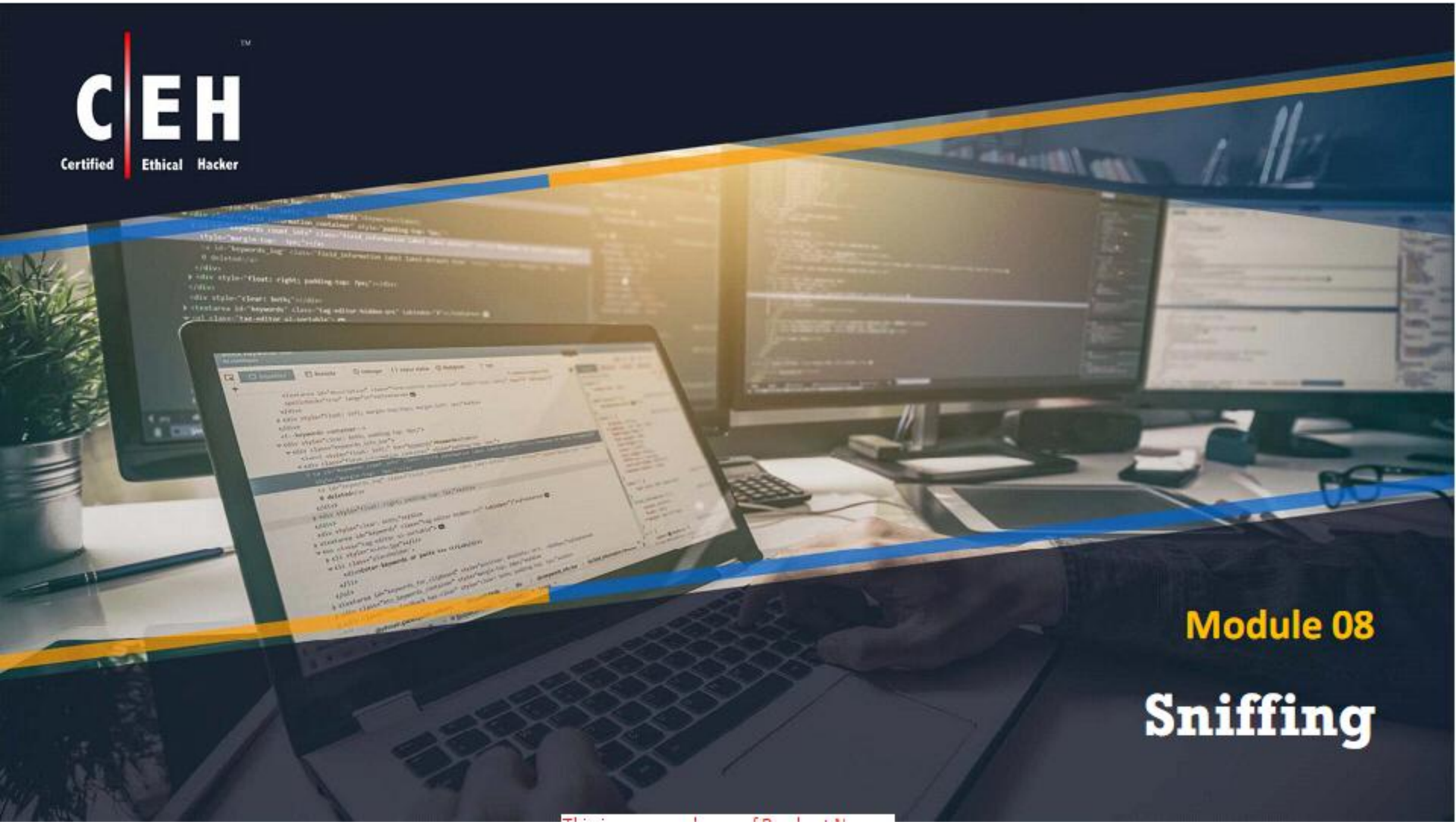

C|EH
Certified Ethical Hacker
Module 08
Sniffing

Module Objectives

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 to Detect Sniffing
- Overview of Sniffing Penetration Testing

Module Flow

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

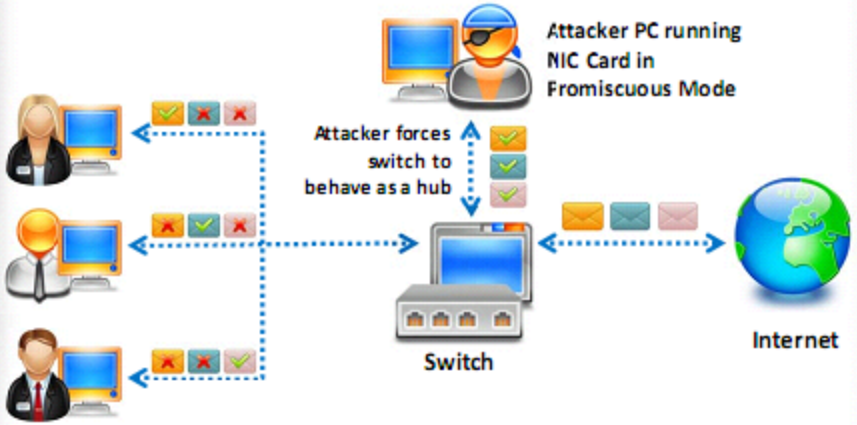
Network Sniffing

Packet Sniffing

- Packet sniffing is a 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 password, chat sessions, account information, etc.

How a Sniffer Works

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



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 use 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- Hub usage is an outdated approach.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

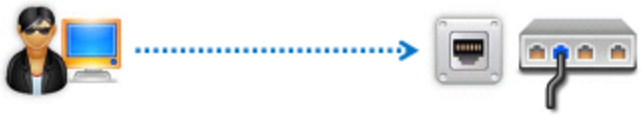
- Active sniffing is used to sniff a **switch-based network**
- Active sniffing involves **injecting Address Resolution Packets (ARP)** into the network to flood the switch's Content Addressable Memory (CAM) table, which keeps track of host-port connection

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 laptop to a switch port



2. He runs discovery tools to learn about network topology

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

4. He poisons the victim machine by using ARP spoofing techniques

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

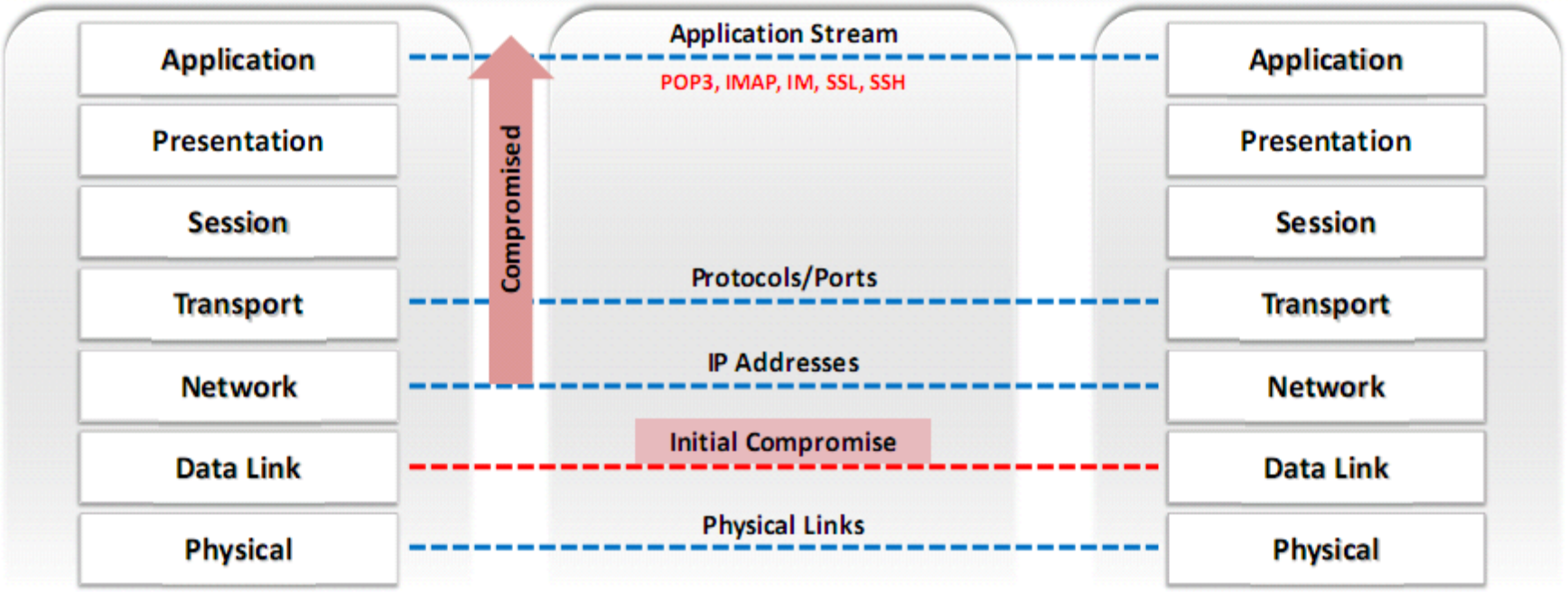
6. The hacker extracts passwords and sensitive data from the redirected traffic

Protocols Vulnerable to Sniffing

Telnet and Rlogin	Keystrokes including user names 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 layer 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

N2X N5540A Agilent Protocol Analyzer

https://www.valuetronics.com

Keysight E2960B

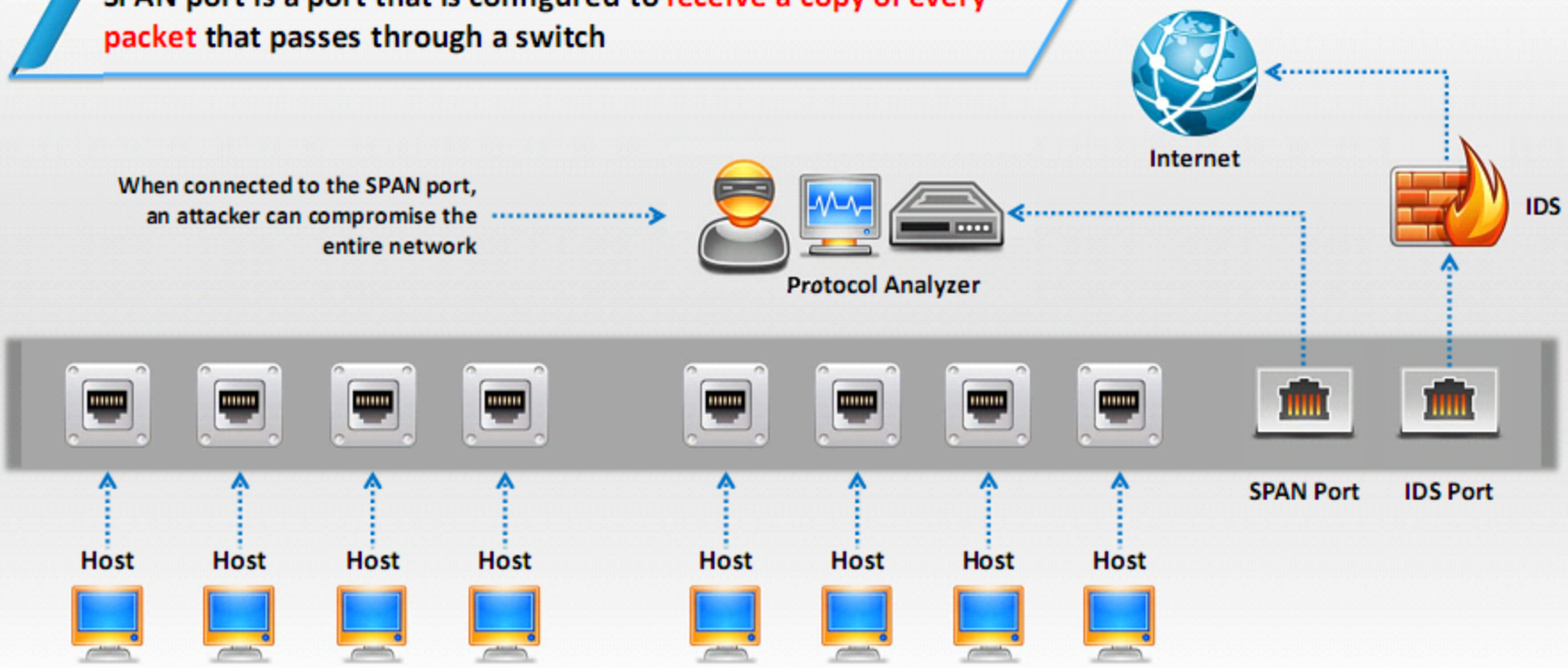
http://www.keysight.com

Hardware Protocol Analyzers

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

SPAN Port

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 monitoring **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

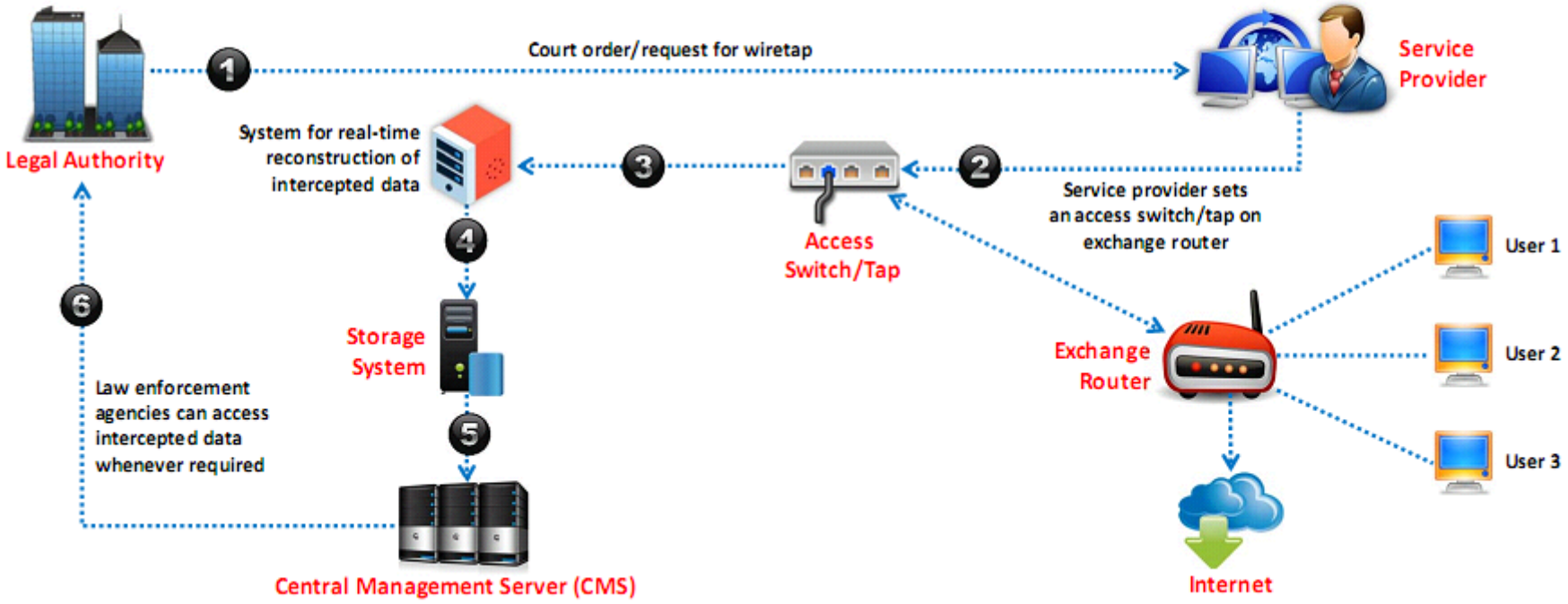
Passive Wiretapping

- It only monitors and records the traffic and collects knowledge of 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

