
EC-Council
C|EH
Certified Ethical Hacker
Module 08
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


3
Sniffing Tools


2
Sniffing Techniques


4
Countermeasures


5
Sniffing Detection Techniques

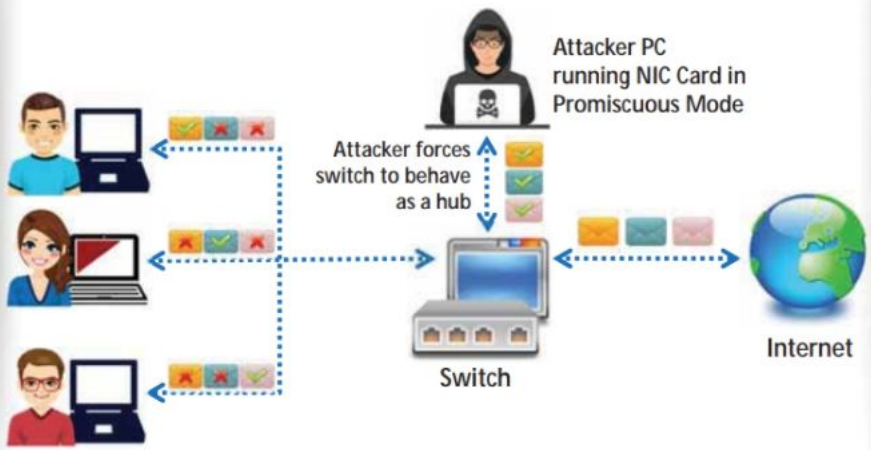
Network Sniffing

PacketSniffing

- 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 SnifferWorks

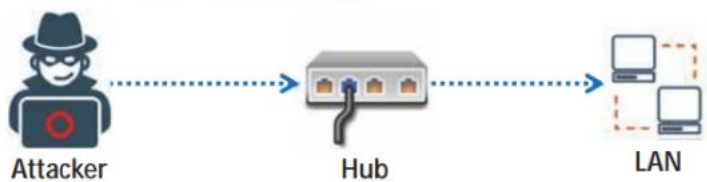
- A sniffer turns the NIC of a system to the promiscuous mode so that it listens to all the data transmitted on its segment



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- Hub usage is an outdated approach.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
HTTP	Data is sent in clear text
POP	Passwords and data are sent in clear text
IMAP	Passwords and data are sent in clear text
SMTP and NNTP	Passwords and data are sent in clear text
FTP	Passwords and data are sent in clear text

