Sniffing

Module 07

Unmask the Invisible Hacker.

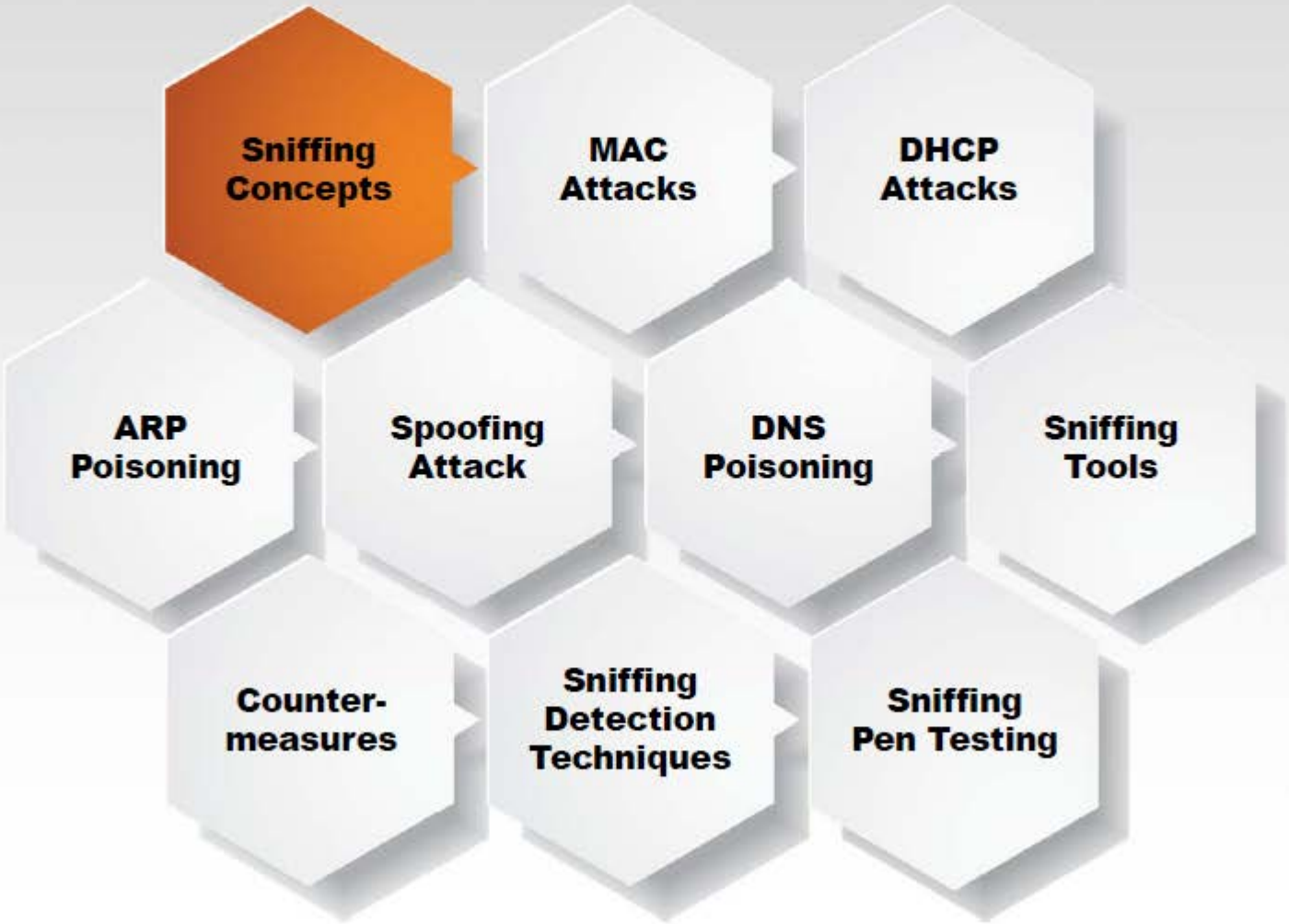



Module Objectives

- Overview of Sniffing Concepts
- Understanding MAC Attacks
- Understanding DHCP Attacks
- Understanding ARP Poisoning
- Understanding MAC Spoofing Attacks
- Understanding DNS poisoning
- Sniffing Tools
- Sniffing Countermeasures
- Understanding Various Techniques to Detect Sniffing
- Overview of Sniffing Pen Testing



Module Flow

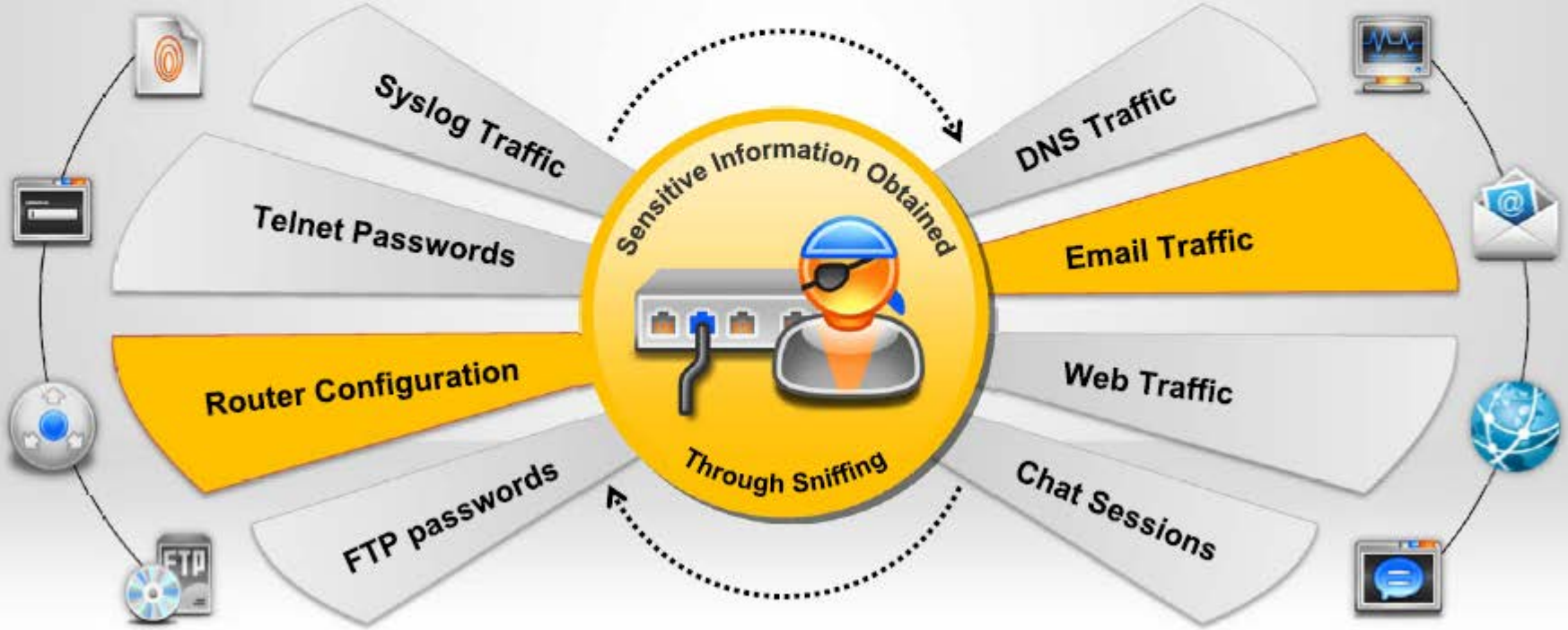


Network Sniffing and Threats

C|EH Certified Ethical Hacker

- Sniffing is a process of monitoring and **capturing all data packets** passing through a given network using sniffing tools
- It is a form of **wiretap** applied to computer networks

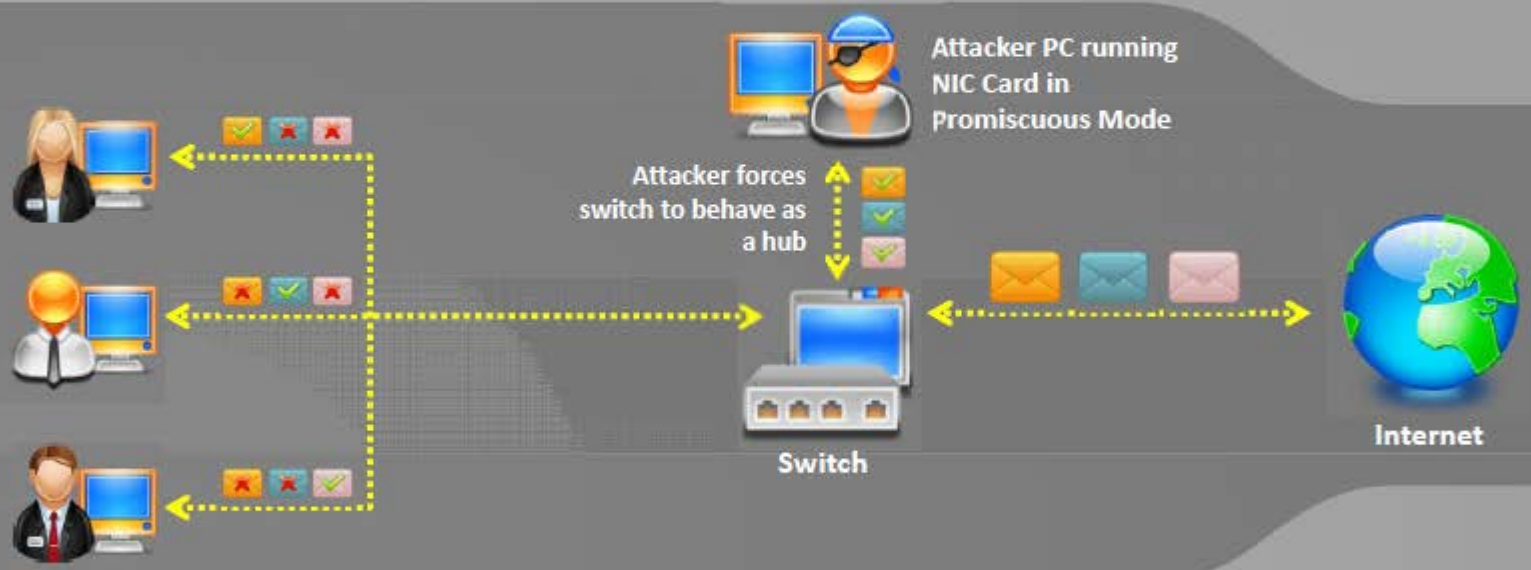
- Many enterprises' **switch ports** are open
- Anyone in the same physical location can plug into the network using an **Ethernet cable**



How a Sniffer Works

Promiscuous Mode

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



A sniffer can constantly monitor all the network traffic to a computer through the NIC by decoding the information encapsulated in the data packet

Decode Information

Types of Sniffing: Passive Sniffing

CEH Certified Ethical Hacker

01 **Passive sniffing** means sniffing through a **hub**, on a hub the traffic is sent to all ports

02 It involves only monitoring of the packets sent by others without sending **any additional data packets** in the network traffic

03 In a network that use hubs to connect systems, all **hosts on the network** can see all traffic therefore attacker can easily capture traffic going through the hub

04 Hub usage is out-dated today. Most modern networks use **switches**

Note: Passive sniffing provides significant stealth advantages over active sniffing

Types of Sniffing: Active Sniffing

CEH Certified Ethical Hacker

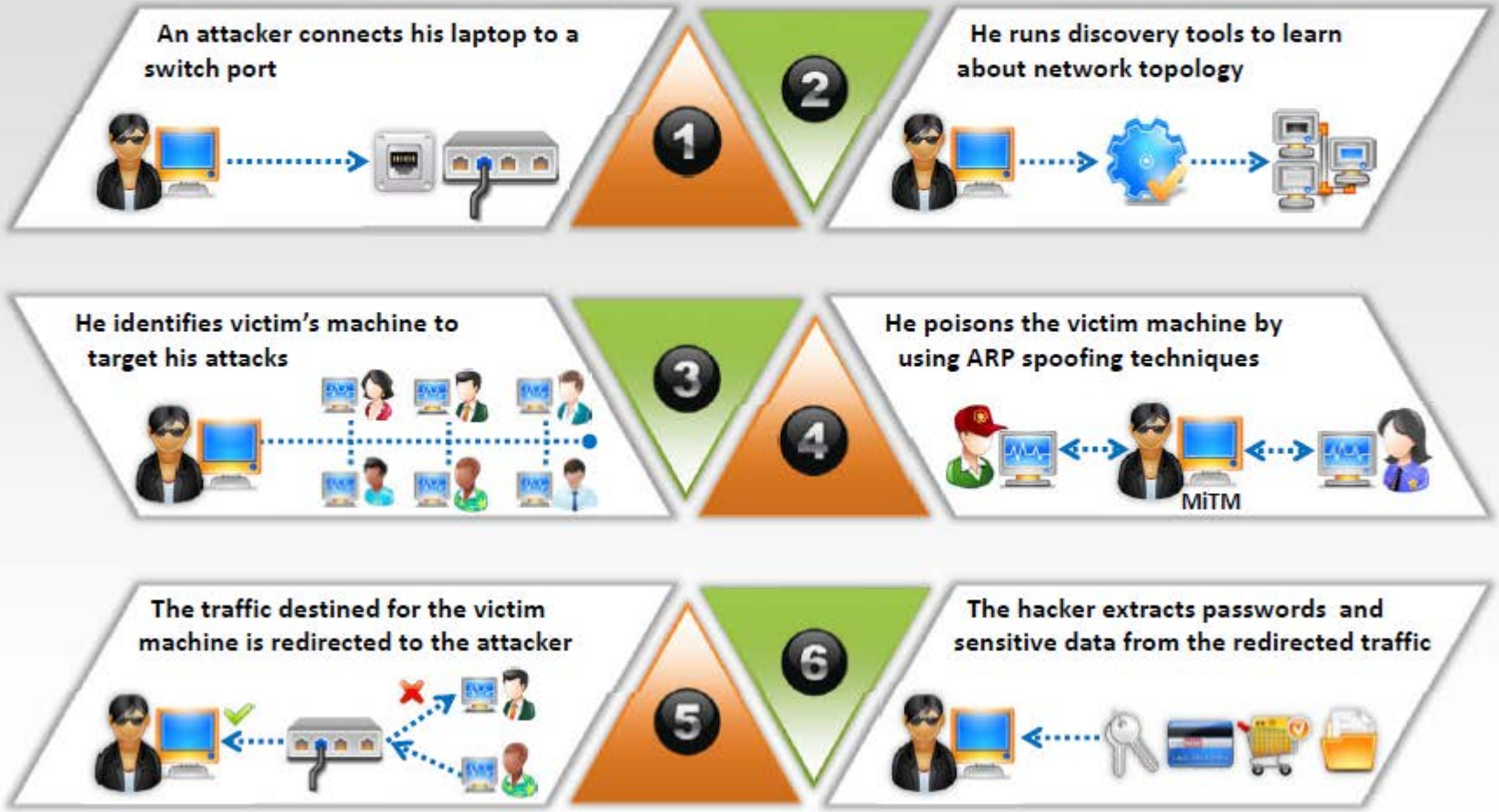
- Active sniffing is used to sniff a **switch-based network**
- Active sniffing involves **injecting address resolution packets (ARP)** into the network to flood the switch's Content Addressable Memory (CAM) table, CAM keeps track of which host is connected to which port

Active Sniffing Techniques

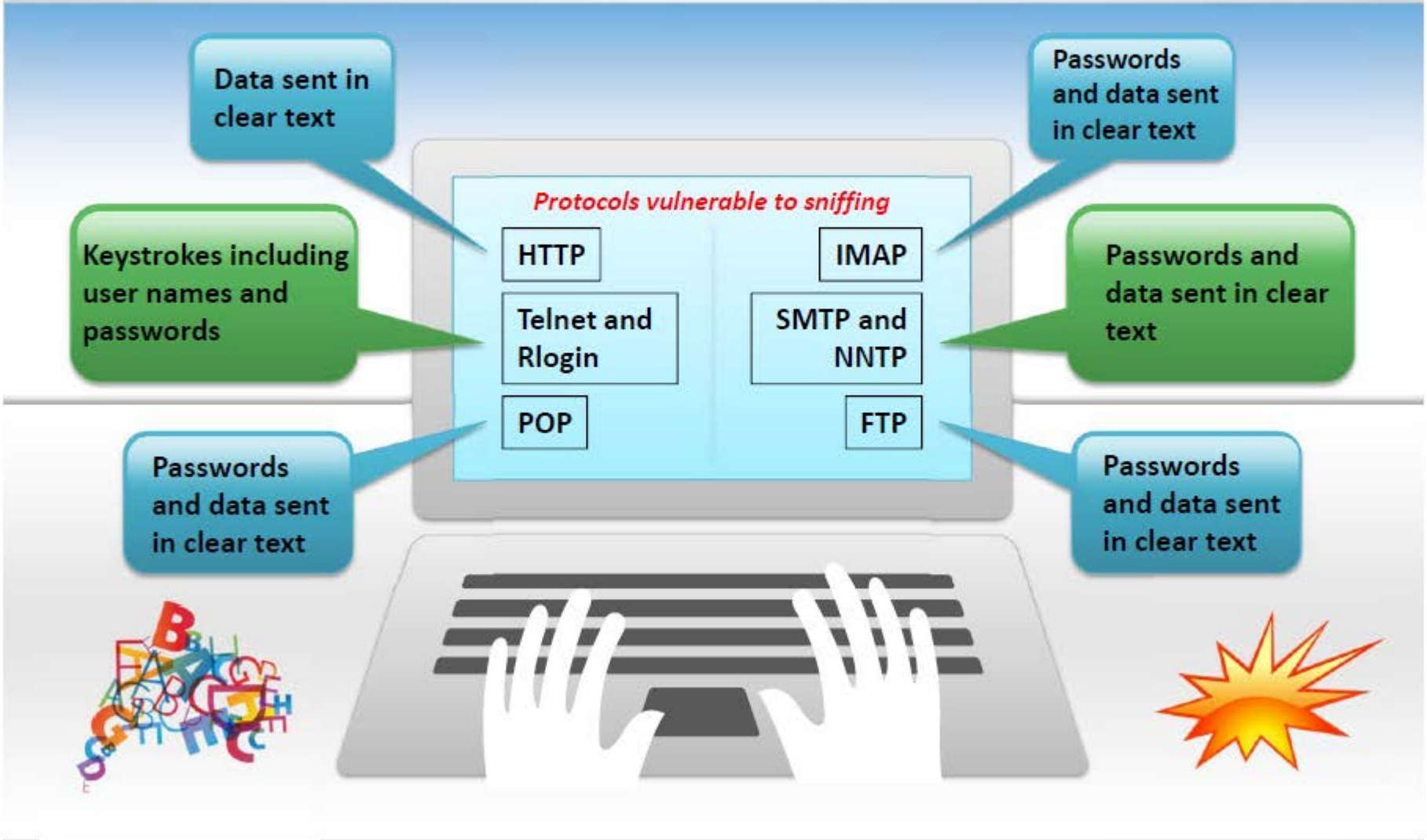
1. MAC Flooding
2. DNS Poisoning
3. ARP Poisoning
4. DHCP Attacks
5. Switch Port Stealing
6. Spoofing Attack

How an Attacker Hacks the Network Using Sniffers

C|EH Certified Ethical Hacker



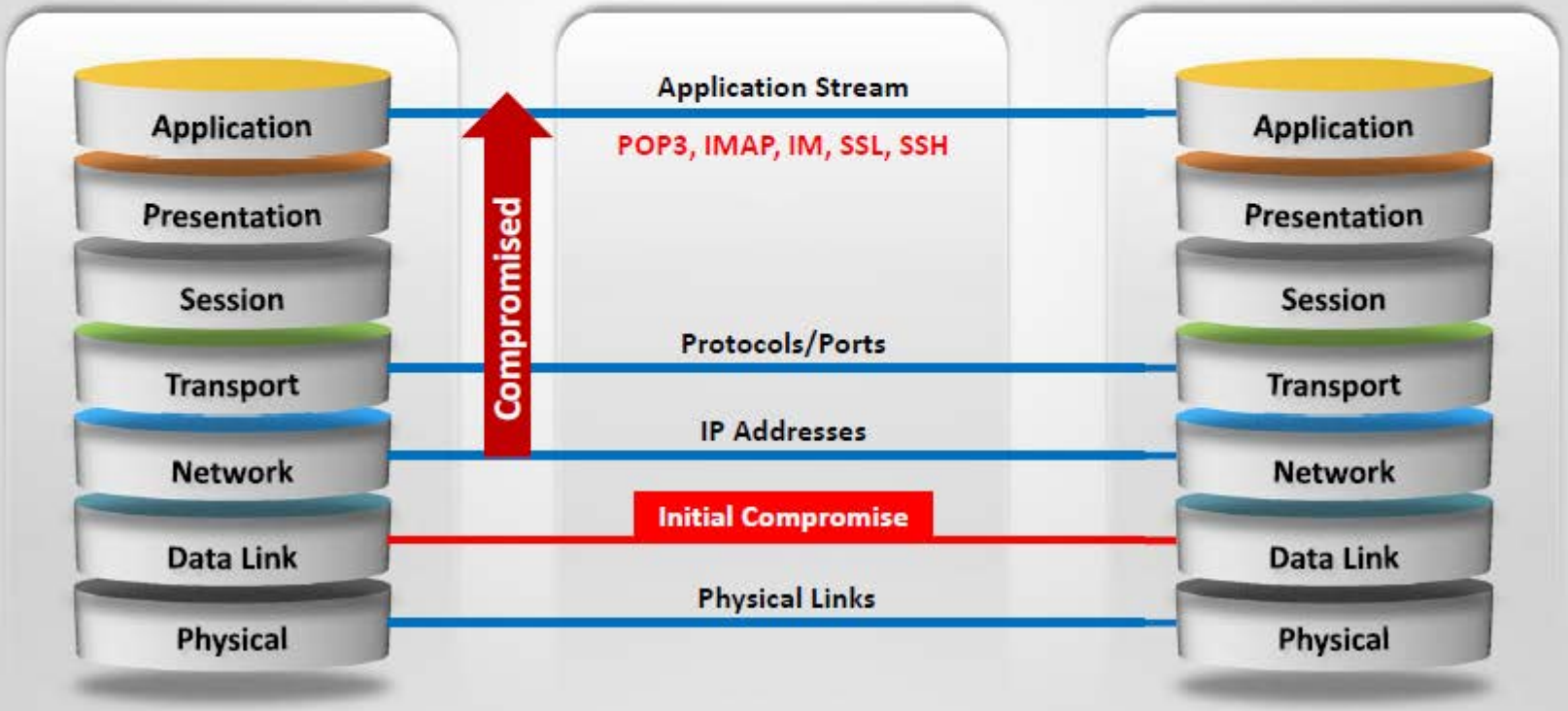
Protocols Vulnerable to Sniffing



Sniffing in the Data Link Layer of the OSI Model

C|EH Certified Ethical Hacker

- 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 Analyzer

A hardware protocol analyzer is a piece of equipment that **captures signals** without altering the traffic in a cable segment

It can be used to monitor network usage and identify **malicious network traffic** generated by hacking software installed in the network

It captures a data packet, decodes it, and analyzes its content according to certain **predetermined rules**

It allows attacker to see individual **data bytes** of each packet passing through the cable

Hardware Protocol Analyzers

C|EH Certified Ethical Hacker

Keysight N2X N5540A

Keysight E2960B

RADCOM PrismLite Protocol Analyzer

RADCOM Prism UltraLite Protocol Analyzer

FLUKE Networks OptiView® XG Network Analyzer

FLUKE Networks OneTouch™ AT Network Assistant

Wiretapping

C|EH Certified Ethical Hacker

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 something into the communication or traffic

Passive Wiretapping

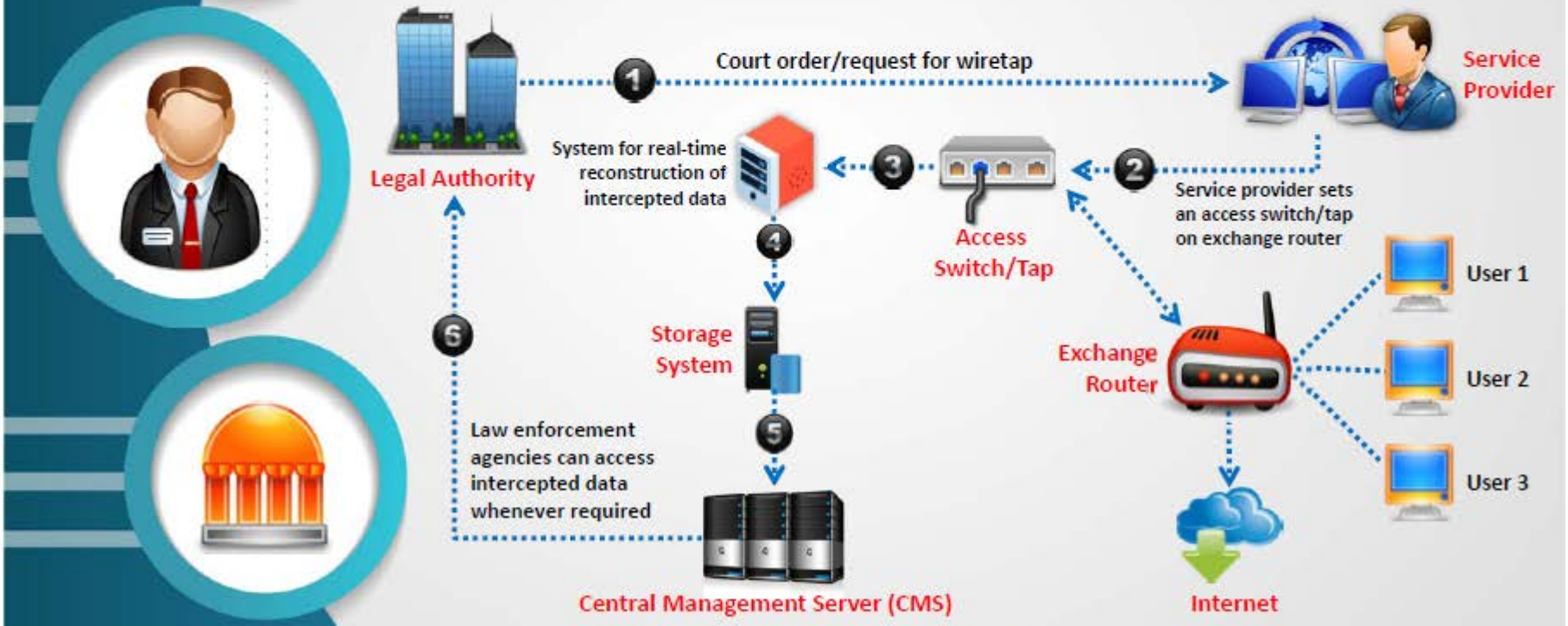
It only monitors and records the traffic and gain knowledge of the data it contains