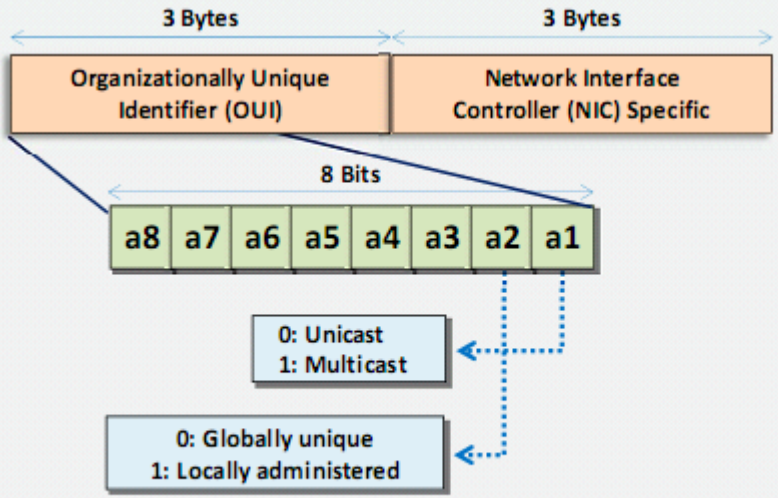
1. Sniffing Concepts
2. Sniffing Techniques
3. Sniffing Tools
4. Countermeasures
5. Sniffing Detection Techniques
6. Sniffing Pen Testing

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

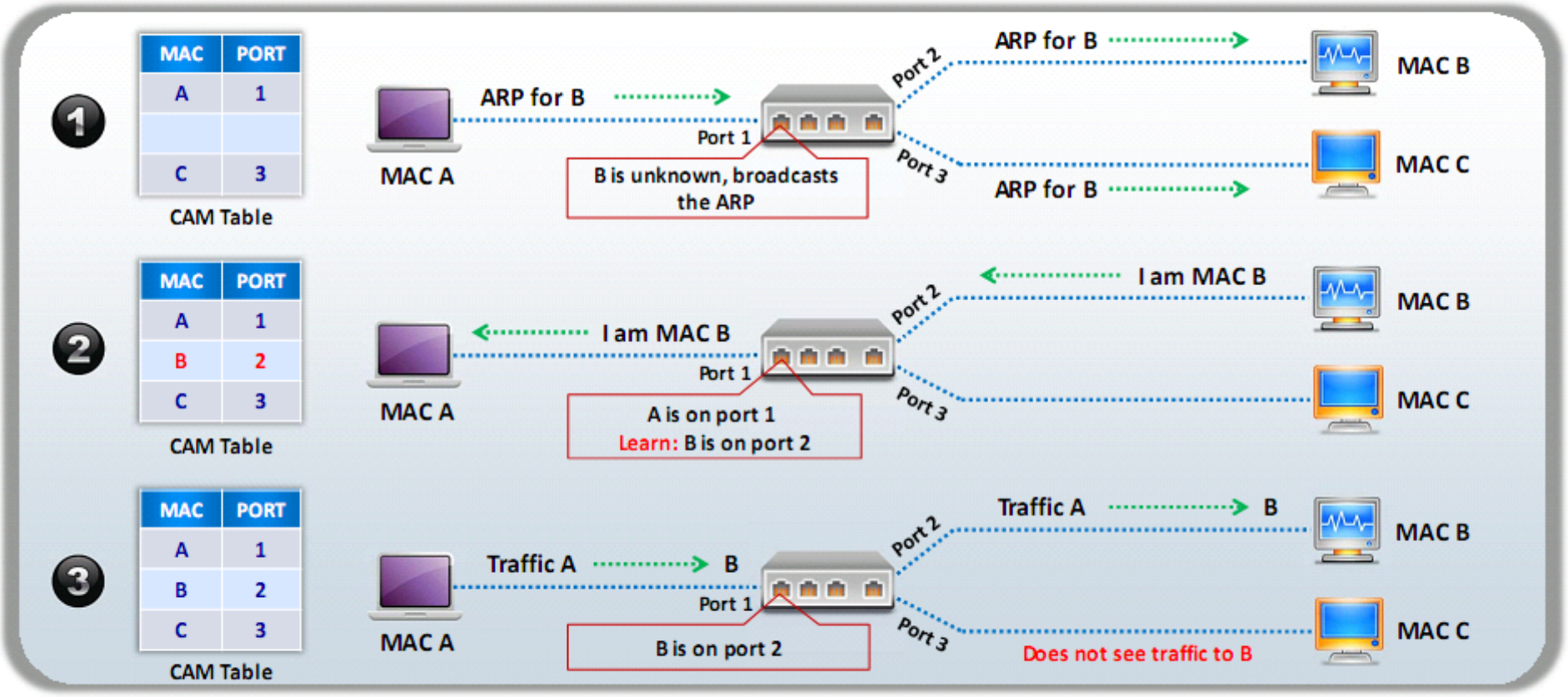
MAC Address



CAM Table

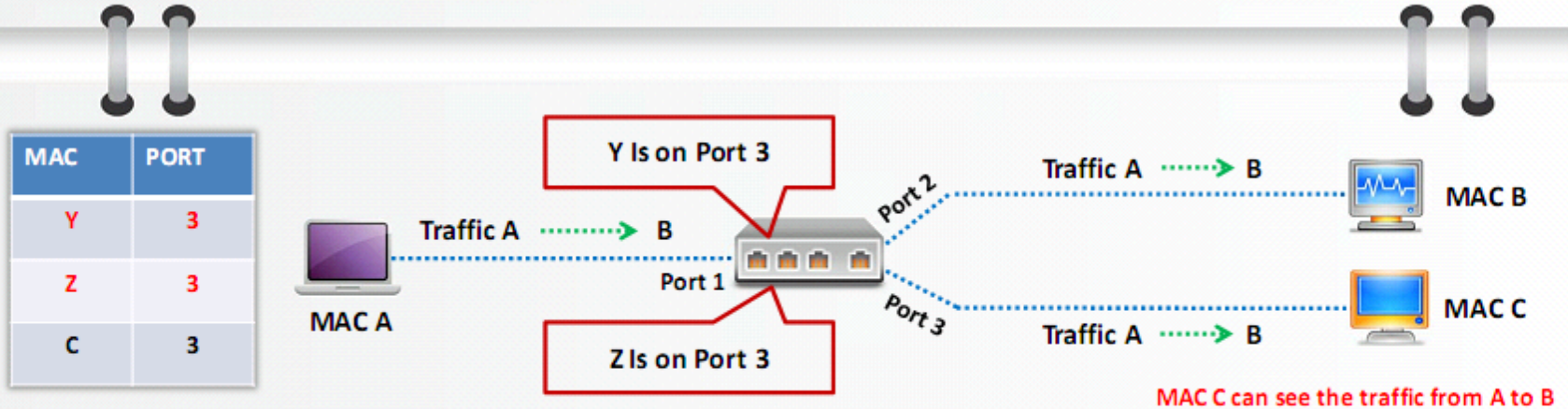
vlan	MAC Add	Type	Learn	Age	Ports
255	00d3.ad34.123g	Dynamic	Yes	0	Gi5/2
5	as23.df45.45t6	Dynamic	Yes	0	Gi2/5
5	er23.23er.t5e3	Dynamic	Yes	0	Gi1/6

How CAM Works



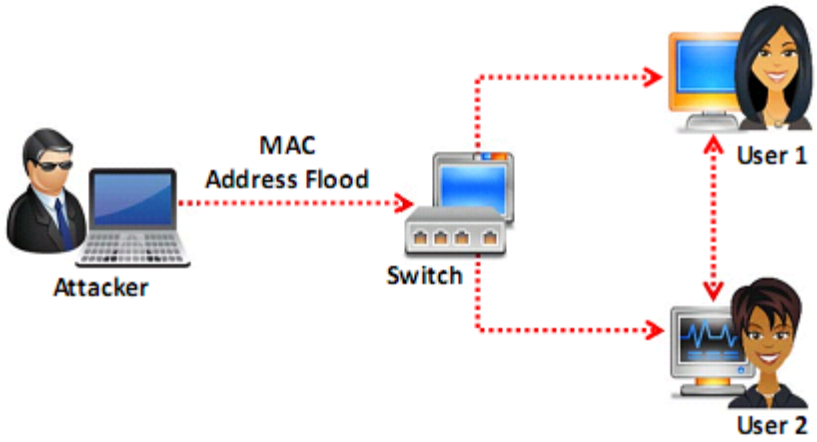
What Happens When CAM Table Is Full?

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



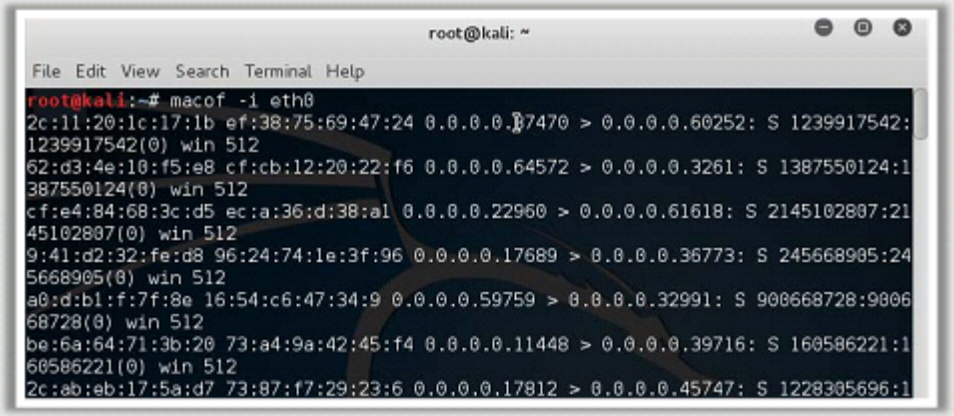
MAC Flooding

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



Mac Flooding Switches with macof

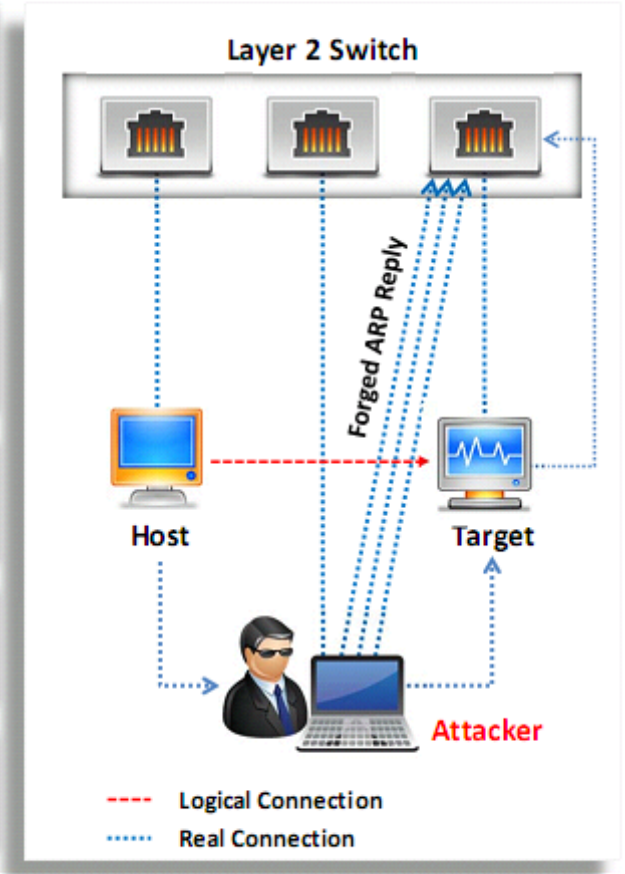
- **macof** is a Unix/Linux tool that is a part of dsniff collection
- macof sends random **source MAC** and **IP addresses**
- This tool **floods the switch's CAM tables** (131,000 per min) by sending bogus MAC entries



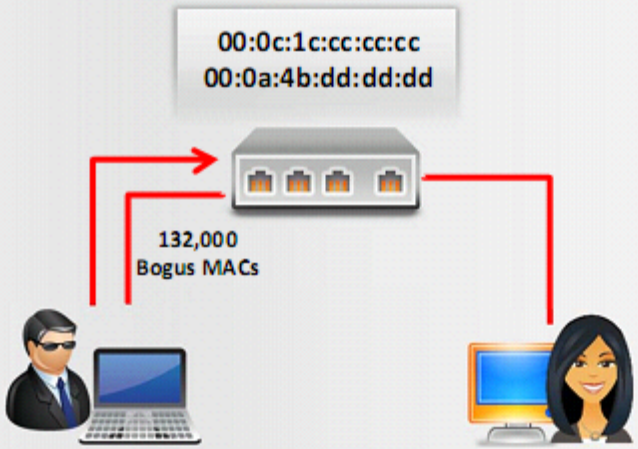
https://www.monkey.org

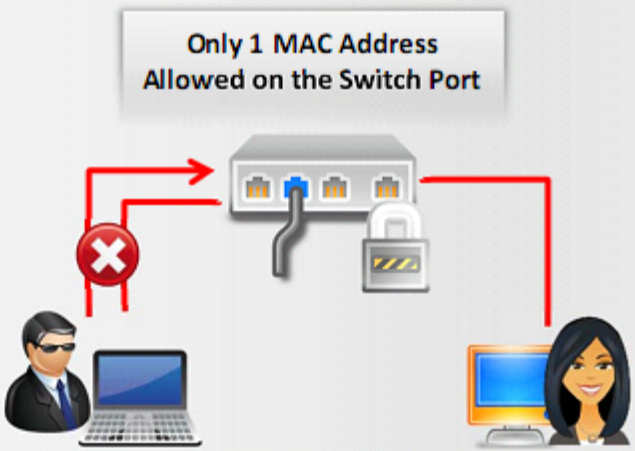
Switch Port Stealing

- Switch Port Stealing sniffing technique uses **MAC flooding** to sniff the packets
- Attacker floods the switch with **forged gratuitous ARP packets** with target MAC address as source and his/her own MAC address as destination
- A **race condition** of attacker's flooded packets and target host packets occur and thus switch has to change its MAC address binding constantly between two different ports
- In such case if attacker is fast enough, he/she will able to **direct the packets** intended for the target host toward his switch port
- Attacker now manages to **steal the target host switch port** and sends ARP request to stolen switch port to discover target hosts' IP address
- When attacker gets ARP reply, this indicates that **target host's switch port binding** has been restored and attacker can now sniff the packets sent toward targeted host



