

# 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

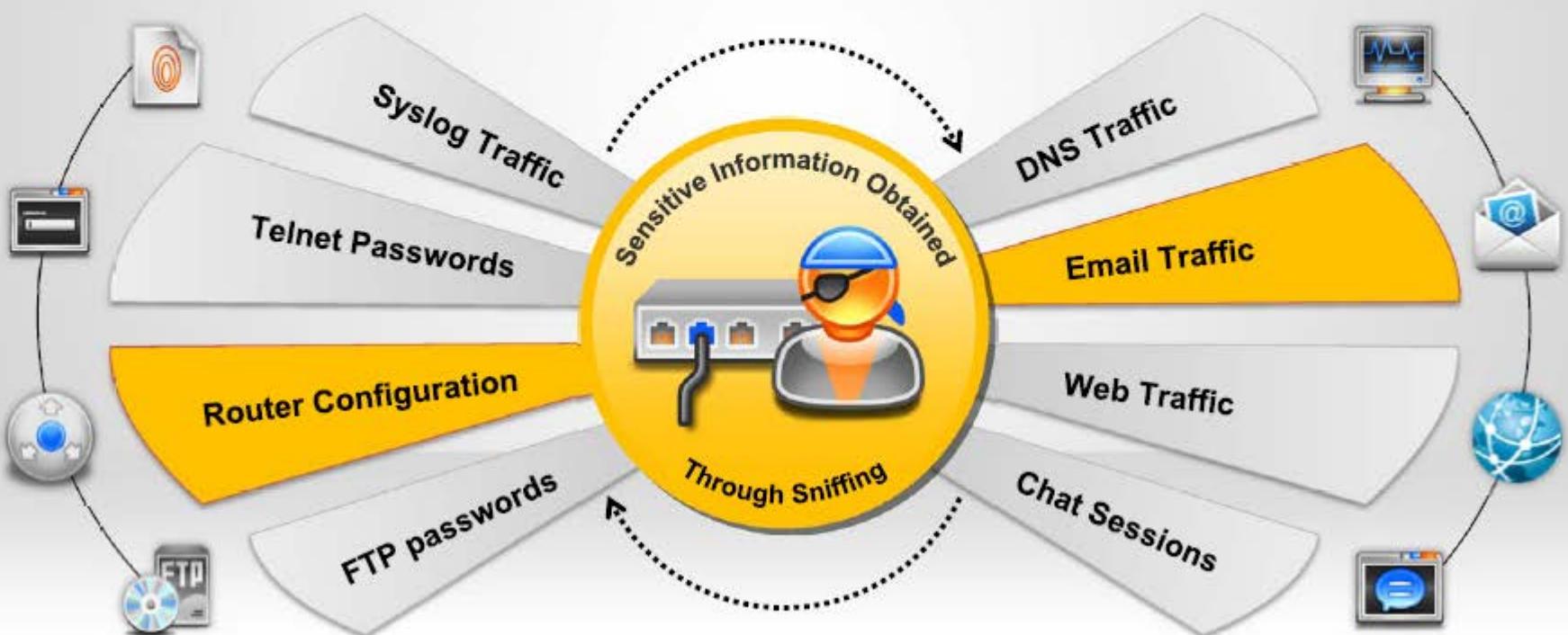


# Network Sniffing and Threats

CEH  
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

CEH  
Certified Ethical Hacker

## 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

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



4

DHCP Attacks

2

DNS Poisoning



5

Switch Port Stealing

3

ARP Poisoning



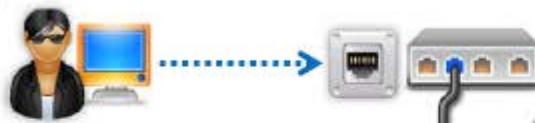
6

Spoofing Attack

# How an Attacker Hacks the Network Using Sniffers

**CEH**  
Certified Ethical Hacker

An attacker connects his laptop to a switch port



He runs discovery tools to learn about network topology



He identifies victim's machine to target his attacks



He poisons the victim machine by using ARP spoofing techniques



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

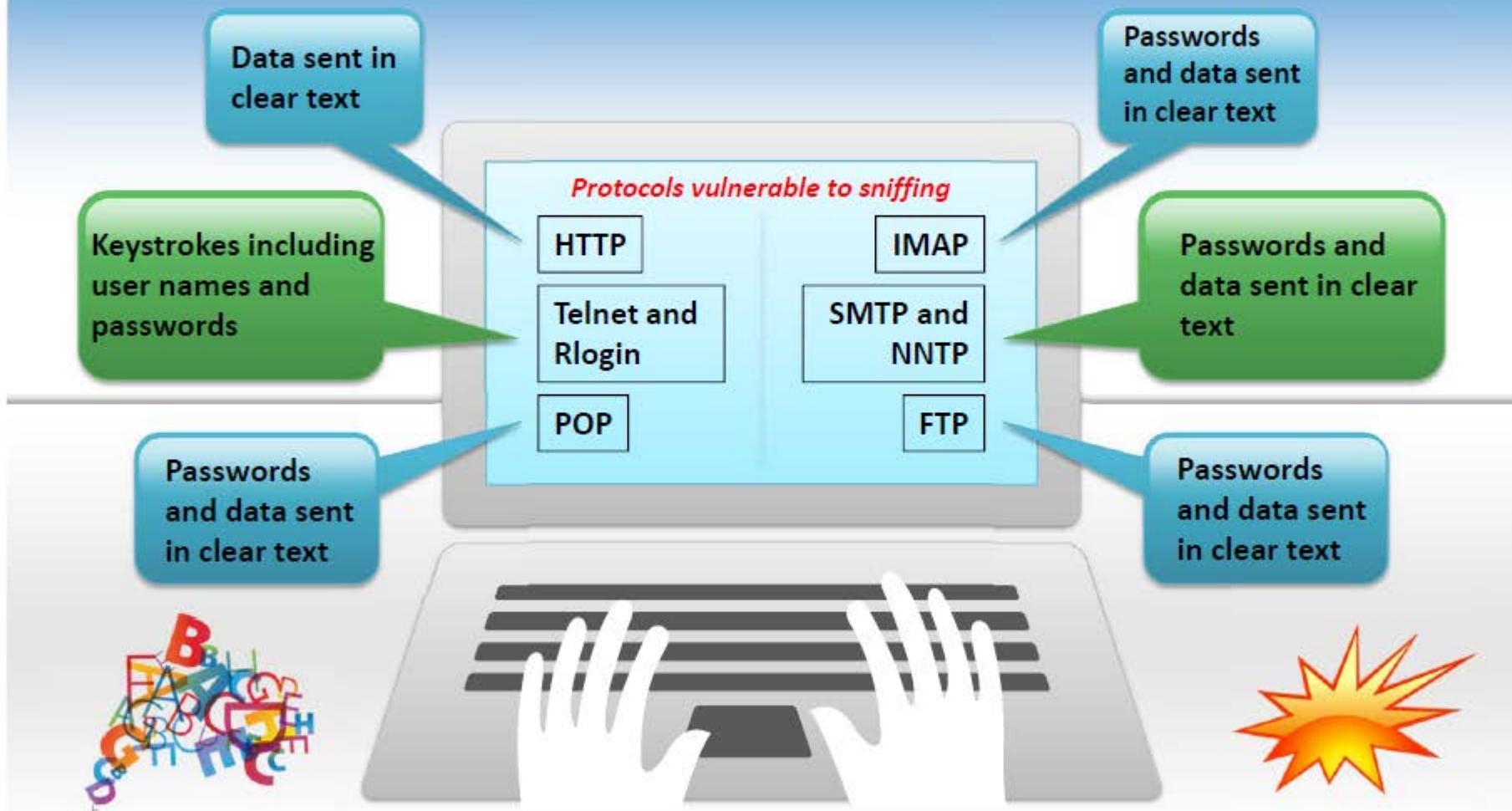


The hacker extracts passwords and sensitive data from the redirected traffic