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

Lawful Interception

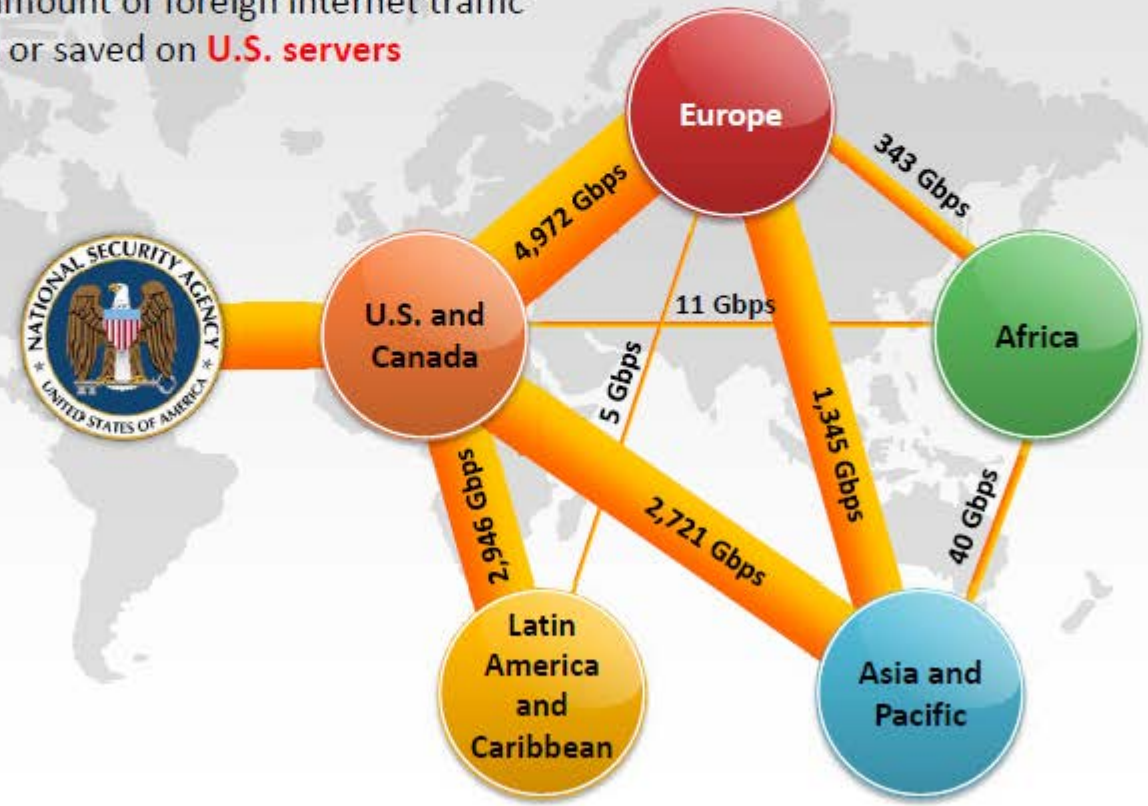
C|EH Certified Ethical Hacker

Lawful interception refers to legally **intercepting data communication** between two end points for surveillance on the traditional telecommunications, VoIP, data, and multiservice networks

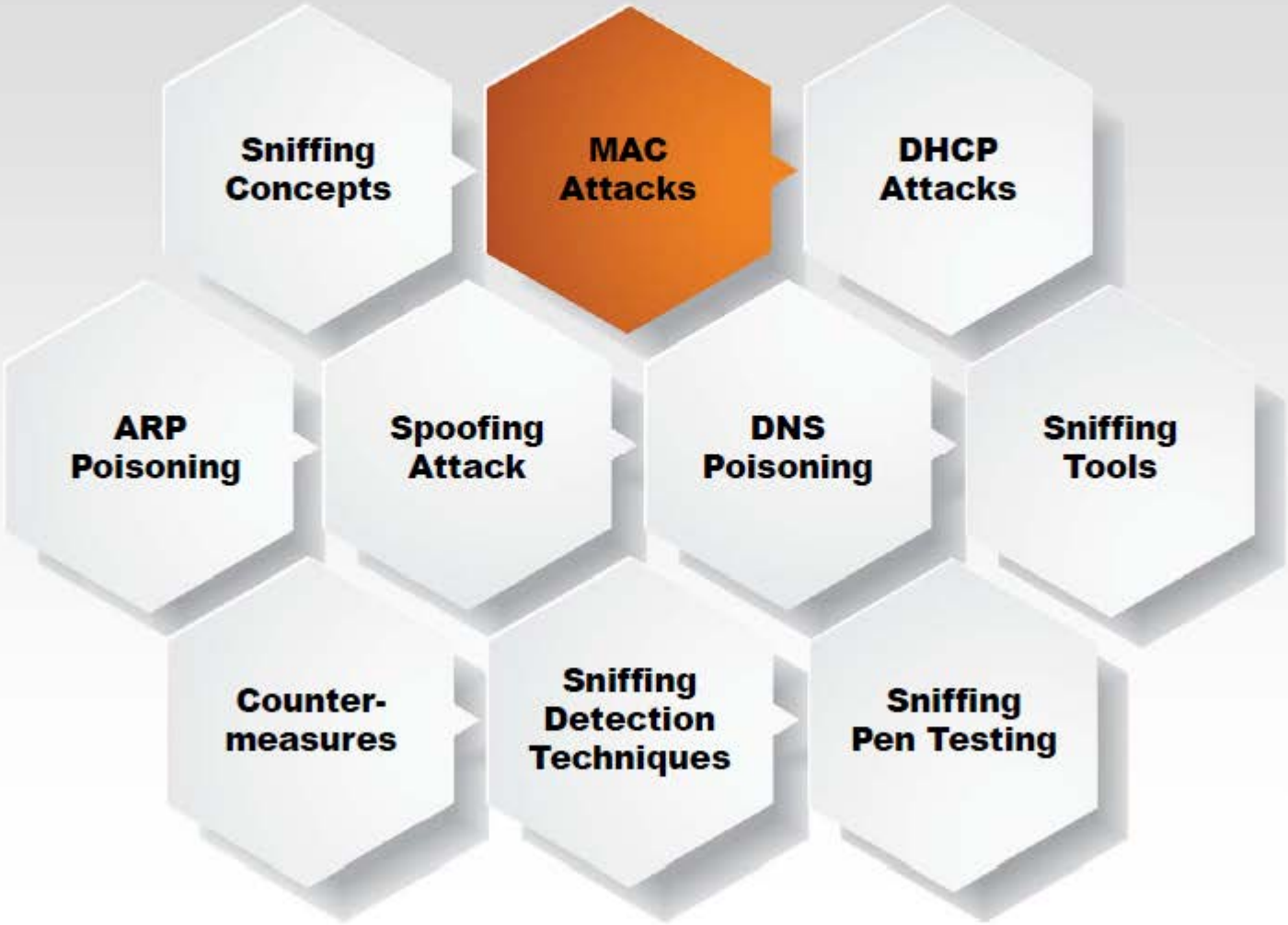


Wiretapping Case Study: PRISM

- PRISM stands for "**Planning Tool for Resource Integration**, **Synchronization**, and **Management**," and is a "**data tool**" designed to collect and process "**foreign intelligence**" that passes through American servers
- NSA wiretaps a huge amount of foreign internet traffic that is routed through or saved on **U.S. servers**



Module Flow

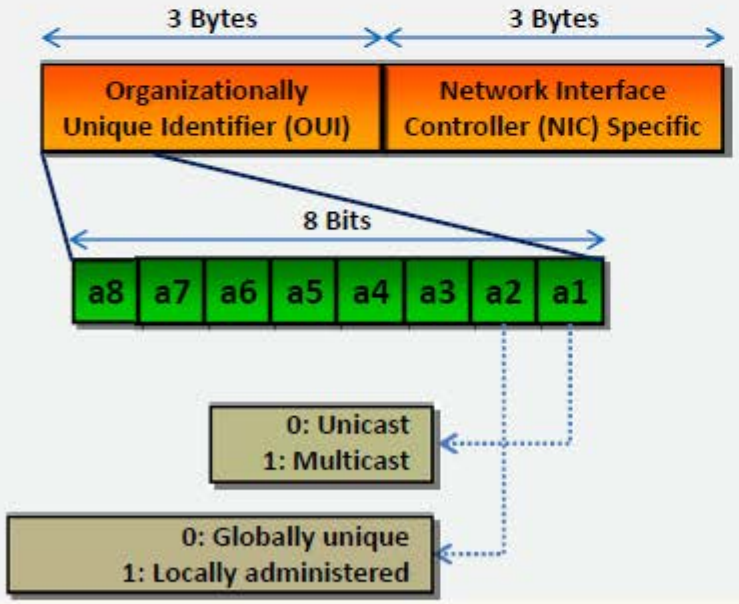


MAC Address/CAM Table

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 VLAN parameters

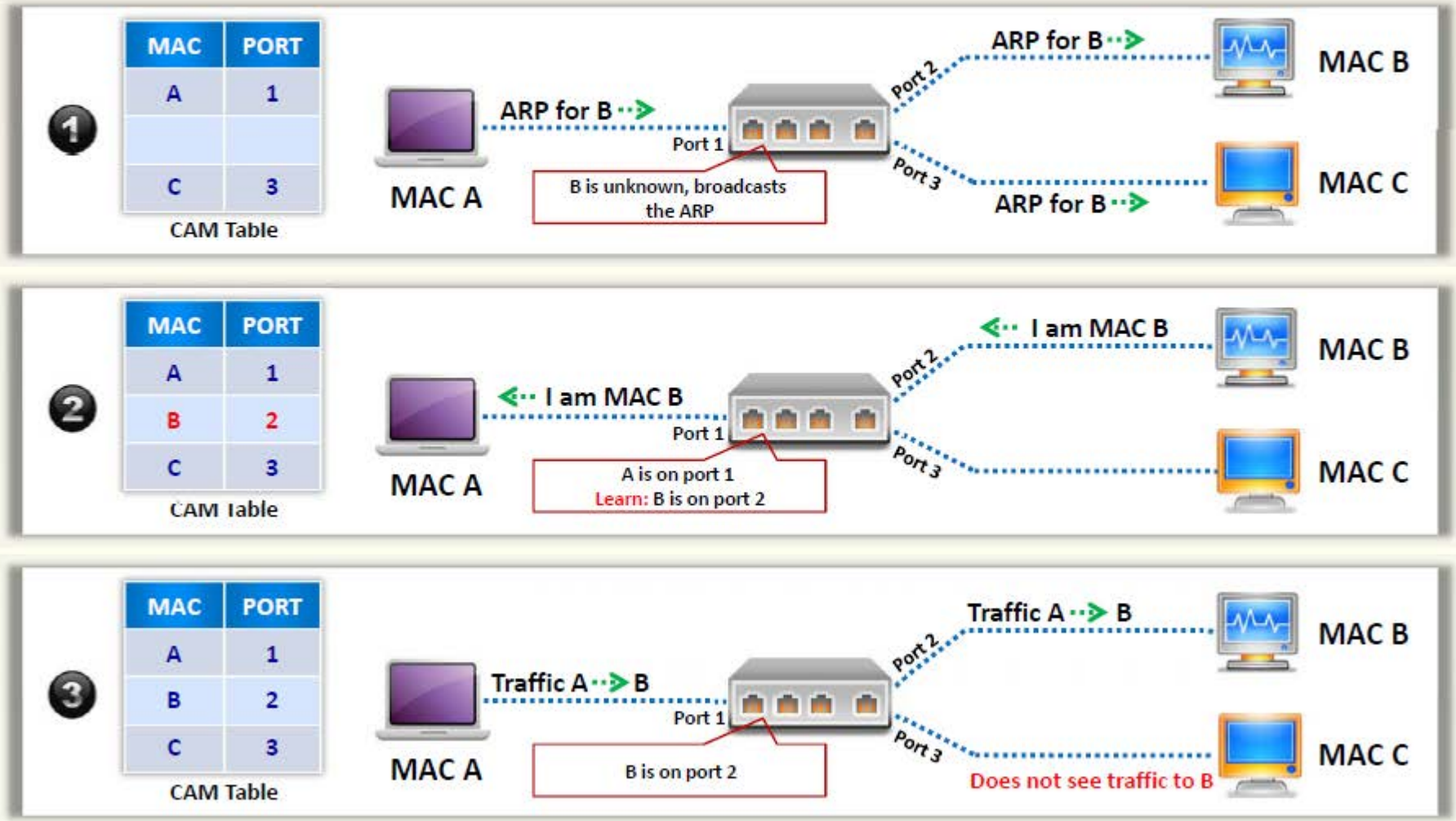
MAC Address



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

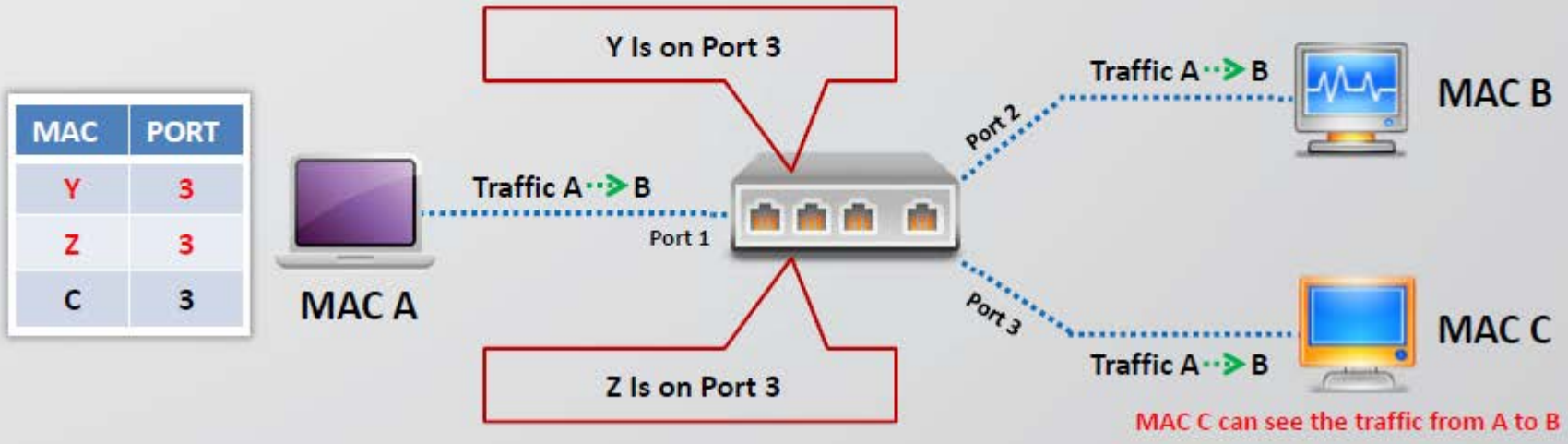


What Happens When CAM Table Is Full?

Once the CAM table on the switch is full, additional ARP request **traffic will flood every port on the switch**

This will **change the behavior of the switch** to reset to it's 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

Switch then **acts as a hub** by broadcasting packets to all machines on the network and 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

Command Prompt

```
macof -i eth1
18:b1:22:12:85:15 13:15:5a:6b:45:c4 0.0.0.0.25684 > 0.0.0.0.86254: S 2658741236:1235486715(0) win 512
12:a8:d8:15:4d:3b ab:4c:cd:5f:ad:cd 0.0.0.0.12387 > 0.0.0.0.78962: S 1238569742:782563145(0) win 512
13:3f:ab:14:25:95 66:ab:6d:4d:b2:85 0.0.0.0.45638 > 0.0.0.0.4568: S 123587152:456312589(0) win 512
a2:2f:85:12:ac:2f 12:85:2f:52:41:25 0.0.0.0.42358 > 0.0.0.0.35842: S 3256789512:3568742158(0) win 512
96:25:a3:5c:52:af 82:12:41:1d:ac:d6 0.0.0.0.45213 > 0.0.0.0.2358: S 3684125687:3256874125(0) win 512
a2:c2:b5:8c:6d:2a 5a:cc:f6:41:8d:df 0.0.0.0.12354 > 0.0.0.0.78521: S 1236542358:3698521475(0) win 512
55:42:ac:85:c5:96 a5:5f:ad:9d:12:aa 0.0.0.0.123 > 0.0.0.0.12369: S 8523695412:8523698742(0) win 512
a9:4d:4c:5a:5d:ad a4:ad:5f:4d:e9:ad 0.0.0.0.23685 > 0.0.0.0.45686: S 236854125:365145752(0) win 512
s3:e5:1a:25:2w:a3 25:35:a8:5d:af:fc 0.0.0.0.23685 > 0.0.0.0.85236: S 8623574125:3698521456(0) win 512
```

http://monkey.org

Switch Port Stealing

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

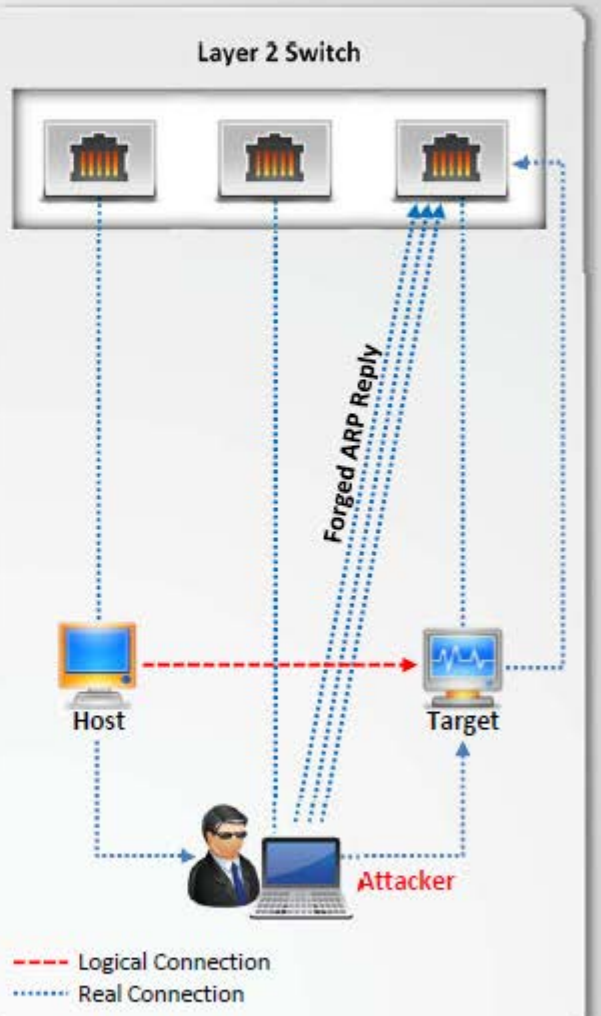
Attacker floods the switch with forged gratuitous ARP packets with target MAC address as source and his own MAC address as destination

A race condition of attacker's flooded packets and target host packets will occur and thus switch has to change his MAC address binding constantly between two different ports

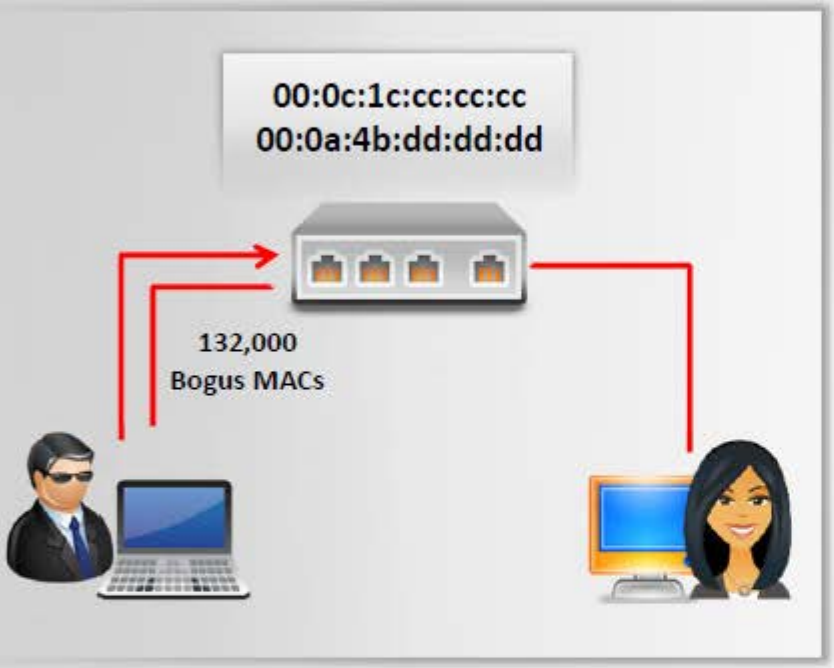
In such case if attacker is fast enough, he will able to direct the packets intended for the target host toward his switch port

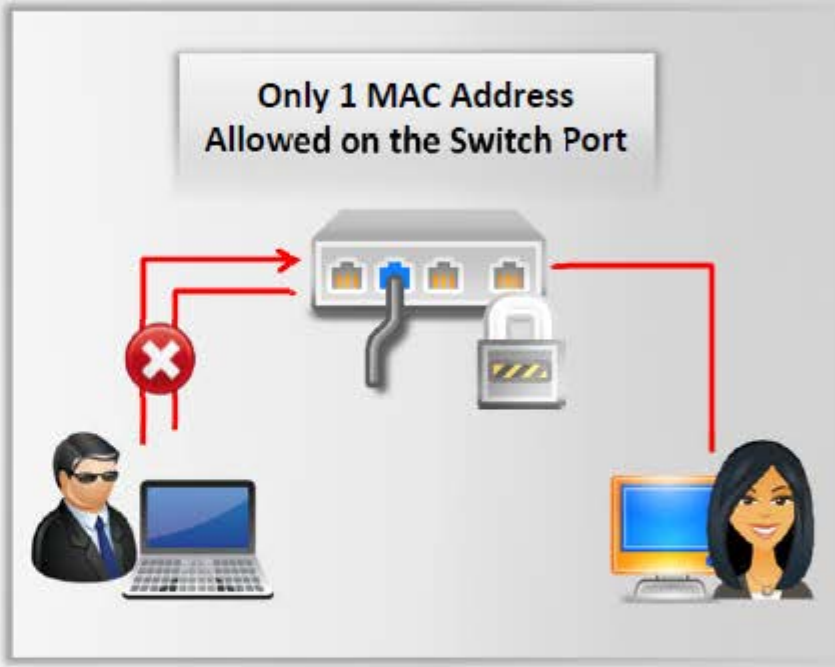
Attacker now manages to steal the target host switch port and sends ARP request to stolen switch port to discover target hosts' IP address

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



How to Defend against MAC Attacks



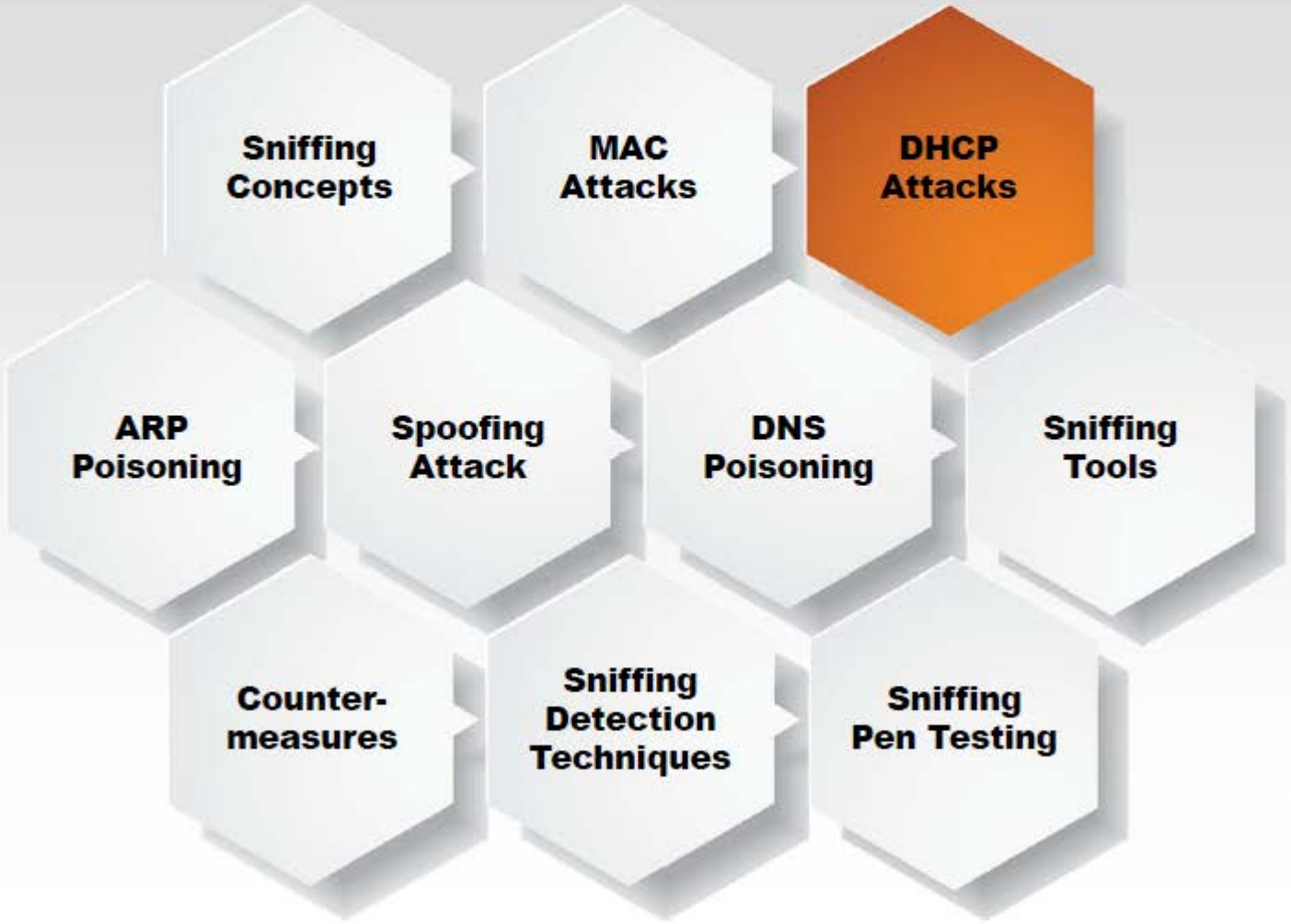


Configuring Port Security on Cisco switch:

- 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

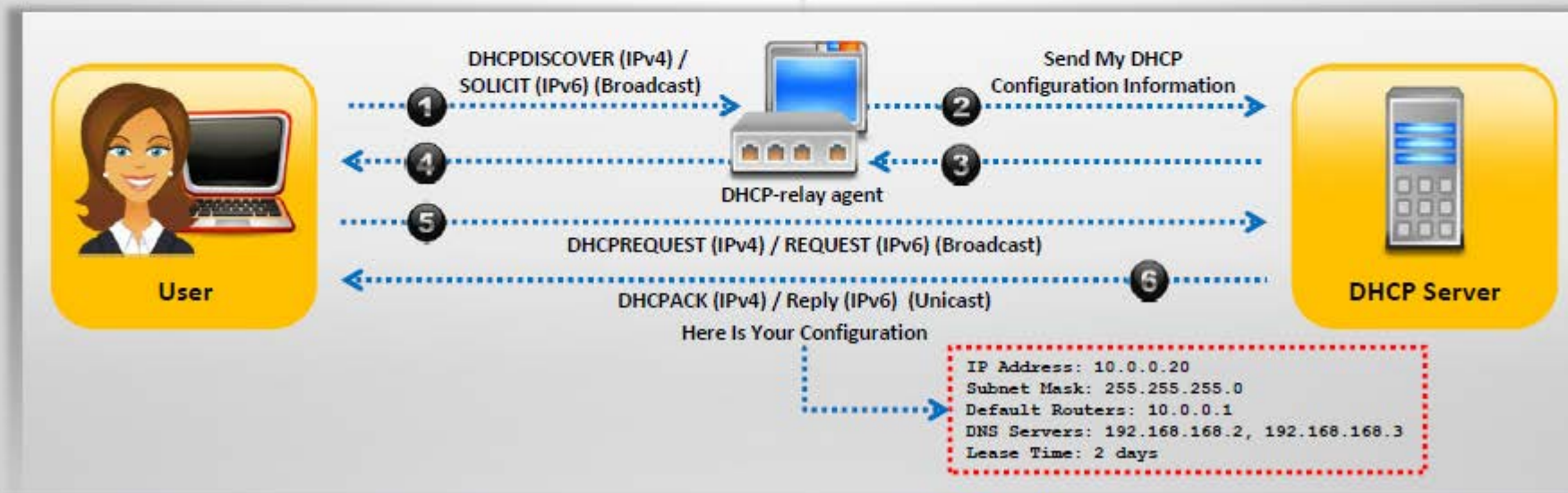
Module Flow



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**

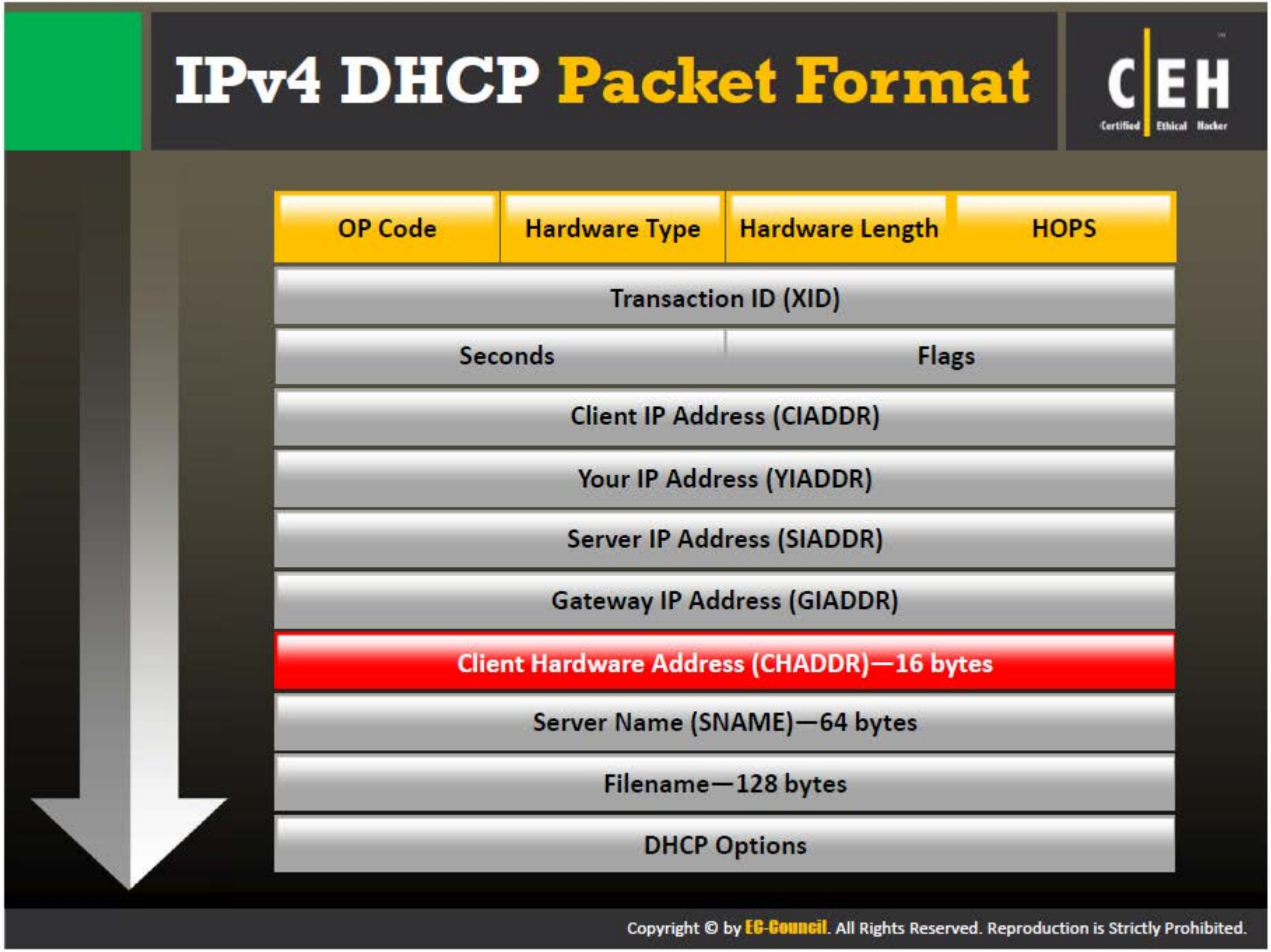
1. Client broadcasts **DHCPDISCOVER/SOLICIT** request asking for DHCP Configuration Information
2. DHCP-relay agent captures the client request and **unicasts** it to the DHCP servers available in the network
3. DHCP server unicasts **DHCPOFFER/ADVERTISE**, which contains client and server's MAC address
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

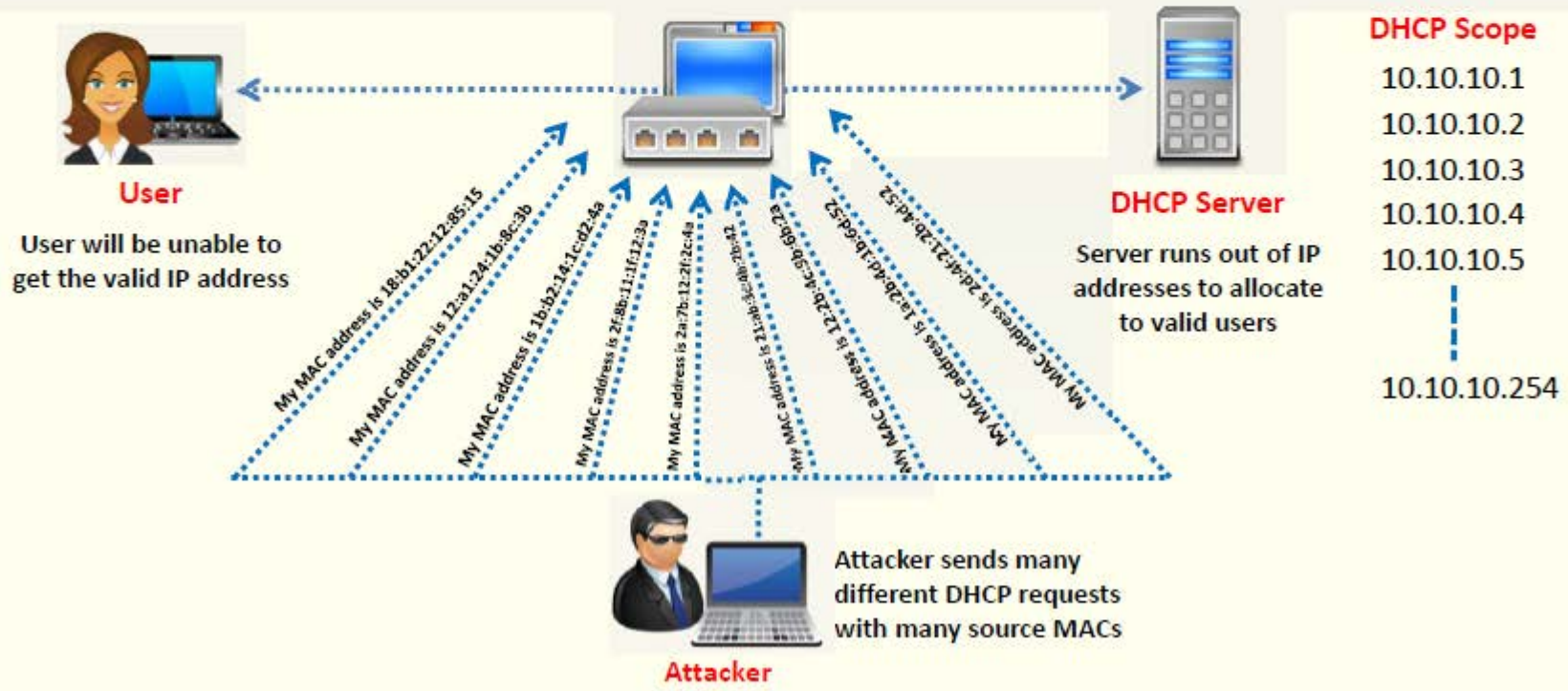
DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client broadcast to locate available DHCP servers
DHCPOffer	Advertise	Server to client in response to DHCPDISCOVER with offer of configuration parameters
DHCPRequest	Request, Confirm, Renew, Rebind	Client message to servers either (a) Requesting 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
- As a result legitimate user is **unable to obtain or renew an IP address** requested via DHCP, failing access to the network access



DHCP Starvation Attack Tools

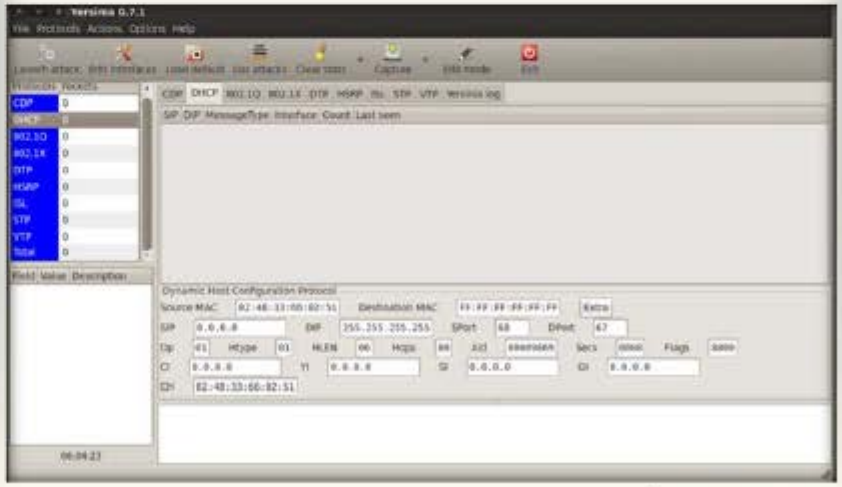
Dhcpstarv

- dhcpstarv implements DHCP starvation attack. It requests **DHCP leases** on specified interface, saves them, and renews on regular basis

http://dhcpstarv.sourceforge.net

Yersinia

- Yersinia is a network tool designed to take advantage of some **weakeness** in different network protocols
- It pretends to be a solid framework for analyzing and testing the **deployed networks and systems**

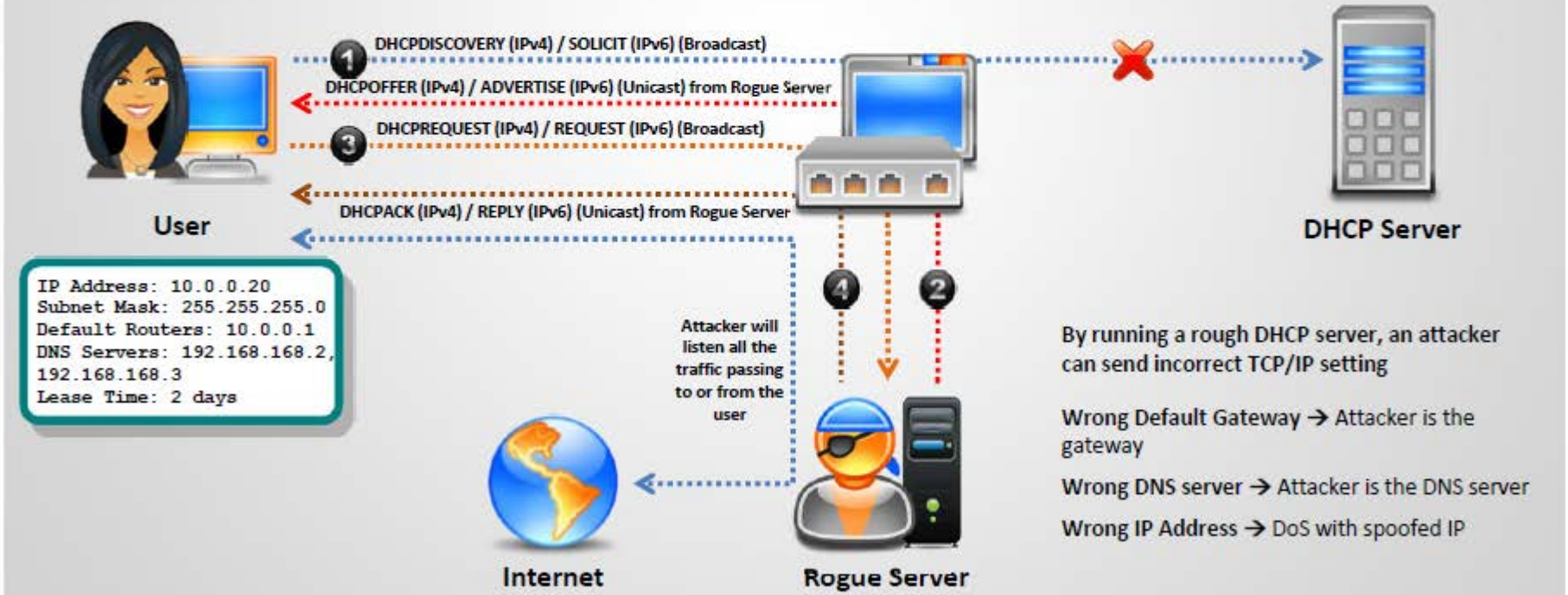


http://www.yersinia.net

Rogue DHCP Server Attack

Attacker sets rogue DHCP server in the network and responds to DHCP requests with bogus IP addresses; this results in compromised network access

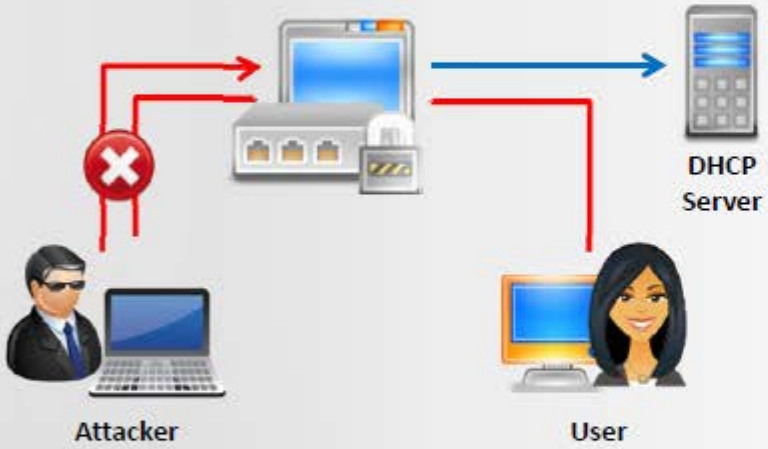
This attack works in conjunction with the DHCP Starvation attack; attacker sends TCP/IP setting to the user after knocking him/her out from the genuine DHCP server