How to Defend against MAC Attacks





Configuring Port Security on Cisco switch:

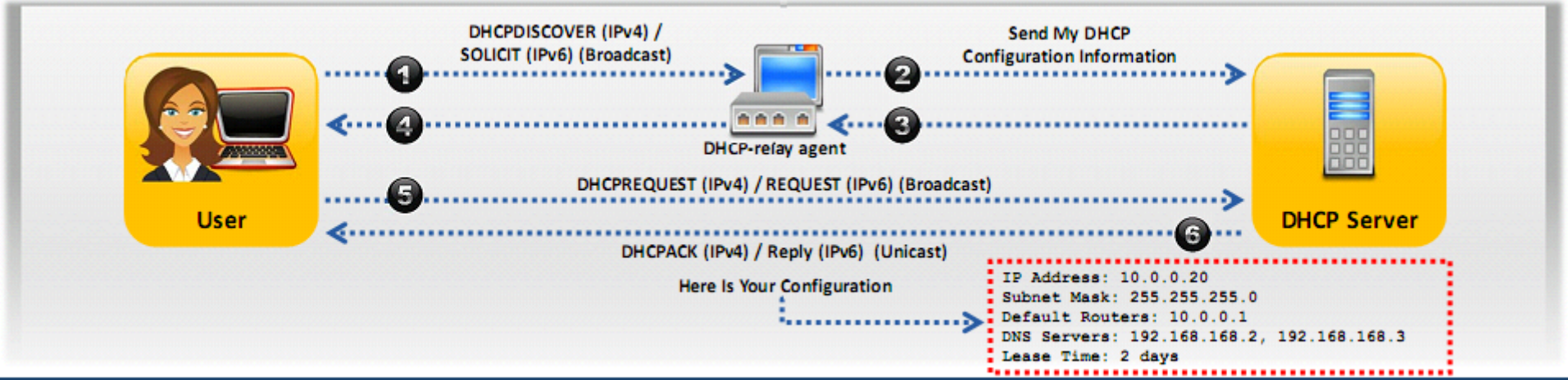
- switchport port-security
- switchport port-security maximum 1 vlan access
- switchport port-security violation restrict
- switchport port-security aging time 2
- switchport port-security aging type inactivity
- snmp-server enable traps port-security trap-rate 5

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

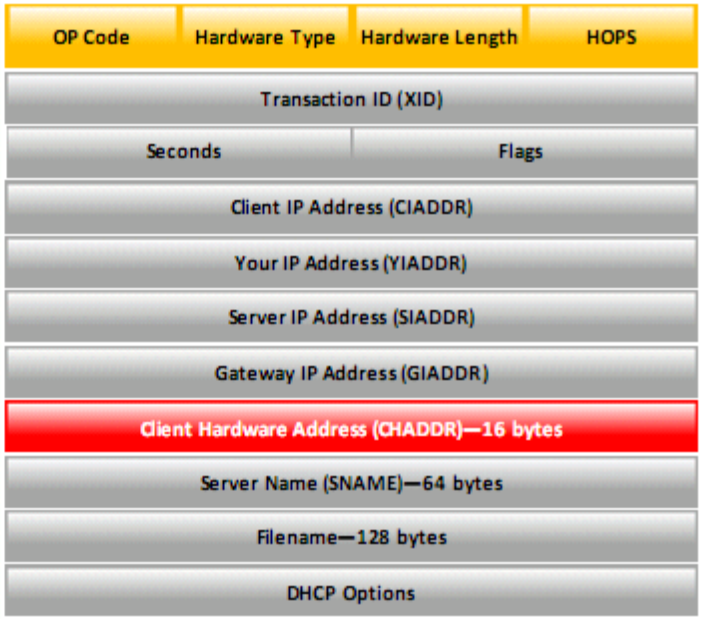
1. Client broadcasts **DHCPDISCOVER/SOLICIT** request asking for DHCP Configuration Information
2. DHCP-relay agent captures the client request and **unicasts** it to the DHCP servers available in the network
3. DHCP server unicasts **DHCPOFFER/ADVERTISE**, which contains client and server's MAC address
4. Relay agent broadcasts **DHCPOFFER/ADVERTISE** in the client's subnet
5. Client broadcasts **DHCPREQUEST/REQUEST** asking DHCP server to provide the DHCP configuration information
6. DHCP server sends unicast **DHCPACK/REPLY** message to the client with the IP config and information



DHCP Request/Reply Messages

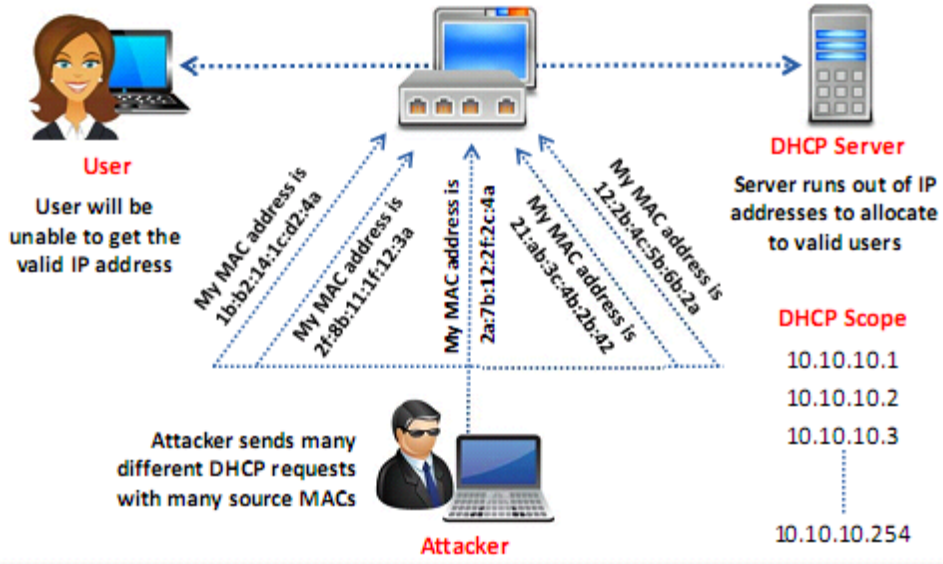
DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client broadcast to locate the available DHCP servers
DHCPOffer	Advertise	Server to client in response to DHCPDISCOVER with offer of configuration parameters
DHCPRequest	Request, Confirm, Renew, Rebind	Client message to servers either (a) requesting offered parameters, (b) confirming correctness of previously allocated address, or (c) extending the lease period
DHCPAck	Reply	Server to client with configuration parameters, including committed network address
DHCPRelease	Release	Client to server relinquishing network address and canceling remaining lease
DHCPDecline	Decline	Client to server indicating network address is already in use
N/A	Reconfigure	Server tells the client 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; client already has 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 client's notion of network address is incorrect (e.g. , Client has moved to new subnet) or client's lease as expired

IPv4 DHCP Packet Format

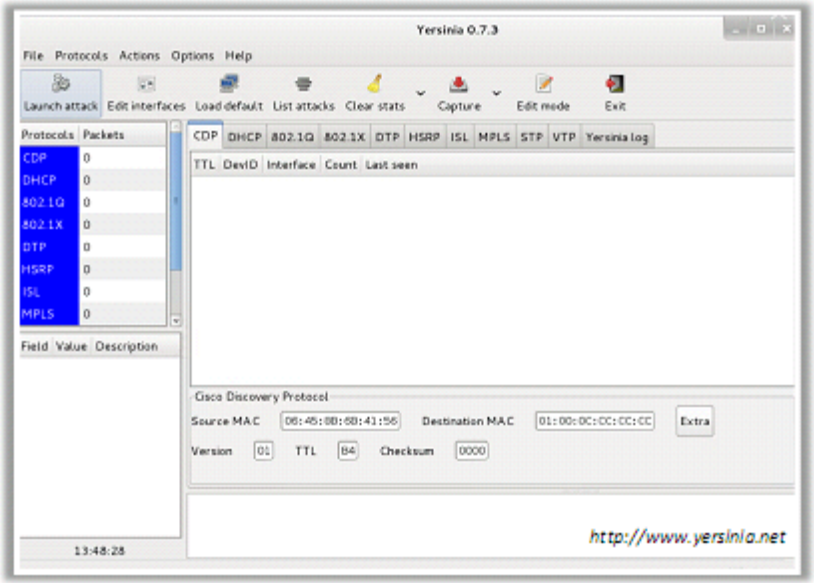


DHCP Starvation Attack

- This is a denial-of-service (DoS) attack on the DHCP servers where attacker broadcasts **forged DHCP requests** and tries to lease all of the DHCP addresses available in the DHCP scope
- Therefore, the legitimate user is **unable to obtain or renew an IP address** requested via DHCP, failing access to the network access



DHCP Starvation Attack Tool: Yersinia

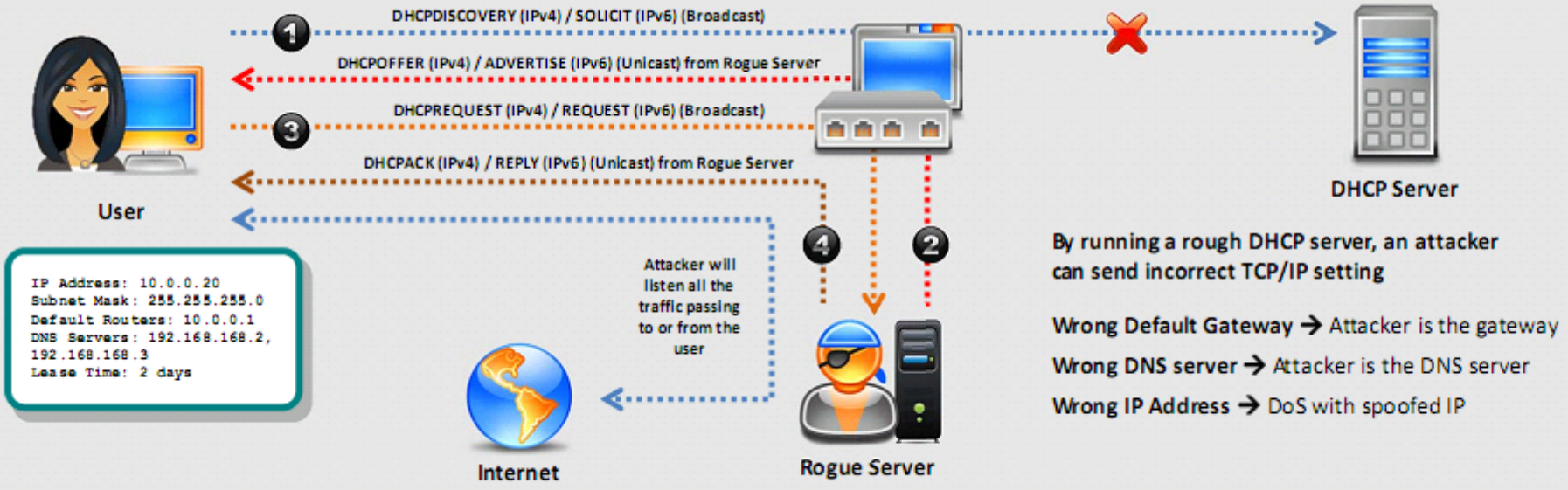


DHCP Starvation Attack Tools

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

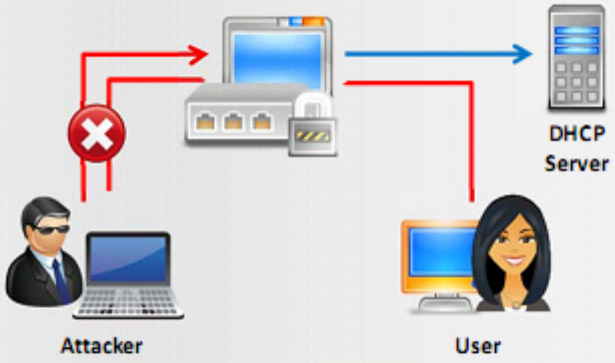
Rogue DHCP Server Attack

1. Attacker sets **rogue DHCP server** in 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; attacker sends **TCP/IP setting** to the user after knocking him/her out from the genuine DHCP server

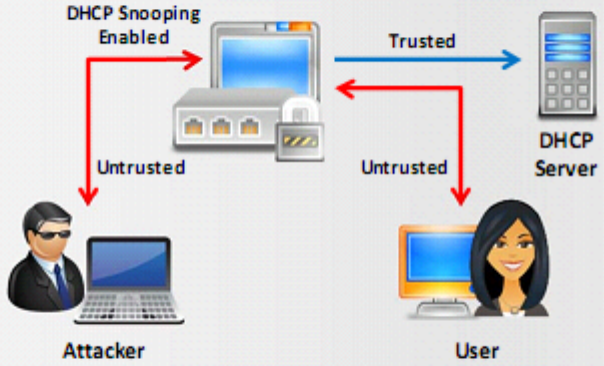


How to Defend Against DHCP Starvation and Rogue Server Attack

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



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



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`

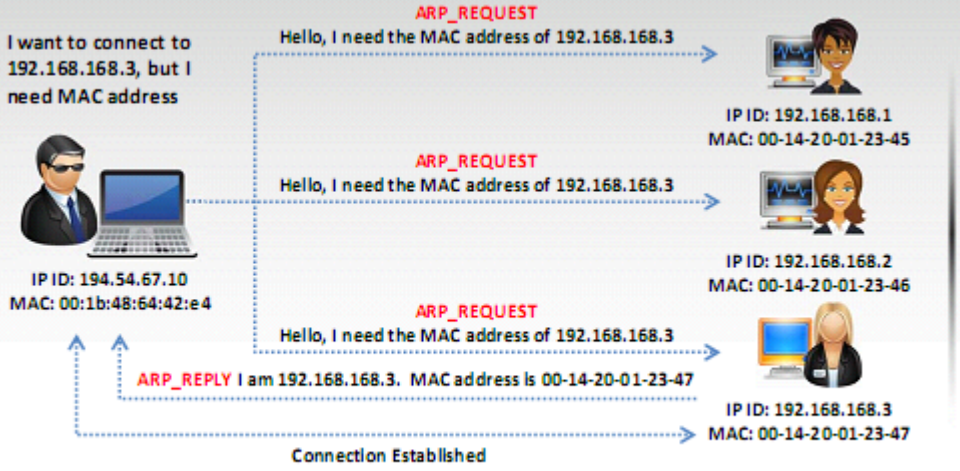
IOS Global Commands

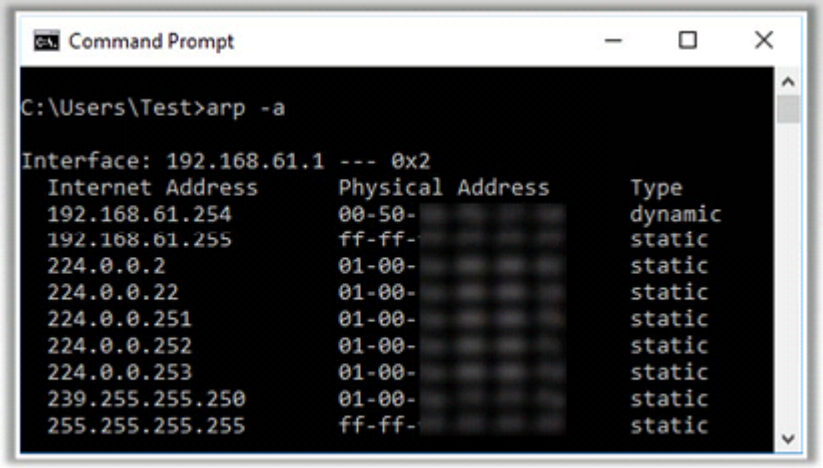
- **`ip dhcp snooping vlan 4,104`** → this is what VLANS to snoop
- **`no ip dhcp snooping information option`** → this allows some DHCP options
- **`ip dhcp snooping`** → this turns on DHCP snooping

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

What Is Address Resolution Protocol (ARP)?

