets sent to the other machines. A sniffer turns the NIC of a system to promiscuous mode so that it listens to all the data transmitted on its segment.

**Types of Sniffing**

* **Passive sniffing** involves sending no packets. It simply captures and monitors the packets flowing in the network. A packet sniffer alone is not preferred for an attack because it works only in a common collision domain. A common collision domain is the sector of the network that is not switched or bridged. Common collision domains are present in hub environments. A switch eliminates the risk of passive sniffing still vulnerable to Active Sniffing
* Compromising physical Security
* Using a trojan horse
* **Active Sniffing** searches for traffic on a switched LAN by actively injecting traffic into it. Active sniffing also refers to sniffing through a switch. In active sniffing, the switched Ethernet does not transmit information to all the systems connected through LAN as it does in a hub-based network. Switches examine data packets for source and destination addresses and then transmit them to the appropriate destinations. However, attackers can actively inject ARP traffic into a LAN to sniff around a switched network and capture the traffic. Switches maintain their own ARP cache in Content Addressable Memory (CAM). CAM is a special type of memory that maintains a record of which host is connected to which port.
* MAC flooding
* DNS and ARP poisoning
* DHCP and spoofing attacks
* Switch port stealing

**How an attacker hacks the Network using Sniffers**

* Discover a switch and connect to it’s one of the ports.
* After successful connection to the network try to find network topologies.
* Analyse topologies to identify victim.
* Now use ARP spoofing techniques to send fake (spoofed) Address Resolution Protocol (ARP) messages.
* Last step helps to divert all the traffic from the victim’s computer to the attacker’s computer (man-in-the-middle (MITM)).
* Now attacker can see all the data packets sent and received by the victim.

**Protocols Vulnerable to Sniffing**

* **Telnet and Rlogin:** Telnet is a protocol used for communicating with a remote host (via port 23) on a network using a command-line terminal. rlogin enables an attacker to log into a network machine remotely via a TCP connection. Neither of these protocols provides encryption.
* **HTTP:** Due to vulnerabilities in the default version of HTTP, websites implementing HTTP transfer user data across the network in plaintext.
* **Simple Network Management Protocol (SNMP)** is a TCP/IP-based protocol used for exchanging management information between devices connected on a network.
* **Simple Mail Transfer Protocol (SMTP)** is used for transmitting email messages over the Internet.
* **Network News Transfer Protocol (NNTP)** distributes, inquiries into, retrieves, and posts news articles using a reliable stream-based transmission of news among ARPA-Internet community.
* **Post Office Protocol (POP)** allows a user’s workstation to access mail from a mailbox server.
* **File Transfer Protocol (FTP)** enables clients to share files between computers in a network. This protocol fails to provide encryption.
* **Internet Message Access Protocol (IMAP)** allows a client to access and manipulate electronic mail messages on a server.

**Sniffing in the Data Link Layer of the OSI Model**

The data link layer is the second layer of the OSI model. In this layer, data packets are encoded and decoded into bits. Sniffers operate at the data link layer and can capture packets from this layer. Networking layers in the OSI model are designed to work independently of each other; thus, if a sniffer sniffs data in the data link layer, the upper OSI layers will not be aware of the sniffing.

**Hardware Protocol Analyzer**

It is a device that interprets traffic passing over a network. It captures signals without altering the traffic segment. Its purpose is to monitor network usage and identify malicious network traffic generated by hacking software installed on the network. It captures a data packet, decodes it, and analyzes its content according to predetermined rules. They are capable of displaying bus states and low-level events such as high-speed negotiation (K/J chirps), transmission errors, and retransmissions. The analyzers provide accurate timestamps of the captured traffic.

**Switched Port Analyzer (SPAN)**

It is a Cisco switch feature, also known as “port mirroring,” that monitors network traffic on one or more ports on the switch. A SPAN port is a port that is configured to receive a copy of every packet that passes through a switch. It helps to analyze and debug data, identify errors, and investigate unauthorized network access. When port mirroring is on, the network switch sends a copy of the network packets from the source port to the destination port, which studies the network packets with the help of a network analyzer.

**Wiretapping**

Wiretapping or telephone tapping, refers to the monitoring of telephone or Internet conversations by a third party with covert intentions. To perform wiretapping, the attacker first selects a target person or host on the network to wiretap and then connects a listening device to the circuit carrying information between the two target phones or hosts.

* The official tapping of telephone lines
* The unofficial tapping of telephone lines
* Recording the conversation

Types of wiretapping:

* Active wiretapping is an MITM attack.
* Passive wiretapping is snooping or eavesdropping.

