

Chapter 08: Sniffing

Introduction

This chapter begins with an overview of sniffing concepts and explores topics such as MAC, DHCP, ARP, MAC spoofing, and DNS poisoning attacks. It then delves into various sniffing tools, countermeasures, and detection techniques. By the end of this chapter, you will be able to:

- Understand sniffing concepts
- Explain various MAC attacks
- Describe DHCP attacks
- Understand ARP poisoning
- Explain different spoofing attacks
- Describe DNS poisoning
- Implement defense mechanisms against sniffing techniques
- Utilize various sniffing tools
- Apply sniffing countermeasures
- Detect sniffing attacks using different techniques

Sniffing Concepts

Sniffing is the process of scanning and monitoring captured data packets passing through a network by using sniffers. The process of sniffing is carried out by using Promiscuous Ports. Enabling the promiscuous mode function on the connected network interface allows capturing all traffic, even when the traffic is not intended for them. Once the packet is captured, you can easily perform the inspection.

There are two types of Sniffing:

1. Active Sniffing
2. Passive Sniffing

Through sniffing, an attacker can capture packets like Syslog traffic, DNS traffic, Web traffic, email, and other types of data flowing across the network. By capturing these packets, an attacker can reveal information such as data, username, and passwords from protocols like HTTP, POP, IMAP, SMTP, NMTP, FTP, Telnet, and Rlogin and other information. Anyone within the LAN or connected remotely can sniff the packets. Let's focus on how sniffers perform their actions and what can be achieved through sniffing.

How Sniffer Works

In the sniffing process, an attacker gets connected to the target network to sniff the packets. Using sniffers, which turn the attacker's system's Network Interface Card (NIC) into promiscuous mode, the attacker captures the packet. Promiscuous mode is a mode of the interface in which the NIC responds to every packet it receives. As you can observe in Figure 8-01, the attacker connected in promiscuous mode accepts each packet, even those packets that are not intended for him.

Once the attacker captures the packets, he can decrypt these packets to extract information. The fundamental concept behind this technique is that if you are connected to a target network through a switch, broadcast, and multicast traffic is forwarded to all ports. Switch forwards the unicast packet to the specific port where the actual host is connected. Switch maintains its MAC table to validate who is connected to which port. In this case, the attacker alters the switch's configuration by using different techniques such as Port Mirroring or Switched Port Analyzer (SPAN). All packets passing through a monitored port will be copied onto a mirror port (the port on which the attacker is connected with a promiscuous mode). If you are connected to a hub, it will transmit all packets to all ports.

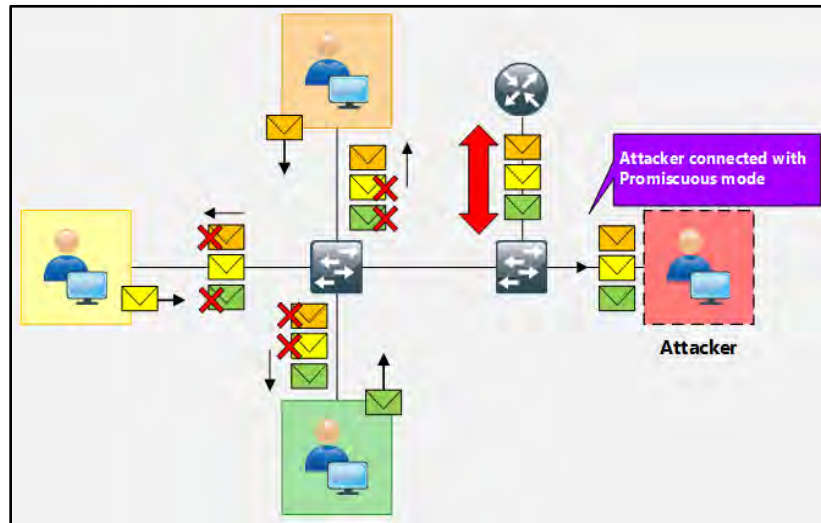


Figure 8-01: Packet Sniffing

Network Sniffing

Packet sniffing involves monitoring and capturing data packets on a network using software or hardware. In hub-based networks, sniffing is straightforward as all traffic is shared across all connected hosts. However, modern networks use switches, which direct data based on MAC addresses, limiting sniffing to within a subnet. Attackers manipulate switches to capture traffic.

Sniffing programs bypass Ethernet NIC filters, enabling the capture of all network traffic. Even in switched networks, sniffers on high-traffic components (like routers or servers) can intercept sensitive data, including passwords, account details, and emails. This data can be exploited for unauthorized access or further attacks.

Effective attacks often combine sniffing with active transmission, making it a significant threat to network security.

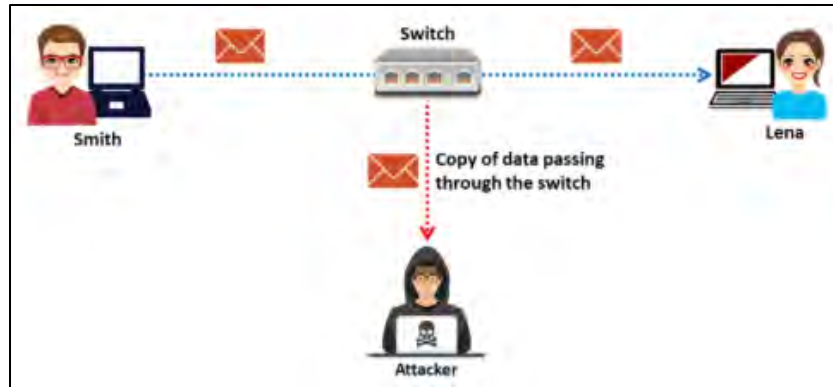


Figure 8-02: Packet Sniffing Scenario

Types of Sniffing

Passive Sniffing

Passive Sniffing is the type of sniffing in which there is no need to send additional packets or involve a device, such as a hub, to receive packets. As we know, the hub broadcasts every packet to its port, which helps the attacker monitor all traffic passing through a hub without effort.

Active Sniffing

Active Sniffing is the type of sniffing in which an attacker has to send additional packets to the connected device, such as a Switch, to start receiving packets. As we know, a unicast packet from the switch is transmitted to a specific port only. The attacker uses certain techniques such as MAC Flooding, DHCP Attacks, DNS poisoning, Switch Port Stealing, ARP Poisoning, and Spoofing to monitor traffic passing through the switch. These techniques are defined in detail later in this chapter.

How Attackers Hack Networks Using Sniffers

Attackers use sniffing tools to intercept and monitor network traffic. The steps involved in executing a sniffing attack are:

- **Accessing the Network:** The attacker identifies a suitable switch and connects a system or laptop to one of its ports.
- **Network Discovery:** Using discovery tools, the attacker gathers information about the network topology.
- **Target Identification:** Analyzing the network topology, the attacker identifies a victim machine to target.
- **ARP Spoofing:** The attacker sends fake Address Resolution Protocol (ARP) messages to deceive devices on the network.
- **Traffic Redirection:** The spoofed ARP messages divert traffic from the victim's machine to the attacker's system, enabling a man-in-the-middle (MITM) attack.
- **Extracting Sensitive Information:** The attacker intercepts all data packets sent and received by the victim, extracting sensitive information like passwords, usernames, credit card details, and PINs.

Protocols Vulnerable to Sniffing

Several protocols are prone to sniffing due to a lack of encryption, enabling attackers to capture sensitive information like passwords:

- **Telnet & Rlogin:** Transfer data in plaintext, allowing attackers to sniff keystrokes, including credentials.
- **HTTP:** Transmits user data in plaintext, exposing credentials to attackers.
- **SNMP:** Early versions (SNMPv1 & SNMPv2) lack strong security, enabling attackers to sniff passwords.
- **SMTP:** Emails and credentials are transmitted in plaintext, making them easy to intercept.
- **NNTP:** Fails to encrypt news data, leaving it vulnerable to sniffing.
- **POP:** Transfers email data in plaintext, exposing it to interception.
- **FTP:** Lacks encryption, allowing attackers to sniff files and user credentials.
- **IMAP:** Insufficient security permits attackers to capture data in plaintext.
- **TFTP:** No authentication or encryption makes data easily accessible on the network.

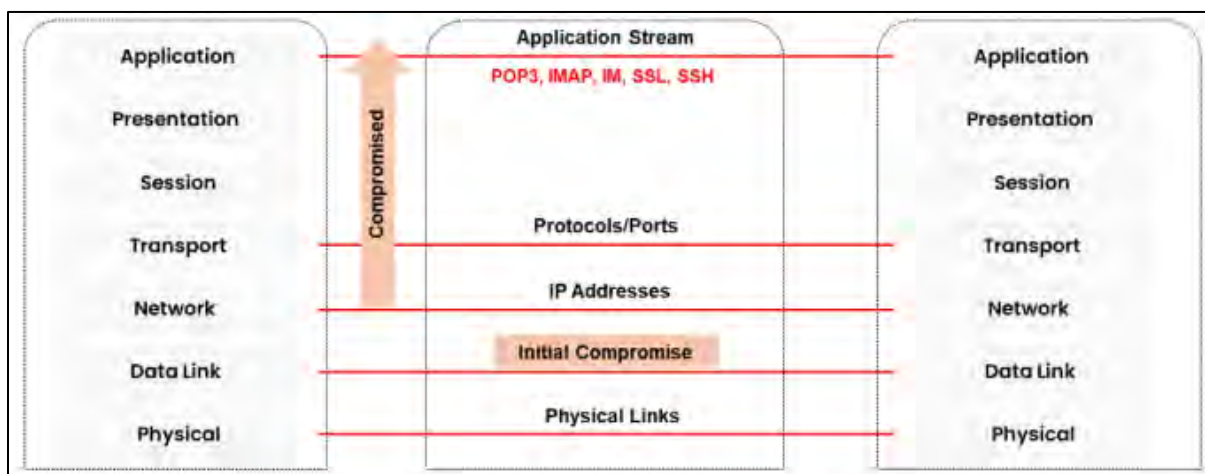


Figure 8-03: Sniffing in the data link layer of OSI Model

Hardware Protocol Analyzer

Protocol Analyzers, either hardware or software, are used to analyze the captured packets and signals over the transmission channel. Hardware Protocol Analyzers are the physical equipment that captures the packets without interfering with network traffic. The major advantages offered by these hardware protocol analyzers are mobility, flexibility, and throughput. Using these hardware analyzers, an attacker can:

- Monitor network usage
- Identify traffic from hacking software
- Decrypt the packet
- Extract the information
- Modify the size of the packet

KEYSIGHT Technologies offers various products. To get updates and information, visit the website www.keysight.com. There are also other hardware protocol analyzer products available in the market from different vendors like RADCOM and Fluke.