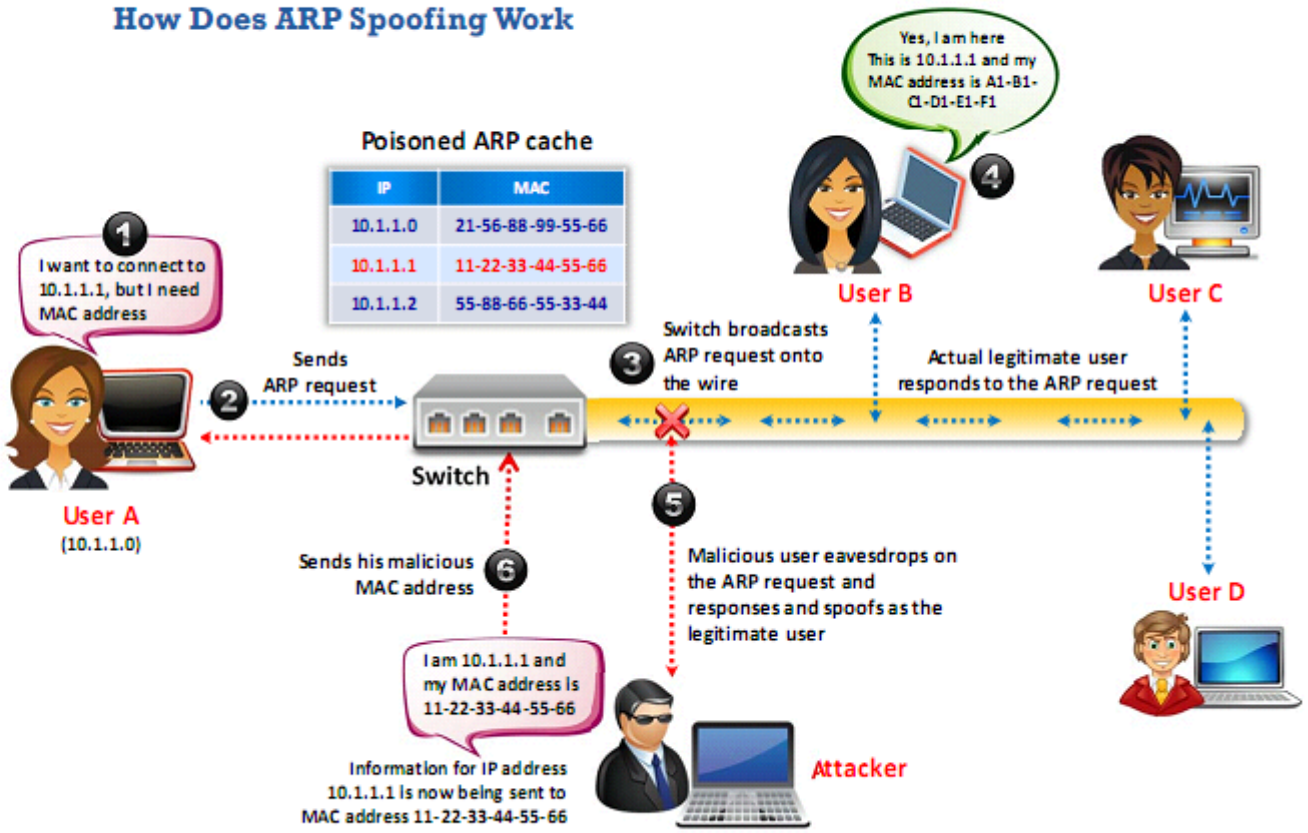
- Address Resolution Protocol (ARP) is a stateless protocol used for **resolving IP addresses to machine (MAC) addresses**
- All network devices (that needs to communicate on the network) broadcasts ARP queries in the network to find out other **machines' MAC addresses**
- When one machine needs to communicate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





ARP Spoofing Attack

- ARP packets can be **forged** to send data to the attacker's machine
- ARP Spoofing involves constructing a large number of **forged ARP request** and reply packets to overload a switch
- Switch is set in '**forwarding mode**' after ARP table is flooded with spoofed ARP replies and attackers can sniff all the network packets
- Attackers flood a target computer's ARP cache with forged entries, which is also known as **poisoning**



Threats of ARP Poisoning

- Using fake **ARP messages**, an attacker can divert all communications between two machines resulting which all traffic is exchanged via his/her 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

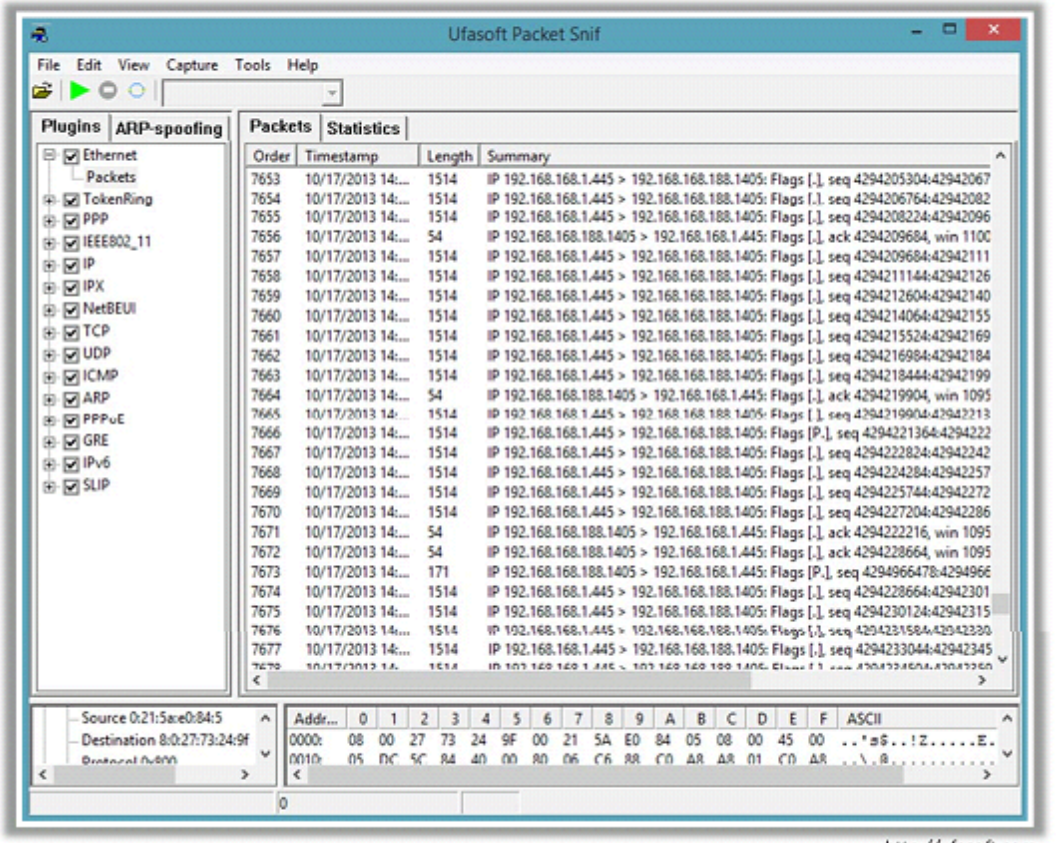
ARP Poisoning Tools

Ufasoft Snif

Ufasoft Snif is an automated ARP poisoning tool that **sniffs passwords** and **email messages** on the network and works on **Wi-Fi network** as well

ARP Poisoning Tools

- BetterCAP (*https://www.bettercap.org*)
- Ettercap (*https://github.com*)
- ArpSpoofTool (*https://sourceforge.net*)
- MITMf (*https://github.com*)
- Cain & Abel (*http://www.oxid.it*)



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

10.10.10.1
MAC A

No ARP entry in the binding table then discard the packet

DHCP Snooping Enabled
Dynamic ARP Inspection Enabled

ARP 10.10.10.1
Saying 10.10.10.2
is MAC C

10.10.10.5
MAC C

ARP 10.10.10.2
Saying 10.10.10.1 is
MAC C

10.10.10.2
MAC B

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

Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

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-      4    FastEthernet
                                           snooping         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
```

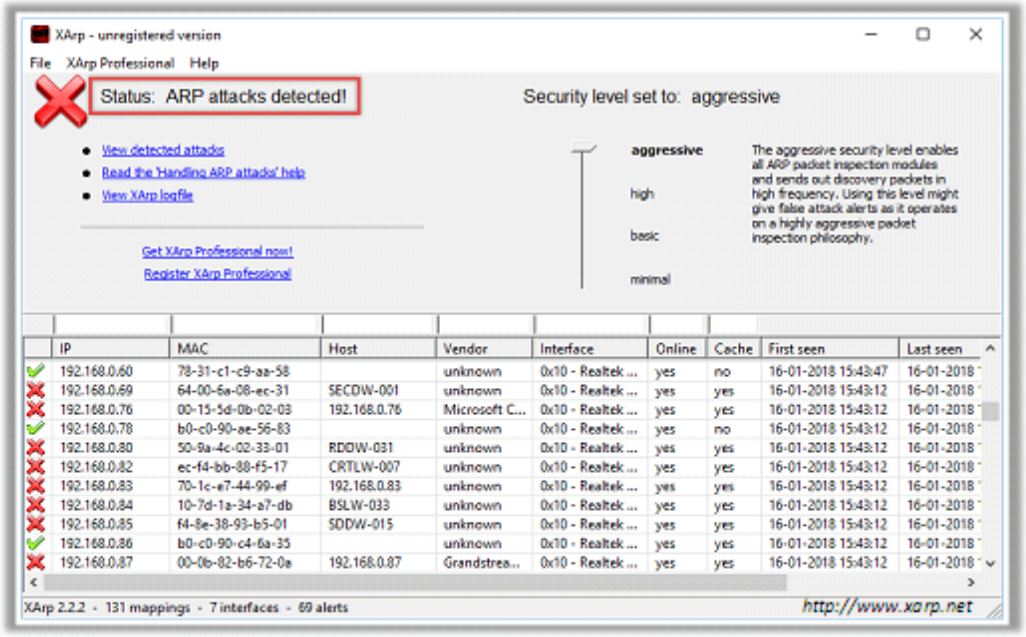
4