**Lawful interception (LI)**

It refers to legally intercepting data communication between two endpoints for surveillance on traditional telecommunications, VoIP, data, and multiservice networks. LI obtains data from a communication network for analysis or evidence. This is useful in activities like infrastructure management and protection, as well as cybersecurity-related issues.

**Sniffing Techniques: Mac Attacks**

**MAC Address**

MAC Address A MAC address uniquely identifies each node of a network. Each device in the network has a MAC address associated with a physical port on the network switch, which makes it possible to designate a specific single point of the network. MAC addresses are used as network addresses for most IEEE 802 network technologies, including Ethernet. The MAC address contains 12-digit hexadecimal numbers, divided into three or six groups. The first six digits indicate the manufacturer, while the next six digits indicate the adapter’s serial number.

**CAM Table**

A CAM table is a dynamic table of fixed-size. It stores information such as MAC addresses available on physical ports along with VLAN parameters associated with them. When a machine sends data to another machine in a network, the data passes through the switch. The switch searches for the destination MAC address (located in the Ethernet frame) in its CAM table, and once the MAC address is found, it forwards data to the machine through the port with which the MAC address is bound.

**Working of CAM Table**

Ethernet switch maintains connections between ports, and the CAM table keeps track of MAC address locations on the switch, but the table is limited in size. If the CAM table is flooded with more MAC addresses than it can hold, the switch will turn into a hub. The CAM table does this to ensure the delivery of data to the intended host.

* Machine A, Machine B, and Machine C, each holding MAC addresses A, B, and C. Machine A, holding the MAC address A, wants to interact with Machine B.
* Machine A broadcasts an ARP request to the switch. The request contains the IP address of the target machine (B) and IP & MAC address of source machine (A).
* Machine B possesses the target/destination IP address, so it sends an ARP reply along with its MAC address. The CAM table stores this MAC address along with the port on which this machine is connected.
* Now, connection is successfully established, and Machine A forwards the traffic to Machine B, while Machine C is unable to see the traffic flowing between them.

**MAC Flooding (CAM Table is full)**

MAC flooding is a technique used to compromise the security of network switches that connect network segments or devices. A CAM table’s limited size renders it susceptible to attacks from MAC flooding, which bombards the switch with fake source MAC addresses until the CAM table is full. The size of the CAM table is fixed, and as it can store only a limited number of MAC addresses in it, an attacker may send numerous fake MAC address to the switch. No problem occurs until the MAC address table is full. Once the MAC address table is full, any further requests may force the switch to enter fail-open mode. In the fail-open mode, the switch starts behaving like a hub and broadcasts incoming traffic through all the ports in the network.

**Switch Port Stealing**

The switch port stealing sniffing technique uses MAC flooding to sniff the packets. The attacker floods the switch with forged gratuitous ARP packets with the target MAC address as the source and his/her own MAC address as the destination. A race condition of the attacker’s flooded packets and target host packets will occur, and thus, the switch has to change its MAC address to bind constantly between two different ports. In this case, if the attacker is fast enough, he/she will able to direct the packets intended for the target host toward his switch port.

* Assume that there are three machines in a network: Host A, the target’s Host B, and the attacker’s Host C.
* Switch port stealing is used to spoof both IP MAC address of the target machine (Host B).
* Attacker’s machine runs a sniffer that turns the machine’s NIC adapter to promiscuous mode.
* Host A with IP address (10.0.0.1), wants to communicate Host B with IP address (10.0.0.2). Therefore, host A sends an ARP request.
* Switch broadcasts this ARP request to all the machines in the network.
* Before Host B, the attacker responds to the ARP request by sending an ARP reply containing the spoofed MAC and IP addresses.
* ARP cache in the switch records the spoofed MAC and IP addresses.
* spoofed MAC address of target Host B and the port connect to the attacker’s machine (Port C) and update the switch’s CAM table. Now, a connection is established between Host A and the attacker’s machine (Host C).
* Now, system will forward all the packets directed towards Host B to Host C through Port C.

**How to Defend against MAC Attacks**

Port security is a feature that identifies and limits the MAC addresses of the machines that can access the port. If you assign a secure MAC address to a secure port, then the port will forward only the packets with source addresses inside the group of defined addresses.