# Protocols Vulnerable to Sniffing

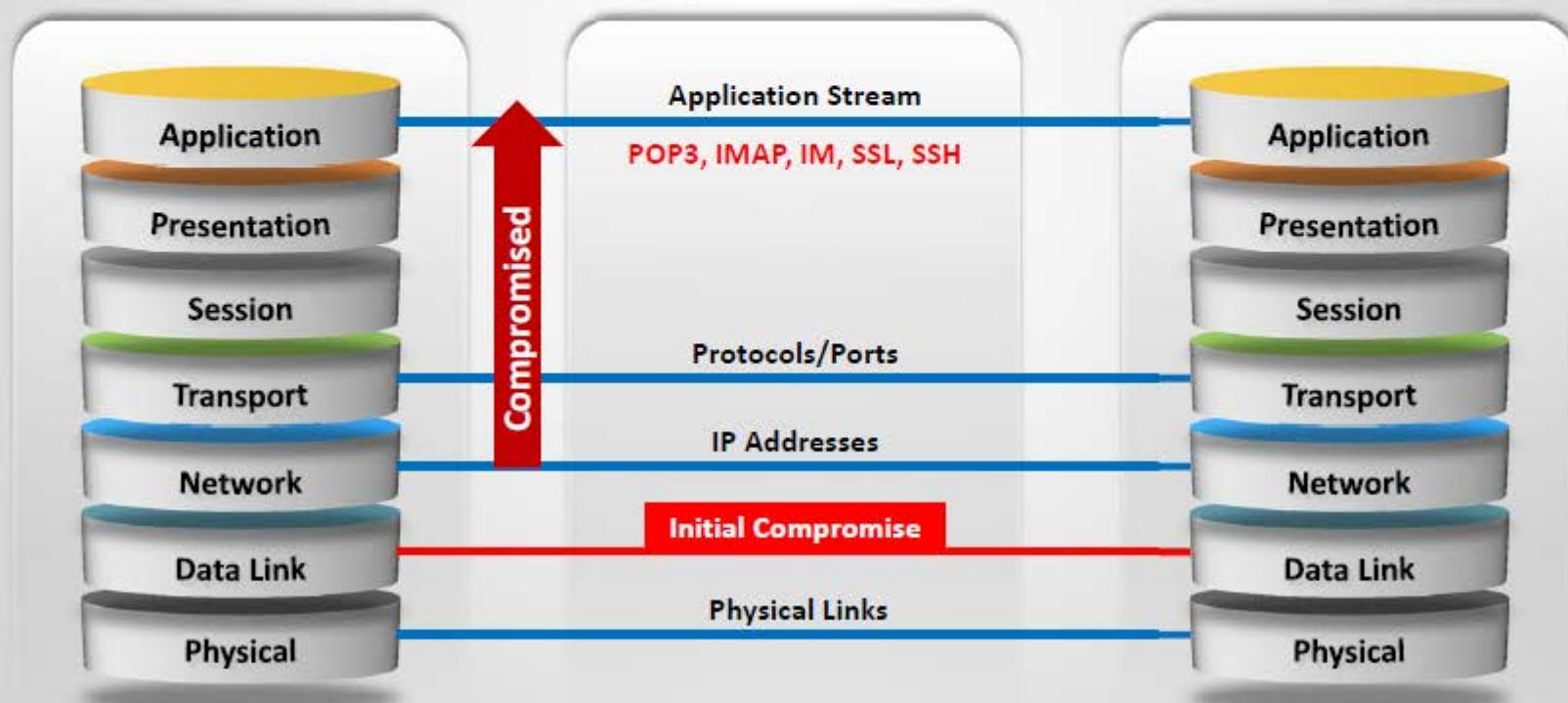
CEH  
Certified Ethical Hacker



# Sniffing in the Data Link Layer of the OSI Model

CEH  
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

CEH  
Certified Ethical Hacker

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

**CEH**  
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

**CEH**  
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



## Active Wiretapping

It monitors, records, alters and also injects something into the communication or traffic

## Passive Wiretapping

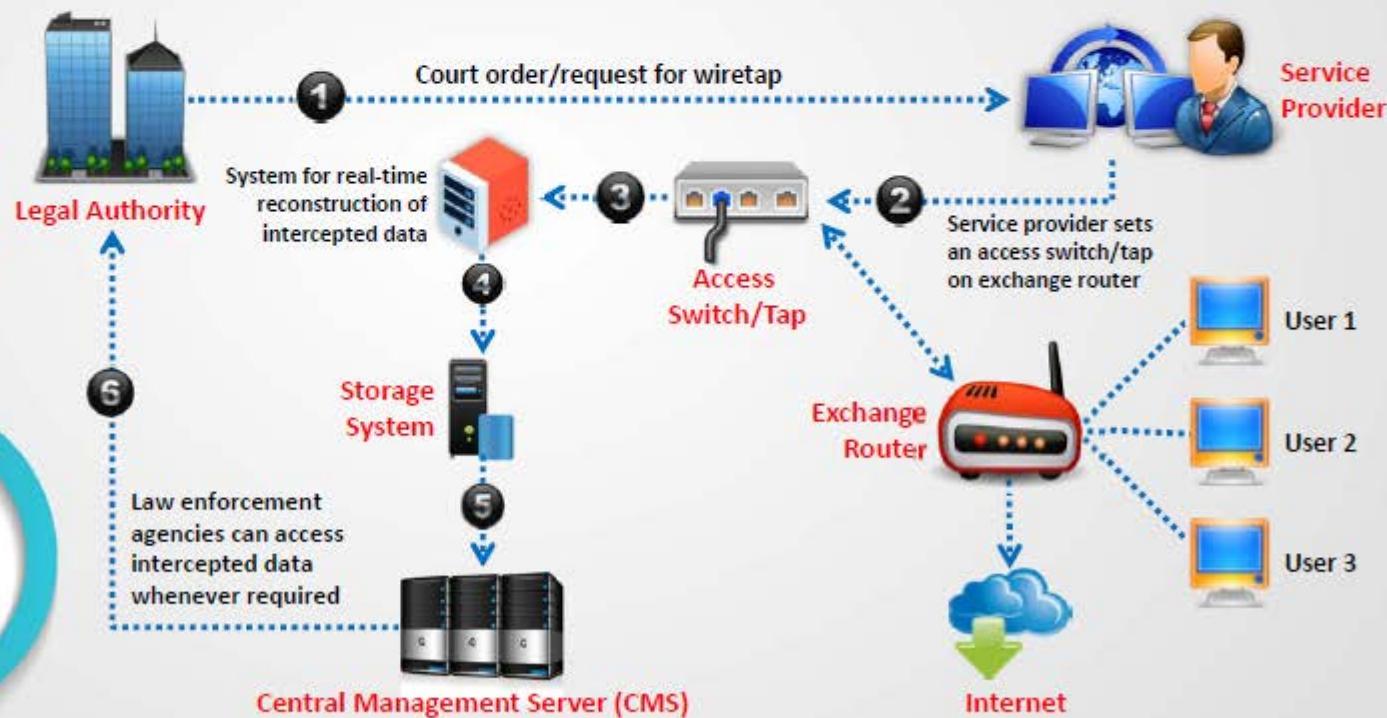
It only monitors and records the traffic and gain knowledge of the data it contains

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

# Lawful Interception



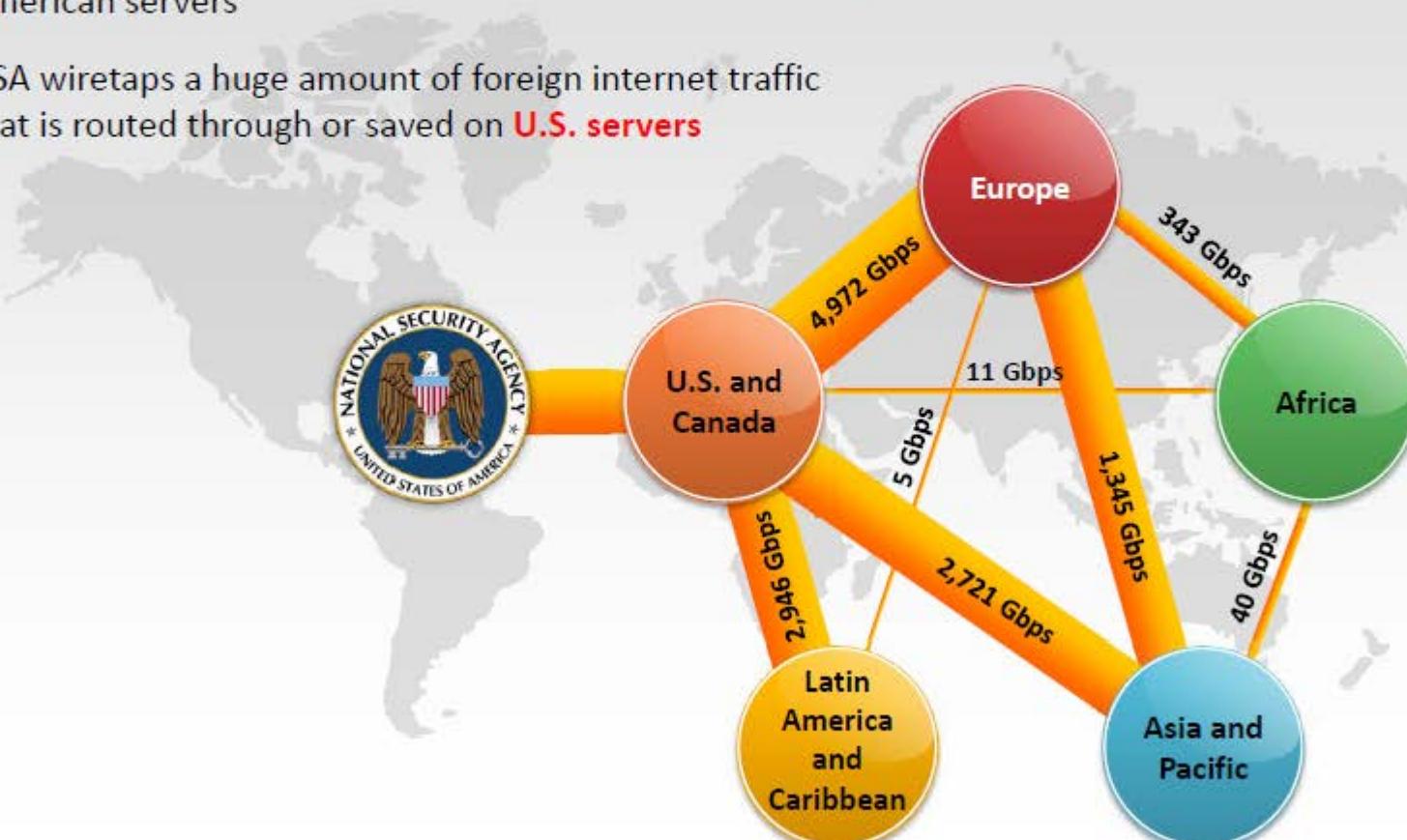
Lawful interception refers to legally **intercepting data communication** between two end points for surveillance on the traditional telecommunications, VoIP, data, and multiservice networks