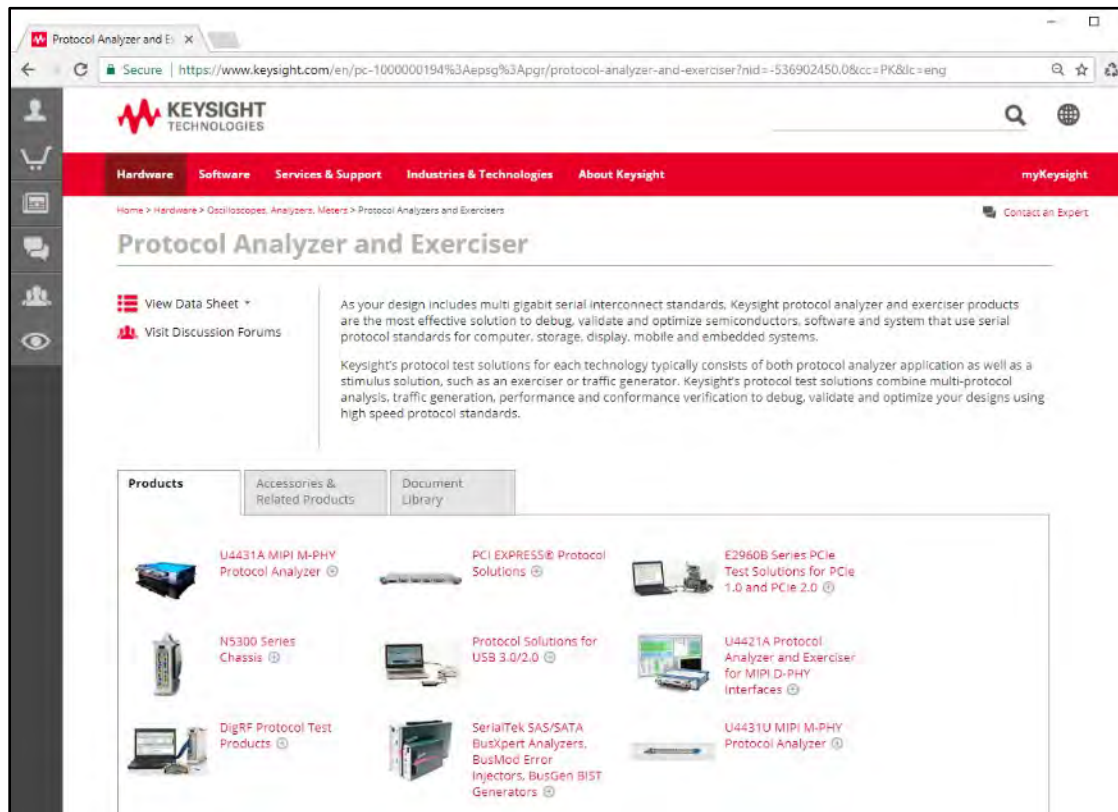


Figure 8-04: KEYSIGHT Technologies Hardware Protocol Analyzer Products

SPAN Port

You have a user who has complained about network performance while no one else in the building is experiencing the same issue. You want to run a Network Analyzer on the port, like Wireshark, to monitor ingress and egress traffic on the port. To do this, you can configure SPAN (Switch Port Analyzer). SPAN allows you to capture traffic from one port on a switch to another port on the same switch.

SPAN makes a copy of all frames destined for a port and copies them to the SPAN destination port. SPAN does not forward certain traffic types, for example, BDPUs, CDP, DTP, VTP, STP traffic. The number of SPAN sessions that can be configured on a switch is model-dependent. For example, Cisco 3560 and 3750 switches only support up to two SPAN sessions at once, whereas Cisco 6500 series switches support up to 16.

SPAN can be configured to capture either inbound, outbound, or both directions of traffic. You can configure a SPAN source as either a specific port, a single port in an Ether channel group, an Ether channel group, or a VLAN. SPAN cannot be configured with a source port of a MEC (Multi-chassis Ether Channel). You also cannot configure the source of a single port and a VLAN. You specify multiple source interfaces when configuring multiple sources for a SPAN session.

PRISM stands for Planning Tool for Resource Integration Synchronization and Management. PRISM is a tool specially designed to collect information passing through American servers. The

Special Source Operation (SSO) division of the National Security Agency (NSA) developed the PRISM program. PRISM is intended for identifying and monitoring a target's suspicious communication. Internet traffic routing through the U.S., or data stored on U.S. servers, are wiretapped by the NSA.

Lawful Inspection

Lawful interception (LI) involves legally intercepting communication data, such as calls, emails, and VoIP, for surveillance and analysis. Network operators or service providers grant legal access to private data for law enforcement agencies (LEAs) to monitor suspicious activities. LI helps manage infrastructure, enhance cybersecurity, and investigate illegal activities.

A typical LI setup includes a tap/access switch to collect ISP traffic, which is sorted by IP domain and sent to systems like E-Detective (ED) for data reconstruction. Supported protocols include POP3, IMAP, SMTP, FTP, and telnet. A Centralized Management Server (CMS) oversees the process. Countries are working to standardize LI procedures globally.

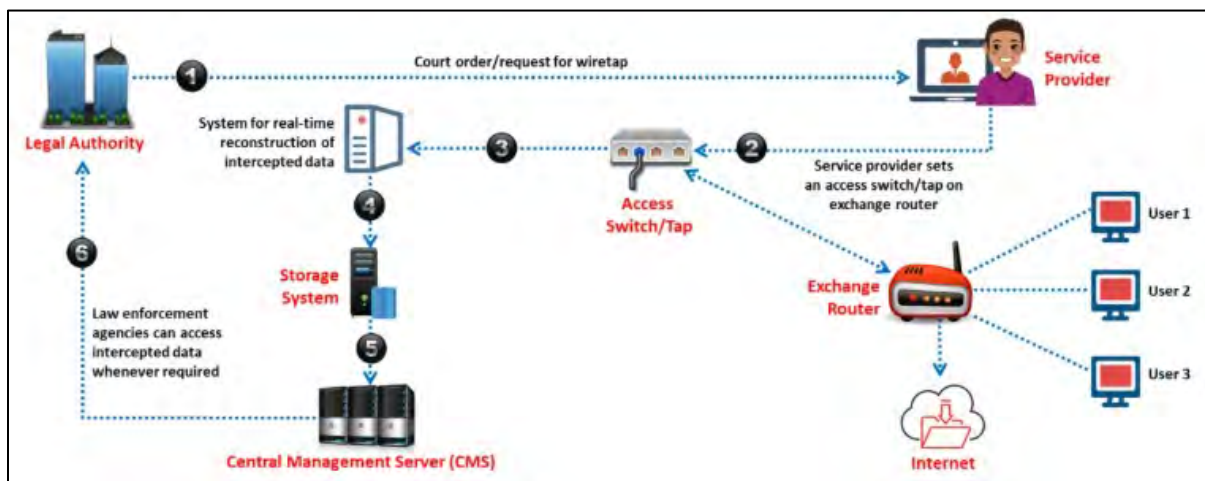


Figure 8-06: Telco/ISP Lawful Solution

MAC Attacks

MAC Address Table/CAM Table

MAC is the abbreviation of Media Access Control. A MAC address is the physical address of a device. It is a 48-bit unique identification number that is assigned to a network device for communication at a data-link layer. A MAC address is comprised of a 24-bit Object Unique Identifier (OUI) and 24-bit Network Interface Controller (NIC). In cases of multiple NICs, the device will have multiple unique MAC addresses.

A MAC address table or Content-Addressable Memory (CAM) table is used in Ethernet switches to record MAC address and its associated information used for forwarding packets. The CAM table records each MAC address—such as the associated VLAN information, learning type, and associated port parameters. These parameters help at the data-link layer to forward packets.

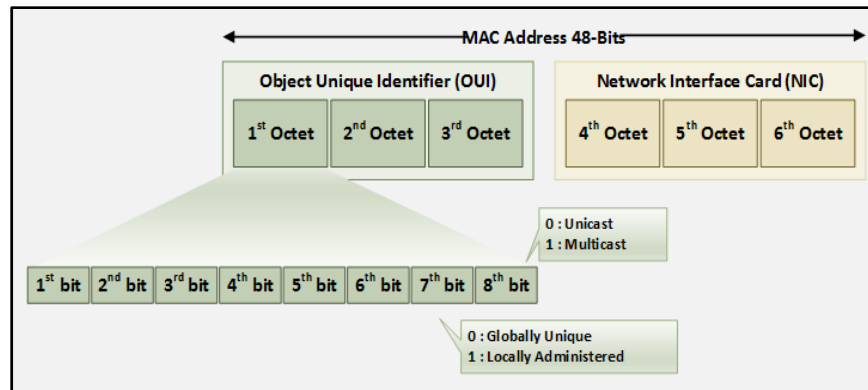


Figure 8-07: MAC Address Bits

How Content Addressable Memory Works

Learning the MAC address of devices is the fundamental responsibility of switches. A switch transparently observes incoming frames. It records the source MAC address of these frames in its MAC address table. It also records the specific port for the source MAC address. Based on this information, it can make intelligent frame forwarding (switching) decisions. Remember that a network machine could be turned off or moved at any point. As a result, the switch must also age MAC addresses and remove them from the table when they have not been seen for some time.

```
Switch#show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----
1       e213.5864.ab8f   DYNAMIC   Gi0/0
1       fa16.3ee3.7d71   DYNAMIC   Gi1/0
```

Figure 8-08: MAC Address Table

A switch supports multiple MAC addresses on all ports so that we can connect individual workstations as well as multiple devices through a switch or router. Through the feature of Dynamic Addressing, a switch updates the source address received from the incoming packets and binds it to the interface from which it is received. As the devices are added or removed, they are updated dynamically. By default, the aging time of a MAC address is 300 seconds. The switch is configured to learn the MAC addresses dynamically by default.

Working of CAM

A CAM table (Content Addressable Memory) dynamically tracks MAC addresses on an Ethernet switch to ensure data is delivered to the intended host. Limited in size, the CAM table can be flooded with excessive MAC addresses, causing the switch to act as a hub. Attackers exploit this vulnerability to sniff network traffic.

When Machine A (MAC A) wants to communicate with Machine B (MAC B), it sends an ARP request containing its MAC and IP addresses to the switch. The switch broadcasts this request to all hosts in the network and waits for a reply from the target machine.

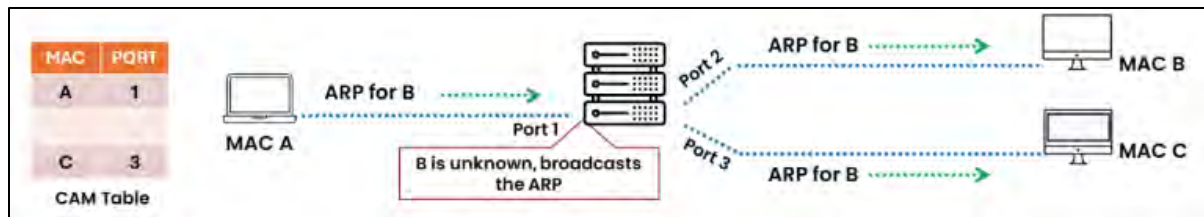


Figure 8-09 (a): Step - 01

Machine B, possessing the target IP, sends an ARP reply with its MAC address. The CAM table stores this MAC and its connected port.

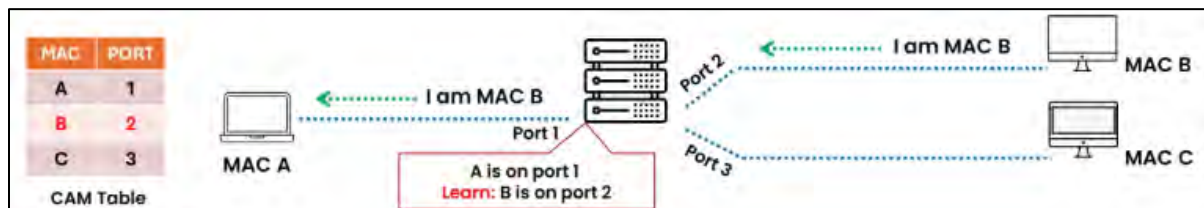


Figure 8-09 (b): Step - 02

Once the connection is established, Machine A sends traffic to Machine B directly, while Machine C cannot see the communication.

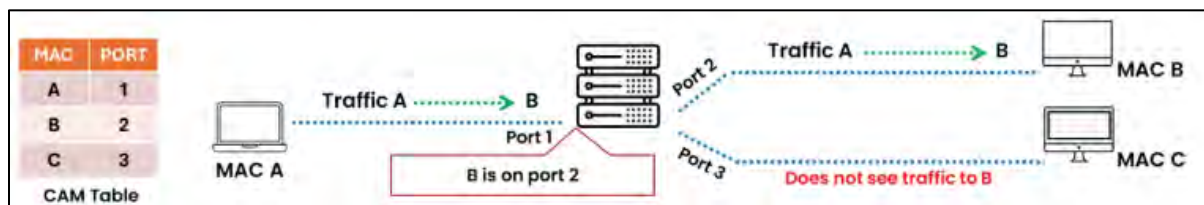


Figure 8-09 (c): Step - 03

Impact of a Full CAM Table

A CAM table stores MAC addresses, switch port data, and VLAN parameters. When overwhelmed by MAC flooding attacks, which send numerous fake MAC addresses, the CAM table reaches its capacity. The switch then behaves like a hub, broadcasting all traffic to every port. This allows attackers to intercept frames sent between hosts. Additionally, the attack can overflow CAM tables on nearby switches, expanding the impact.