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



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
```

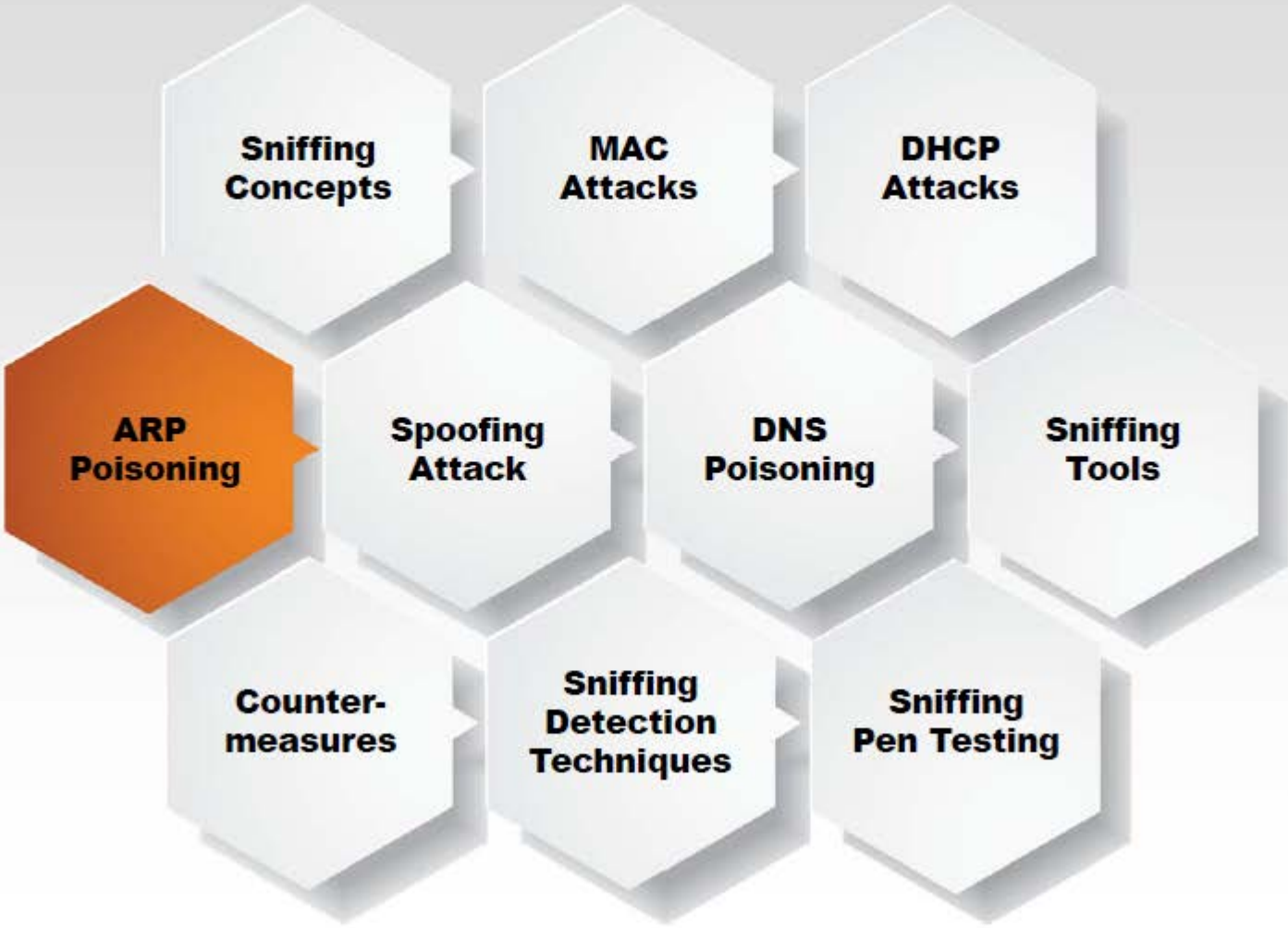
Enable **DHCP snooping** that allows switch to accept DHCP transaction coming only from a trusted port

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

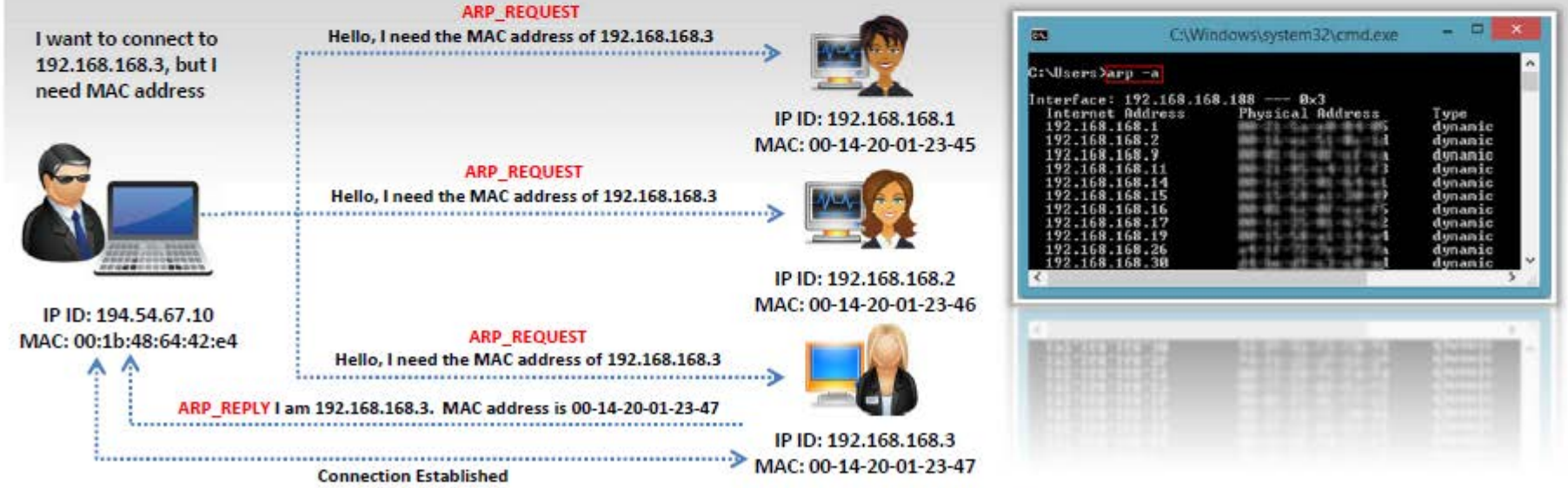
Note: All ports in the VLAN are not trusted by default

Module Flow



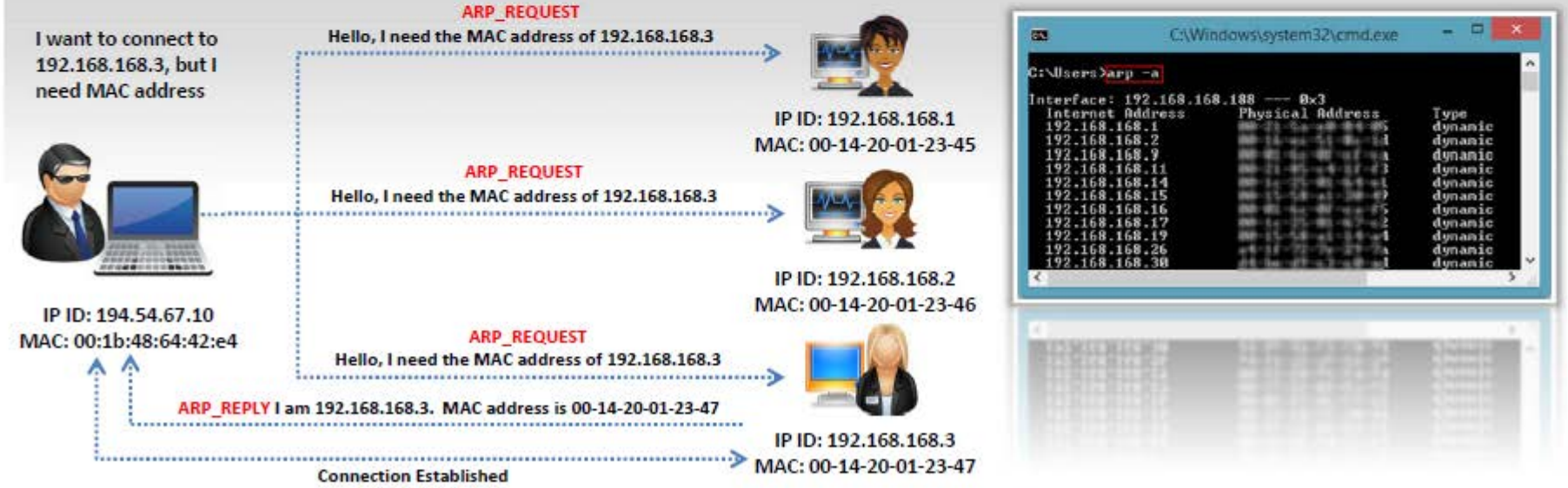
What Is Address Resolution Protocol (ARP)?

- 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 communication will take place



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 communication will take place



ARP Spoofing Attack

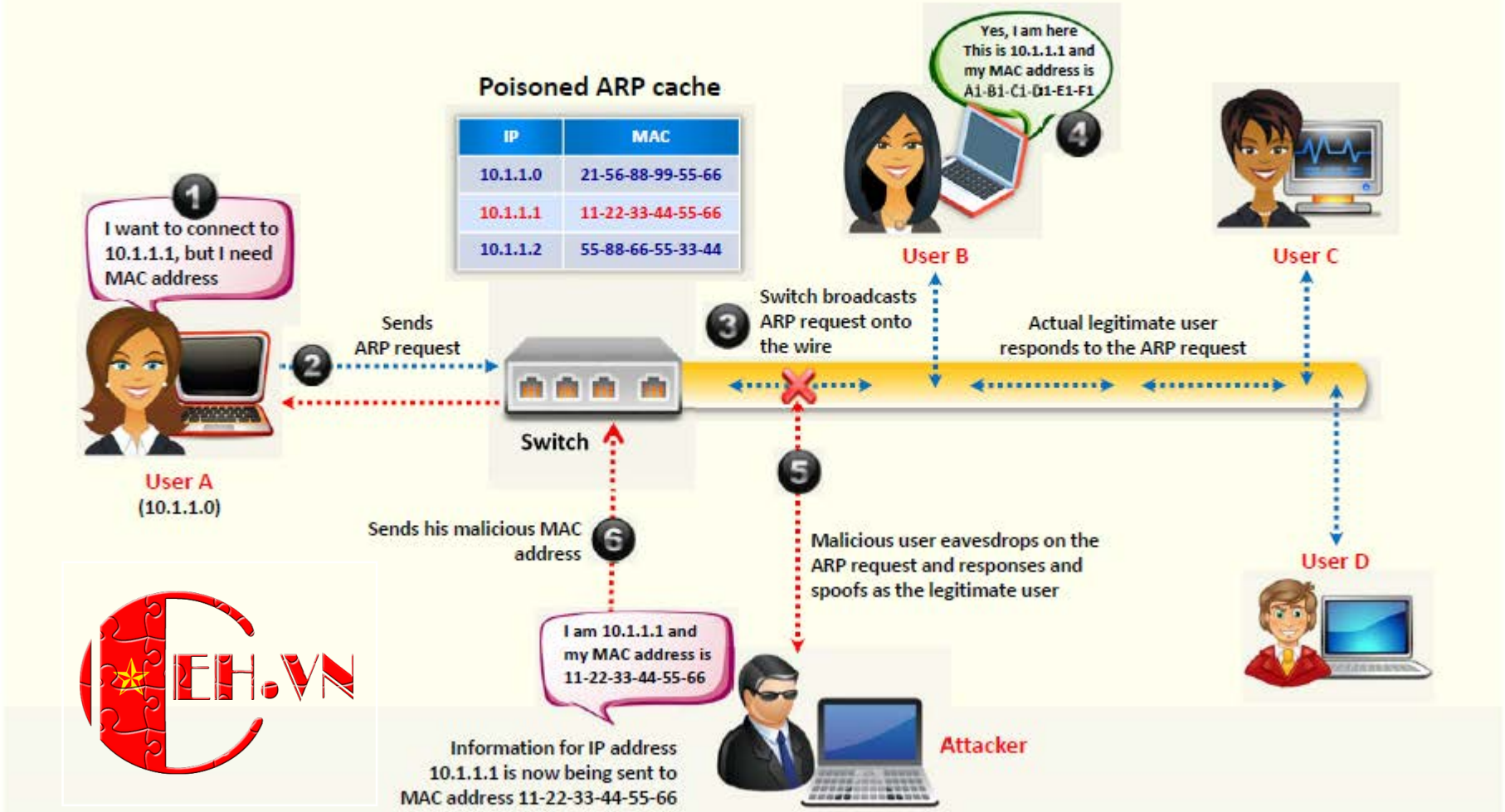
ARP packets can be **forged** to send data to the attacker's machine

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**

How Does ARP Spoofing Work



Threats of ARP Poisoning

C|EH Certified Ethical Hacker

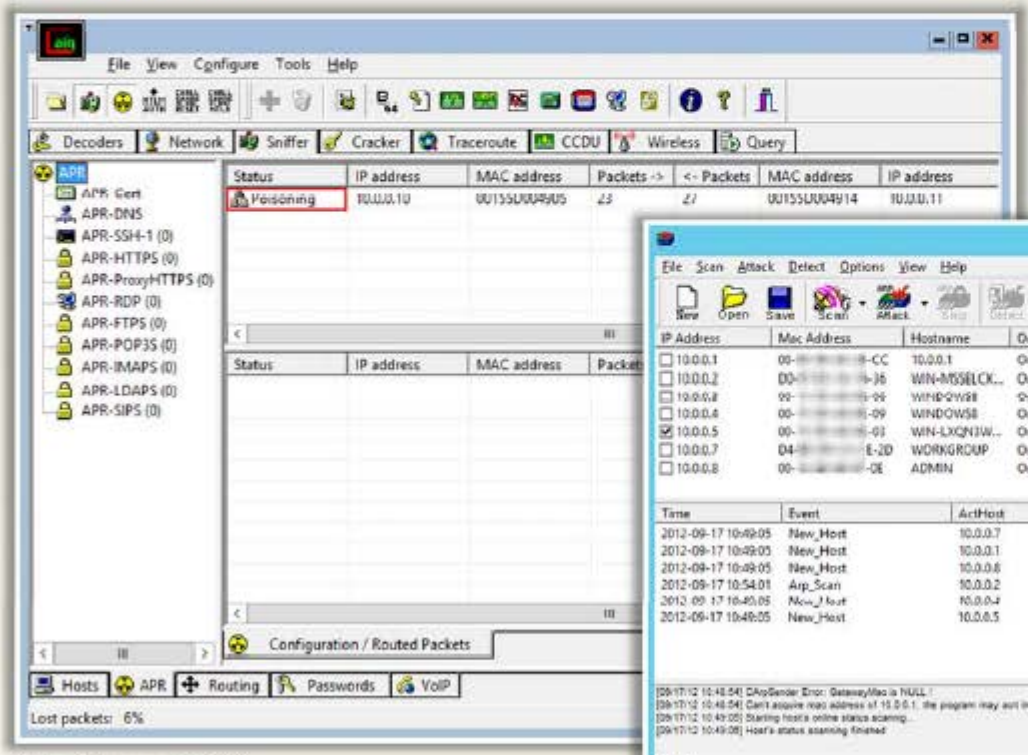
Using fake **ARP messages**, an attacker can divert all communications between two machines so that all traffic is exchanged via his/her PC

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

ARP Poisoning Tools: Cain & Abel and WinArpAttacker

Cain & Abel

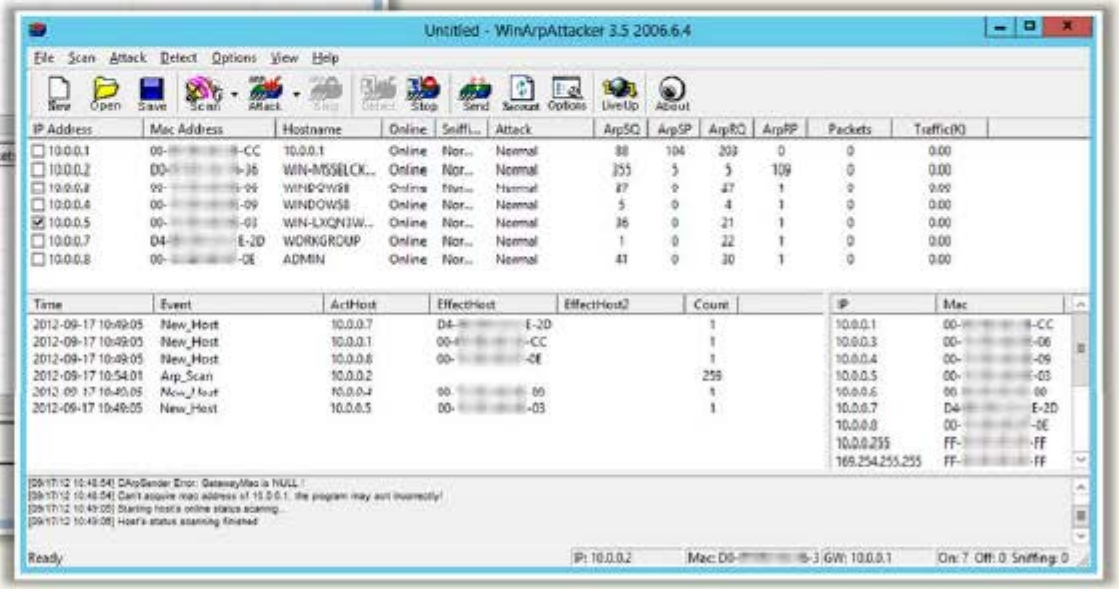
- Cain & Abel allows sniffing packets of various protocols on **switched LANs** by hijacking IP traffic of multiple hosts concurrently



http://www.oxid.it

WinArpAttacker

WinArpAttacker sends **IP conflict packets** to target computers as fast as possible and diverts all communications

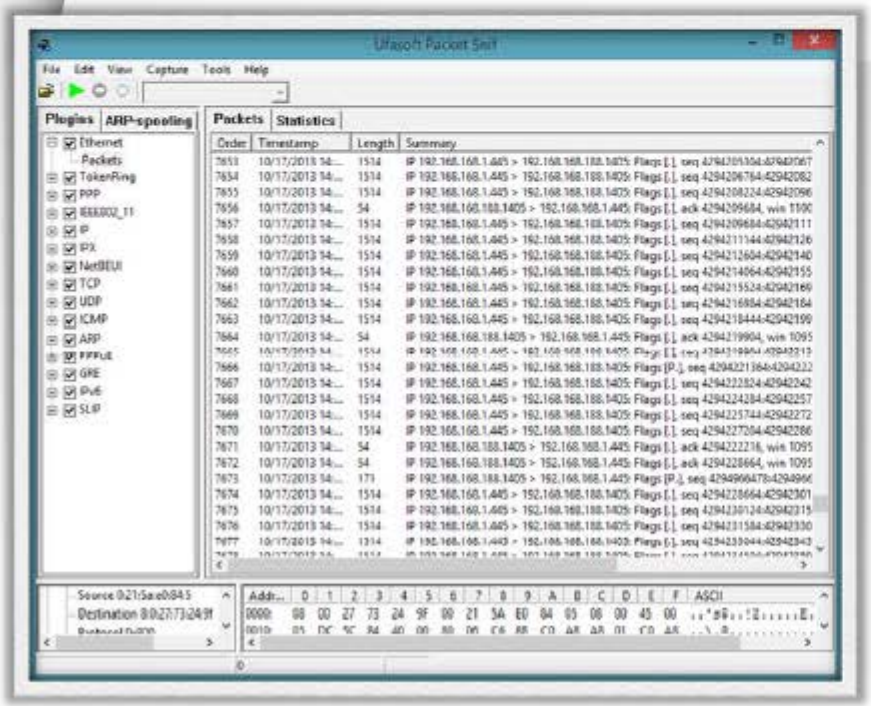


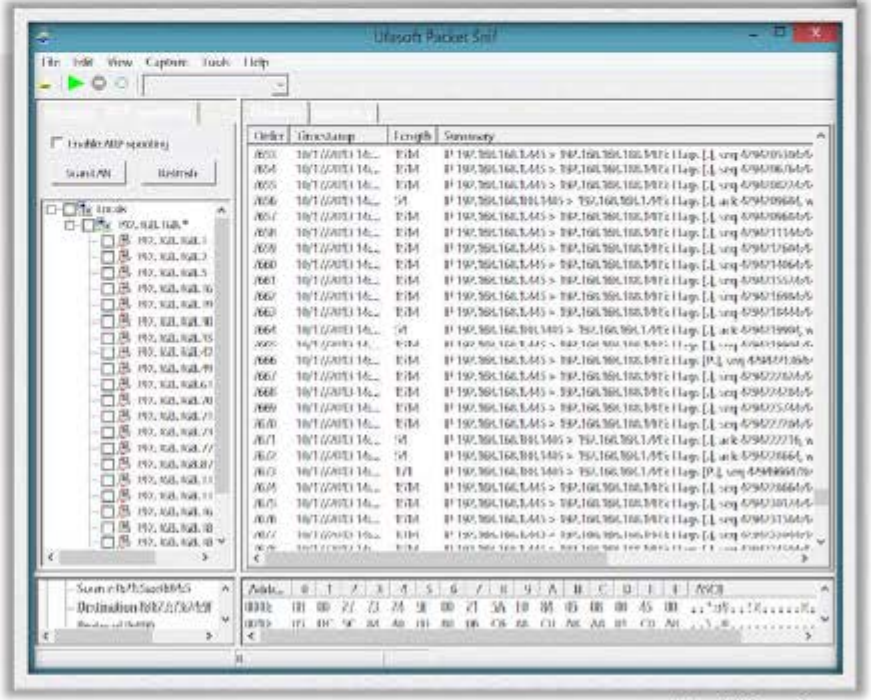
http://www.xfocus.net

ARP Poisoning Tool: Ufasoft Snif

C|EH Certified Ethical Hacker

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



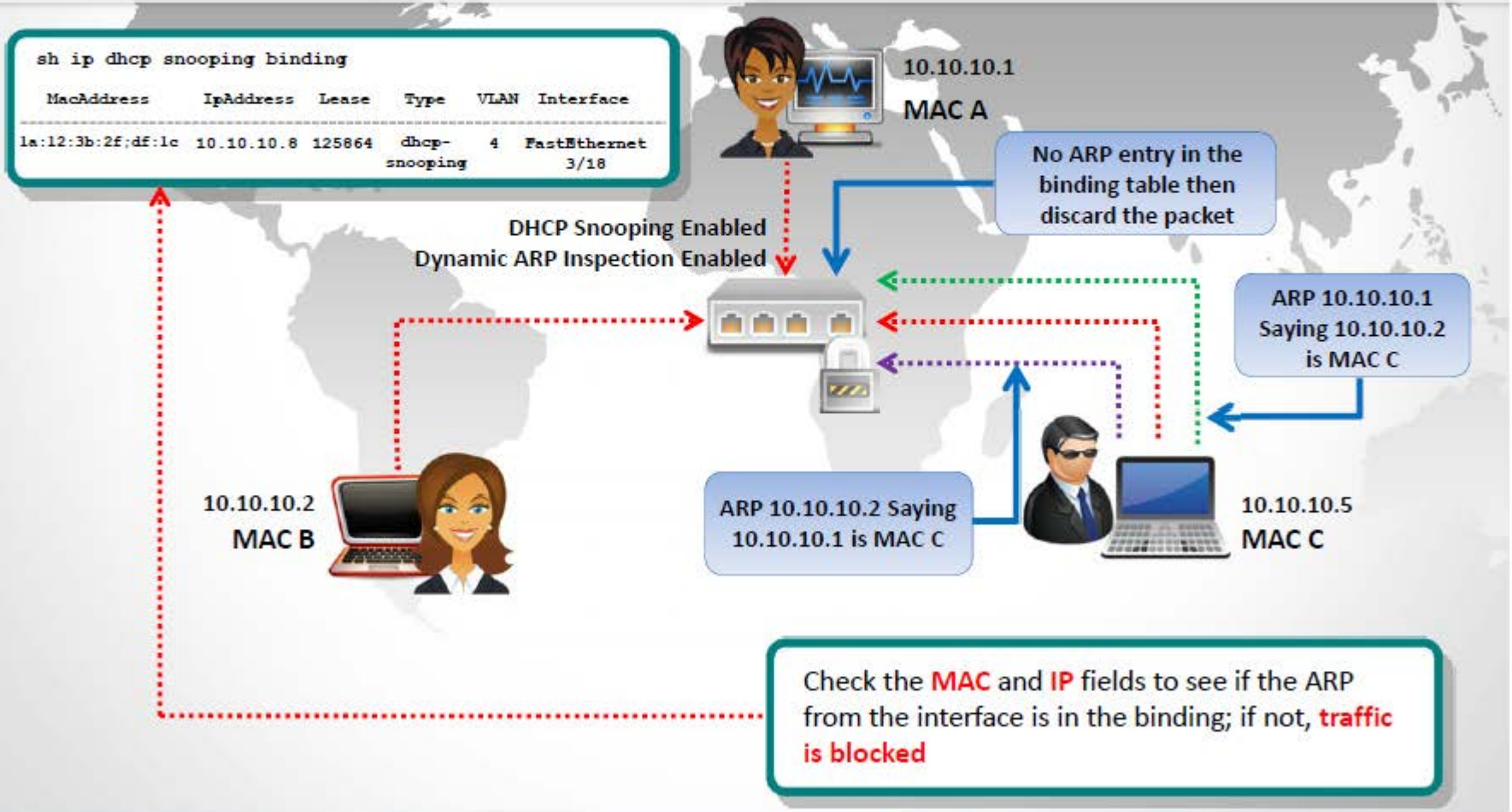


http://ufasoft.com

How to Defend Against ARP Poisoning

C|EH Certified Ethical Hacker

Implement Dynamic ARP Inspection Using DHCP Snooping Binding Table



Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

C|EH Certified Ethical Hacker

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

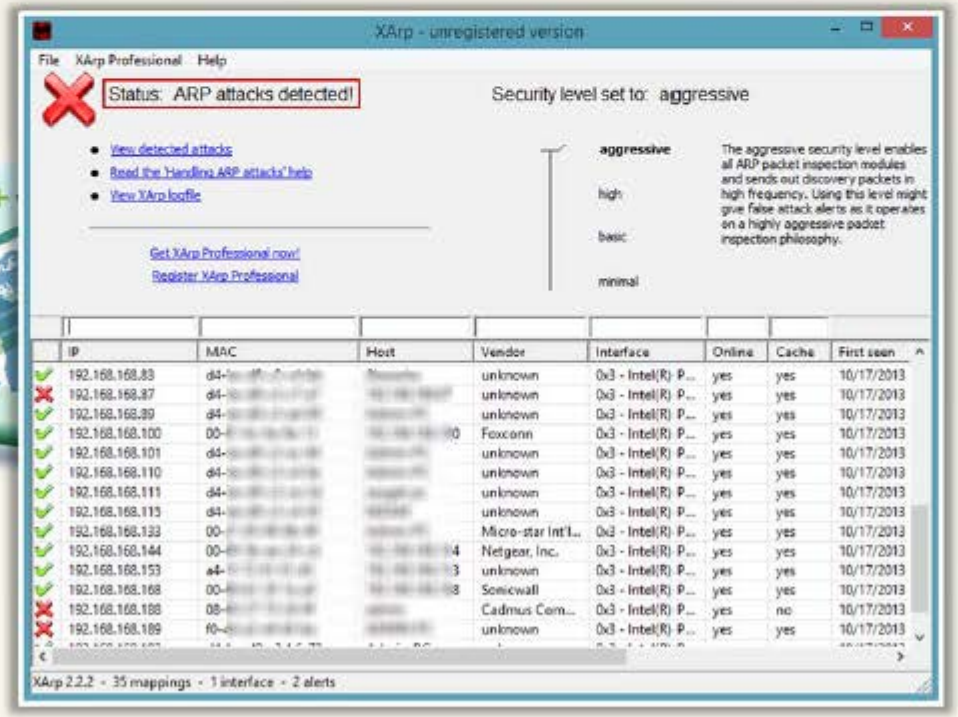
```
Switch(config)# ip arp inspection vlan 10
Switch(config)# ^Z
Switch# show ip arp inspection
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan  Configuration  Operation  ACL Match   Static ACL
 10     Enabled       Active
Vlan  ACL 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.ffff/192.168.10.1/05:37:31 UTC
Mon Mar 1 2012])
```

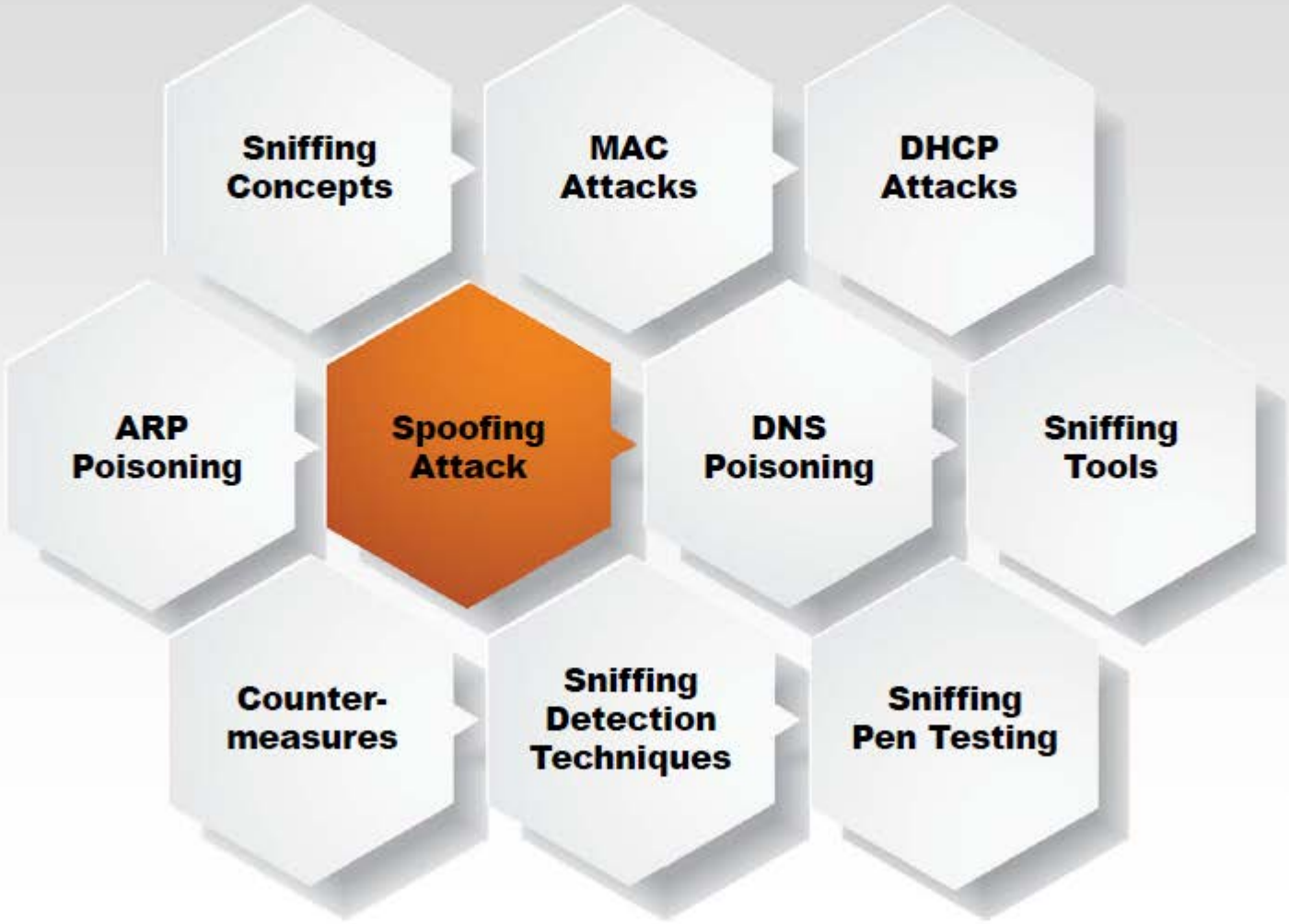
ARP Spoofing Detection: XArp

- XArp helps users to detect **ARP attacks** and keep their data private
- It allows administrators to **monitor whole subnets** for ARP attacks
- Different **security levels** and fine tuning possibilities allow normal and power users to efficiently use XArp to detect ARP attacks



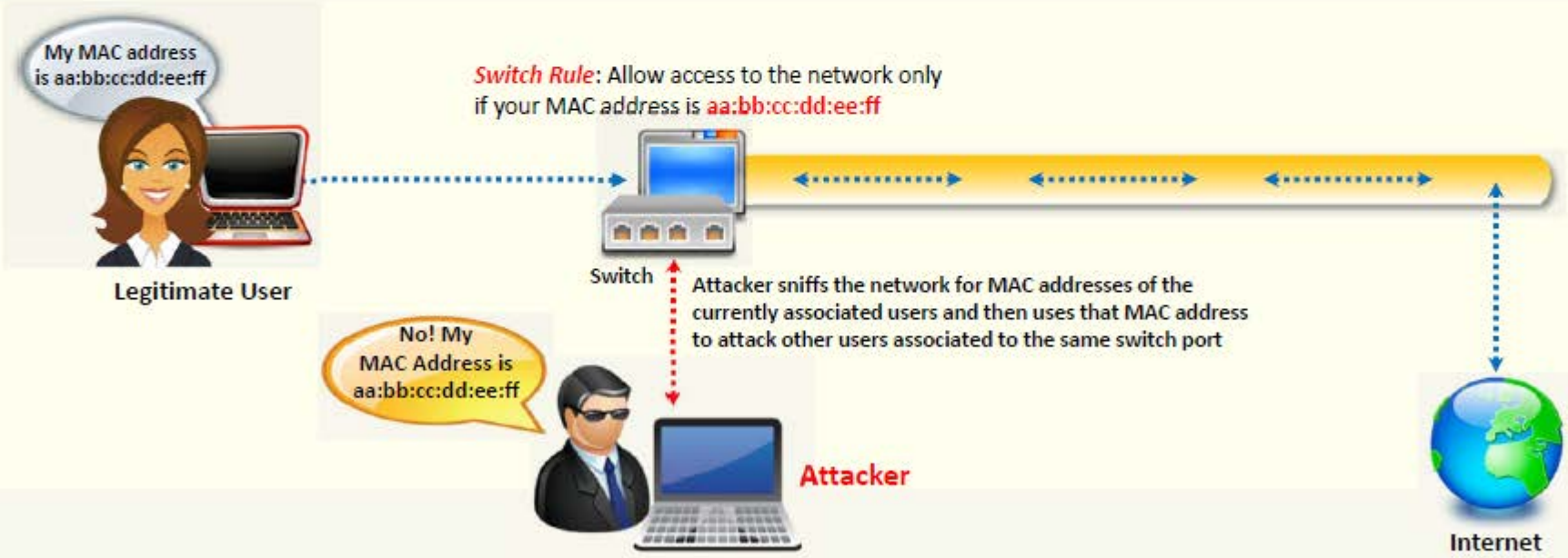
http://www.chrismc.de

Module Flow



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 already on the network



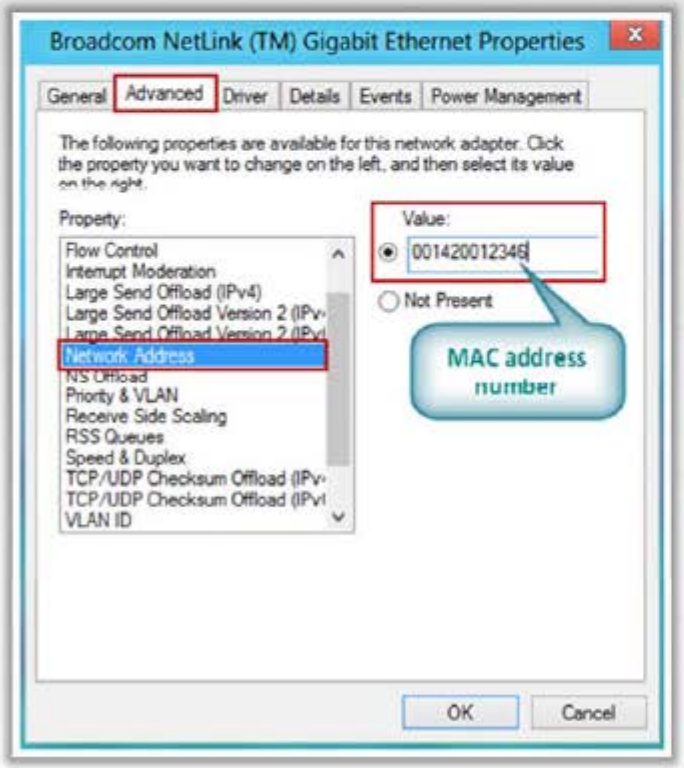
Note: This technique can be used to bypass Wireless Access Points' MAC filtering

MAC Spoofing Technique: Windows

C|EH Certified Ethical Hacker

In Windows 8 OS

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



