
SNIFFING

Module Objectives

- Overview of Sniffing Concepts
- Understanding Various Sniffing Techniques
- Understanding How to Defend Against Various Sniffing Techniques
- Overview of Various Sniffing Tools
- Understanding Different Sniffing Countermeasures
- Understanding Different Techniques and Tools to Detect Sniffing

Module Flow

1. Sniffing Concepts
2. Sniffing Techniques
3. Sniffing Tools
4. Countermeasures
5. Sniffing Detection Techniques

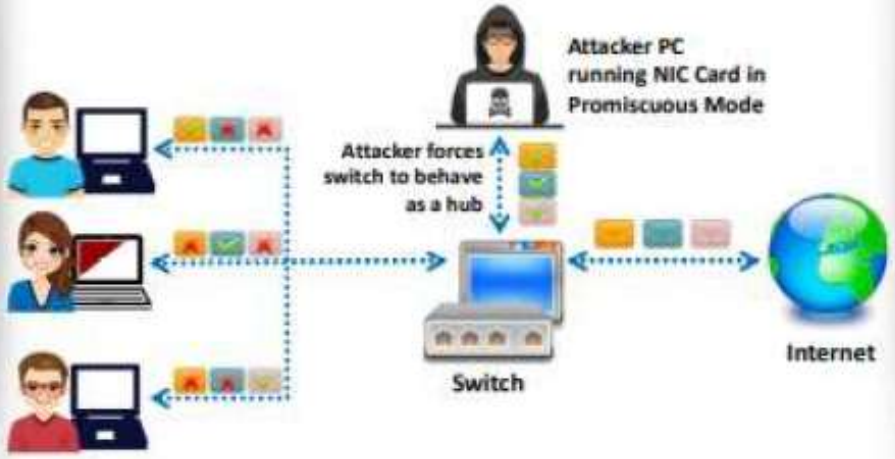
Network Sniffing

Packet Sniffing

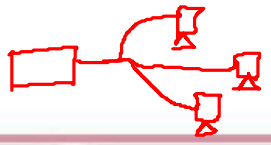
- Packet sniffing is the process of **monitoring and capturing all data packets** passing through a given network using a software application or hardware device
- It allows an attacker to observe and **access the entire network traffic** from a given point
- Packet sniffing allows an attacker to **gather 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- Hub usage is an outdated approach.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

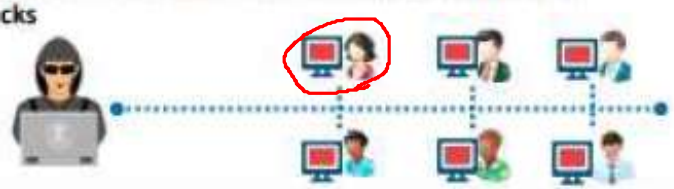
- **MAC Flooding**
- **DHCP Attacks**
- **DNS Poisoning**
- **Switch Port Stealing**
- **ARP Poisoning**
- **Spoofing Attack**

How an Attacker Hacks the Network Using Sniffers

1. An attacker connects his desktop/laptop to a switch port

2. He/she runs discovery tools to learn about network topology

3. He/she identifies a victim's machine to target his/her attacks



4. He/she poisons the victim's machine by using ARP spoofing techniques

5. The traffic destined for the victim's machine is redirected to the attacker

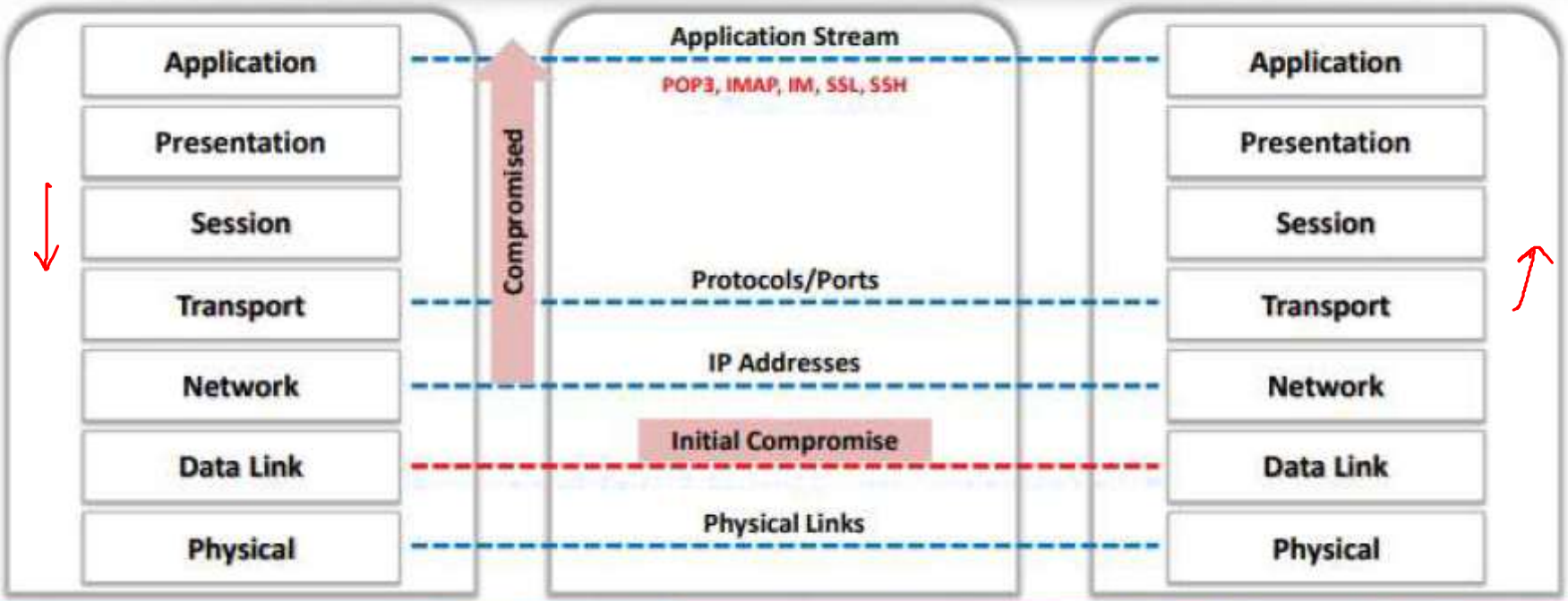
6. The hacker extracts passwords and sensitive data from the redirected traffic

Protocols Vulnerable to Sniffing

Telnet and Rlogin	Keystrokes including usernames and passwords are sent in clear text
IMAP	Passwords and data are sent in clear text
HTTP	Data is sent in clear text
SMTP and NNTP	Passwords and data are sent in clear text
POP	Passwords and data are sent in clear text
FTP	Passwords and data are sent in clear text

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



Hardware Protocol Analyzers

1. A hardware protocol analyzer is a piece of equipment that **captures signals** without altering the traffic in a cable segment
2. It can be used to monitor network usage and identify **malicious network traffic** generated by hacking software installed in the network
3. It captures a data packet, decodes it, and analyzes its content based on certain **predetermined rules**
4. It allows the attacker to see individual **data bytes** of each packet passing through the cable

Voyager M4x Protocol Analyzer

https://teledynelecroy.com

N2X N5540A Agilent Protocol Analyzer

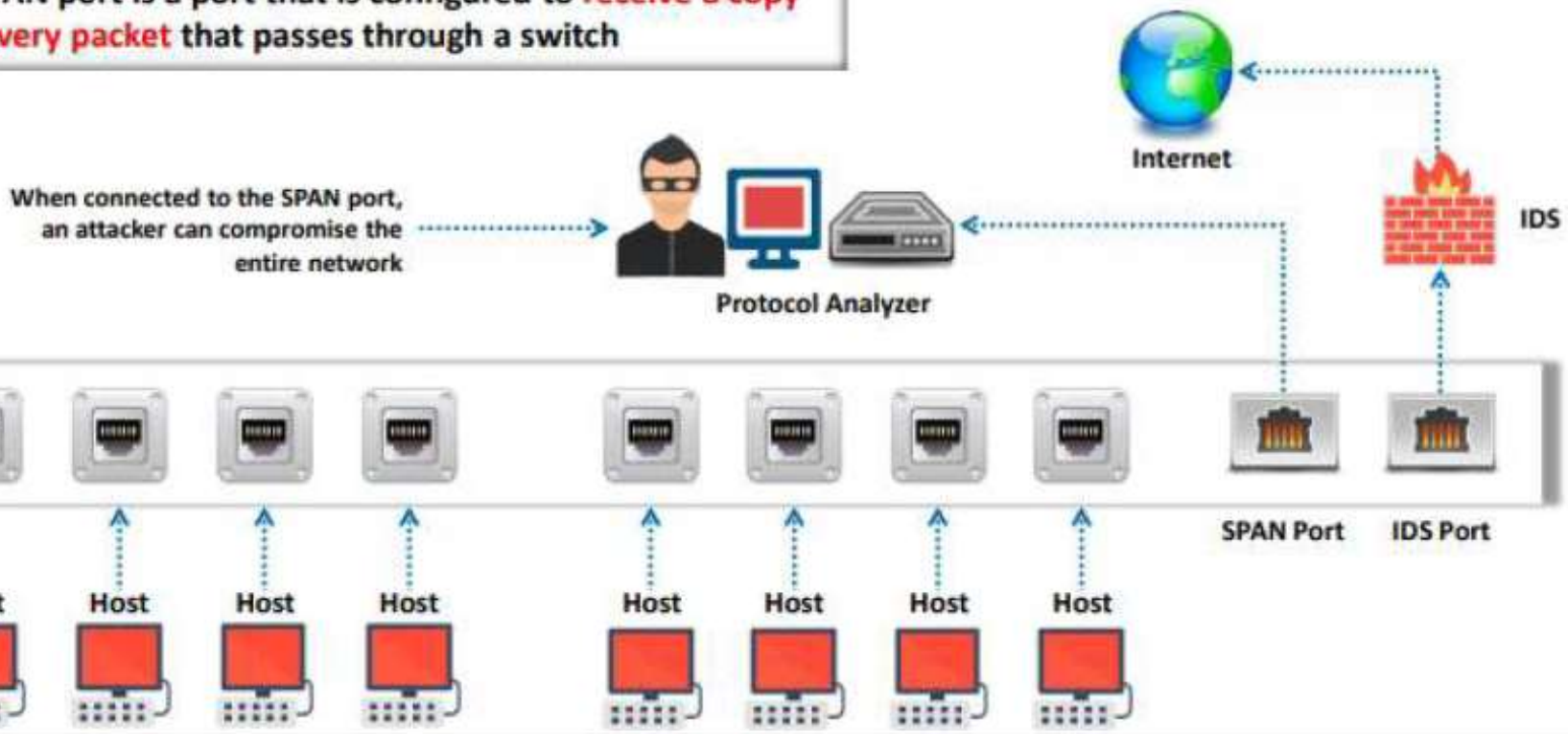
https://www.valuetronics.com

Hardware Protocol Analyzers

- Keysight E2960B (*https://www.keysight.com*)
- STINGA Protocol Analyzer (*https://utelsystems.com*)
- NETSCOUT's OneTouch AT Network Assistant (*https://enterprise.netscout.com*)
- NETSCOUT's OptiView XG Network Analysis Tablet (*https://enterprise.netscout.com*)
- Agilent (Keysight) Technologies 8753ES (*https://www.microlease.com*)

SPAN Port

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



Wiretapping

1. Wiretapping is the process of the monitoring of **telephone** and **Internet** conversations by a third party
2. Attackers **connect a listening device** (hardware, software, or a combination of both) to the circuit carrying information between two phones or hosts on the Internet
3. It allows an attacker to **monitor**, **intercept**, **access**, and **record information** contained in a data flow in a communication system

Types of Wiretapping

Active Wiretapping

- **It monitors, records, alters, and also injects data into the communication or traffic**

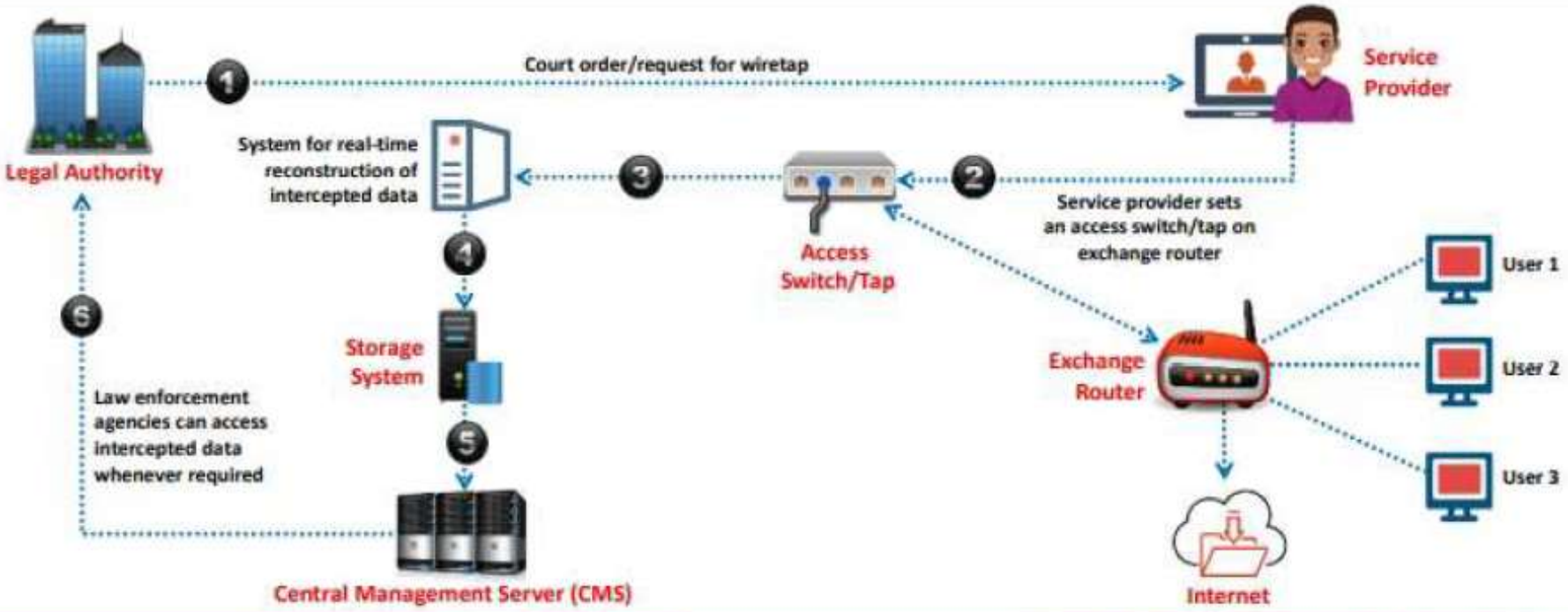
Passive Wiretapping

- **It only monitors and records the traffic and collects knowledge regarding the data it contains**

Note: Wiretapping without a warrant or the consent of the concerned person is a criminal offense in most countries

Lawful Interception

- Lawful interception refers to legally **intercepting data communication** between two end points for surveillance on the traditional telecommunications, Voice over Internet Protocol (VoIP), data, and multiservice networks