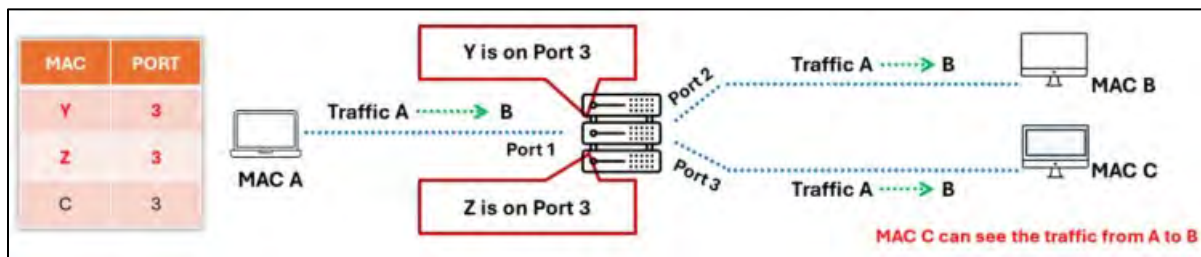


Figure 8-10: Flooding a CAM Table

MAC Flooding

MAC flooding is a technique in which an attacker sends random MAC addresses mapped with random IP to overflow the storage capacity of a CAM table. A switch then acts as a hub because a CAM table has a fixed length. It will now broadcast the packet on all ports, which helps an attacker sniff the packet with ease. A Unix/Linux utility known as “**macof**”, offers MAC flooding. Using macof, a random source MAC and IP can be sent to an interface.

Switch Port Stealing

Switch Port Stealing is also a packet sniffing technique that uses MAC flooding to sniff the packets. In this technique, the attacker sends a false ARP packet with the source MAC address of the target and his own destination address, as the attacker is impersonating the target host (let's say Host A). When this is forwarded to the switch, the switch will update the CAM table. When Host A sends a packet, the switch will have to update it again. This will create a “winning the race” condition in which if the attacker sends the ARP with Host A's MAC address, the switch will send packets to the attacker, assuming Host A is connected to this port.

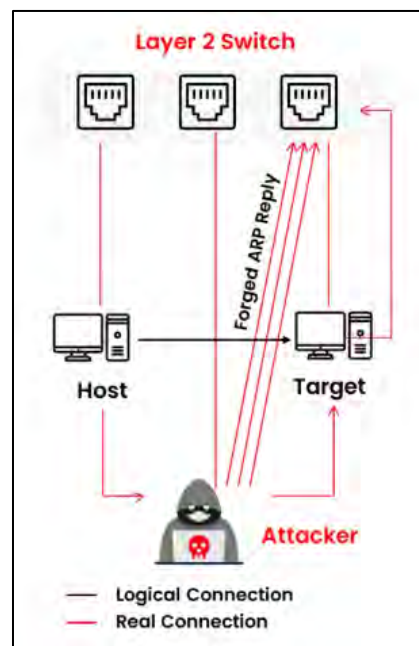


Figure 8-11: Switch Port Stealing

Defending Against MAC Attacks

Port Security is used to secure the ports. You can either bind a known MAC address with a port (static) or specify the limit to learn the MAC on a port (dynamic). You can also enforce a violation action on a port. Hence, if an attacker tries to connect his PC or embedded device to the switch port, the port is configured to support a specific MAC address only. An attacker's attempt to connect on the port will violate the condition, and the port will shut down or restrict the traffic flow on that port. In dynamic port security, you must specify the number of allowed MAC addresses,

and the switch will allow only that number simultaneously without regard to what those MAC addresses are.

Configuring Port Security

The Cisco Switch offers port security to prevent MAC attacks. You can configure the switch either for statically defined MAC Addresses only or dynamic MAC learning up to the specified range, or you can configure port security with a combination of both, as shown below. The following configuration on the Cisco Switch will allow a specific MAC address and four additional MAC addresses.

```
Port Security Configuration
Switch(config)# interface ethernet o/o
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
//Enabling Port Security
Switch(config-if)# switchport port-security mac-address <mac-address>
//Adding static MAC address to be allowed on Ethernet o/o
Switch(config-if)# switchport port-security maximum 4
//Configuring dynamic MAC addresses (maximum up to 4 MAC addresses) to be allowed on
Ethernet o/o
Switch(config-if)# switchport port-security violation shutdown
//Configuring Violation action as shutdown
Switch(config-if)# exit
```

DHCP Attacks

Dynamic Host Configuration Protocol (DHCP) Operation

DHCP is the process of allocating the IP address dynamically so that these addresses are assigned automatically and can be reused when hosts do not need them. Round Trip time is the measurement of time from the discovery of the DHCP server to obtaining the leased IP address. RTT can be used to determine the performance of DHCP. Using UDP broadcast, a DHCP client sends an initial DHCP-Discover packet because it does not have information about the network to which they are connected. The DHCP server replies to the DHCP-Discover packet with a DHCP-Offer Packet offering the configuration parameters. The DHCP client will send a DHCP-Request packet destined for the DHCP server requesting configuration parameters. Finally, the DHCP server will send the DHCP-Acknowledgement packet containing configuration parameters.

DHCPv4 uses two different ports:

- UDP port 67 for Server
- UDP port 68 for Client

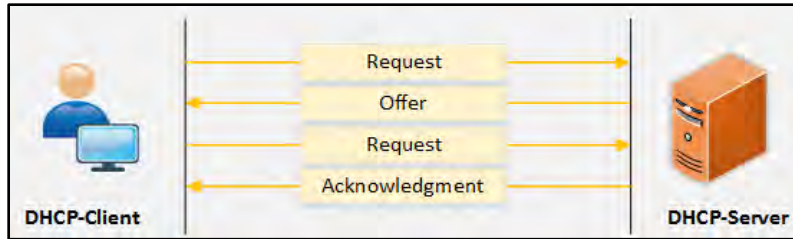


Figure 8-12: IPv4 DHCP Requests

A DHCP Relay Agent forwards the DHCP packets from server to client and client to server. The relay agent helps the communication by forwarding requests and replies between client and server. When receiving a DHCP message, the relay agent generates a new DHCP request, including default gateway information and the Relay-Agent information option (Option-82), and sends it to a remote DHCP server. When the Relay Agent gets the reply from the server, it removes Option 82 and forwards it back to the client.

The working of the relay agent and the DHCPv6 server is the same as the IPv4 relay agent and DHCPv4 server. The DHCP server receives the request and assigns the IP address, DNS, lease time, and other necessary information to the client, whereas the relay server forwards the DHCP messages.

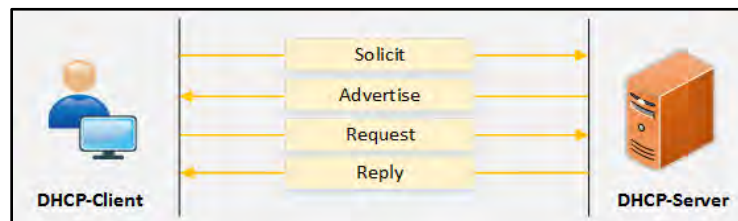


Figure 8-13: IPv6 DHCP Requests

DHCPv6 uses two different ports:

- UDP port 546 for clients
- UDP port 547 for servers

IPv4 DHCP Packet Format

DHCP facilitates communication on IP networks by configuring devices with IP addresses and other network parameters. Operating in a client-server model, it delivers host-specific settings and allocates network addresses. DHCP messages share the same format as BOOTP messages to ensure compatibility with BOOTP relay agents, avoiding changes to existing BOOTP client initialization software.

OP Code	Hardware Type	Hardware Length	HOPS
Transaction ID (XID)			
Seconds		Flags	
Client IP Address (CIADDR)			
Your IP Address (YIADDR)			
Server IP Address (SIADDR)			
Gateway IP Address (GIADDR)			
Client Hardware Address (CHADDR)—16 bytes			
Server Name (SNAME)—64 bytes			
Filename—128 bytes			
DHCP Options			

Figure 8-14: IPv4 DHCP Packet Format

DHCP Starvation Attack

A DHCP starvation attack floods a DHCP server with numerous spoofed requests, exhausting its pool of available IP addresses and causing a Denial-of-Service (DoS) attack. As a result, legitimate users cannot obtain or renew IP addresses, preventing network access. Tools like Yersinia, Hyenae, and Gobbler are commonly used to generate requests with spoofed MAC addresses in such attacks.

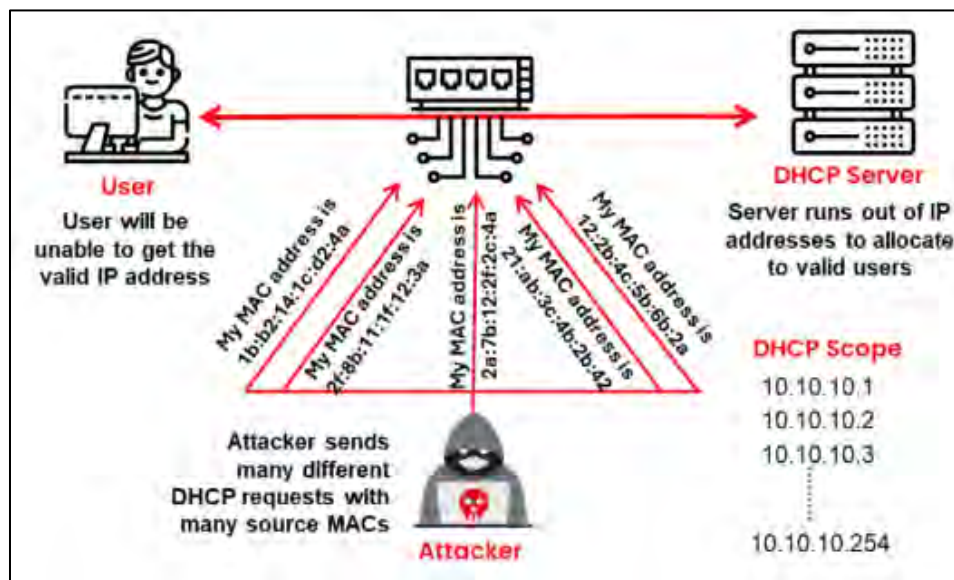


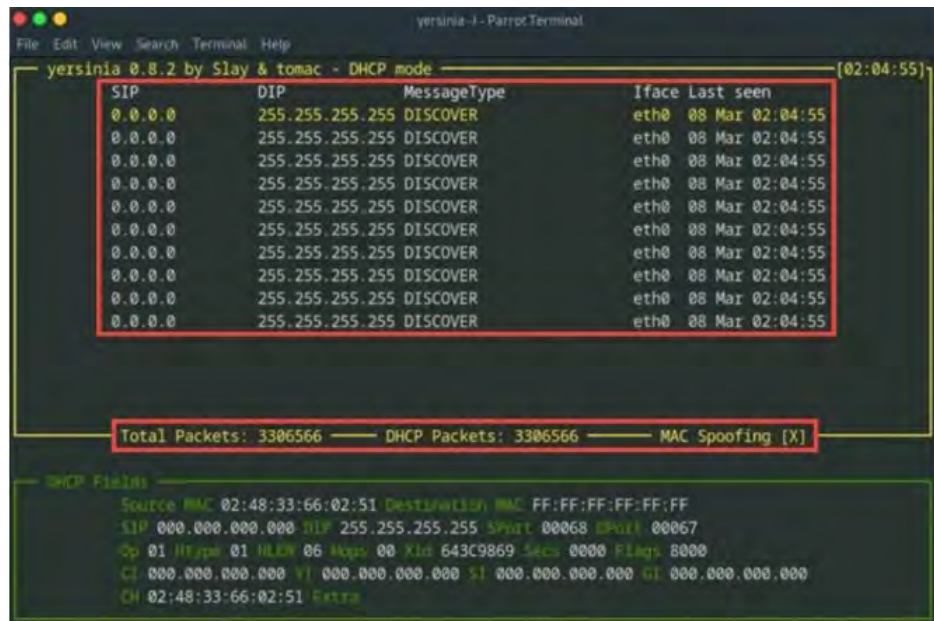
Figure 8-15: DHCP Starvation Attack

DHCP Starvation Attack Tool

Tools for DHCP starvation attacks overwhelm DHCP servers with excessive requests, depleting their address pools and preventing them from assigning configurations to new clients.