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

VoyagerM4x Protocol Analyzer

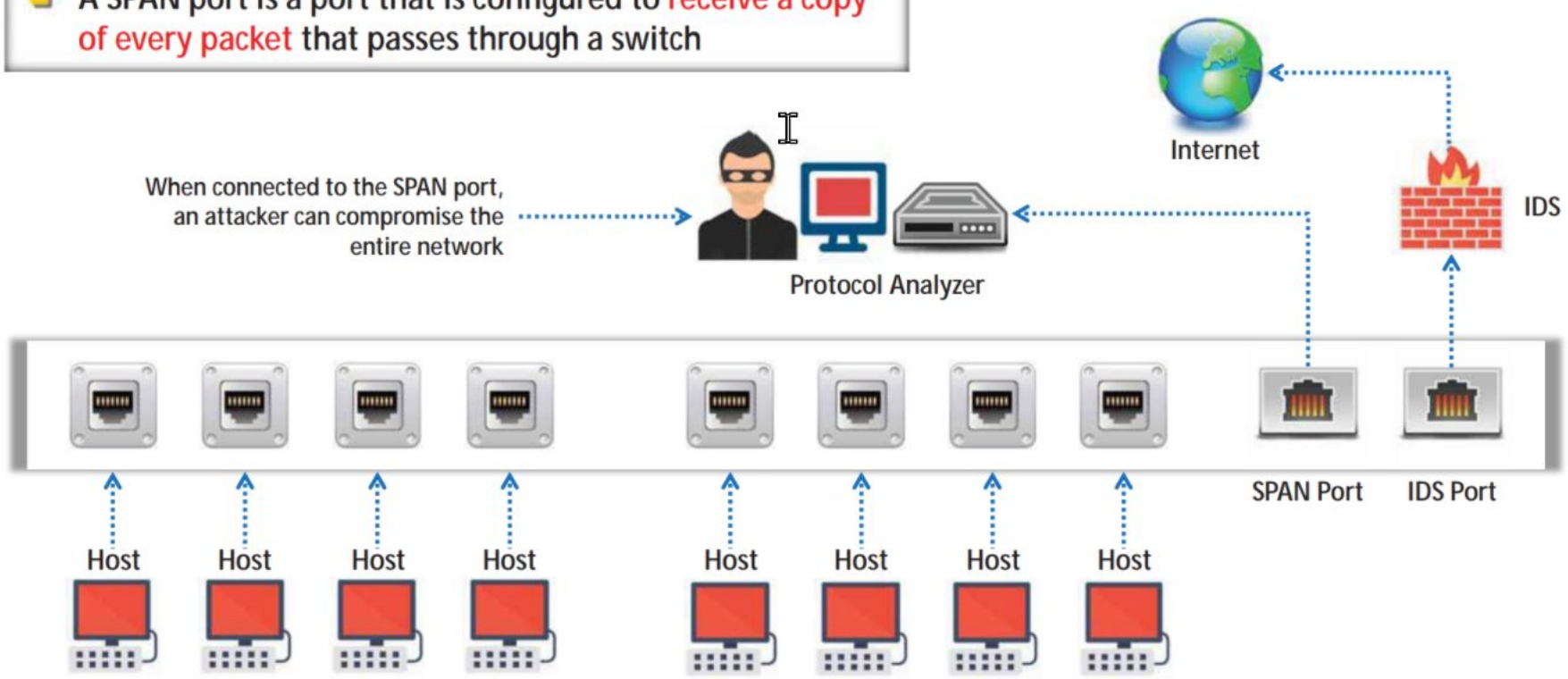
N2X N5540A Agilent Protocol Analyzer

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



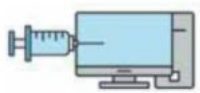
Wiretapping

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

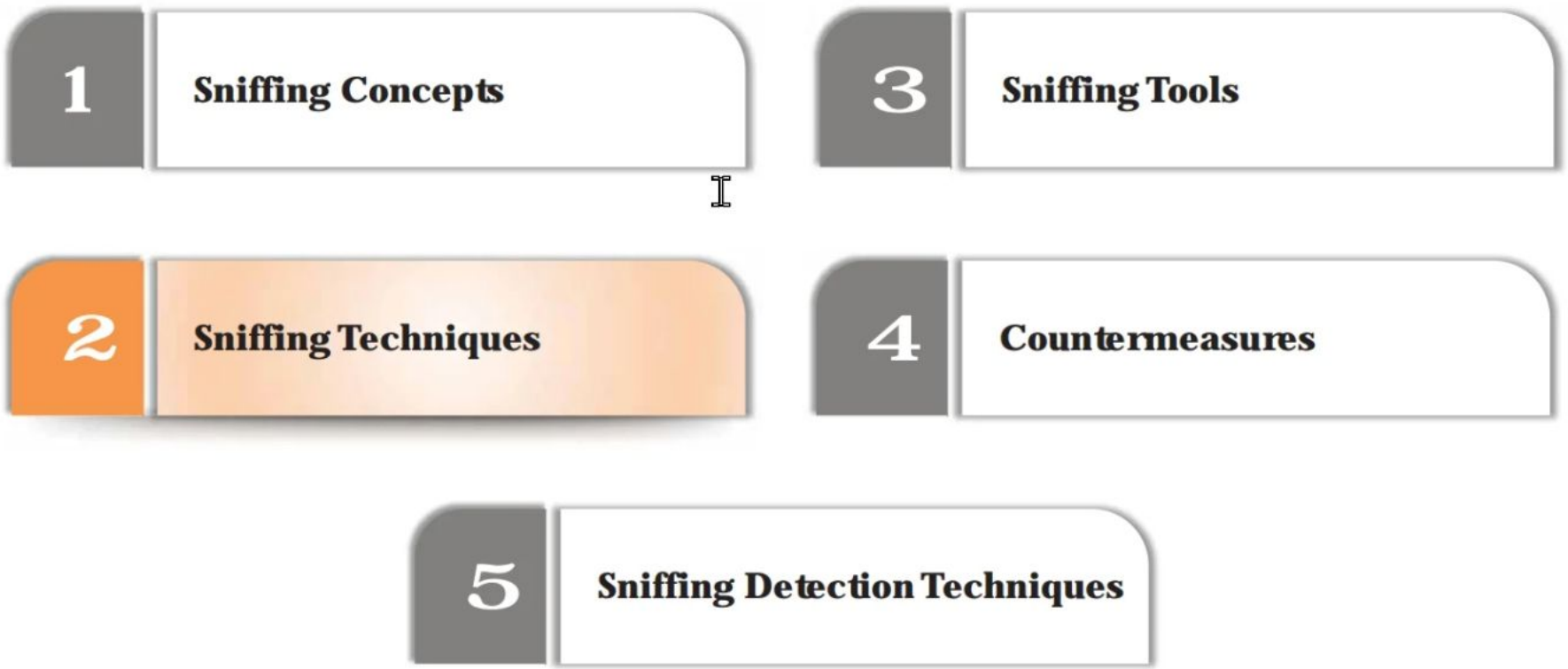


Passive Wiretapping

- 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

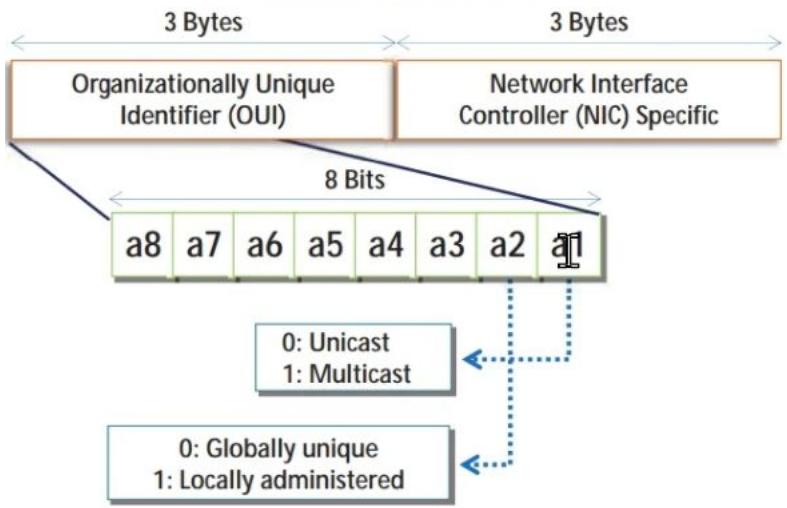
Module Flow


1
Sniffing Concepts
3
Sniffing Tools
2
Sniffing Techniques
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

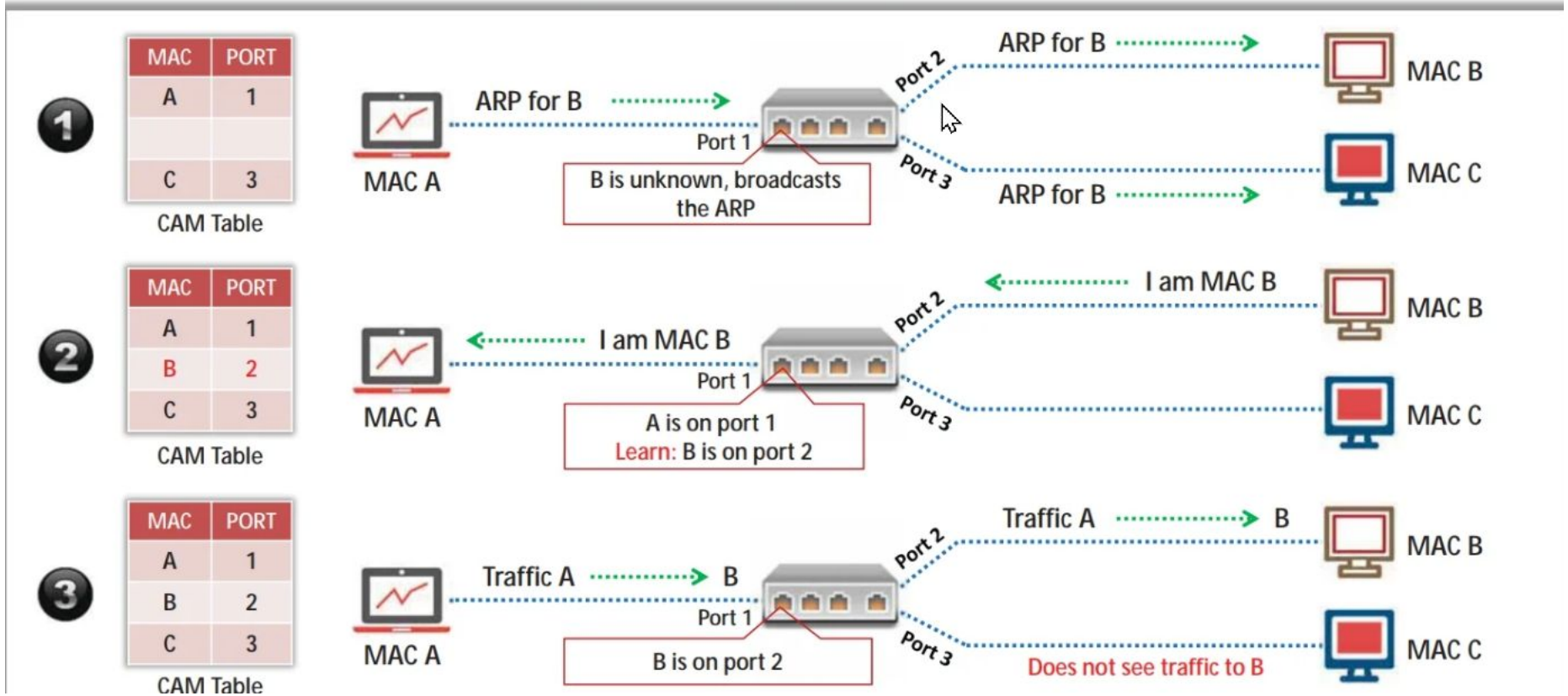
MAC Address



CAM Table

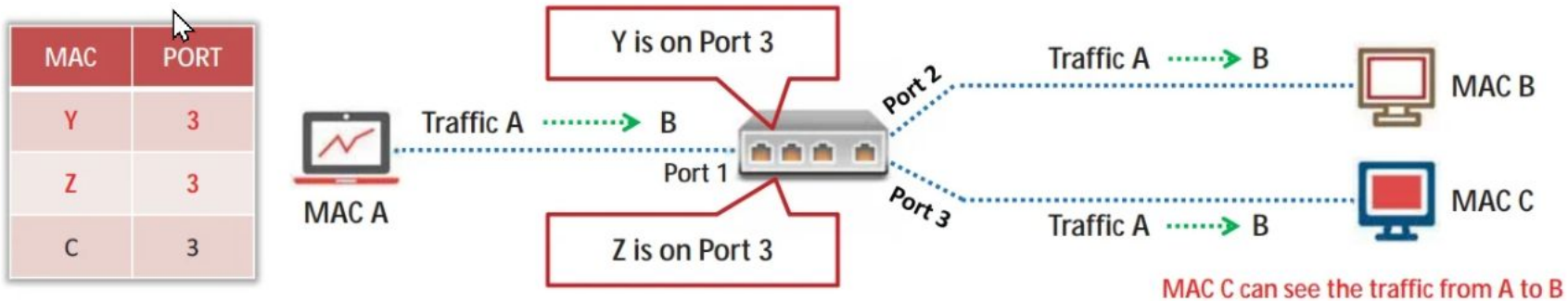
vlan	MAC Add	Type	Learn	Age	Ports
255	00d3.ad34.123g	Dynamic	Yes	0	Gi5/2
5	as23.df45.45t6	Dynamic	Yes	0	Gi2/5
5	er23.23er.t5e3	Dynamic	Yes	0	Gi1/6

How CAM Works



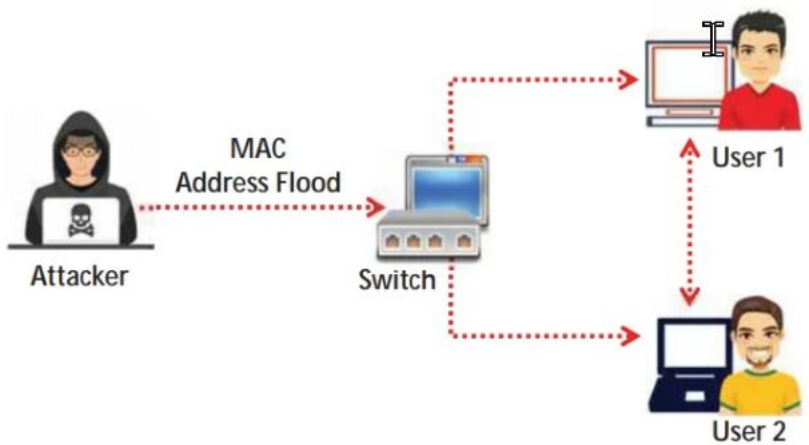
What Happens When a CAM Table Is Full?

- 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



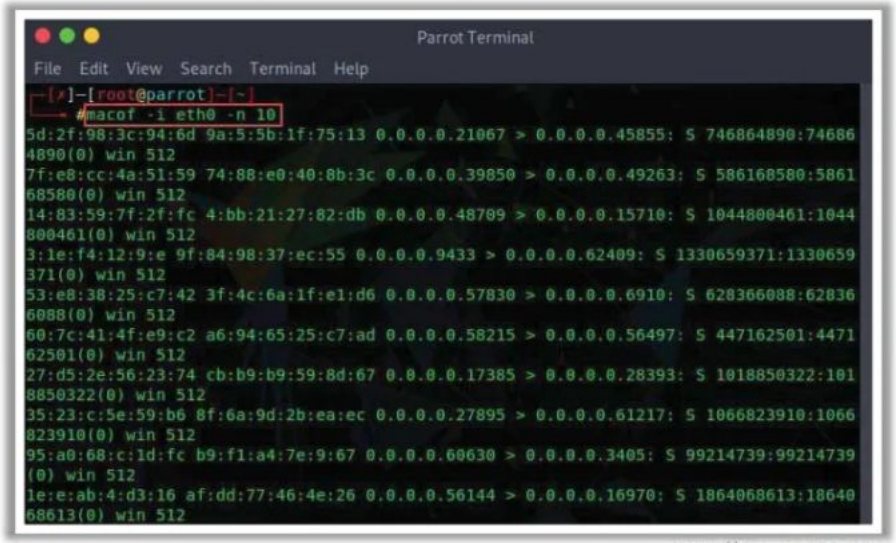
MAC Flooding

- 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

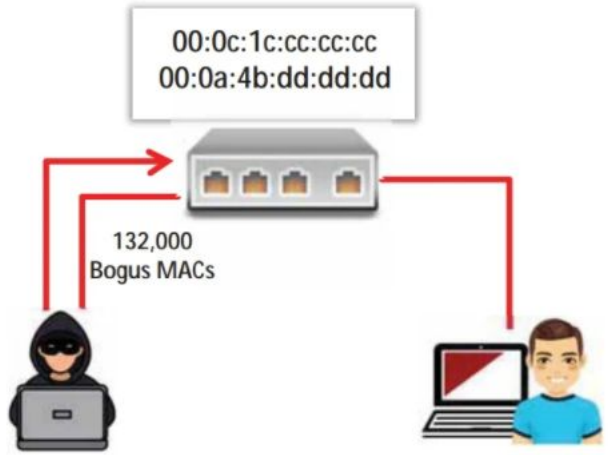


Mac Flooding Switches with macof

- 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

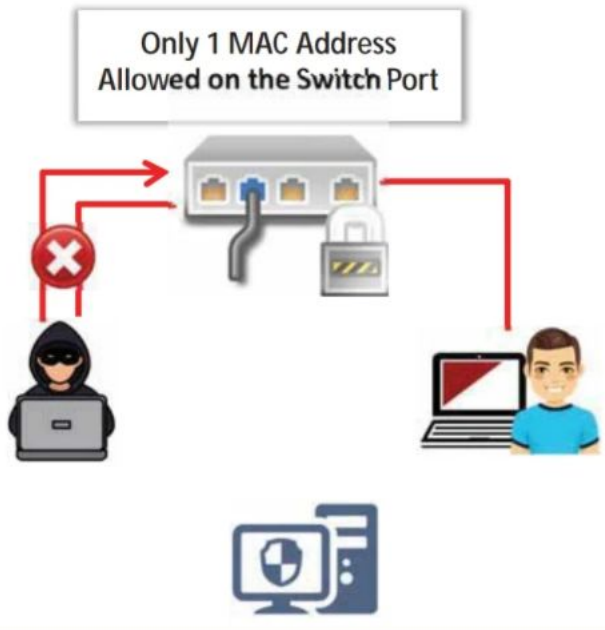


How to Defend against MAC Attacks



Configuring PortSecurity on Cisco Switch:

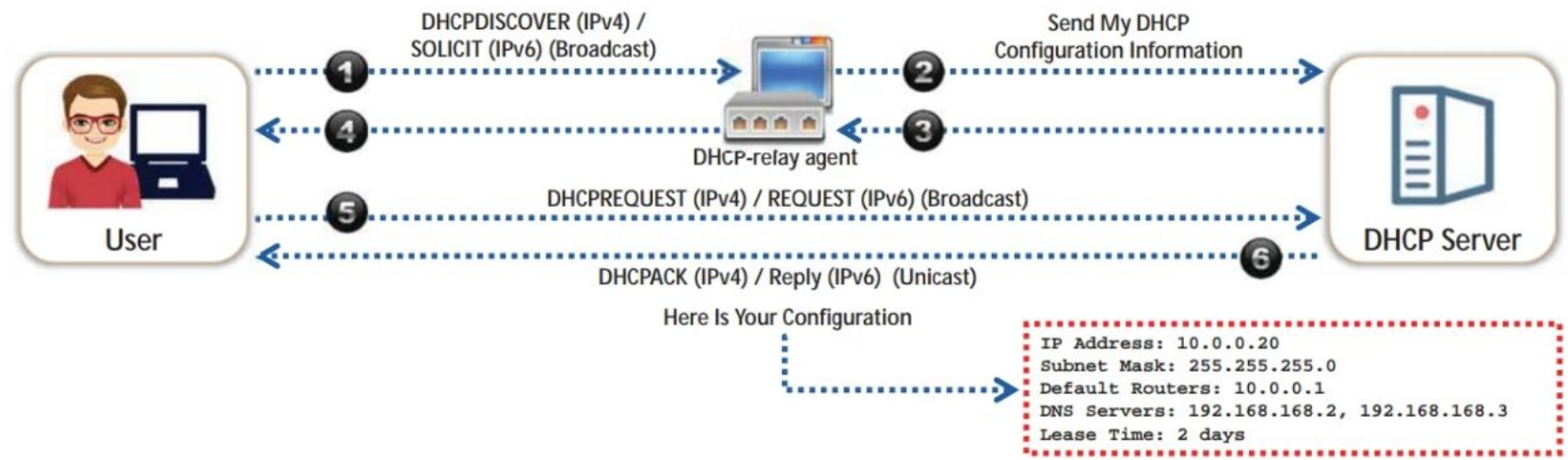
- switchport port-security
- switchport port-security maximum 1 vlan access
- switchport port-security violation restrict
- switchport port-security aging time 2
- switchport port-security aging type inactivity
- snmp-server enable traps port-security trap-rate 5



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

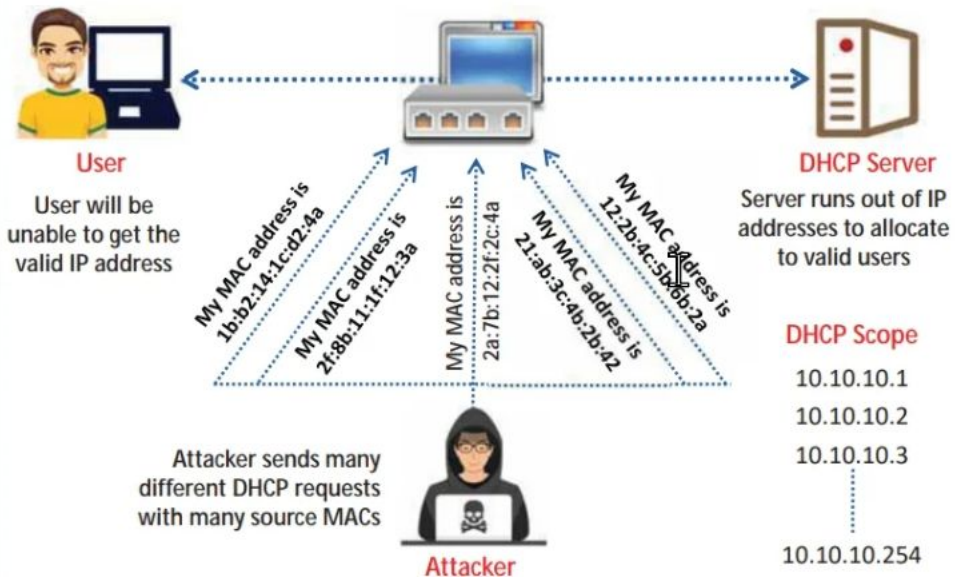
How DHCP Works

- 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

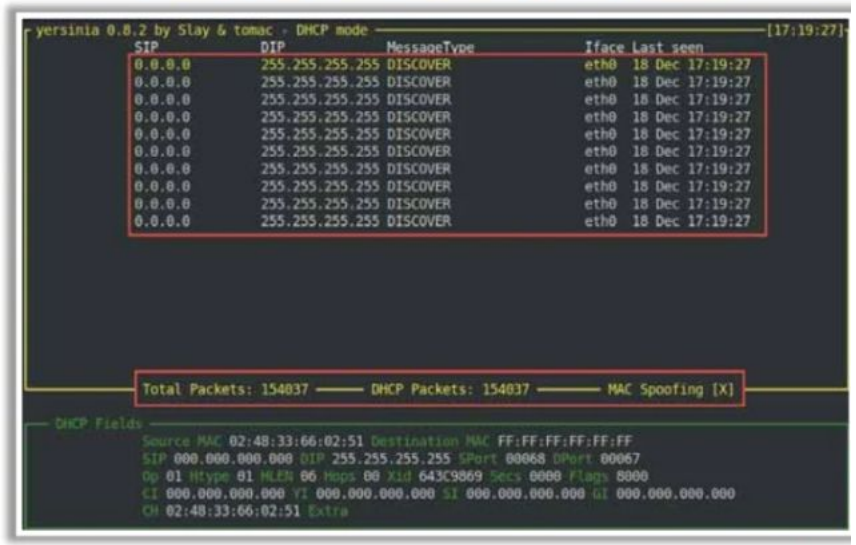


DHCP Starvation Attack

- 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



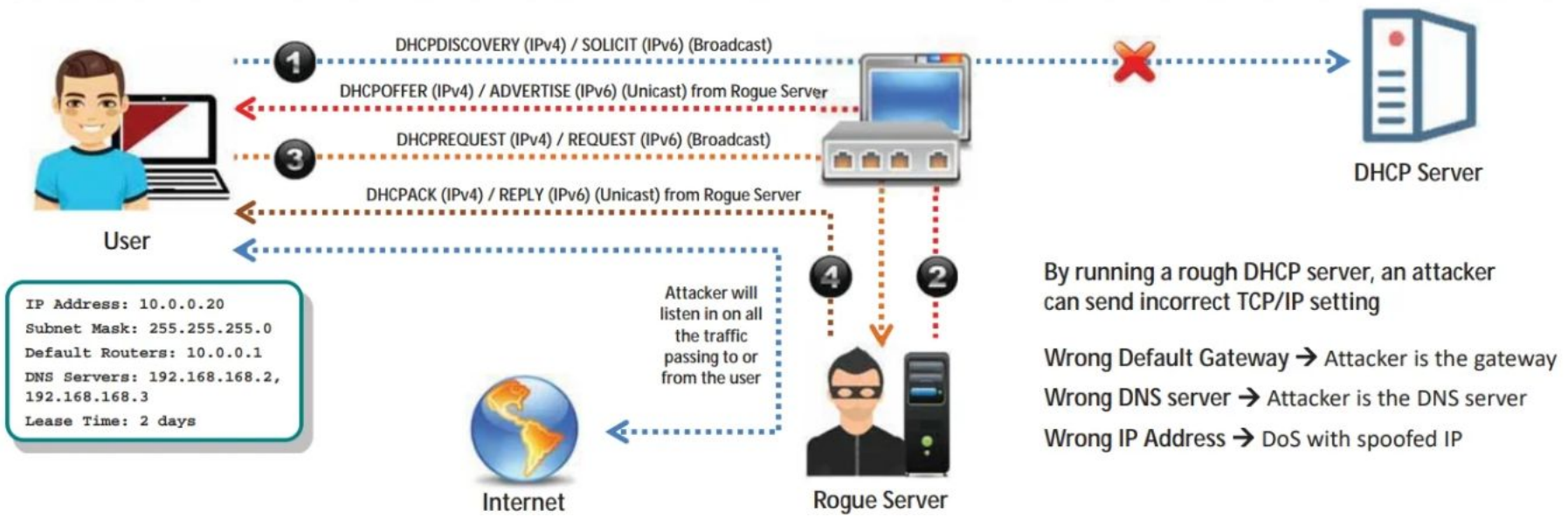
https://sourceforge.net

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

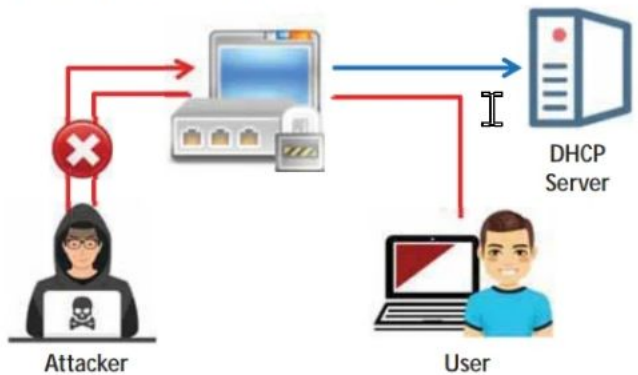
Wrong Default Gateway → Attacker is the gateway

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

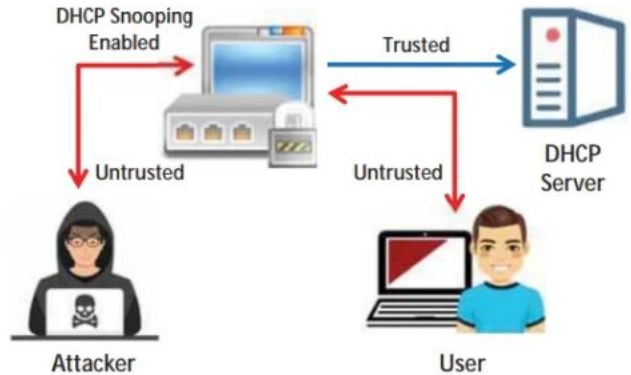
- Enable port security to defend against DHCP starvation attacks
  - Configuring the MAC limit on the switch's edge ports drops the packets from further MACs once the limit is reached