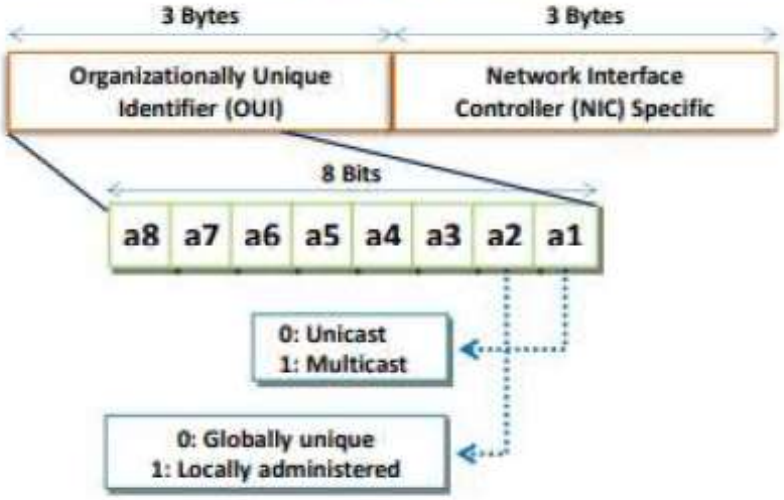
Module Flow

1. Sniffing Concepts
2. Sniffing Techniques
3. Sniffing Tools
4. Countermeasures
5. Sniffing Detection 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

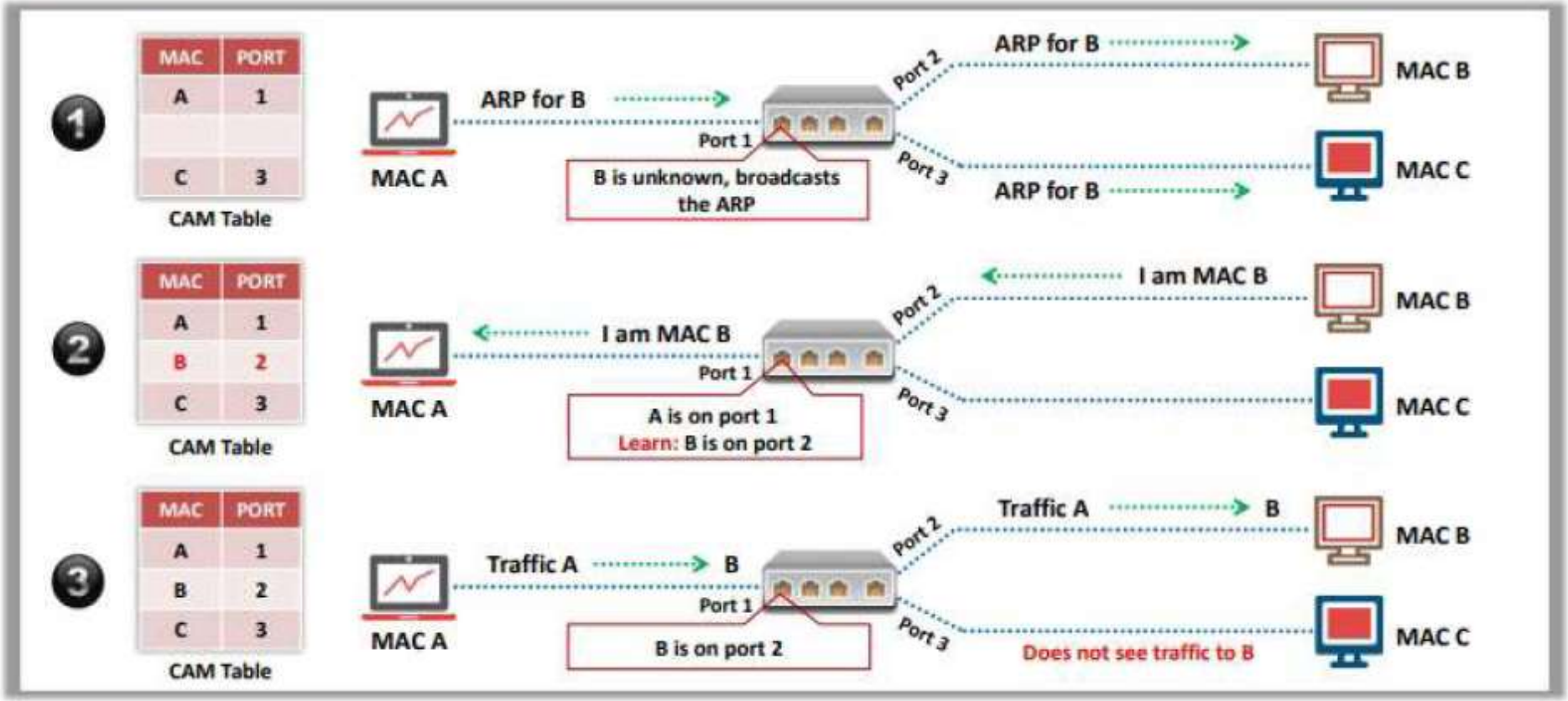
MAC Address



CAM Table

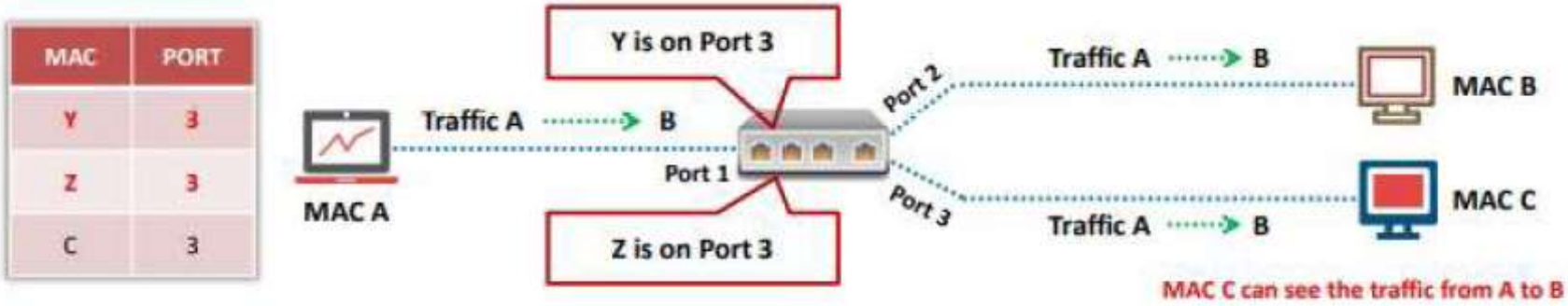
vlan	MAC Add	Type	Learn	Age	Ports
255	00d3.ad34.123g	Dynamic	Yes	0	Gi5/2
5	as23.df45.45t6	Dynamic	Yes	0	Gi2/5
5	er23.23er.t5e3	Dynamic	Yes	0	Gi1/6

How CAM Works



What Happens When a CAM Table Is Full?

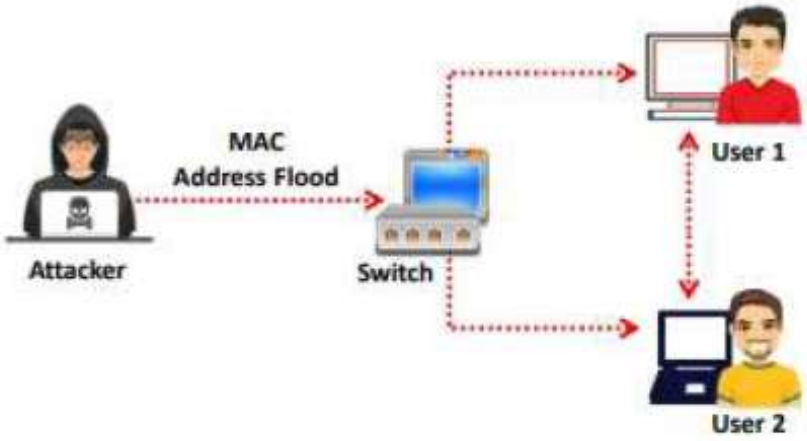
- Once the CAM table fills up on a switch, additional ARP request **traffic floods every port on the switch**
- This will **change the behavior of the switch** to reset to its learning mode, broadcasting on every port like a hub
- This attack will also **fill the CAM tables of adjacent switches**



MAC Flooding

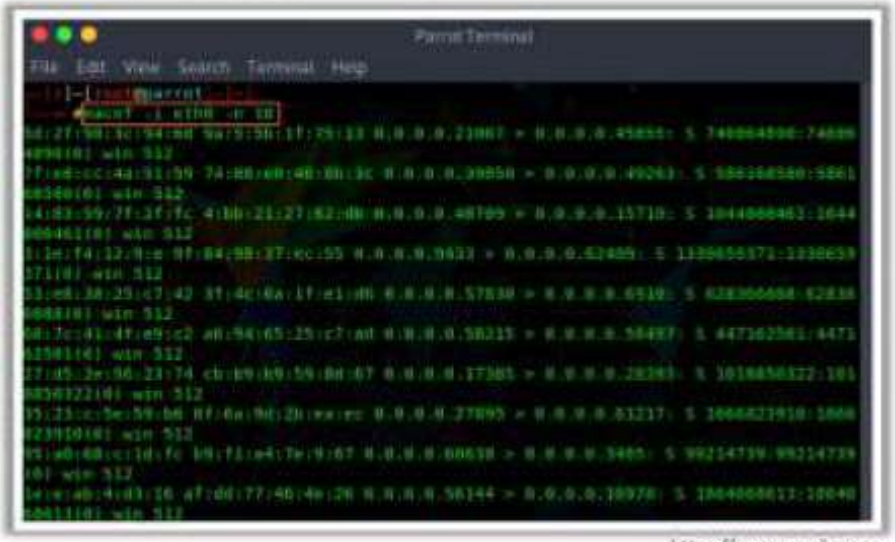
macof -i eth0 -n 10

- 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

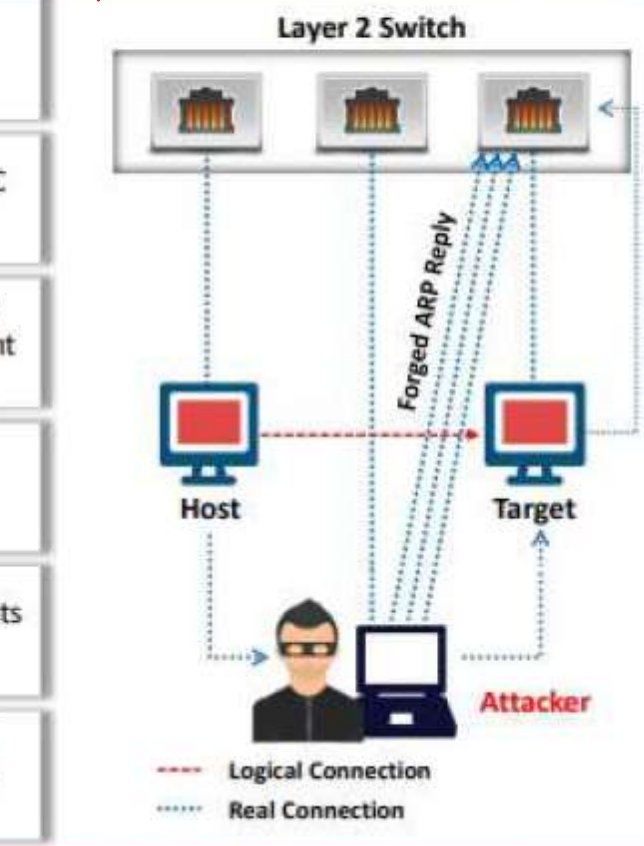
- **macof** is a Unix/Linux tool that is a part of the dsniff collection
- macof sends random **source MAC** and **IP addresses**
- This tool **floods the switch's CAM tables** (131,000 per min) by sending bogus MAC entries



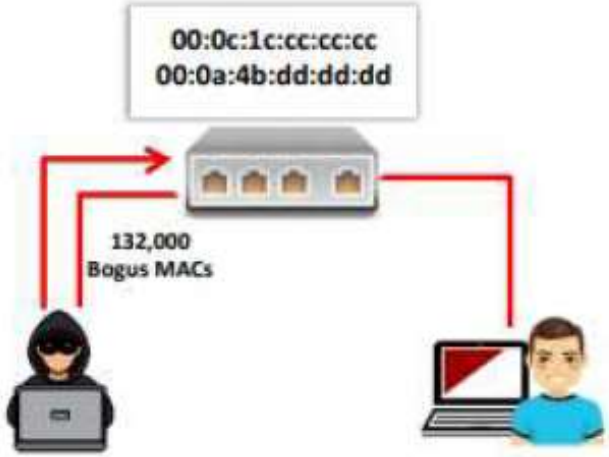
https://www.monkey.org

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



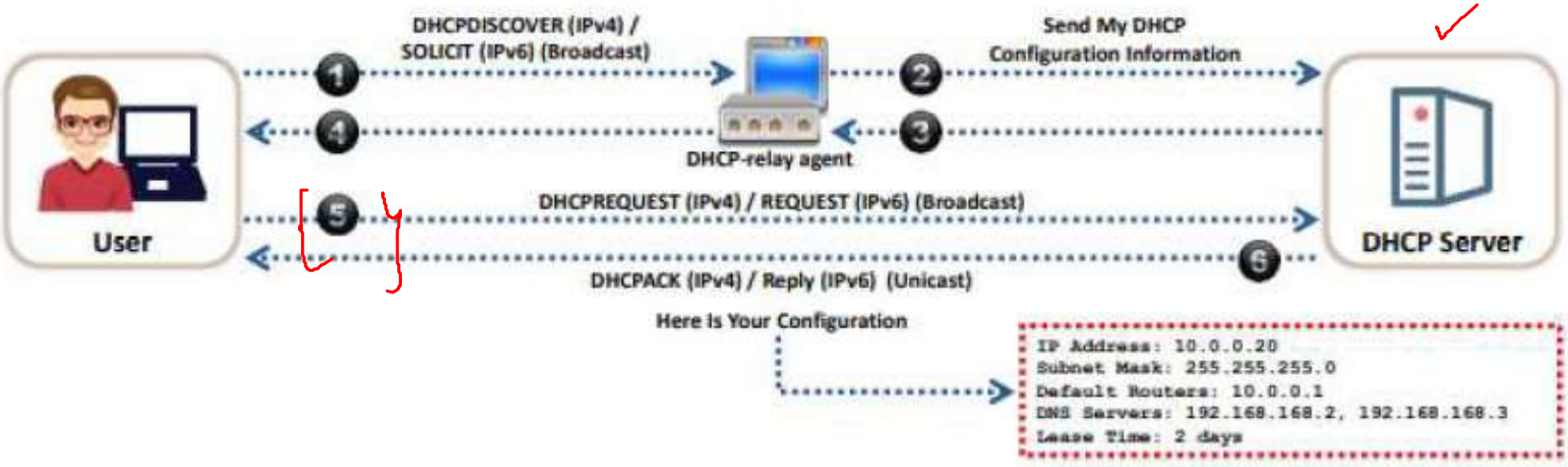
Configuring Port Security on Cisco Switch:

- switchport port-security
- switchport port-security maximum 1 vlan access
- 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