# Wiretapping Case Study: PRISM

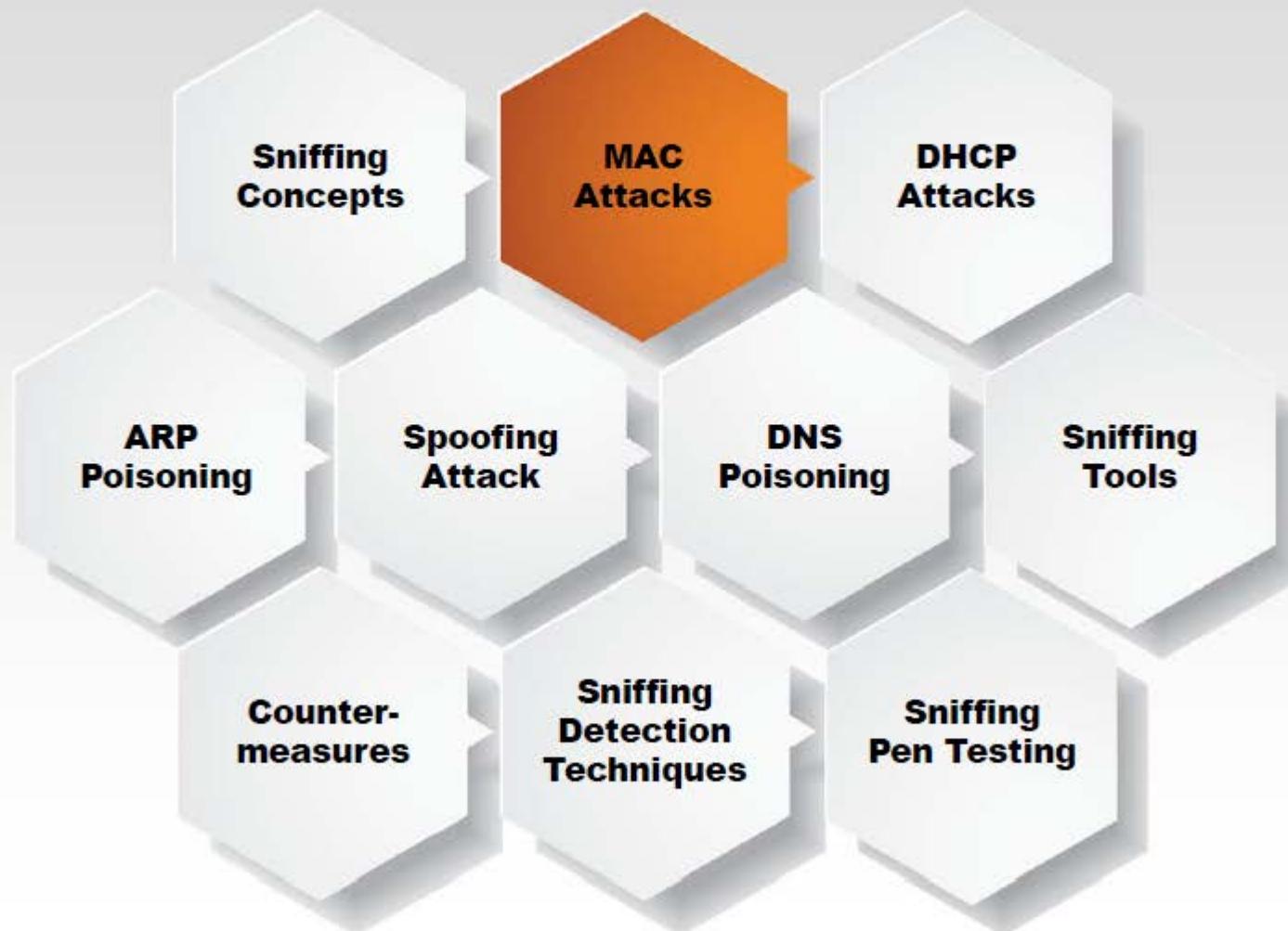
C|EH  
Certified Ethical Hacker

- 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

**CEH**  
Certified Ethical Hacker



# MAC Address/CAM Table

CEH  
Certified Ethical Hacker

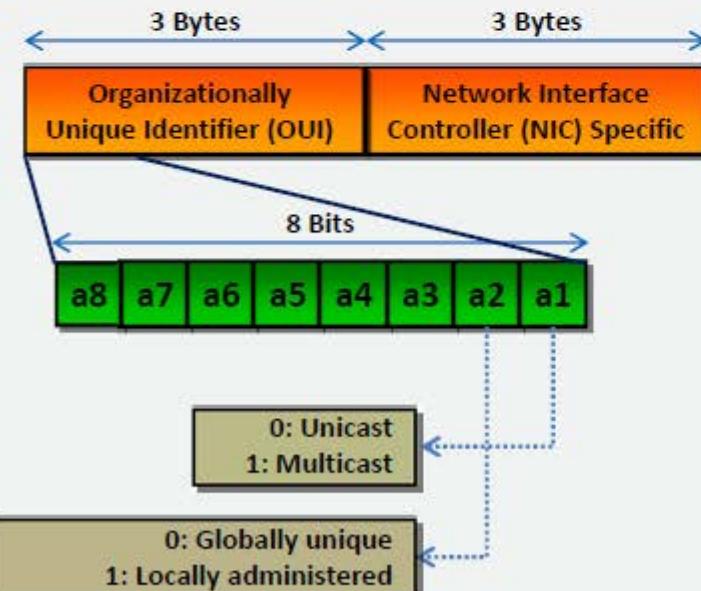


Each switch has a **fixed size dynamic Content Addressable Memory (CAM) table**



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	Dyna mic	Yes	0	Gi5/2
5	as23.df45.45t6	Dyna mic	Yes	0	Gi2/5
5	er23.23er.t5e3	Dyna mic	Yes	0	Gi1/6

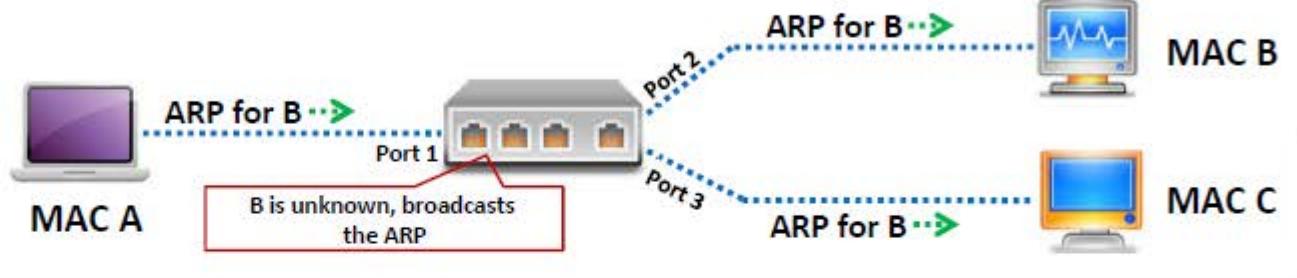


# How CAM Works

CEH  
Certified Ethical Hacker

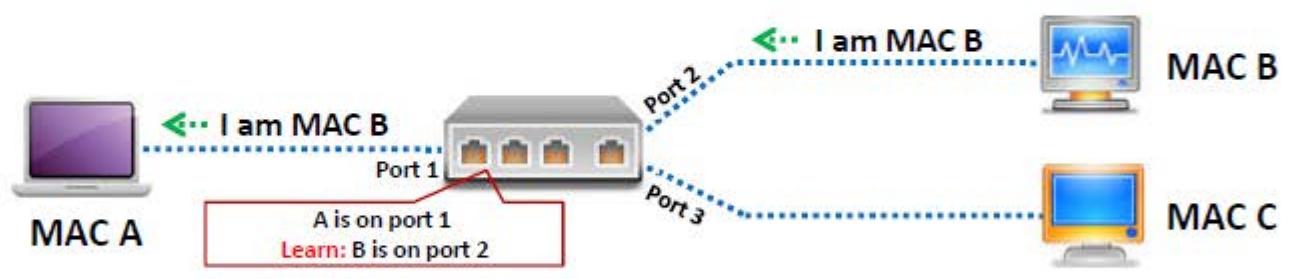
MAC	PORT
A	1
C	3

CAM Table



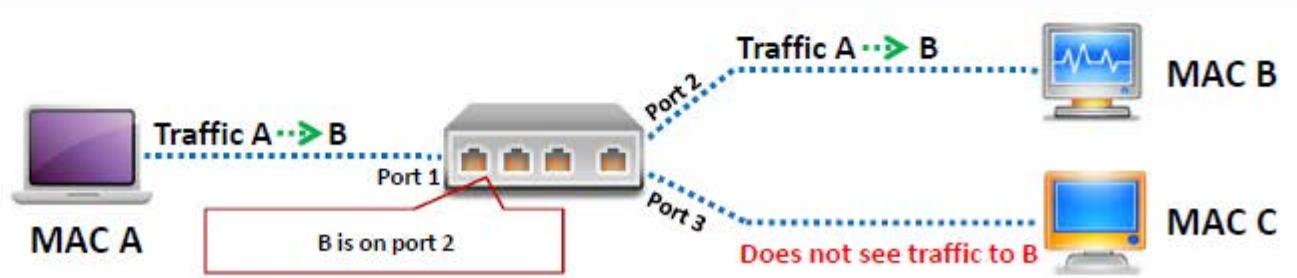
MAC	PORT
A	1
B	2
C	3

CAM Table



MAC	PORT
A	1
B	2
C	3

CAM Table



# What Happens When CAM Table Is Full?

CEH  
Certified Ethical Hacker



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



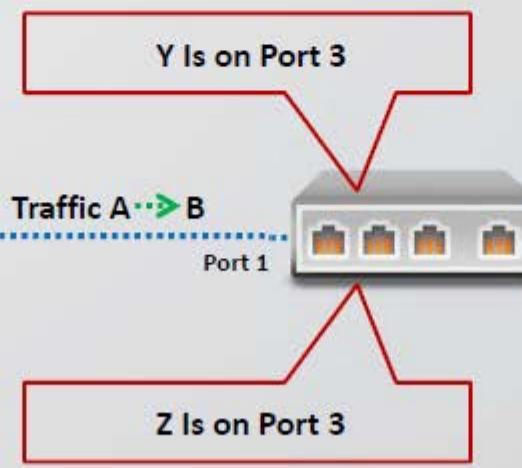
This attack will also **fill the CAM tables of adjacent switches**