Yersinia

Yersinia is a network analysis tool that exploits vulnerabilities in various network protocols, including DHCP. It serves as a framework for testing and analyzing network systems. Attackers often use Yersinia to perform DHCP starvation attacks by simulating numerous spoofed DHCP requests.



The screenshot shows the Yersinia terminal interface running in DHCP mode. It displays a table of spoofed DHCP DISCOVER packets and summary statistics.

SIP	DIP	MessageType	Iface	Last seen
0.0.0.0	255.255.255.255	DISCOVER	eth0	08 Mar 02:04:55
0.0.0.0	255.255.255.255	DISCOVER	eth0	08 Mar 02:04:55
0.0.0.0	255.255.255.255	DISCOVER	eth0	08 Mar 02:04:55
0.0.0.0	255.255.255.255	DISCOVER	eth0	08 Mar 02:04:55
0.0.0.0	255.255.255.255	DISCOVER	eth0	08 Mar 02:04:55
0.0.0.0	255.255.255.255	DISCOVER	eth0	08 Mar 02:04:55
0.0.0.0	255.255.255.255	DISCOVER	eth0	08 Mar 02:04:55
0.0.0.0	255.255.255.255	DISCOVER	eth0	08 Mar 02:04:55
0.0.0.0	255.255.255.255	DISCOVER	eth0	08 Mar 02:04:55
0.0.0.0	255.255.255.255	DISCOVER	eth0	08 Mar 02:04:55

Summary statistics:

- Total Packets: 3306566
- DHCP Packets: 3306566
- MAC Spoofing [X]

DHCP Fields:

- Source MAC: 02:48:33:66:02:51
- Destination MAC: FF:FF:FF:FF:FF:FF
- SIP: 000.000.000.000
- DIP: 255.255.255.255
- SPort: 00068
- DPort: 00067
- Op: 01
- HType: 01
- HLen: 06
- Xid: 643C9869
- Secs: 0000
- Flags: 0000
- CI: 000.000.000.000
- YI: 000.000.000.000
- SI: 000.000.000.000
- GI: 000.000.000.000
- CH: 02:48:33:66:02:51
- Extra:

Figure 8-16: Yersinia

Rogue DHCP Server Attack

A Rogue DHCP Server Attack is performed by deploying the rogue DHCP server in the network along with the Starvation attack. When a legitimate DHCP server is under denial-of-service attack, DHCP clients cannot gain IP addresses from the legitimate DHCP server. A fake DHCP server replies to upcoming DHCP Discovery (IPv4) or Solicit (IPv6) packets with a configuration parameter that directs traffic towards it.

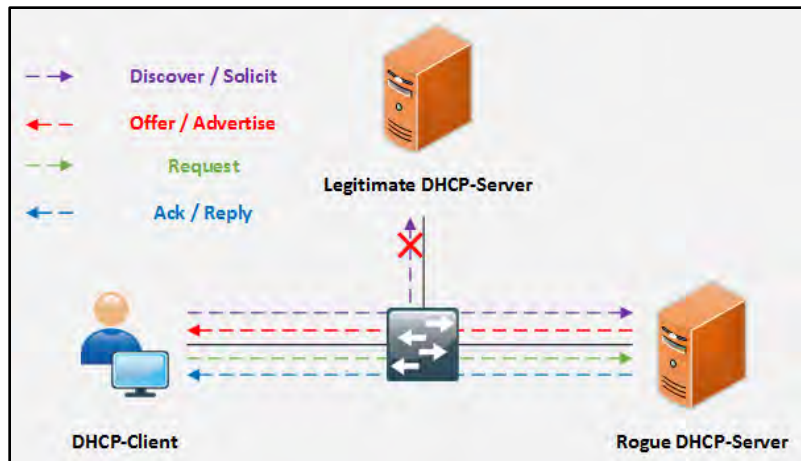


Figure 8-17: Rogue DHCP Server Attack

Defending Against DHCP Starvation and Rogue Server Attack

DHCP Snooping

It is actually very easy for someone to accidentally or maliciously bring a DHCP server into a corporate environment. DHCP Snooping is all about protection against such attacks. In order to mitigate against such attacks, the DHCP snooping feature is enabled on networking devices to identify from DHCP traffic only the trusted ports. It allows ingress and egress DHCP traffic. Any access port that tries to reply to the DHCP requests will be ignored because the device will only allow the DHCP process from a trusted port as defined by the networking team. It is a security feature that provides network security by filtering untrusted DHCP messages and building and maintaining a DHCP snooping binding database known as a DHCP Snooping Binding Table. DHCP snooping differentiates between untrusted interfaces connected to the end user/host and trusted interfaces connected to the legitimate DHCP server or any trusted device.

Port Security

Enabling Port Security will also mitigate against these attacks by limiting the port to learning a maximum number of MAC addresses, configuring violation actions, aging time, etc.

ARP Poisoning

Address Resolution Protocol (ARP)

ARP is a stateless protocol that is used within a broadcast domain to ensure communication by resolving the IP address to MAC address mapping. It is in charge of L3 to L2 address mappings. ARP protocol ensures the binding of IP addresses and MAC addresses. By broadcasting the ARP request with an IP address, the switch can learn the associated MAC address information from the reply of the specific host. In the event that there is no map or the map is unknown, the source will send a broadcast to all nodes. Only the node with a coordinating MAC address for that IP will answer the demand with the MAC address mapping packet. The switch will feed the MAC address and its connected port information into its fixed length CAM table.

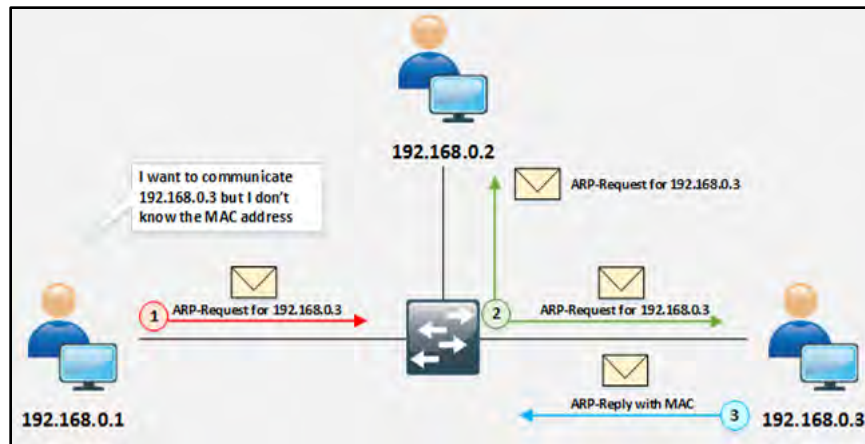


Figure 8-18: ARP Operation

As shown in Figure 8-18, the source generates an ARP query by broadcasting the ARP packet. A node with the MAC address that the query is destined for will reply only to the packet. The frame is flooded out of all ports (other than the port on which the frame was received) if CAM table entries are full. This also happens when the destination MAC address in the frame is the broadcast address. The MAC flooding technique is used to turn a switch into a hub, in which the switch starts broadcasting each and every packet. In this scenario, each user can catch the packets, even those that are not intended for them.

ARP Spoofing Attack

In ARP spoofing, an attacker sends forged ARP packets over a Local Area Network (LAN). In this case, the switch will update the attacker's MAC Address with the IP address of a legitimate user or server. Once an attacker's MAC address is learned, together with the IP address of an authentic user, the switch will start forwarding the packets to the attacker, assuming that it is the MAC of the user. Using an ARP Spoofing attack, an attacker can steal information by extracting it from the packet intended for a user over LAN that it received. Apart from stealing information, ARP spoofing can be used for:

- Session Hijacking
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Packet Sniffing
- Data Interception
- Connection Hijacking
- VoIP Tapping
- Connection Resetting
- Stealing Passwords

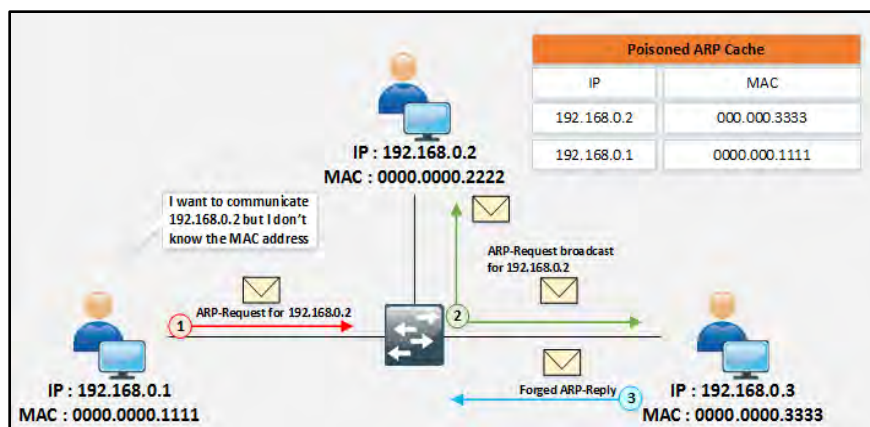


Figure 8-19: ARP Spoofing Attack

Defending ARP Poisoning

Dynamic ARP Inspection (DAI)

DAI is used with DHCP snooping. ARP is a Layer 2 protocol that functions on IP-to-MAC bindings. Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets within a network. DAI investigates the ARP packets by intercepting, logging, and discarding the invalid IP-MAC address bindings. DHCP snooping is required in order to build the MAC-to-IP bindings for DAI validation.

Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

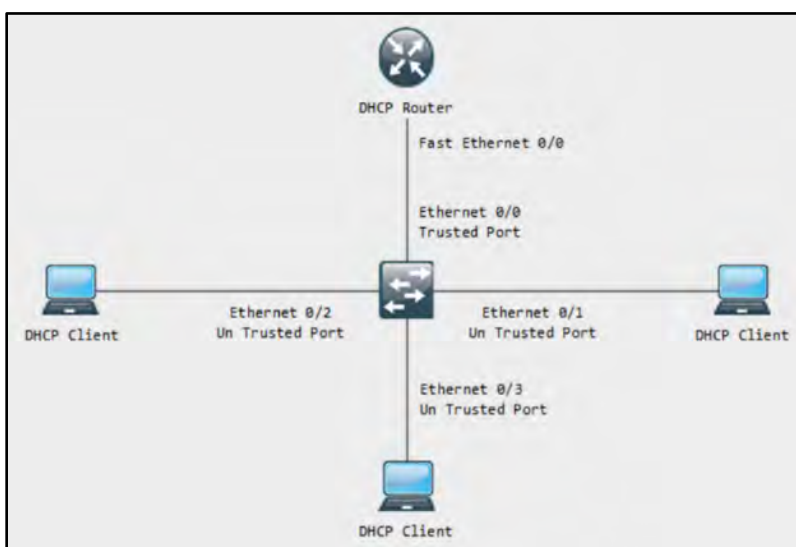


Figure 8-20: Network Diagram

Configuration:

Switch> **en**

Switch# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# **ip dhcp snooping**

```
Switch(config)# ip dhcp snooping vlan 1
```

```
Switch(config)# int eth 0/0
```

```
Switch(config-if)# ip dhcp snooping trust
```

```
Switch(config-if)# ex
```

```
Switch(config)# int eth 0/1
```

```
Switch(config-if)# ip dhcp snooping information option allow-untrusted
```

```
Switch(config)# int eth 0/2
```

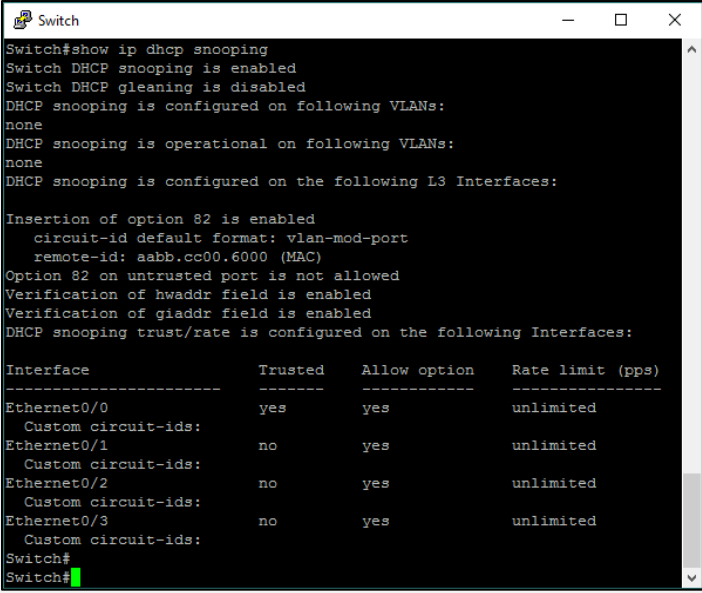
```
Switch(config-if)# ip dhcp snooping information option allow-untrusted
```

```
Switch(config)# int eth 0/3
```

```
Switch(config-if)# ip dhcp snooping information option allow-untrusted
```

Verification:

```
Switch# show ip dhcp snooping
```



```
Switch
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
none
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: aabb.cc00.6000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface           Trusted    Allow option    Rate limit (pps)
-----
Ethernet0/0          yes       yes             unlimited
  Custom circuit-ids:
Ethernet0/1          no        yes             unlimited
  Custom circuit-ids:
Ethernet0/2          no        yes             unlimited
  Custom circuit-ids:
Ethernet0/3          no        yes             unlimited
  Custom circuit-ids:
Switch#
Switch#
```

The command output shown in the above figure displays trusted and untrusted interfaces along with “Allow Options”.

Configuring Dynamic ARP Inspection

```
Switch(config)# ip arp inspection vlan <vlan number>
```

Verification Command:

```
Switch(config)# do show ip arp inspection
```

ARP Spoofing Prevention

The following are a few best practices that can assist you in protecting your network from ARP spoofing:

Use a Virtual Private Network (VPN)—a VPN enables connections to the Internet through a secure tunnel for devices. This renders every communication encrypted and useless to an attacker using ARP spoofing.

Use static ARP - to stop devices from listening for ARP responses for a certain IP address. Static ARP entries are defined using the ARP protocol. For example, if a workstation consistently connects to the same router, you can set a static ARP entry for that router to thwart attacks.

Use packet filtering - By seeing contradicting source information in ARP packets, packet filtering solutions can detect poisoned ARP packets and prevent them from reaching network devices.

Run a spoofing attack - to see if your current protections are effective. This should be done in conjunction with your IT and security staff. If the attack is successful, locate any gaps in your defenses and fill them.

ARP Spoofing Tools

Many open-source tools are available to accomplish ARP spoofing; some of the more popular ones are listed below.

arpspoof

Network auditing can be done with arpspoof. Using ARP poisoning and other techniques, this tool enables an attacker to intercept network traffic, alter it, and steal passwords and other data.

Features:

- Redirects traffic on the local network by fabricating ARP responses and forwarding them to either a particular target or all hosts along the local network pathways.
- Simple testing package
- Use in concert with other tools for more complex attacks.

Netcommander

An open-source graphical utility with a better user interface than the original command-line tool is called Netcommander.

Features:

- It requires Libnet 1.1.2 or newer and operates on Linux and macOS.
- Man-in-the-middle attacks against wireless networks or any other circumstance where the local IP address is known can be carried out using it.

Larp

A simple ARP spoofing tool called Larp can be used to test ARP cache poisoning.

The ARP protocol is implemented by Larp using Scapy. Before using this tool, Scapy must be installed, but Kali Linux already has Scapy preinstalled, making the process simple.

The intended users of this software are security experts and pentesters.

Features:

- For experienced users, it offers a variety of choices, including using a different interface, target port, etc.
- The two most common purposes are network spoofing and penetration testing.

Aranea

Aranea is a Java-based, open-source web proxy that lets users intercept HTTP(S) requests and answers between a victim's browser and the victim. The user can then immediately alter these requests and responses and evaluate the performance of websites.

Features:

- Aranea is a quick DNS spoofing tool built on Libpcap.
- It is organized, flexible, and multithreaded.
- The hostnames are specified using regular expressions.

KickThemOut

With an ARP spoofing tool called as KickThemOut, you can remove devices from your network by sending fake ARP queries to the intended computers. Man-in-the-middle attacks and DNS poisoning are further uses for it.

Features:

- IPv4 and IPv6 address monitoring.
- You can manage several network interfaces with a single daemon.
- Traffic with VLAN tags (802.1Q) is watched.
- Options include Stdout, plain text files, Syslog, sqlite3, and MySQL.
- IP address output and logging are both kept.

Cain & Abel

It is a general network surveillance tool with ARP spoofing capabilities. It can sniff traffic, decrypt keys, recover passwords, attack clients and servers, and many other things.

Using Cain & Abel, you can also intercept cleartext passwords from network traffic. It operates by observing network activity and quickly determining passwords.

Features:

- The speed of wireless packet injection is increased.
- Talks using VoIP can be recorded.
- passwords that have been scrambled being decoded.
- It is laborious to calculate hashes.
- Passwords that have been cached being accessible

Arpoison

Arpoison is a very strong ARP spoofer. It is a straightforward, lightweight tool that attacks your computer with an ARP spoofing attack. It is simple to use and effective if you are trying to spoof your MAC address.

Features:

- Vicious and Normal are its two modes. Arpoison will give out free ARP responses to every IP address on the local network when it is in the "vicious" mode. It is a noisy method that is only useful in the short run.
- Only in "regular mode" would Arpoison respond to ARP requests for a specific target IP address.
- Uses Libnet 1.1x

Spoofing Attack

MAC Spoofing/Duplicating

MAC Spoofing is the technique of manipulating a MAC address to impersonate the authentic user or launch attacks such as denial-of-service. A MAC address is built on a network interface controller that cannot be changed, but some drivers enable changing the MAC address. This masking process of MAC addresses is known as MAC Spoofing. An attacker sniffs users' active MAC addresses on switch ports and duplicates the MAC address. Duplicating the MAC can intercept the traffic, and traffic destined to the legitimate user may be directed to the attacker.

MAC Spoofing Tool

There are several tools available that offer MAC spoofing with ease. Some popular tools are:

- Technitium MAC Address Changer
- SMAC

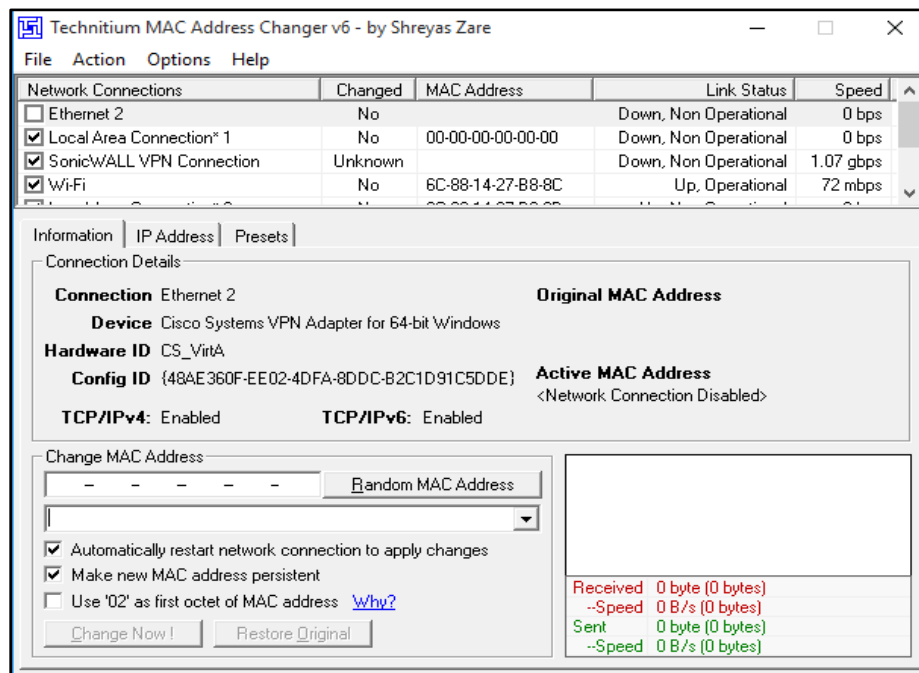


Figure 8-21: Technitium MAC Address Changer

How to Defend Against MAC Spoofing

In order to defend against MAC spoofing, DHCP Snooping and Dynamic ARP Inspection are effective techniques to use. Additionally, a source guard feature is configured on client-facing switch ports.

An IP source guard is a port-based feature that provides a source IP address filtering at Layer 2. The source guard feature monitors and prevents the host from impersonating another host by assuming the authentic host's IP address. In this way, the malicious host is restricted to using its assigned IP address. Source guard uses dynamic DHCP snooping or static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports.

Initially, all types of inbound IP traffic from the protected port are blocked, except for DHCP packets. When a client receives an IP address from the DHCP server or static IP source binding by the administrator, the traffic with an assigned source IP address is permitted from that port. All bogus packets will be denied. In this way, the source guard protects against attack by claiming a neighbor host's IP address. The source guard creates an implicit Port Access Control List (PACL).

STP Attack

STP

A Layer 2 network technique called Spanning Tree Protocol (STP) is used to stop loops from forming inside a network topology. STP was developed to prevent issues when computers exchange data over redundant channels in a local area network (LAN).

STP Attack

There should be a switch at the top called the root in an STP network configuration. The root switch is selected based on the switch with the lowest defined priority (0 through 65,535). A switch starts the process of locating other switches and determining which switch is the root bridge as soon as it is powered on. The network topology is constructed from the perspective of connection once a root bridge has been chosen.

All redundant pathways are barred from accessing the root bridge, which is determined by the switches.

Using bridge protocol data units (BPDU), STP transmits topology and configuration change notifications and acknowledgments (TCN/TCA).

When an attacker, hacker, or unauthorized user impersonates the topology's root bridge, it is known as an STP manipulation attack.

In an effort to compel an STP recalculation, the attacker broadcasts an STP configuration/topology change BPDU.

The BPDU signaled states that the system of the attacker has a lower bridge priority.

The attacker can then view numerous frames that were passed to it from other switches.

When the root bridge changes, STP recalculation can disrupt the network, which can result in a denial-of-service (DoS) condition.

The attacker in the figure below is leveraging STP network topology changes to make its host the root bridge.

