Module 08

Sniffing

Learning Objectives

01 Summarize Sniffing Concepts

02 Demonstrate Different Sniffing Techniques

03 Use Sniffing Tools

04 Explain Sniffing Countermeasures

Objective 01

Summarize Sniffing Concepts

Network Sniffing

Packet Sniffing

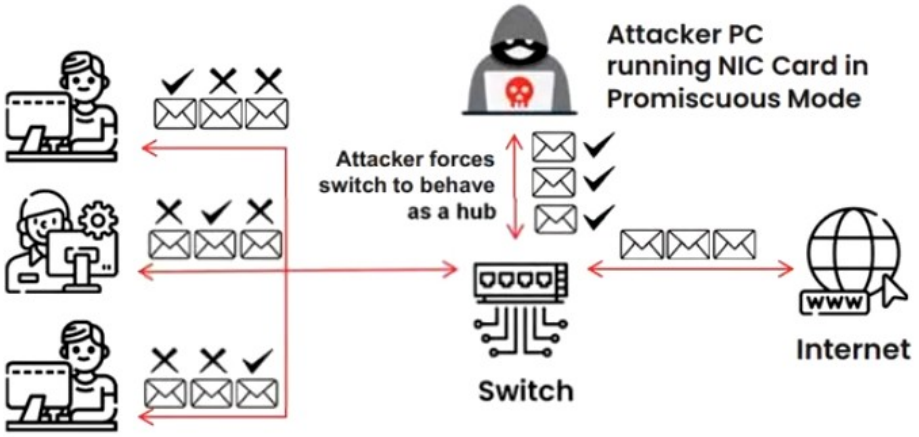
Packet sniffing is the process of monitoring and capturing all data packets passing through a given network using a software application or hardware device

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

Packet sniffing allows an attacker to gather sensitive information such as Telnet passwords, email traffic, syslog traffic, router configuration, web traffic, DNS traffic, FTP passwords, chat sessions, and account information

How a Sniffer Works

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



Types of Sniffing

Passive Sniffing

- Passive sniffing refers to sniffing through a hub, wherein the traffic is sent to all ports
- It involves monitoring packets sent by others without sending any additional data packets in the network traffic
- In a network that uses hubs to connect systems, 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- Hub usage is an outdated approach.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

Note: Passive sniffing provides significant stealth advantages over active sniffing

Active Sniffing

- Active sniffing is used to sniff a switch-based network
- Active sniffing involves injecting Address Resolution Packets (ARP) into the network to flood the switch's Content Addressable Memory (CAM) table, which keeps track of host-port connections

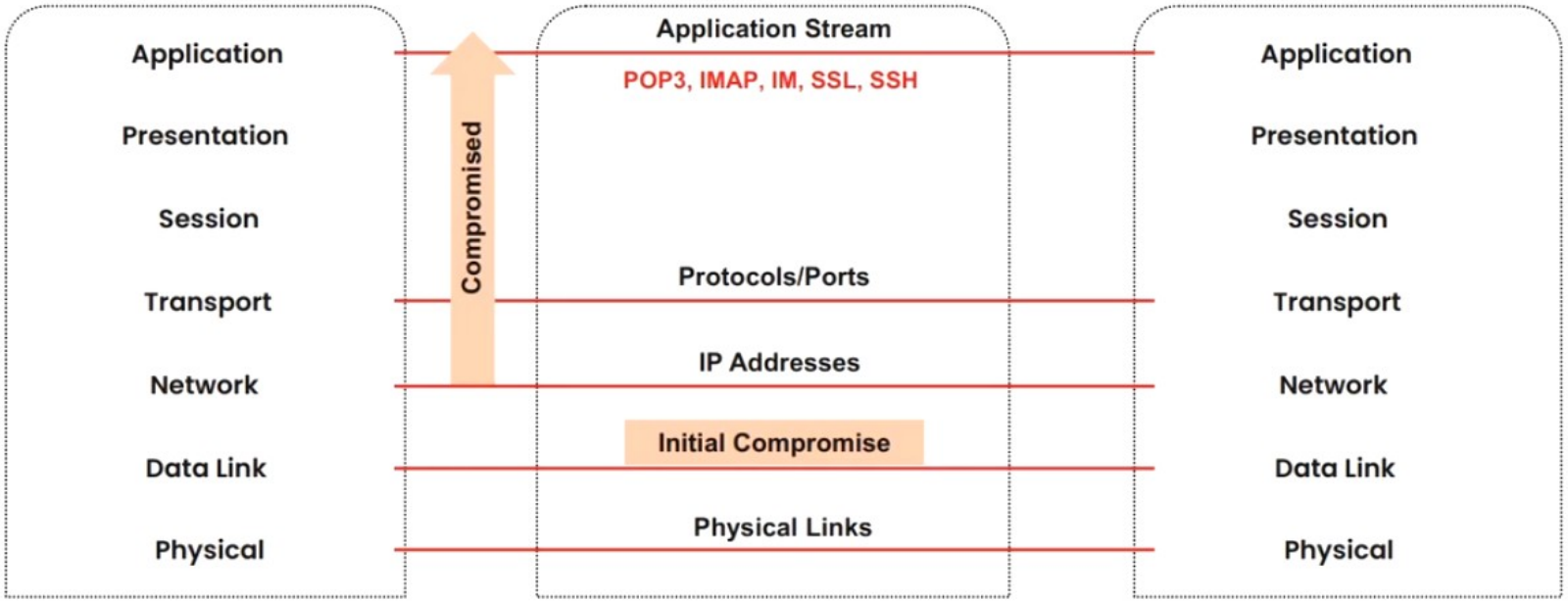
Active Sniffing Techniques

MAC Flooding	**DHCP Attacks**
DNS Poisoning	**Switch Port Stealing**
ARP Poisoning	**Spoofing Attack**

Sniffing in the Data Link Layer of the OSI Model

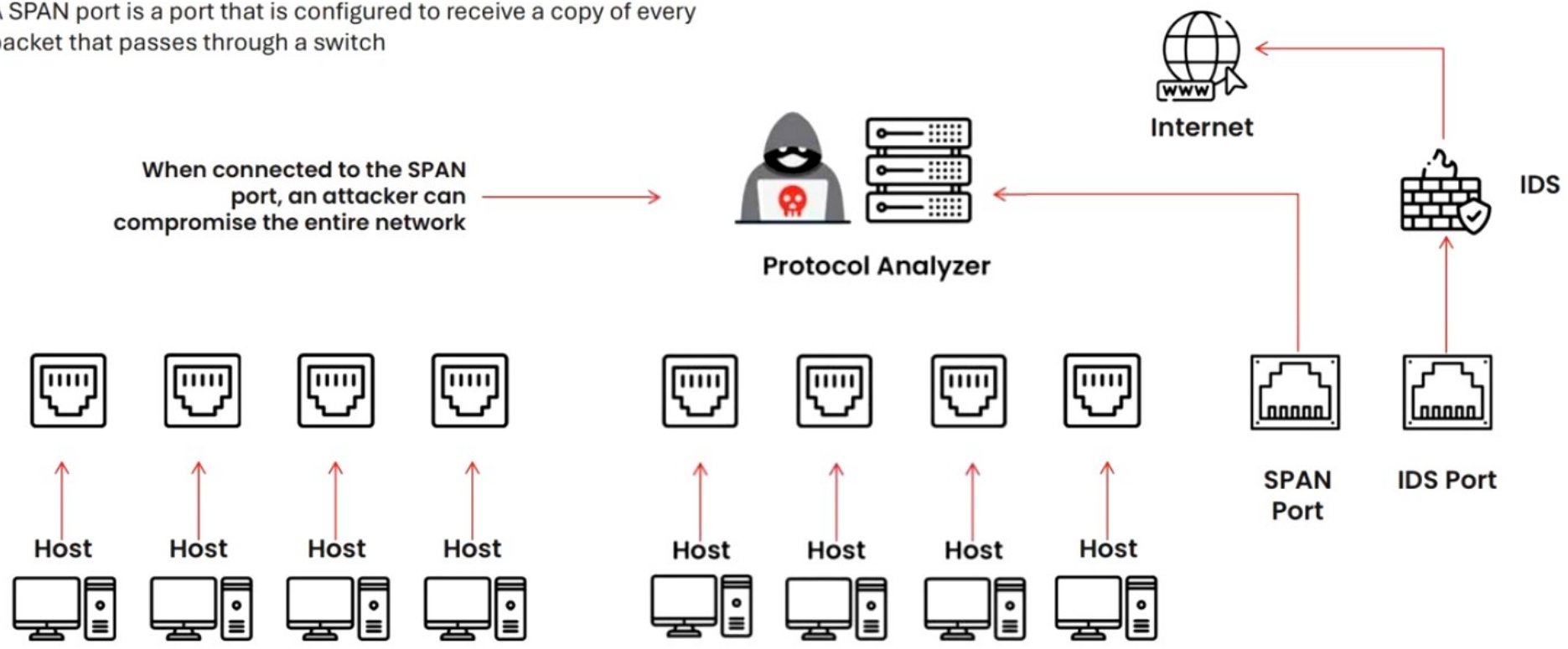
Sniffers operate at the data link layer of the OSI model

Networking layers in the OSI model are designed to work independently of each other; if a sniffer sniffs data in the data link layer, the upper OSI layers will not be aware of the sniffing



SPAN Port

A SPAN port is a port that is configured to receive a copy of every packet that passes through a switch



Objective 02

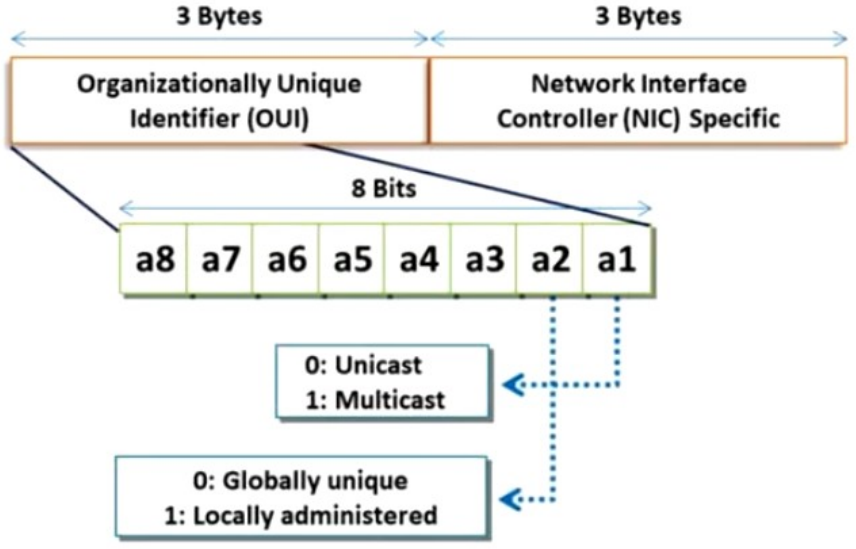
Demonstrate Different Sniffing Techniques