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



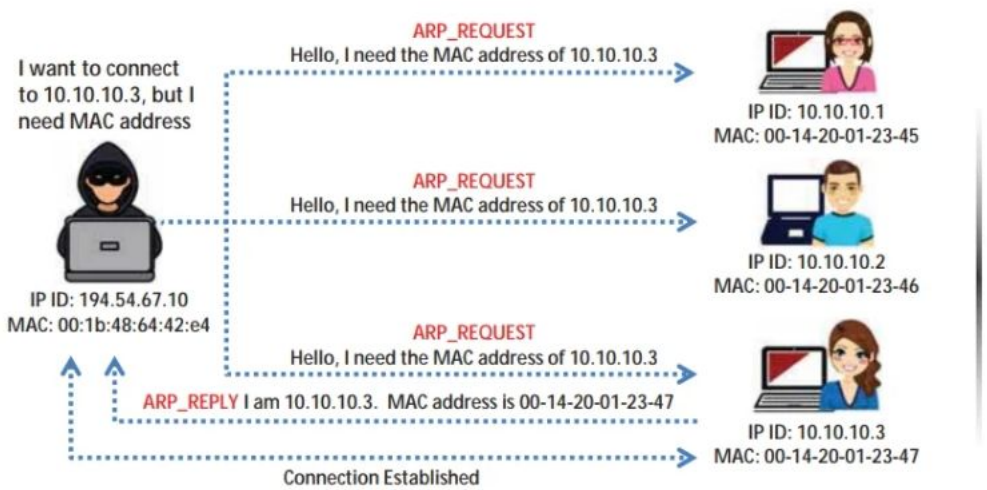
IOS Global Commands

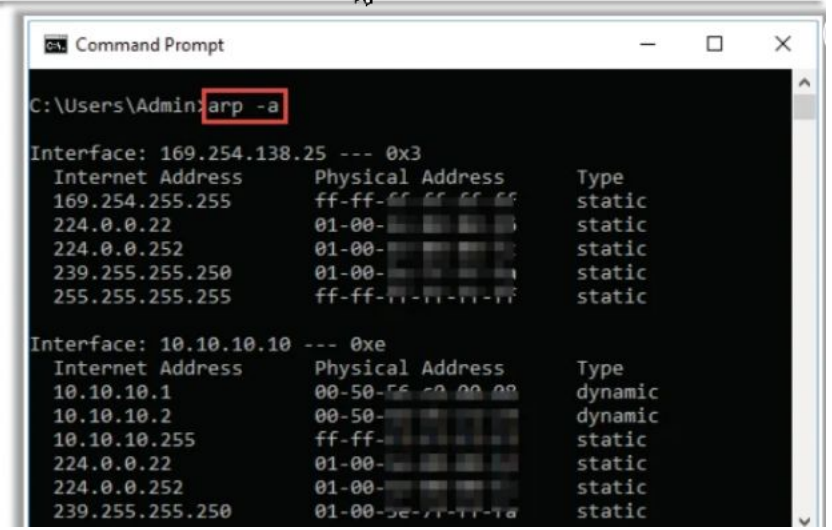
- **`ip dhcp snooping`** → this turns on DHCP snooping
- **`ip dhcp snooping vlan 4,104`** → this configures VLANs to snoop
- **`ip dhcp snooping trust`** → this configures interface as trusted

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

What Is Address Resolution Protocol (ARP)?

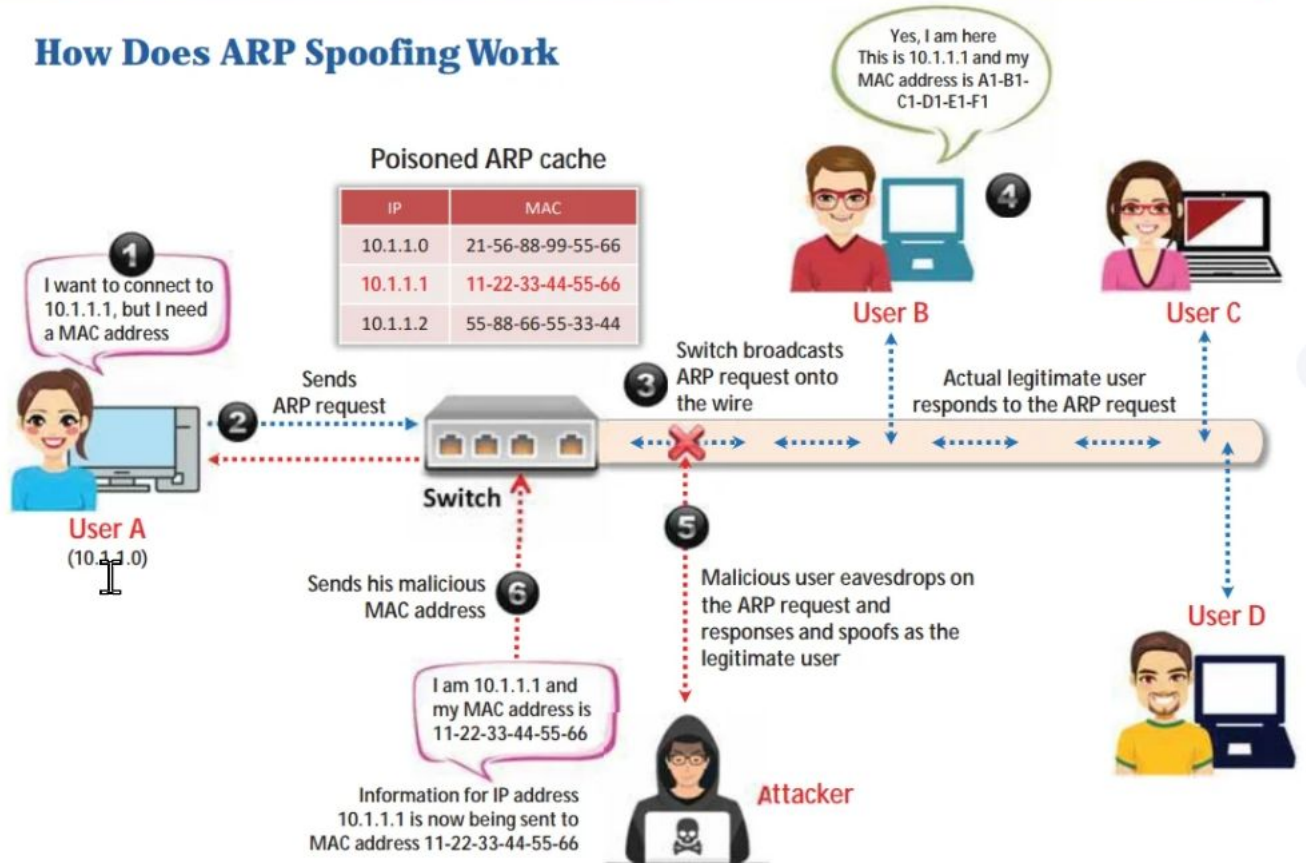
- Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine (MAC) addresses
- All network devices (that need to communicate on the network) broadcast ARP queries on the network to discover other machines' MAC addresses
- When one machine needs to communicate 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



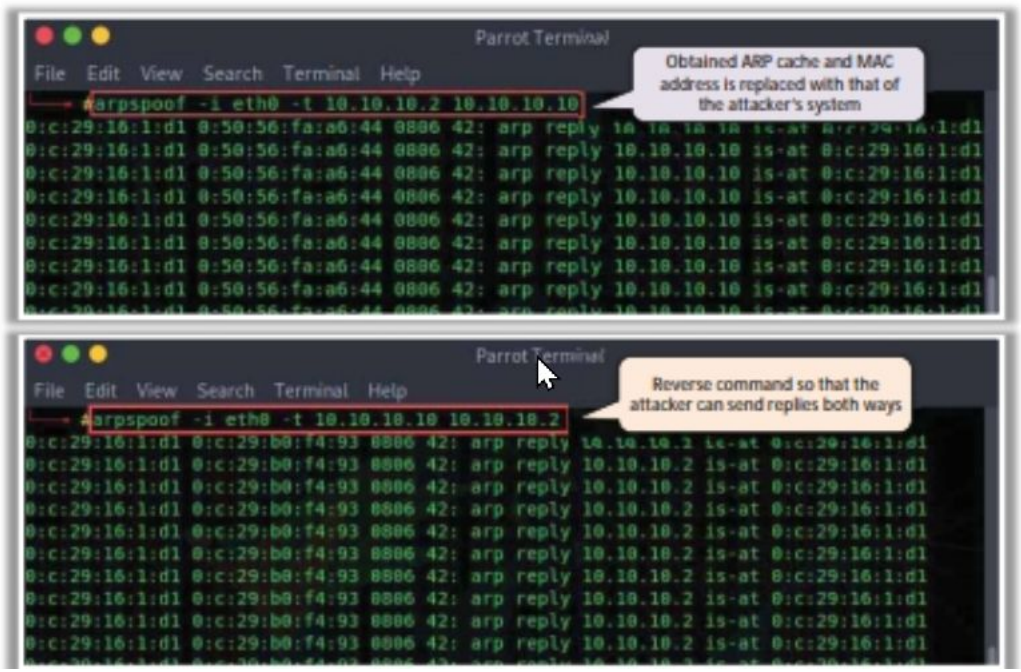
Threats of ARP Poisoning

- 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
2. Session Hijacking
3. VoIP Call Tapping
4. Manipulating Data
5. Man-in-the-Middle Attack
6. Data Interception
7. Connection Hijacking
8. Connection Resetting
9. Stealing Passwords
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

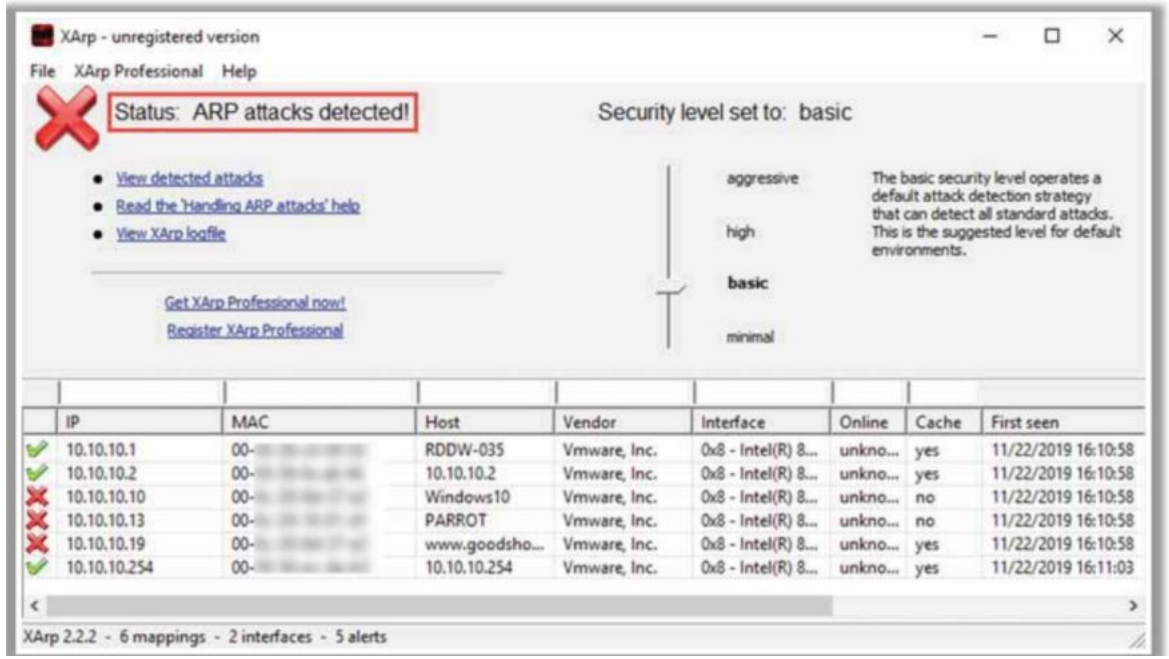


- **BetterCAP** — *https://www.bettercap.org*
- **Ettercap** — *http://www.ettercap-project.org*
- **dsniff** — *https://www.monkey.org*
- **MITMf** — *https://github.com*
- **Arpoison** — *https://sourceforge.net*