How DHCP Works

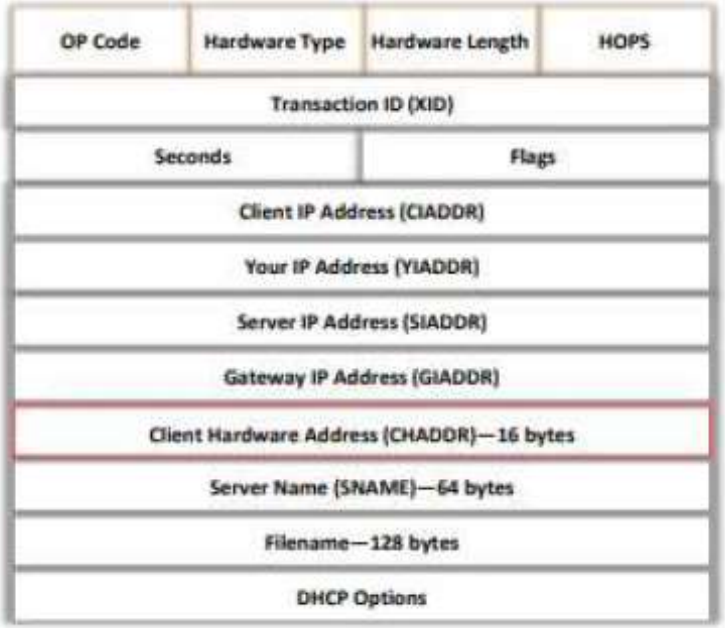
- DHCP servers maintain **TCP/IP configuration information**, such as valid TCP/IP configuration parameters, valid IP addresses, and the duration of the lease offered by the server, in a database
- It provides address configurations to DHCP-enabled clients in the form of a **lease offer**



DHCP Request/Reply Messages

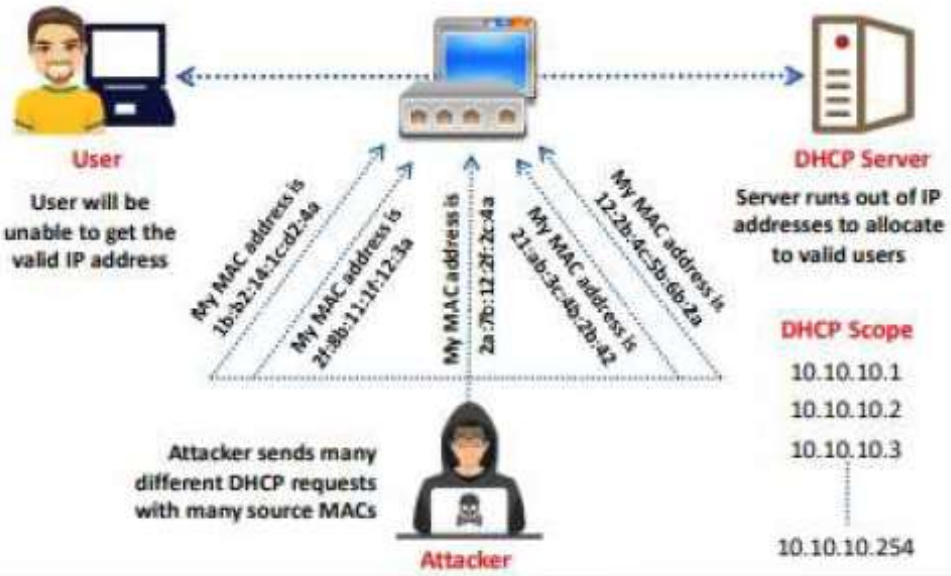
DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client broadcast to locate the available DHCP servers
DHCPOffer	Advertise	Server to client in response to DHCPDiscover with the offer of configuration parameters
DHCPRequest	Request, Confirm, Renew, Rebind	Client to servers either (a) requesting offered parameters, (b) confirming the correctness of the previously allocated address, or (c) extending the lease period
DHCPAck	Reply	Server to client with configuration parameters, including the committed network address
DHCPRelease	Release	Client to server relinquishing the network address and canceling the remaining lease
DHCPDecline	Decline	Client to server indicating that the network address is already in use
N/A	Reconfigure	Server to client saying that it has new or updated configuration settings. The client then sends either a renew/reply or Information-request/reply transaction to get the updated information
DHCPInform	Information Request	Client to server asking only for local configuration parameters; the client already has the externally configured network address
N/A	Relay-Forward	A relay agent sends a relay-forward message to relay messages to servers, either directly or through another relay agent
N/A	Relay-Reply	A server sends a relay-reply message to a relay agent containing a message that the relay agent delivers to a client
DHCPNAK	N/A	Server to client indicating that the client's notion of the network address is incorrect (e.g., the client has moved to a new subnet) or the client's lease has expired

IPv4 DHCP Packet Format

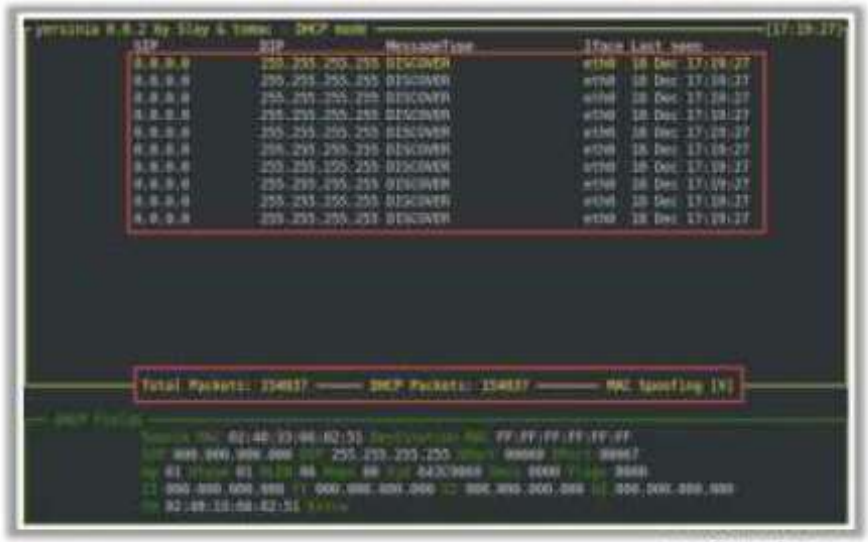


DHCP Starvation Attack

- 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



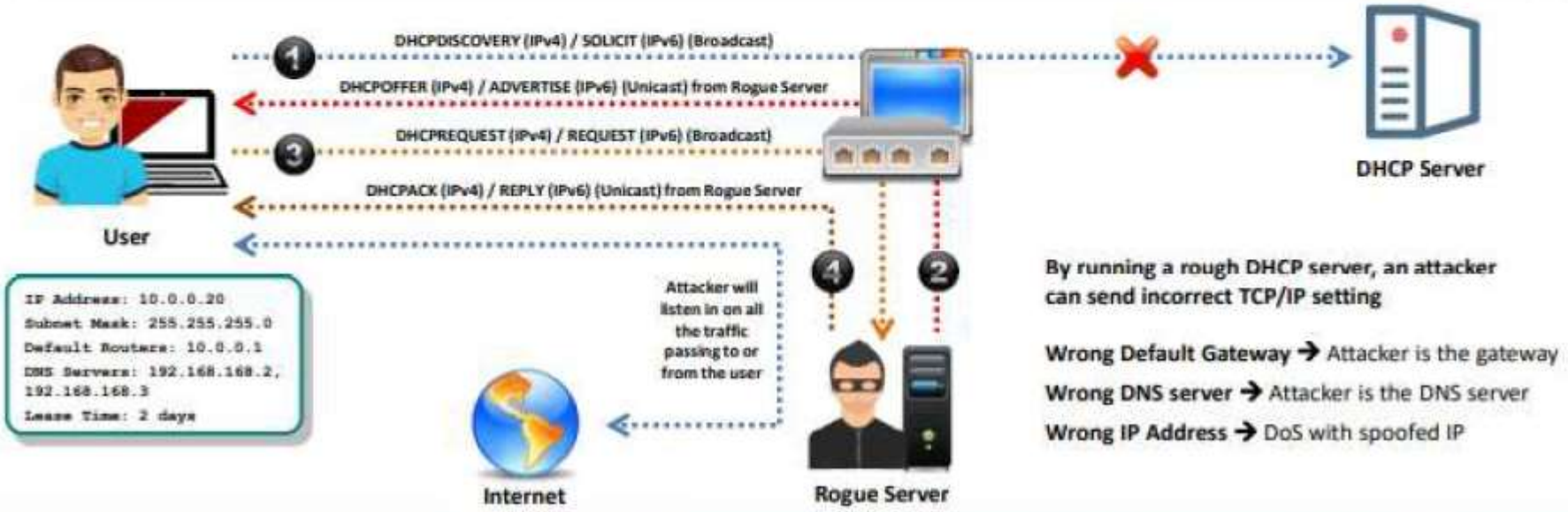
https://sourceforge.net

DHCP Starvation Attack Tools

- Hyenae (*https://sourceforge.net*)
- dhcpstarv (*https://github.com*)
- Gobbler (*https://sourceforge.net*)
- DHCPig (*https://github.com*)

Rogue DHCP Server Attack

1. 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
2. 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

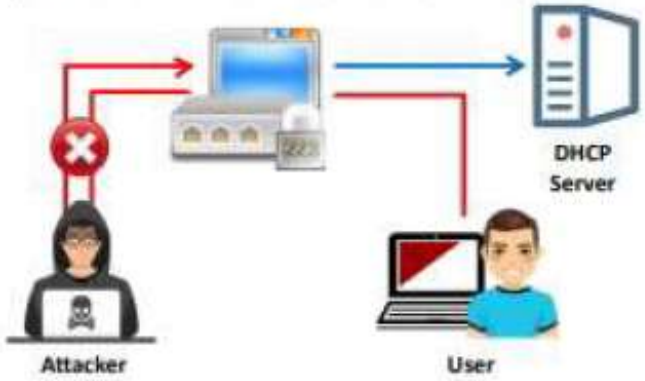
Wrong Default Gateway → Attacker is the gateway

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

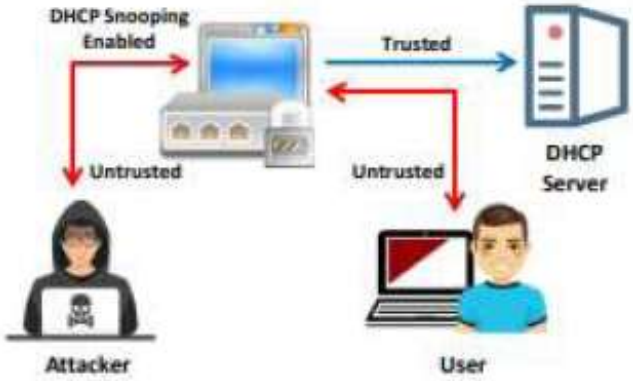
- **Enable port security** to defend against DHCP starvation attacks
  - Configuring the MAC limit on the switch's edge ports drops the packets from further MACs once the limit is reached



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



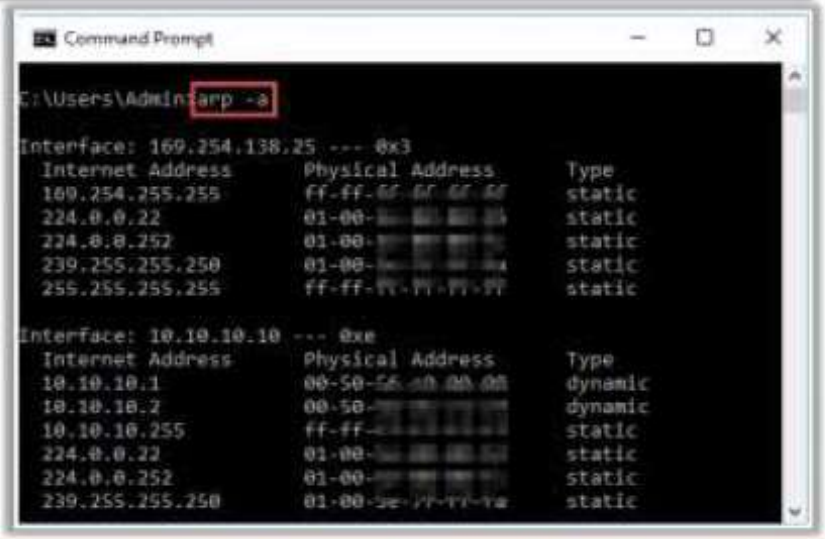
IOS Global Commands

- **`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

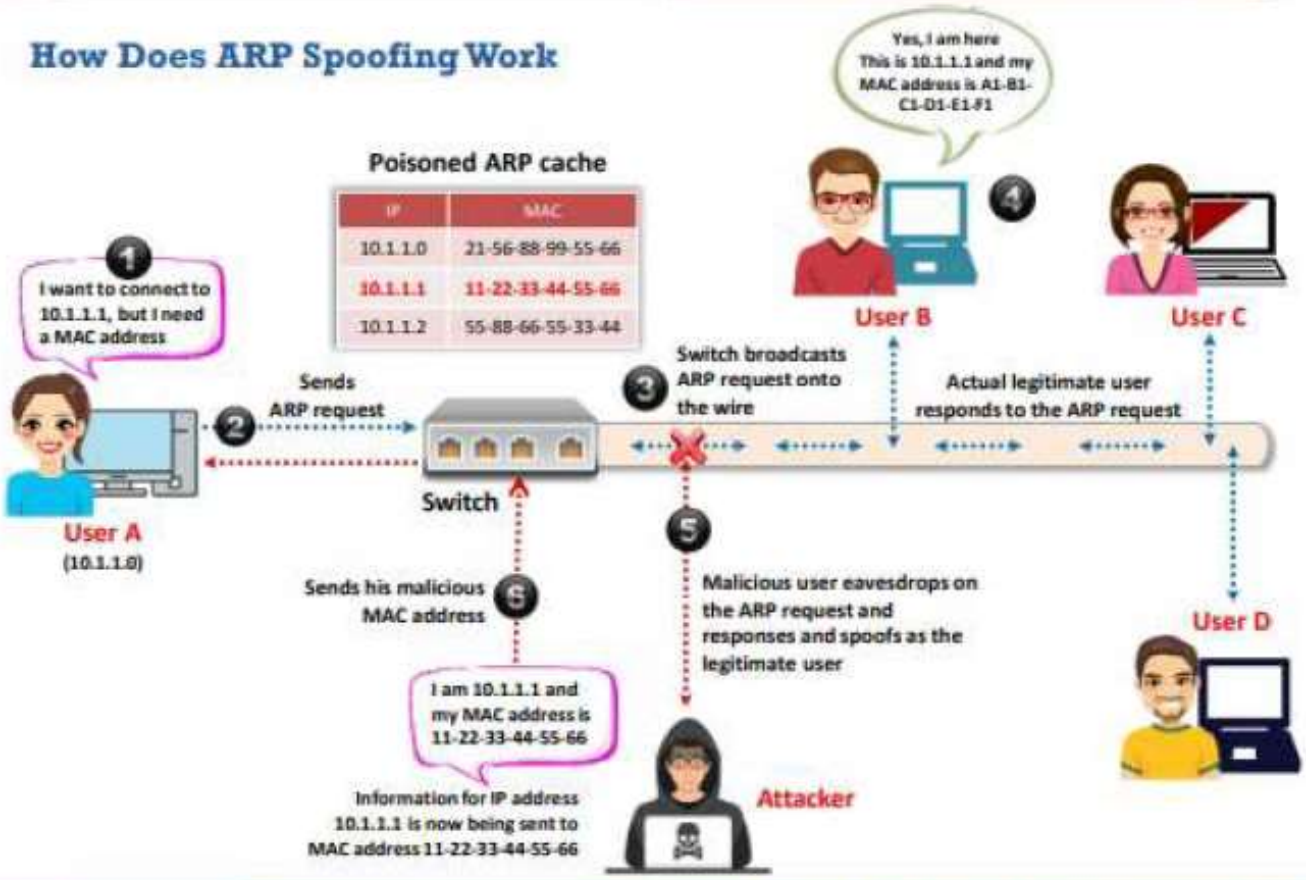
What Is Address Resolution Protocol (ARP)?

