**Sniffing**

**Sniffing Concept**

Packet sniffing is a process of monitoring and capturing all data packets passing through a given network using a software application or hardware devices.

It allows an attacker to observe and access entire network traffic from a given point.

Packet sniffing allows an attacker to gather sensitive information such as Telnet passwords, email traffic, web traffic, FTP passwords,..

*Protocols Vulnerable to Sniffing*

* Telnet
* HTTP
* POP
* FTP
* IMAP

*Practice*







*How a Sniffer Works*

Sniffer turns the NIC of a system to the promiscuous mode so that it listens to all the data transmitted on its segment.

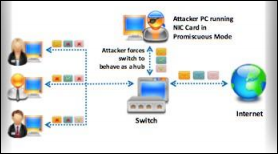


Figure 1. How a Sniffer works

**Type of Sniffing**

*Passive Sniffing*

Passive Sniffing refers to sniffing through a hub, wherein the traffic is sent to all ports.

In a network that use hubs to connect system, all hosts on the network can see the all traffic and therefore, the attacker can easily capture traffic going through the hub.

Hub usage is an outdated approach. Most modern networks now use switches.



Figure 2. Passive Sniffer with Hub

*Active Sniffing*

Active Sniffing is used to sniff a switch-based network

**Sniffing Technique**

Attacker use various sniffing techniques such as MAC attacks, DHCP attacks, ARP poisoning, DNS poisoning, etc to steal and manipulate sensitive data.

**Sniffing Technique: MAC Attack**

*MAC Address/CAM Table*

Each switch has a fixed size dynamic Content Addressable Memory table (CAM table).

The CAM table stores information such as MAC addresses avaiable on physical ports with their associated vitual LAN (VLAN) parameters.

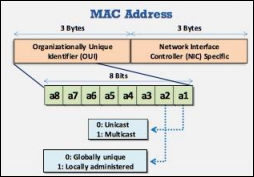


Figure 3. MAC Address



Figure 4. CAM Table

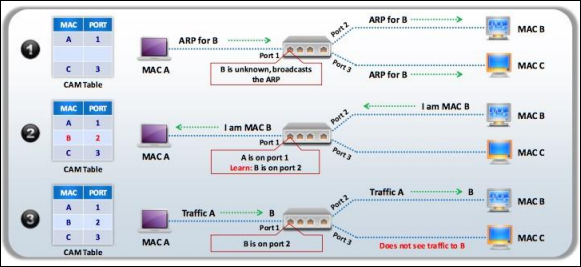


Figure 5. How CAM work

Once the CAM table fill up on a switch, additional ARP request trafficc flood every port on the switch.

This will change the behavior of the switch to reset to its learning mode, broadcasting on every port similar to a hub.

MAC flooding involves flooding of CAM table with fake MAC address and IP pairs until it is full. The switch then acts as a hub by broadcasting packets to all machines on the network and therefore, the attacker can sniff the traffic easily.



Figure 6. MAC Flooding

MAC Flooding switches with macof:

Macof is a Linux tool that sends random source MAC and IP Addresses and flood the switch’s CAM tables by sending bogus MAC entries.

Defend against MAC attacks:

Port security config – This feature identifies and limits the MAC addresses of the machines that can access the port.

**Sniffing Technique: DHCP Attack**

DHCP servers maintain TCP/IP configuration information in a database such as valid TCP/IP configuratioiin parameters, valid IP address and duration of the lease offered by the server. It provides address configurations to DHCP-enabled clients in the form of a lease offer.

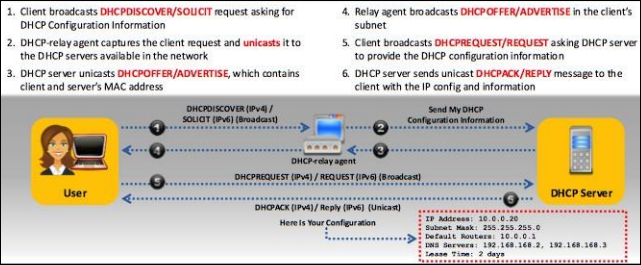


Figure 7. The Working of DHCP

*DHCP Starvation Attack*

This is a DoS attack on the DHCP servers where attacker broadcasts forged DHCP requests and tries to lease all of the DHCP addresses avaiable in the DHCP scope. Therefore, the legitimate user is unable to obtain or renew an IP address requested via DHCP, falling access to the network.