A security violation occurs

* When a port is configured as a secure port, and the maximum number of secure MAC addresses is reached
* When the MAC address of the machine that is attempting to access the port does not match any of the identified secure MAC addresses

Steps to restrict traffic through a port by limiting and identifying MAC addresses of the stations allowed to access the port:

* **interface interface\_id** Enters interface configuration mode and enters the physical interface to configure
* **switchport mode access** Sets the interface mode as access; an interface in the default mode cannot be configured as a secure port.
* **switchport port-security** Enables port security on the interface.
* **switchport port-security maximum value** Sets the maximum number of secure MAC addresses for the interface. (1 to 3072)
* **switchport port-security violation {restrict | shutdown}** Sets the violation mode, the action to be taken when a security violation is detected.
* **switchport port-security limit rate invalid-source-mac** Sets the rate limit for bad packets.
* **switchport port-security mac-address mac\_address** secure MAC address for interface.
* **switchport port-security mac-address sticky** Enables sticky learning on the interface.
* **end** Returns to privileged EXEC mode.
* **show port-security address** Verifies your entries.

**Sniffing Technique: DHCP Attacks**

**How DHCP works**

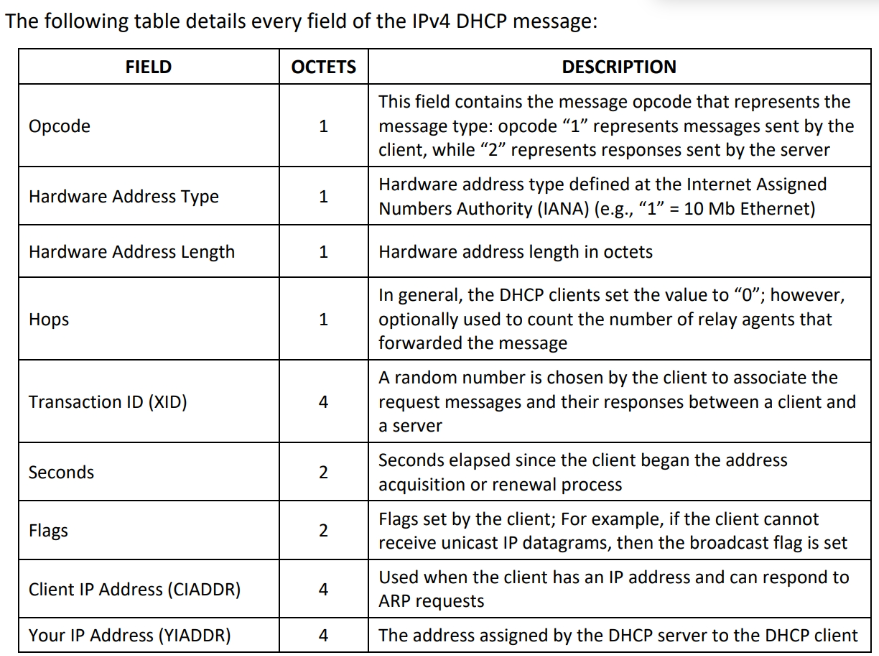
DHCP is a client–server protocol that provides an IP address to an IP host. In addition to the IP address, the DHCP server also provides configuration-related information such as the default gateway and subnet mask. When a DHCP client device boots up, it participates in traffic broadcasting. DHCP can assign IP configuration to hosts connecting to a network.