ARP Spoofing Detection Tools

XArp

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



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

ArpON
https://sourceforge.net

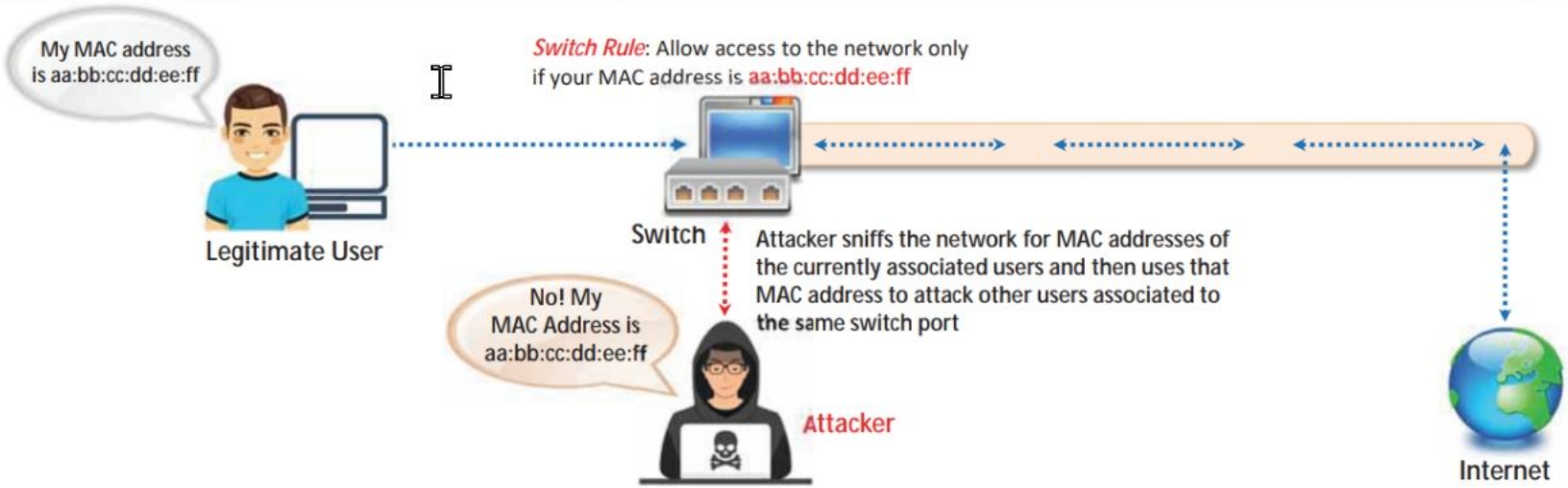
ARP AntiSpoofer
https://sourceforge.net

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

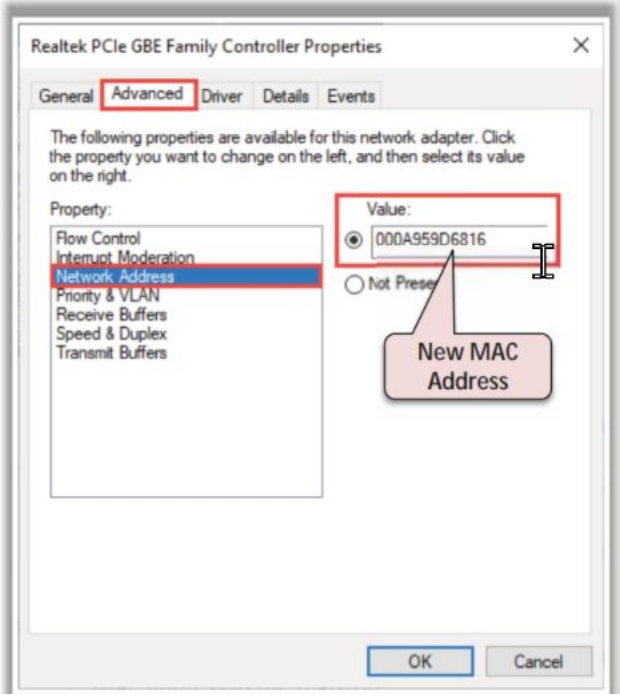


Note: This technique can be used to bypass Wireless Access Points' MAC filtering

MAC Spoofing Technique: Windows

In Windows 10OS

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)

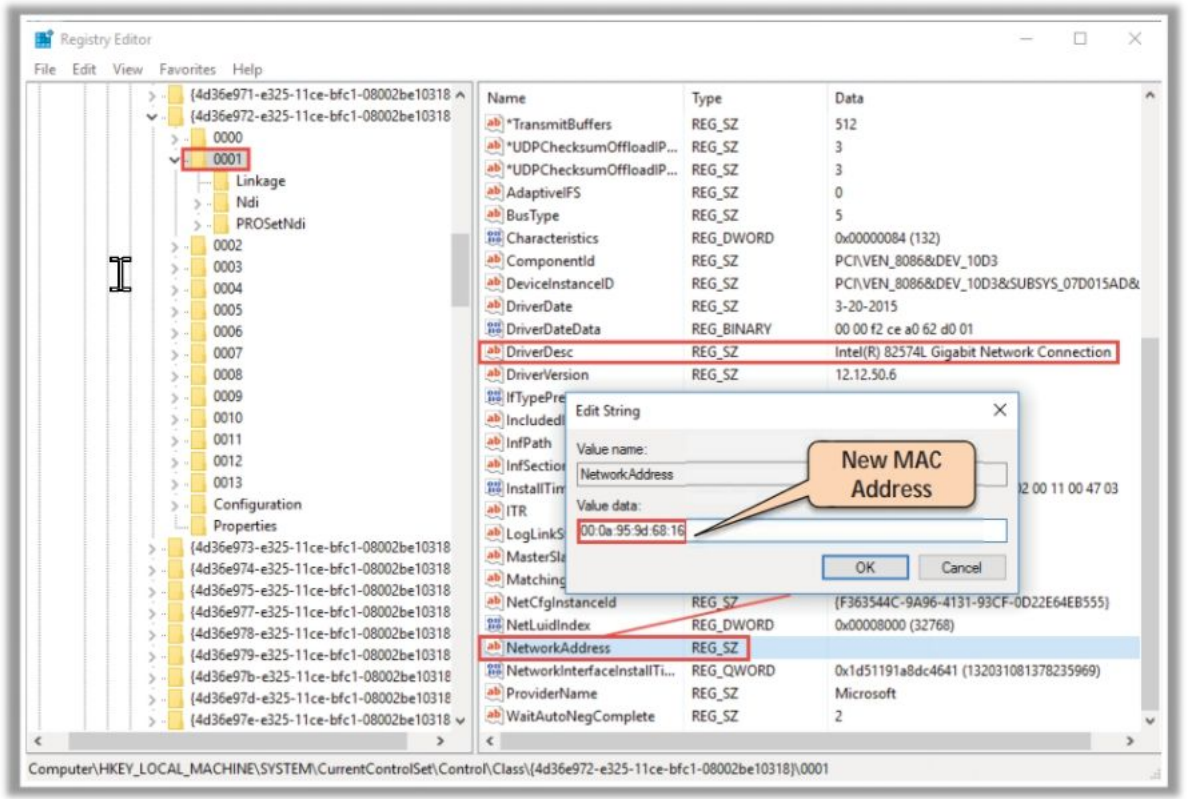
MAC Spoofing Technique: Windows (Cont'd)

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

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

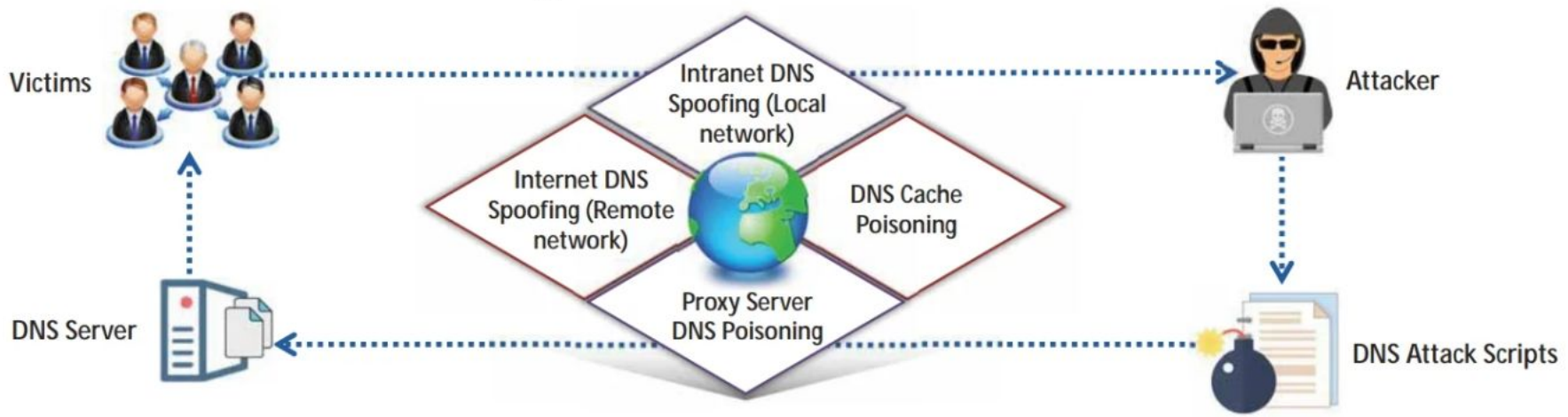
  Note: Do not type **Regedit** to start the registry editor