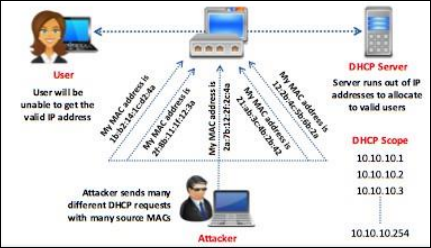


Figure 8. DHCP Starvation

Tools:

* Yersinia
* Pig
* Etc…

*Rogue DHCP Server Attack*

Attacker sets rogue DHCP server in the network and respond to DHCP requets with bogus IP addresses resulting in compromised network access.

This attack works in conjunction with DHCP starvation attack, attacker sends TCP/IP setting to the user after knocking him/her out from the genuine DHCP server.

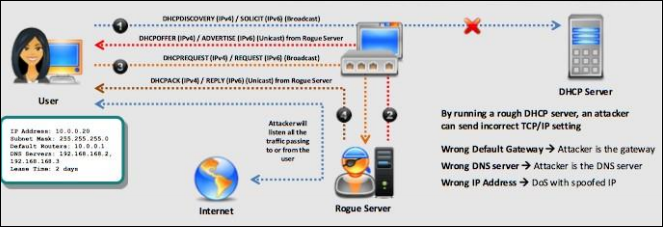


Figure 9. DHCP Rouge Server

Demo attack: <https://www.youtube.com/watch?v=nSR7K6ui_gc>

Defends:

* Enable port security to defend against DHCP starvation attack: Configuring MAC limit on switch edge ports drops the packets from futher MACs once the limit is reached.



* Enable DHCP snooping that allows switch to accept DHCP transaction directed from a trusted port



**Sniffing Technique: ARP Poisoning**

Address Resolution Protocol (ARP) is stateless protocol used for resolving IP address to MAC address. All network devices that needs to communicate on the network broadcasts ARP queries in the network to find out other machines’ MAC addresses. When one machine needs to communicate with another, it looks up its ARP table. If the MAC address is not found in the table, the ARP\_REQUEST is broadcasted over the network. All machines on the network will compare this IP address to their MAC address. If one of the machine in the network identifies with this address, it will respond to ARP\_REQUEST with its IP and MAC address. The requesting machine will store the address pair in the ARP table and begin with the communication.

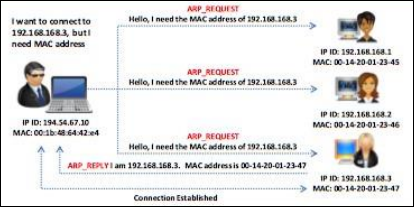


Figure 10. ARP

***arp -a***

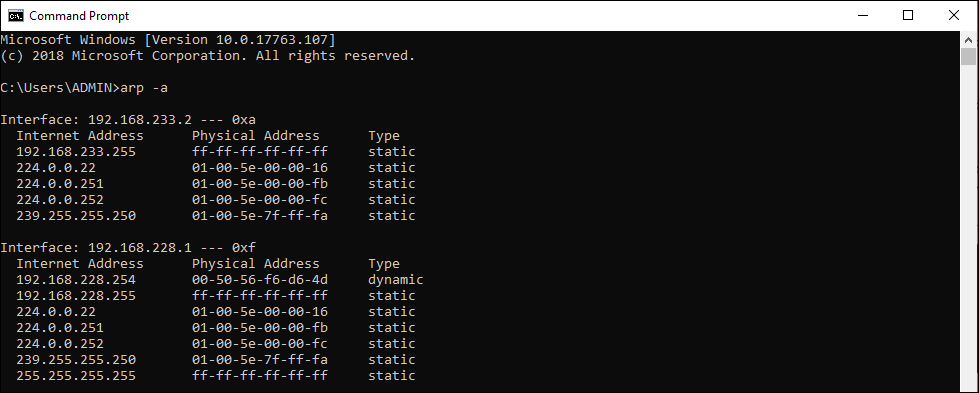


Figure 11. ARP table

ARP Spoofing Attack

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. Switch is set in “forwarding mode” after ARP table is flooded with spoofed ARP replies and attackers can sniff all the network packets. Attackers flood a target computer’s ARP cache with forged entries, which also know as poisoning.