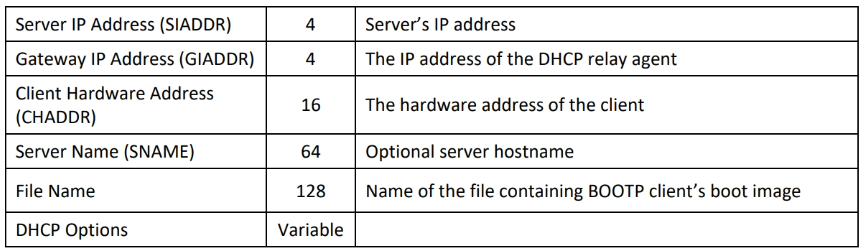
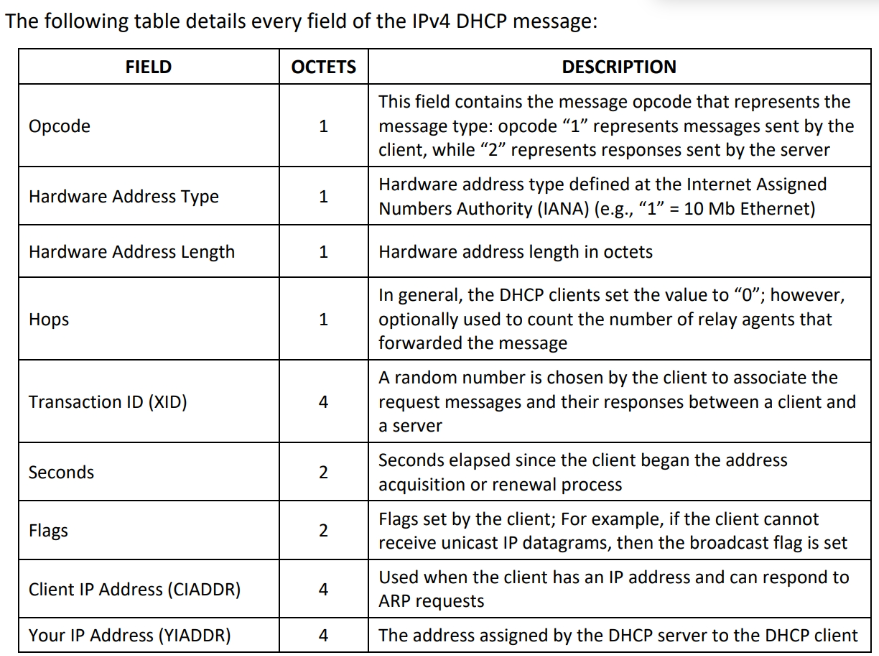
* Client broadcasts a DHCPDISCOVER/SOLICIT request asking for DHCP configuration Information.
* DHCP-relay agent captures client request and unicasts it to DHCP servers available in network.
* DHCP server unicasts DHCPOFFER/ADVERTISE, which has client’s and server’s MAC addresses.
* The relay agent broadcasts DHCPOFFER/ADVERTISE in the client’s subnet.
* Client broadcasts DHCPREQUEST/REQUEST asking the DHCP server to provide the DHCP configuration information.
* DHCP server sends a unicast DHCPACK/REPLY message to the client with IP configuration and information.

**DHCP Request/Reply Messages**

A device that already has an IP address can use the simple request/reply exchange to obtain other configuration parameters from a DHCP server. When the DHCP client receives a DHCP offer, the client immediately responds by sending back a DHCP request packet. A client can broadcast a DHCPINFORM message to request that any available server send its parameters on the usage of the network. DHCP servers respond with the requested parameters and/or default parameters carried in DHCP options of a DHCPACK message. If a DHCP request comes from a hardware address that is in the DHCP server’s reserved pool and the request is not for the IP address that this DHCP server offered, the DHCP server’s offer is invalid.

**IPv4 DHCP Packet Format**

DHCP enables communication on an IP network by configuring network devices. It assigns IP addresses and other information to computers so that they can communicate on the network in the client–server mode. DHCP has two functionalities: delivering host-specific configuration parameters and allocating network addresses to hosts. DHCP messages have the same format as that of Bootstrap Protocol (BOOTP) messages.

  
**DHCP Starvation Attack**

In a DHCP starvation attack, an attacker floods the DHCP server by sending numerous DHCP requests and uses all of the available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a DoS attack. Because of this issue, valid users cannot obtain or renew their IP addresses; thus, they fail to access their network.

Defend Against DHCP Starvation

Enable port security to defend against a DHCP starvation attack. Port security limits the maximum number of MAC addresses on the switch port. When the limit is exceeded, the switch drops subsequent MAC address requests (packets) from external sources

* **switchport port-**security configures the switch port parameters to enable port security.
* **switchport port-security maximum 1** configures the maximum number of secure MAC addresses for the port as 1.
* **switchport port-security violation** restrict drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed.
* **switchport port-security aging time 2** sets the aging time as 2 minutes.
* **switchport port-security aging type inactivity** sets the aging type as inactivity aging.

**Rogue DHCP Server Attack**

In addition to DHCP starvation attacks, an attacker can perform MITM attacks such as sniffing. An attacker who succeeds in exhausting the DHCP server’s IP address space can set up a rogue DHCP server on the network, which is not under the control of the network administrator. The rogue DHCP server impersonates a legitimate server and offers IP addresses and other network information to other clients in the network, acting as a default gateway.

In a rogue DHCP server attack, an attacker will introduce a rogue server into the network. This rogue server can respond to clients’ DHCP discovery requests. Although both the rogue and actual DHCP servers respond to the request, the client accepts the response that comes first. The DHCP response from the attacker’s rogue DHCP server may assign the IP address that serves as a client’s default gateway. As a result, the attacker’s IP address receives all the traffic from the client. The attacker then captures all the traffic and forwards it to the appropriate default gateway. The client thinks that everything is functioning correctly.

Defend Against Rogue Server Attack

The DHCP snooping feature that is available on switches can mitigate against rogue DHCP servers. It is configured on the port on which the valid DHCP server is connected. Once configured, DHCP snooping does not allow other ports on the switch to respond to DHCP Discover packets sent by clients.