MAC	PORT
Y	3
Z	3
C	3



MAC A



MAC B



MAC C

# MAC Flooding

CEH  
Certified Ethical Hacker

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



```
C:\ 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

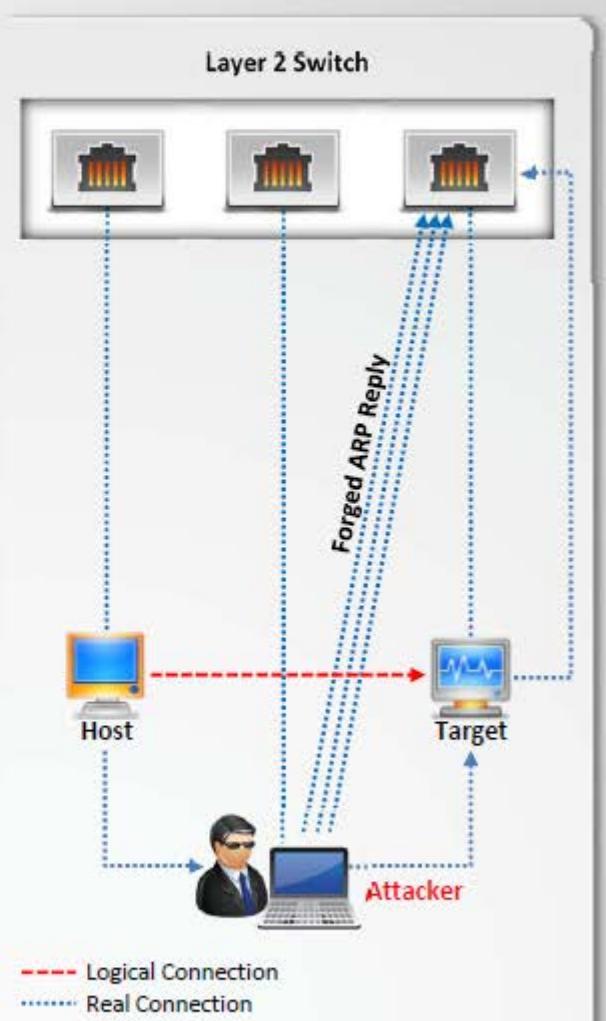
Attacker floods the switch with **forged gratuitous ARP packets** with target MAC address as source and his own MAC address as destination

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

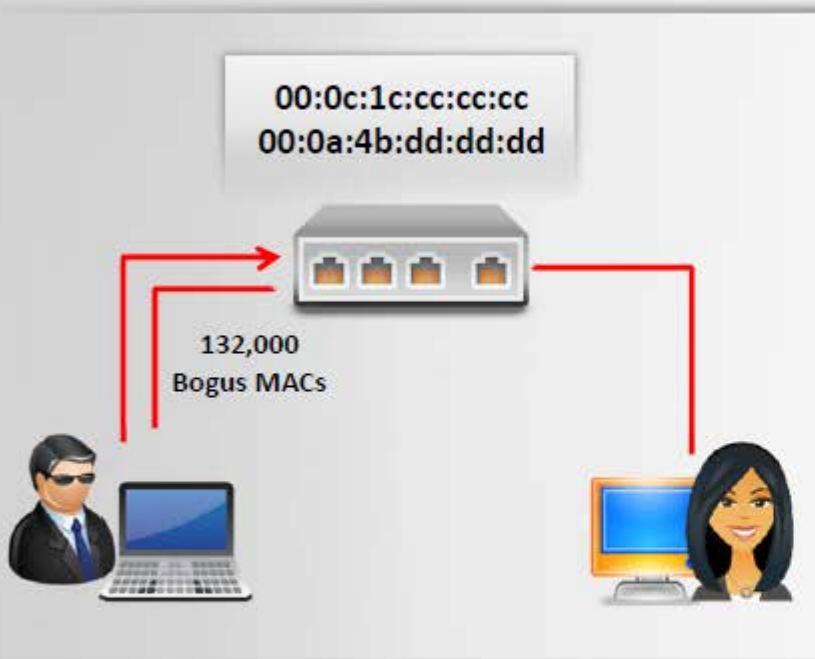
Attacker now manages to **steal the target host switch port** and sends ARP request to stolen switch port to discover target hosts' IP address

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



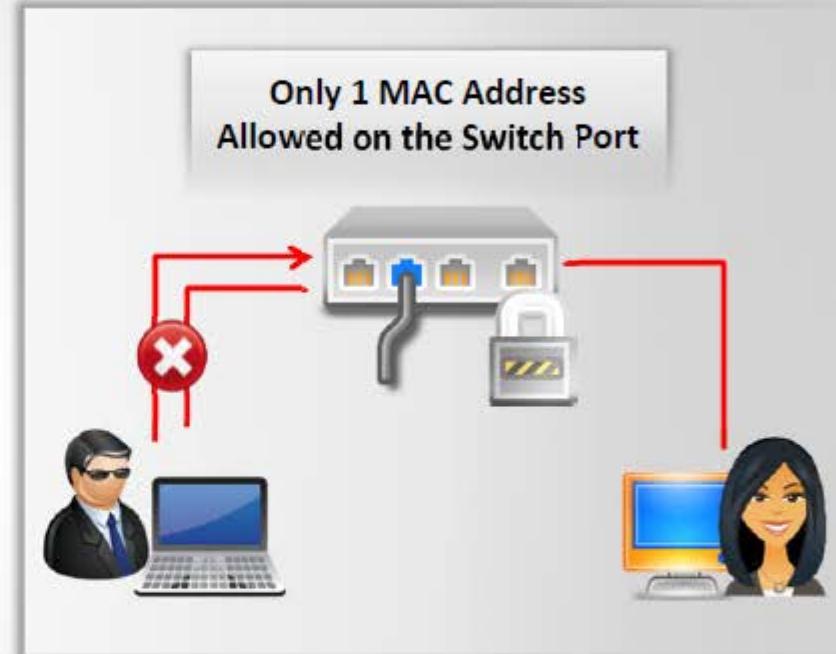
# How to Defend against MAC Attacks

CEH  
Certified Ethical Hacker



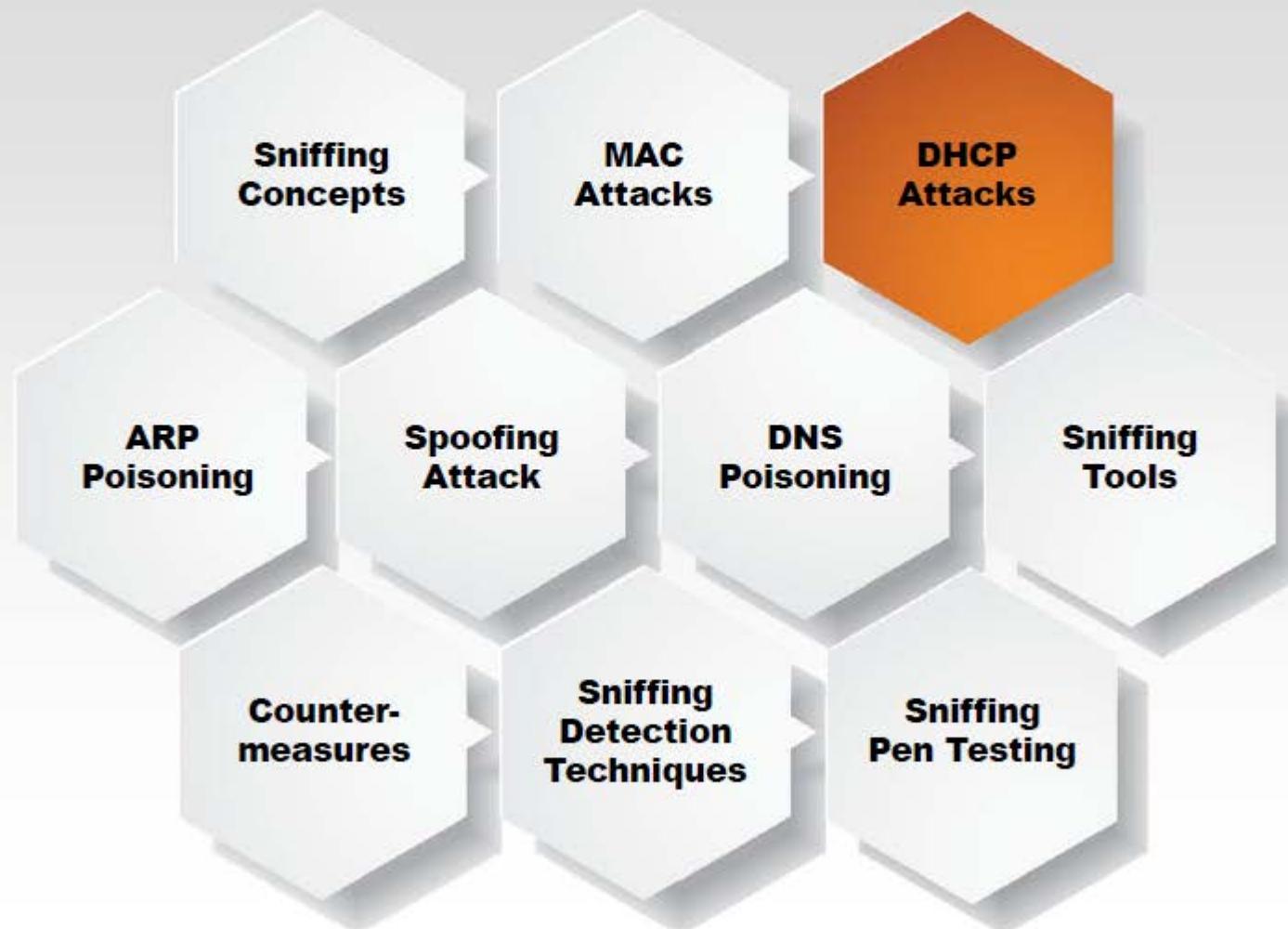
## Configuring Port Security on Cisco switch:

- 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

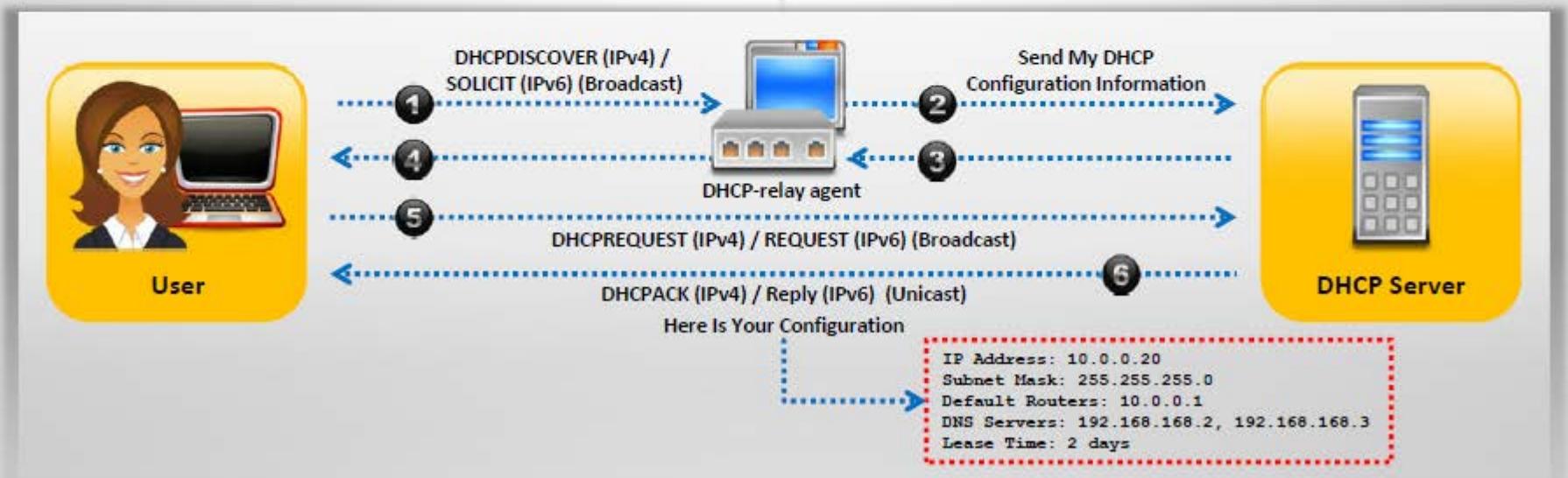


# How DHCP Works

CEH  
Certified Ethical Hacker

- 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**