```
%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 Oct 30 2017])
```

ARP Spoofing Detection Tools

XArp

- XArp is a security tool that helps users **detect ARP attacks** and **ensure data privacy**
- It allows administrators to monitor whole **subnets** for ARP attacks



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

ArpON
http://arpon.sourceforge.net

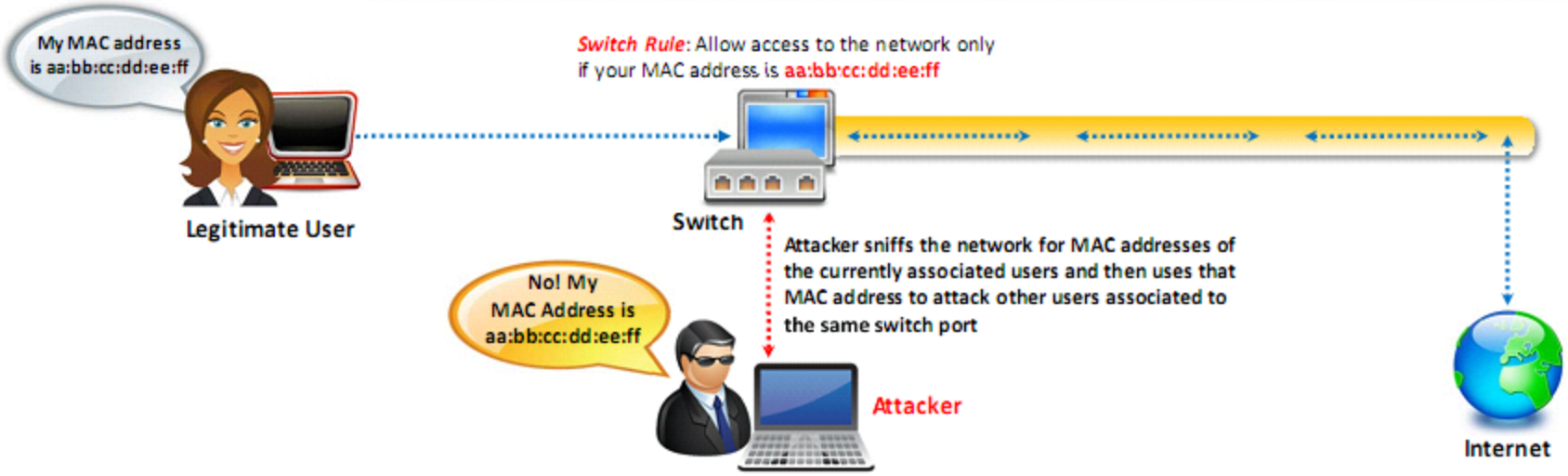
ARP AntiSpoofer
https://sourceforge.net

ARPStraw
https://github.com

shARP
https://github.com

MAC Spoofing/Duplicating

- 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

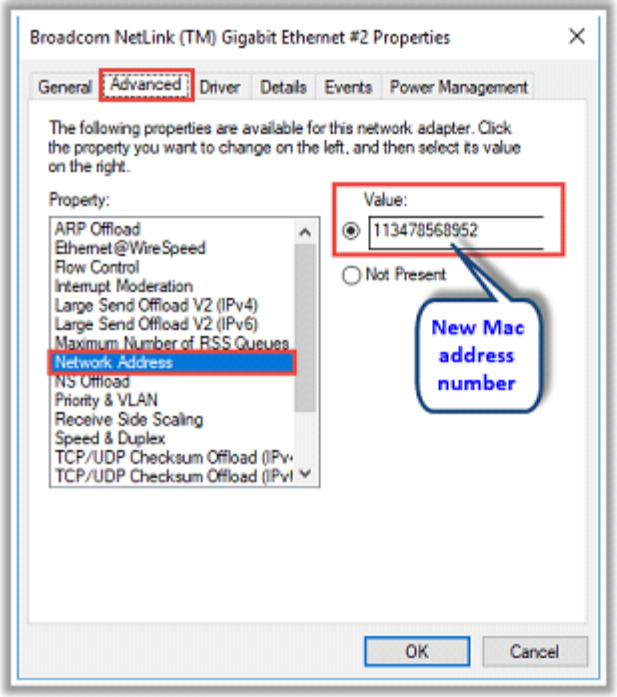


Note: This technique can be used to bypass Wireless Access Points' MAC filtering

MAC Spoofing Technique: Windows

In Windows 10 OS

Method 1: If the network interface card supports 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 the **Ethernet** and then click on the **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 "**-**" in between
6. Type "**ipconfig/all**" or "**net config rdr**" in command prompt to verify the changes
7. If the changes are visible then **reboot** the system, else try method 2 (change MAC address in the registry)

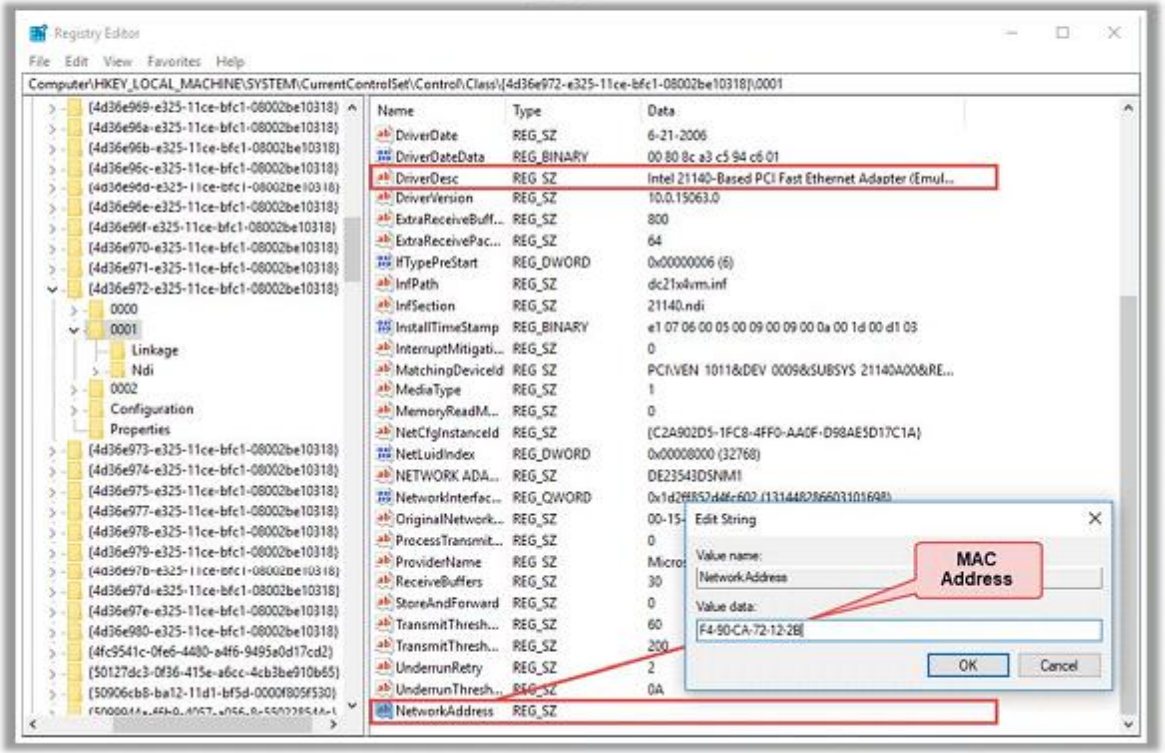
MAC Spoofing Technique: Windows (Cont'd)

Method 2: Steps to change MAC address in Registry

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

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

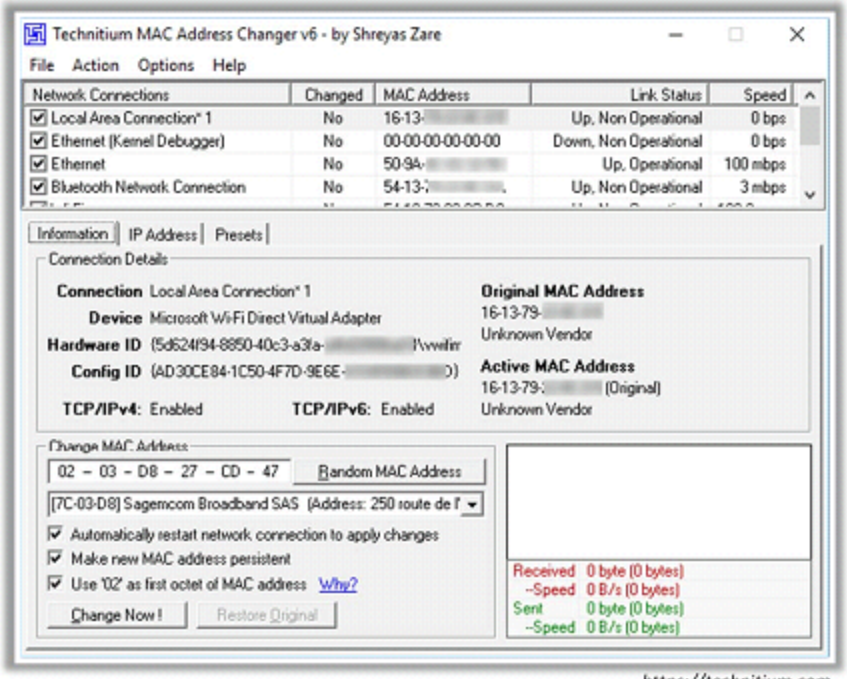
- Go to **"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}** and double click on it to expand the tree
- 4-digit sub keys representing network adapters will be found (starting with 0000, 0001, 0002, etc.)
- Search for the proper "**DriverDesc**" key to find the desired interface
- Edit, or add, the string key "**NetworkAddress**" (data type "REG_SZ") to contain the new MAC address
- **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) Media Access Control (MAC) Address of your Network Interface Card (NIC) instantly



https://technitium.com

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

Change MAC Address
https://lizardsystems.com

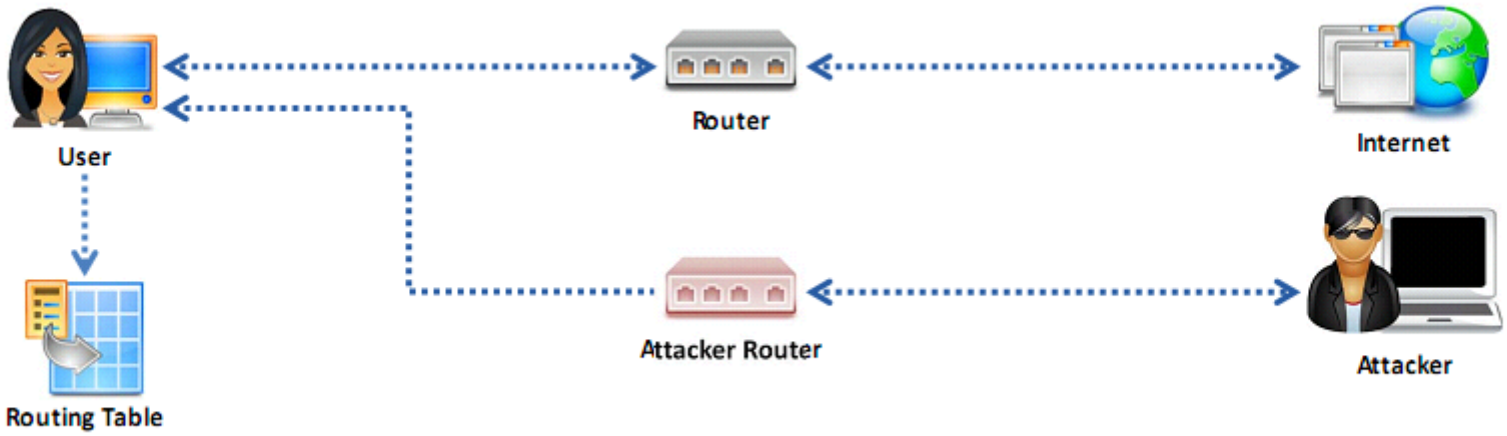
GhostMAC
http://ghostmac.fevermedia.ro

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

SMAC
http://www.klcconsulting.net

IRDP Spoofing

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



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

10.10.10.1
MAC A

DHCP Snooping Enabled
Dynamic ARP Inspection Enabled
IP Source Guard Enabled

If IP and MAC entry in the binding table does not match, then discard the packet

Traffic Sent with IP 10.10.10.5 Mac B

Traffic Sent with IP 10.10.10.2 Mac C

10.10.10.5
MAC C

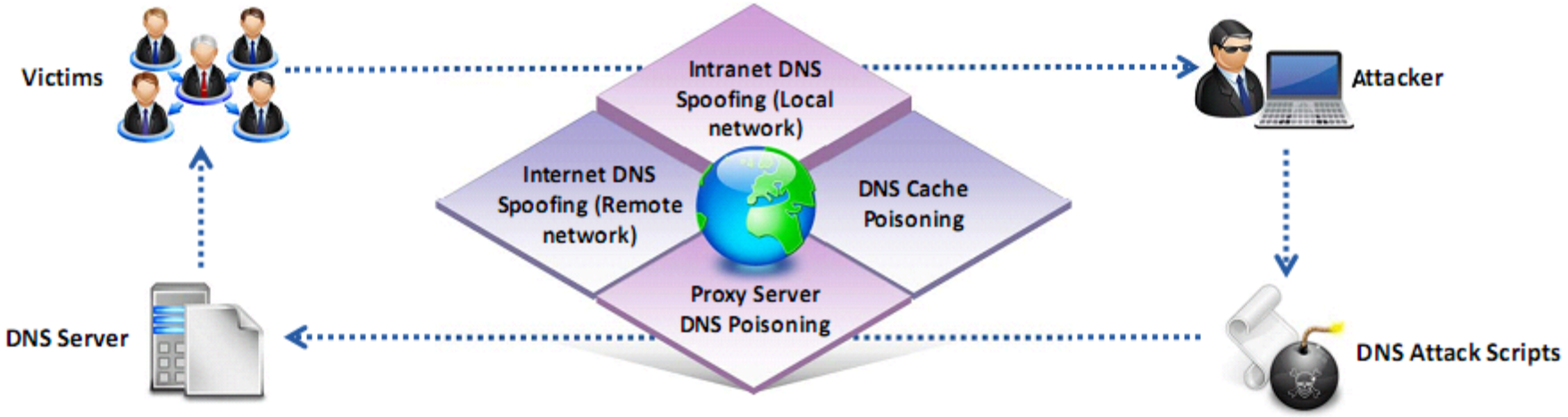
Received Traffic Source IP 10.10.10.2 Mac B

10.10.10.2
MAC B

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