1. Go to **Right bottom** of the screen → **Settings** → **Control Panel** → **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 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)

C|EH Certified Ethical Hacker

Method 2: Steps to change MAC address in Registry

- Go to **Start** → **Run**, type **regedt32** to start registry editor

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

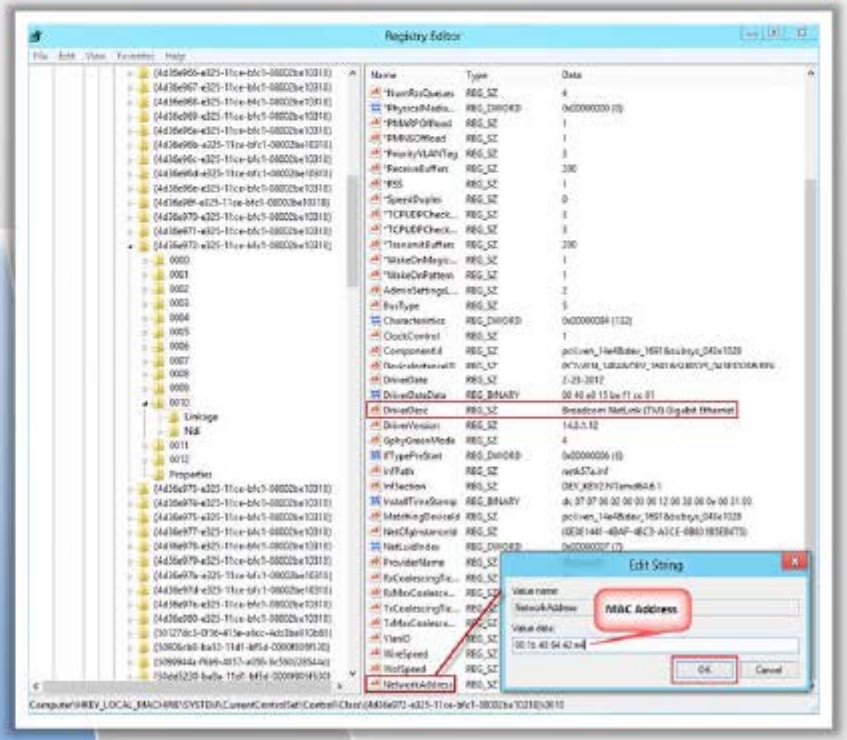
- Go to "**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}** and double click on it to expand the tree

- 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

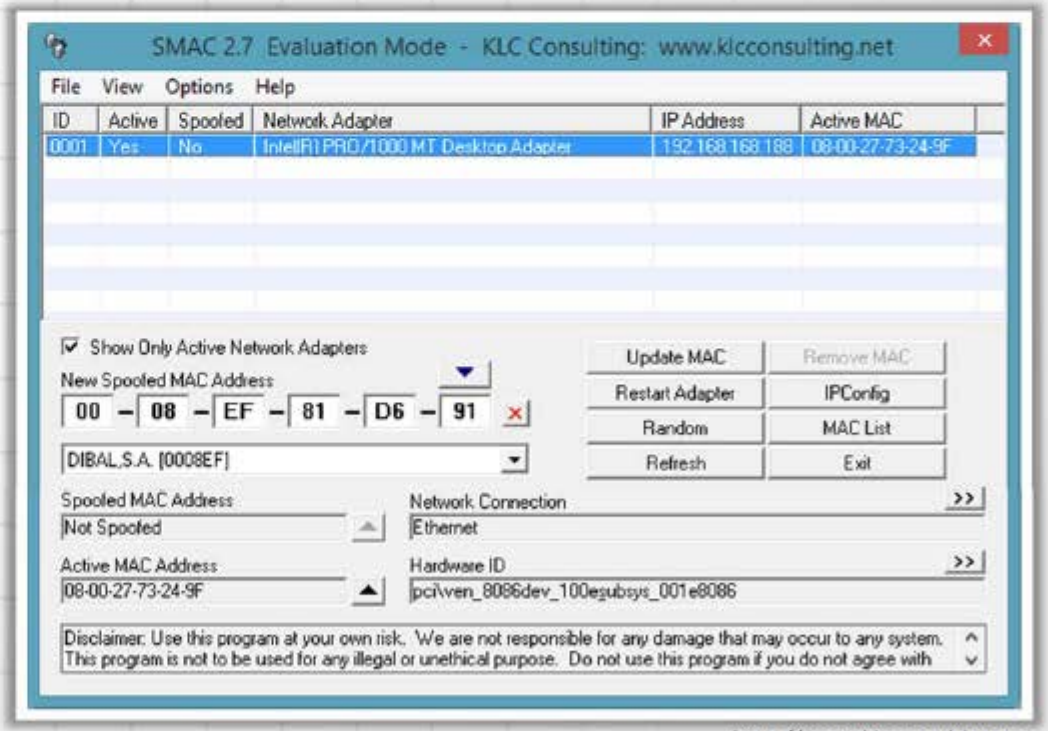


MAC Spoofing Tool: SMAC

SMAC is a MAC Address Changer (Spoofer) that allows users to **change MAC address** for any network interface cards (NIC) on the Windows systems

Features

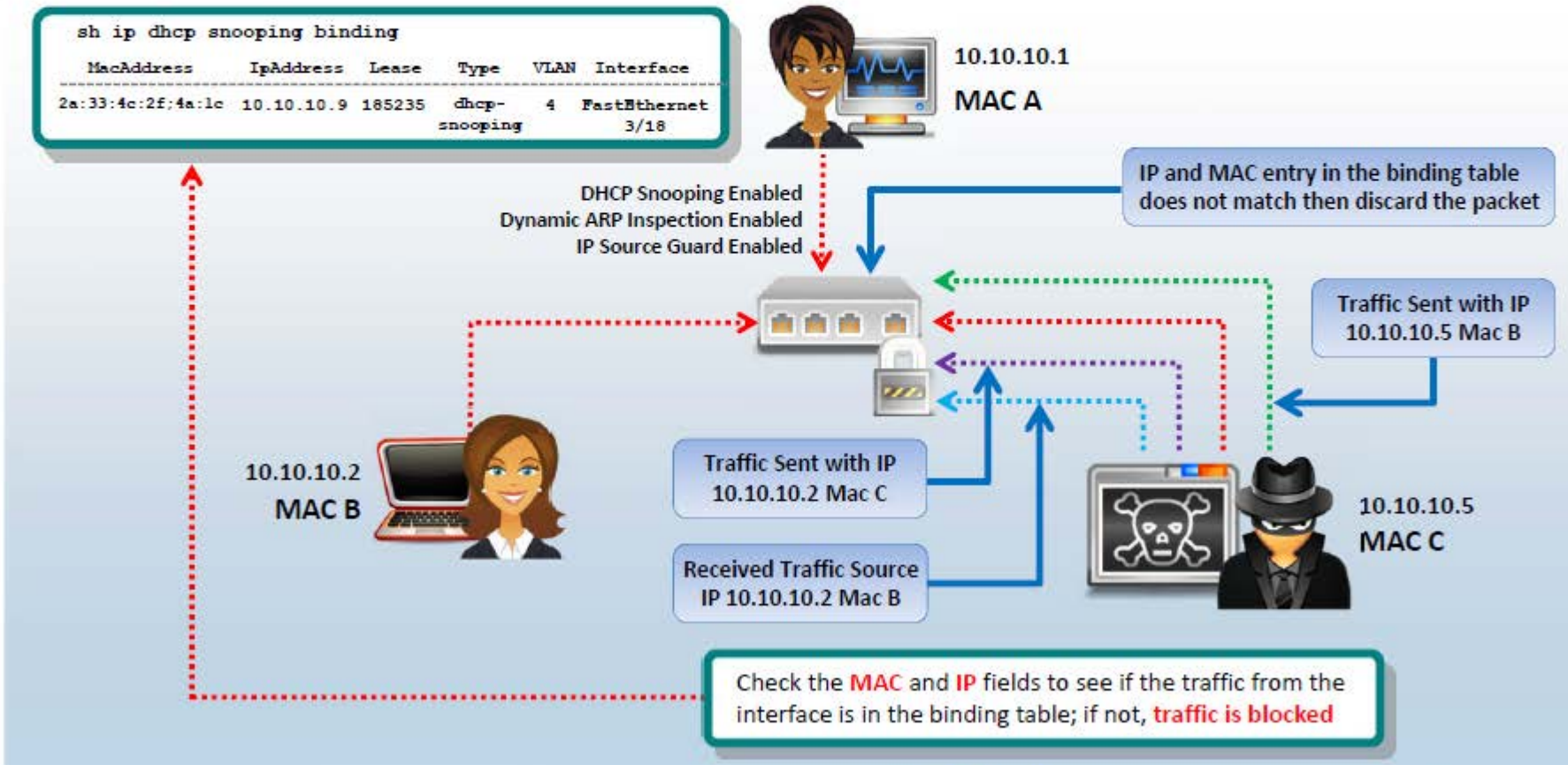
- Automatically activates new **MAC address** right after changing it
- Shows the **manufacturer** of the MAC address
- Randomly **generates any New MAC address** or based on a selected manufacturer



http://www.klcconsulting.net

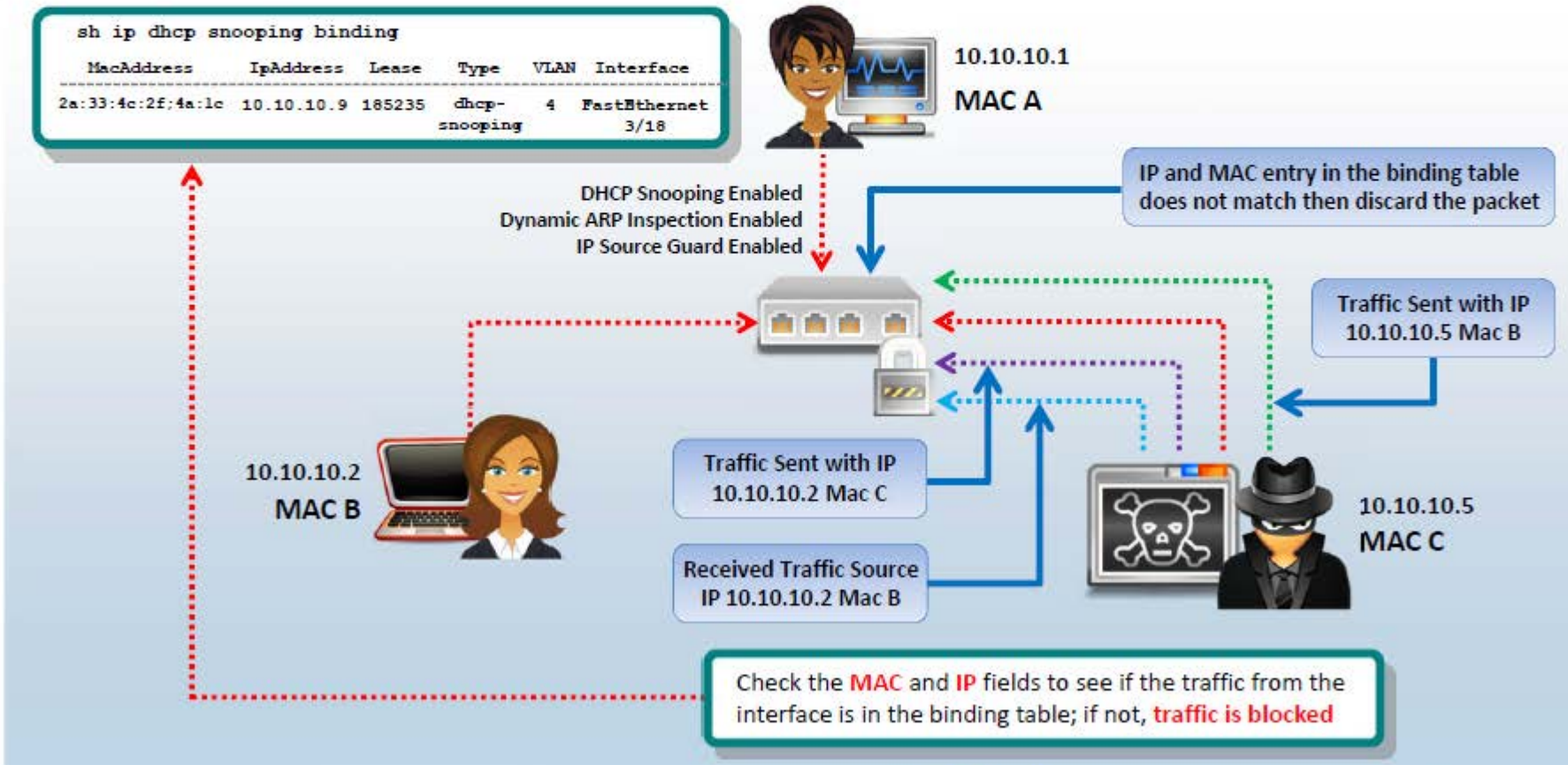
How to Defend Against MAC Spoofing

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

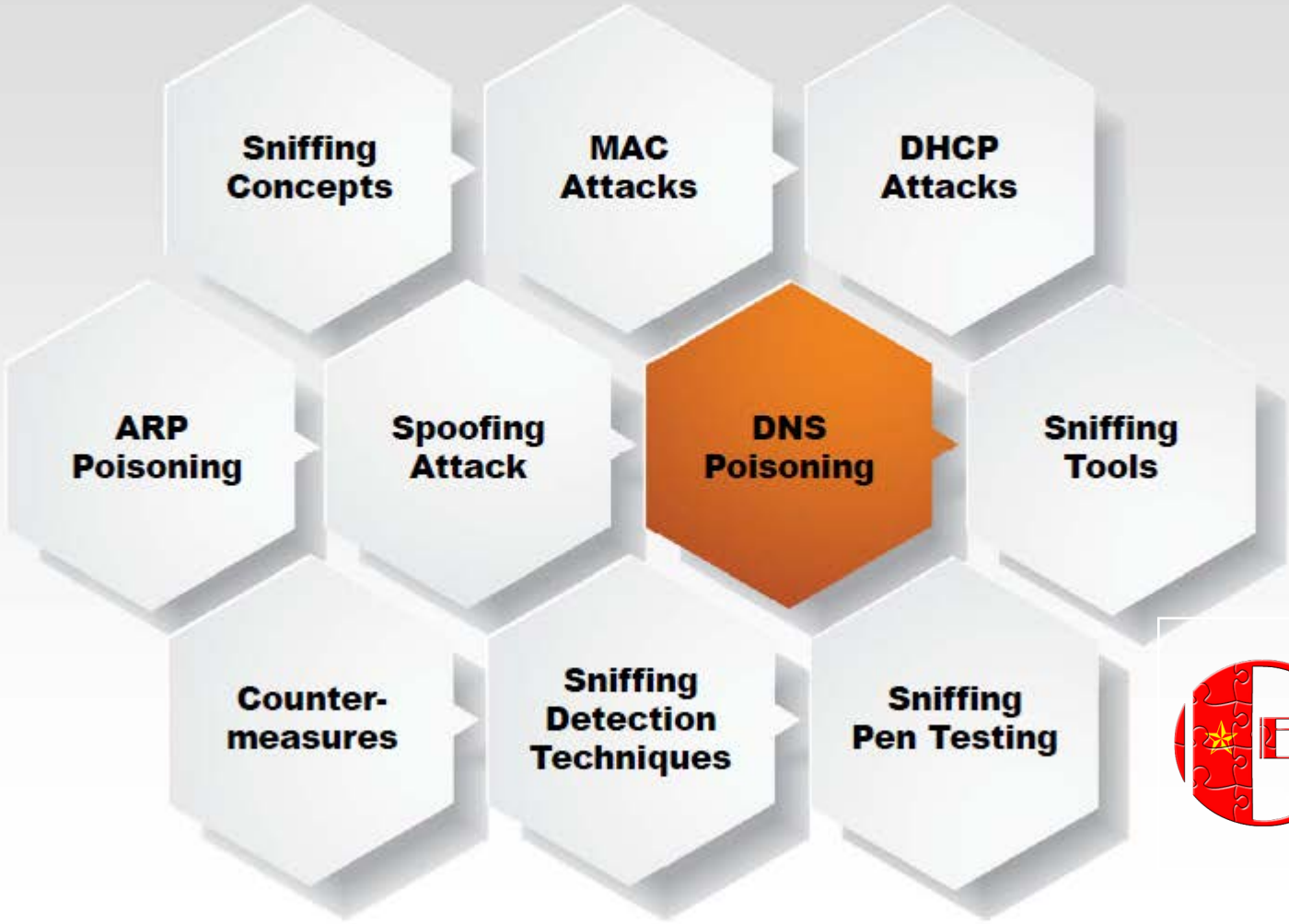


How to Defend Against MAC Spoofing

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



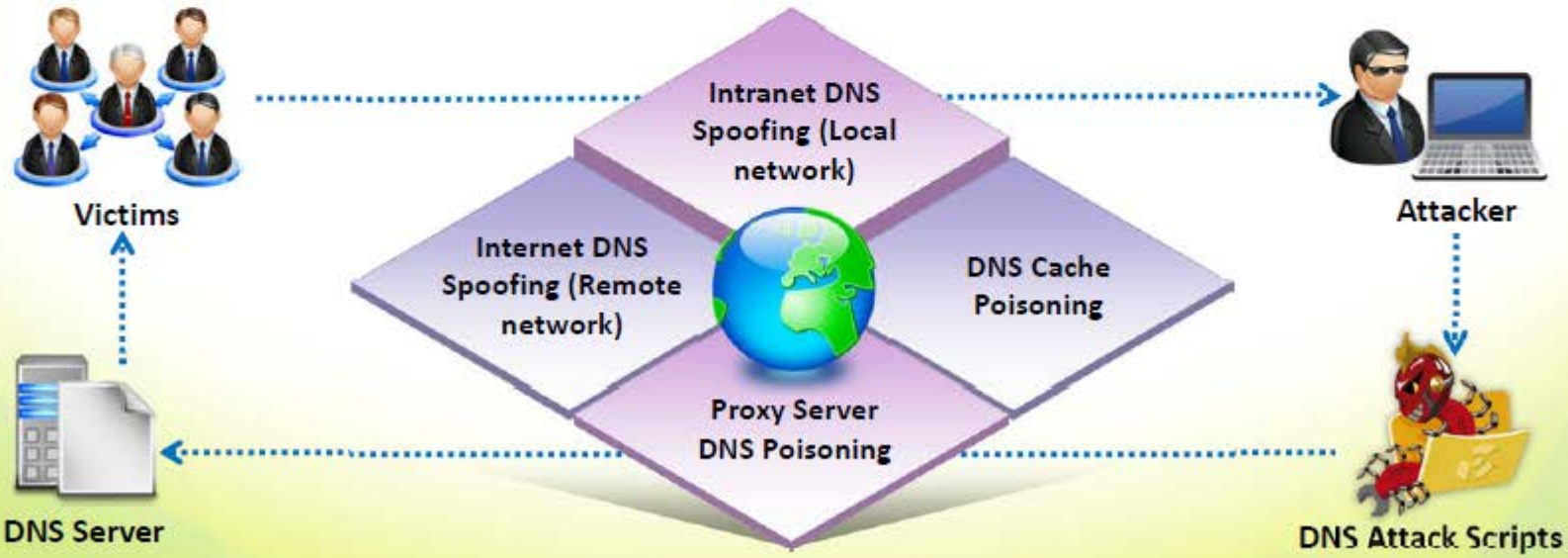
Module Flow



DNS Poisoning Techniques

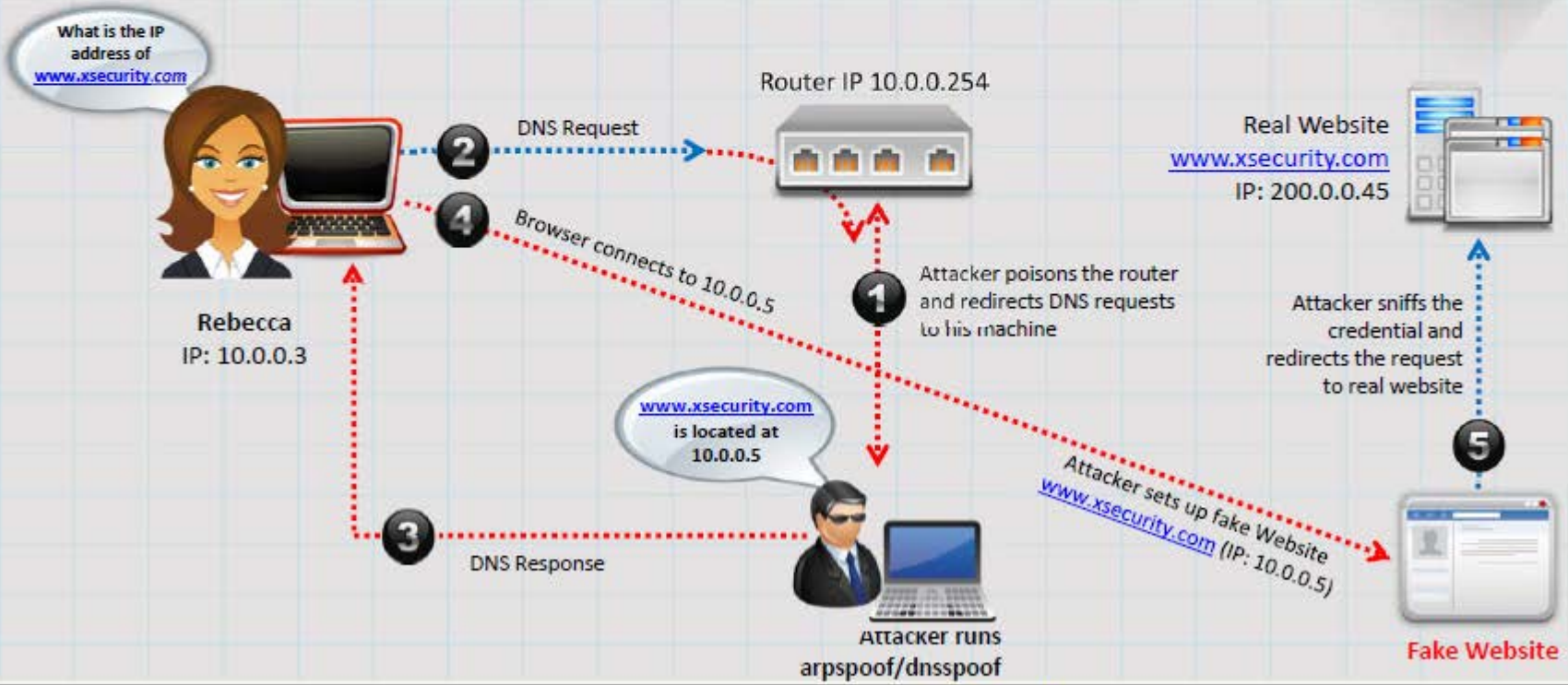
- DNS poisoning is a technique that **tricks a DNS server** into believing that it has received authentic information when, in reality, it has not
- It results in **substitution of a false IP address** at the DNS level where web addresses are converted into numeric IP addresses

- 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 same names as that of the target server

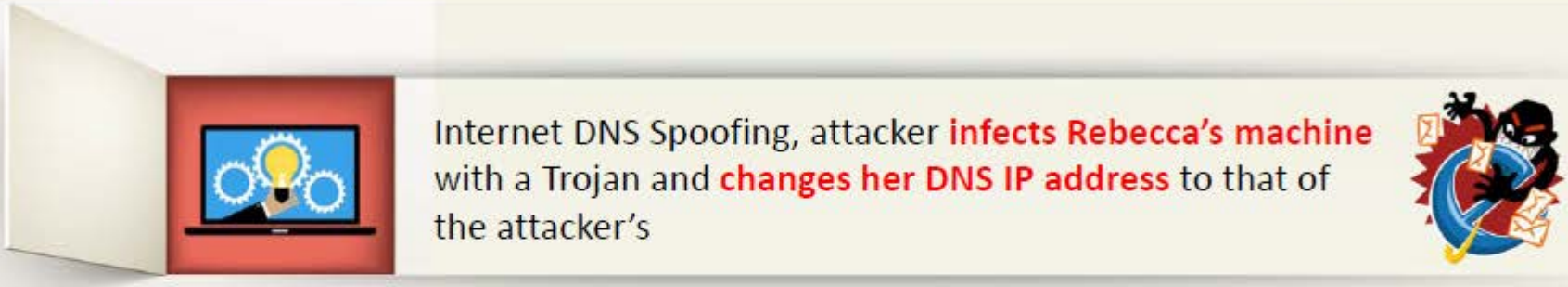


Intranet DNS Spoofing

- For this technique, you must be connected to the **local area network (LAN)** and be able to sniff packets
- It works well against **switches** with ARP poisoning the router

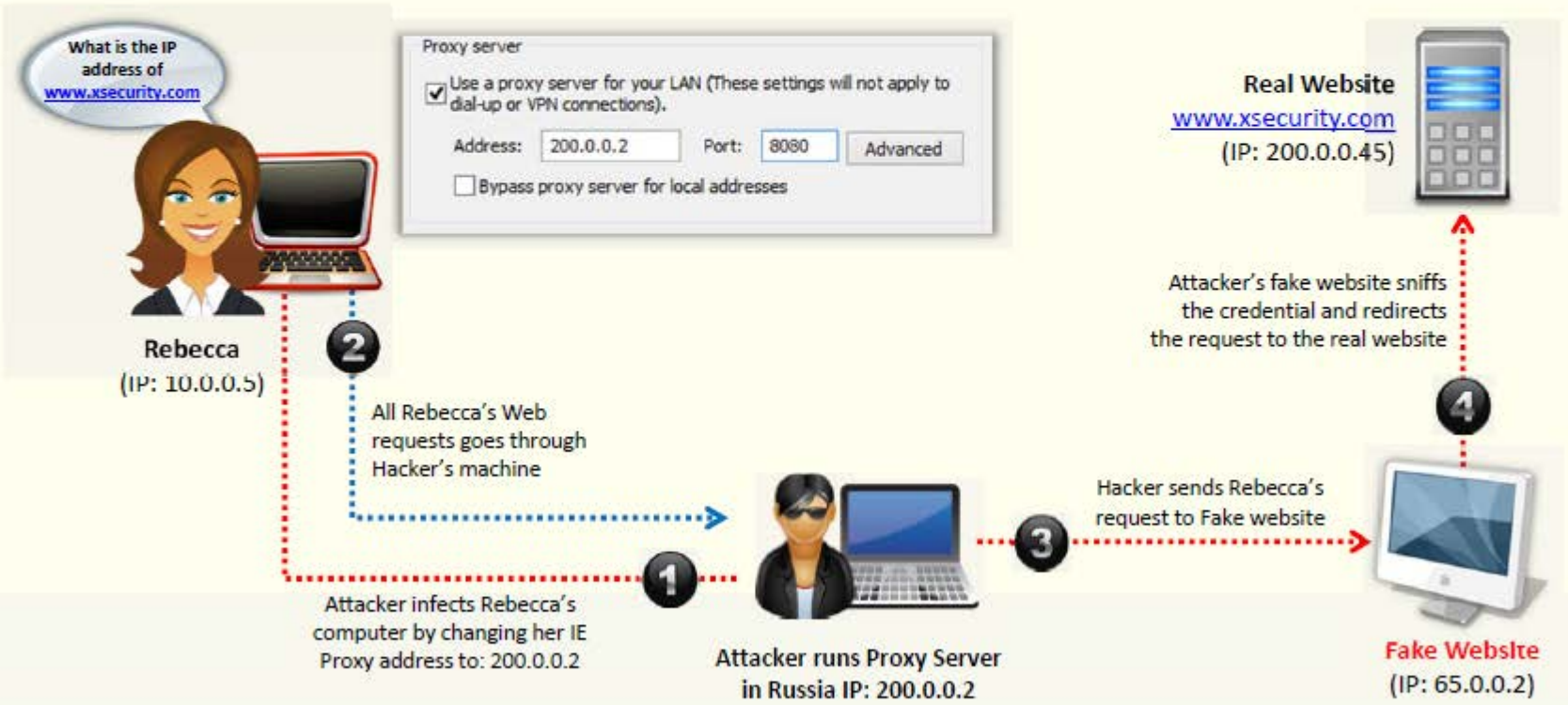


Internet DNS Spoofing



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

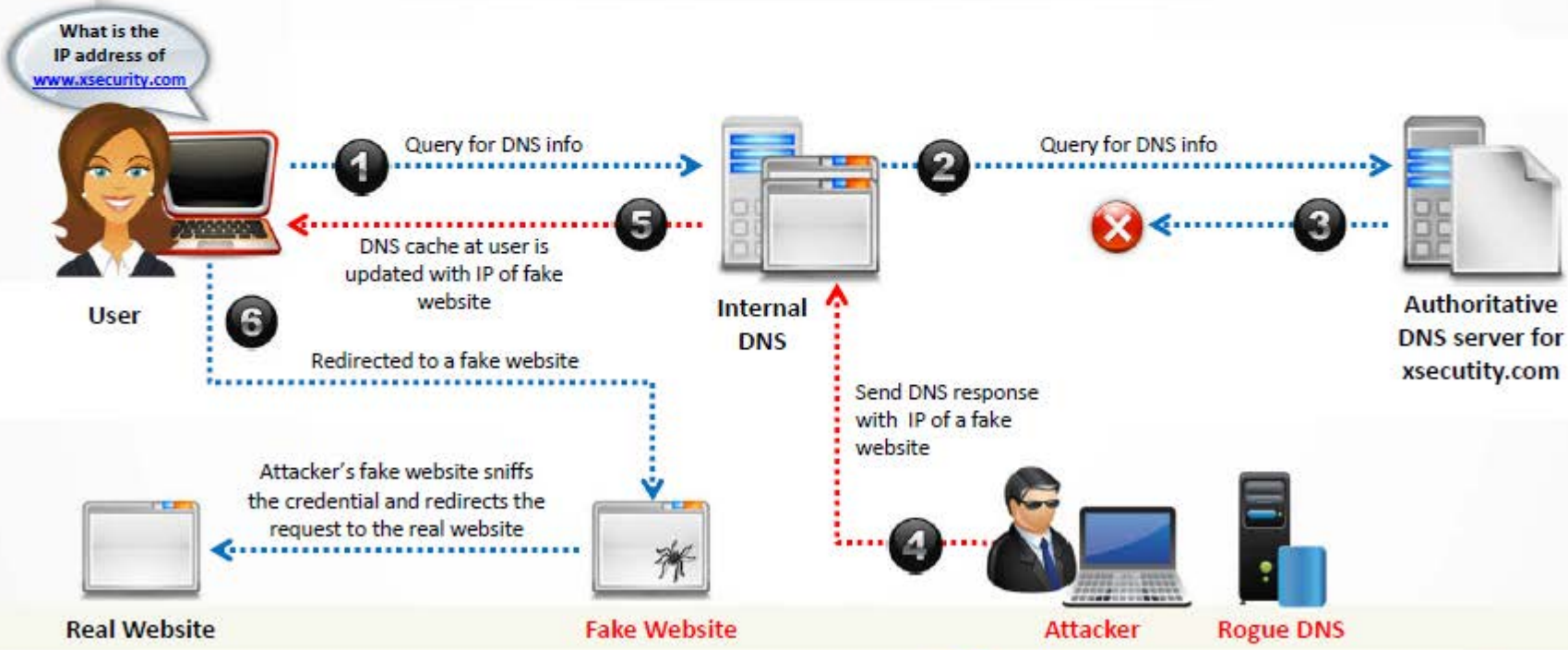


DNS Cache Poisoning

C|EH Certified Ethical Hacker

01 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

02 If the DNS resolver cannot validate that the DNS responses have come from an **authoritative source**, it will cache the **incorrect entries** locally and serve them to users who make the same request



How to Defend Against DNS Spoofing

CEH Certified Ethical Hacker

Resolve all DNS queries to local DNS server

Block DNS requests from going to external servers

Configure firewall to restrict external DNS lookup

Implement IDS and deploy it correctly

Implement DNSSEC

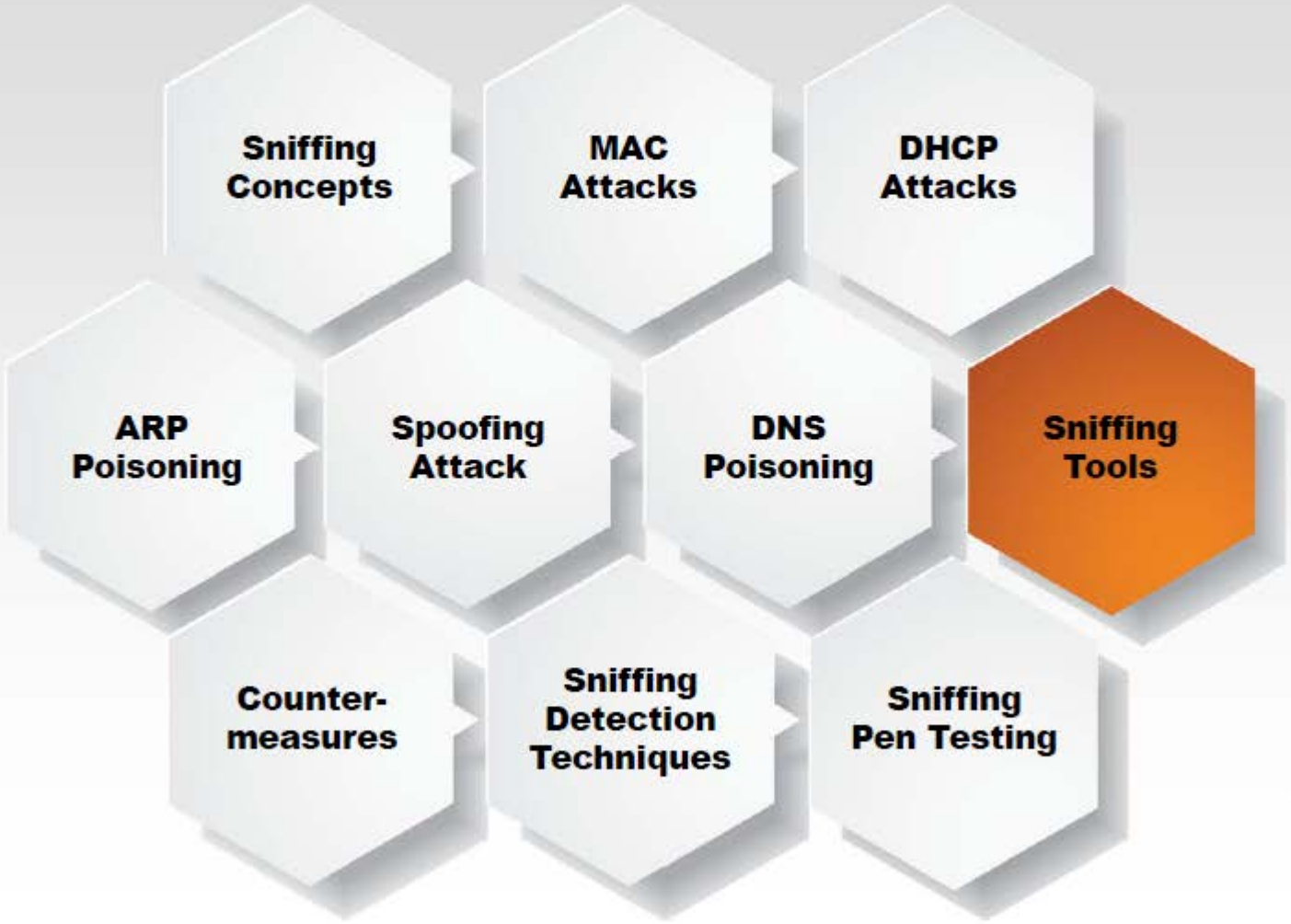
Configure DNS resolver to use a new random source port for each outgoing query

Restrict DNS recusing service, either full or partial, to authorized users

Use DNS Non-Existent Domain (NXDOMAIN) Rate Limiting

Secure your internal machines

Module Flow



Sniffing Tool: Wireshark

C|EH Certified Ethical Hacker

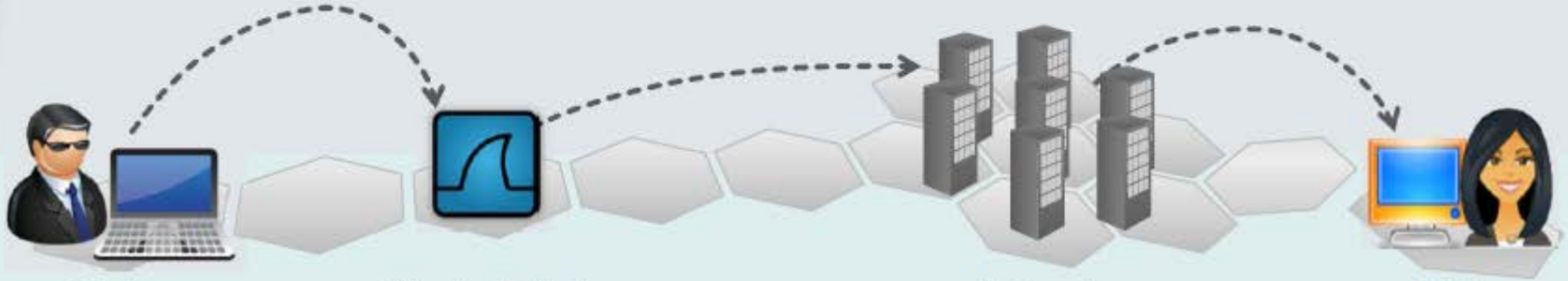
01 It lets you **capture and interactively browse the traffic** running on a computer network

02 Wireshark uses **Winpcap** to capture packets, so it can only capture the packets on the networks supported by Winpcap