- 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



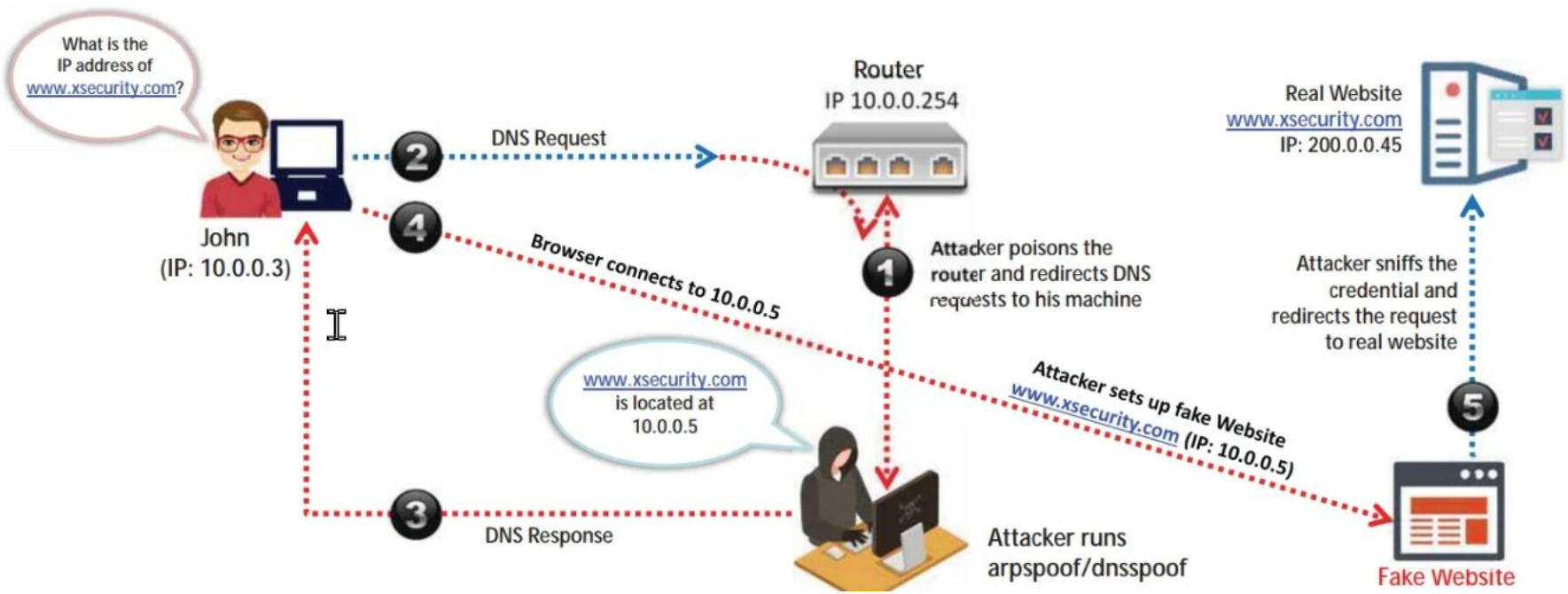
DNS Poisoning Techniques

- 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



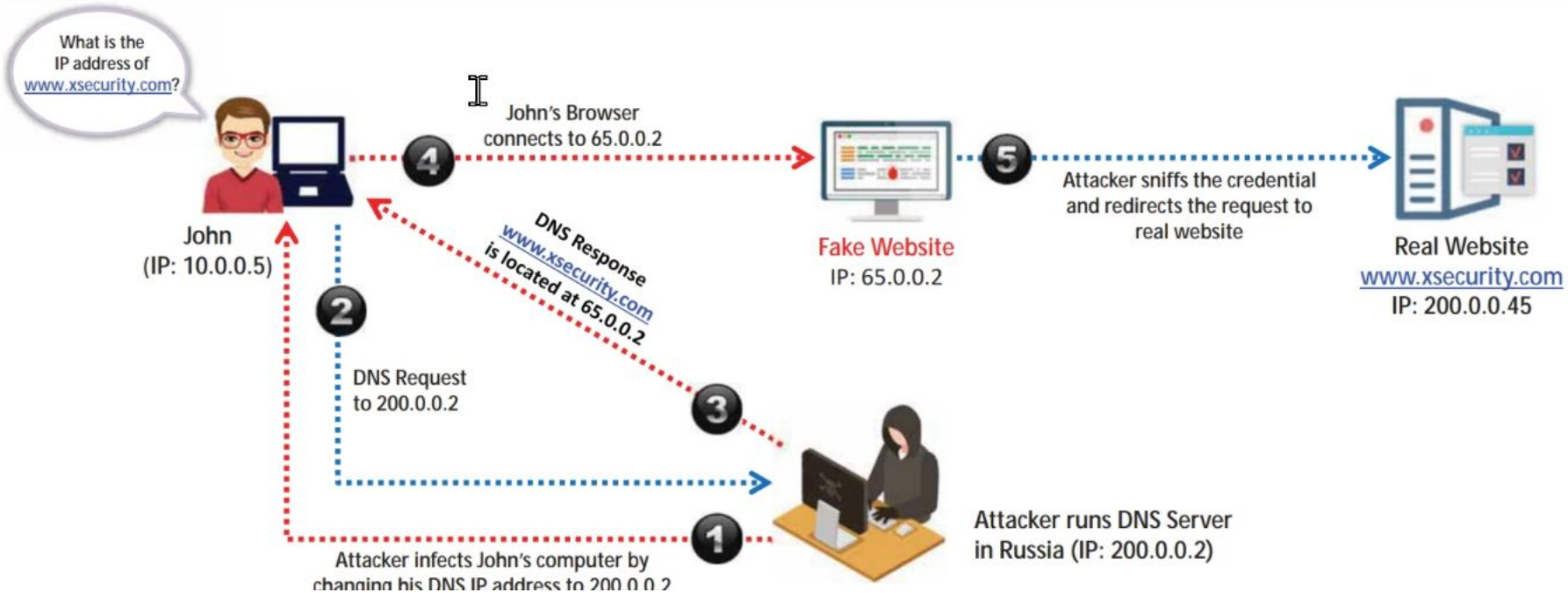
Intranet DNS Spoofing

- 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



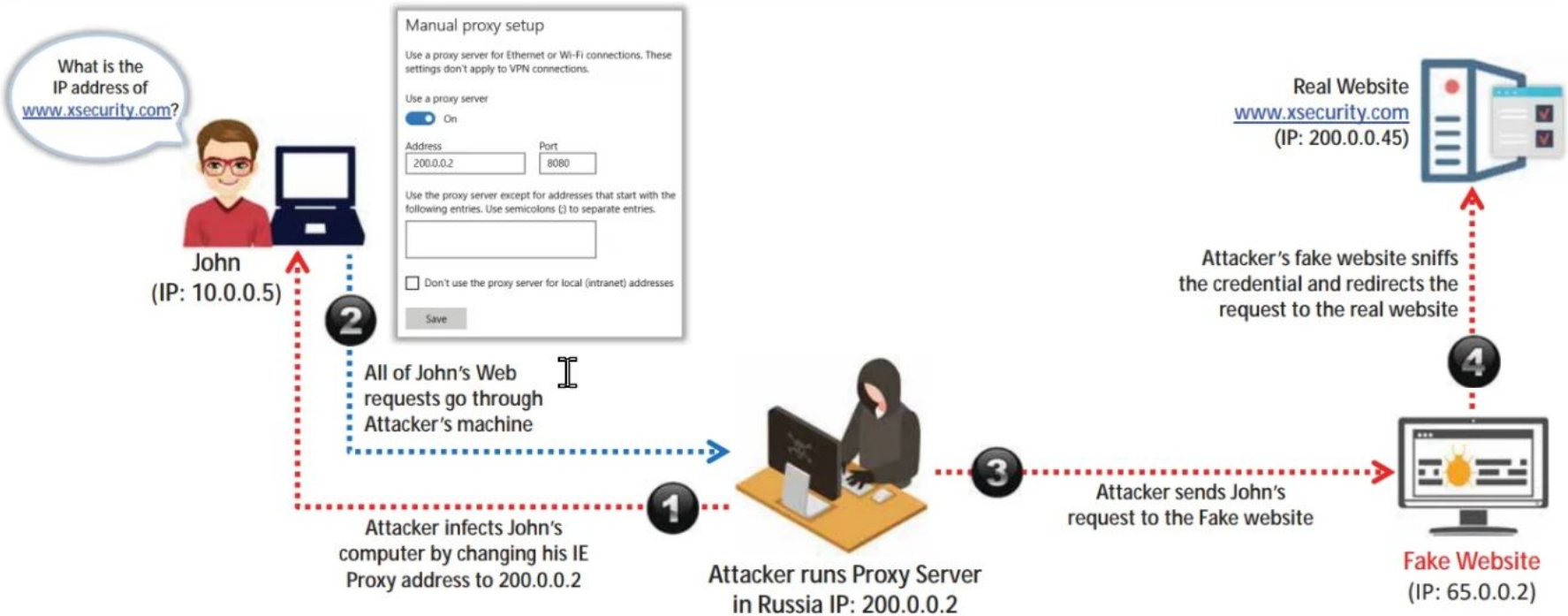
Internet DNS Spoofing

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

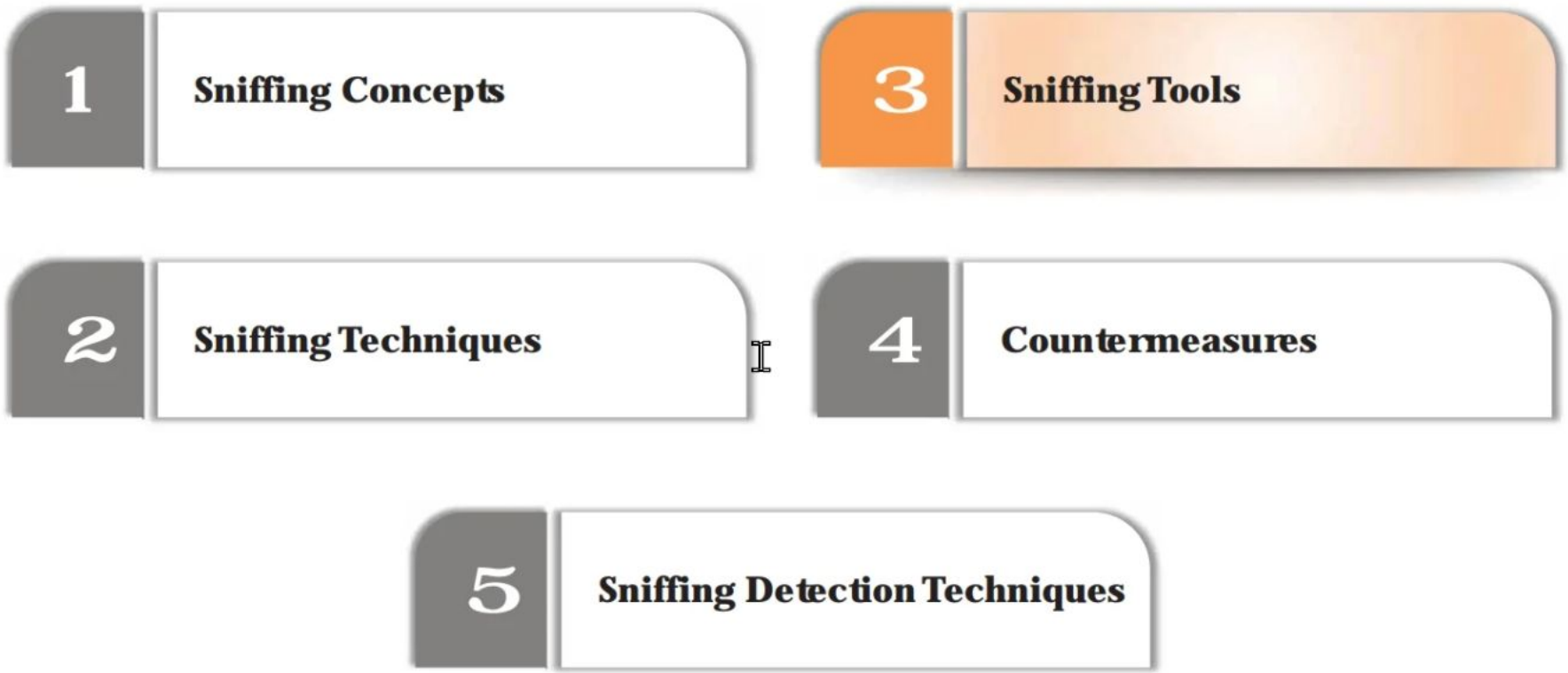


Proxy Server DNS Poisoning