Steps to configure DHCP snooping:

* **ip dhcp snooping** Enables DHCP snooping globally.
* **ip dhcp snooping vlan number [number] | vlan {vlan range}]** Enables or disables DHCP snooping on one or more VLANs. For example: ip dhcp snooping vlan 4,104
* **ip dhcp snooping trust** Configures the interface as trusted or untrusted.
* **ip dhcp snooping limit rate** Configures the number of DHCP packets per second (pps) that an interface can receive.
* **end** Exits configuration mode.
* **show ip dhcp snooping** Verifies the configuration.

**Sniffing Technique: ARP Poisoning**

**Adders Resolution Protocol (ARP)**

Address Resolution Protocol (ARP) is a stateless TCP/IP protocol that maps IP network addresses to the addresses (hardware addresses) used by a data link protocol. Using this protocol, a user can easily obtain the MAC address of any device on a network. Apart from the switch, the host machines also use the ARP protocol for obtaining MAC addresses. ARP is used by the host machine when it wants to send a packet to another device, and has to mention the destination MAC address in the packet sent.

The process of obtaining the MAC address using ARP is as follows:

* The source machine generates an ARP request packet containing the source MAC & IP address, and destination IP address, and sends it to the switch.
* Then, switch reads the MAC address of source and searches for this address in its CAM table.
* switch updates all new entries. If the entry is not found, the switch adds the MAC address and its incoming port to its CAM table and broadcasts ARP request packet into the network.
* Each device in the network receives the broadcast ARP request packet. Only the system with an IP address that matches the destination IP address replies with an ARP reply packet.
* The ARP reply message is then read by the switch, which adds the entry to its MAC table and forwards the message to the destination machine.
* Further, this machine updates the destination machine’s IP and MAC address entries into its ARP table, and now communication can take place.

**ARP Spoofing**

ARP packets can be forged to send data to the attacker’s machine. ARP spoofing involves constructing a large number of forged ARP request and reply packets to overload a switch. When a machine sends an ARP request, it assumes that the ARP reply will come from the right machine. ARP provides no means of verifying the authenticity of the responding device. Even systems that have not made an ARP request can accept the ARP replies coming from other devices. Attackers use this flaw in ARP to create malformed ARP replies containing spoofed IP and MAC addresses. Assuming it to be the legitimate ARP reply, the victim’s computer blindly accepts the ARP entry into its ARP table. Once the ARP table is flooded with spoofed ARP replies, the switch is set in forwarding mode, and the attacker intercepts all the data that flows from the victim’s machine  
  
**Working of ARP Spoofing**

ARP spoofing is a method of attacking an Ethernet LAN. When a legitimate user initiates a session with another user in the same layer 2 broadcast domain, the switch broadcasts an ARP request using the recipient's IP address, while the sender waits for the recipient to respond with a MAC address. An attacker eavesdropping on this unprotected layer 2 broadcast domain can respond to the broadcast ARP request and replies to the sender by spoofing the intended recipient’s IP address. The attacker runs a sniffer and turns the machine’s NIC adapter to promiscuous mode. It succeeds by changing the IP address of the attacker’s computer to that of the target computer. A forged ARP request and reply packet can find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends frames to the attacker’s computer, where the attacker can modify the frames before sending them to the source machine (User A) in an MITM attack.

**Threats of ARP spoofing**

* Packet Sniffing
* Session Hijacking
* VoIP Call Tapping
* Manipulating Data
* Man-in-the-Middle Attack
* Data Interception
* Connection Hijacking
* Connection Resetting
* Stealing Passwords
* DoS Attack

**How to Defend Against ARP Poisoning**

Implementation of Dynamic ARP Inspection (DAI) prevents poisoning attacks. DAI is a security feature that validates ARP packets in a network. When DAI activates on a VLAN, all ports on the VLAN are considered to be untrusted by default. DAI validates the ARP packets using a DHCP snooping binding table. The DHCP snooping binding table consists of MAC addresses, IP addresses, and VLAN interfaces acquired by listening to DHCP message exchanges. To validate the ARP packet, the DAI performs IP-address-to-MAC-address binding inspection stored in the DHCP snooping database before forwarding the packet to its destination. If any invalid IP address binds a MAC address, the DAI will discard the ARP packet. This eliminates the risk of MITM attacks. DAI ensures the relay of only valid ARP requests and responses.

**Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches**

To configure DHCP snooping on a Cisco switch, ensure DHCP snooping is enabled both globally and per access VLAN. To enable DHCP snooping, execute the following commands:

* **Switch(config)# ip dhcp snooping** configuring DHCP snooping in global configuration mode
* **Switch(config)# ip dhcp snooping vlan 10 Switch(config)# ^Z** Configuring DHCP snooping for a VLAN
* **Switch# show ip dhcp snooping** to view the DHCP snooping status
* **Switch(config)# show ip dhcp snooping binding** to view the DHCP snooping table

To enable DAI for multiple VLANs, specify a range of VLAN numbers.

* Command to configure ARP inspection for a VLAN

**Switch(config)# ip arp inspection vlan 10**

**Switch(config)# ^Z**

* Command to configure ARP inspection for a range of VLANs

**Switch(config)# ip arp inspection vlan 10, 11, 12, 13** Or

**Switch(config)# ip arp inspection vlan 10-13**

* To view the ARP inspection status

**Switch(config)# show ip arp inspection**

**Sniffing Technique: Spoofing Attacks  
MAC Spoofing/Duplicating**

AC duplicating refers to spoofing a MAC address with the MAC address of a legitimate user on the network. A MAC duplicating attack involves sniffing a network for MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port. Then, the attacker spoofs a MAC address with the MAC address of the legitimate client.

**MAC Spoofing Technique: Windows**

Method1:

* Start Control Panel Network and Internet Networking and Sharing Center.
* Click on Ethernet and then click on Properties in the Ethernet Status window.
* In Ethernet Properties window, click on the Configure and then on the Advanced tab.
* Under the “Property” section, browse for Network Address and click on it.
* On the right-hand side, under “Value,” type new MAC address you want to assign & click OK.
* Type “ipconfig/all” or “net config rdr” in the command prompt to verify the changes.

Method2:

* Do not type Regedit to start the registry editor. Go to "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318} and double-click on it to expand the tree.
* Four-digit sub keys representing network adapters will be found (starting with 0000, 0001).
* Search for the proper “DriverDesc” key to find the desired interface.
* Right-click on the appropriate sub key and add the new string value “NetworkAddress” (data type “REG\_SZ”) to contain the new MAC address.
* Right-click on the “NetworkAddress” string value on the right side and select Modify...
* Now, in “Edit String” dialog box, enter new MAC address in “Value data” field and click “OK.”
* Disable and then re-enable the network interface that was changed, or reboot the system.

**How to Defend Against MAC Spoofing**

To detect MAC spoofing, it is necessary to know all the MAC addresses in the network. The best way to defend against MAC address spoofing is to place the server behind the router. This is because routers depend only on IP addresses, whereas switches depend on MAC addresses for communication in a network. Making changes to the port security interface configuration is another way to prevent MAC spoofing attacks.

Techniques to defend against MAC Spoofing

* **DHCP Snooping Binding Table:** The DHCP snooping process filters untrusted DHCP messages and helps to build and bind a DHCP binding table. This table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information.
* **Dynamic ARP Inspection:** While performing a DAI, the system will automatically drop invalid IP–MAC address bindings.
* **IP Source Guard:** IP Source Guard is a security feature in switches that restricts the IP traffic on untrusted layer 2 ports by filtering traffic based on the DHCP snooping binding database.
* **Retrieval of MAC Address:** You should always retrieve the MAC address from the NIC directly.
* **Implementation of IEEE 802.1X Suites:** This is a type of network protocol for port-based Network Access Control (PNAC), and its main purpose is to enforce access control at the point where a user joins the network.
* **Encrypt the Communication**
* **AAA (Authentication, Authorization, and Accounting):** to filter MAC Addresses

**IRDP Spoofing**

ICMP Router Discovery Protocol (IRDP) is a routing protocol that allows a host to discover the IP addresses of active routers on its subnet by listening to router advertisement and solicitation messages on its network. The attacker can add default route entries on a system remotely by spoofing router advertisement messages. As IRDP does not require any authentication, the target host will prefer the default route defined by the attacker over the default route provided by the DHCP server. The attacker accomplishes this by setting the preference level and lifetime of the route at high values to ensure that the target hosts will choose it as the preferred route. An attacker can use this to send spoofed router advertisement messages so that all the data packets travel through the attacker’s system. Attackers can use IRDP spoofing to launch Following attacks.

* **Passive Sniffing:** In a switched network, the attacker spoofs IRDP traffic to re-route the outbound traffic of target hosts through the attacker’s machine.
* **MITM:** Once sniffing starts, the attacker acts as a proxy between the victim and the destination. The attacker plays an MITM role and tries to modify the traffic.
* **DoS:** IRDP spoofing allows remote attackers to add wrong route entries into the victim’s routing table. The wrong address entry causes DoS.