- Client broadcasts **DHCPDISCOVER/SOLICIT** request asking for DHCP Configuration Information
- DHCP-relay agent captures the client request and **unicasts** it to the DHCP servers available in the network
- DHCP server unicasts **DHCPOFFER/ADVERTISE**, which contains client and server's MAC address
- Relay agent broadcasts **DHCPOFFER/ADVERTISE** in the client's subnet
- Client broadcasts **DHCPREQUEST/REQUEST** asking DHCP server to provide the DHCP configuration information
- 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
DHCPIinform	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 has expired

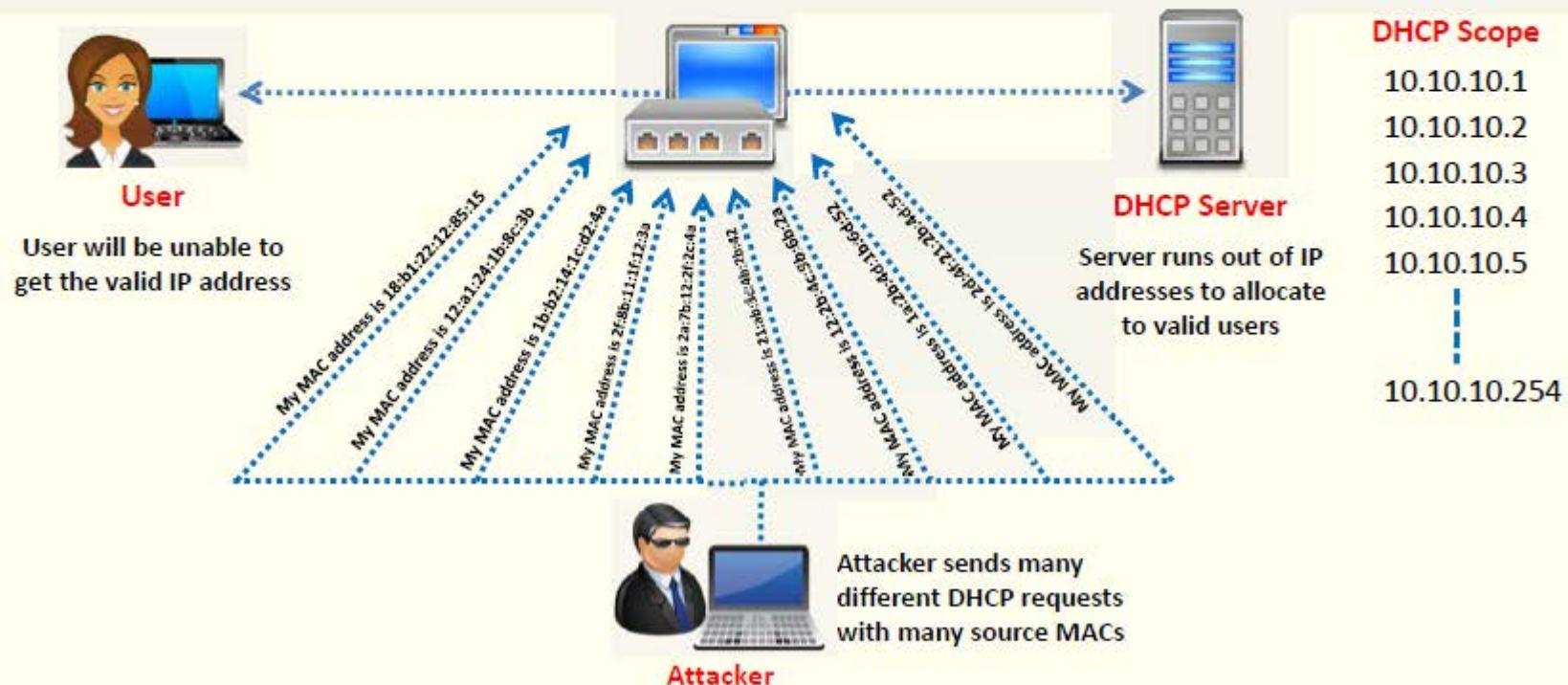
# IPv4 DHCP Packet Format

CEH  
Certified Ethical Hacker

OP Code	Hardware Type	Hardware Length	HOPS
Transaction ID (XID)			
Seconds		Flags	
Client IP Address (CIADDR)			
Your IP Address (YIADDR)			
Server IP Address (SIADDR)			
Gateway IP Address (GIADDR)			
Client Hardware Address (CHADDR)—16 bytes			
Server Name (SNAME)—64 bytes			
Filename—128 bytes			
DHCP Options			

# 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

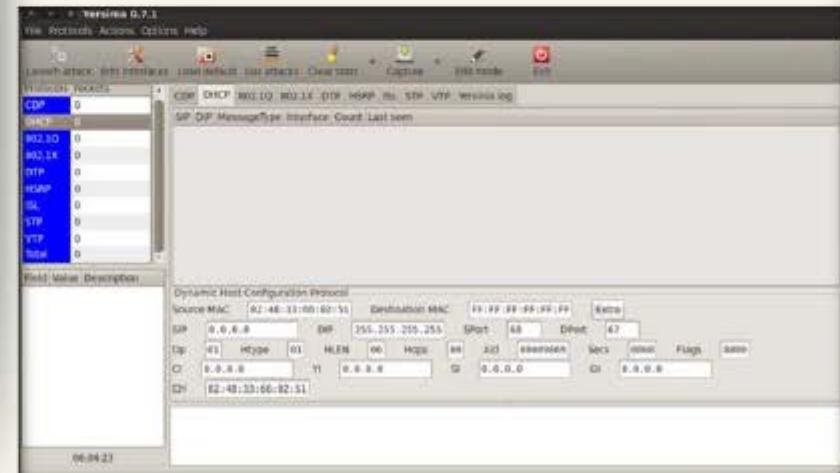