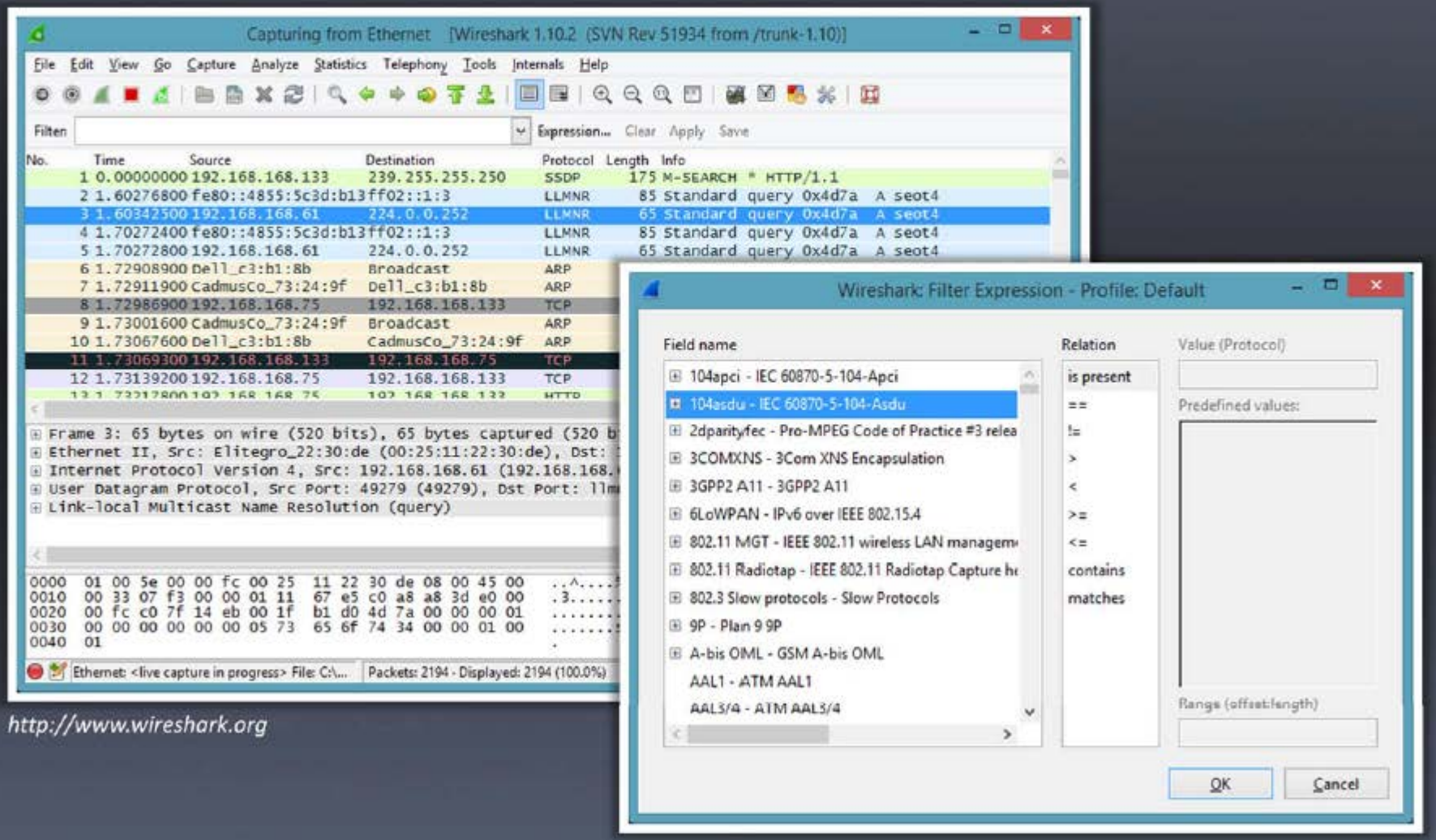
03 It **captures live network traffic** from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI networks

04 Captured files can be programmatically edited via **command-line**

05 A **set of filters** for customized data display can be refined using a display filter

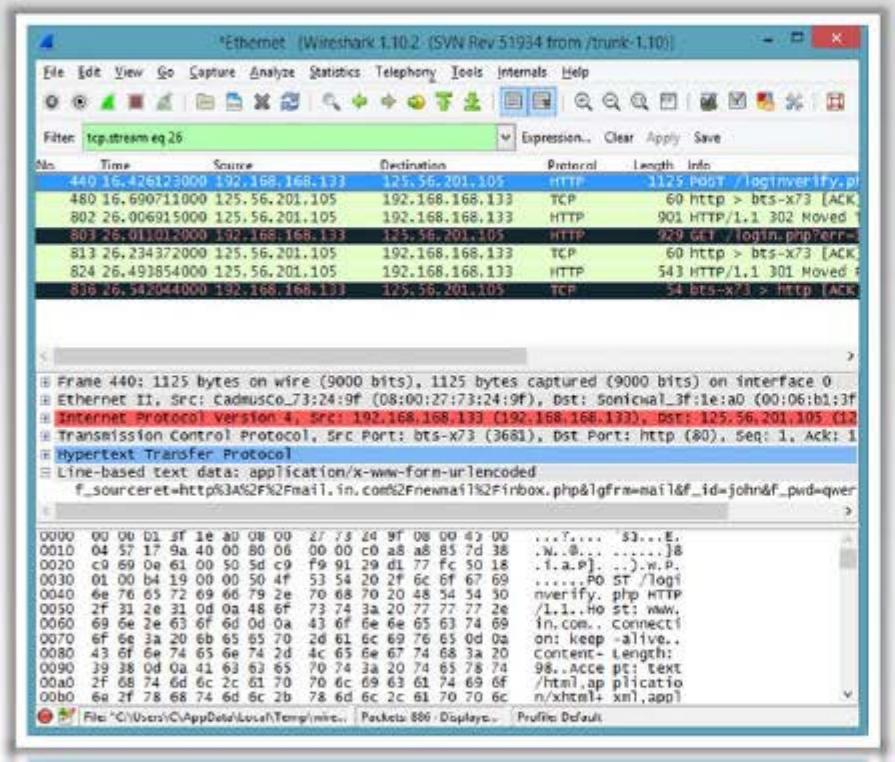


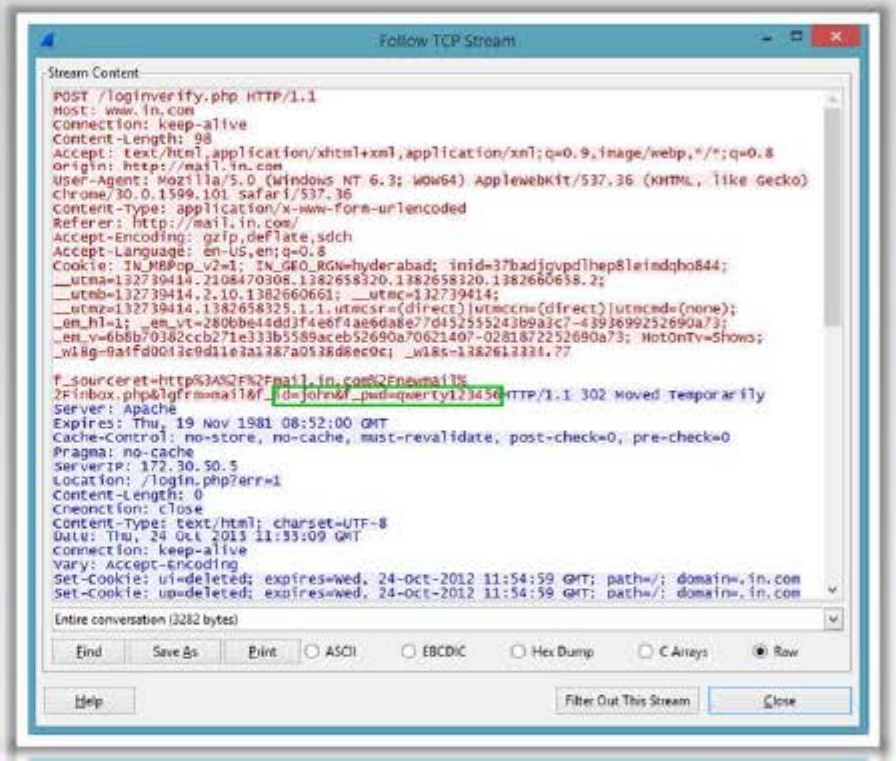
Sniffing Tool: Wireshark (Cont'd)



http://www.wireshark.org

Follow TCP Stream in Wireshark





Password revealed in TCP Stream

Display Filters in Wireshark

C|EH Certified Ethical Hacker

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

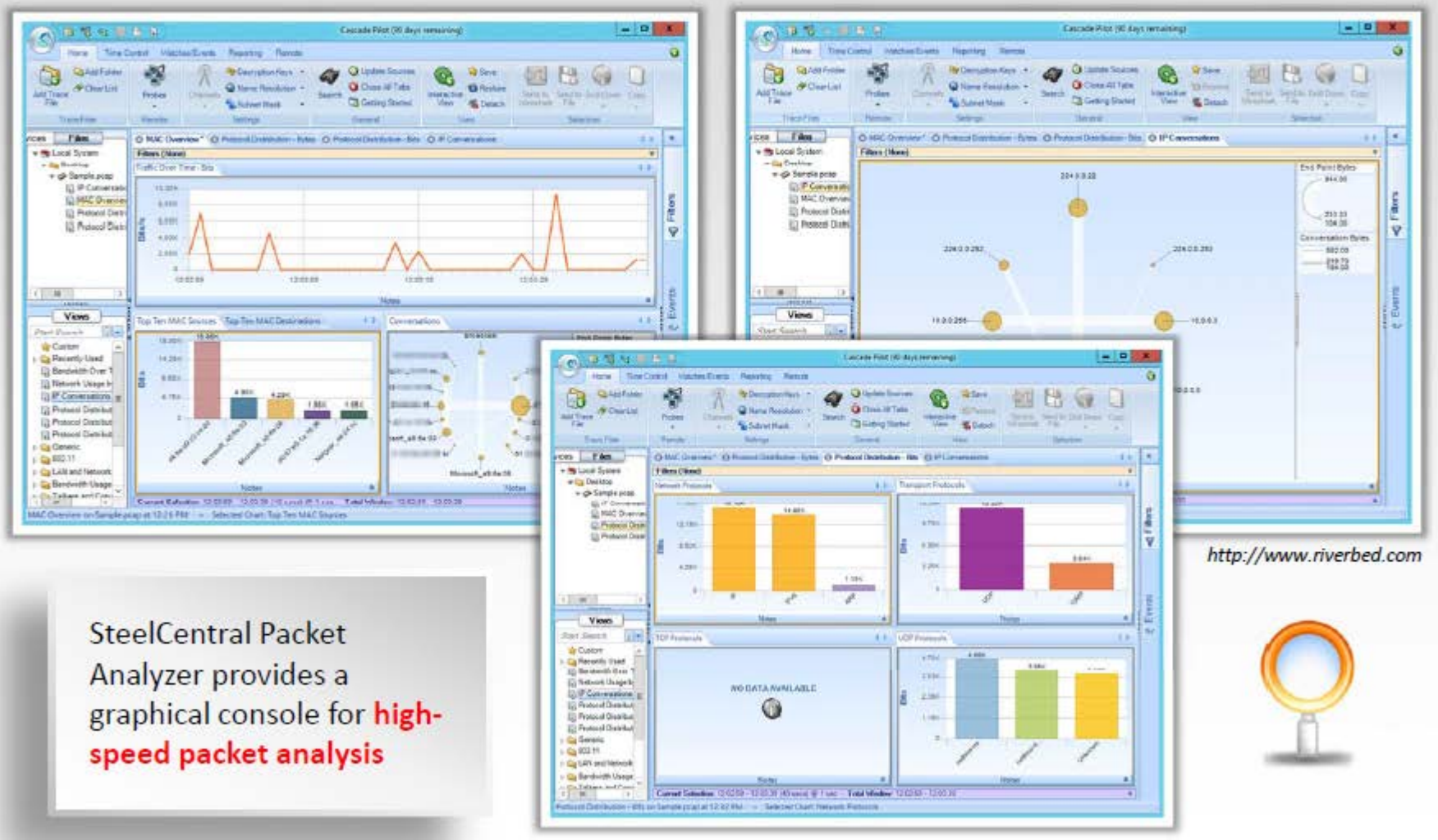
- `ip.dst == 10.0.1.50 && frame.pkt_len > 400`
- `ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30`
- `ip.src==205.153.63.30 or ip.dst==205.153.63.30`

Additional Wireshark Filters

C|EH Certified Ethical Hacker

01	`tcp.flags.reset==1` Displays all TCP resets	
02	`udp contains 33:27:58` Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset	
03	`http.request` Displays all HTTP GET requests	
04	`tcp.analysis. retransmission` Displays all retransmissions in the trace	
05	`tcp contains traffic` Displays all TCP packets that contain the word 'traffic'	
06	`!(arp or icmp or dns)` Masks out arp, icmp, dns, or other protocols and allows you to view traffic of you interest	

Sniffing Tool: SteelCentral Packet Analyzer

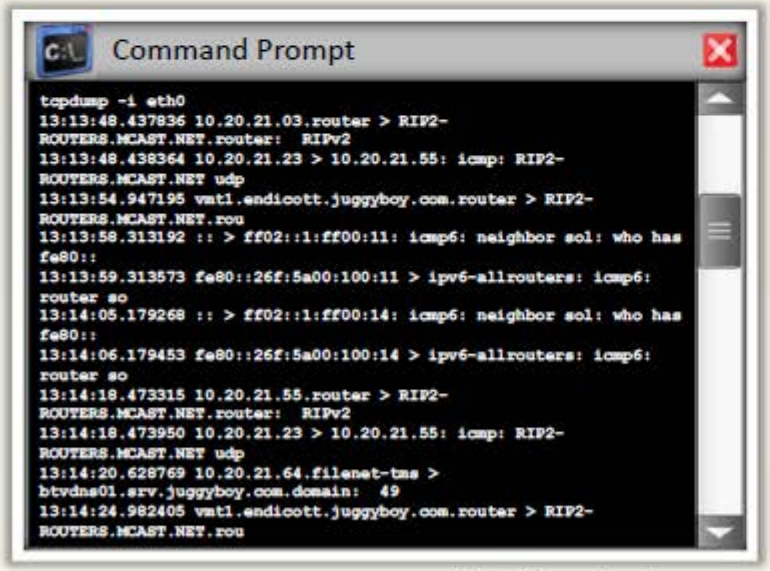


Sniffing Tool: Tcpdump/Windump

TCPdump is a **command line interface packet sniffer** which runs on Linux and Windows

TCPDump

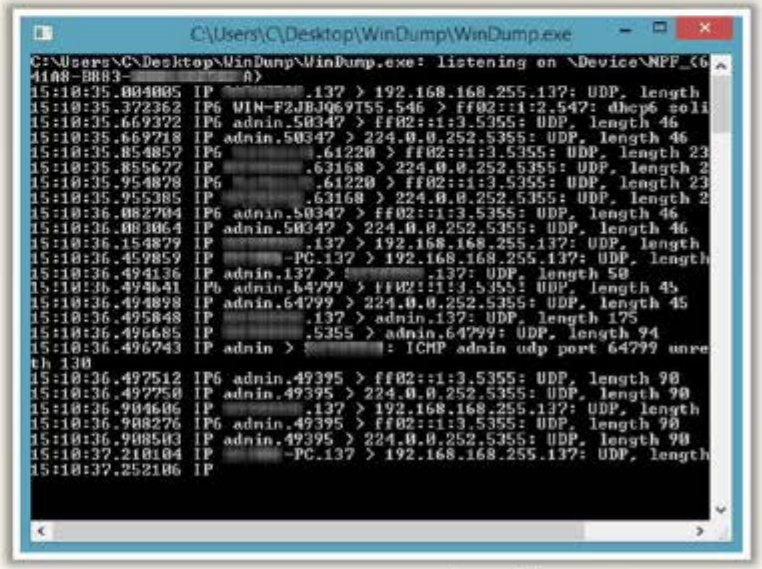
Runs on Linux and UNIX systems



http://www.tcpdump.org

WinDump

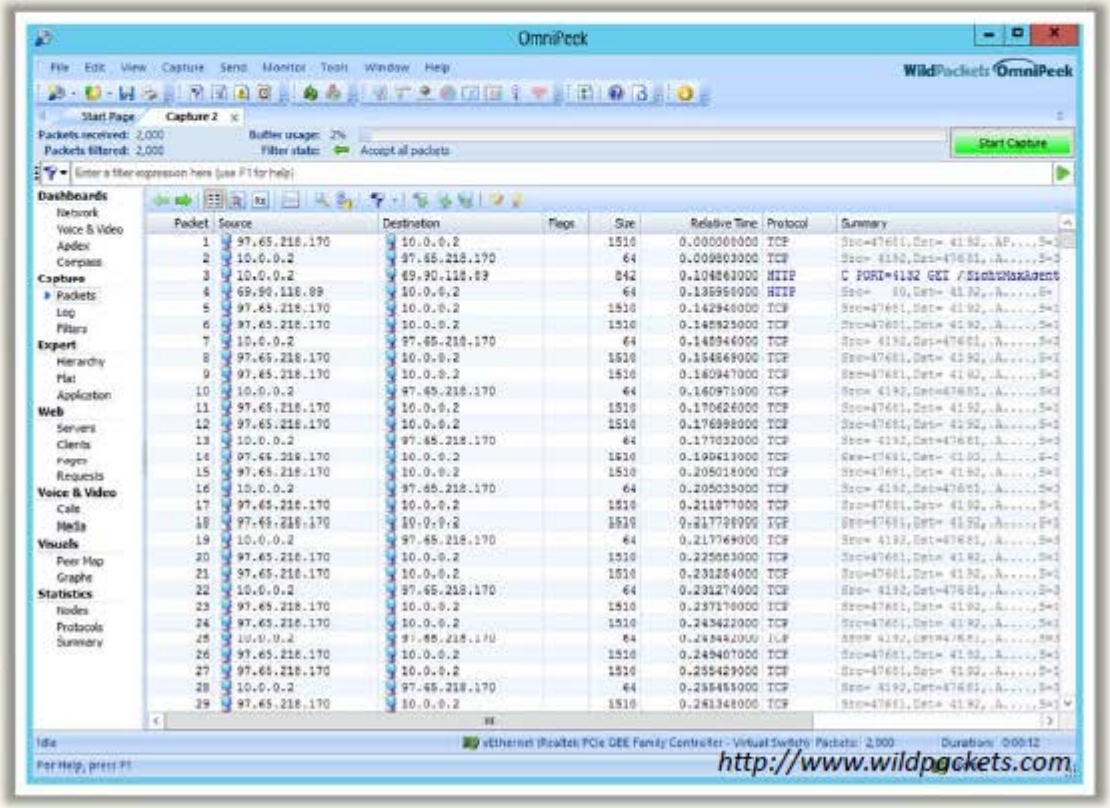
Runs on Windows systems



http://www.winpcap.org

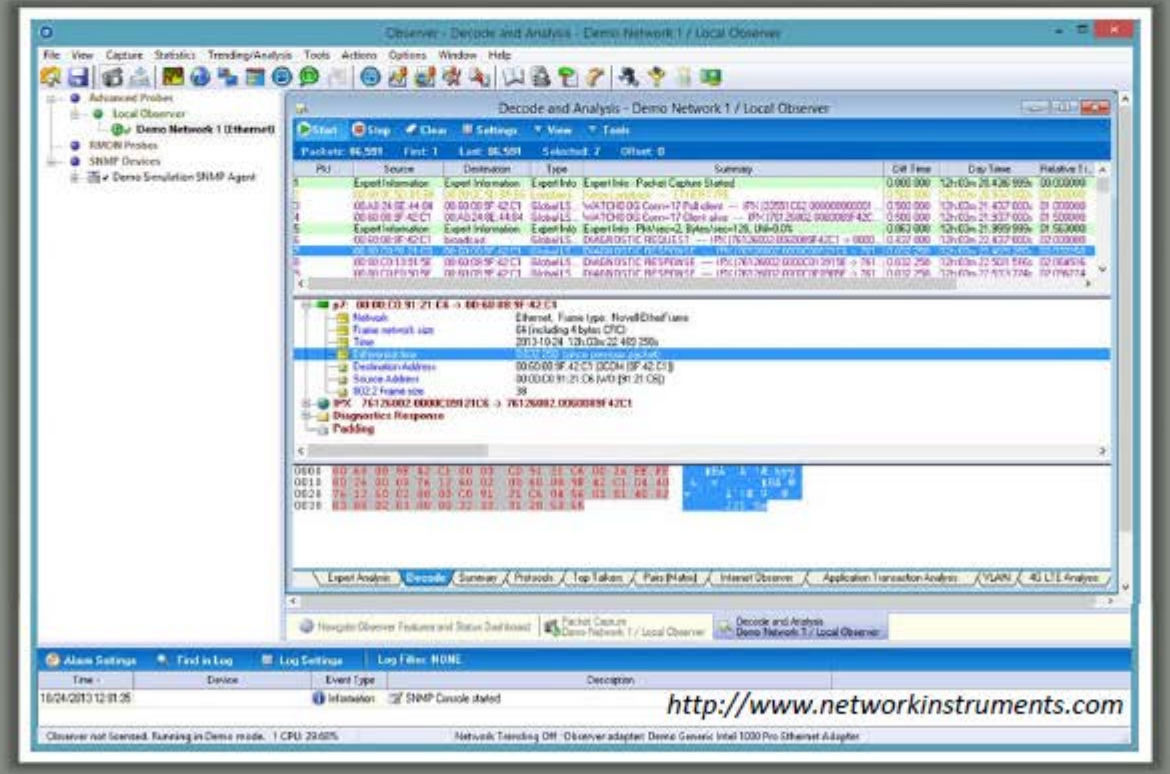
Network Packet Analyzer: OmniPeek Network Analyzer

- OmniPeek sniffer displays a Google Map in the OmniPeek capture window showing the **locations of all the public IP addresses of captured packets**
- This feature is a great way to monitor the network in real time, and show from where in the world that **traffic is coming**



Network Packet Analyzer: Observer

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

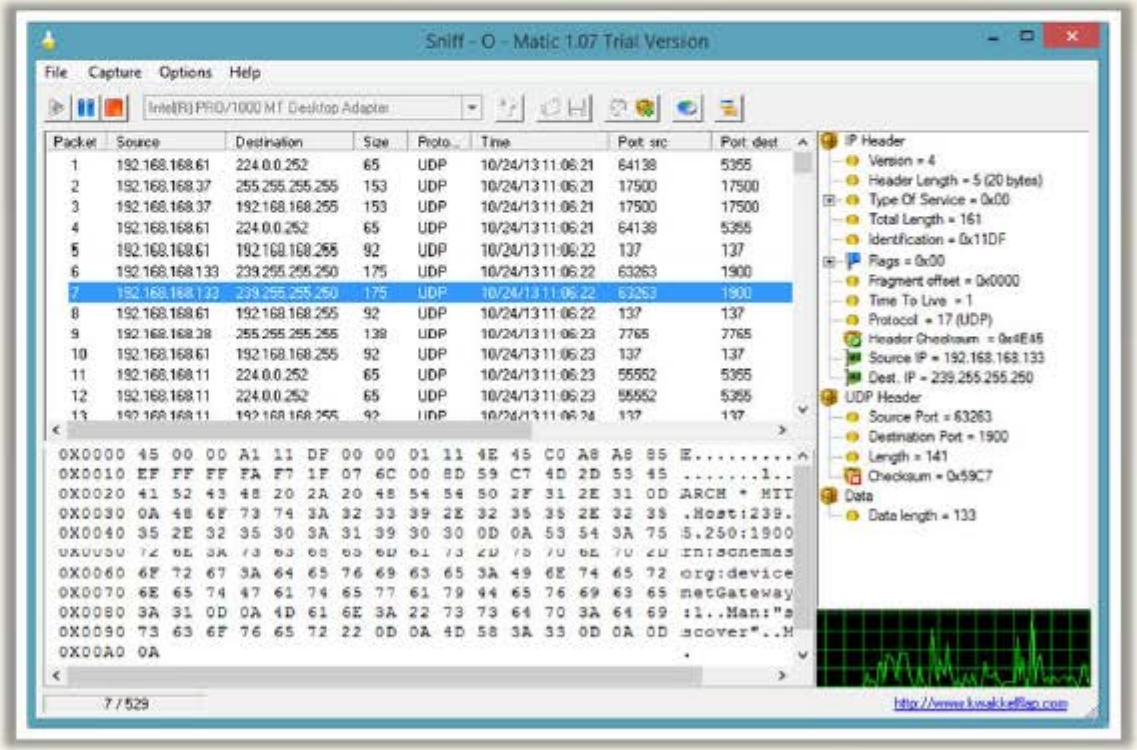


Network Packet Analyzer: Sniff-O-Matic

Sniff-O-Matic is a network protocol analyzer and packet sniffer that **captures network traffic** and enables you to **analyze the data**

Features

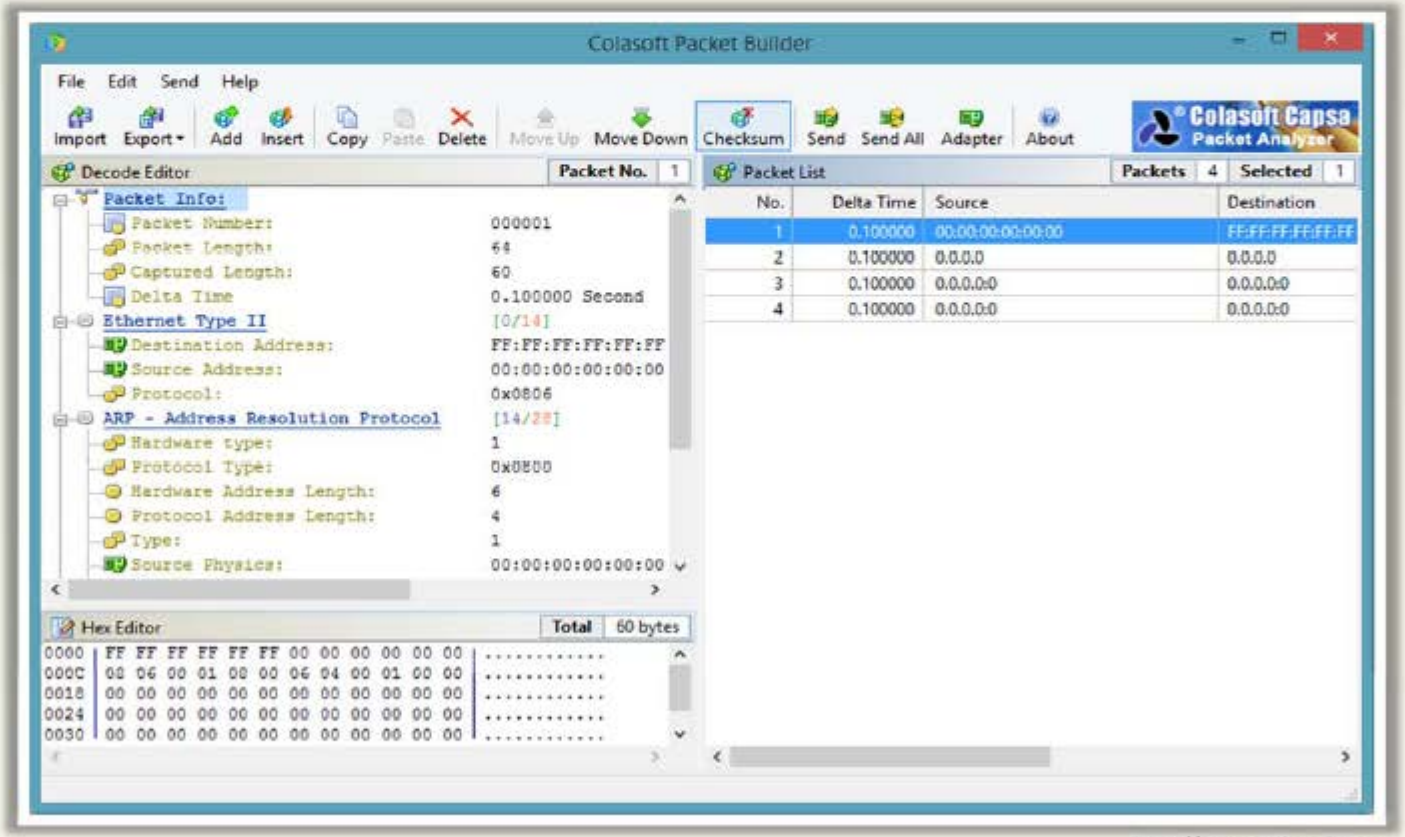
- Capture IP packets on your LAN without packet loss
- Monitor network activity in real time
- Filters to show only the packets you want
- Realtime checksum calculation
- Save and load captured packets
- Traffic charts with filter info



http://www.kwakkelflap.com

TCP/IP Packet Crafter: Colasoft Packet Builder

Colasoft Packet Builder allows user to select one from the provided templates: **Ethernet Packet**, **ARP Packet**, **IP Packet**, **TCP Packet** and **UDP Packet**, and **change the parameters** in the decoder editor, hexadecimal editor, or ASCII editor to create a packet

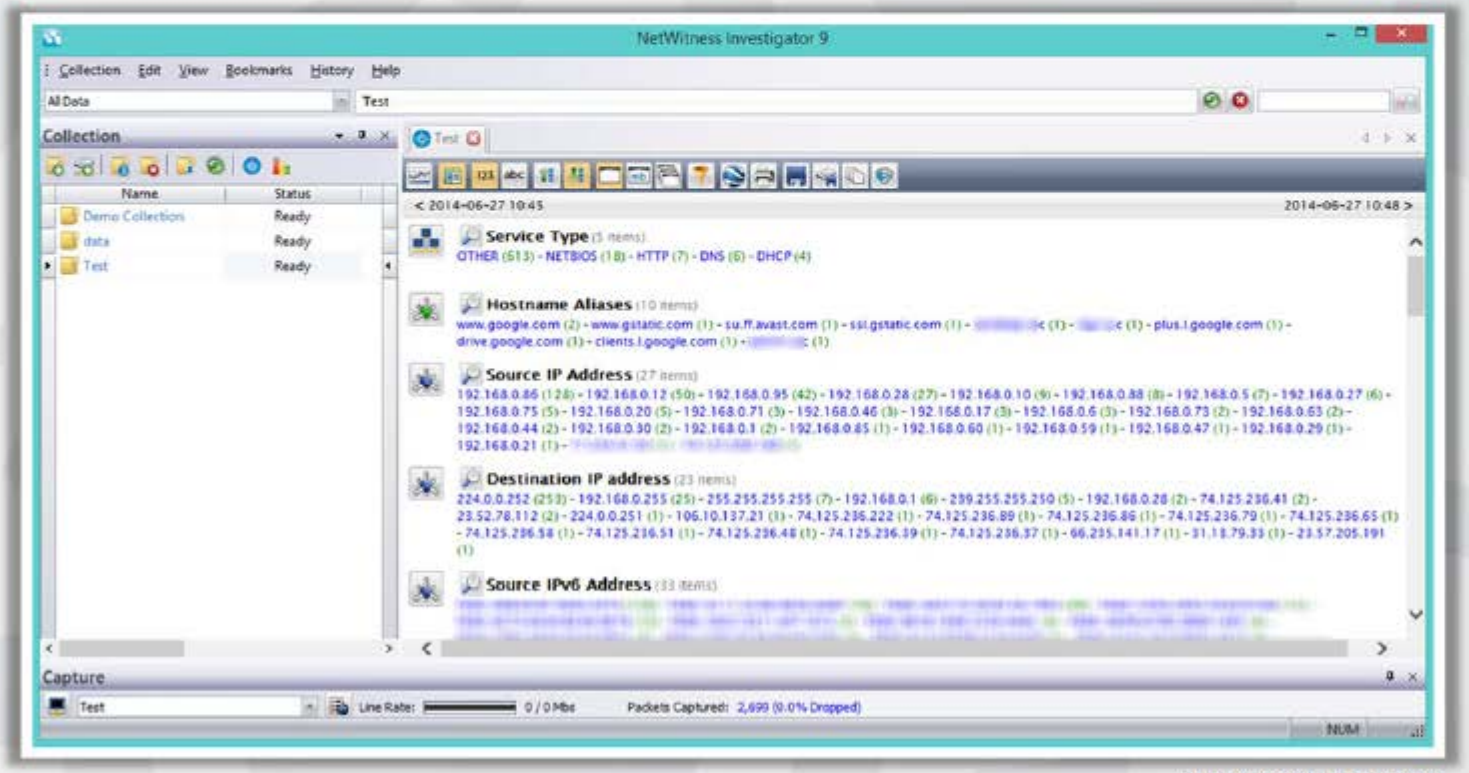


http://www.colasoft.com

Network Packet Analyzer: RSA NetWitness Investigator

C|EH Certified Ethical Hacker

RSA NetWitness Investigator captures live traffic and process packet files from virtually any existing network collection devices