- 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

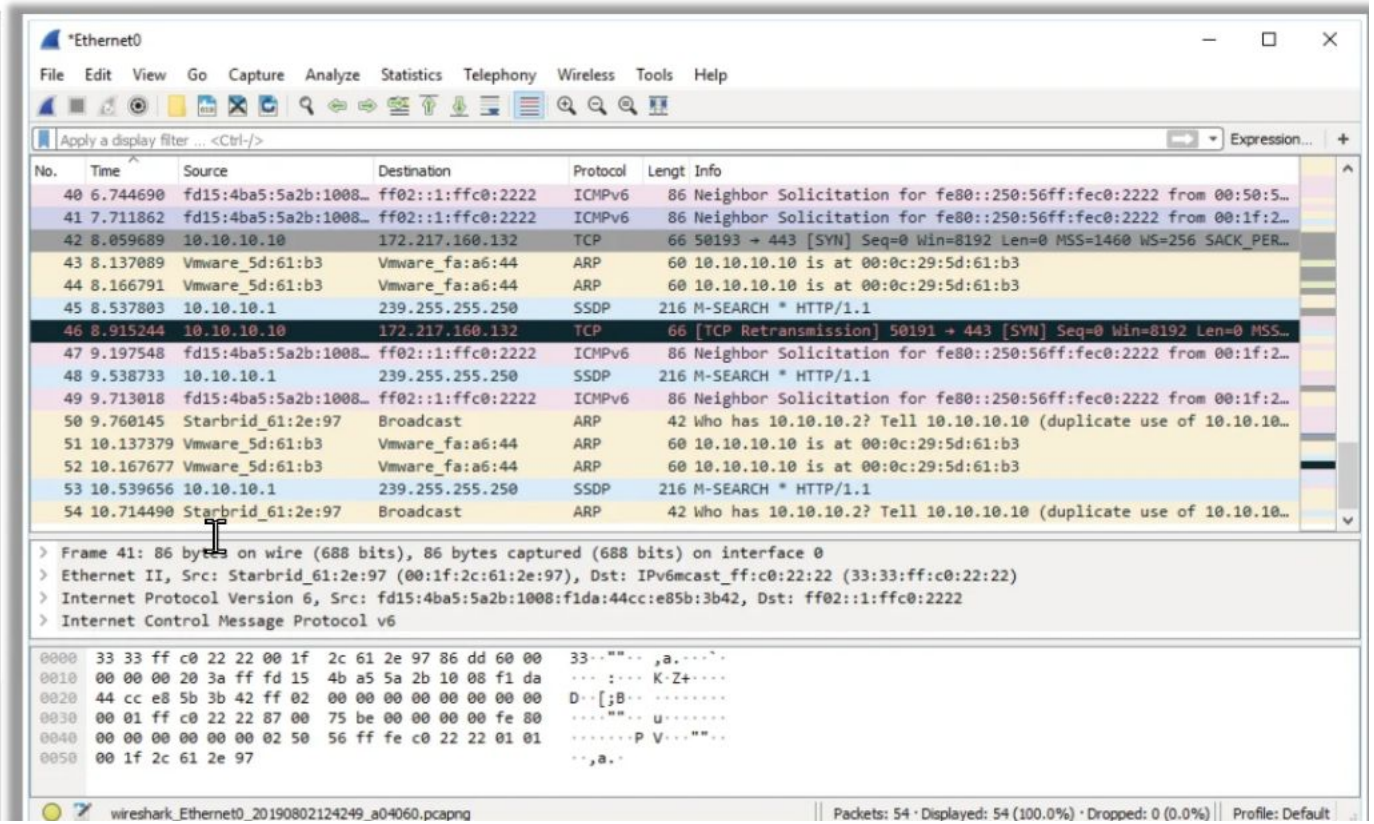


Module Flow

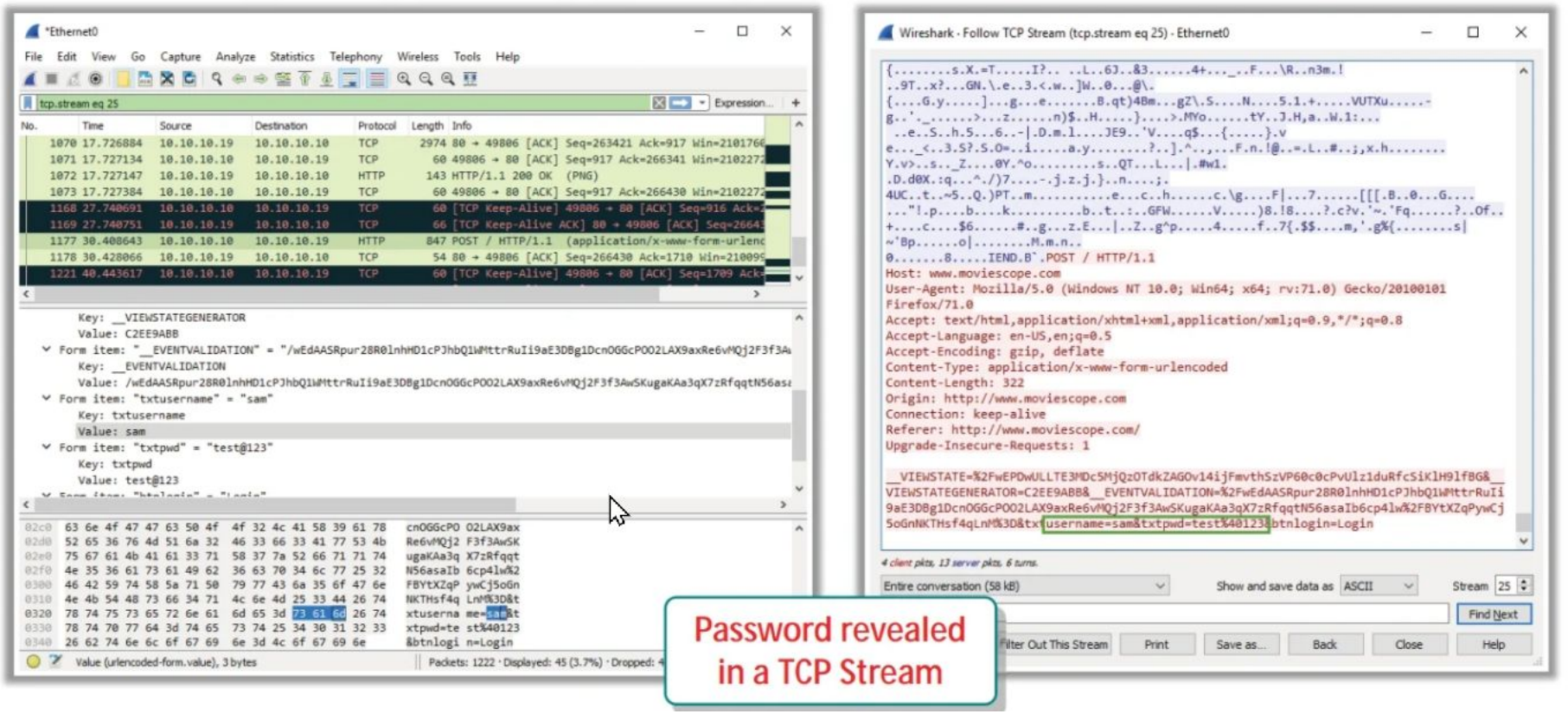

1
Sniffing Concepts
3
Sniffing Tools
2
Sniffing Techniques
4
Countermeasures
5
Sniffing Detection Techniques

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



Follow TCP Stream in Wireshark



Display Filters in Wireshark

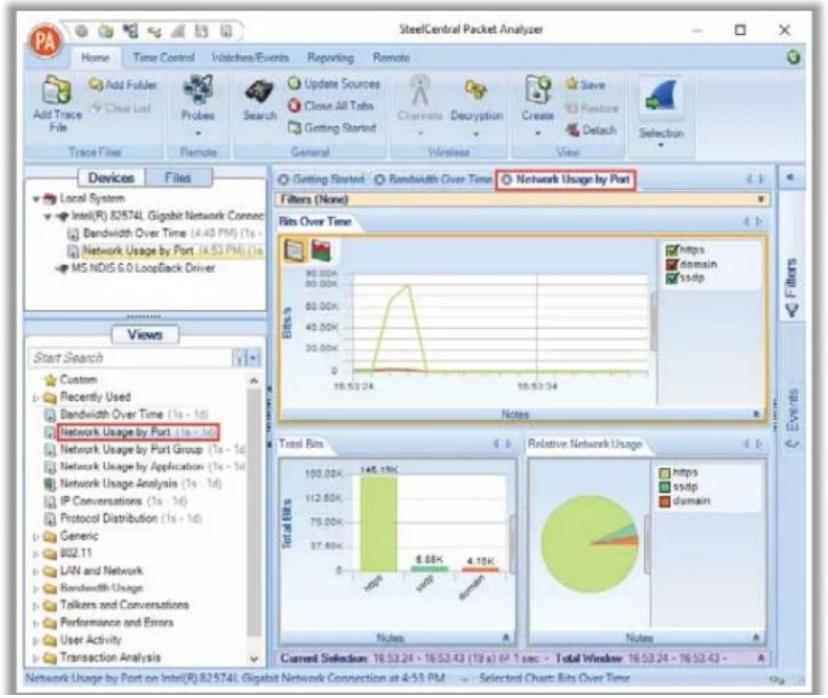
Display filters are used to change the view of packets in the captured files