- Address Resolution Protocol (ARP) is a stateless protocol used for **resolving IP addresses to machine (MAC) addresses**
- All network devices (that need to communicate on the network) broadcast ARP queries on the network to discover other **machines' MAC addresses**
- When one machine needs to communicate with another, it looks up the IP address in its ARP table. If the MAC address is not found in the table, the **ARP_REQUEST** is broadcast over the network
- All machines on the network will compare this IP address to their own IP address
- If one of the machines on the network identifies with this IP address, it will respond to the **ARP_REQUEST** with its IP address (confirmation) and MAC address. The requesting machine will store the address pair in the ARP table and start the communication



ARP Spoofing Attack

- ARP packets can be **forged** to send data to the attacker's machine
- 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**



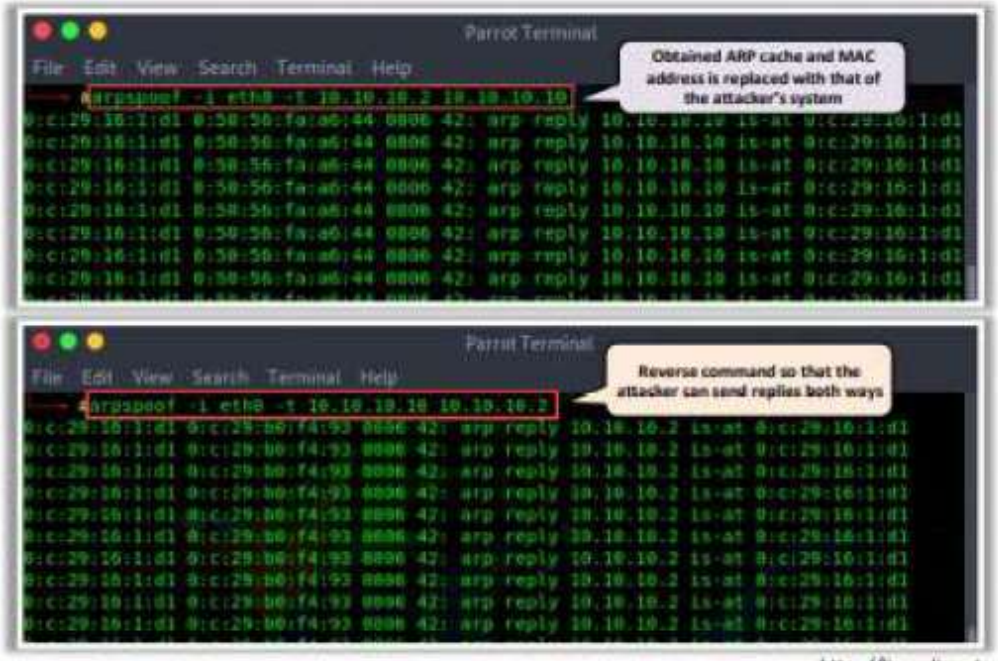
Threats of ARP Poisoning

- Using fake **ARP messages**, an attacker can divert all communications between two machines, resulting in all traffic being exchanged via the attacker's PC

1 Packet Sniffing	6 Data Interception
2 Session Hijacking	7 Connection Hijacking
3 VoIP Call Tapping	8 Connection Resetting
4 Manipulating Data	9 Stealing Passwords
5 Man-in-the-Middle Attack	10 Denial-of-Service (DoS) Attack

ARP Poisoning Tools

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



https://linux.die.net

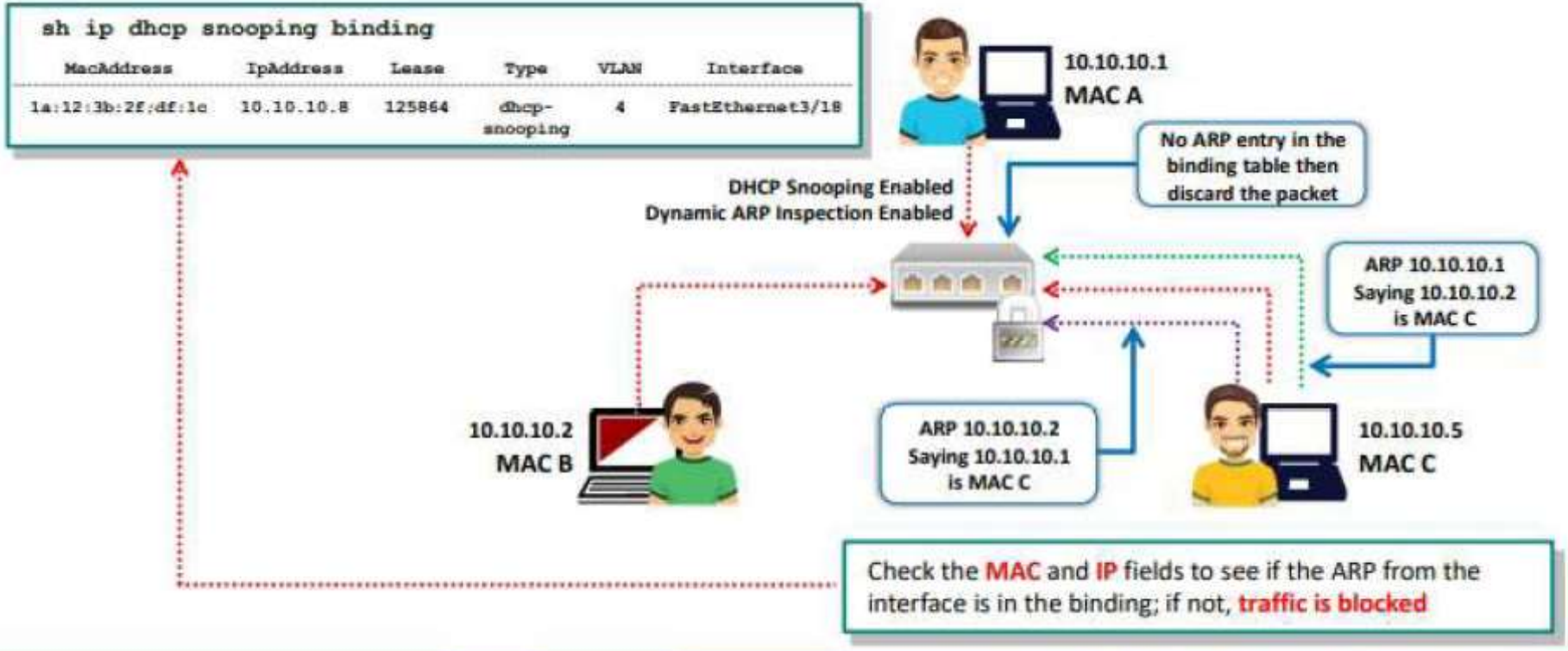
- **BetterCAP** — https://www.bettercap.org
- **Ettercap** — http://www.ettercap-project.org
- **dsniff** — https://www.monkey.org
- **MITMf** — https://github.com
- **Arpoison** — https://sourceforge.net

How to Defend Against ARP Poisoning

Implement **Dynamic ARP Inspection** Using DHCP Snooping Binding Table

```
sh ip dhcp snooping binding
```

MacAddress	IpAddress	Lease	Type	VLAN	Interface
1a:12:3b:2f:df:1c	10.10.10.8	125864	dhcp-snooping	4	FastEthernet3/18



Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

C|EH

1

```
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)
---------------      -------     ----------------
```

2

```
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	FastEthernet 0/3

Total number of bindings: 1

3

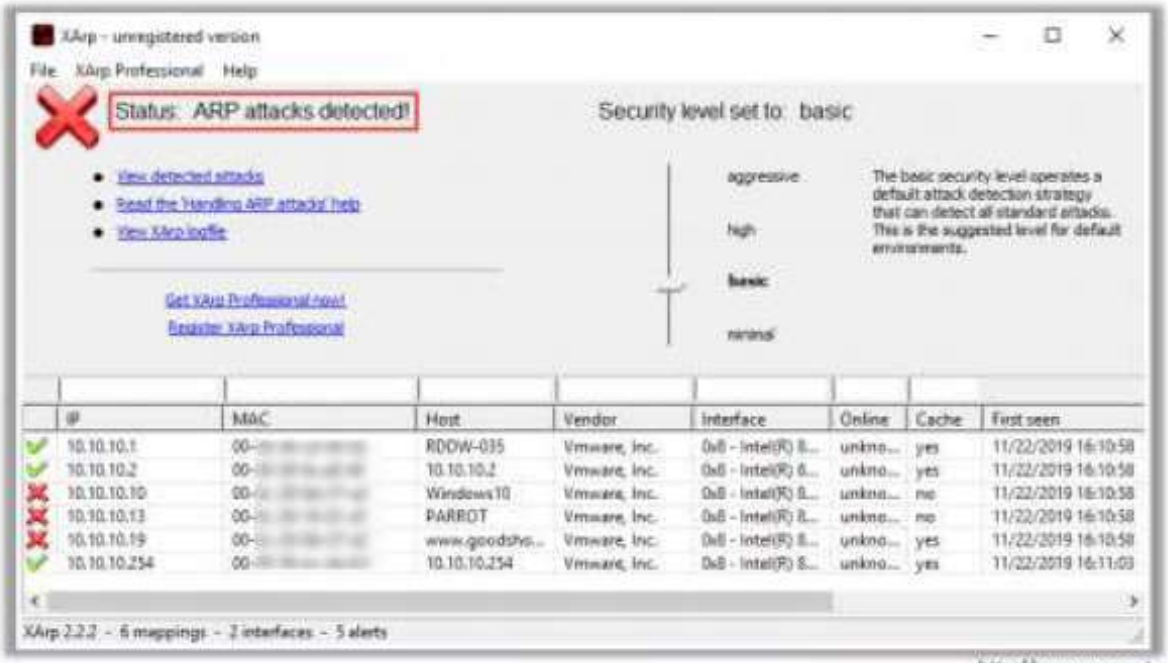
```
Switch(config)# ip arp inspection vlan 10
Switch(config)# ^Z
Switch# show ip arp inspection
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan  Configuration  Operation  ACL Match   Static ACL
 10     Enabled       Active
Vlan  ACL Logging  DHCP Logging  Probe Logging
 10     Deny         Deny          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
```

4

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs
(Res) on Fa0/5, vlan
10.([0013.6050.acf4/192.168.10.1/ffff.ffff.fff
f/192.168.10.1/05:37:31 UTC Mon Jul 08 2019])
```

ARP Spoofing Detection Tools

XArp | XArp is a security tool that helps administrators **detect ARP attacks** and **ensure data privacy**



http://www.xarp.net

Capsa Network Analyzer
https://www.colasoft.com

ArpON
https://sourceforge.net

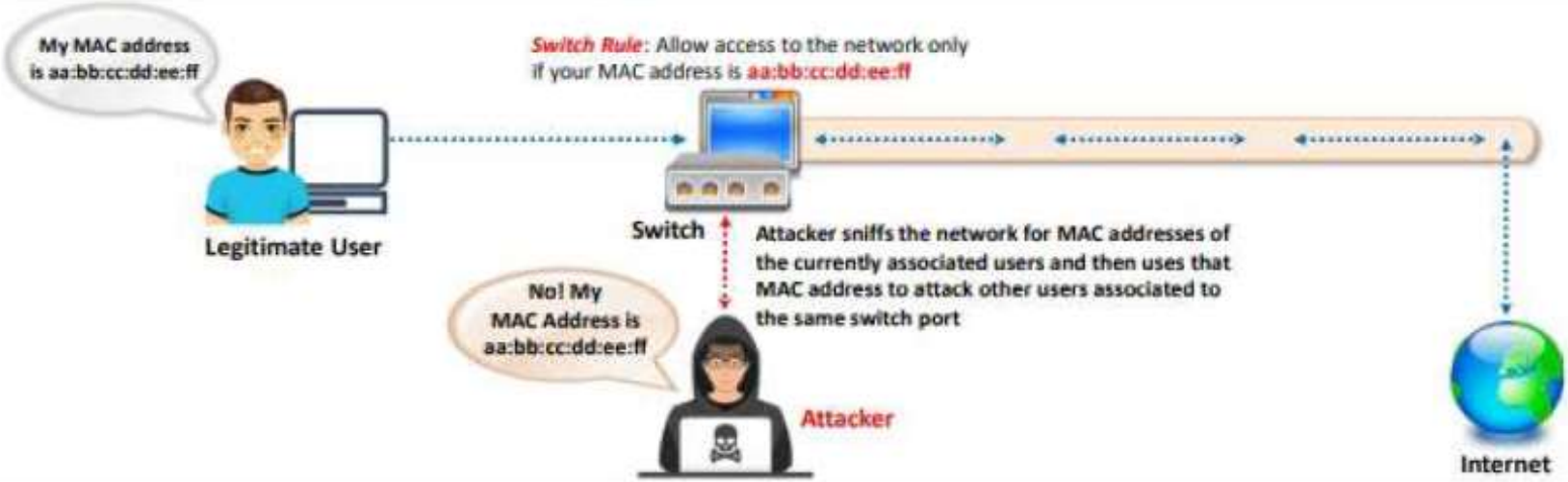
ARP AntiSpoofer
https://sourceforge.net

ARPStraw
https://github.com

shARP
https://github.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

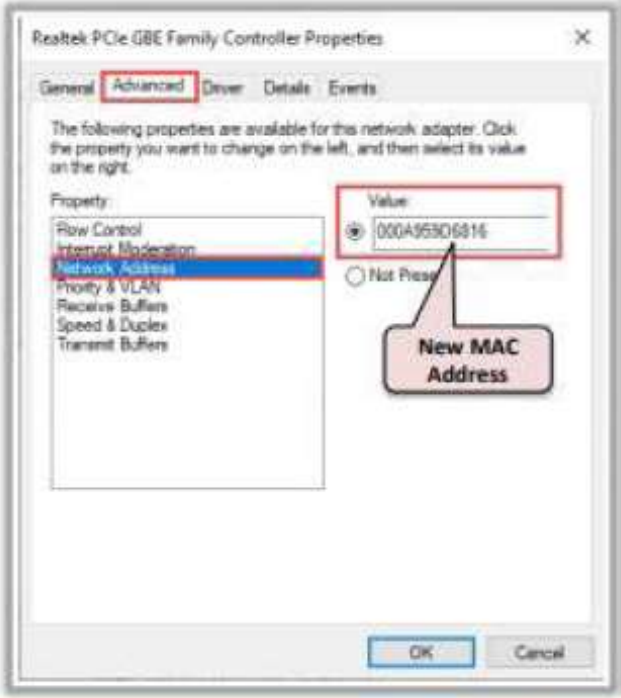


Note: This technique can be used to bypass Wireless Access Points' MAC filtering

MAC Spoofing Technique: Windows

In Windows 10 OS

Method 1: If the network interface card supports a clone MAC address, then follow these steps:



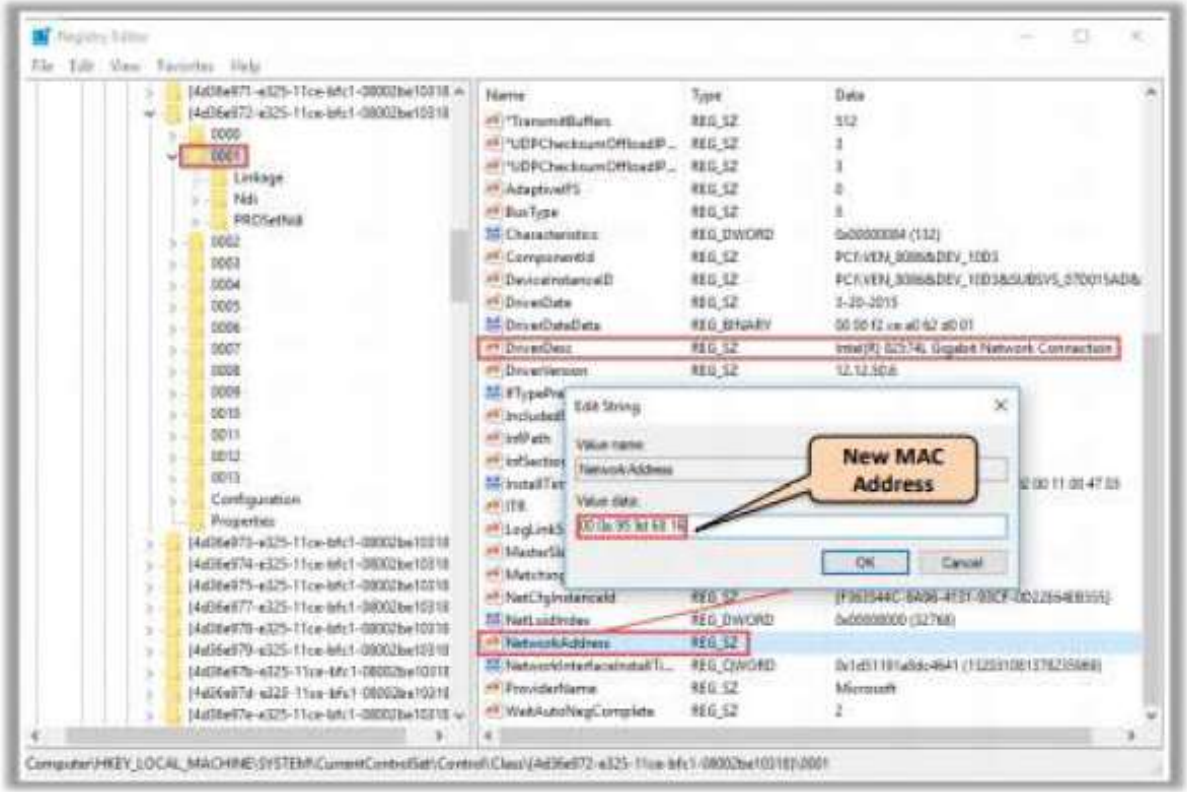
1. Click **Start** and search for **Control Panel** and open it, then navigate to **Network and Internet** → **Networking and Sharing Center**
2. Click on **Ethernet** and then click on **Properties** in the **Ethernet Status** window
3. In the **Ethernet Properties** window, click on the **Configure** button and then click on the **Advanced** tab
4. Under the "**Property**" section, browse for **Network Address** and click on it
5. On the right side, under "**Value**," type in the new MAC address you would like to assign and click **OK**
   Note: Enter the MAC address number without a ":" between the number pairs
6. Type "**ipconfig/all**" or "**net config rdr**" in the command prompt to verify the changes
7. If the changes are visible then **reboot** the system, otherwise try method 2 (change MAC address in the registry)

MAC Spoofing Technique: Windows (Cont'd)

Method 2: Steps to change the MAC address in the Registry

- Press **Win + R** to open Run, type **regedt32** to start the registry editor

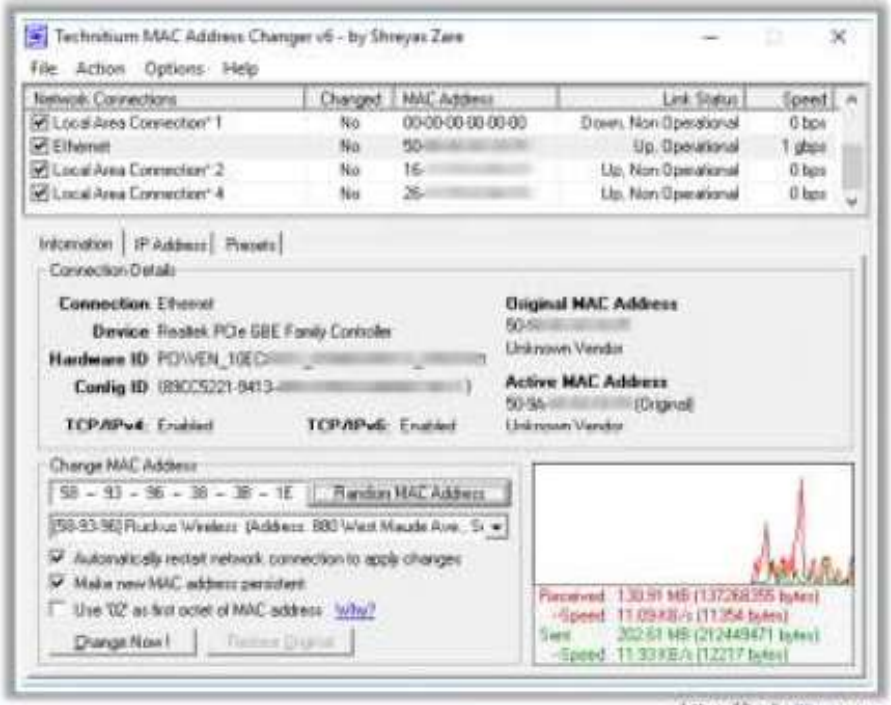
  Note: Do not type **Regedit** to start the registry editor
- Go to "**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}** and double click on it to expand the tree
- 4-digit sub keys representing network adapters will be displayed (starting with 0000, 0001, 0002, etc.)
- Search for the proper "**DriverDesc**" key to find the desired interface
- Right-click on the appropriate sub key and add, new string value "**NetworkAddress**" (data type "REG_SZ") to contain the new MAC address
- Right click on the "**NetworkAddress**" string value on the right side and select **Modify...**
- In the "**Edit String**" dialogue box, "**Value data**" field enter the new MAC address and click "**OK**"
- **Disable** and then **re-enable** the network interface that was changed or reboot the system



MAC Spoofing Tools

Technitium MAC Address Changer

Technitium MAC Address Changer (TMAC) allows you to change (spoof) the **Media Access Control** (MAC) Address of your **Network Interface Card** (NIC) instantly



https://technitium.com

SMAC
http://www.klcconsulting.net

MAC Address Changer
https://www.novirusthanks.org

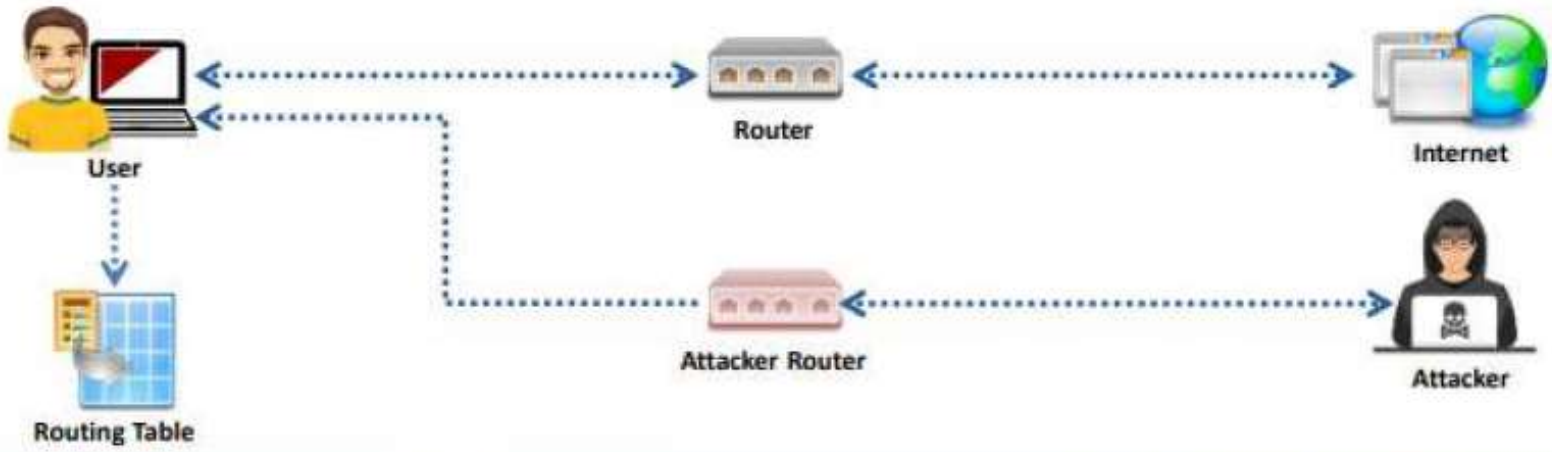
Change MAC Address
https://lizardsystems.com

Easy Mac Changer
https://github.com

Spoof-Me-Now
https://sourceforge.net

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

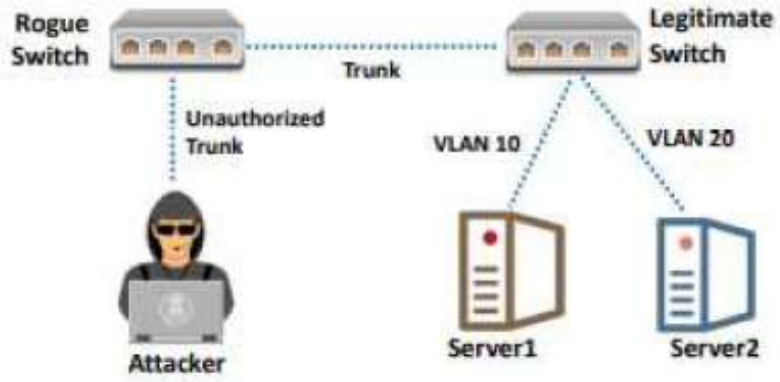


VLAN Hopping

- VLAN hopping is a technique used to **target network resources** present on a virtual LAN
- It can be performed by using two primary methods: **Switch Spoofing** and **Double Tagging**
- Attackers perform **VLAN hopping attacks** to steal sensitive information such as passwords, modify, corrupt or delete data, install malicious codes or programs, and spread viruses, Trojans, and worms throughout the network