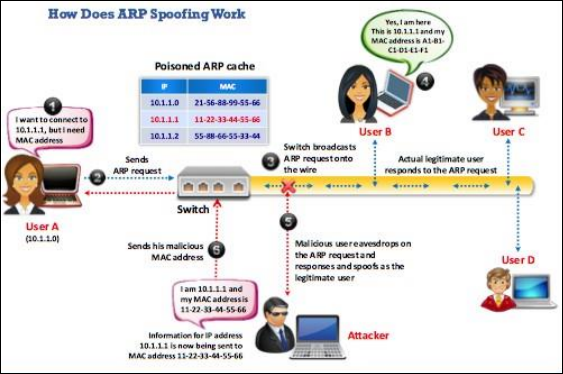
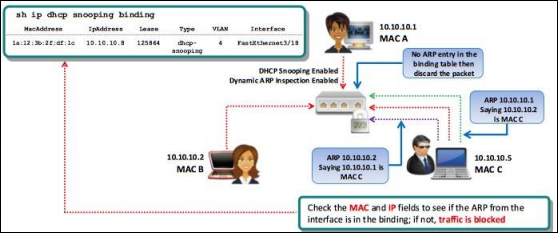


Figure 12. ARP Spoofing

Demo: <https://www.youtube.com/watch?v=4RVA4gb-PZI>

Prevent: Use DHCP snooping binding table, dynamic ARP inspection.



**Sniffing Technique: MAC Spoofing/Duplicating**

MAC duplicating attack is lauched by sniffing a network for MAC addresses of clients who are actively associated with a switch port and re-using one of those addresses. By listening to the traffic on the network, a malicious user can intercept and use a legitimate user’s MAC address to receive all the traffic destined for the user. This attack allows an attacker to gain access to the network and take ove someone’s identity on the network.

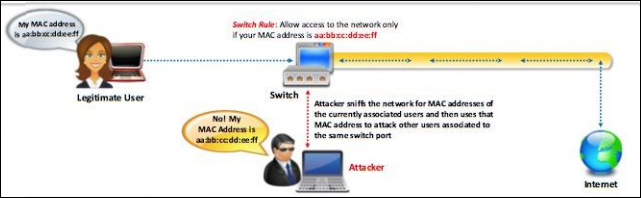


Figure 13. MAC Duplicating

***ipconfig /all***

***Open network and sharing center => Change adapter setting => Ethernet => Properties => Configure => Advance => Locally Administered Address***

Prevent: Use DHCP snooping binding table, dynamic ARP inspection.

**Sniffing Technique: DNS Poisoning**

DNS cache poisoning refers to altering or adding forged DNS records into the DNS resolver cache so that a DNS query is redirected to a malicious site.

If the DNS resolver cannot validate that the DNS responses have been received from an authoritative source, it will cache the incorrect entries locally and serve them to users who make the similar request.

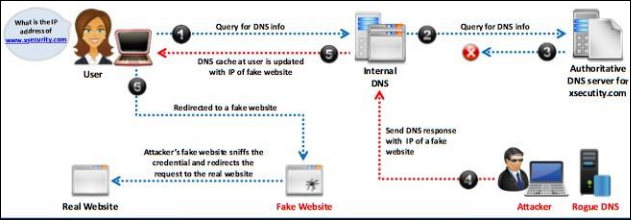


Figure 14. DNS Cache Poisoning

Demo: <https://www.youtube.com/watch?v=5CUG7isl8Ew>

**Questions**

1. Which of the following best describes active sniffing? (Choose all that apply.)

**A.**   Active sniffing is usually required when hubs are in place.

**B.**   Active sniffing is usually required when switches are in place.

**C.**   Active sniffing is harder to detect than passive sniffing.

**D.**   Active sniffing is easier to detect than passive sniffing.

2. Machine A (with MAC address 00-01-02-AA-BB-CC) and Machine B (00-01-02-BB-CC-DD) are on the same subnet. Machine C, with address 00-01-02-CC-DD-EE, is on a different subnet. While the attacker is sniffing on the fully switched network, Machine B sends a message to Machine C. If an attacker on Machine A wanted to receive a copy of this message, which of the following circumstances would be necessary?

**A.**   The ARP cache of the router would need to be poisoned, changing the entry for Machine A to 00-01-02-CC-DD-EE.

**B.**   The ARP cache of Machine B would need to be poisoned, changing the entry for the default gateway to 00-01-02-AA-BB-CC.

**C.**   The ARP cache of Machine C would need to be poisoned, changing the entry for the default gateway to 00-01-02-AA-BB-CC.

**D.**   The ARP cache of Machine A would need to be poisoned, changing the entry for Machine C to 00-01-02-BB-CC-DD.

3. Which of the following are appropriate active sniffing techniques against a switched network? (Choose all that apply.)

**A.**   ARP poisoning

**B.**   MAC flooding

**C.**   SYN flooding

**D.**   Birthday attack

**A.**   Firewalking

4. Which of the following techniques can be used to gather information from a fully switched network or to disable some of the traffic isolation features of a switch? (Choose two.)

**A.**   DHCP starvation

**B.**   MAC flooding

**C.**   Promiscuous mode

**D.**   ARP spoofing