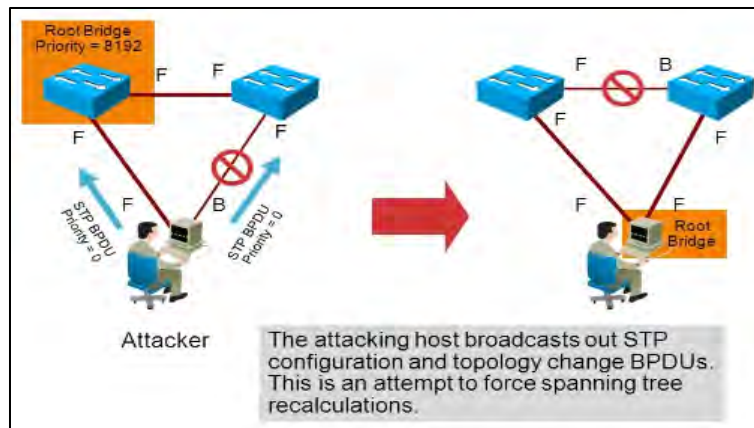


Figure 8-22: STP Attack

How to Prevent STP Attack

Use the root guard and BPDU guard capabilities in the Cisco IOS Software to prevent STP manipulation. These instructions keep an eye on where the root bridge and STP domain borders are placed.

The root bridge can be placed anywhere in the network thanks to the STP root guard feature. All active network topology is maintained predictably using the STP BPDU guard.

The configuration below demonstrates how to enable BPDU guard using portfast to disable ports upon BPDU message detection and to disable ports that would become the root bridge as a result of their BPDU advertisement.

```
Switch#configure terminal
Switch(config)#spanning-tree portfast bpduguard
Switch(config)#interface fa0/12
Switch(config)#spanning-tree guard root
```

DNS Poisoning Techniques

DNS poisoning, or DNS spoofing, manipulates DNS servers to redirect victims to malicious servers by altering DNS table entries. This leads to false IP address resolution, tricking victims into connecting to attackers' servers instead of legitimate ones. Once connected, attackers can compromise systems and steal data.

Common Techniques:

- Intranet DNS Spoofing: Targets DNS servers within a local network.
- Internet DNS Spoofing: Exploits DNS servers on the internet.
- Proxy Server DNS Poisoning: Alters DNS entries on a proxy server.
- DNS Cache Poisoning: Injects false information into a DNS cache to redirect users.

This attack exploits DNS, which translates domain names (e.g., www.eccouncil.org) into IP addresses (e.g., 208.66.172.56), affecting the integrity of domain-to-IP resolution.

Intranet DNS Spoofing

In an intranet DNS spoofing attack, an attacker within a local area network (LAN) employs Address Resolution Protocol (ARP) poisoning to intercept and manipulate DNS requests. By sending malicious ARP messages, the attacker associates their MAC address with the IP address of the network's router or DNS server. This redirection causes DNS queries from clients to be sent to the attacker's machine instead of the legitimate server.

Once the attacker receives a DNS request, they respond with a forged DNS reply, directing the client to a counterfeit website under the attacker's control. Unsuspecting users may then enter sensitive information, such as passwords, into the fake site, allowing the attacker to capture this data. After harvesting the information, the attacker might redirect the client to the legitimate website to avoid suspicion.

This method effectively enables a man-in-the-middle attack, compromising the security of the intranet and endangering user data.

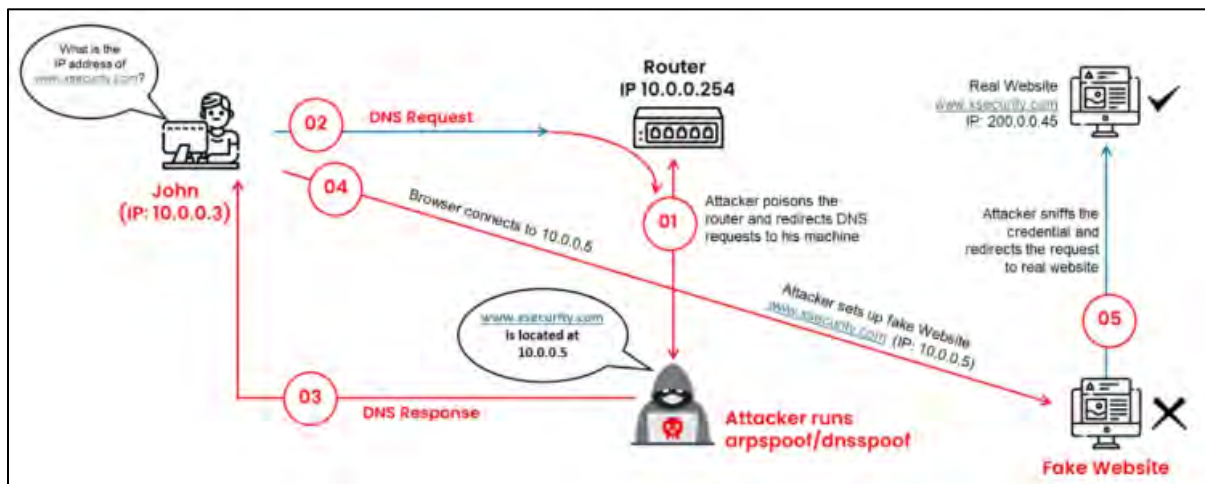


Figure 8-23: Intranet DNS Spoofing

Internet DNS Spoofing

Internet DNS spoofing, also known as remote DNS poisoning, is a cyberattack where an attacker manipulates the Domain Name System (DNS) to redirect a victim's traffic to malicious sites. This is often achieved by setting up a rogue DNS server and using malware, such as Trojans, to alter the DNS settings on the victim's computer. By changing the primary DNS entries to point to the attacker's server, the victim's internet traffic is redirected, allowing the attacker to intercept sensitive information.

UPGUARD

This attack is a form of man-in-the-middle (MITM) attack, enabling the attacker to monitor and capture confidential data transmitted by the victim.

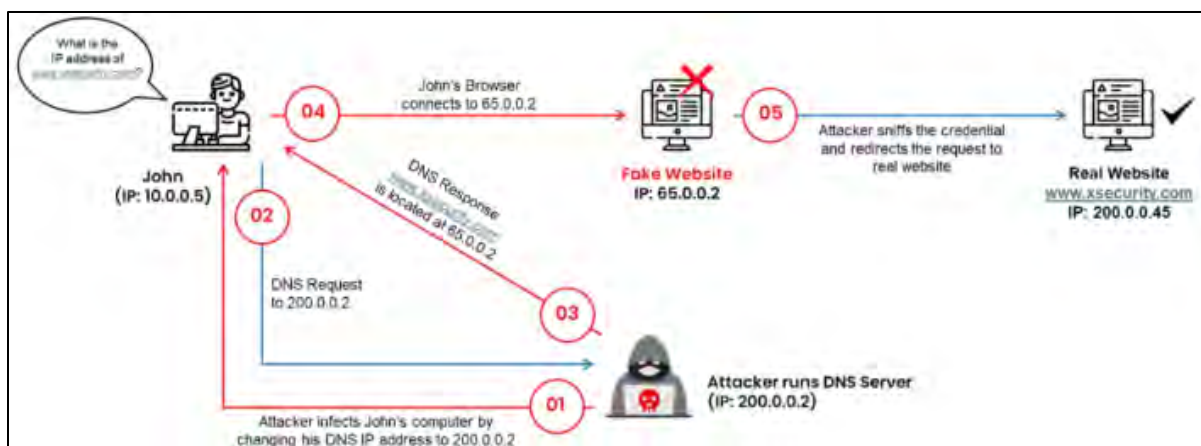


Figure 8-24: Internet DNS Spoofing

Proxy Server DNS Spoofing

In a proxy server DNS poisoning attack, an attacker sets up a rogue proxy server configured with a fraudulent DNS. Using malware, such as a Trojan, the attacker alters the victim's proxy settings to route their internet traffic through the malicious proxy. Consequently, when the victim attempts to access a legitimate website, the proxy redirects the request to a counterfeit site controlled by the attacker. This enables the attacker to intercept sensitive information, such as login credentials, before optionally forwarding the victim to the actual website to avoid detection.

This method effectively allows the attacker to perform a man-in-the-middle attack, compromising the victim's data security. Implementing robust security measures, such as up-to-date antivirus software and cautious handling of unsolicited downloads, can help prevent such attacks.

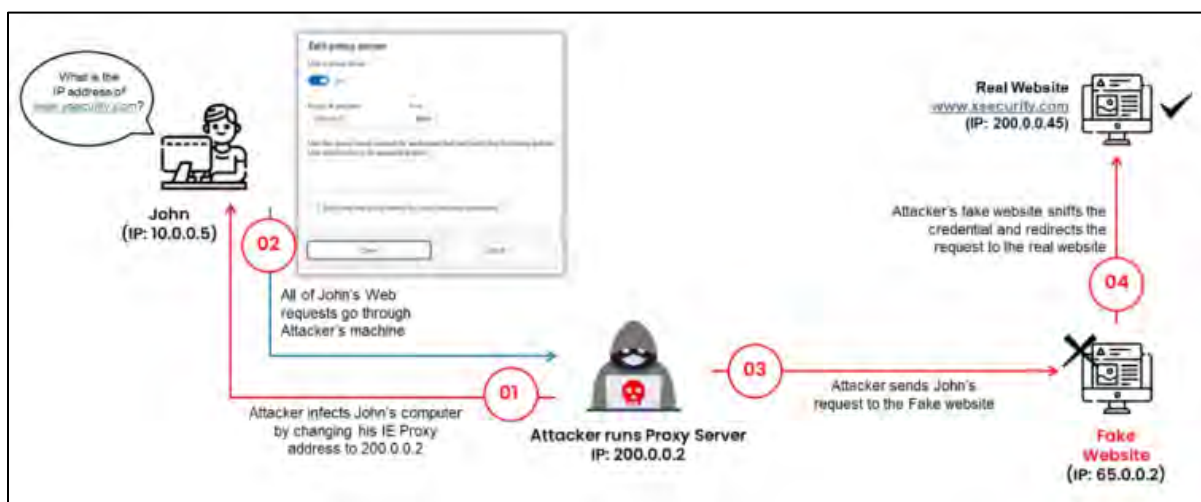


Figure 8-25: Proxy Server DNS Spoofing

DNS Cache Poisoning

DNS cache poisoning involves altering or adding fake DNS records to a DNS resolver's cache to redirect users to malicious sites. Attackers exploit the DNS system, which stores recently resolved domain names in cache memory for faster resolution.

When a user requests a domain, the resolver checks its cache for a matching entry. If the cache contains a forged record inserted by the attacker, the resolver uses the fake IP address, redirecting the user to a malicious server. This compromises data security and enables phishing or other attacks.

Mitigation includes using DNSSEC (DNS Security Extensions) to validate DNS responses and prevent unauthorized changes.

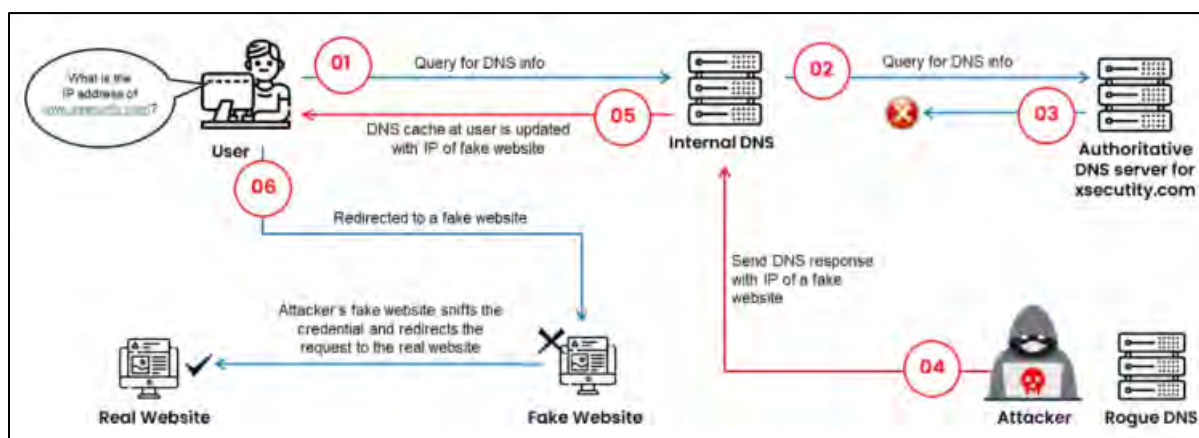


Figure 8-26: DNS Cache Spoofing

SAD DNS Attack

SAD DNS (Side-channel Attacked DNS) is a modern variant of DNS cache poisoning that enables attackers to inject malicious DNS records into a DNS resolver's cache. This manipulation redirects user traffic to attacker-controlled servers, facilitating man-in-the-middle (MITM) attacks. Unlike traditional DNS cache poisoning, SAD DNS exploits side-channel vulnerabilities in the DNS infrastructure, allowing attackers to predict certain parameters and successfully poison the cache without being on the same network as the victim.