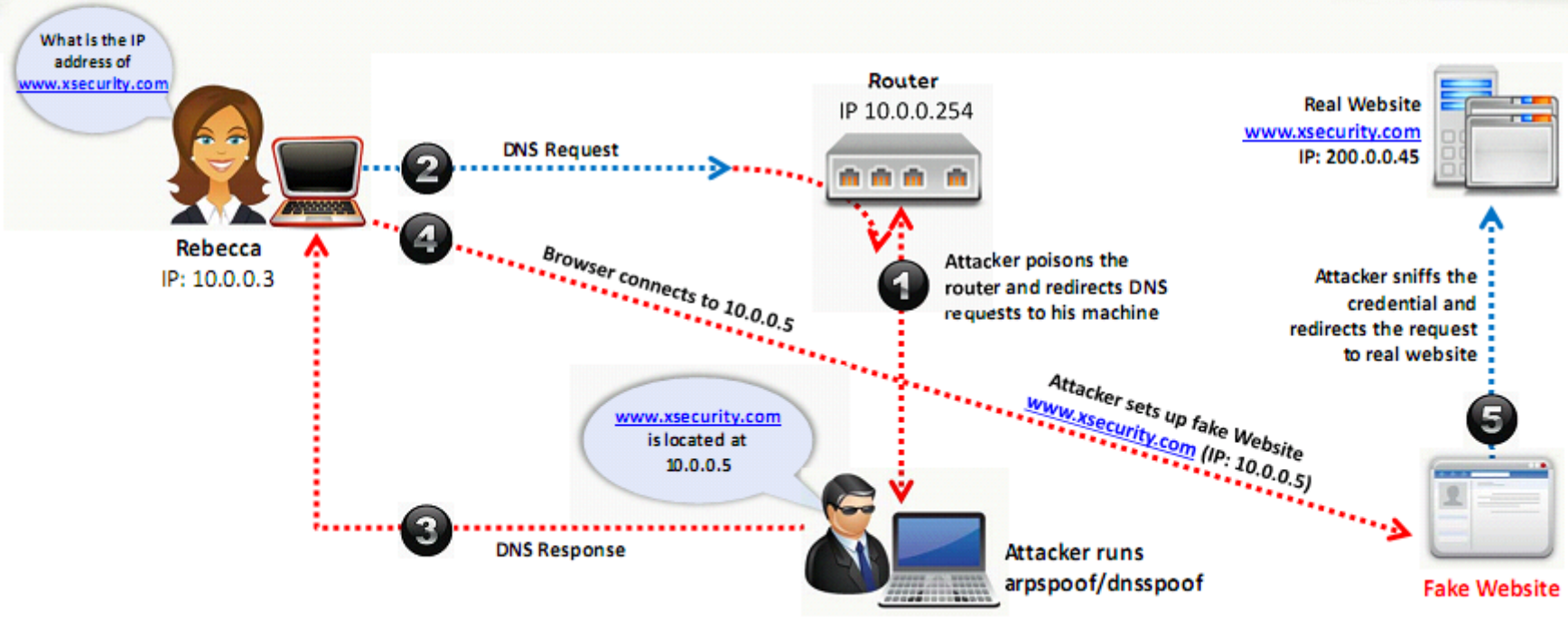
DNS Poisoning Techniques

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



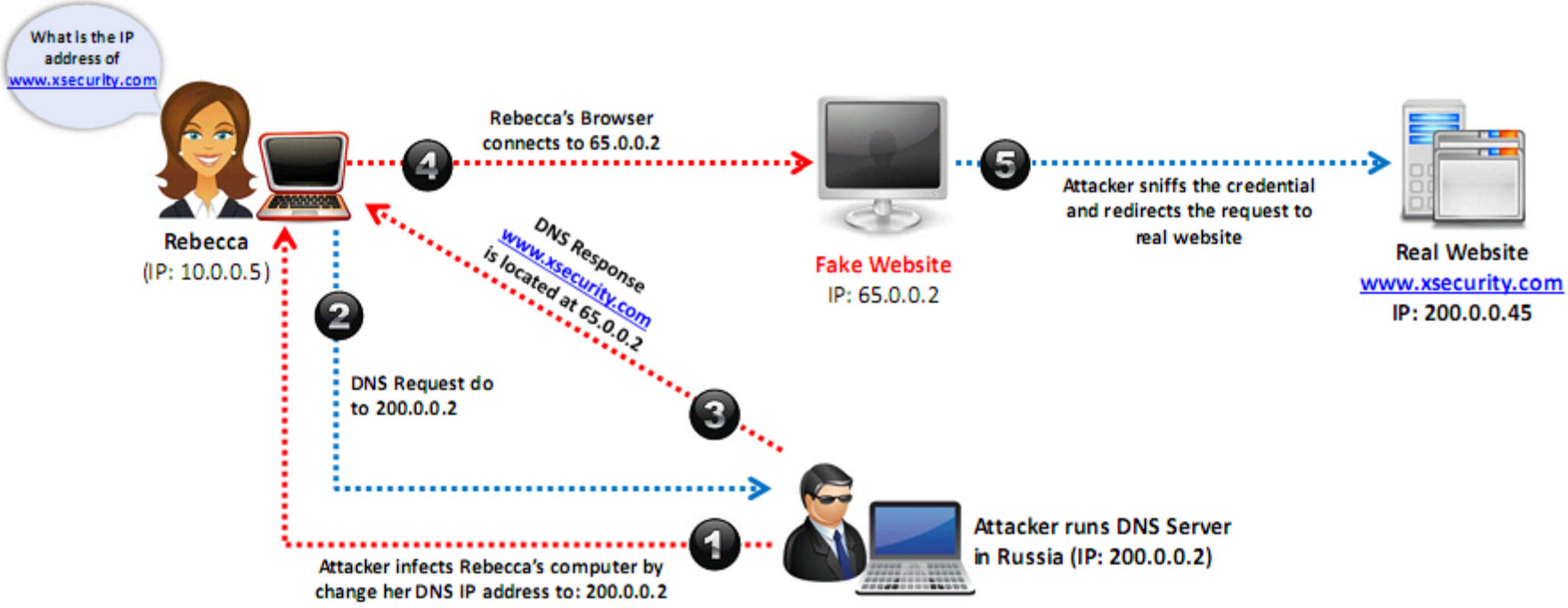
Intranet DNS Spoofing

- For this technique, the 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



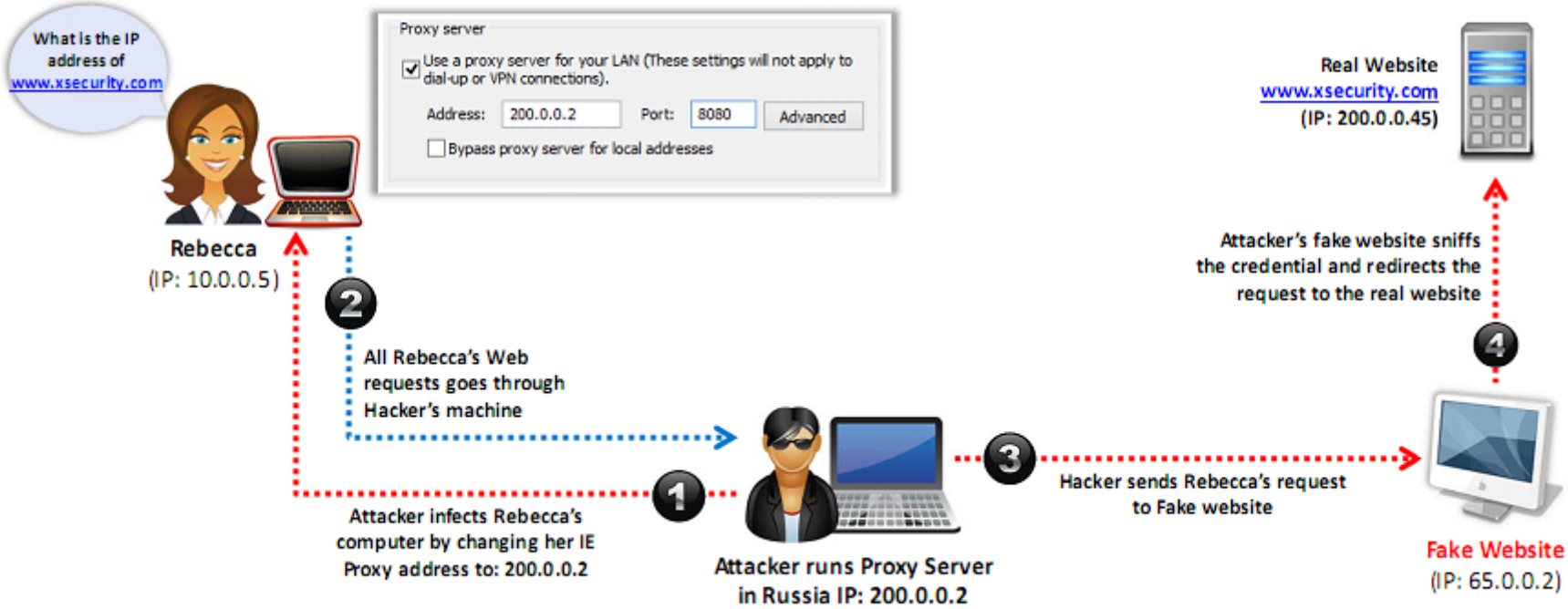
Internet DNS Spoofing

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



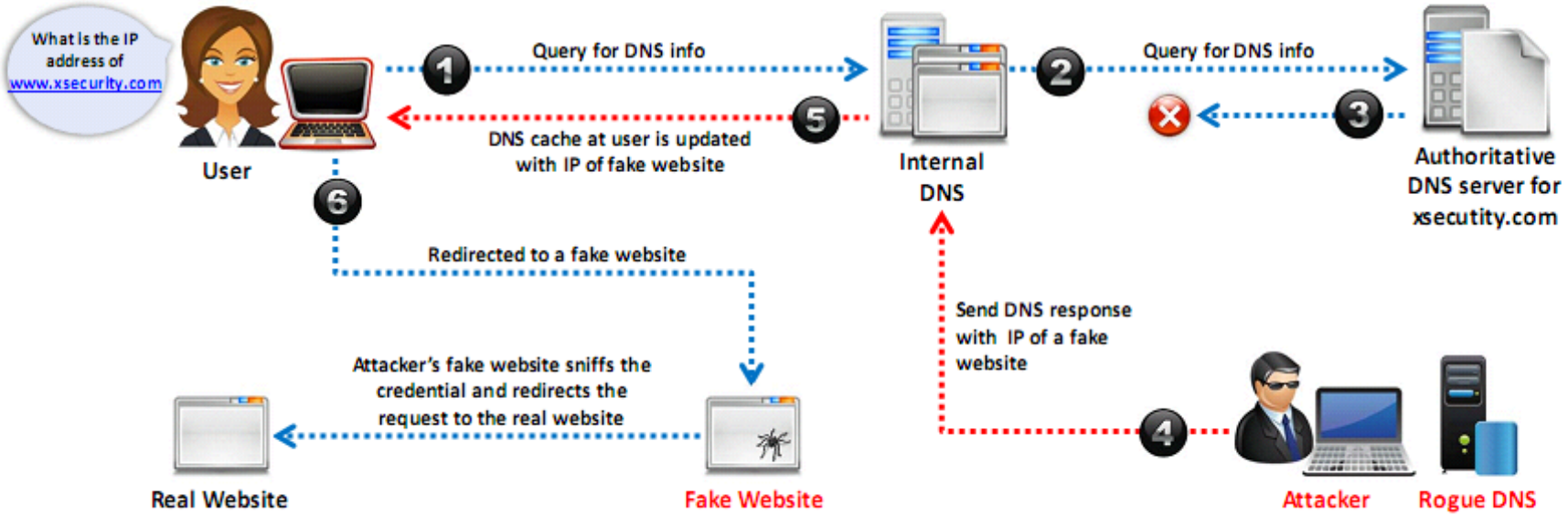
Proxy Server DNS Poisoning

Attacker sends a Trojan to Rebecca's machine that changes her **proxy server settings** in Internet Explorer to that of the attacker's and redirects to 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 the similar request



How to Defend Against DNS Spoofing

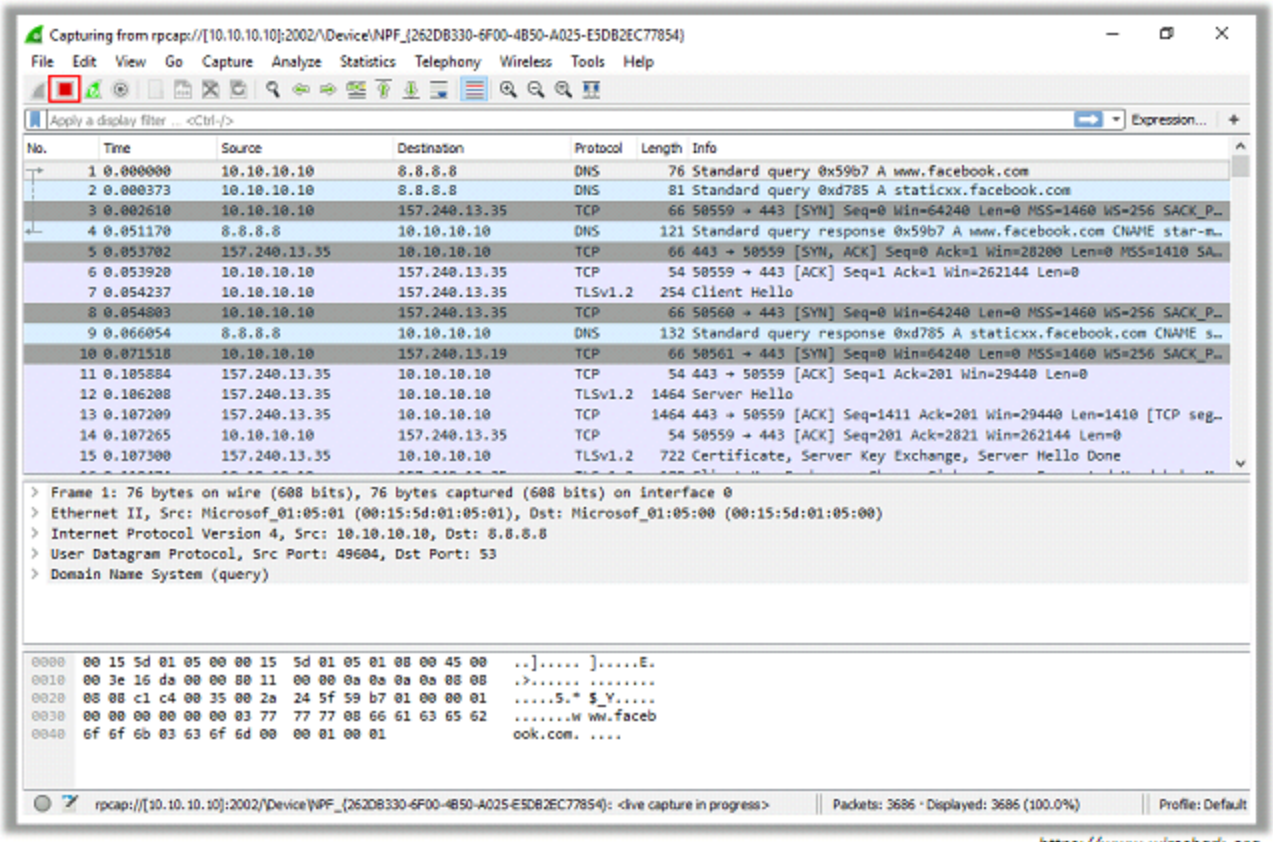
1. Implement Domain Name System Security Extension (DNSSEC)
2. Use Secure Socket Layer (SSL) for securing the traffic
3. Resolve all DNS queries to local DNS server
4. Block DNS requests being sent to external servers
5. Configure firewall to restrict external DNS lookup
6. Implement intrusion detection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

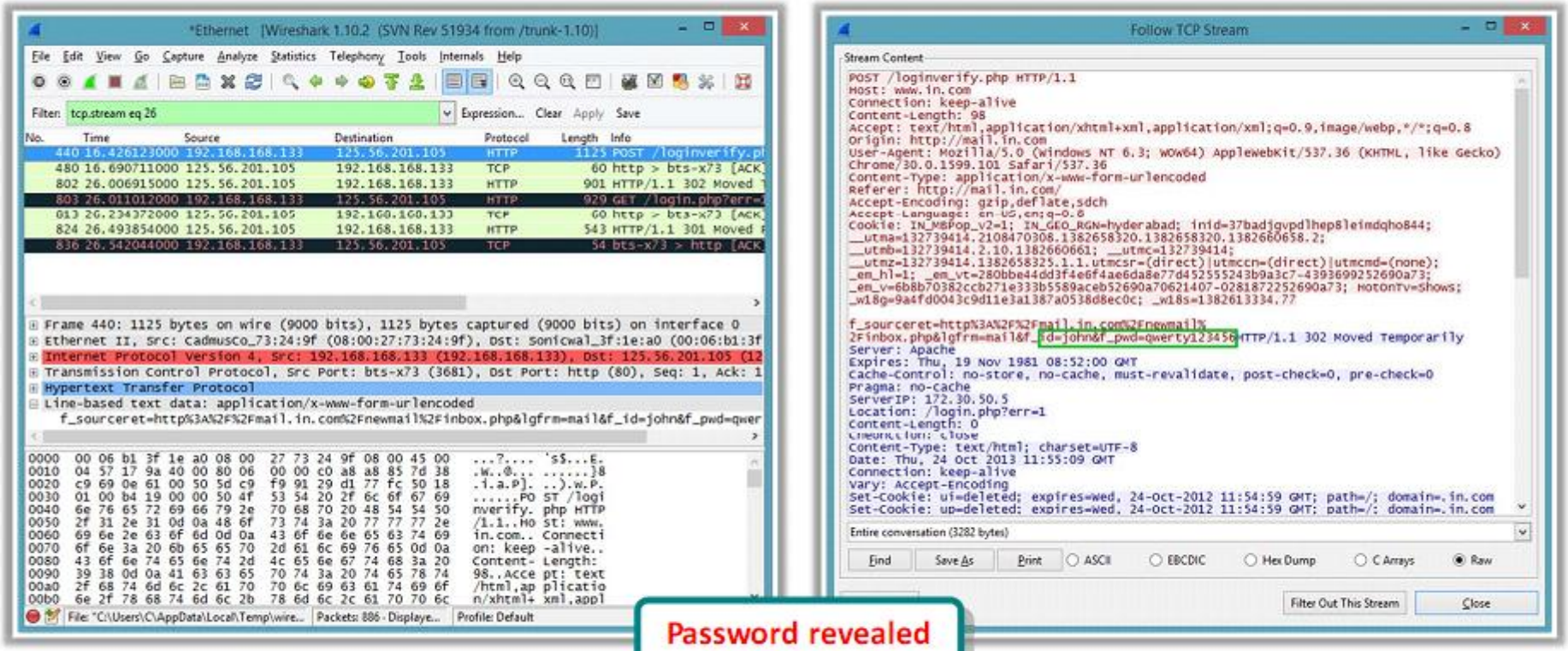
Sniffing Tool: Wireshark

- 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, FDDI networks
- A **set of filters** for customized data display can be refined using a display filter



https://www.wireshark.org

Follow TCP Stream in Wireshark



Password revealed in TCP Stream

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, 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 you 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

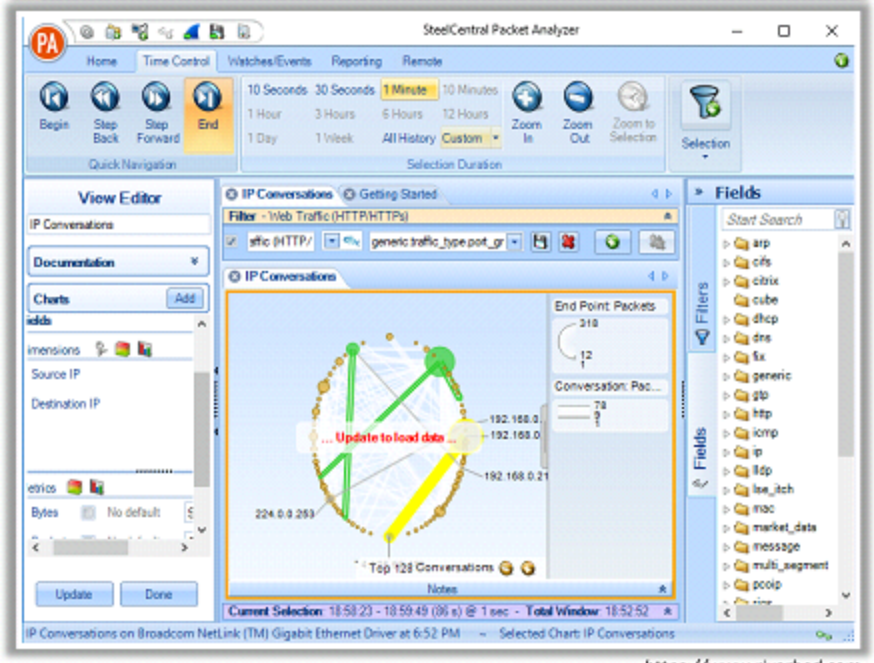
9. `ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16`
   Displays only traffic in the LAN (192.168.x.x), between workstations and servers -- no Internet

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 and Capsa Network Analyzer

SteelCentral Packet Analyzer

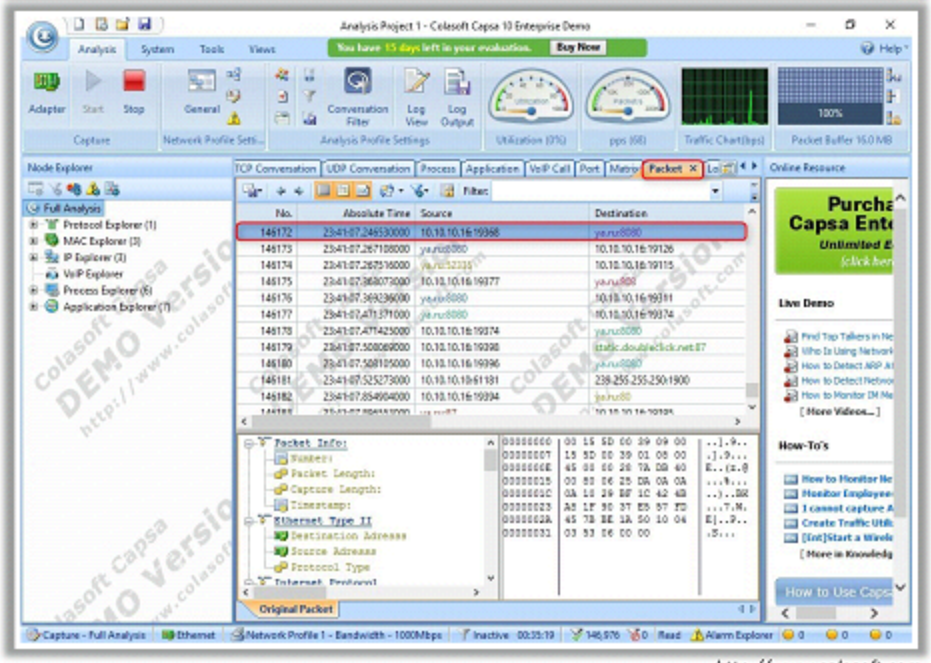
- SteelCentral Packet Analyzer provides a graphical console for **high-speed packet analysis**



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 graphic way

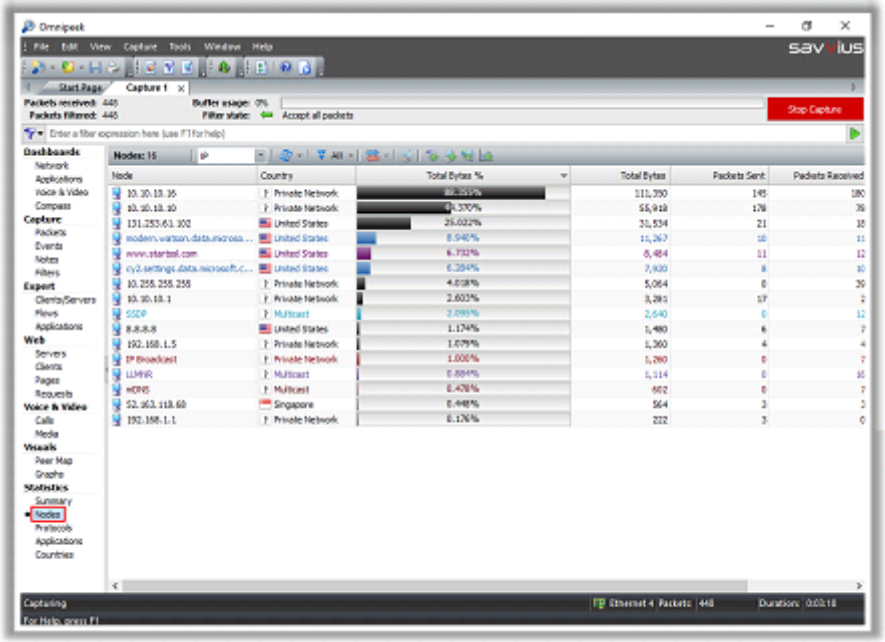


http://www.colasoft.com

Sniffing Tools: OmniPeek and Observer Analyzer

OmniPeek

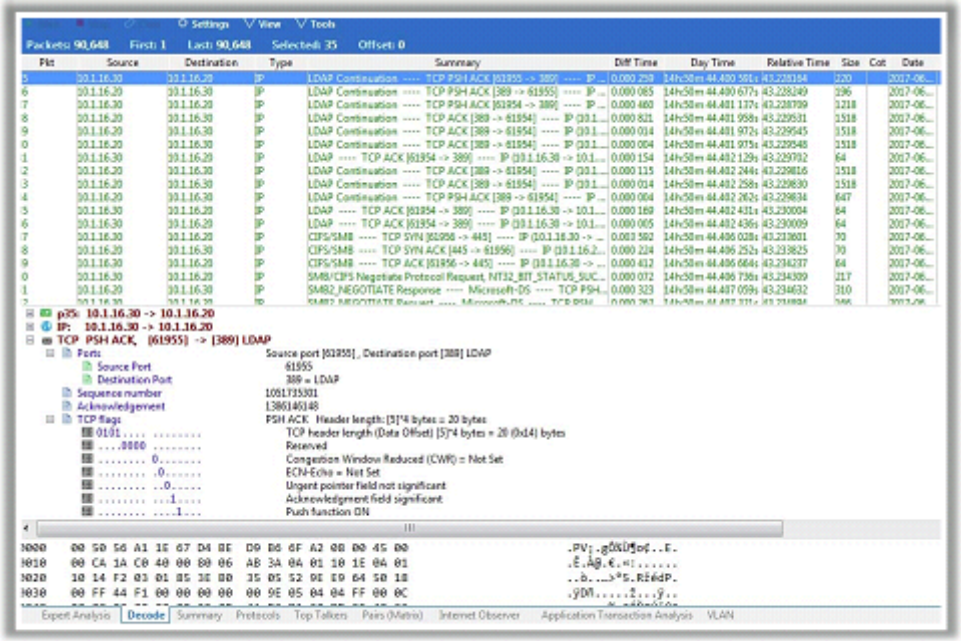
- OmniPeek sniffer displays a Google Map in the OmniPeek capture window showing the **locations of all the public IP addresses of captured packets**



https://www.savvius.com

Observer Analyzer

- Observer provides a comprehensive drill-down into network traffic and provides **back-in-time analysis**, reporting, trending, alarms, application tools, and **route monitoring capabilities**



https://www.viavisolutions.com

Additional Sniffing Tools

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

CommView
https://www.tamos.com

CSniffer
https://www.mcafee.com