http://www.emc.com

Additional Sniffing Tools

C|EH Certified Ethical Hacker

Ace Password Sniffer
http://www.effetech.com

EffeTech HTTP Sniffer
http://www.effetech.com

IPgrab
http://ipgrab.sourceforge.net

ntopng
http://www.ntop.org

Big-Mother
http://www.tupsoft.com

Ettercap
http://ettercap.sourceforge.net

EtherDetect Packet Sniffer
http://www.etherdetect.com

SmartSniff
http://www.nirsoft.net

dsniff
http://monkey.org

EtherApe
http://etherape.sourceforge.net

Additional Sniffing Tools (Cont'd)

C|EH Certified Ethical Hacker

Network Probe
http://www.objectplanet.com

CommView
http://www.tamos.com

WebSiteSniffer
http://www.nirsoft.net

NetResident
http://www.tamos.com

ICQ Sniffer
http://www.etherboss.com

Kismet
http://www.kismetwireless.net

MaaTec Network Analyzer
http://www.maatec.com

AIM Sniffer
http://www.effetech.com

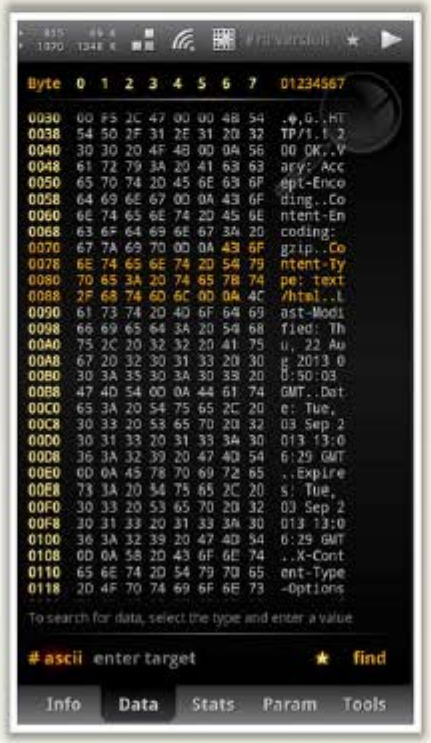
Alchemy Network Monitor
http://www.mishelpers.com

Netstumbler
http://www.netstumbler.com

Packet Sniffing Tools for Mobile: Wi.cap. Network Sniffer Pro and FaceNiff

Wi.cap. Network Sniffer Pro

Mobile network packet sniffer for **ROOT ARM droids**



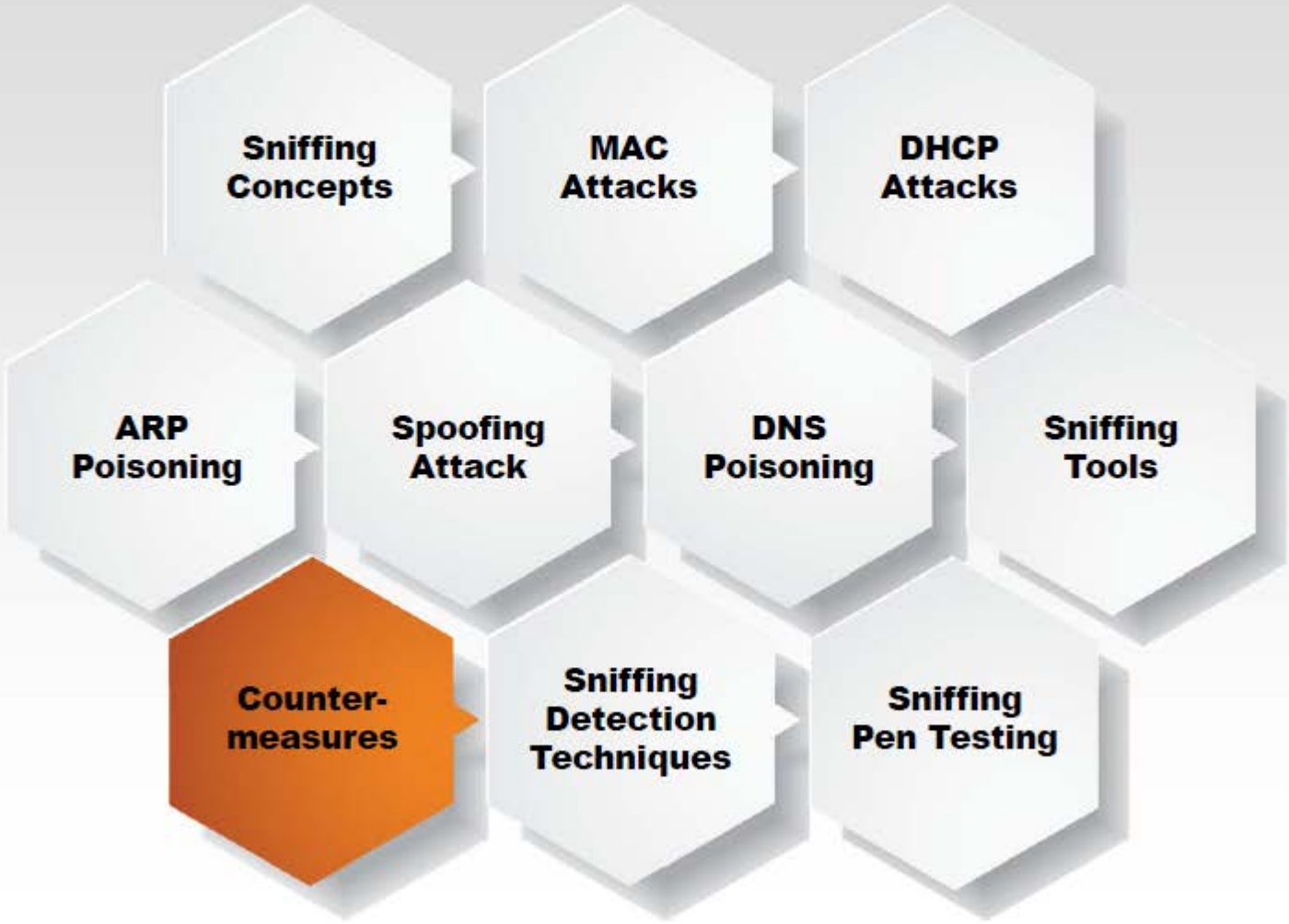
https://play.google.com

FaceNiff

FaceNiff is an Android app that allows you to **sniff and intercept web session profiles** over the Wi-Fi

http://faceniff.ponury.net

Module Flow



How to Defend Against Sniffing (Cont'd)

- Use **HTTPS** instead of HTTP to protect user names and passwords
- Use **switch instead of hub** as switch delivers data only to the intended recipient
- Use **SFTP**, instead of FTP for secure transfer of files
- Use **PGP** and **S/MIPE**, **VPN**, **IPSec**, **SSL/TLS**, **Secure Shell (SSH)** and One-time passwords (OTP)
- Always encrypt the wireless traffic with a **strong encryption protocol** such as WPA and WPA2
- **Retrieve MAC** directly from NIC instead of OS; this prevents MAC address spoofing
- Use **tools** to determine if any NICs are running in the promiscuous mode

Module Flow

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

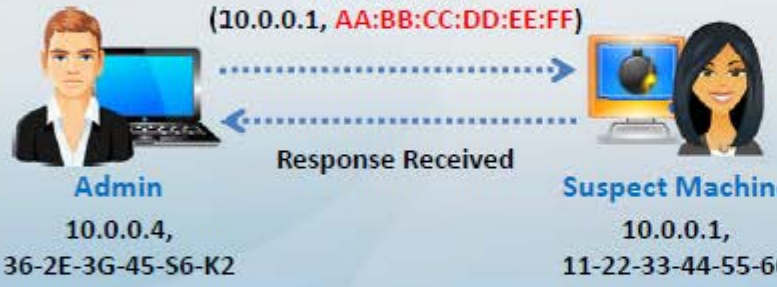
- **Run IDS** and notice if the **MAC address** of certain machines has changed (Example: router's MAC address)
- IDS can alert the administrator about **suspicious activities**

Network Tools

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

Sniffer Detection Technique: Ping Method

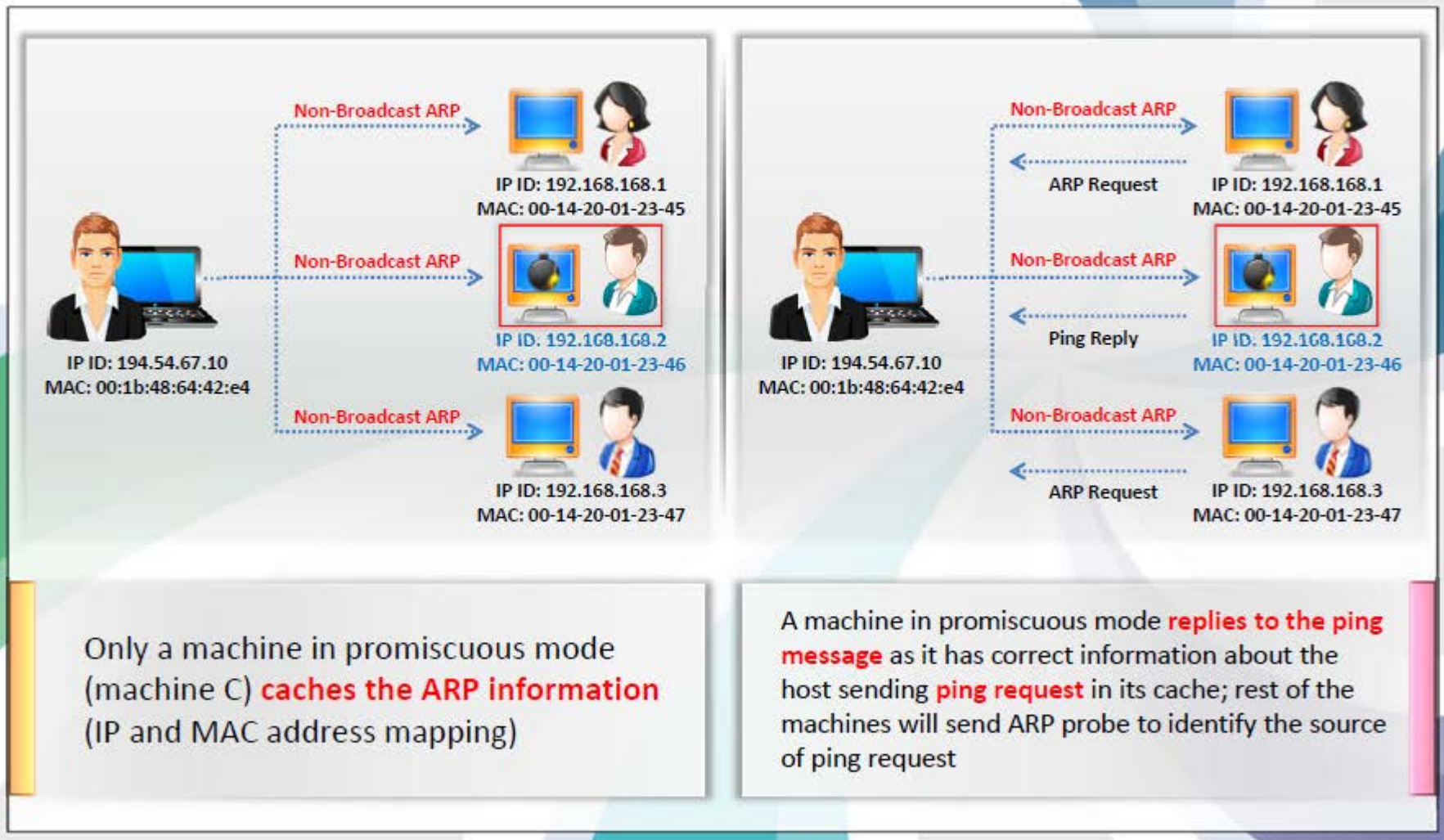
Promiscuous Mode



Non-Promiscuous Mode

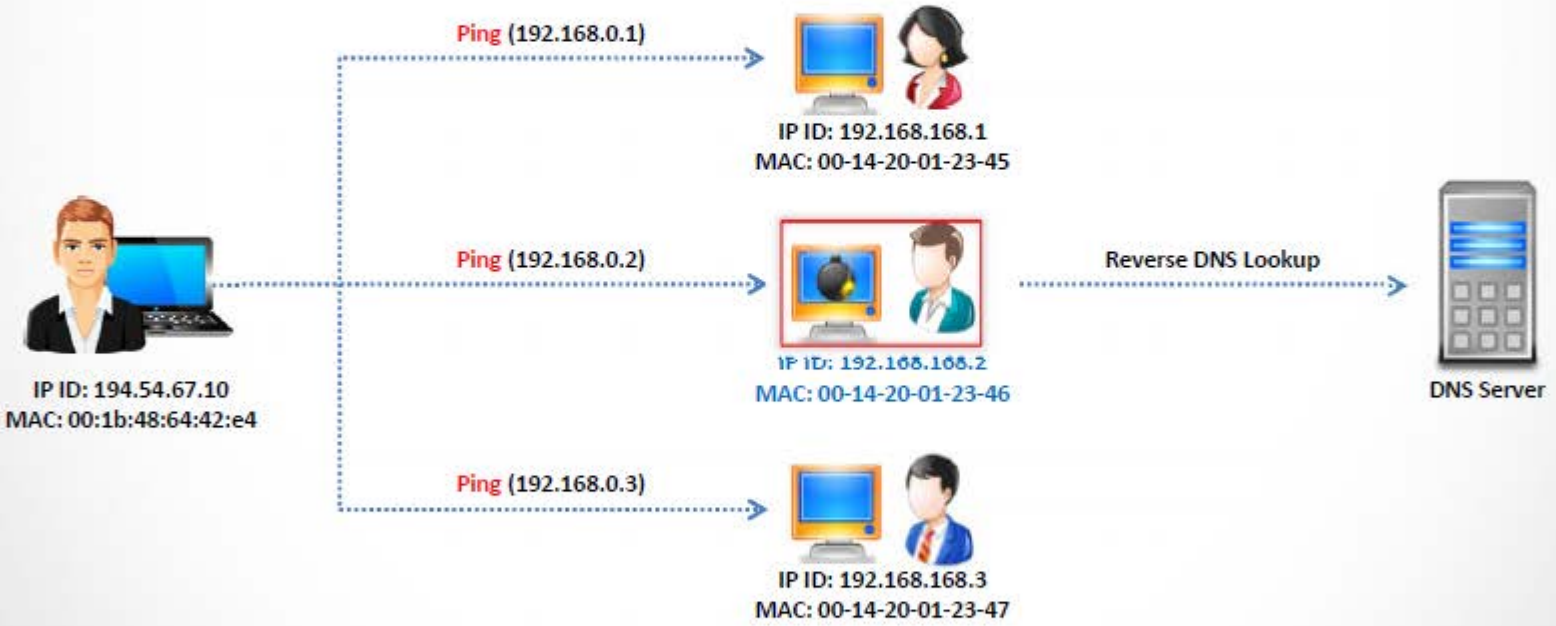
Send a ping request to the suspect machine with its IP address and **incorrect MAC address**. The Ethernet adapter rejects it, as the MAC address does not match, whereas the suspect machine running the **sniffer responds** to it as it does not reject packets with a different MAC address

Sniffer Detection Technique: ARP Method



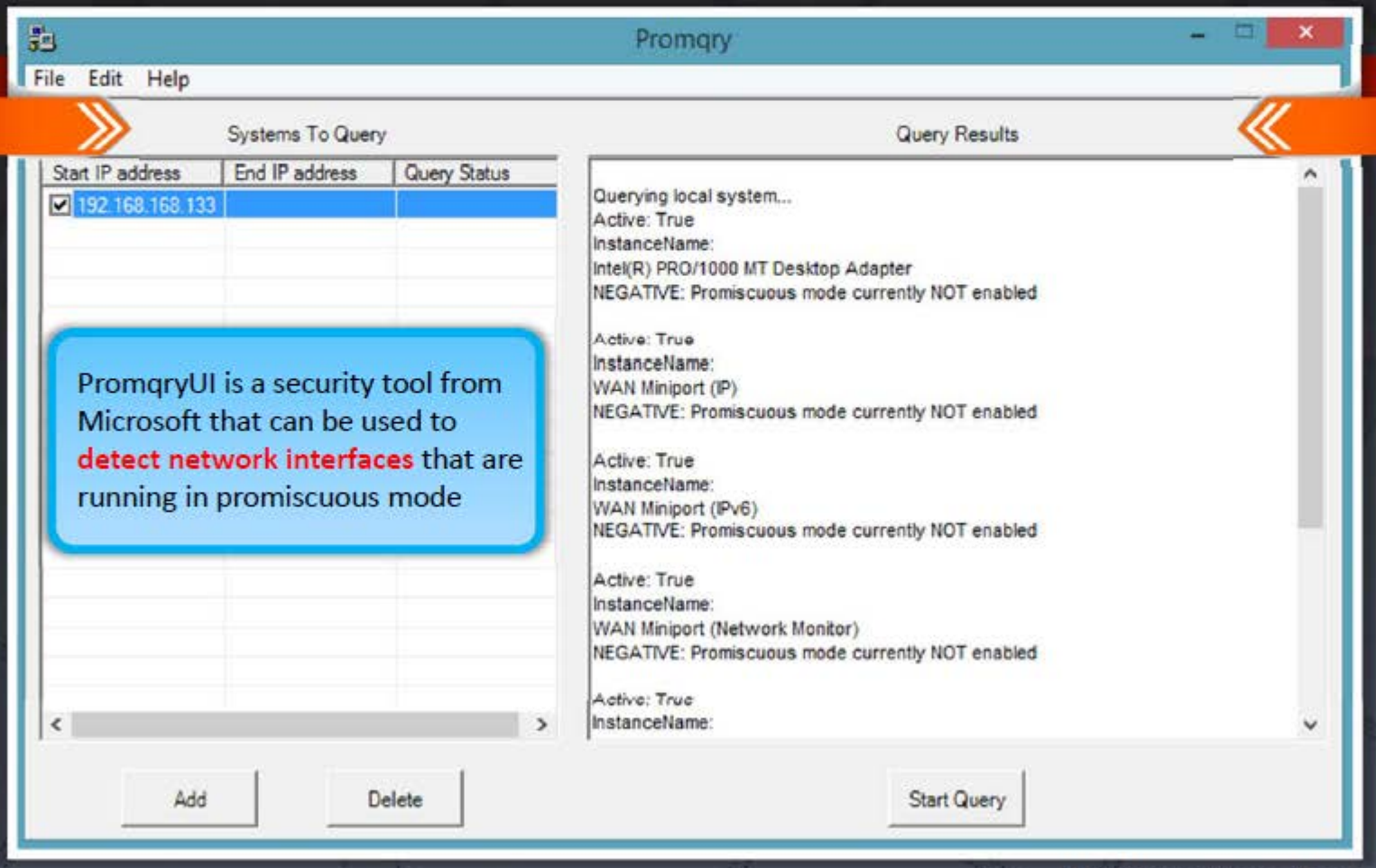
Sniffer Detection Technique: DNS Method

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

Promiscuous Detection Tool: PromqryUI

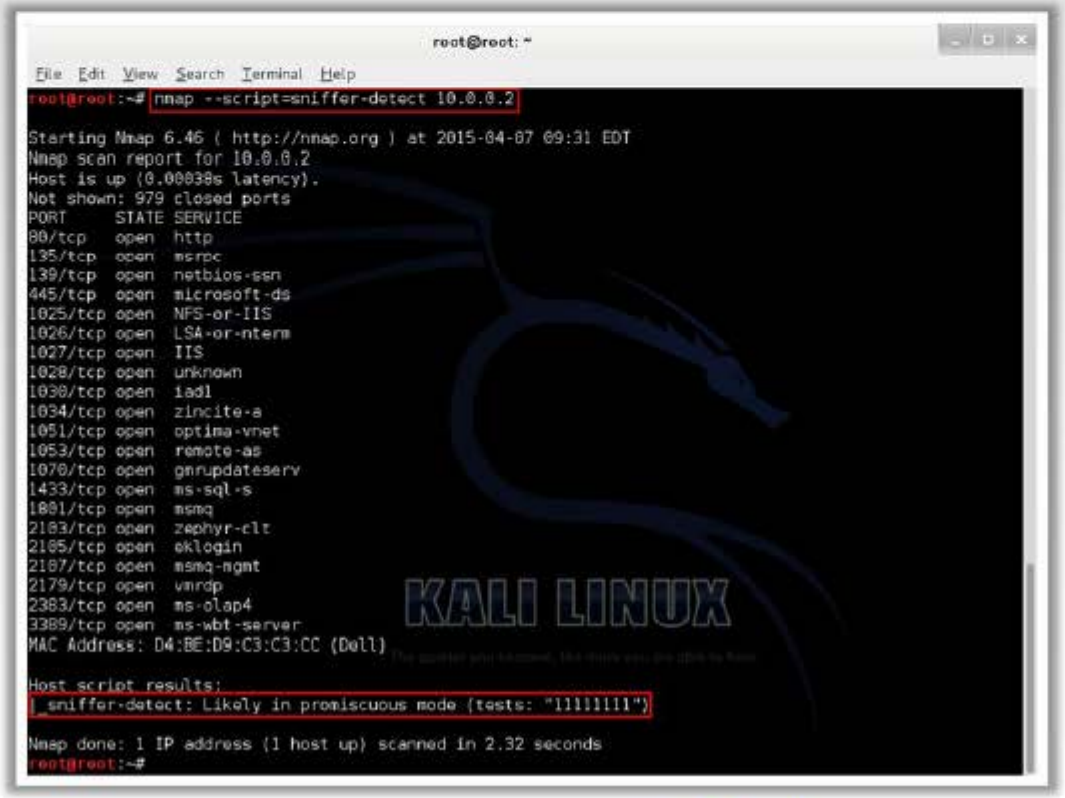


PromqryUI is a security tool from Microsoft that can be used to **detect network interfaces** that are running in promiscuous mode

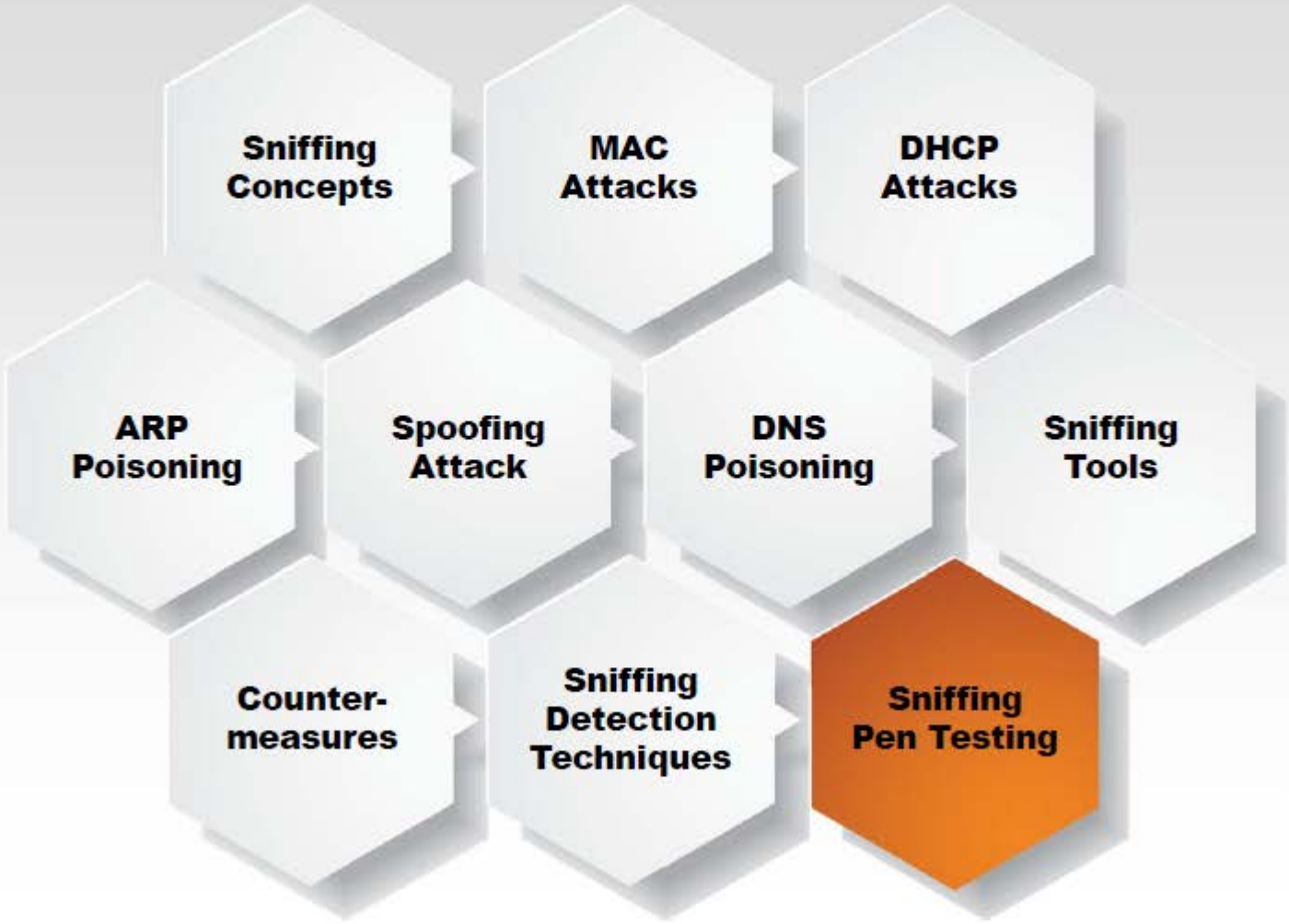
Promiscuous Detection Tool: Nmap

- 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]
```