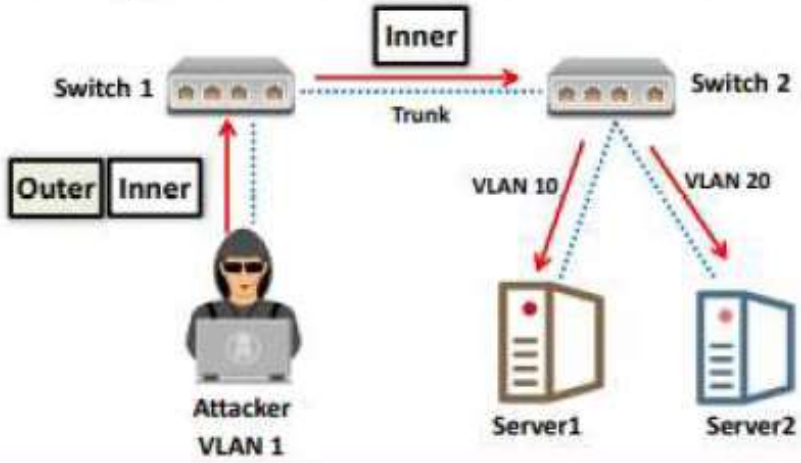
Switch Spoofing

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



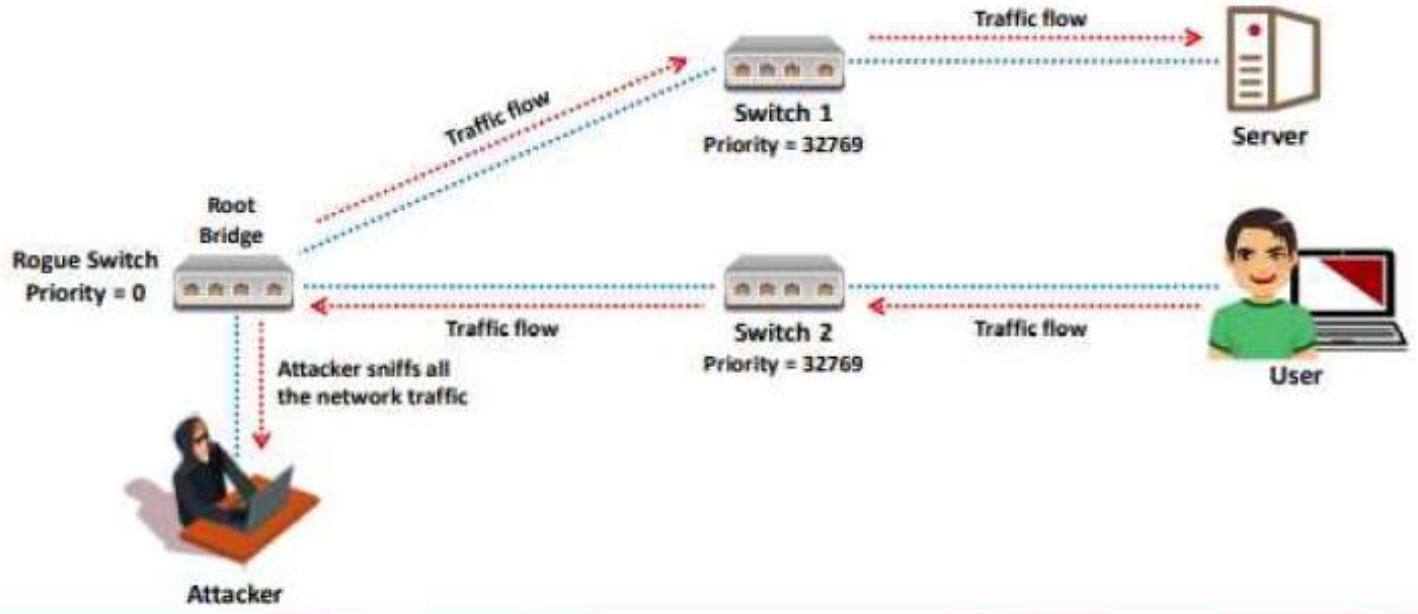
Double Tagging

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



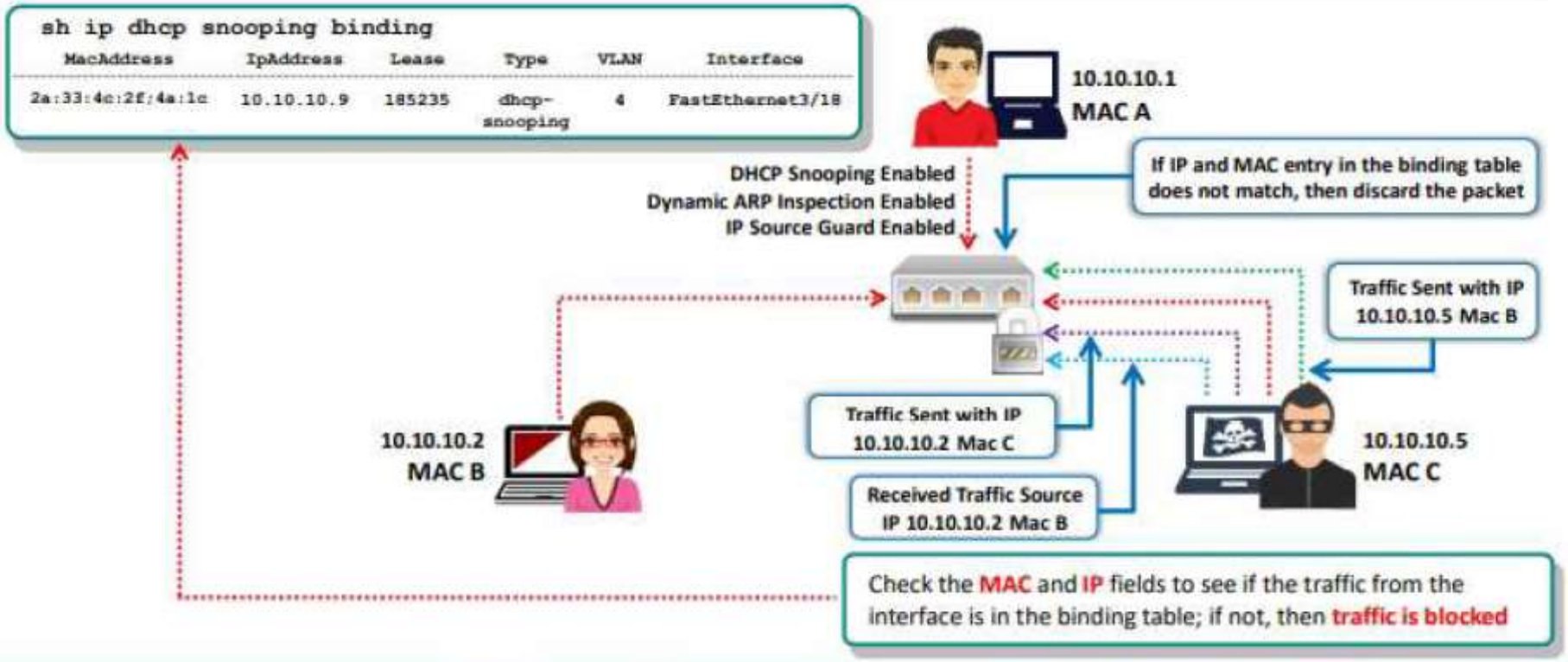
STP Attack

- 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



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:

```
Switch(config-if)# switchport mode
trunk

Switch(config-if)# switchport mode
nonegotiate
```

Defend against Double Tagging

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

```
switchport access vlan 2
```

- Ensure that the native VLANs on all trunk ports are changed to an **unused VLAN ID**:

```
switchport trunk native vlan 999
```

- Ensure that the **native VLANs** on all trunk ports are explicitly tagged:

```
vlan dot1q tag native
```

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 gigabiteethernet slot/port
spanning-tree portfast bpduguard
```

Loop Guard

- To enable the loop guard on an interface:

```
configure terminal
interface gigabiteethernet slot/port
spanning-tree guard loop
```

Root Guard

- To enable the root guard feature on an interface:

```
configure terminal
interface gigabiteethernet slot/port
spanning-tree guard root
```

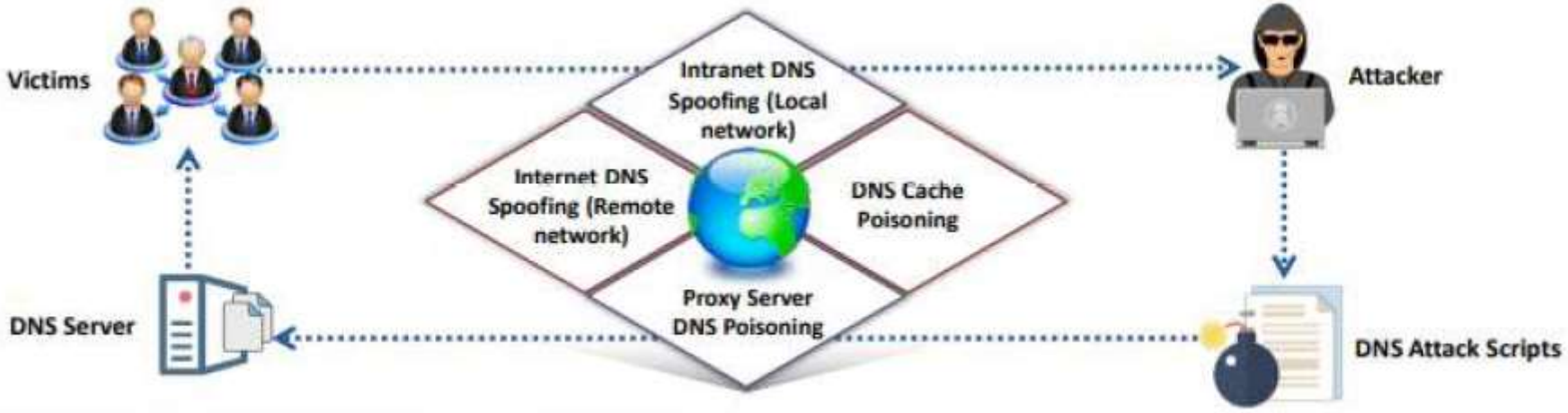
UDLD (Unidirectional Link Detection)

- To enable UDLD on an interface:

```
configure terminal
interface gigabiteethernet slot/port
udld { enable | disable | aggressive }
```

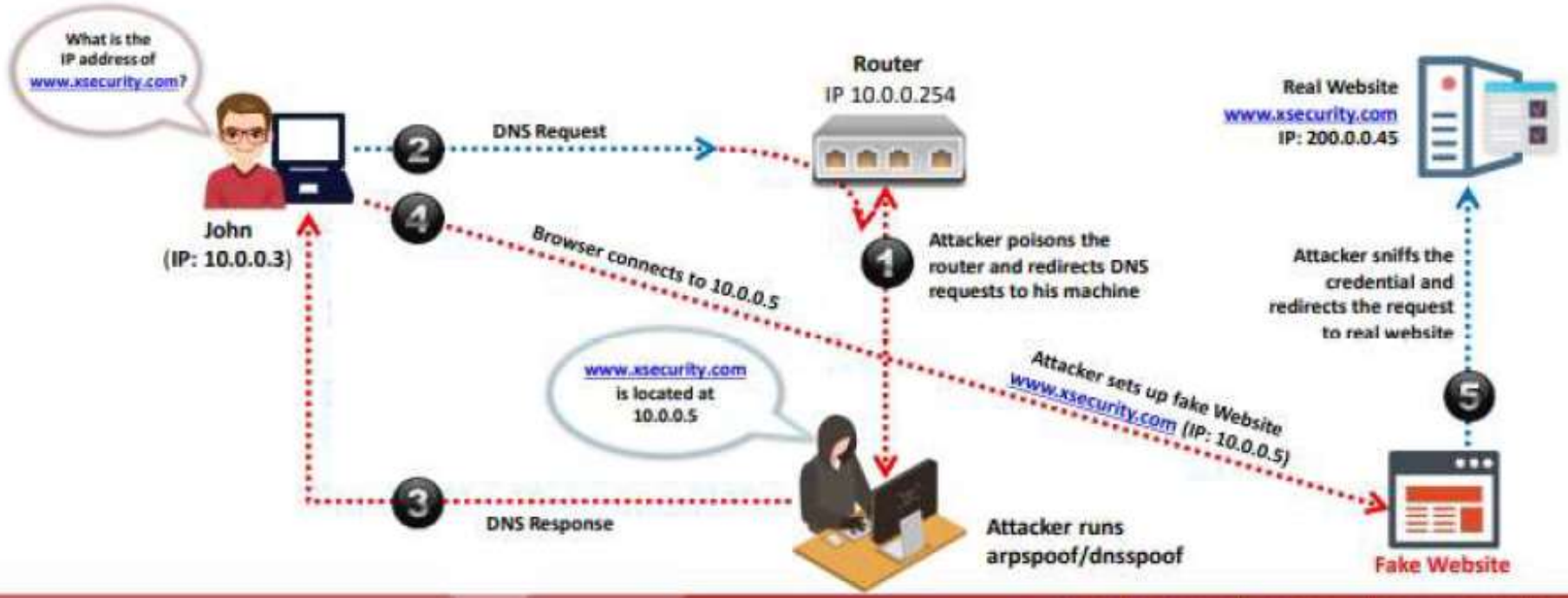
DNS Poisoning Techniques

- 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
- The attacker can create **fake DNS entries** for the server (containing malicious content) with names similar to that of the target server



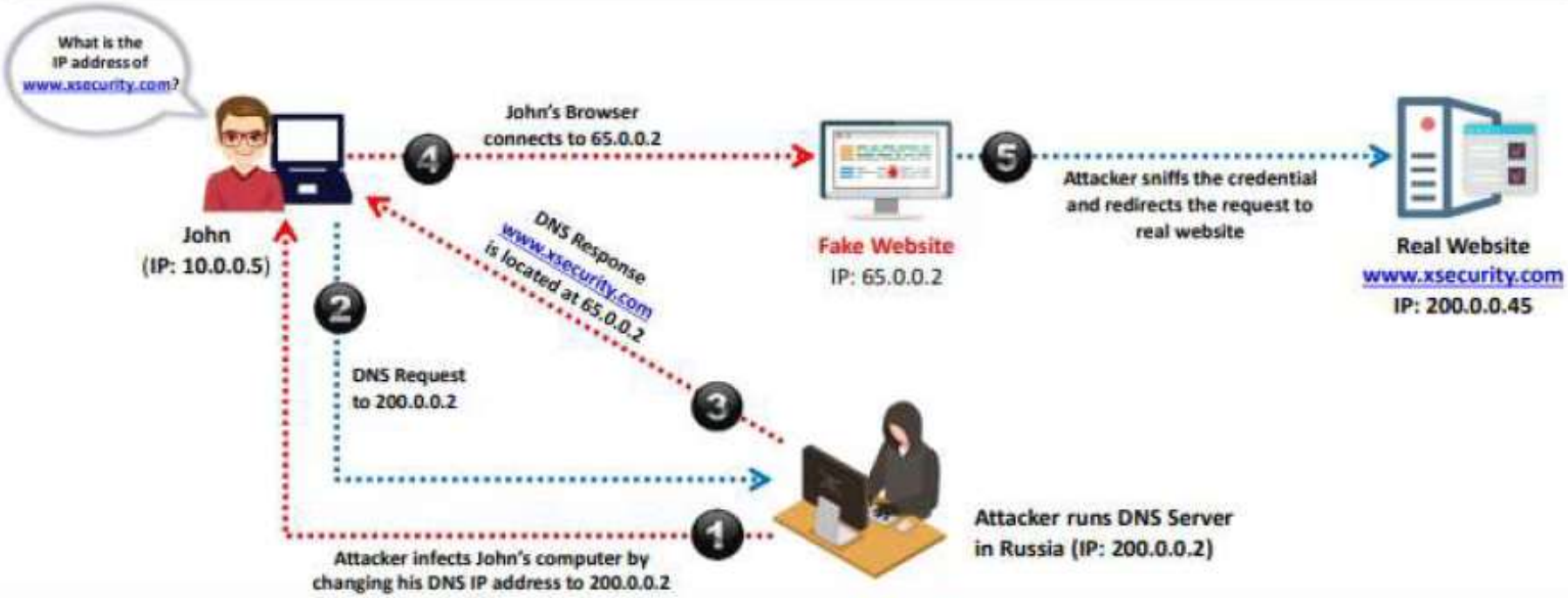
Intranet DNS Spoofing

- 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



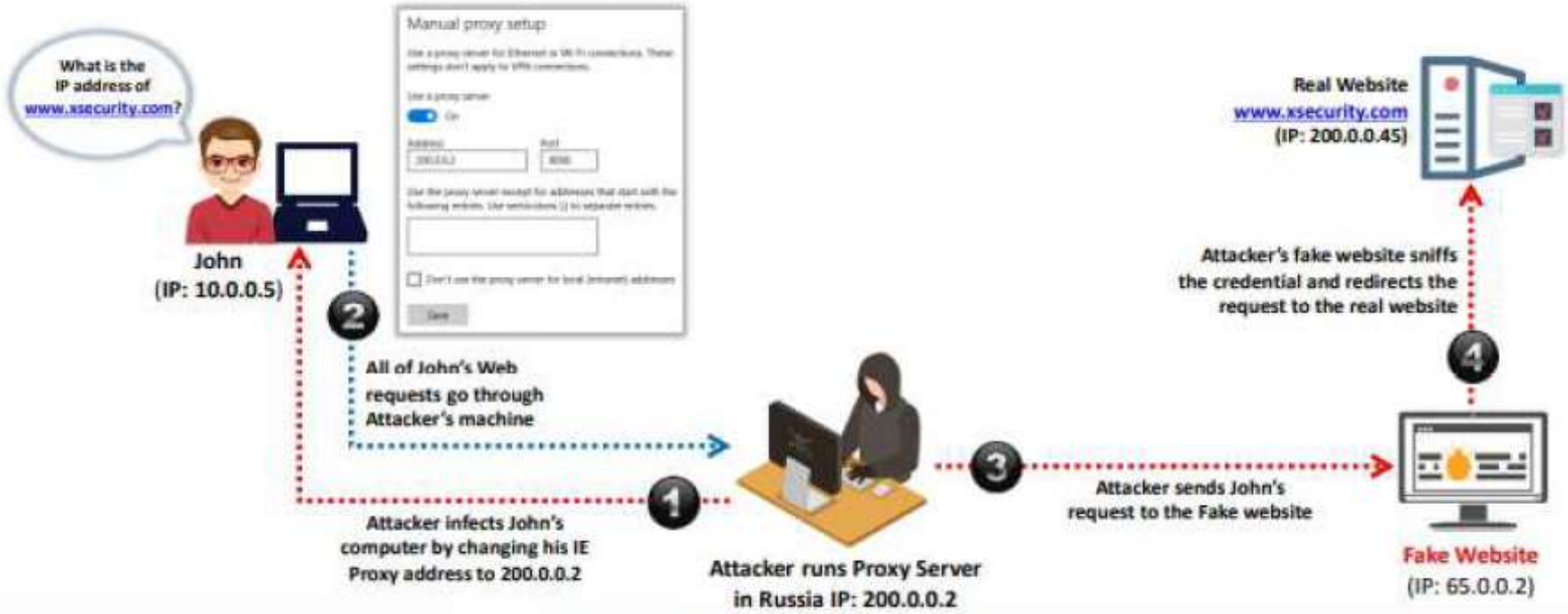
Internet DNS Spoofing

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



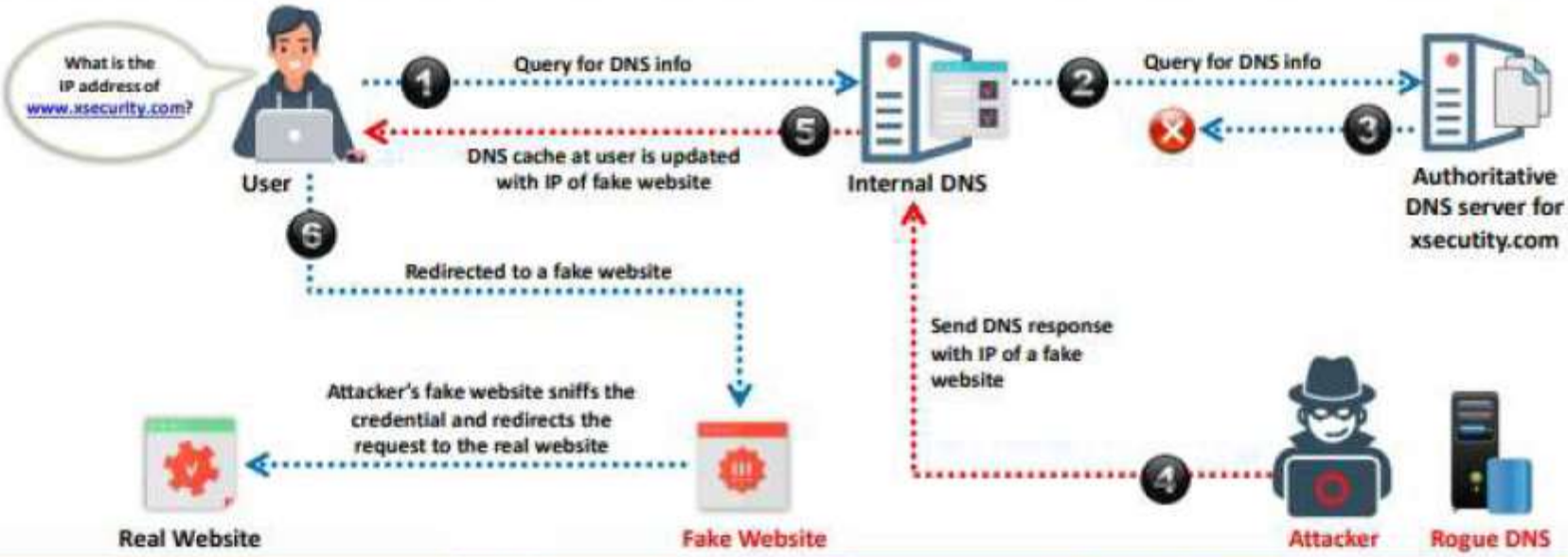
Proxy Server DNS Poisoning

- 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



DNS Poisoning Tools

DerpNSpoof | DerpNSpoof is a DNS poisoning tool that assists in spoofing the **DNS query packet** of a certain IP address or a group of hosts in the network

https://github.com

- **DNS Spoof** — https://github.com
- **DNS-poison** — https://github.com
- **Ettercap** — http://www.ettercap-project.org
- **Evilgrade** — https://github.com
- **TORNADO** — https://github.com

How to Defend Against DNS Spoofing

C|EH

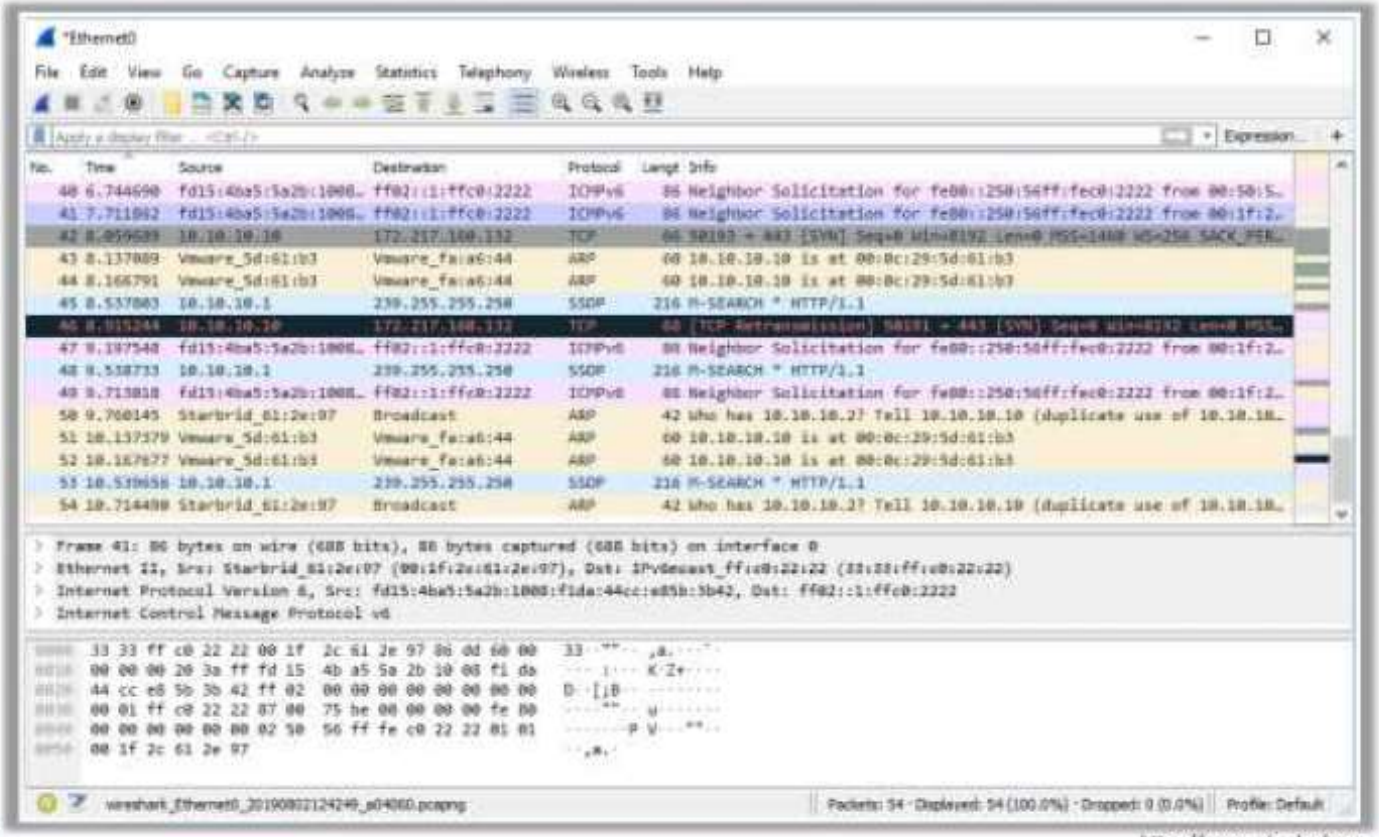
1. Implement a Domain Name System Security Extension (DNSSEC)
2. Use a Secure Socket Layer (SSL) for securing the traffic
3. Resolve all DNS queries to a local DNS server
4. Block DNS requests being sent to external servers
5. Configure a firewall to restrict external DNS lookups
6. Implement an intrusion detection system (IDS) and deploy it correctly
7. Configure the DNS resolver to use a new random source port for each outgoing query
8. Restrict the DNS recusing service, either fully or partially, to authorized users
9. Use DNS Non-Existent Domain (NXDOMAIN) Rate Limiting
10. Secure your internal machines
11. Use a static ARP and IP table
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

Module Flow

1. Sniffing Concepts
2. Sniffing Techniques
3. Sniffing Tools
4. Countermeasures
5. Sniffing Detection Techniques

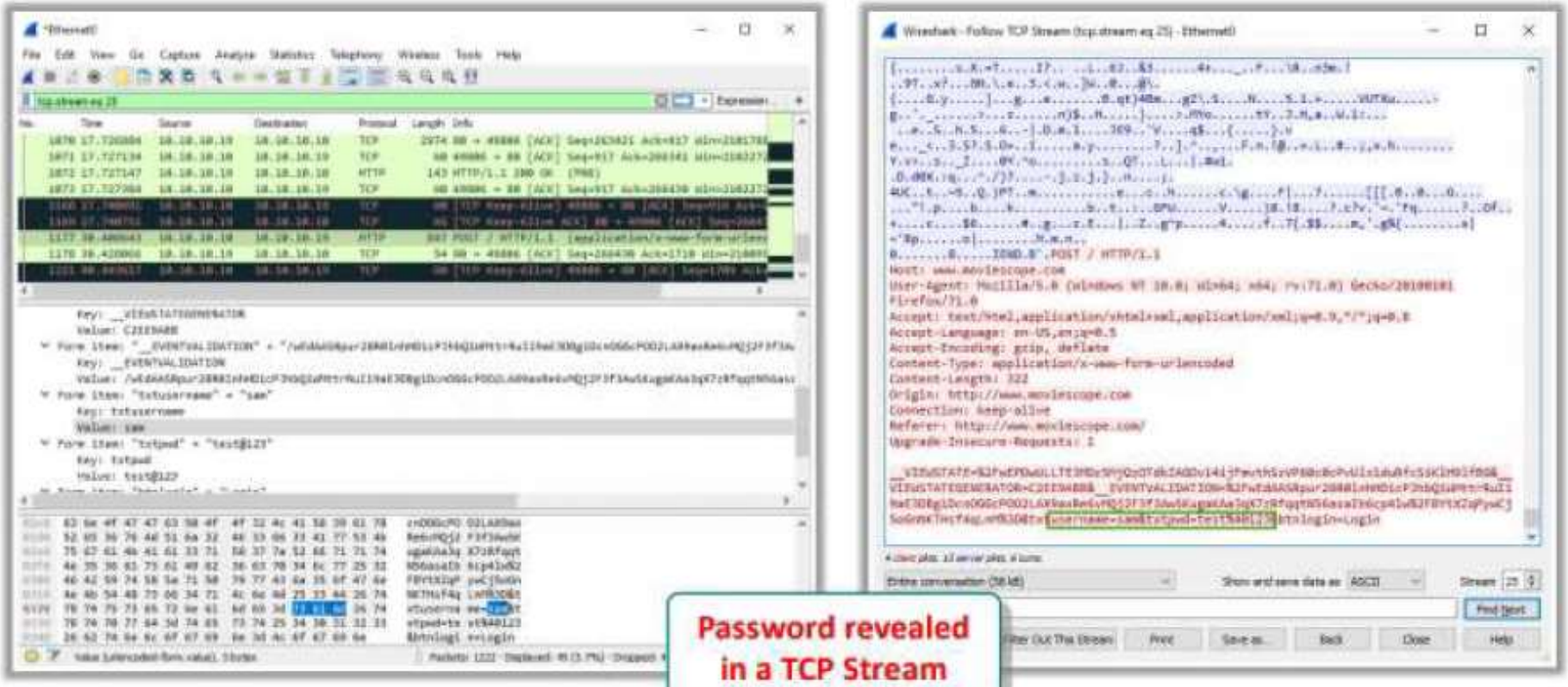
Sniffing Tool: Wireshark

- It lets you **capture and interactively browse the traffic** running on a computer network
- Wireshark uses **Winpcap** to capture packets on its own supported networks
- It **captures live network traffic** from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks
- A **set of filters** for customized data displays can be used



https://www.wireshark.org

Follow TCP Stream in Wireshark



Display Filters in Wireshark

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

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

Additional Wireshark Filters

1. `tcp.flags.reset==1`
   Displays all TCP resets

2. `udp contains 33:27:58`
   Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset

3. `http.request`
   Displays all HTTP GET requests

4. `tcp.analysis. Retransmission`
   Displays all retransmissions in the trace

5. `tcp contains traffic`
   Displays all TCP packets that contain the word "traffic"

6. `!(arp or icmp or dns)`
   Masks out arp, icmp, dns, or other protocols and allows you to view traffic of your interest

7. `tcp.port == 4000`
   Sets a filter for any TCP packet with 4000 as a source or destination port