- dhcpstarv implements DHCP starvation attack. It requests **DHCP leases** on specified interface, saves them, and renews on regular basis



<http://dhcpstarv.sourceforge.net>

## Yersinia

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



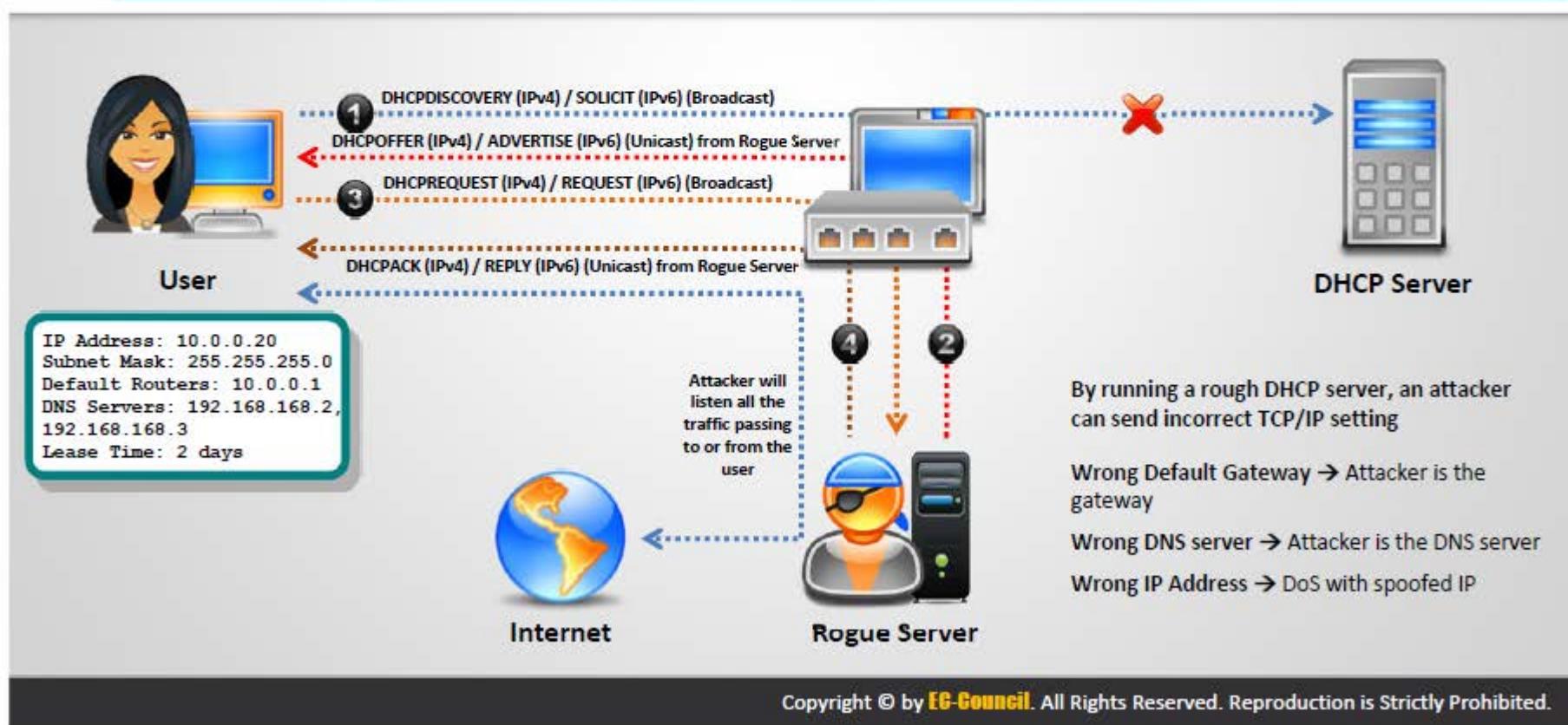
<http://www.yersinia.net>

# Rogue DHCP Server Attack

CEH  
Certified Ethical Hacker

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

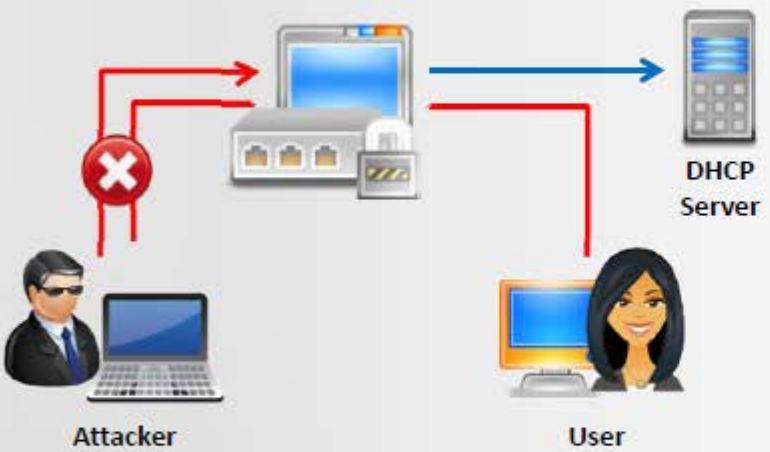


# How to Defend Against DHCP Starvation and Rogue Server Attack



**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

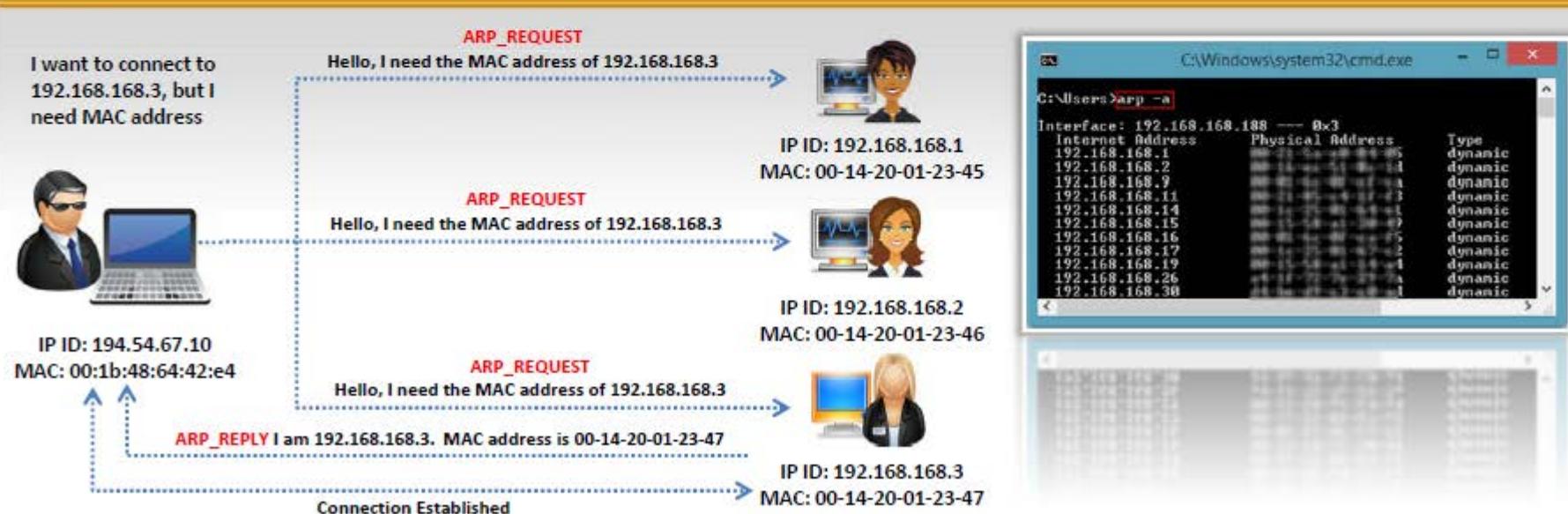
# Module Flow



# What Is Address Resolution Protocol (ARP)?



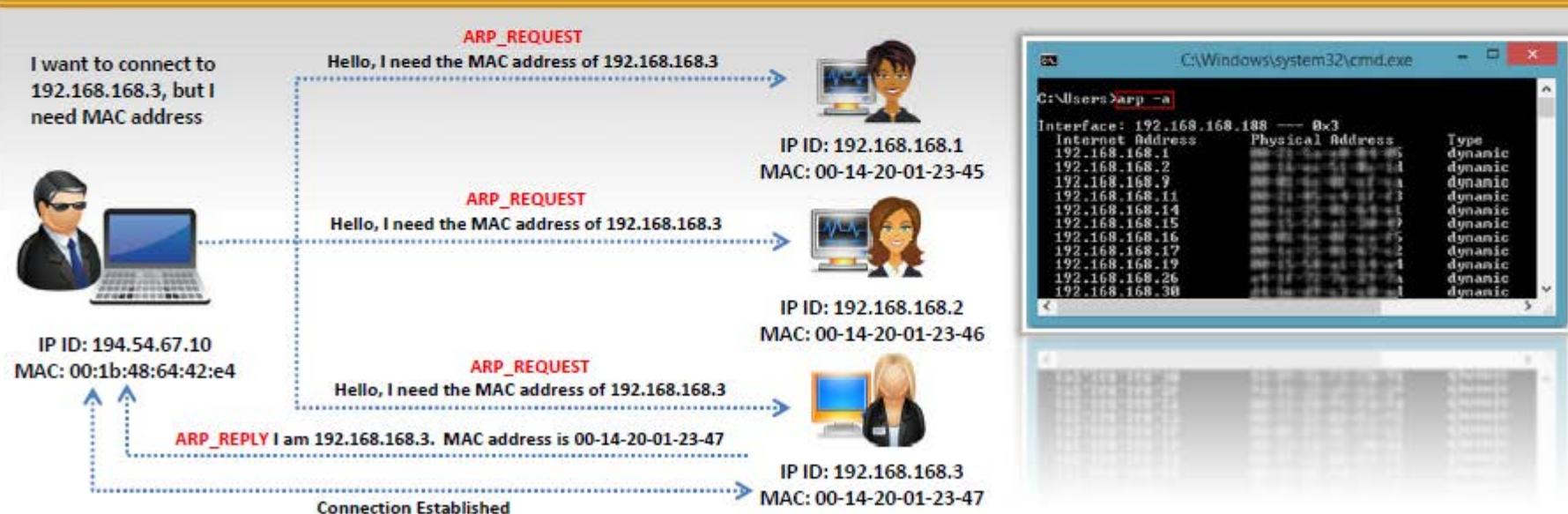
- Address Resolution Protocol (ARP) is a stateless protocol used for **resolving IP addresses to machine (MAC) addresses**
- All network devices (that needs to communicate on the network) broadcasts ARP queries in the network to find out other **machines' MAC addresses**
- When one machine needs to communicate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

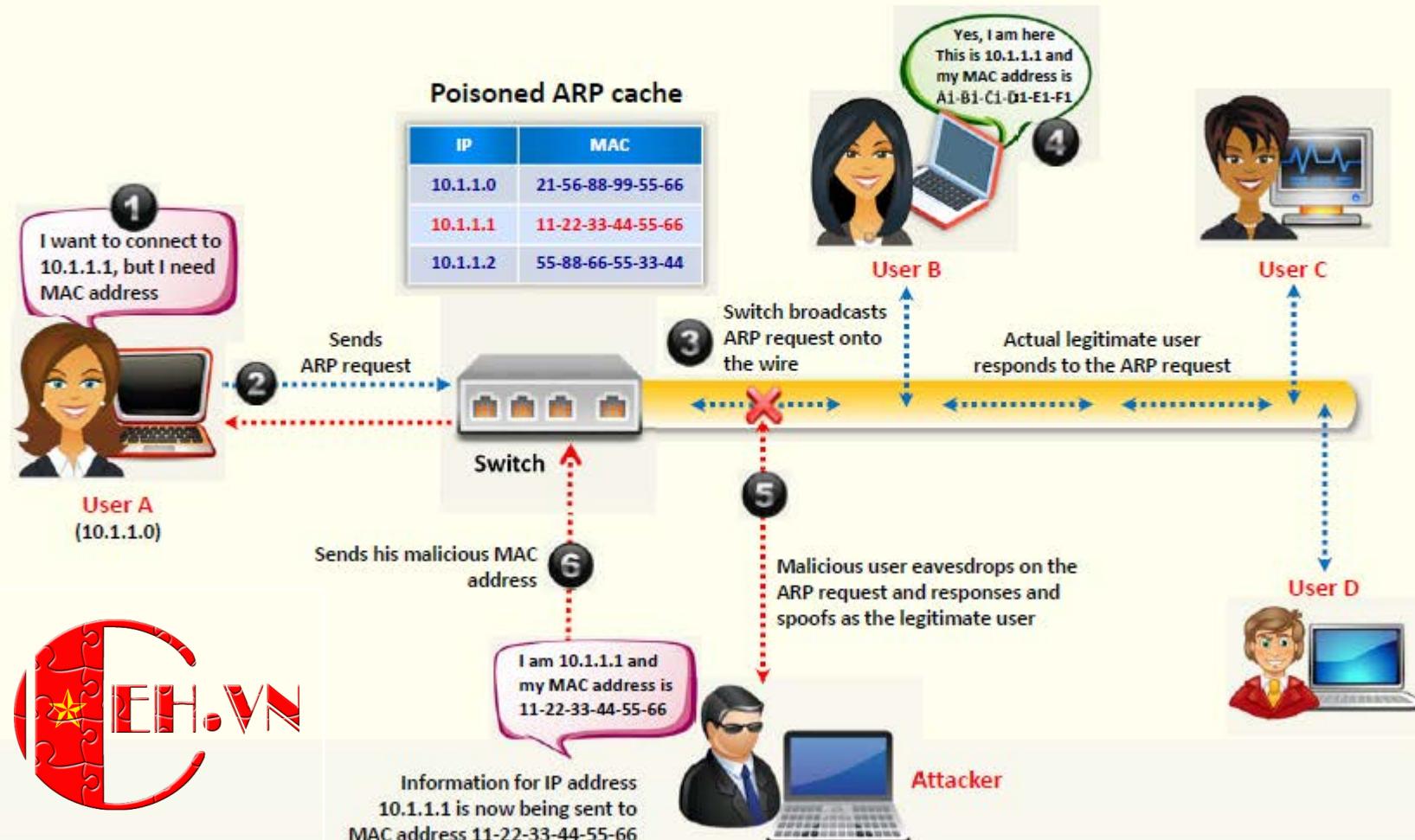