Module Flow



Sniffing Pen 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:

Audit the network traffic for malicious content

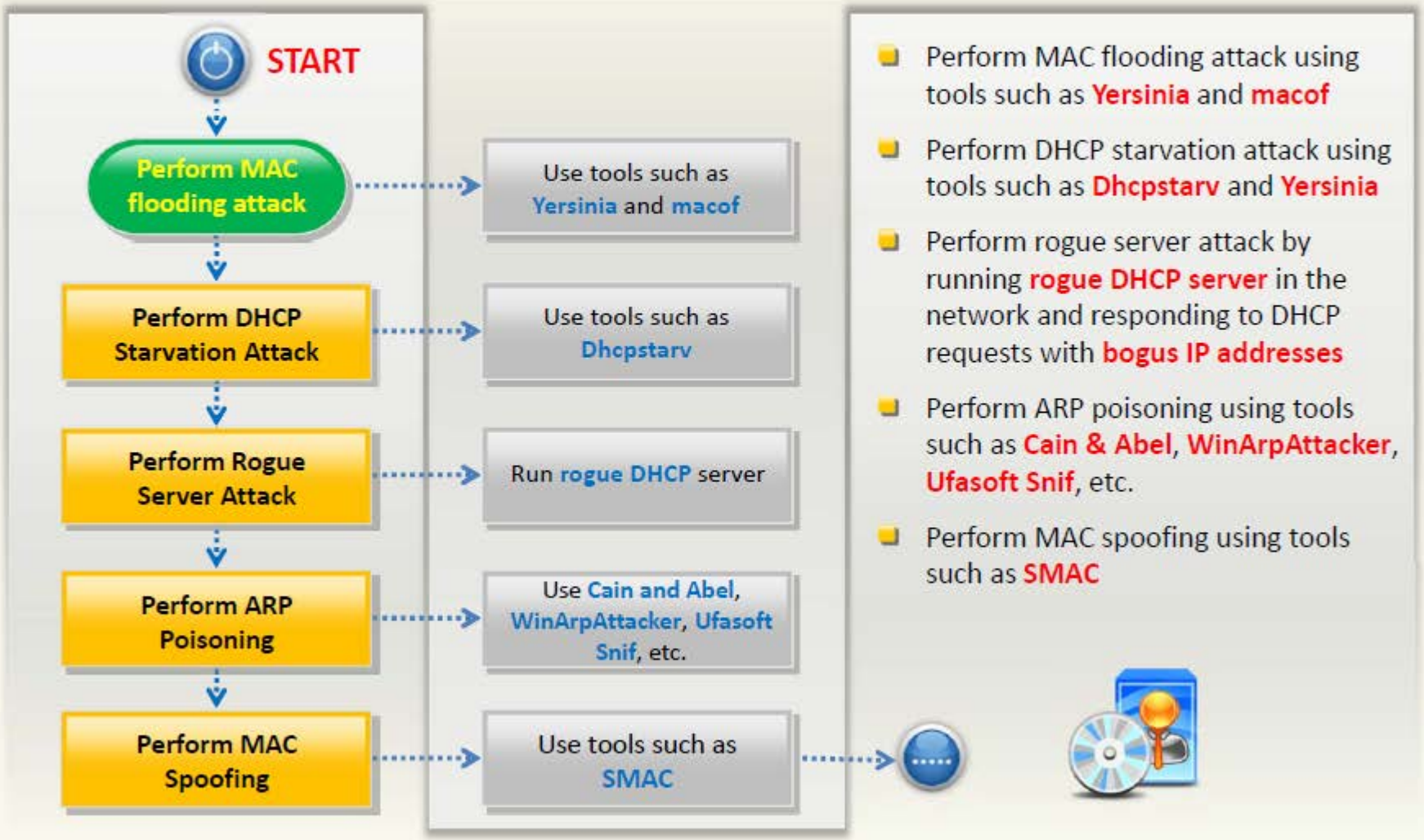
Implement security mechanism such as SSL and VPN to secure the network traffic

Identify rogue sniffing application in the network

Discover rogue DHCP and DNS servers in the network

Discover the presence of **unauthorized networking devices**

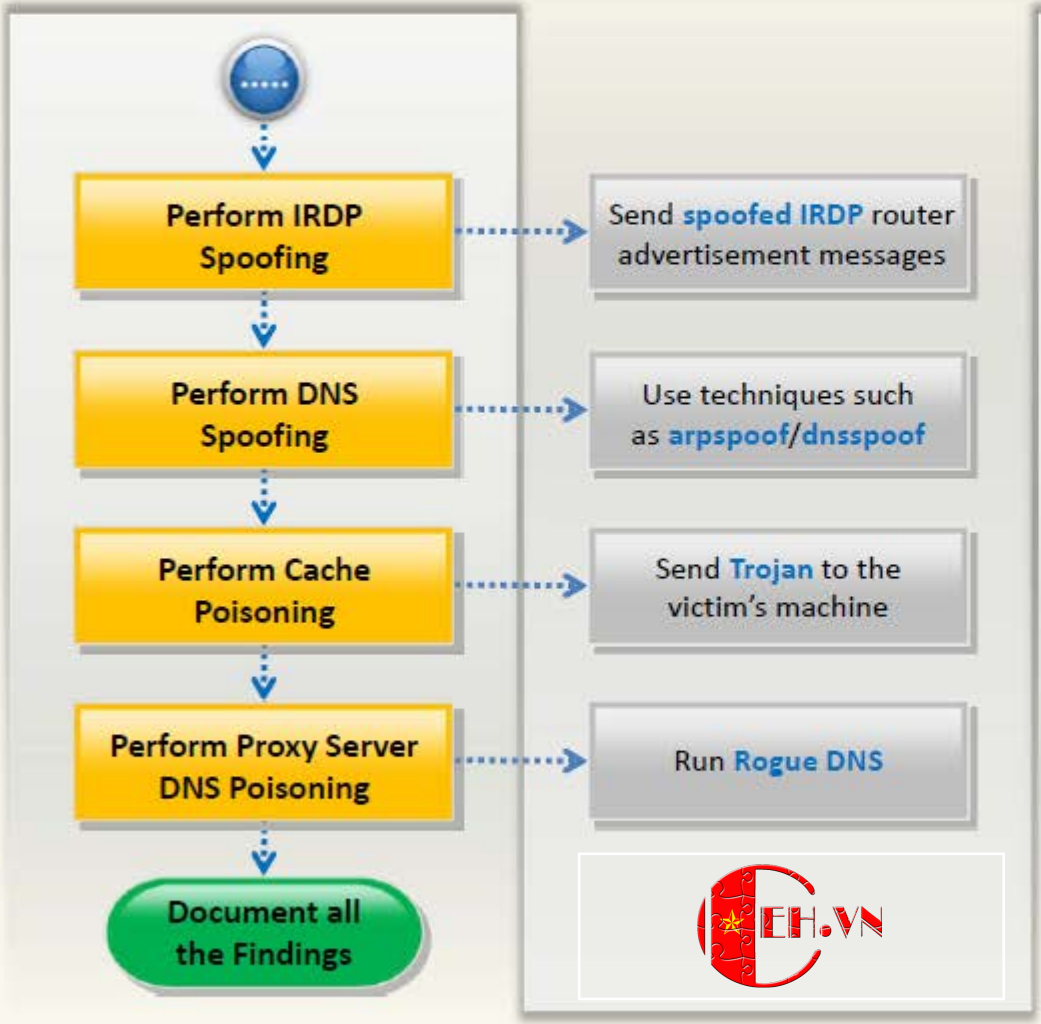
Sniffing Pen Testing (Cont'd)



- Perform MAC flooding attack using tools such as **Yersinia** and **macof**
- Perform DHCP starvation attack using tools such as **Dhcpstarv** and **Yersinia**
- 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 **Cain & Abel**, **WinArpAttacker**, **Ufasoft Snif**, etc.
- Perform MAC spoofing using tools such as **SMAC**

Sniffing Pen Testing (Cont'd)

- Perform 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 proxy server settings in IE 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