8. `tcp.port eq 25 or icmp`
   Displays only SMTP (port 25) and ICMP traffic

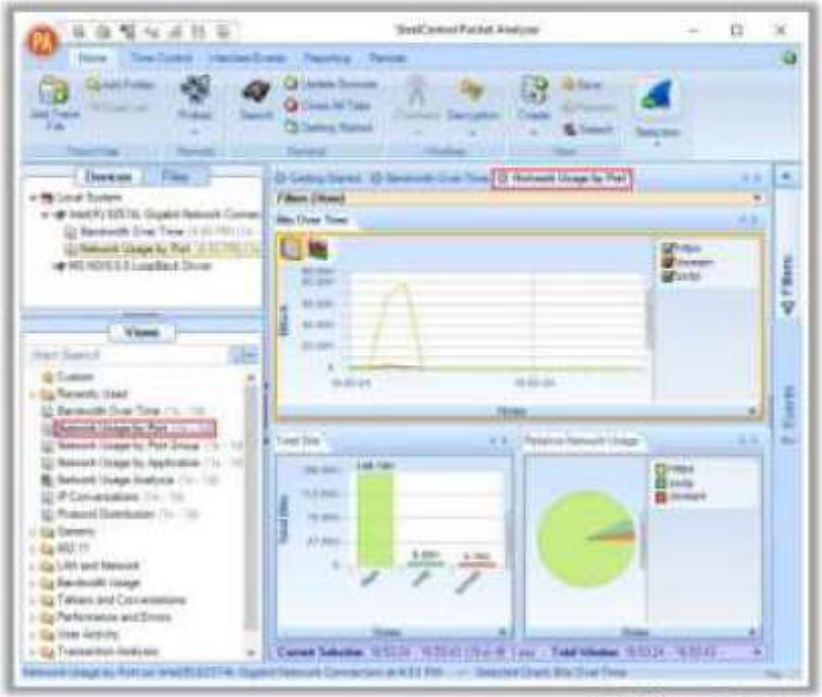
9. `ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16`
   Displays only traffic in the LAN (192.168.x.x), between workstations and servers — no Internet

10. `ip.src != xxx.xxx.xxx.xxx && ip.dst != xxx.xxx.xxx.xxx && sip`
    Filter by a protocol (e.g. SIP) and filter out unwanted IPs

Sniffing Tools

SteelCentral Packet Analyzer

SteelCentral Packet Analyzer provides a graphical console for **high-speed packet analysis**



https://www.riverbed.com

Capsa Network Analyzer

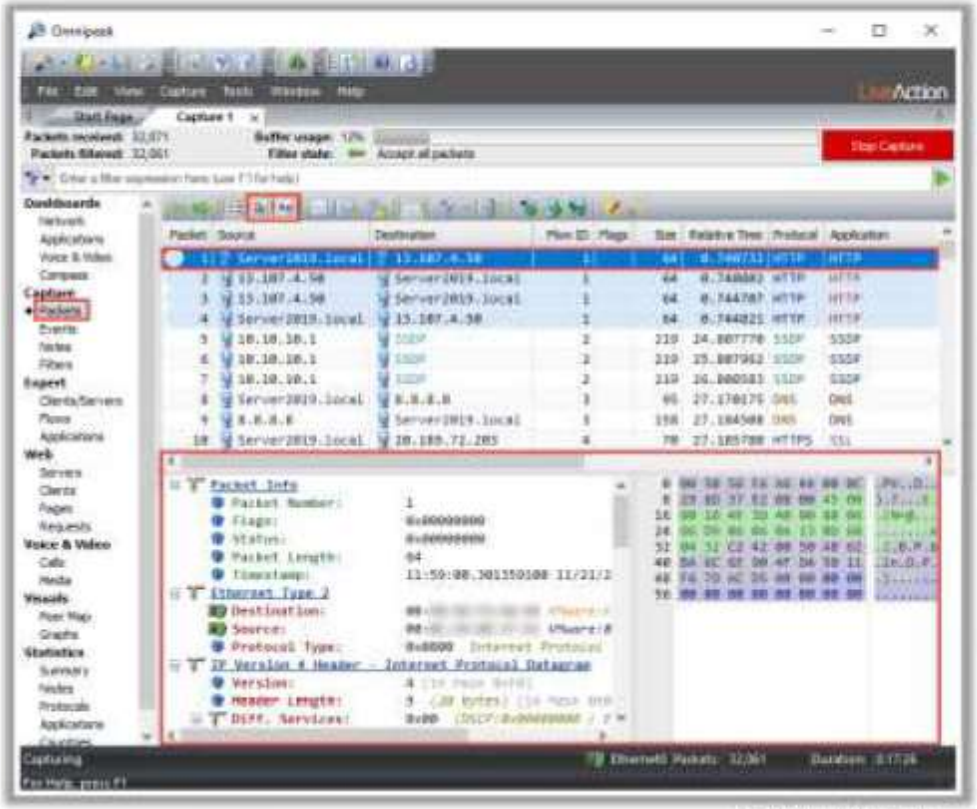
Capsa Network Analyzer **captures all data transmitted over the network** and provides a wide range of analysis statistics in an intuitive and graphical way

https://www.colasoft.com

Sniffing Tools (Cont'd)

OmniPeek

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



Observer Analyzer
https://www.viavisolutions.com

PRTG Network Monitor
https://www.paessler.com

SolarWinds Deep Packet Inspection and Analysis
https://www.solarwinds.com

Xplico
https://www.xplico.org

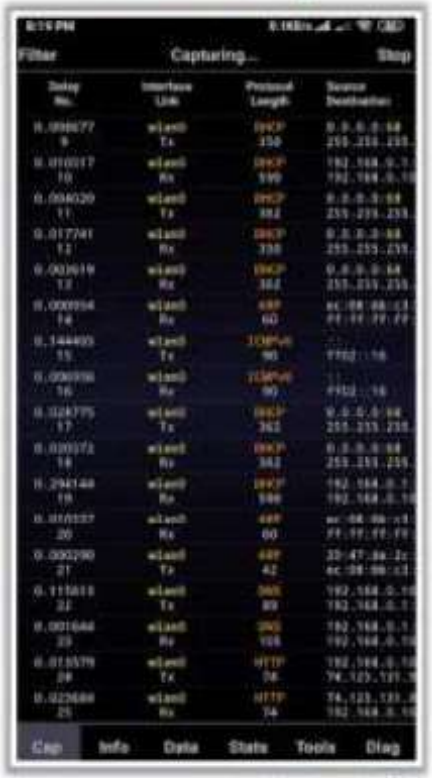
Colasoft Packet Builder
https://www.colasoft.com

https://www.liveaction.com

Packet Sniffing Tools for Mobile Phones

CEH

Sniffer Wicap

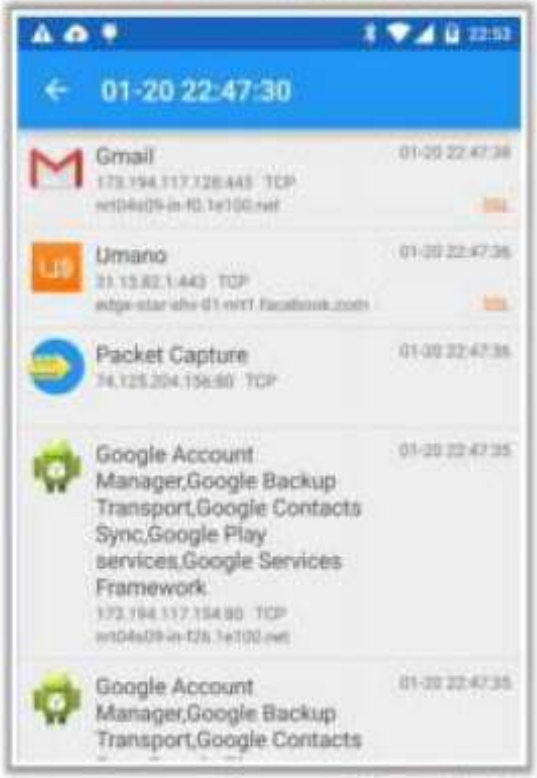


https://play.google.com

FaceNiff

http://faceniff.ponury.net

Packet Capture



https://play.google.com

Module Flow

1. Sniffing Concepts
2. Sniffing Techniques
3. Sniffing Tools
4. Countermeasures
5. Sniffing Detection Techniques

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)

C|EH

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 WPA and WPA2
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 the concept of **Access Control List (ACL)** to allow access to only a fixed range of **trusted IP addresses** in a network

Module Flow

1. Sniffing Concepts
2. Sniffing Techniques
3. Sniffing Tools
4. Countermeasures
5. Sniffing Detection Techniques

How to Detect Sniffing

C|EH

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

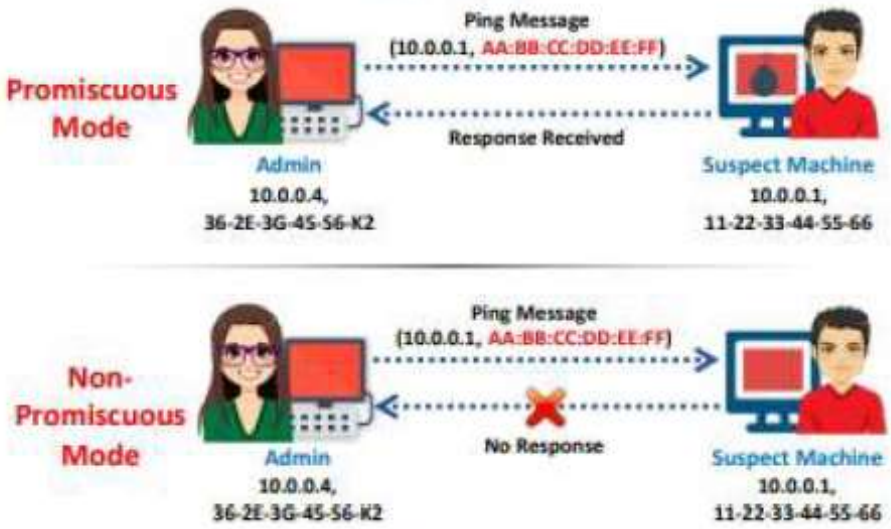
- **Run IDS** and see if the **MAC address** of any of the machines has changed (Example: router's MAC address)
- IDS can alert the administrator about **suspicious activities**

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

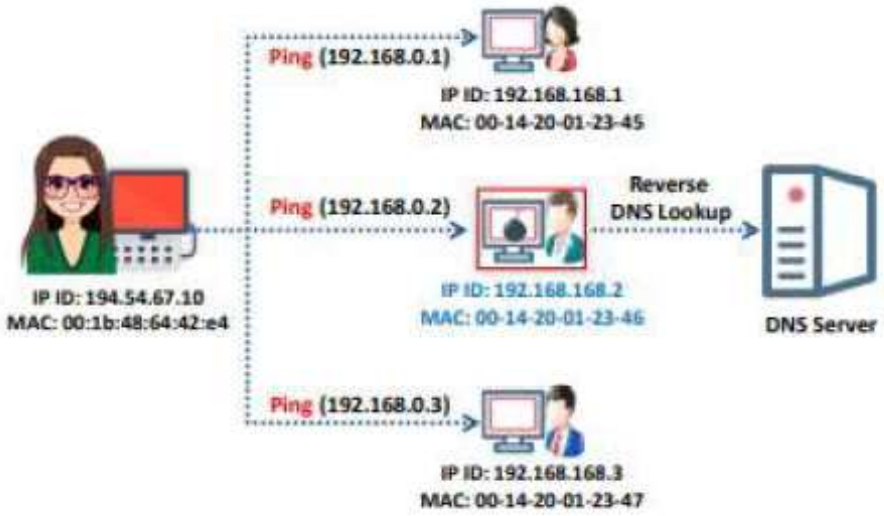
Ping Method



- 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

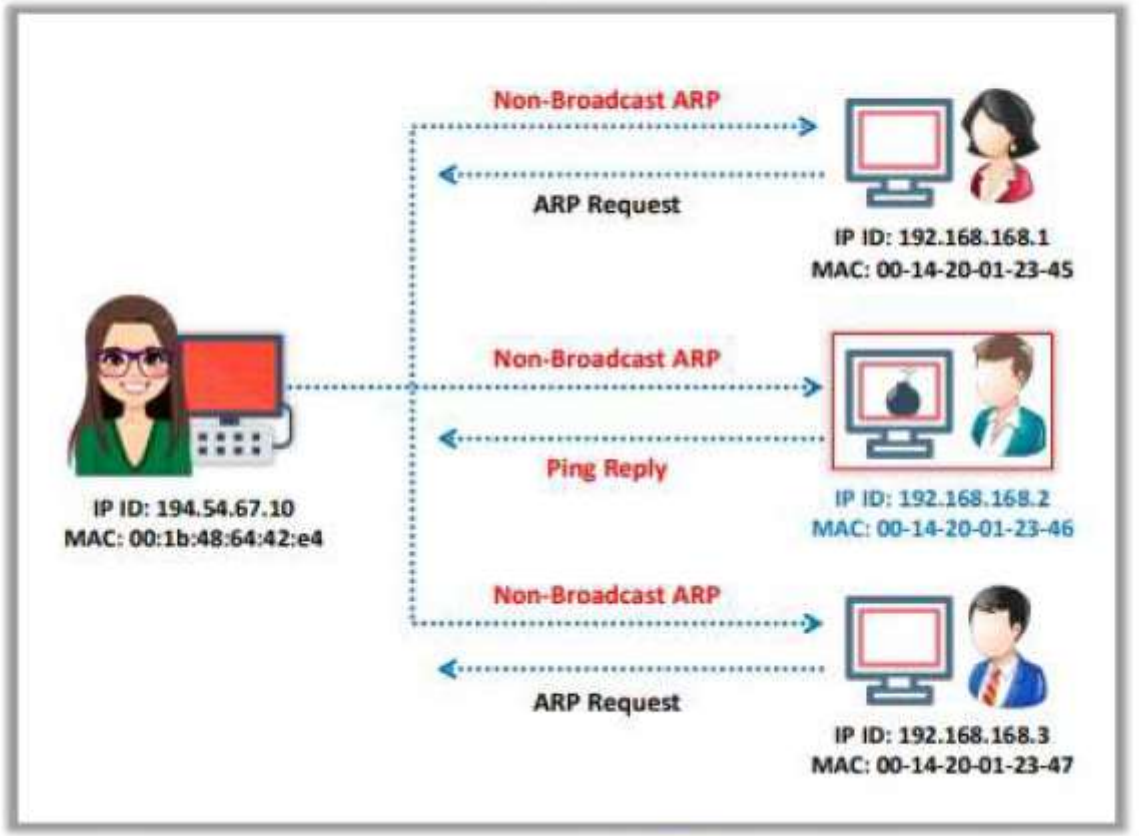
- Most of the sniffers perform **reverse DNS lookups** to identify the machine from the IP address



- 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

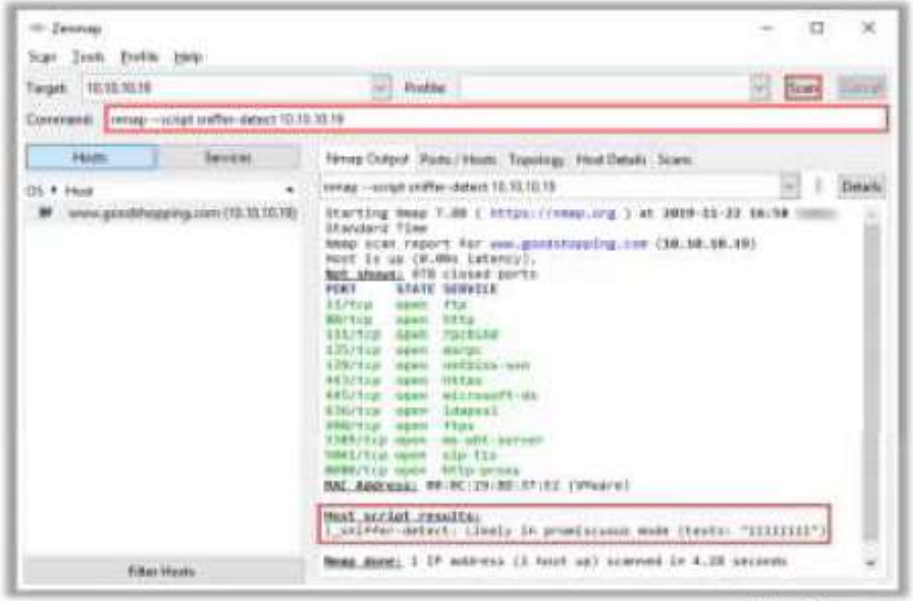
Nmap

- 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:

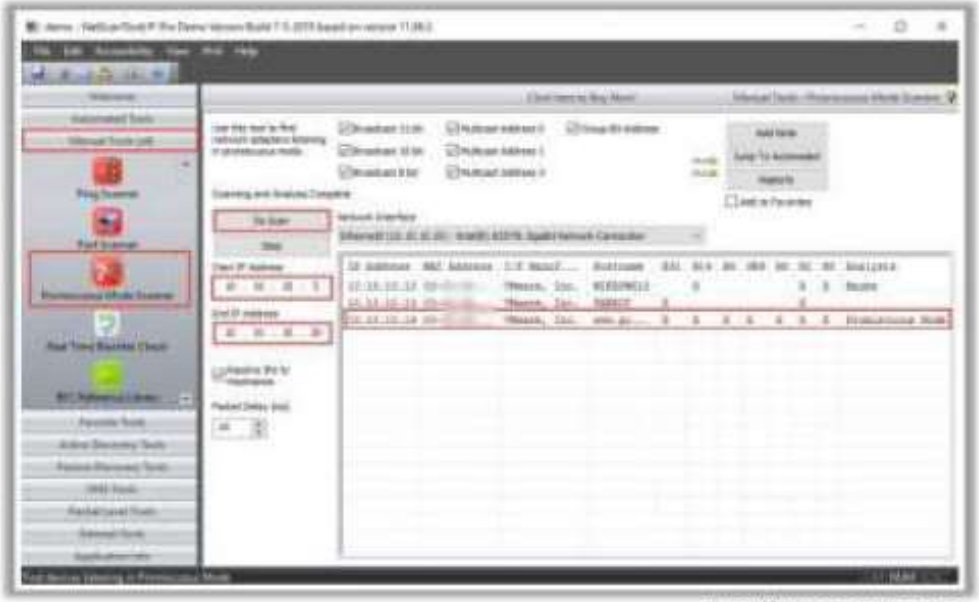
```
nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]
```

NetScan Tools 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://nmap.org



https://www.netscantools.com

Module Summary

- In this module, we have discussed the following:
  - Sniffing concepts along with protocols vulnerable to sniffing and various hardware protocol analyzers
  - 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


THANK YOU!