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

NetResident
https://www.tamos.com

EtherApe
http://etherape.sourceforge.net

RSA NetWitness Investigator
https://community.rsa.com

ntopng
http://www.ntop.org

Network Probe
http://www.objectplanet.com

tcpdump
http://www.tcpdump.org

SmartSniff
http://www.nirsoft.net

WebSiteSniffer
http://www.nirsoft.net

NetFlow Analyzer
https://www.manageengine.com

Free Network Analyzer
https://freenetworkanalyzer.com

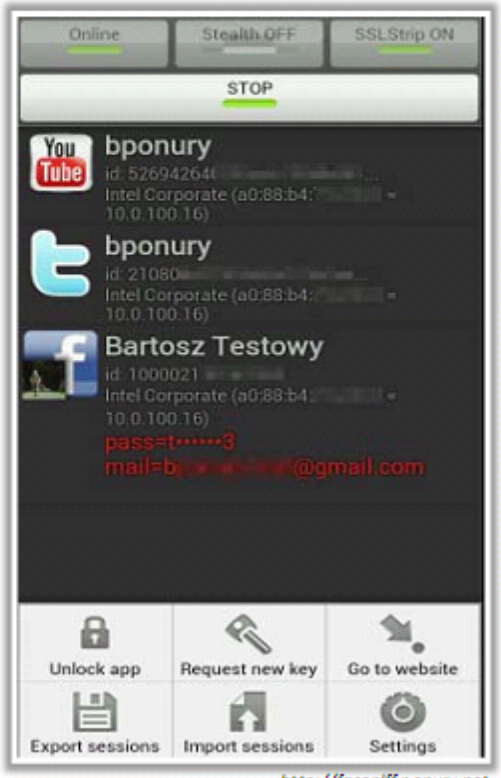
Kismet
https://www.kismetwireless.net

Packet Sniffing Tools for Mobile

Wi.cap. Network Sniffer Pro

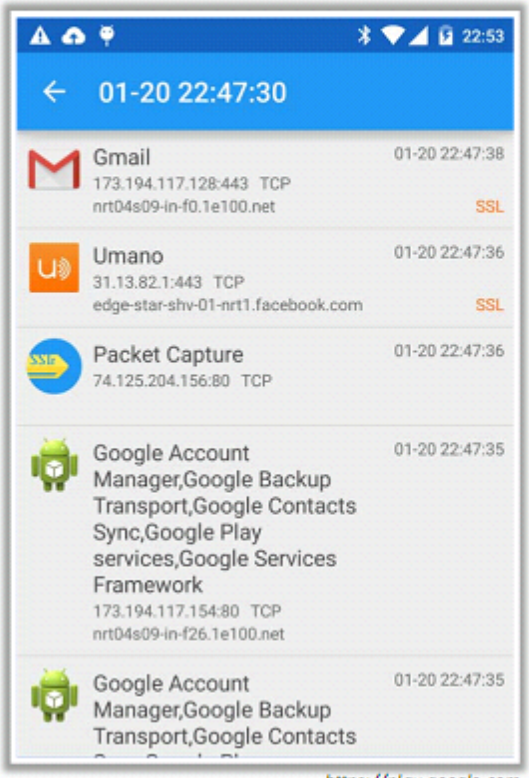
https://play.google.com

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
6. Sniffing Pen Testing

How to Defend Against Sniffing

01	Restrict the 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 the 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 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, SSL for email connection, etc. to protect wireless network users against sniffing attacks

How to Defend Against Sniffing (Cont'd)

08 Use **HTTPS** instead of HTTP to protect user names and passwords

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

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

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

12 Always encrypt the wireless traffic with a **strong encryption protocol** such as WPA and WPA2

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

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

15 Use a concept of **ACL** or Access Control List 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
6. Sniffing Pen Testing

How to Detect Sniffing

Promiscuous Mode

- You will 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

IDS

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

Network Tools

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

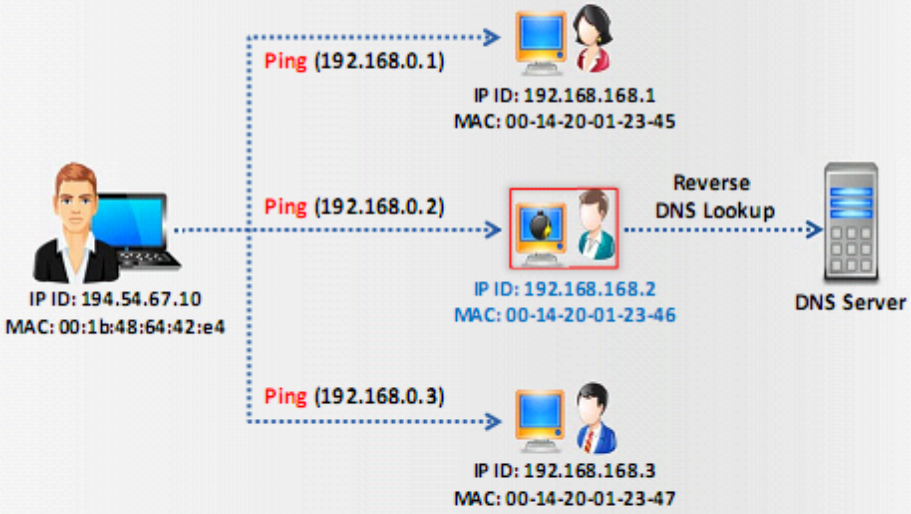
Sniffer Detection Techniques: Ping Method and DNS Method

Ping Method

- Sends a ping request to the suspect machine with its IP address and **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

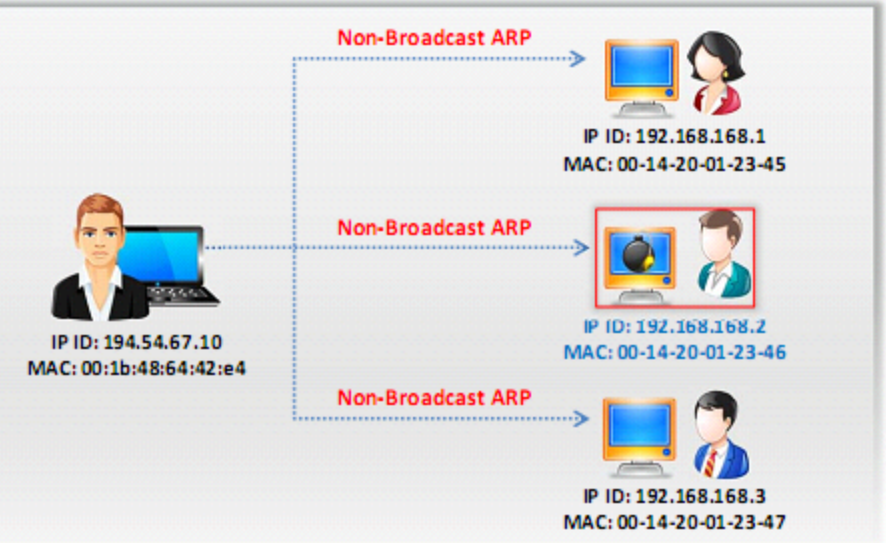
DNS Method

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

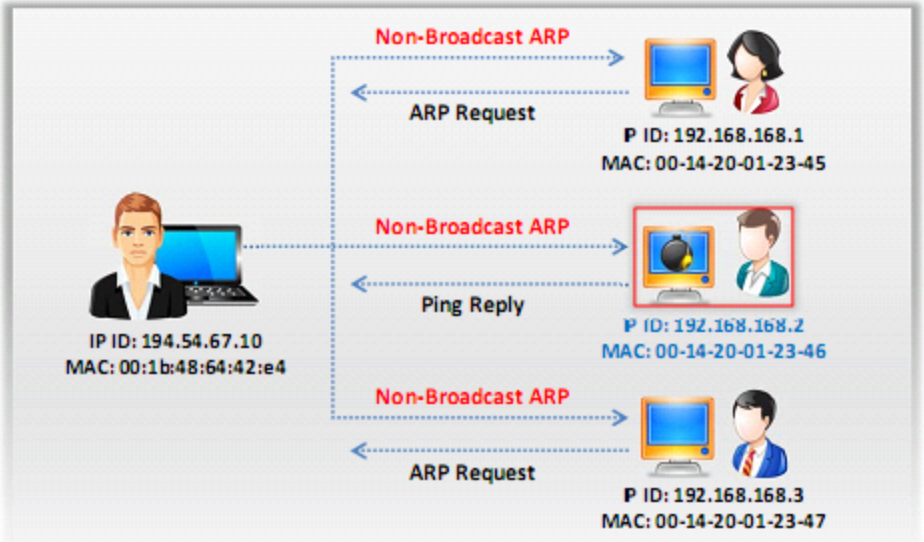


- A machine generating **reverse DNS lookup traffic** will be most likely running a sniffer

Sniffer Detection Technique: ARP Method



Only a machine in promiscuous mode (machine C) **caches the ARP information** (IP and MAC address mapping)

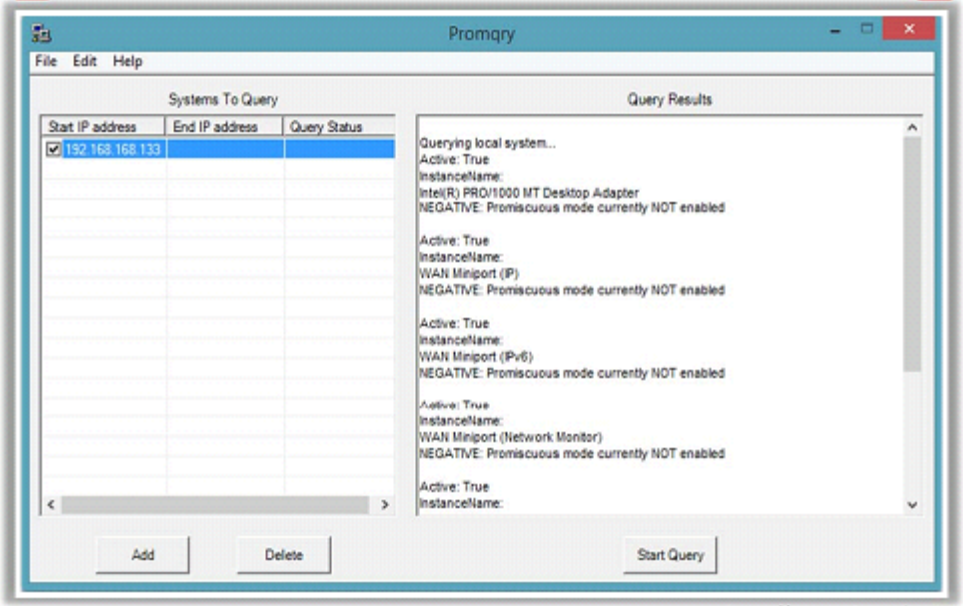


A machine in promiscuous mode **responds to the ping message** as it has correct information about the host sending the **ping request** in its cache; rest of the machines will send ARP probe to identify the source of ping request

Promiscuous Detection Tools

PromqryUI