MAC Address/CAM Table

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

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

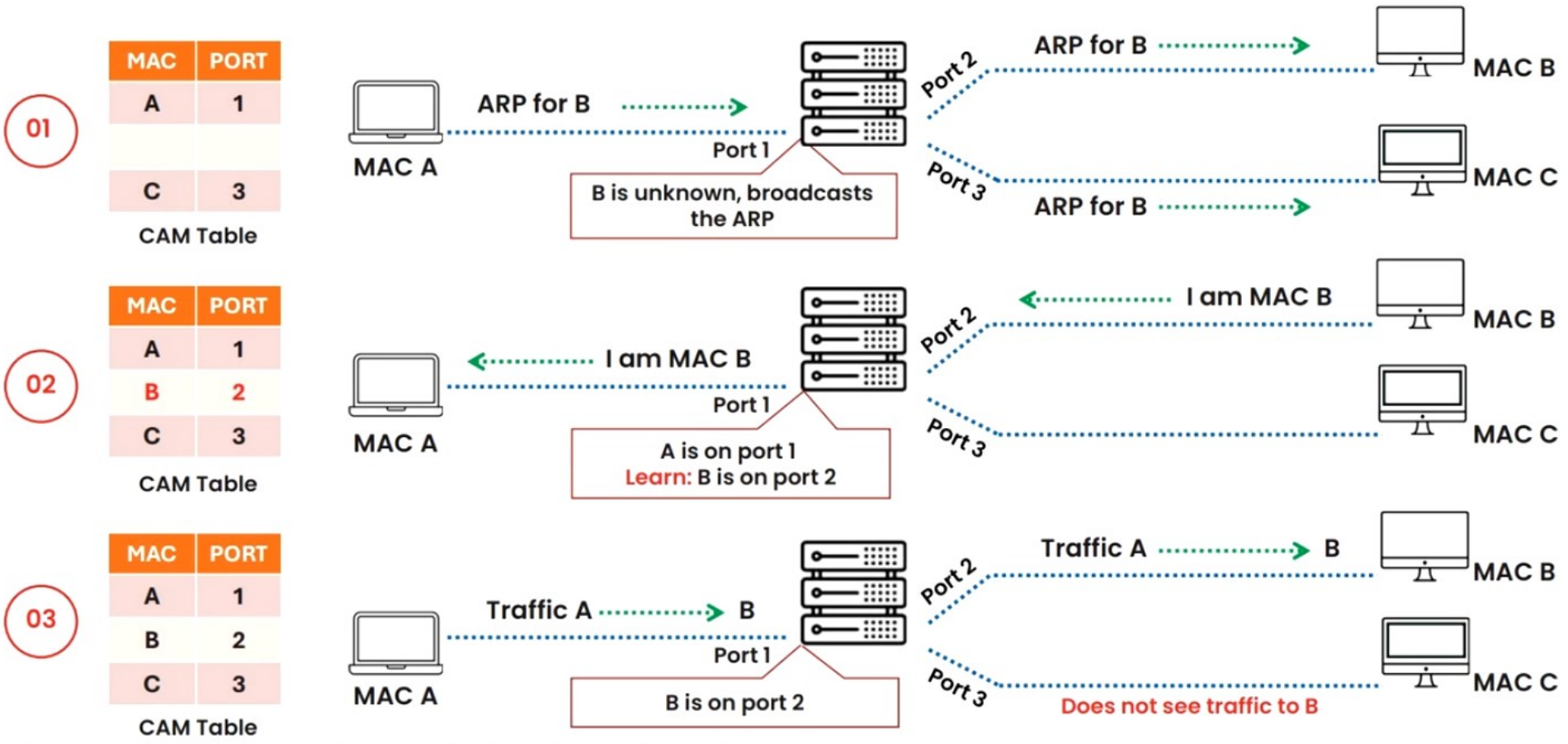
MAC Address



CAM Table

vlan	MAC Add	Type	Learn	Age	Ports
255	00:d3:ad:34:12:3g	Dynamic	Yes	0	Gi5/2
5	as:23:df:45:45:t6	Dynamic	Yes	0	Gi2/5
5	er:23:23:er:t5:e3	Dynamic	Yes	0	Gi1/6

How CAM Works



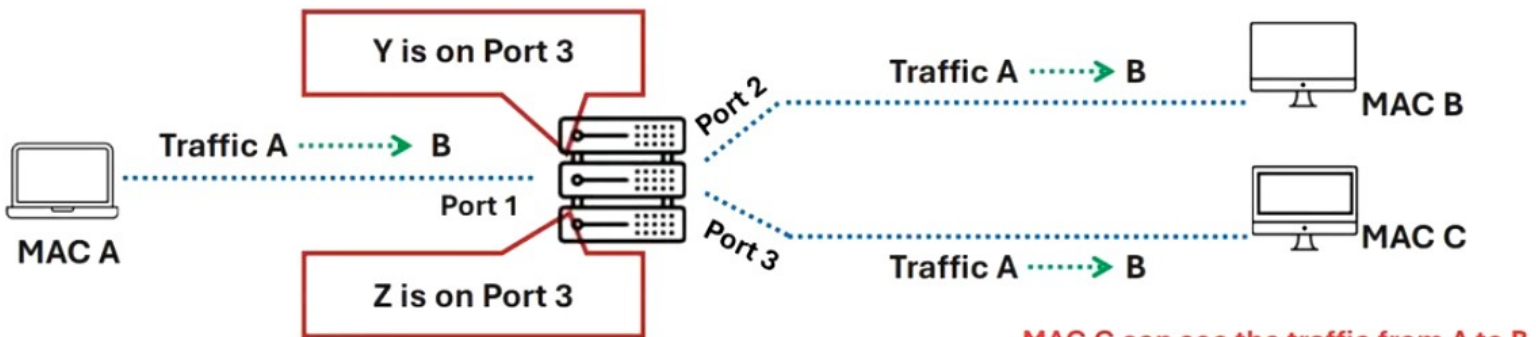
What Happens When a CAM Table Is Full?

Once the CAM table fills up on a switch, additional ARP request traffic floods every port on the switch

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

This attack will also fill the CAM tables of adjacent switches

MAC	PORT
Y	3
Z	3
C	3

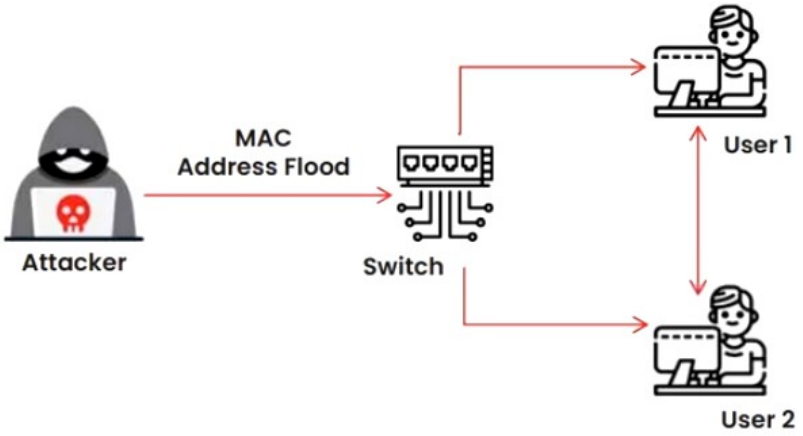


MAC C can see the traffic from A to B

MAC Flooding

MAC flooding involves the flooding of the 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 attackers can sniff the traffic easily

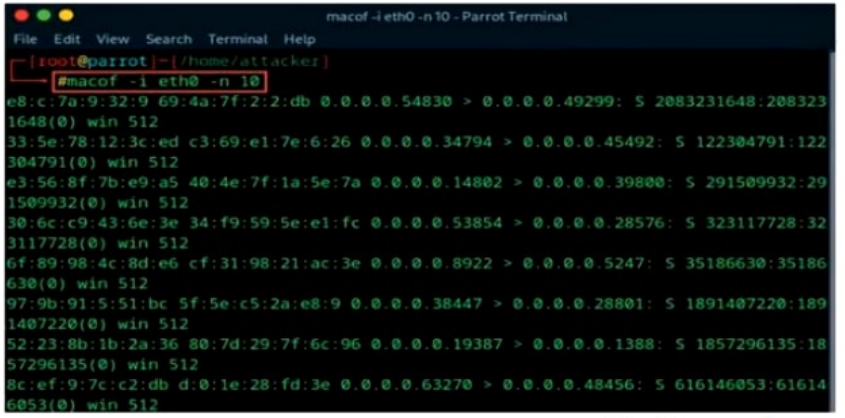


Mac Flooding Switches with macof

macof is a Unix/Linux tool that is a part of the dsniff collection

macof sends random source MAC and IP addresses

This tool floods the switch's CAM tables (131,000 per min) by sending bogus MAC entries



https://www.monkey.org

Switch Port Stealing

The Switch Port Stealing sniffing technique uses MAC flooding to sniff the packets

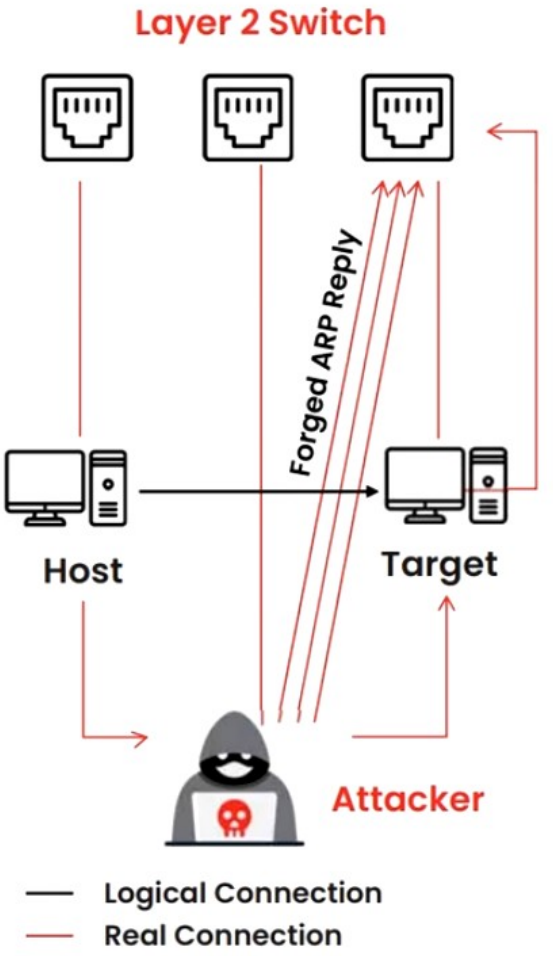
The attacker floods the switch with forged gratuitous ARP packets with the target MAC address as the source and his/her own MAC address as the destination

A race condition of the attacker's flooded packets and the target host's packets occurs; thus the switch must change its MAC address, binding constantly between two different ports

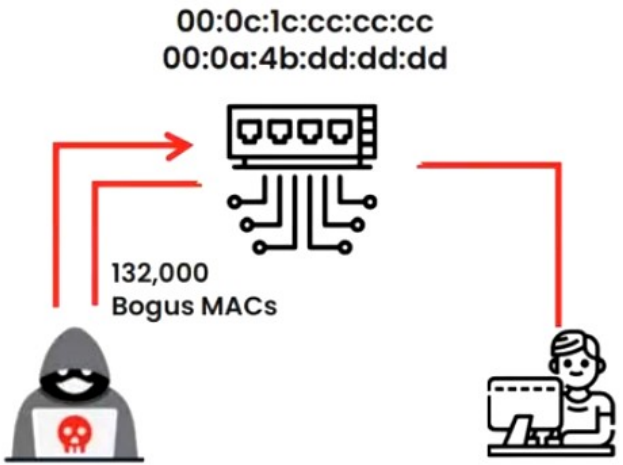
In such a case, if the attacker is fast enough, he/she will able to direct the packets intended for the target host toward his/her switch port

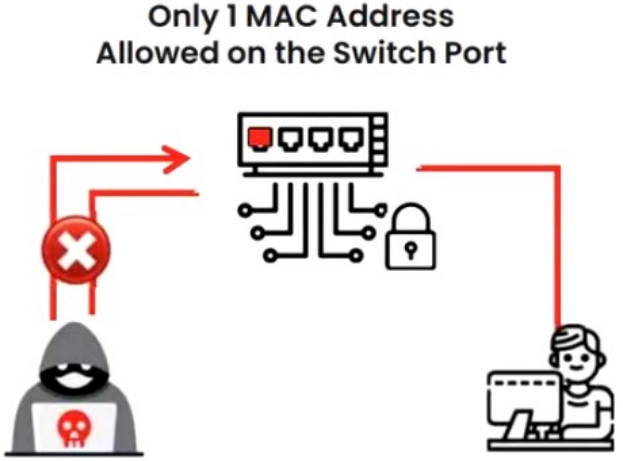
The attacker now manages to steal the target host's switch port and sends ARP requests to the stolen switch port to discover the target host's IP address

When the attacker gets an ARP reply, this indicates that the target host's switch port binding has been restored, and the attacker can now sniff the packets sent toward the targeted host



How to Defend against MAC Attacks





Configuring Port Security on Cisco Switch:

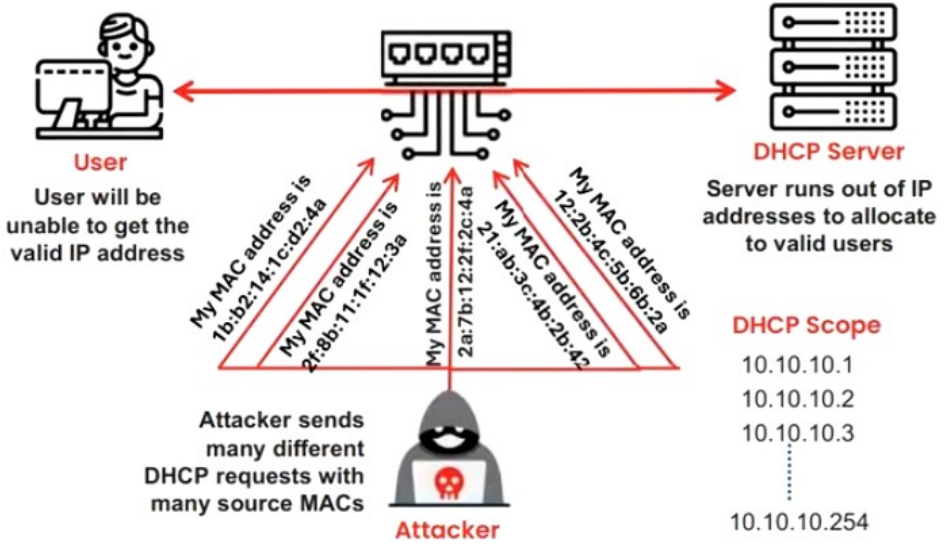
- switchport port-security
- switchport port-security maximum {1-3072}
- switchport port-security violation restrict
- switchport port-security aging time 2
- switchport port-security aging type inactivity
- snmp-server enable traps port-security trap-rate 5