**VLAN Hopping**

Virtual local area network (VLAN) hopping is a technique used to target network resources present on a VLAN. The main purpose behind a VLAN hopping attack is to gain access to the traffic flowing in other VLANs present in the same network, which is otherwise inaccessible. VLAN hopping attacks can be performed via two primary methods, as given below:

* **Switch Spoofing**: the attacker connects a rogue switch into the network by tricking a legitimate switch and thereby creating a trunk link between them. After establishing a trunk link, the traffic from multiple VLANs can be sent to and through the rogue switch, therefore allowing an attacker to sniff and view the packet content.

Defend Against Switch Spoofing Perform the following steps to configure a switch:

* Explicitly configure the ports as access ports, and ensure that all access ports are configured not to negotiate trunks:

**switchport mode access**

**switchport mode nonegotiate**

* Ensure that all trunk ports are configured not to negotiate trunks:

**switchport mode trunk**

**switchport mode nonegotiate**

* **Double tagging:** the attacker adds and modifies tags in the Ethernet frame, thereby allowing the flow of traffic through any VLAN in the network. The Ethernet frame that is sent by the attacker contains two 802.1Q tags, inner and outer; the inner tag is the VLAN tag of a target switch that the attacker wants to reach, and the outer tag is the native VLAN of the attacker. When the switch receives the Ethernet frame, it strips off the outer tag, as it is same as the tag for the native VLAN, and forwards the frame with an inner tag on all its trunk interfaces.

Defend Against Double Tagging Perform the following steps to configure a switch:

* Ensure that each access port is assigned with VLAN except the default VLAN (VLAN 1):

**switchport access vlan 2**

* Ensure that the native VLANs on all trunk ports are changed to an unused VLAN ID: **switchport trunk native vlan 999**
* Ensure that the native VLANs on all trunk ports are explicitly tagged:

**vlan dot1q tag native**

**STP Attack**

In a Spanning Tree Protocol (STP) attack, attackers connect a rogue switch into the network to change the operation of the STP protocol and sniff all the network traffic. STP is used in LAN-switched networks with the primary function of removing potential loops within the network. In this process, a switch inside the network is appointed as the root bridge. After the selection of the root bridge, other switches in the network connect to it by selecting a root port (the closest port to the root bridge). The root bridge is selected with the help of Bridge Protocol Data Units (BPDUs). BIDs (BPDU identification number) consist of the Bridge Priority and the MAC address. By default, the value of the Bridge Priority is 32769. If an attacker has access to two switches, he/she introduces a rogue switch in the network with a priority lower than any other switch in the network. This makes rogue switch the root bridge.

* **BPDU Guard:** BPDU guard must be enabled on the ports that should never receive a BPDU from their connected devices. This is used to avoid the transmission of BPDUs on PortFast-enabled ports. This feature helps in preventing potential bridging loops in the network. If BPDU guard is enabled on a switch interface and an unauthorized switch connects to it, the port will be set to errdisable mode when a BPDU is received.
* **configure terminal**
* **interface gigabiteethernet slot/port**
* **spanning-tree portfast bpduguard**
* **Root Guard:** Root guard protects the root bridge and ensures that it remains as the root in the STP topology. It forces the interfaces to become the designated ports (forwarding ports) to prevent the nearby switches from becoming root switches. Therefore, if a port enabled with the root guard feature receives a superior BPDU, it converts that port into a loop inconsistent state.
* **configure terminal**
* **interface gigabiteethernet slot/port**
* **spanning-tree guard root**
* **Loop Guard:** Loop guard improves the stability of the network by preventing it against the bridging loops.
* **configure terminal**
* **interface gigabiteethernet slot/port**
* **spanning-tree guard loop**
* **UDLD (Unidirectional Link Detection**): UDLD enables devices to detect the existence of unidirectional links and further disable the affected interfaces in the network. These unidirectional links in the network can cause STP topology loops.
* **configure terminal**
* **interface gigabiteethernet slot/port**
* **udld { enable | disable | aggressive }**

**Sniffing Techniques: DNS Poisoning**

DNS is the protocol that translates a domain name (e.g., www.eccouncil.org) into an IP address (e.g., 208.66.172.56). The protocol uses DNS tables that contain the domain name and its equivalent IP address stored in a distributed large database. In DNS poisoning, also known as DNS spoofing, the attacker tricks a DNS server into believing that it has received authentic information when, in reality, it has not received any. The attacker tries to redirect the victim to a malicious server instead of the legitimate server. The attacker does this by manipulating the DNS table entries in the DNS. The attacker can create fake DNS entries for the server containing malicious content with the same names as that of the target server.