- PromqryUI is a security tool from Microsoft that can be used to detect network interfaces that are running in promiscuous mode

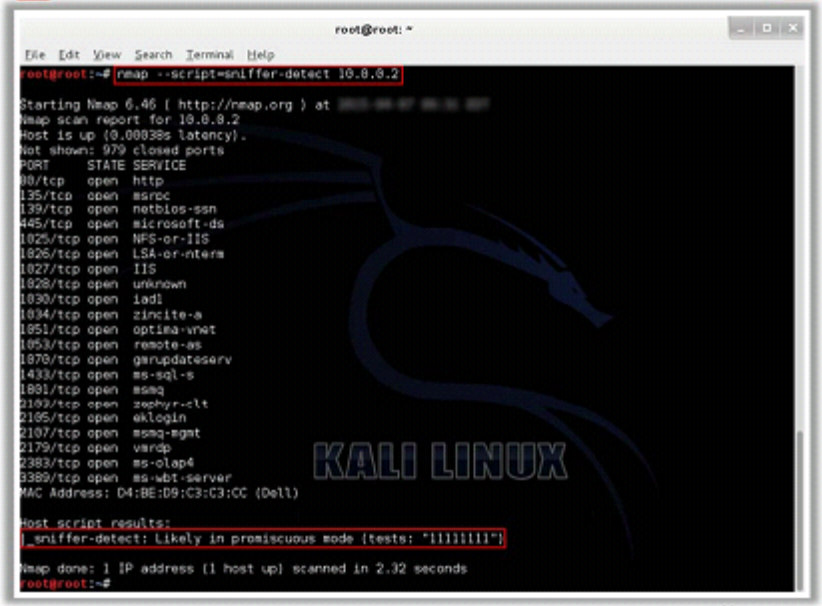


https://www.microsoft.com

Nmap

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

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



https://nmap.org

Module Flow

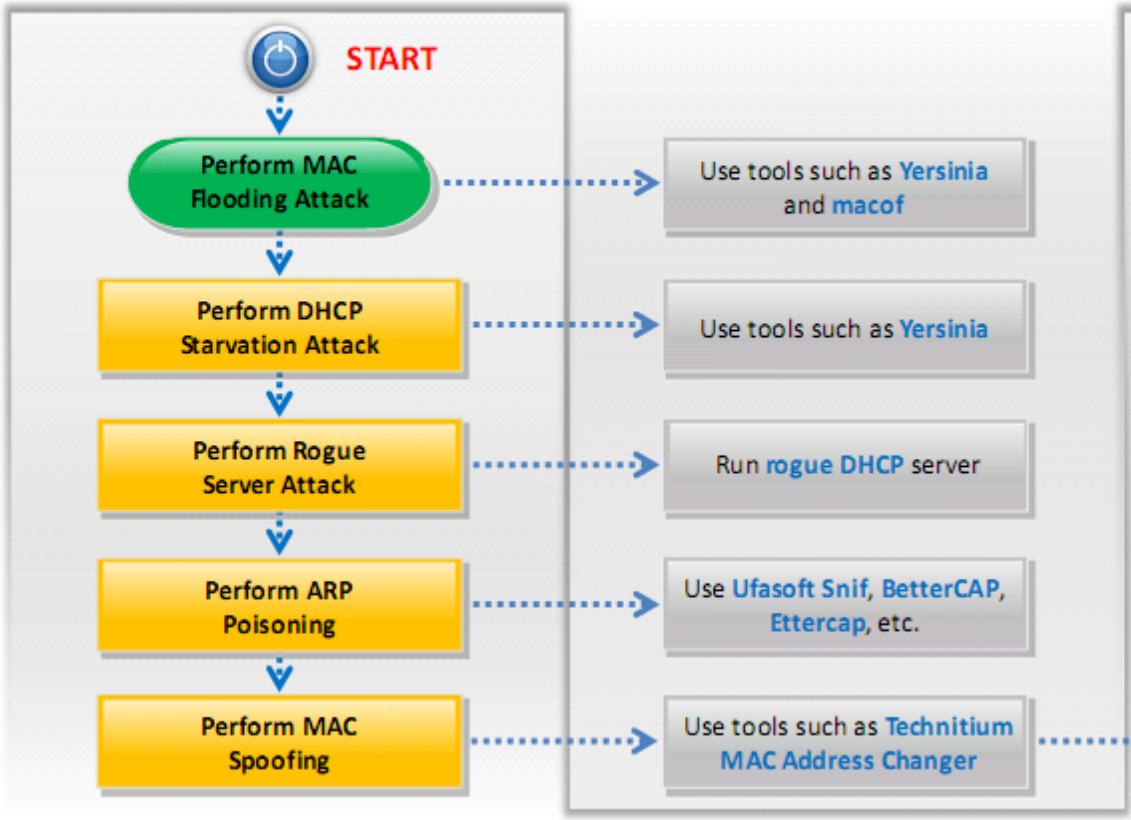
1. Sniffing Concepts
2. Sniffing Techniques
3. Sniffing Tools
4. Countermeasures
5. Sniffing Detection Techniques
6. Sniffing Pen Testing

Sniffing Penetration Testing

- Sniffing pen test is used to check if the **data transmission** from an organization is **secure from sniffing and interception attacks**
- Sniffing pen test helps administrators to:

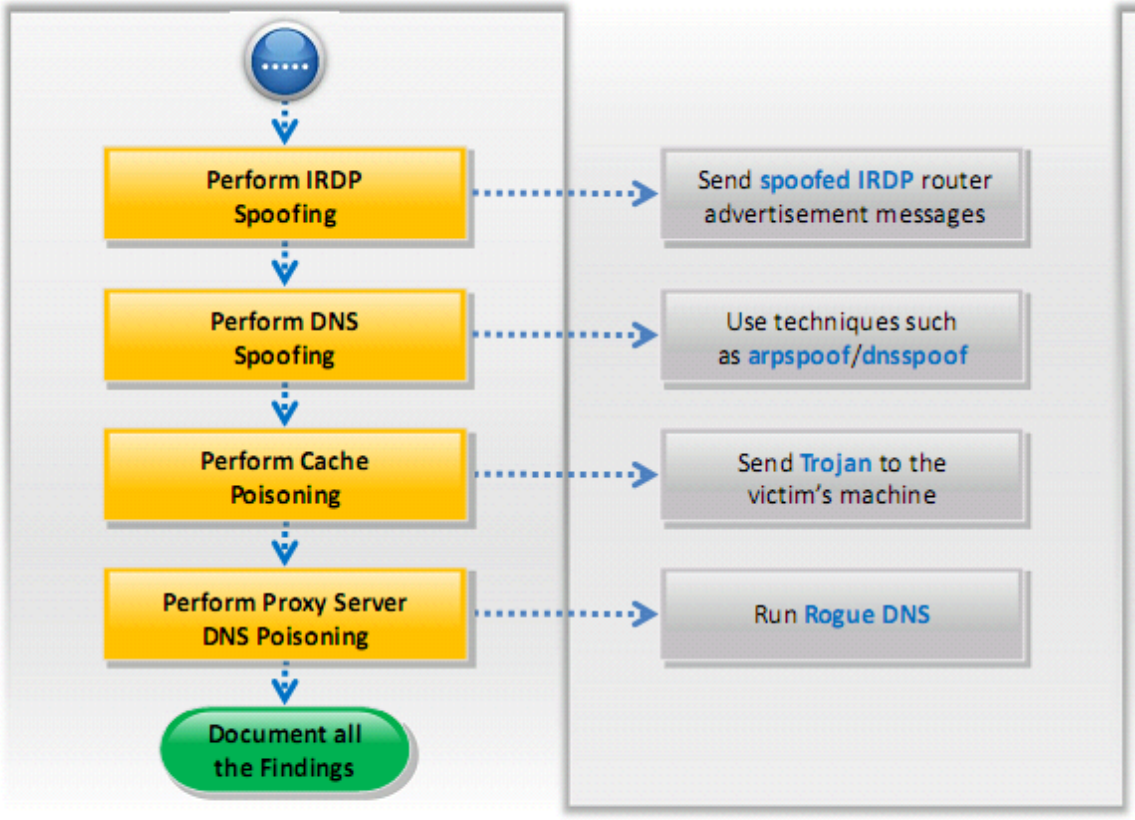
1. **Audit the network traffic** for malicious content
2. **Implement security mechanism** such as SSL and VPN to secure the network traffic
3. **Identify rogue sniffing application** in the network
4. **Discover rogue DHCP and DNS servers** in the network
5. Discover the presence of **unauthorized networking devices**

Sniffing Penetration Testing (Cont'd)



- Perform MAC flooding attack using tools such as Yersinia and macof
- Perform DHCP starvation attack using tools such as Yersinia and Hyenae
- Perform rogue server attack by running rogue DHCP server in the network and responding to DHCP requests with bogus IP addresses
- Perform ARP poisoning using tools such as Ufasoft Snif, BetterCAP, Ettercap, etc.
- Perform MAC spoofing using tools such as Technitium MAC Address Changer (TMAC)

Sniffing Penetration Testing (Cont'd)



- Perform Internet Router Discovery Protocol (IRDP) spoofing by sending spoofed IRDP router advertisement messages
- Perform DNS spoofing using techniques such as arpspoof/dnsspoof
- Perform cache poisoning by sending Trojan to the victim's machine that changes IE Proxy Settings to that of attackers, thus redirecting to fake website
- Perform proxy server DNS poisoning by running rogue DNS

Module Summary

- By placing a packet sniffer in a network, attackers can capture and analyze all the network traffic
- Attackers can sniff confidential information such as email and chat conversations, passwords, and web traffic
- Sniffing is broadly categorized as passive and active; passive sniffing refers to sniffing from a hub-based network, whereas active sniffing refers to sniffing from a switch-based network
- 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 layer will not be aware of the problem
- Attackers use MAC attacks, DHCP attacks, ARP poisoning attacks, spoofing attacks, and DNS poisoning techniques to sniff network traffic
- Major countermeasures for sniffing include using static IP addresses and static ARP tables, and using encrypted sessions such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, SSL for data transmission