Port security can be used to restrict inbound traffic from only a selected set of MAC addresses and limit MAC flooding attack

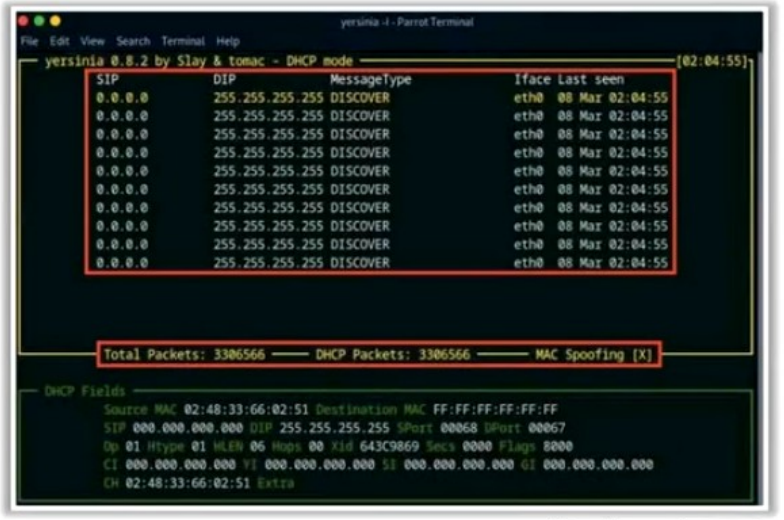
DHCP Starvation Attack

This is a denial-of-service (DoS) attack on the DHCP servers where the attacker broadcasts forged DHCP requests and tries to lease all the DHCP addresses available in the DHCP scope

Therefore, the legitimate user is unable to obtain or renew an IP address requested via DHCP, and fails to get access to the network



DHCP Starvation Attack Tool: Yersinia



https://sourceforge.net

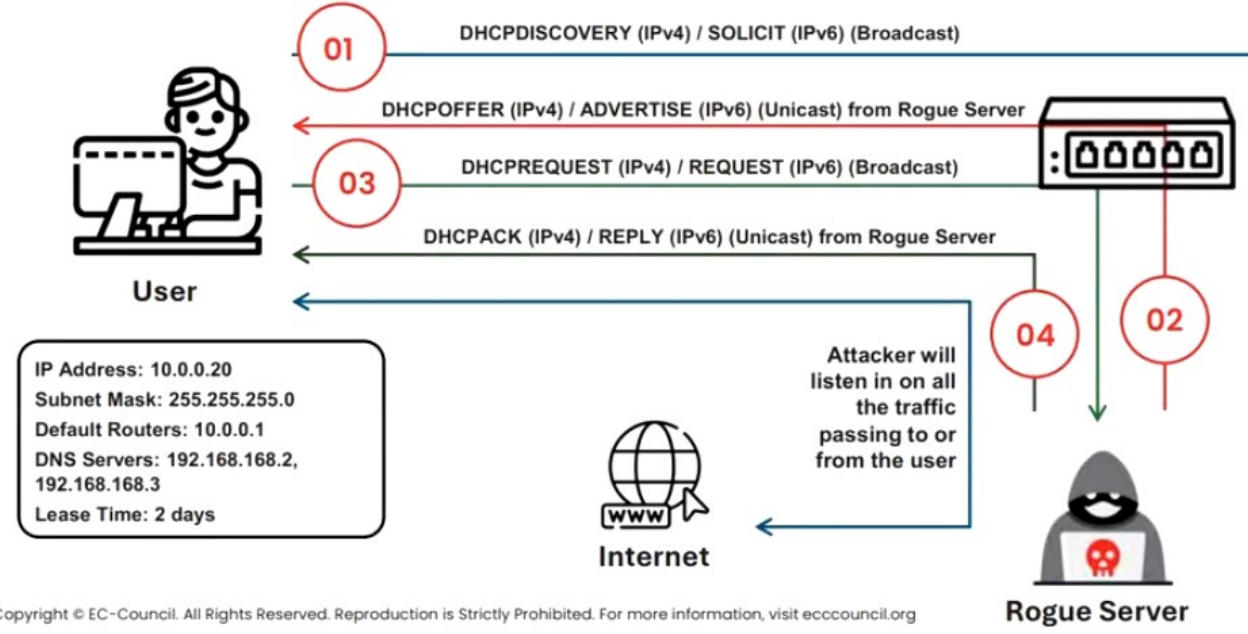
DHCP Starvation Attack Tools

- dhcpStarvation.py (https://github.com)
- Metasploit (https://www.metasploit.com)
- Hyenae (https://sourceforge.net)
- DHCPig (https://github.com)

Rogue DHCP Server Attack

The attacker sets up a rogue DHCP server on the network and responds to DHCP requests with bogus IP addresses resulting in compromised network access

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



By running a rough DHCP server, an attacker can send incorrect TCP/IP setting

Wrong Default Gateway → Attacker is the gateway

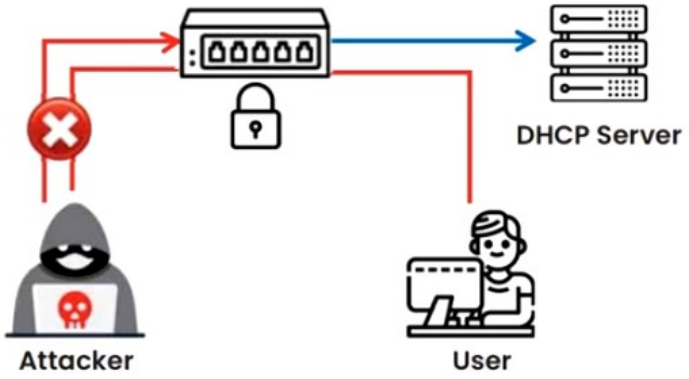
Wrong DNS server → Attacker is the DNS server

Wrong IP Address → DoS with spoofed IP

How to Defend Against DHCP Starvation and Rogue Server Attacks

Enable port security to defend against DHCP starvation attacks

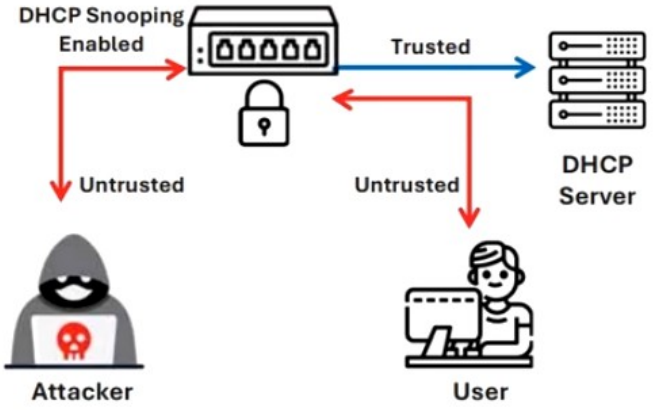
- Configuring the MAC limit on the switch's edge ports drops the packets from further MACs once the limit is reached



IOS Switch Commands

- switchport port-security
- switchport port-security maximum 1
- switchport port-security violation restrict
- switchport port-security aging time 2
- switchport port-security aging type inactivity
- switchport port-security mac-address sticky

Enable DHCP snooping, which allows the switch to accept a DHCP transaction directed from a trusted port



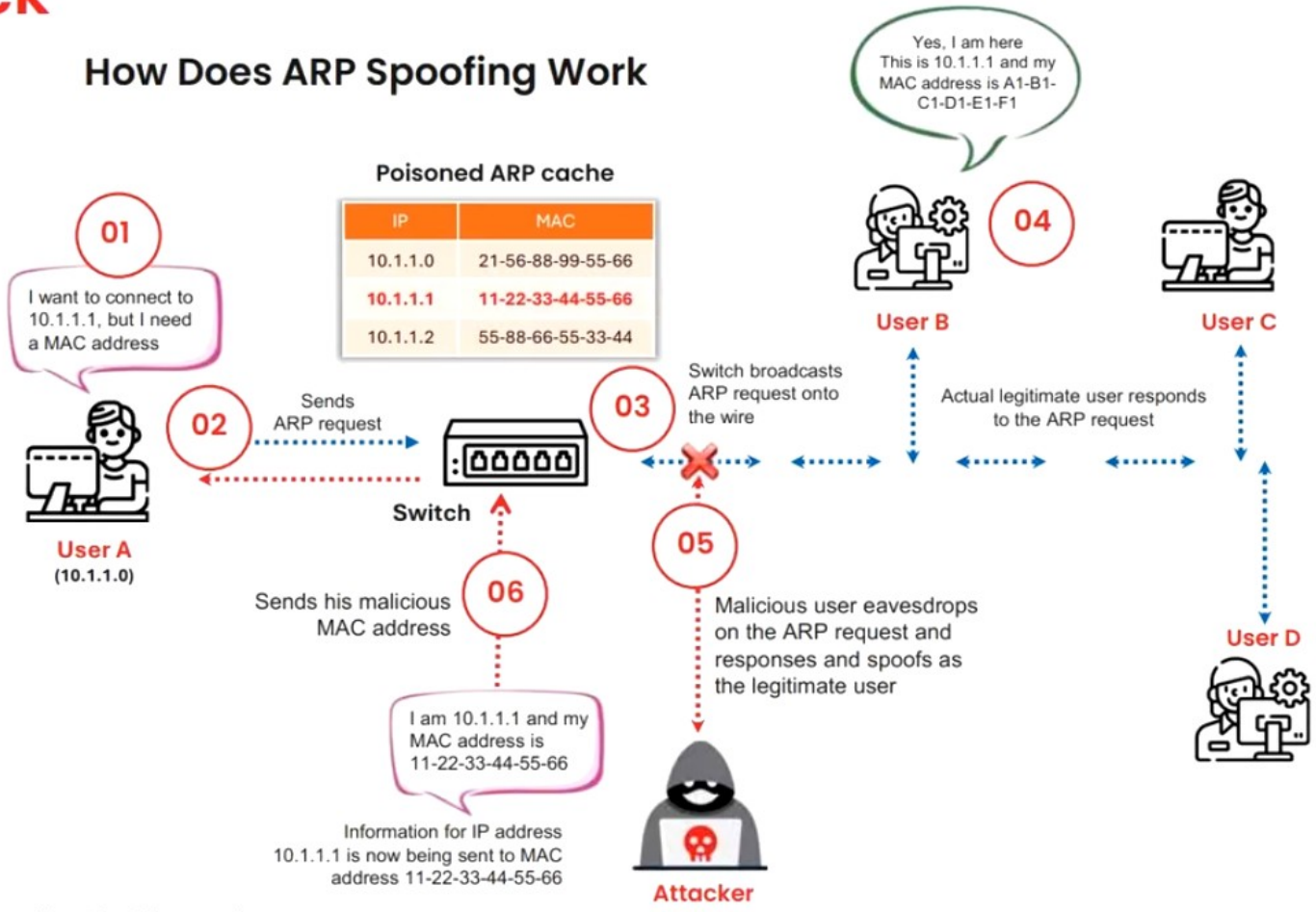
IOS Global Commands

- ip dhcp snooping → this turns on DHCP snooping
- ip dhcp snooping vlan 4,104 → this configures VLANs to snoop
- ip dhcp snooping trust → this configures interface as trusted