DNS Poisoning Tool

Attackers utilize various tools to perform DNS poisoning by redirecting domain names to different IP addresses specified in fake DNS entries. One such tool is:

DerpNSpoof: A Python-based DNS spoofing tool that assists in spoofing DNS query packets for specific IP addresses or groups of hosts within a network. Users can create a list of fake DNS records and load it into the tool to redirect victims to malicious websites.

By employing such tools, attackers can effectively manipulate DNS responses, leading users to unintended and potentially harmful destinations.

Sniffing Tools

Wireshark

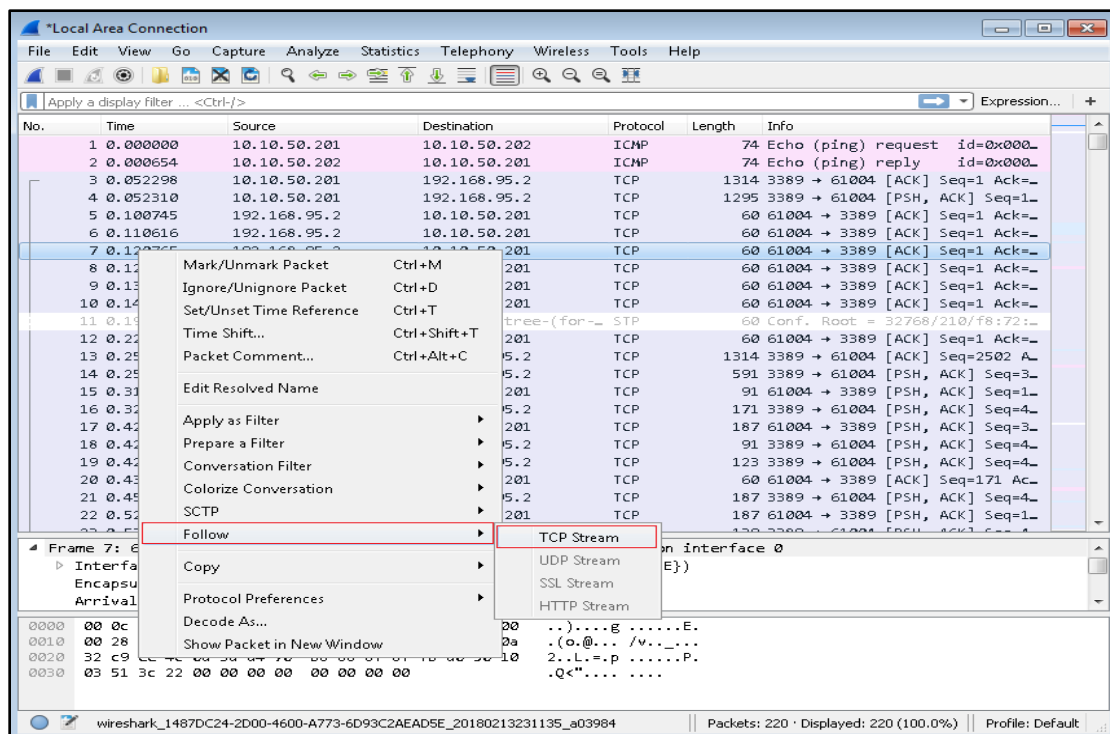
Wireshark is the most popular and widely used Network Protocol Analyzer tool across commercial, governmental, non-profit, and educational organizations. It is a free, open-source tool available for Windows, Linux, MAC, BSD, Solaris, and other platforms natively. Wireshark also offers a terminal version called TShark.

Follow the TCP Stream in Wireshark

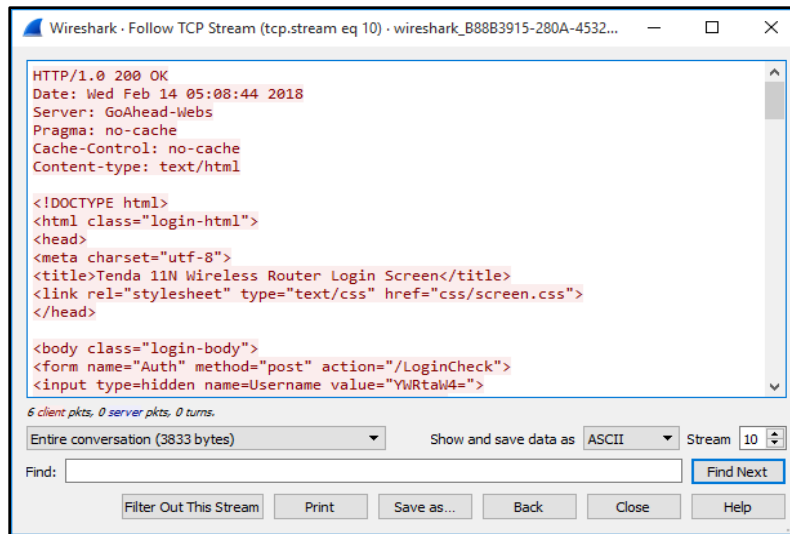
Working on TCP-based protocols can be very helpful by using the “Follow TCP Stream” feature.

This helps to examine the data from a TCP stream in the way that the application layer sees it.

Perhaps you are looking for passwords in a Telnet stream.



Examine the data from the captured packet.



Filters in Wireshark

Following are the Wireshark filters for filtering the output.

Operator	Function	Example
==	Equal	ip.addr == 192.168.1.1
eq	Equal	tcp.port eq 23
!=	Not equal	ip.addr != 192.168.1.1
ne	Not equal	ip.src ne 192.168.1.1
contains	Contains specified value	http contains "http://www.ipspecialist.net"

Table 8-01: Wireshark Filters

Display Filters in Wireshark

Wireshark offers robust display filters to streamline traffic analysis on target networks based on protocol type, IP address, port, and more. These filters refine the view of captured packets, making it easier to focus on specific data. To set up a filter, simply input the protocol name (e.g., arp, http, tcp, udp, dns, ip) into Wireshark's filter box. Multiple filters can be applied simultaneously. Below are examples of common Wireshark display filters:

Display Filters by Category

Filtering by Protocol

- Input protocol names like arp, http, tcp, udp, dns, or ip in the filter box.

Monitoring Specific Ports

- tcp.port==23
- ip.addr==192.168.1.100
- ip.addr==192.168.1.100 && tcp.port==23

Filtering by IP Address

- Single IP: ip.addr == 10.0.0.4

- Multiple IPs: `ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5`

Advanced Filtering

- `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 Wireshark Filters

Specific TCP or UDP Filters

- `tcp.flags.reset==1`: Shows all TCP resets.
- `udp contains 33:27:58`: Filters packets with hex values `0x33 0x27 0x58`.

HTTP and Analysis Filters

- `http.request`: Displays all HTTP GET requests.
- `tcp.analysis.retransmission`: Highlights retransmissions in the trace.

Custom TCP Content Filters

- `tcp contains traffic`: Displays TCP packets containing the word “traffic”.

Protocol-Specific and Combined Filters

- `!(arp or icmp or dns)`: Excludes ARP, ICMP, and DNS traffic.
- `tcp.port == 4000`: Filters packets where TCP port 4000 is the source or destination.
- `tcp.port eq 25 or icmp`: Isolates SMTP (port 25) and ICMP traffic.

LAN and Network-Specific Filters

- `ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16`: Focuses on LAN traffic between devices (192.168.x.x).
- `ip.src != xxx.xxx.xxx.xxx && ip.dst != xxx.xxx.xxx.xxx && sip`: Filters by a protocol like SIP while excluding specific IPs.

These examples illustrate how Wireshark's display filters empower users to isolate and analyze network traffic effectively, ensuring a tailored and efficient troubleshooting experience.

Sniffing Tools

Capsa Portable Network Analyzer

Capsa is a versatile portable network performance analysis and diagnostic tool designed to capture and analyze packets efficiently. It features a user-friendly interface, making it an excellent choice for monitoring and protecting networks in critical business environments.

While Capsa is primarily used for legitimate purposes such as identifying network vulnerabilities and optimizing performance, attackers may exploit it to sniff packets on a target network, potentially exposing sensitive data and network weaknesses.

By leveraging its capabilities, network administrators can gain valuable insights to secure their infrastructure and mitigate risks effectively.

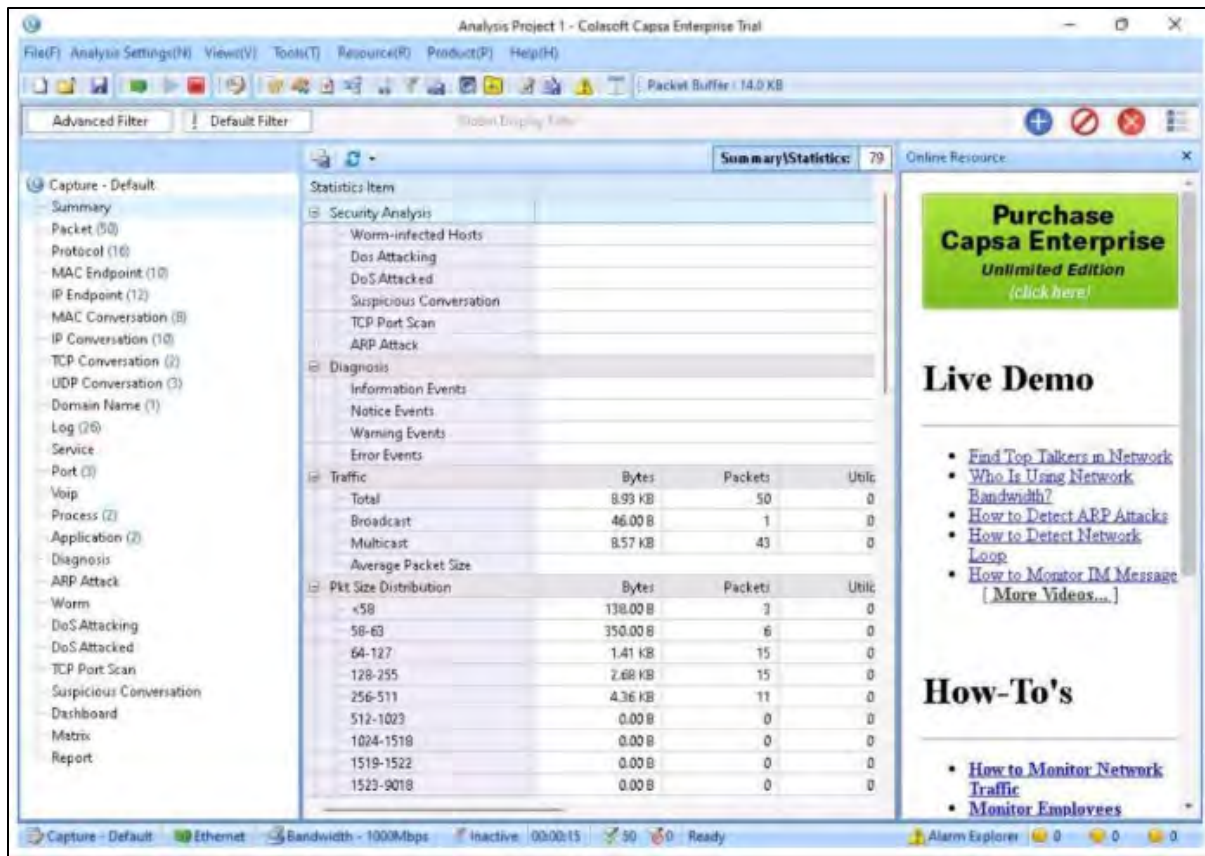


Figure 8-28: Capsa Portable Network Analyzer

OmniPeek

OmniPeek is a powerful network analyzer offering real-time visibility and expert analysis across various segments of the target network. This tool enables users to drill down into data, identify, and resolve performance bottlenecks effectively.