Switch is set in '**forwarding mode**' after ARP table is flooded with spoofed ARP replies and attackers can sniff all the network packets



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



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



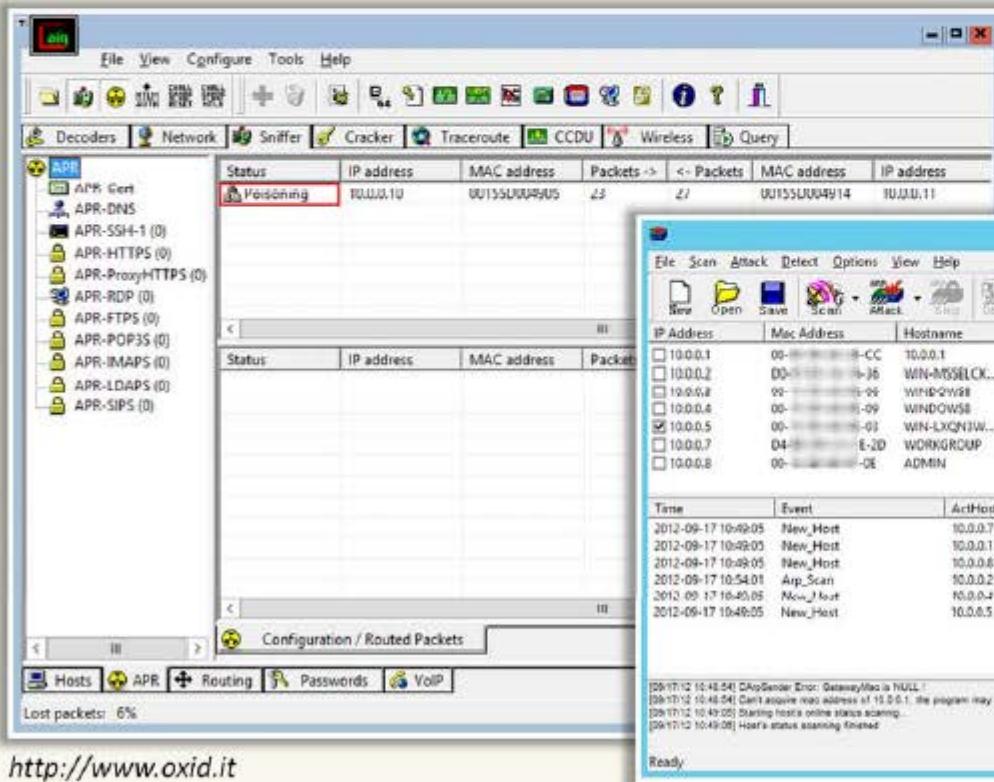
Denial-of-Service (DoS) Attack

# ARP Poisoning Tools: Cain & Abel and WinArpAttacker



## Cain & Abel

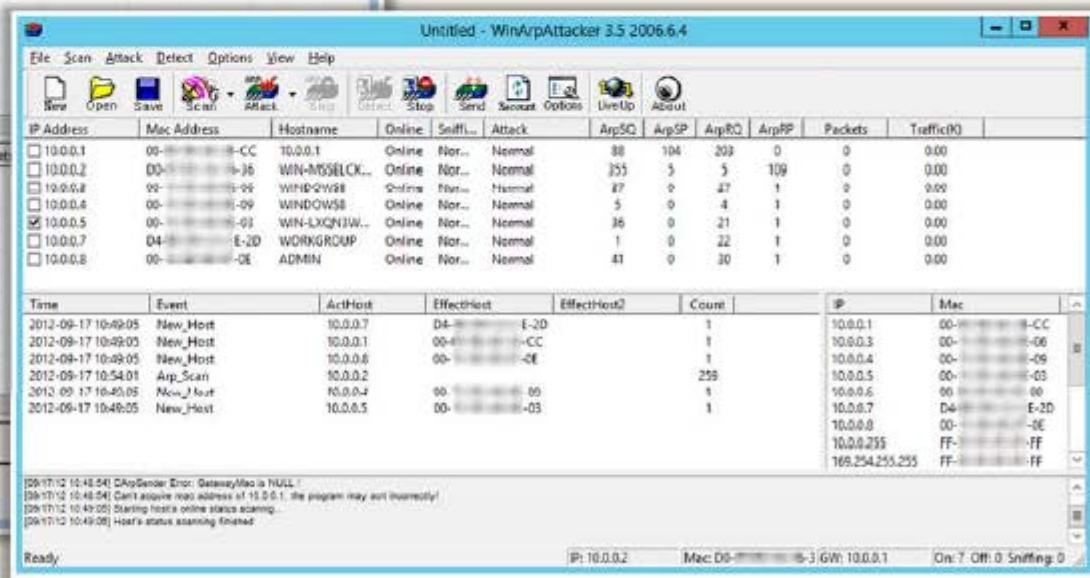
- Cain & Abel allows sniffing packets of various protocols on **switched LANs** by hijacking IP traffic of multiple hosts concurrently



<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

CEH  
Certified Ethical Hacker

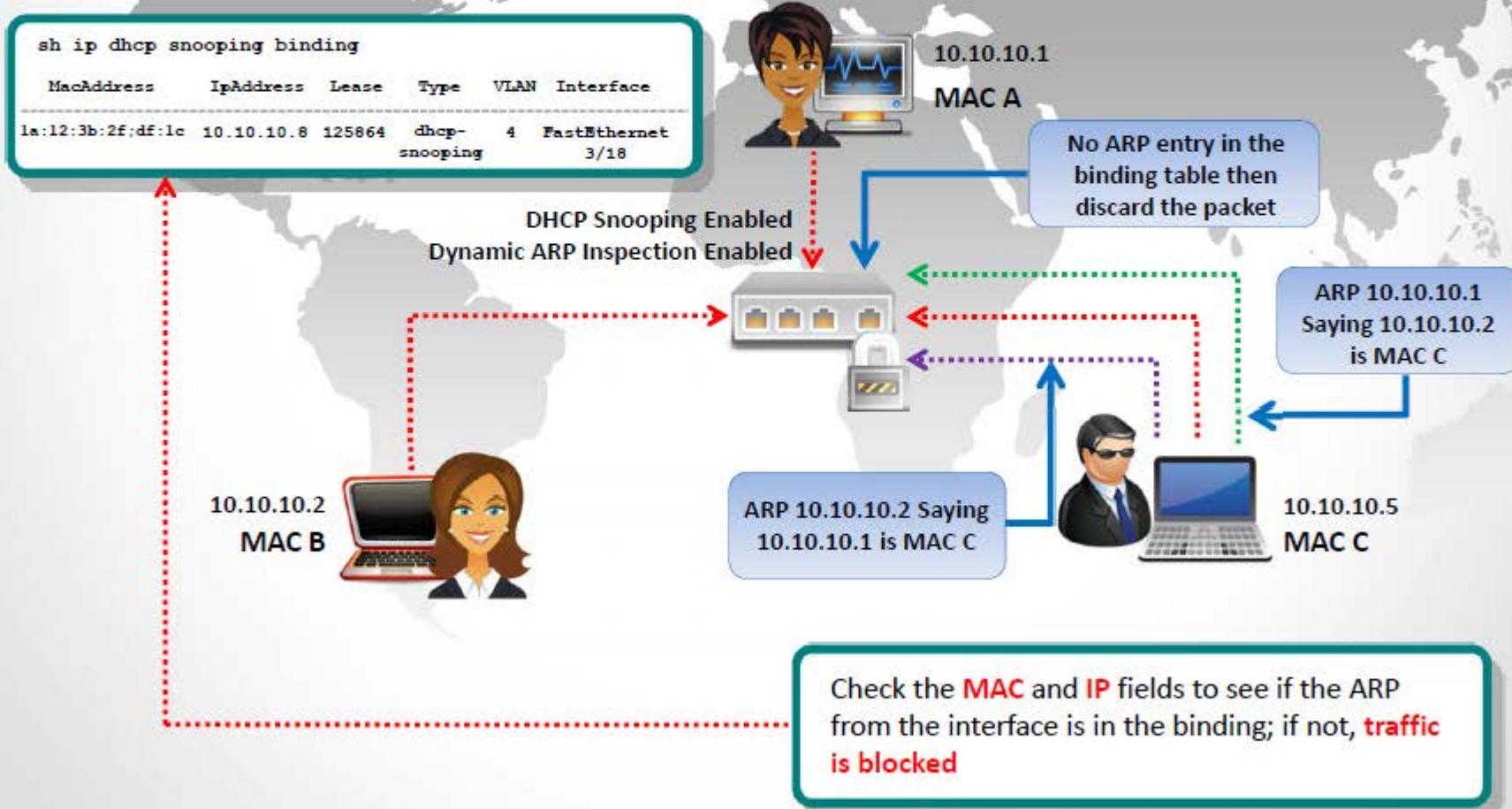


Ufasoft Snif is an automated ARP poisoning tool that sniffs **passwords** and **email messages** on the network and works on **Wi-Fi network** as well.

# How to Defend Against ARP Poisoning



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



# Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches



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

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
```