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

Sniffing Tools

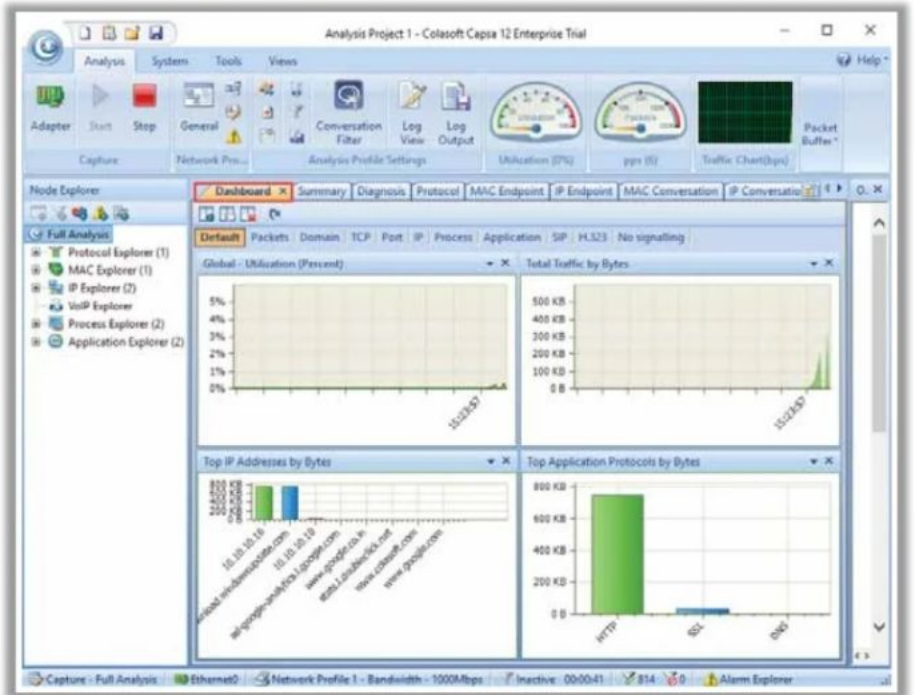
SteelCentral Packet Analyzer

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



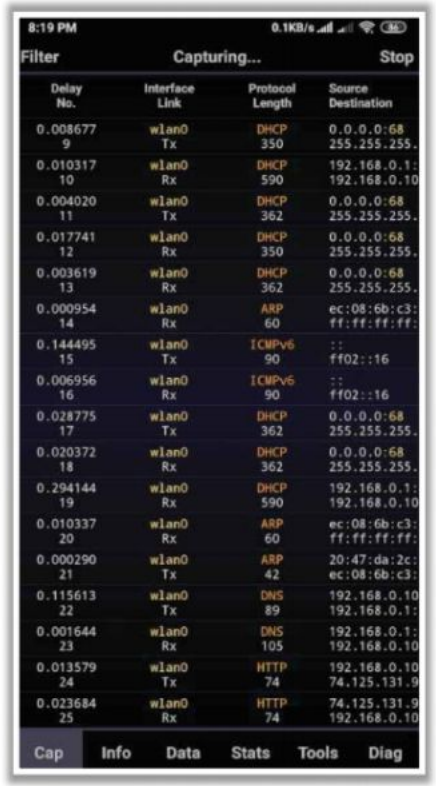
Capsa Network Analyzer

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



Packet Sniffing Tools for Mobile Phones

SnifferWicap

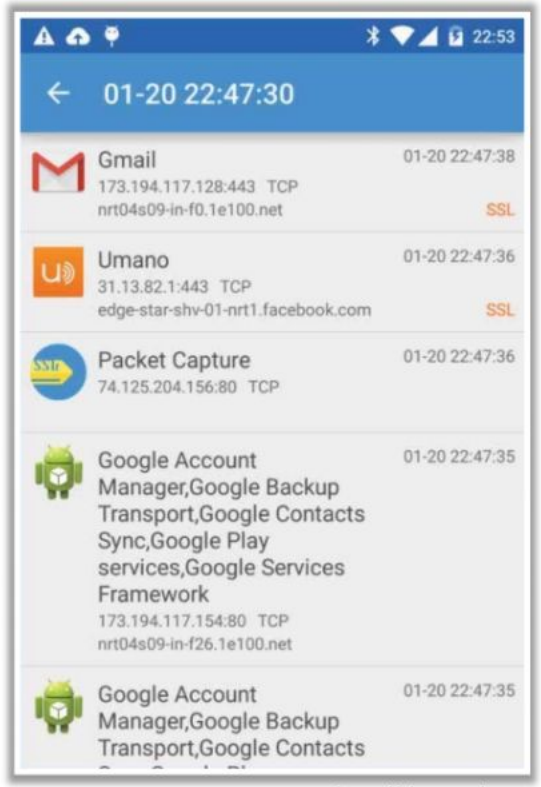


https://play.google.com

FaceNiff

http://faceniff.ponury.net

PacketCapture



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

Module Flow

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

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

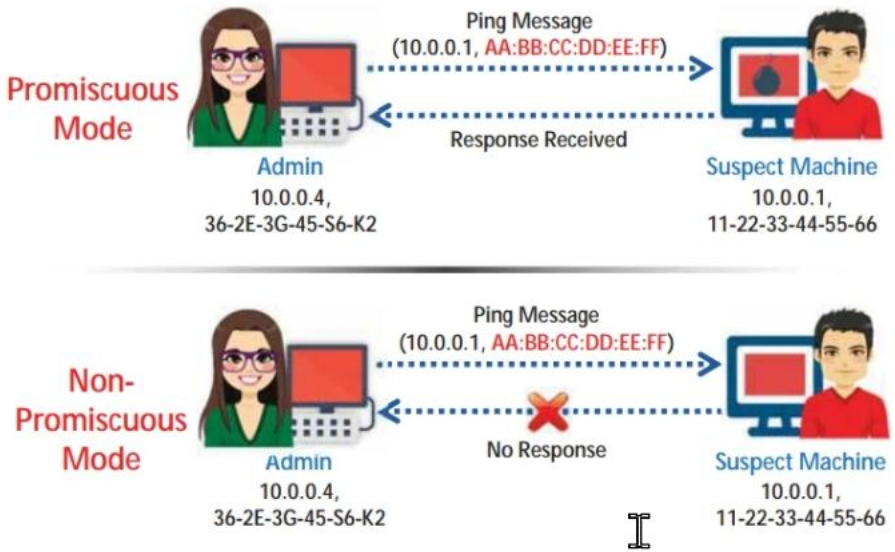
- Run IDS and see if the MAC address of any of the machines has changed (Example: router's MAC address)
- IDS can alert the administrator about suspicious activities

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

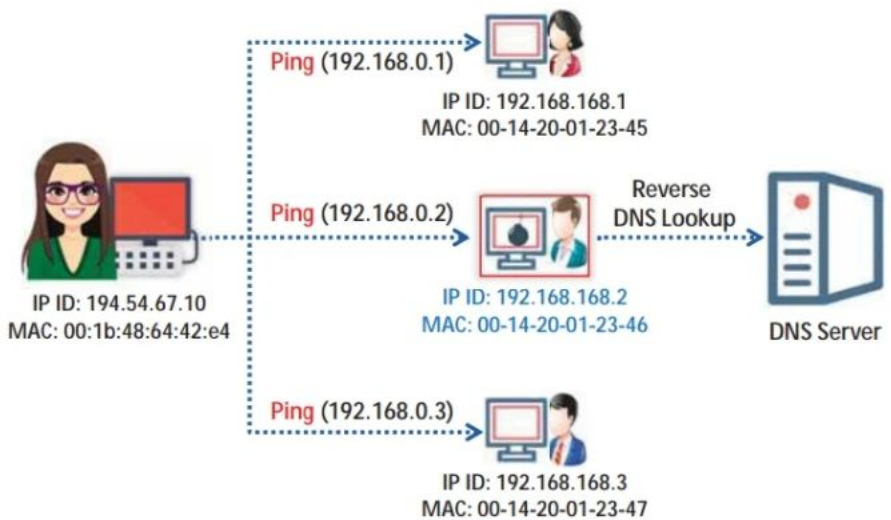
Ping Method



- 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

Promiscuous Detection Tools

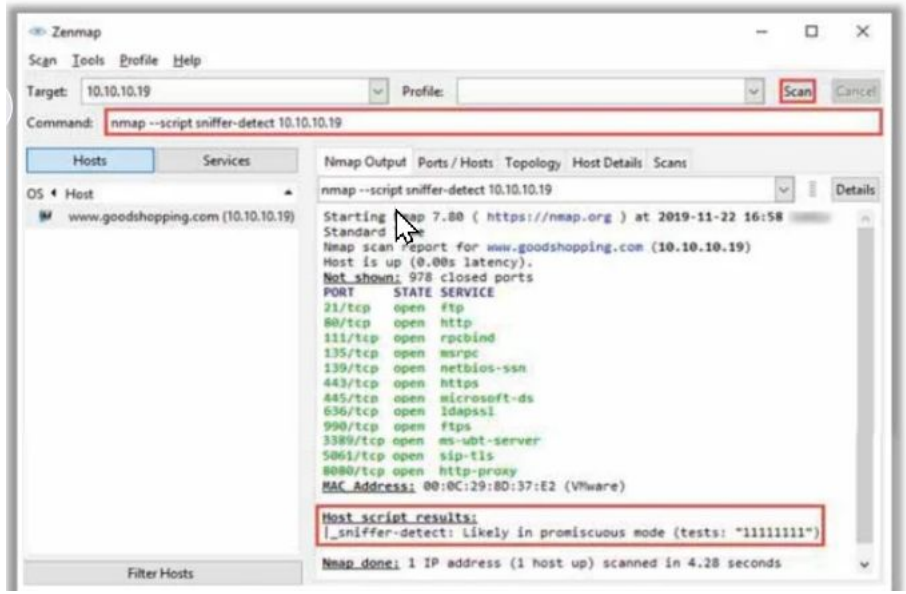
Nmap

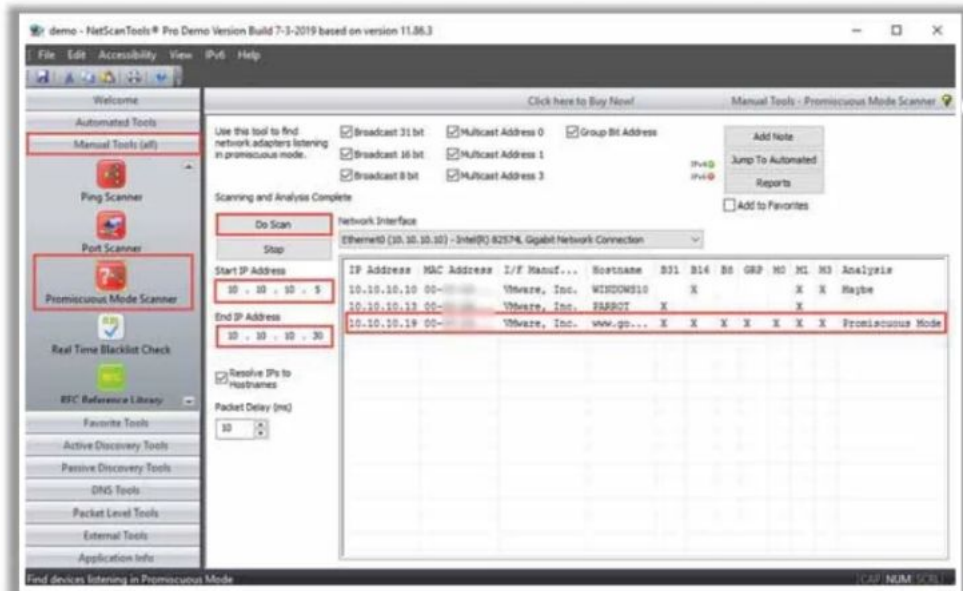
- Nmap's NSE script allows you to check if a system on a local Ethernet has its network card in the promiscuous mode
- Command to detect NIC in promiscuous mode:

```
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





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