Note: All ports in the VLAN are not trusted by default

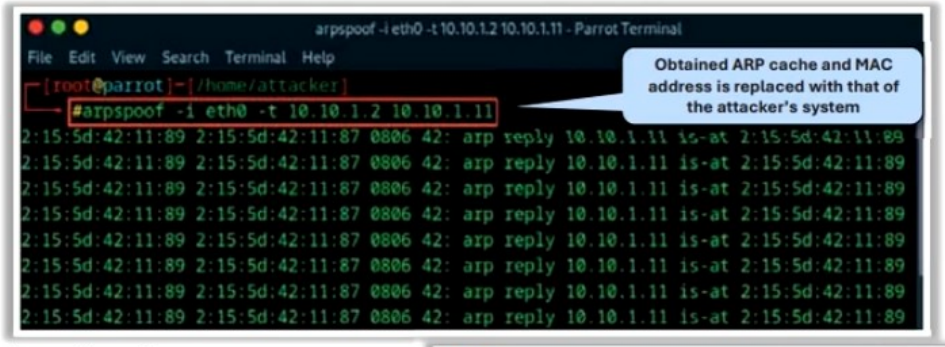
ARP Spoofing Attack

- Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine (MAC) addresses
- ARP spoofing involves constructing many forged ARP request and reply packets to overload the switch
- The switch is set in "forwarding mode" after the ARP table is flooded with spoofed ARP replies, and attackers can then sniff all the network packets
- Attackers flood a target computer's ARP cache with forged entries, which is also known as poisoning



ARP Spoofing/Poisoning Tools

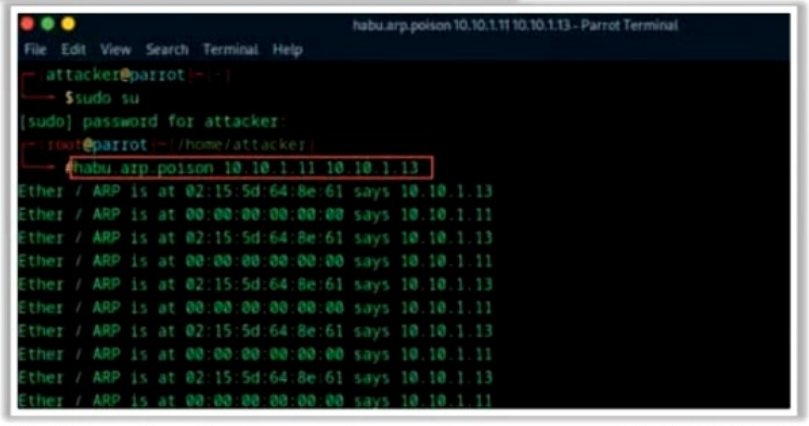
arpspoof arpspoof **redirects packets** from a target host (or all hosts) on the LAN that are intended for another host on the LAN by forging ARP replies



https://linux.die.net

Habu

Habu is a hacking toolkit that provides various commands to perform ARP poisoning, sniffing, DHCP starvation, etc.

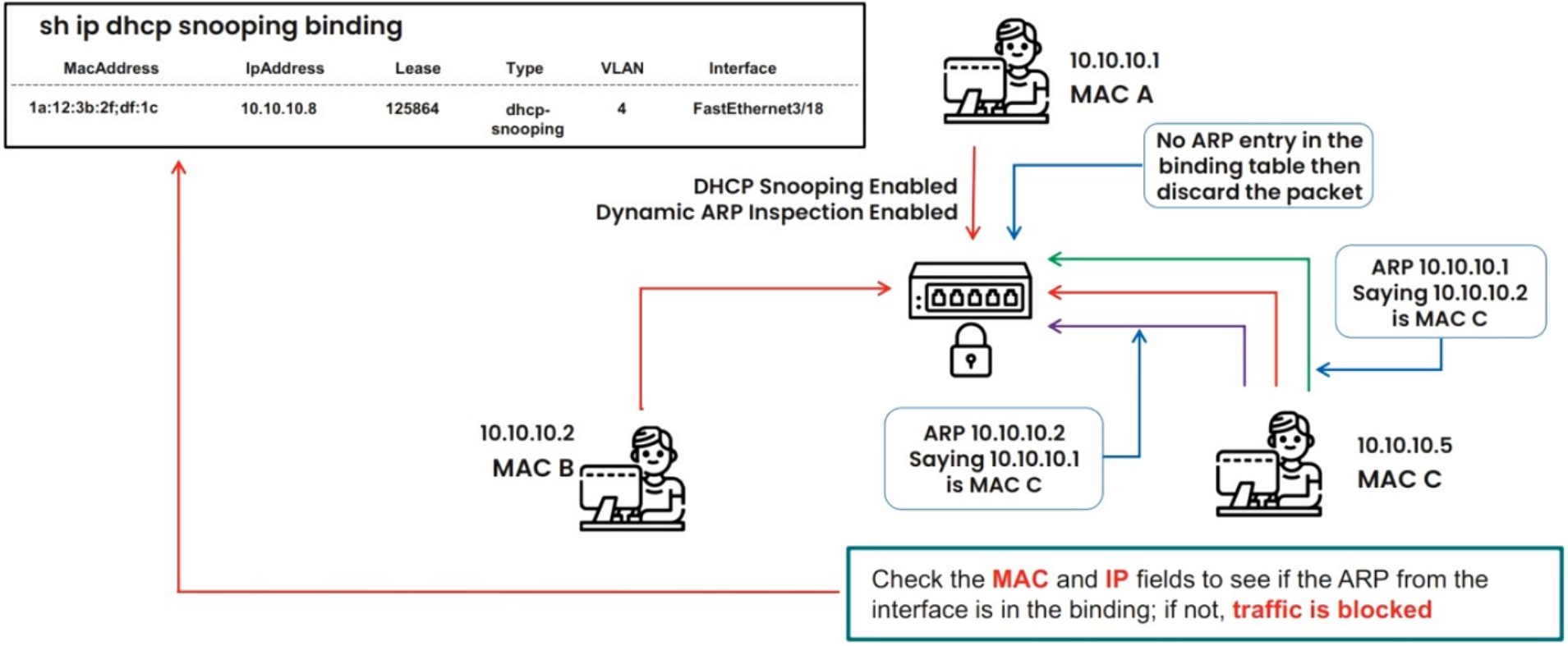


https://github.com

- **bettercap** *https://www.bettercap.org*
- **Ettercap** *https://www.ettercap-project.org*
- **RITM** *https://github.com*
- **ARP Spoofer** *https://github.com*
- **larp** *https://github.com*

How to Defend Against ARP Poisoning

Implement Dynamic ARP Inspection Using DHCP Snooping Binding Table



Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

01

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ^Z
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 10
DHCP snooping is operational on following VLANs: 10
DHCP snooping is configured on the following L3 Interfaces:
.....
DHCP snooping trust/rate is configured on the following Interfaces:

Interface          Trusted    Rate limit (pps)
---------------    -------    ----------------
```

02

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

MacAddress	IpAddress	Lease	Type	VLAN	Interface
1a:12:3b:2f;df:1c	10.10.10.8	125864	dhcp-snooping	4	FastEthernet0/3

Total number of bindings: 1

03

```
Switch(config)# ip arp inspection vlan 10
Switch(config)# ^Z
Switch# show ip arp inspection
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan  Configuration  Operation  ACL Match  Static ACL
 10    Enabled       Active
Vlan  ACL Logging  DHCP Logging  Probe Logging
 10    Deny          Arp           Off
Vlan  Forwarded  Dropped  DHCP Drops  ACL Drops
 10       0         0          0          0
Vlan  DHCP Permits  ACL Permits  Probe Permits  Source MAC Failures
 10         0           0            0                0
Vlan  Dest MAC Failures  IP Validation Failures  Invalid Protocol Data
 10          0                  0                      0
```

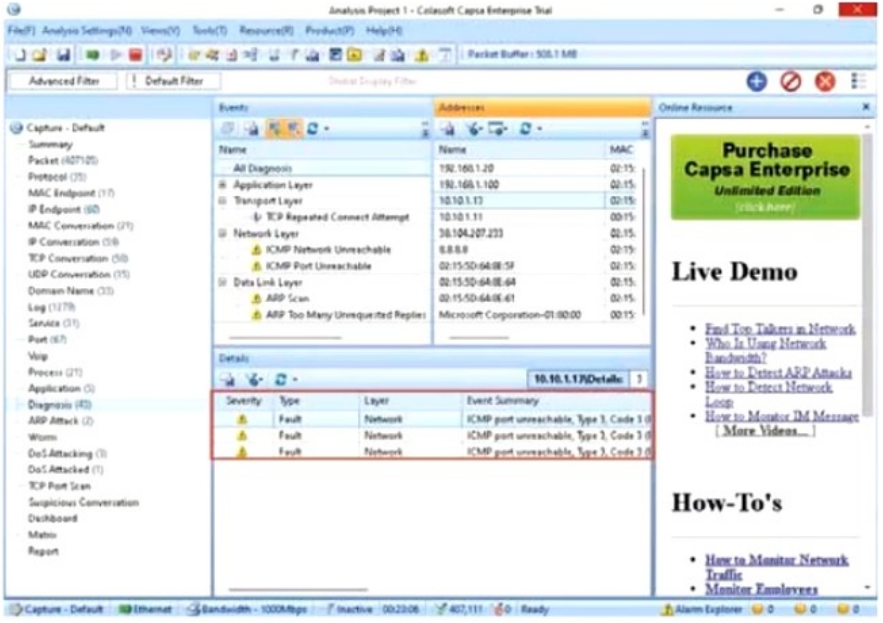
04

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/5,
vlan 10.([0013.6050.acf4/192.168.10.1/ffff.ffff.ffff/192.168.10.1/05:37:31
UTC Tue Apr 16 2024])
```

ARP Spoofing Detection Tools

Capsa Portable Network Analyzer

It helps security professionals in quickly detecting ARP poisoning and ARP flooding attacks and in locating the attack source



https://www.colasoft.com

Wireshark
https://www.wireshark.org

OpUtils
https://www.manageengine.com

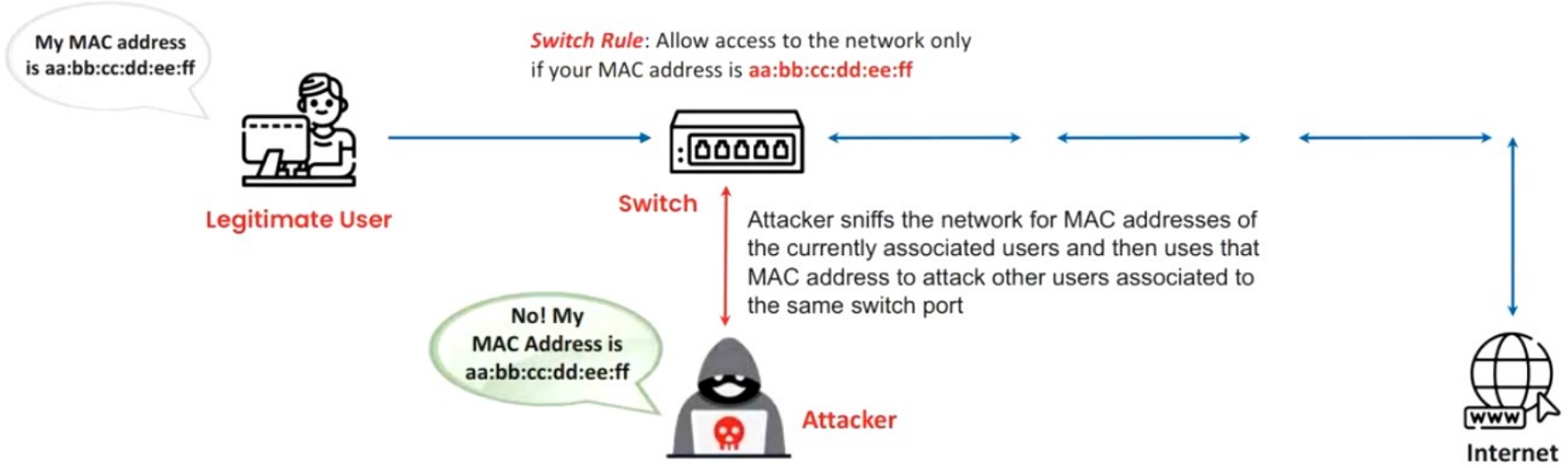
netspionage
https://github.com

NetProbe
https://github.com

ARP-GUARD
https://arp-guard.com

MAC Spoofing/Duplicating

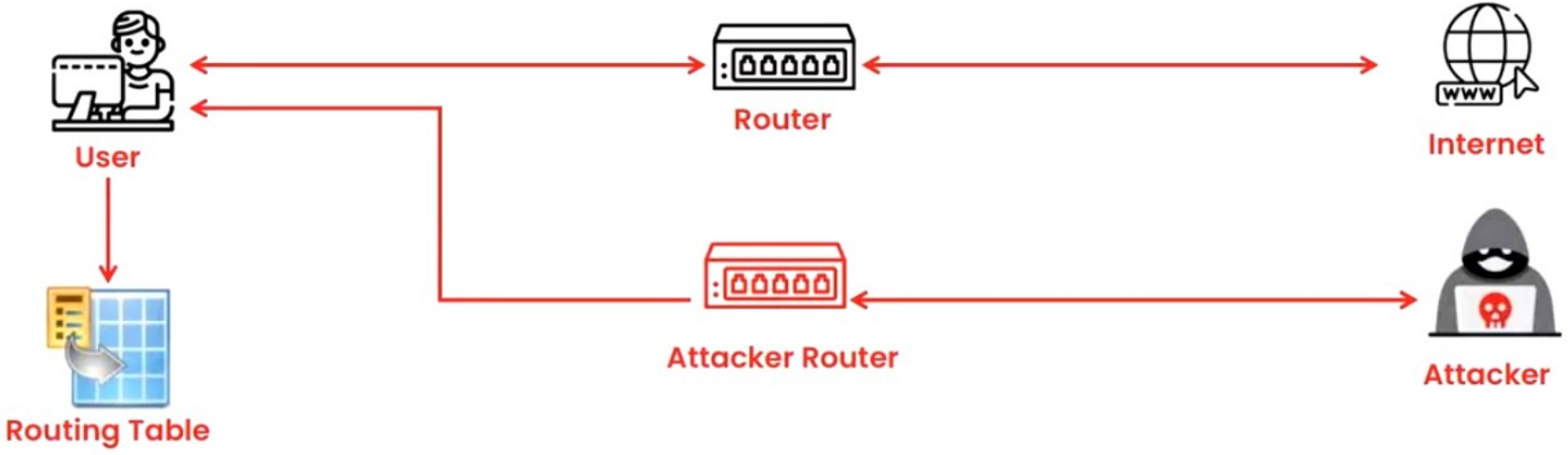
- A MAC duplicating attack is launched by sniffing a network for MAC addresses of clients who are actively associated with a switch port and re-using one of those addresses
- By listening to the traffic on the network, a malicious user can intercept and use a legitimate user's MAC address to receive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