**DNS Poisoning Techniques**

* **Intranet DNS Spoofing**

An attacker can perform this attack on a switched LAN with the help of the ARP poisoning technique. Attacker must be connected to the LAN and be able to sniff the traffic or packets. An attacker who succeeds in sniffing the ID of the DNS request from the intranet can send a malicious reply to the sender before the actual DNS server. Attacker poisons the router by running arpspoof/dnsspoof to redirect DNS requests of clients to the attacker’s machine. When a client (John) sends a DNS request to the router, the poisoned router sends the DNS request packet to the attacker’s machine. Upon receiving the DNS request, the attacker sends a fake DNS response that redirects the client to a fake website set up by the attacker. Attacker owns the website and can see all the information submitted by the client to that website.

* **Internet DNS Spoofing**

Internet DNS poisoning is also known as remote DNS poisoning. The attacker sets up a rogue DNS server with a static IP address. Attackers perform attack with the help of Trojans when the victim’s system connects to the Internet. This is an MITM attack in which the attacker changes the primary DNS entries of the victim’s computer. The attacker replaces the victim’s DNS IP address with a fake IP address that resolves to the attacker’s system. Thus, the victim’s traffic redirects to the attacker’s system.

* **Proxy Server DNS Poisoning**

The attacker sets up a proxy server on the attacker’s system. The attacker also configures a fraudulent DNS and makes its IP address a primary DNS entry in the proxy server. The attacker changes the proxy server settings of the victim with the help of a Trojan. The proxy serves as a primary DNS and redirects the victim’s traffic to the fake website.

* DNS cache poisoning

Itrefers to altering or adding forged DNS records in the DNS resolver cache so that a DNS query is redirected to a malicious site. The DNS system uses cache memory to hold the recently resolved domain names. The attacker populates it with recently used domain names and their respective IP address entries. When a user request is received, the DNS resolver first checks the DNS cache; if the system finds the domain name that the user requested in the cache, the resolver will quickly send its respective IP address. Thus, it reduces the traffic and time of DNS resolving.  
Attackers target and make changes or add entries to this DNS cache. If the DNS resolver cannot validate that the DNS responses have come from an authoritative source, it will cache the incorrect entries locally and serve them to users who make the same request. The attacker replaces the user-requested IP address with the fake IP address and, when the user requests that domain name, the DNS resolver checks the entry in the DNS cache and picks the matched (poised) entry.

**How to Defend Against DNS Spoofing**

* Implement Domain Name System Security Extension (DNSSEC)
* Use Secure Socket Layer (SSL) for securing the traffic
* Resolve all DNS queries to a local DNS server
* Block DNS requests being sent to external servers
* Configure a firewall to restrict external DNS lookup
* Implement an intrusion detection system (IDS) and deploy it correctly
* Configure the DNS resolver to use a new random source port for each outgoing query
* Restrict the DNS recusing service, either full or partial, to authorized users
* Use DNS non-existent domain (NXDOMAIN) rate limiting
* Do not allow outgoing traffic to use UDP port 53 as a default source port

**Sniffing detection technique**

* **Ping Method:** To detect a sniffer on a network, identify the system on the network running in promiscuous mode. The ping method is useful in detecting a system that runs in promiscuous mode, which in turn helps to detect sniffers installed on the network. Just send a ping request to the suspected machine with its IP address and incorrect MAC address. The Ethernet adapter will reject it because the MAC address does not match, whereas the suspect machine running the sniffer responds to it, as it does not reject packets with a different MAC address.
* **DNS Method:** The reverse DNS lookup is the opposite of the DNS lookup method. Sniffers using reverse DNS lookup increase network traffic. This increase in network traffic can be an indication of the presence of a sniffer on the network. The computers on this network are in promiscuous mode.  
  Users can perform a reverse DNS lookup remotely or locally. Monitor the organization’s DNS server to identify incoming reverse DNS lookups. The method of sending ICMP requests to a non-existing IP address can also monitor reverse DNS lookups. The computer performing the reverse DNS lookup would respond to the ping, thus identifying it as hosting a sniffer.
* **ARP Method:** This technique sends a non-broadcast ARP to all the nodes in the network. The node that runs in promiscuous mode on the network will cache the local ARP address. Then, it will broadcast a ping message on the network with the local IP address but a different MAC address. In this case, only the node that has the MAC address (cached earlier) will be able to respond to your broadcast ping request. A machine in promiscuous mode replies to the ping message, as it has the correct information about the host that is sending ping requests in its cache; the remaining machines will send an ARP probe to identify the source of the ping request. This will detect the node on which the sniffer is running.