Key features include:

- **Real-Time Analysis:** Monitors network traffic live for immediate insights.
- **Analytic Plug-ins:** Enhances targeted visualization and search capabilities.
- **Google Maps Plug-in:** Integrates a Google map within the capture window to display the geographic locations of public IP addresses from captured packets.

Defending Against Sniffing

Best practices against Sniffing include the following approaches to protecting network traffic:

- Using HTTPS instead of HTTP
- Using SFTP instead of FTP
- Use Switch instead of Hub
- Configure Port Security
- Configure DHCP Snooping
- Configure Dynamic ARP Inspection
- Configure Source Guard

- Use Sniffing Detection tool to detect NIC functioning in a Promiscuous Mode
- Use Strong Encryption Protocols

Sniffing Detection Techniques

Ping Method

The Ping technique is used to detect a sniffer. A ping request is sent to the suspect IP address with a spoofed MAC address. The NIC will not respond to the packet if it is not running in promiscuous mode. In cases where the suspect is running a sniffer, it will respond to the packet. This is an older technique and is not very reliable.

ARP Method

Using ARP, sniffers can be detected with the help of the ARP Cache. By sending a non-broadcast ARP packet to the sniffer, the MAC address will be cached if the NIC is running in promiscuous mode. The next step is to send a broadcast ping with a spoofed MAC address. If the machine is running in promiscuous mode, it replies to the packets of the known MAC address from the sniffed non-broadcasted ARP packets.

Promiscuous Detection Tool

Sniffers have the ability to record all network communication while in promiscuous mode. Promiscuous Detection tools such as **PromqryUI** or **Nmap** can also be used for the detection of a Network Interface Card running in Promiscuous Mode. These tools are GUI-based application software.

PromqryUI - A security tool from Microsoft called PromqryUI can be used to identify network interfaces that are active in promiscuous mode.

Nmap - You may determine whether a target on a local Ethernet has its network card in promiscuous mode by using Nmap's NSE script.

command to identify a NIC operating in promiscuous mode:

```
nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]
```

Countermeasures

Defending Against Sniffing

- Restrict physical network access to prevent unauthorized installations.
- Use encryption (e.g., HTTPS, SSH, SFTP, WPA3) for secure data transmission.
- Employ static IPs, ARP tables, and MAC address locking to thwart spoofing.
- Disable SSID broadcasts and use VLANs for network segmentation.
- Monitor traffic with IDS/IPS and detect NICs in promiscuous mode.
- Implement complex passwords, MAC filtering, and VPNs for added security.

Detecting Sniffing

- **Promiscuous Mode:** Use tools like Nmap or NetScanTools Pro to identify devices capturing all packets.
- **Ping Method:** Identify systems responding to non-broadcast ARP requests.

- **DNS Method:** Monitor reverse DNS lookups for unusual traffic patterns.
- **ARP Method:** Detect nodes responding to cached ARP addresses.

Tools for Detection

- **Nmap:** Detect NICs in promiscuous mode.
- **NetScanTools Pro:** Identify interfaces listening for all Ethernet packets.

Summary

This chapter covered sniffing concepts, including sniffing at the data link layer of the OSI Model. We explored various sniffing techniques such as MAC attacks, DHCP attacks, ARP poisoning, spoofing attacks, and DNS poisoning, along with their countermeasures. Additionally, we reviewed several sniffing tools and detailed methods to prevent sniffing attacks. The chapter concluded with an in-depth discussion on sniffing detection techniques.

Mind Map

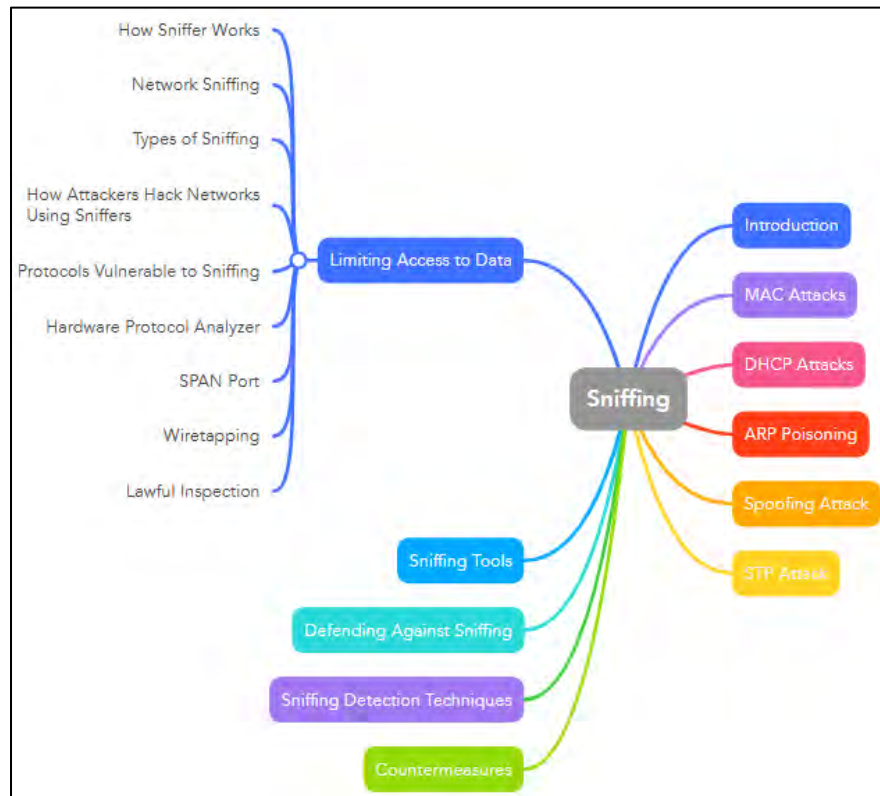


Figure 8-29: Mind Map-Sniffing

Practice Questions

1. Sniffing is performed over _____.
 - A. Static Port
 - B. Dynamic Port
 - C. Promiscuous Port

D. Management Port

2. Sniffing without interfering is known as _____.
 - A. Active Sniffing
 - B. Passive Sniffing
 - C. Static Sniffing
 - D. Dynamic Sniffing
3. The port, which sends a copy of the packet over another port at layer 2 is called _____.
 - A. SPAN Port
 - B. Promiscuous Port
 - C. Management Port
 - D. Data Port
4. Wiretapping with legal authorization is called _____.
 - A. Lawful Interception (LI)
 - B. Active Wiretapping
 - C. Passive Wiretapping
 - D. PRISM
5. Which is the best option for defense against ARP poisoning?
 - A. Port Security
 - B. DHCP Snooping
 - C. DAI with DHCP Snooping
 - D. Port Security with DHCP Snooping
6. Which of the following Wireshark filters displays packets from 10.0.0.1?
 - A. ip.addr != 10.0.0.1
 - B. ip.addr ne 10.0.0.1
 - C. ip.addr == 10.0.0.1
 - D. ip.addr - 10.0.0.1
7. Which of the following can be used for the detection of a Network Interface Card running?
 - A. PromqryUI
 - B. Nmap
 - C. None of the above
 - D. Both A and B

8. Which of the following is used to intercept and sniff traffic on a local network and also used for network auditing?
 - A. PromqryUI
 - B. arpspoof
 - C. Larp
 - D. Netcommander
9. Which of the following automatically assigns an Internet Protocol (IP) host with its IP address and other configuration data like the subnet mask and default gateway?
 - A. ARP
 - B. STP
 - C. DHCP
 - D. DNS
10. Which of the following tools can be used to test ARP cache poisoning?
 - A. Larp
 - B. arpspoof
 - C. Netcommander
 - D. Aranea

Answers

1. Answer: C

Explanation: In the process of Sniffing, an attacker gets connected to the target network to sniff the packets. Using Sniffers, which turns the attacker's system's Network Interface Card (NIC) into promiscuous mode, the attacker captures the packet. Promiscuous mode is the interface mode in which NIC responds to every packet it receives.

2. Answer: B

Explanation: Passive Sniffing is the sniffing type in which there is no need to send additional packets or interfere with the device, such as a hub, to receive packets. As we know, the hub broadcasts every packet to its ports, which helps the attacker monitor all traffic passing through the hub without effort.

3. Answer: A

Explanation: SPAN makes a copy of all frames destined for a port and copies them to the SPAN destination port.

4. Answer: A

Explanation: Lawful Interception (LI) is a process of wiretapping with legal authorization, which allows law enforcement agencies to wiretap the communication of the individual user selectively.

5. Answer: C

Explanation: DAI is used with DHCP snooping; IP-to-MAC bindings can be tracked from DHCP transactions to protect against ARP poisoning (an attacker trying to get your traffic instead of to your destination). DHCP snooping is required to build the MAC-to-IP bindings for DAI validation.

6. Answer: C

Explanation: The following are the filters of Wireshark to filter the output:

Operator Function Example:

== Equal ip.addr == 192.168.1.1

eq Equal tcp.port eq 23

!= Not equal ip.addr != 192.168.1.1

ne Not equal it.src ne 192.168.1.1

contains Contains specified value http contains <http://www.ipspecialist.net>

7. Answer: D

Explanation: Promiscuous Detection tools such as **PromqryUI** or **Nmap** can also be used for the detection of a Network Interface Card running in Promiscuous Mode. These tools are GUI-based application software.

- **PromqryUI** - A security tool from Microsoft called PromqryUI can be used to identify active network interfaces in promiscuous mode.

- **Nmap** - You may determine whether a target on a local Ethernet has its network card in promiscuous mode by using Nmap's NSE script.

8. Answer: B

Explanation: Arpspoof is a tool used for ARP (Address Resolution Protocol) spoofing, which allows an attacker to redirect network traffic by forging ARP replies. This technique is often used to intercept and sniff traffic on a local network, making it an effective way to eavesdrop on communication between hosts. However, it is important to note that ARP spoofing is a potentially malicious activity and can be used for unauthorized and harmful purposes. It is commonly used by security professionals and network administrators for legitimate security testing and network auditing.

9. Answer: C

Explanation: DHCP is the process of allocating the IP address dynamically so that these addresses are assigned automatically and can be reused when hosts do not need them. Round Trip time is the measurement of time from discovery of the DHCP server up to obtaining the leased IP address. RTT can be used to determine the performance of DHCP. Using a UDP broadcast, a DHCP client sends an initial DHCP-Discover packet because it does not have information about the network to which they are connected. The DHCP server replies to the DHCP-Discover packet with a DHCP-Offer Packet offering the configuration parameters. The DHCP client will send a DHCP-Request packet destined for the DHCP server requesting configuration parameters. Finally, the DHCP server will send the DHCP-Acknowledgement packet containing configuration parameters.

10. Answer: A

Explanation: A simple ARP spoofing tool called Larp can be used to test ARP cache poisoning. The ARP protocol is implemented by Larp using Scapy. Before using this tool, Scapy must be installed, but Kali Linux already has Scapy preinstalled, making the process simple.

The intended users of this software are security experts and pentesters.