Note: This technique can be used to bypass Wireless Access Points' MAC filtering

IRDP Spoofing

- ICMP Router Discovery Protocol (IRDP) is a routing protocol that allows a host to discover the IP addresses of active routers on their subnet by listening to router advertisement and soliciting messages on their network
- The attacker sends a spoofed IRDP router advertisement message to the host on the subnet, causing it to change its default router to whatever the attacker chooses
- This attack allows the attacker to sniff the traffic and collect valuable information from the packets
- Attackers can use IRDP spoofing to launch man-in-the-middle, denial-of-service, and passive sniffing attacks

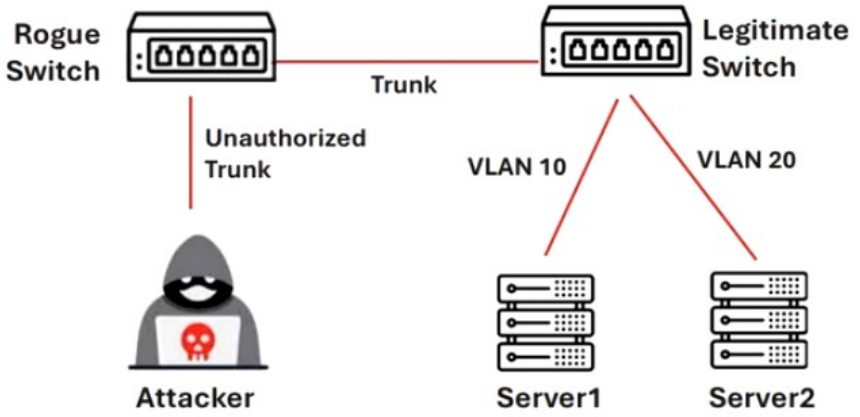


VLAN Hopping

- VLAN Hopping is a network attack method used to gain unauthorized access to resources on a virtual local area network (VLAN)
- This type of attack allows an attacker to bypass network segmentation controls, which are put in place to isolate network traffic for security and management reasons.

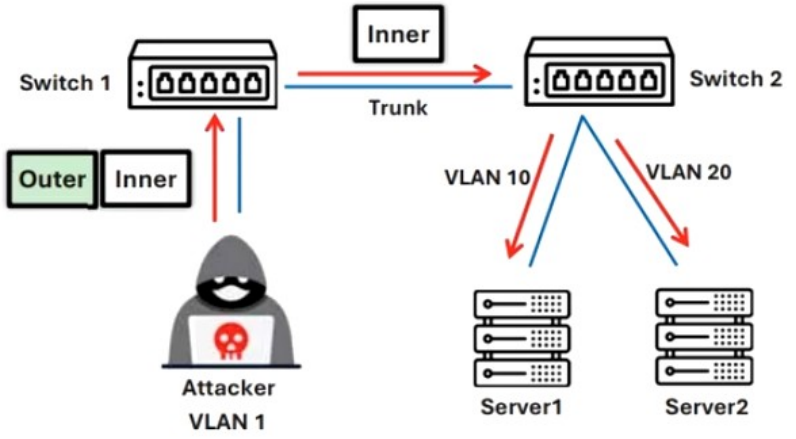
Switch Spoofing

Attackers connect a rogue switch onto the network by tricking a legitimate switch and thereby creating a trunk link between them



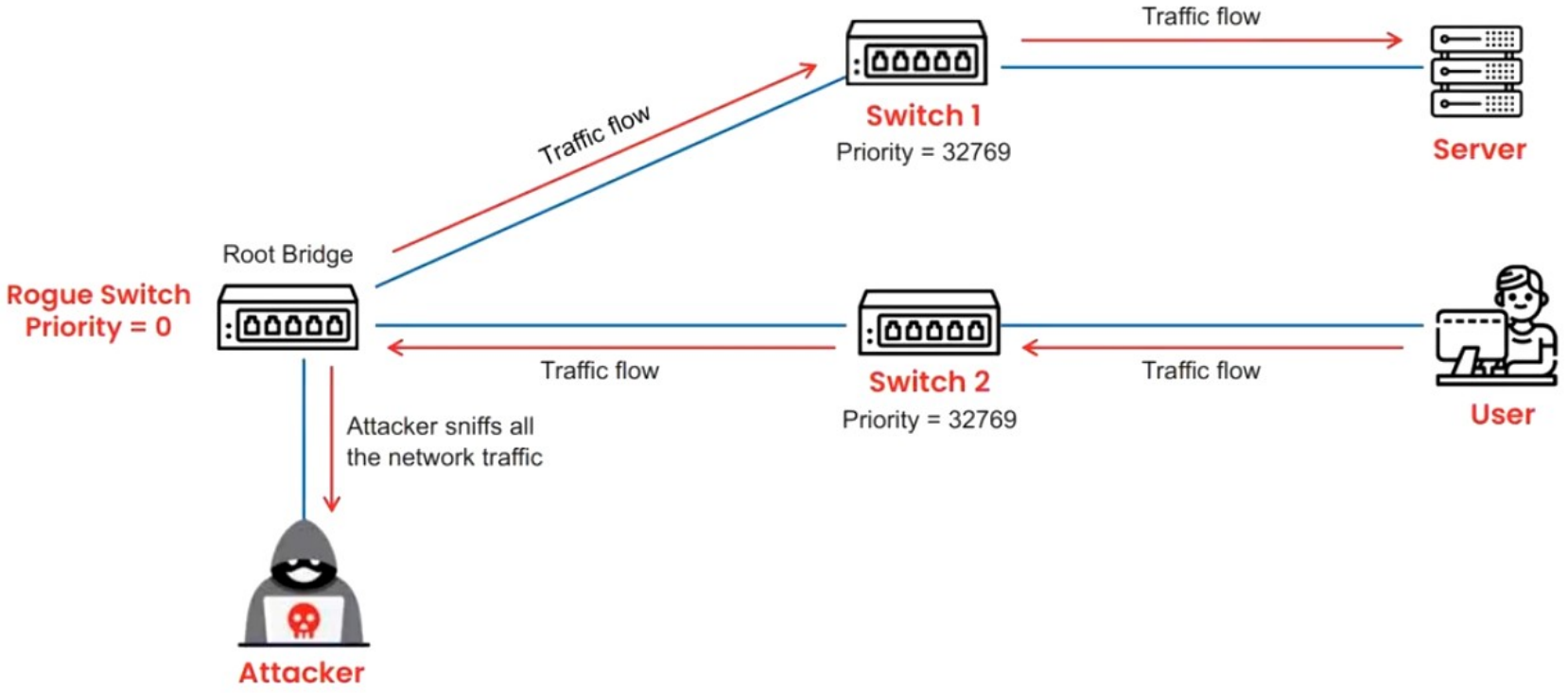
Double Tagging

Attackers add and modify tags in the Ethernet frame, thereby allowing the flow of traffic through any VLAN in the network



STP Attack

- Attackers connect a rogue switch into the network to change the operations of the STP protocol and sniff all the network traffic
- Attackers configure the rogue switch such that its priority is less than that of any other switch in the network, which makes it the root bridge, thus allowing the attackers to sniff all the traffic flowing in the network

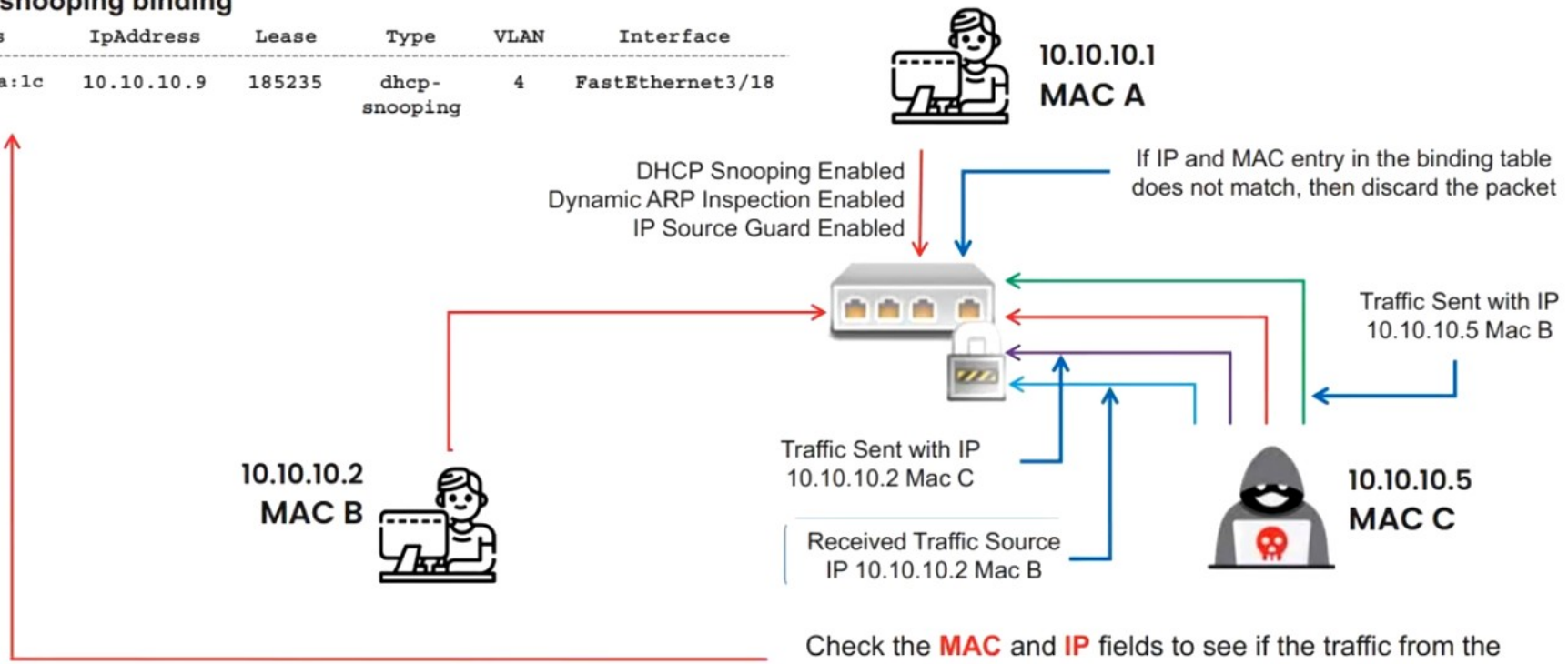


How to Defend Against MAC Spoofing

Use DHCP Snooping Binding Table, Dynamic ARP Inspection, and IP Source Guard

sh ip dhcp snooping binding

MacAddress	IpAddress	Lease	Type	VLAN	Interface
2a:33:4c:2f;4a:1c	10.10.10.9	185235	dhcp-snooping	4	FastEthernet3/18



Check the **MAC** and **IP** fields to see if the traffic from the interface is in the binding table; if not, then **traffic is blocked**

How to Defend Against VLAN Hopping

Defend against Switch Spoofing

- 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

Defend against Double Tagging

- Ensure to specify the default VLAN, which is used if the interface stops trunking:

  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

How to Defend Against STP Attacks

To prevent an STP attack, the following security features must be implemented:

BPDU Guard

To enable the BPDU guard on all PortFast edge ports:

- configure terminal
- interface gigabitethernet slot/port
- spanning-tree portfast bpduguard

Loop Guard

To enable the BPDU guard on all PortFast edge ports:

- configure terminal
- interface gigabitethernet slot/port
- spanning-tree portfast bpduguard

Root Guard

To enable the root guard feature on an interface:

- configure terminal
- interface gigabitethernet slot/port
- spanning-tree guard root

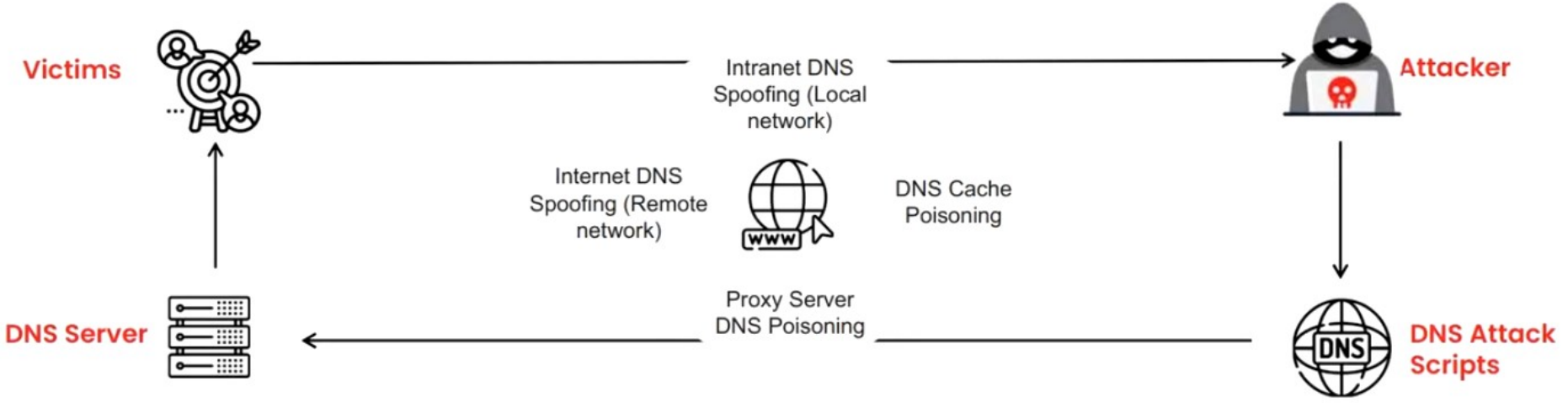
UDLD (Unidirectional Link Detection)

To enable UDLD on an interface:

- configure terminal
- interface gigabitethernet slot/port
- udld { enable | disable | aggressive }

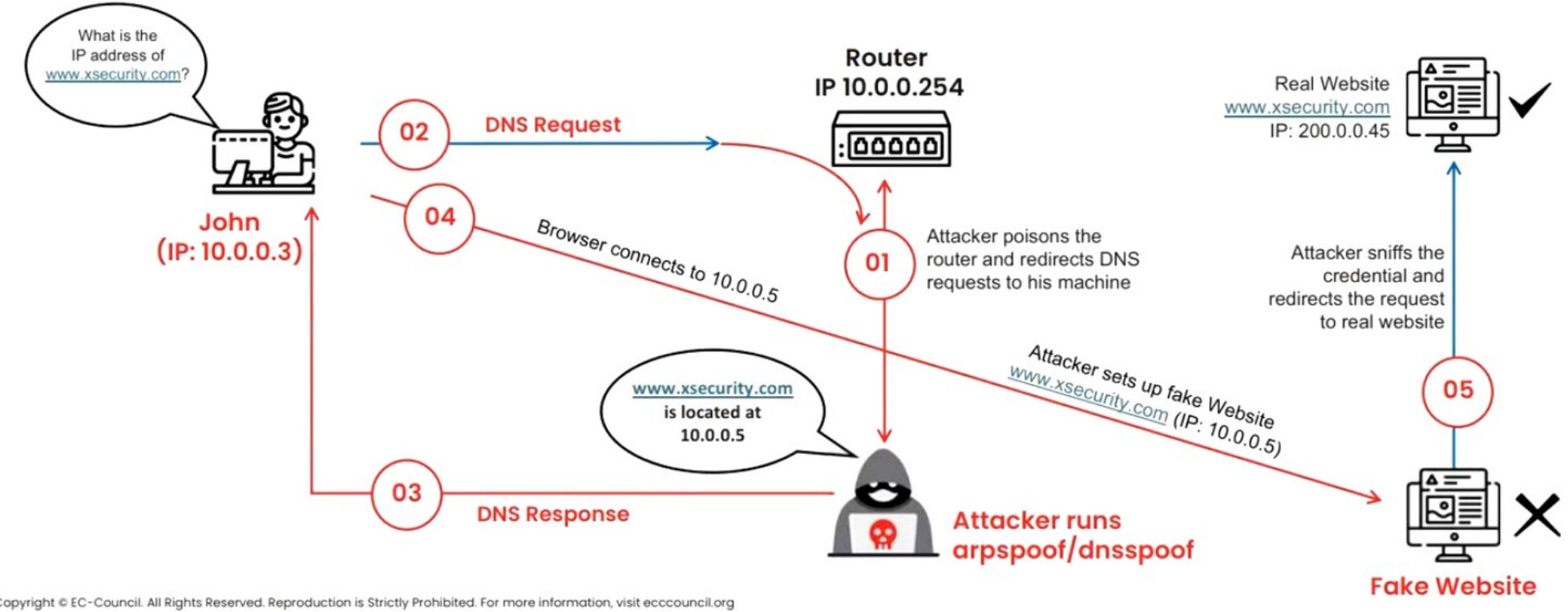
DNS Poisoning Techniques

- DNS poisoning is a technique that tricks a DNS server into believing that it has received authentic information when it has not received any
- It results in the substitution of a false IP address at the DNS level where the web addresses are converted into numeric IP addresses
- It allows the attacker to replace IP address entries for a target site on a given DNS server with the IP address of the server he/she controls
- Attackers use DNS poisoning tools such as DerpNSpoof to create fake DNS entries for the server (containing malicious content) with names similar to that of the target server



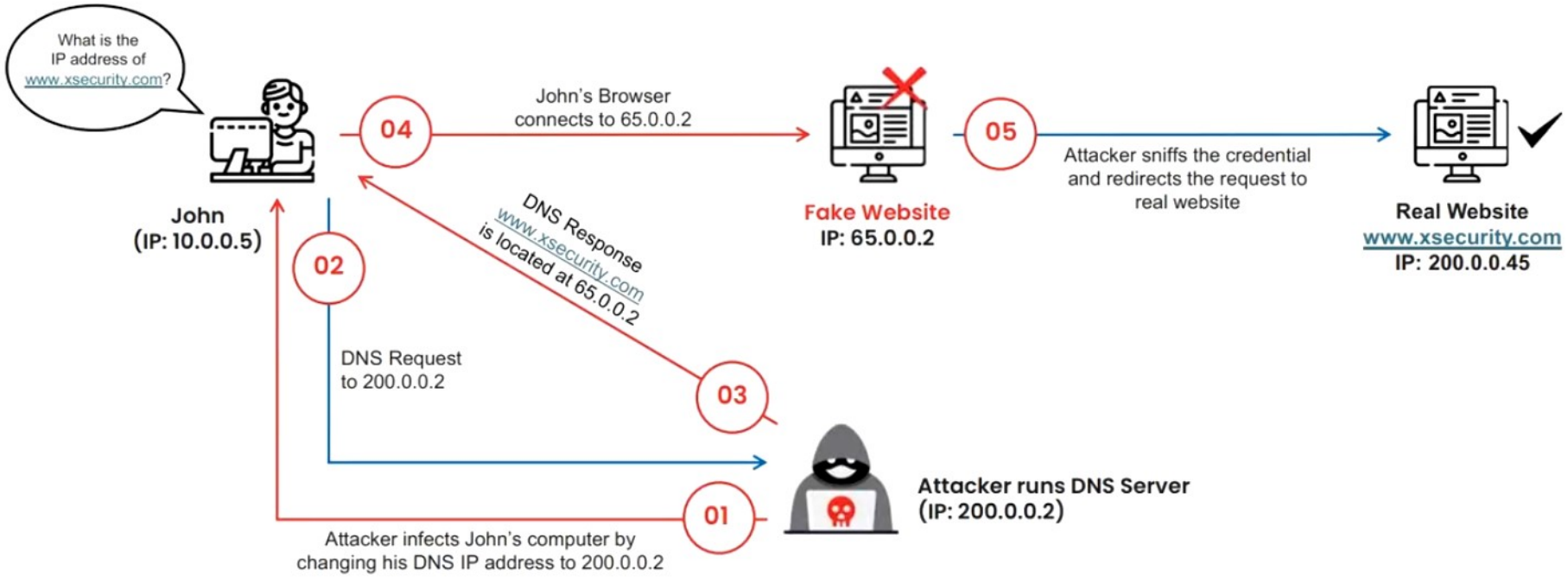
Intranet DNS Spoofing

- In this technique, the attacker's system must be connected to the local area network (LAN) and be able to sniff packets
- It works well against switches with ARP Poison Routing



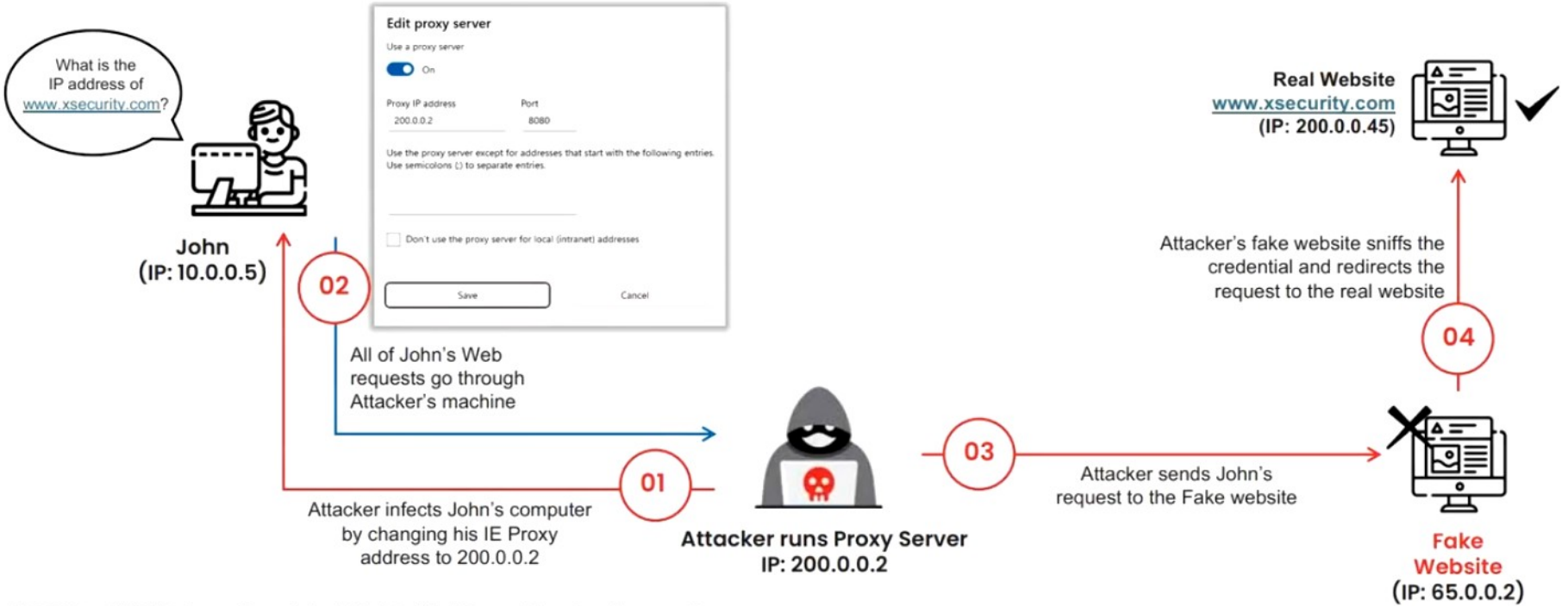
Internet DNS Spoofing

Internet DNS Spoofing, the attacker infects John's machine with a Trojan and changes his DNS IP address to that of the attacker's



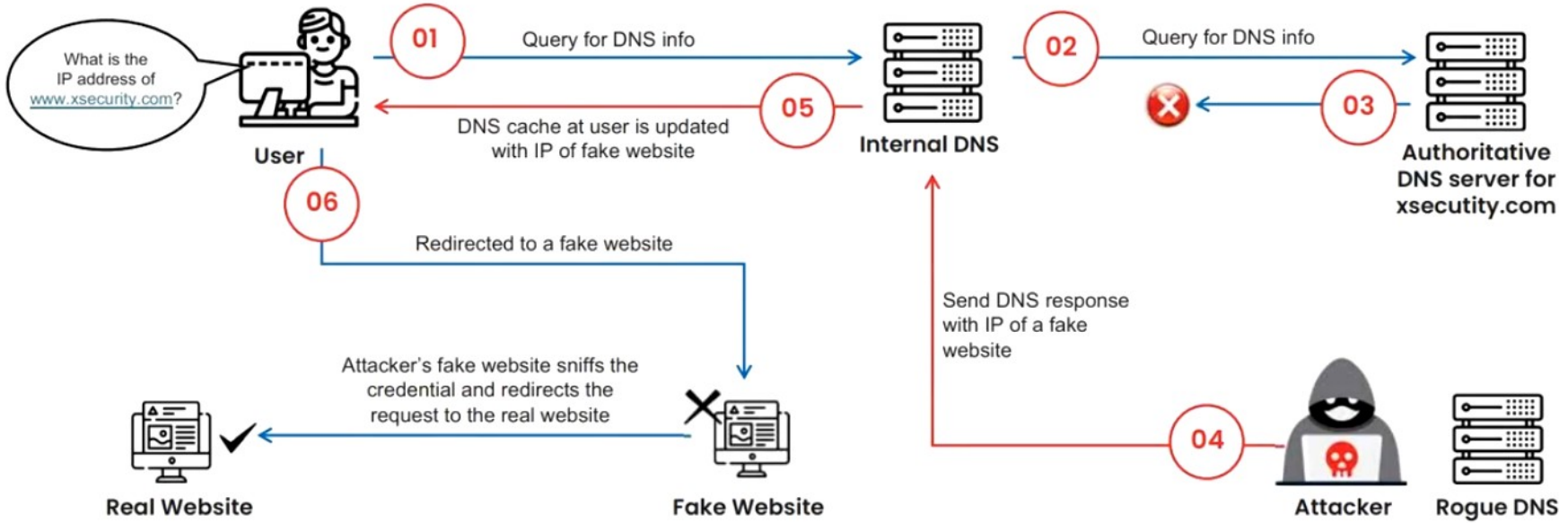
Proxy Server DNS Poisoning

The attacker sends a Trojan to John's machine that changes his proxy server settings in Internet Explorer to that of the attacker's and redirects to the fake website



DNS Cache 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 a similar request



How to Defend Against DNS Spoofing

01 Implement a Domain Name System Security Extension (DNSSEC)

02 Use a Secure Socket Layer (SSL) for securing the traffic

03 Resolve all DNS queries to a local DNS server

04 Block DNS requests to external servers

05 Configure a firewall to restrict external DNS lookup

06 Implement an intrusion detection system (IDS) and deploy it correctly

07 Configure the DNS resolver to use a new random source port for each outgoing query

08 Restrict the DNS recusing service, full or partial, to authorized users

09 Use DNS Non-Existent Domain (NXDOMAIN) rate limiting

10 Secure internal machines

11 Use a static ARP and IP tables

12 Use Secure Shell (SSH) encryption

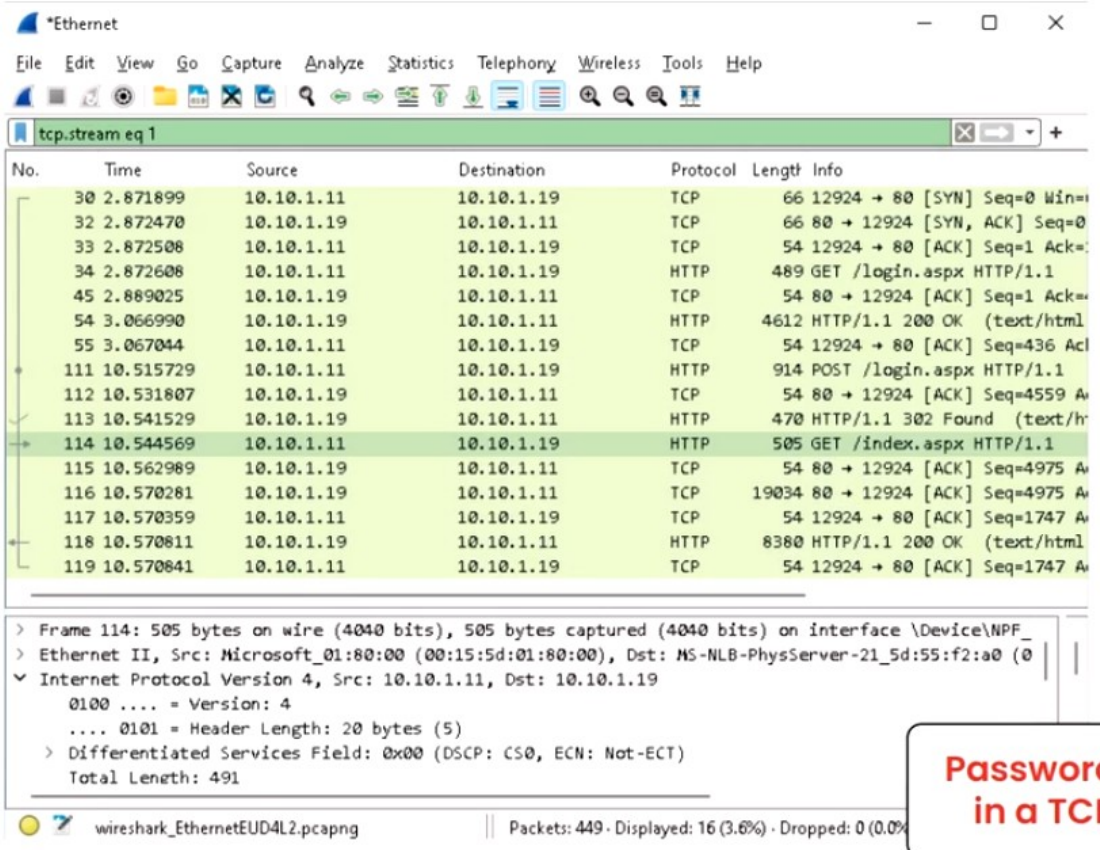
13 Do not allow outgoing traffic to use UDP port 53 as a default source port

14 Audit the DNS server regularly to remove vulnerabilities

Objective 03

Use Sniffing Tools

Sniffing Tool: Wireshark (Follow TCP Stream)



Password revealed in a TCP Stream

Display Filters in Wireshark

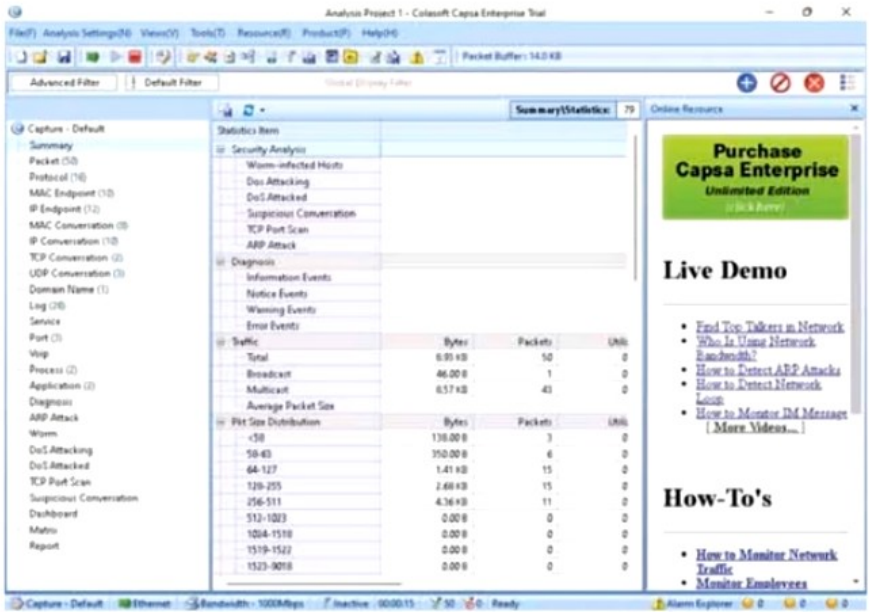
Display filters are used to change the view of packets in the captured files

01	Display Filtering by Protocol	Example: Type the protocol in the filter box; arp, http, tcp, udp, dns, or ip
02	Monitoring the Specific Ports	• tcp.port==23 • ip.addr==192.168.1.100 machine ip.addr==192.168.1.100 && tcp.port==23
03	Filtering by Multiple IP Addresses	ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5
04	Filtering by IP Address	ip.addr == 10.0.0.4
05	Other Filters	• ip.dst == 10.0.1.50 && frame.pkt_len > 400 • ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30 • ip.src==205.153.63.30 or ip.dst==205.153.63.30

Sniffing Tools

Capsa Portable Network Analyzer

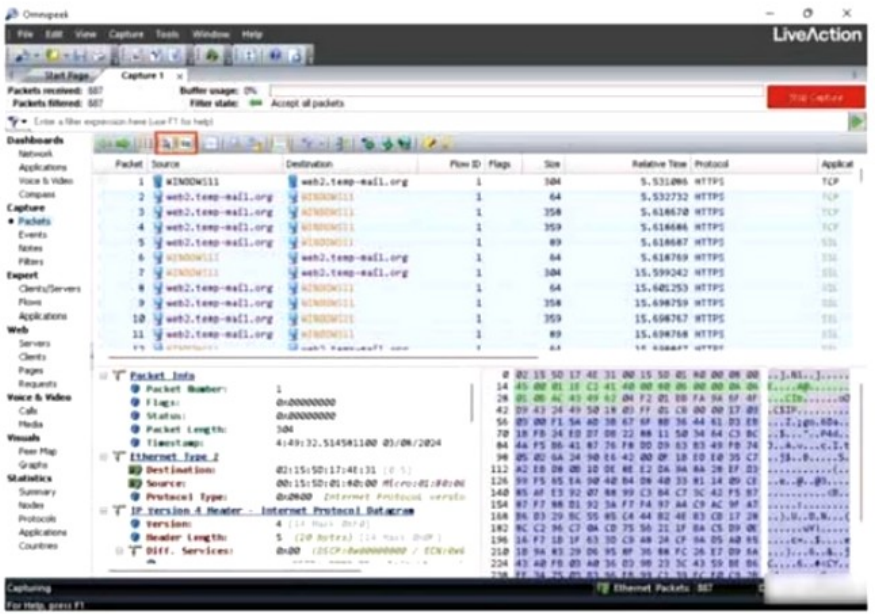
Capsa, a portable network performance analysis and diagnostics tool, provides packet capture and analysis capabilities with an easy-to-use interface



https://www.colasoft.com

OmniPeek

OmniPeek sniffer displays a Google Map in the OmniPeek capture window showing the locations of all the public IP addresses of captured packets



https://www.liveaction.com

Other Tools:

- **RITA (Real Intelligence Threat Analytics)** — *https://github.com*
- **Observer Analyzer** — *https://www.viavisolutions.com*
- **PRTG Network Monitor** — *https://www.paessler.com*
- **Network Performance Monitor** — *https://www.solarwinds.com*

Objective 04

Explain Sniffing Countermeasures

How to Defend Against Sniffing

01 Restrict physical access to the network media to ensure that a packet sniffer cannot be installed

02 Use end-to-end encryption to protect confidential information

03 Permanently add the MAC address of the gateway to the ARP cache

04 Use static IP addresses and ARP tables to prevent attackers from adding spoofed ARP entries for machines in the network

05 Turn off network identification broadcasts, and if possible, restrict the network to authorized users to protect the network from being discovered with sniffing tools

06 Use IPv6 instead of IPv4 protocol

07 Use encrypted sessions, such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, and SSL for email connections, to protect wireless network users against sniffing attacks

How to Defend Against Sniffing (Cont'd)

08 Use HTTPS instead of HTTP to protect usernames and passwords

09 Use a switch instead of a hub as a switch delivers data to the intended recipient only

10 Use Secure File Transfer Protocol (SFTP), instead of FTP for the secure transfer of files

11 Use PGP and S/MIME, VPN, IPsec, SSL/TLS, Secure Shell (SSH), and One-time passwords (OTPs)

12 Always encrypt wireless traffic with a strong encryption protocol such as WPA2 and WPA3

13 Retrieve the MAC directly from the NIC instead of the OS; this prevents MAC address spoofing

14 Use tools to determine if any NICs are running in the promiscuous mode

15 Use access-control lists (ACLs) to allow access only to a fixed range of trusted IP addresses in a network

How to Detect Sniffing

Check the Devices Running in Promiscuous Mode

- You need to check which machines are running in the promiscuous mode
- Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety

Run IDS

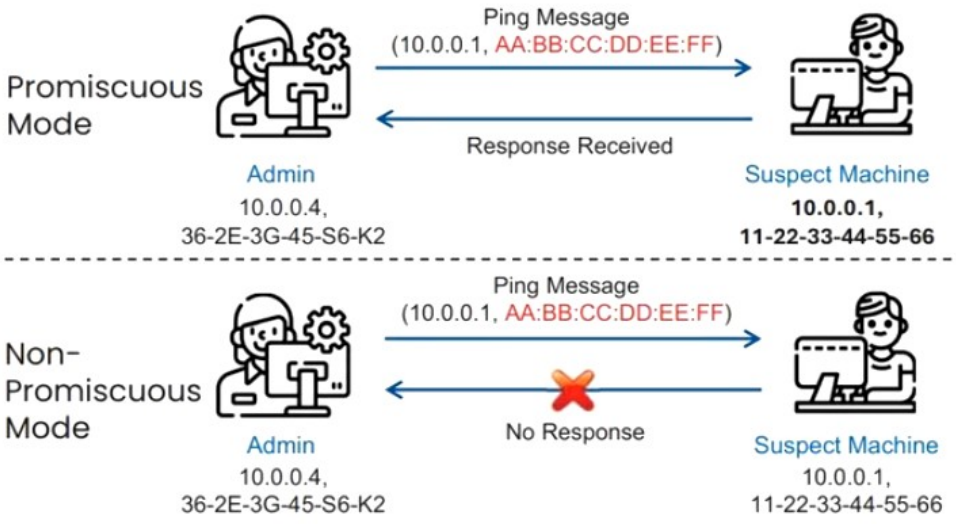
- Run IDS and see if the MAC address of any of the machines has changed (Example: router's MAC address)
- IDS can alert the administrator about suspicious activities

Run Network Tools

- Run network tools such as Capsa Portable Network Analyzer to monitor the network for detecting strange packets
- Enables you to collect, consolidate, centralize, and analyze traffic data across different network resources and technologies

Sniffer Detection Techniques: Ping Method and DNS Method

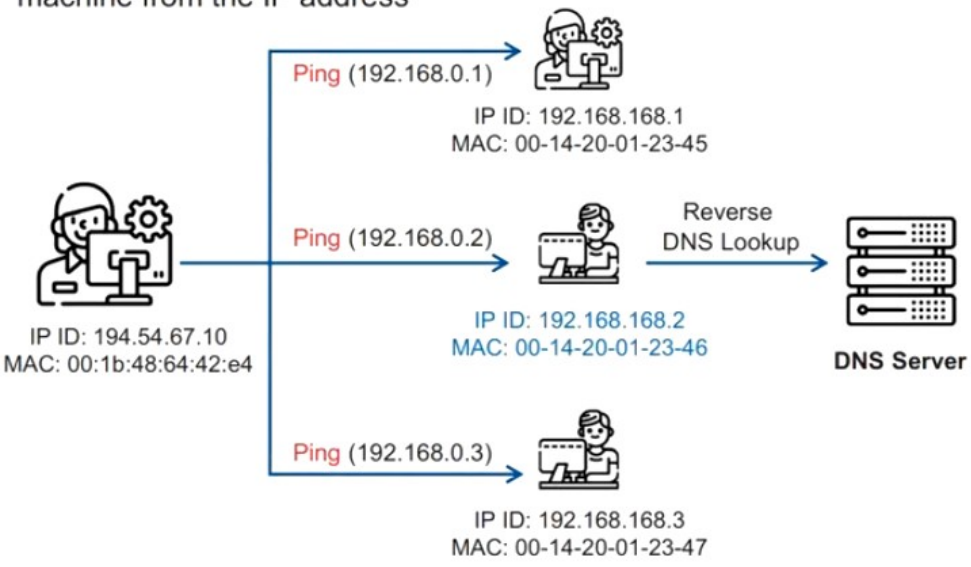
Ping Method



Sends a ping request to the suspect machine with its IP address and an **incorrect MAC address**. The Ethernet adapter rejects it, as 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

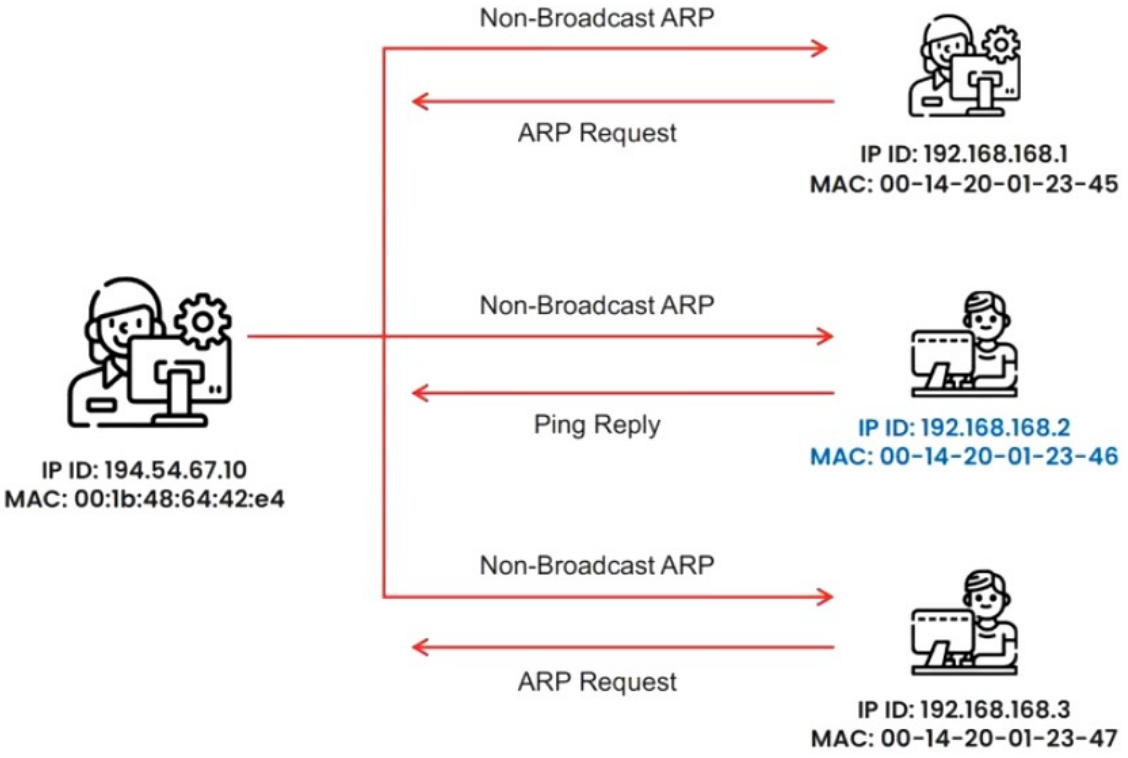
Most of the sniffers perform **reverse DNS lookups** to identify the machine from the IP address



A machine generating **reverse DNS lookup traffic** is very likely to be running a sniffer

Sniffer Detection Techniques: ARP Method

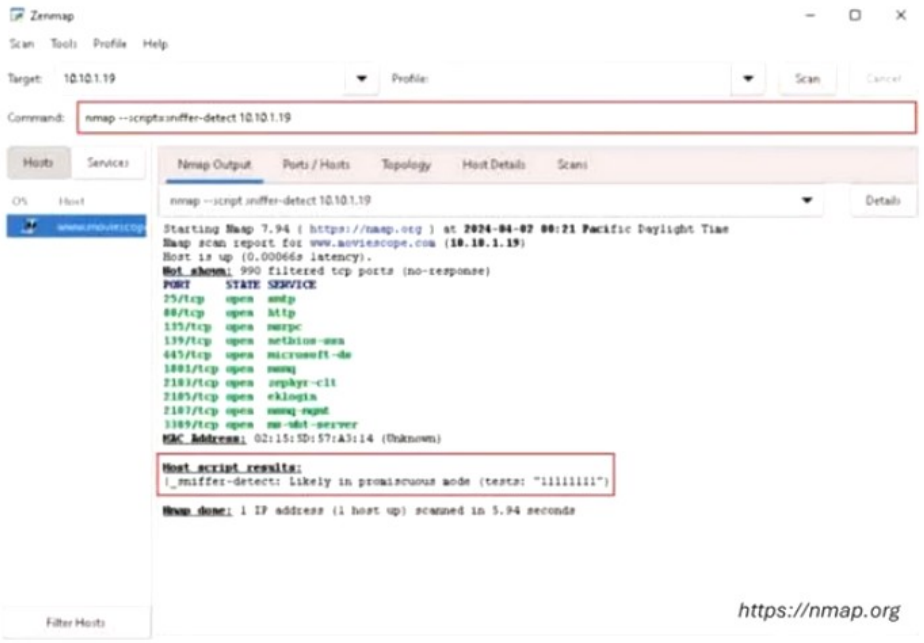
- Only the machine in the promiscuous mode (machine C) caches the ARP information (IP and MAC address mapping)
- A machine in the promiscuous mode responds to the ping message as it has the correct information about the host sending the ping requests in its cache; the rest of the machines will send an ARP probe to identify the source of the ping request



Promiscuous Detection Tools

Nmap

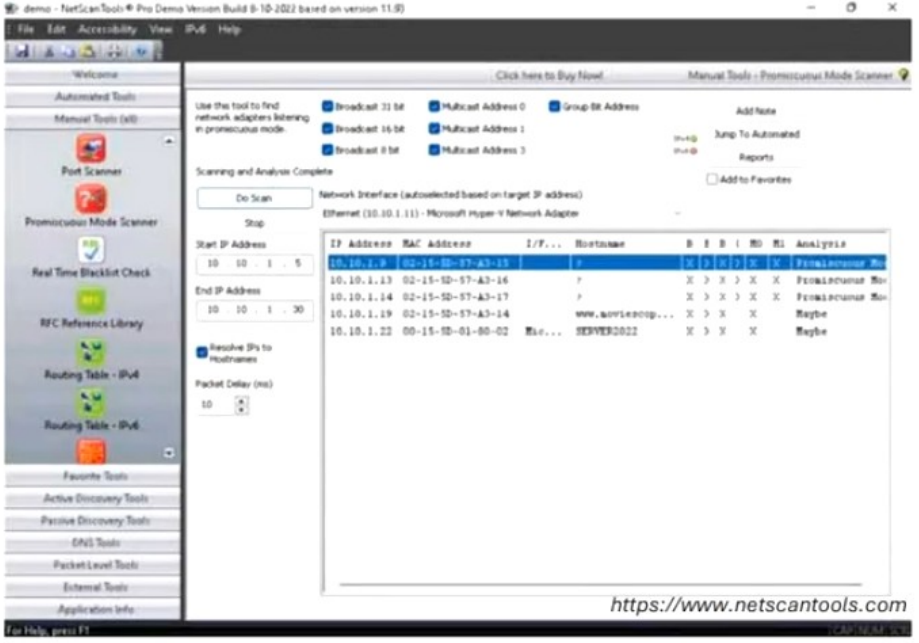
- Nmap's NSE script allows you to check if a system on a local Ethernet has its network card in the promiscuous mode
- Command to detect NIC in promiscuous mode:
  nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]



https://nmap.org

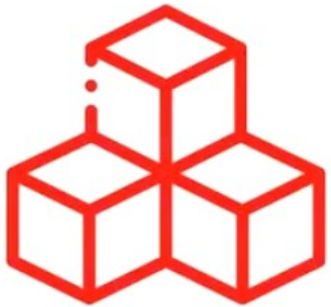
NetScanTools Pro

NetScanTools Pro includes a Promiscuous Mode Scanner tool to scan your subnet for network interfaces listening for all ethernet packets in the promiscuous mode



https://www.netscantools.com

Module Summary



- In this module, we have discussed the following:
  - Sniffing concepts along with sniffing in the data link layer of the OSI Model
  - Various sniffing techniques such as MAC attacks, DHCP attacks, ARP poisoning, spoofing attacks, DNS poisoning, etc. along with their countermeasures
  - Various sniffing tools
  - Various countermeasures that are to be employed in order to prevent sniffing attacks
  - The module concluded with a detailed discussion on various sniffing detection techniques
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform social engineering to steal critical information related to the target organization