2

```
Switch# show ip dhcp snooping binding
MacAddress      IpAddress Lease     Type      VLAN      Interface
1a:12:3b:2f:df:1c 10.10.10.8 125864  dhcp-snooping  4  FastEthernet
                                         0/3
Total number of bindings: 1
```

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

CEH  
Certified Ethical Hacker



- 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

XArp - unregistered version

Status: ARP attacks detected!

Security level set to: aggressive

aggressive      The aggressive security level enables all ARP packet inspection modules and sends out discovery packets in high frequency. Using this level might give false attack alerts as it operates on a highly aggressive packet inspection philosophy.

high

basic

minimal

Get XArp Professional now!  
Register XArp Professional

IP	MAC	Host	Vendor	Interface	Online	Cache	First seen
192.168.168.83	d4-...-08	Windows	unknown	0x3 - Intel(R) P...	yes	yes	10/17/2013
192.168.168.87	d4-...-08	Windows	unknown	0x3 - Intel(R) P...	yes	yes	10/17/2013
192.168.168.99	d4-...-08	Windows	unknown	0x3 - Intel(R) P...	yes	yes	10/17/2013
192.168.168.100	00-...-08	Windows	0	Foxconn	0x3 - Intel(R) P...	yes	10/17/2013
192.168.168.101	d4-...-08	Windows	unknown	0x3 - Intel(R) P...	yes	yes	10/17/2013
192.168.168.110	d4-...-08	Windows	unknown	0x3 - Intel(R) P...	yes	yes	10/17/2013
192.168.168.111	d4-...-08	Windows	unknown	0x3 - Intel(R) P...	yes	yes	10/17/2013
192.168.168.113	d4-...-08	Windows	unknown	0x3 - Intel(R) P...	yes	yes	10/17/2013
192.168.168.133	00-...-08	Windows	Micro-star Int'l...	0x3 - Intel(R) P...	yes	yes	10/17/2013
192.168.168.144	00-...-08	Windows	4	Netgear, Inc.	0x3 - Intel(R) P...	yes	10/17/2013
192.168.168.153	a4-...-08	Windows	3	unknown	0x3 - Intel(R) P...	yes	10/17/2013
192.168.168.168	00-...-08	Windows	3	Sonicwall	0x3 - Intel(R) P...	yes	10/17/2013
192.168.168.188	08-...-08	Cadmus Com...	Cadmus Com...	0x3 - Intel(R) P...	yes	no	10/17/2013
192.168.168.189	f0-...-08	Windows	unknown	0x3 - Intel(R) P...	yes	yes	10/17/2013

XArp 2.2.2 - 35 mappings - 1 interface - 2 alerts

OK

< >

Alert 1 of 2

10/17/2013 15:32:55

DirectedRequestFilter: targeted request, destination mac of arp request not set to broadcast/invalid address

Interface : 0x3 [ethernet]  
source mac: 08-...-08 E  
dest mac : d4-...-08 7  
type : 0x806 [arp]  
direction : out  
type : request  
source ip : 192.168.168.188  
dest ip : 192.168.168.87  
source mac: 08-...-08 E  
dest mac : d4-...-08 7

<http://www.chrismc.de>

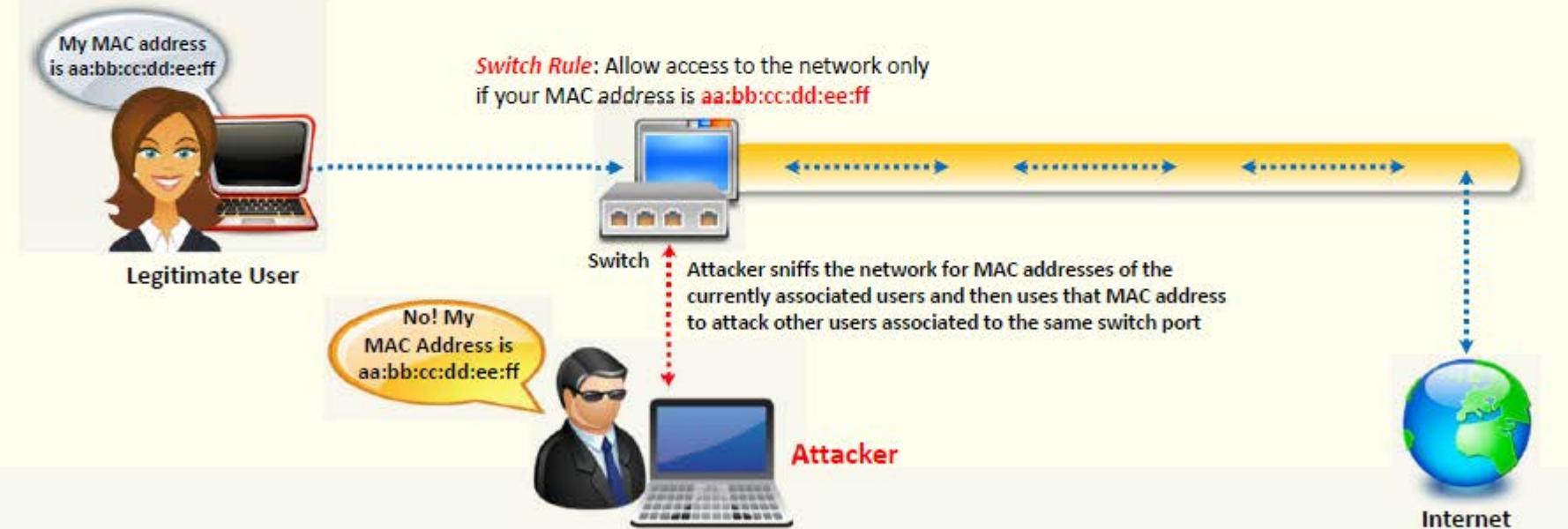
# Module Flow



# MAC Spoofing/Duplicating

CEH  
Certified Ethical Hacker

- 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



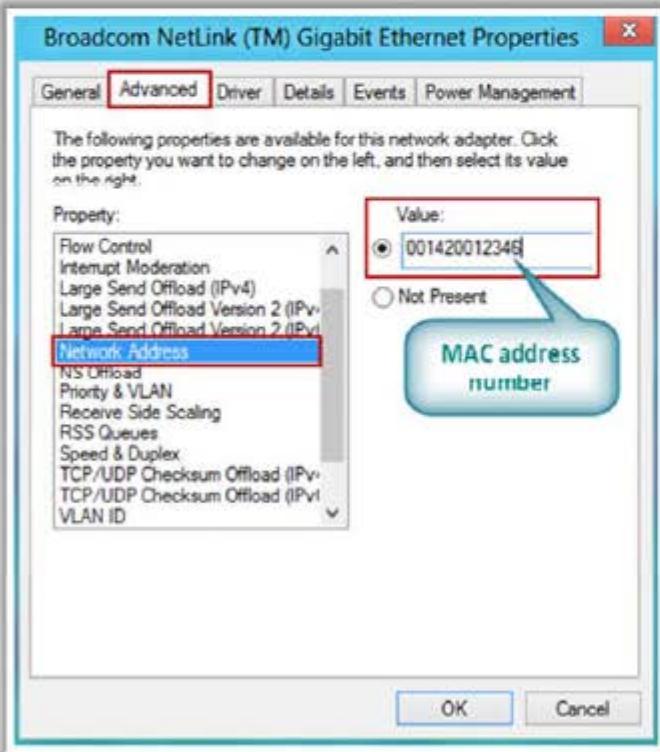
**Note:** This technique can be used to bypass Wireless Access Points' MAC filtering

# MAC Spoofing Technique: Windows



## 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)

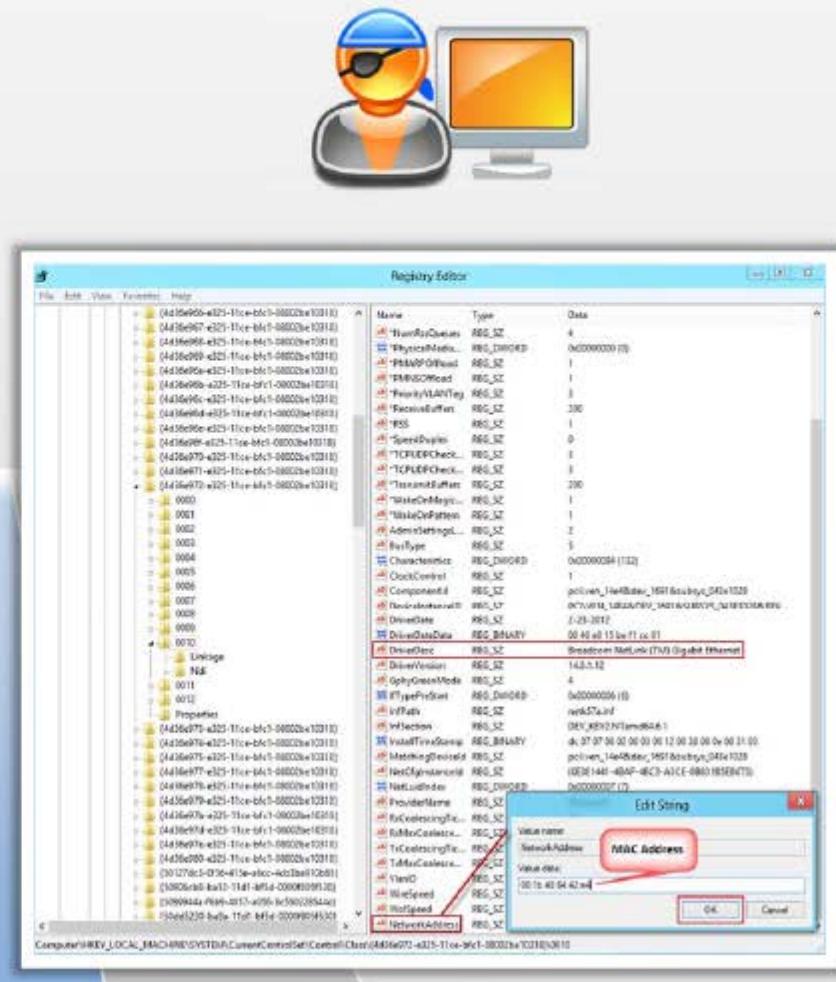


## Method 2: Steps to change MAC address in Registry

- Go to **Start → Run**, type **regedit32** to start registry editor

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

- Go to  
**"HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControls et\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

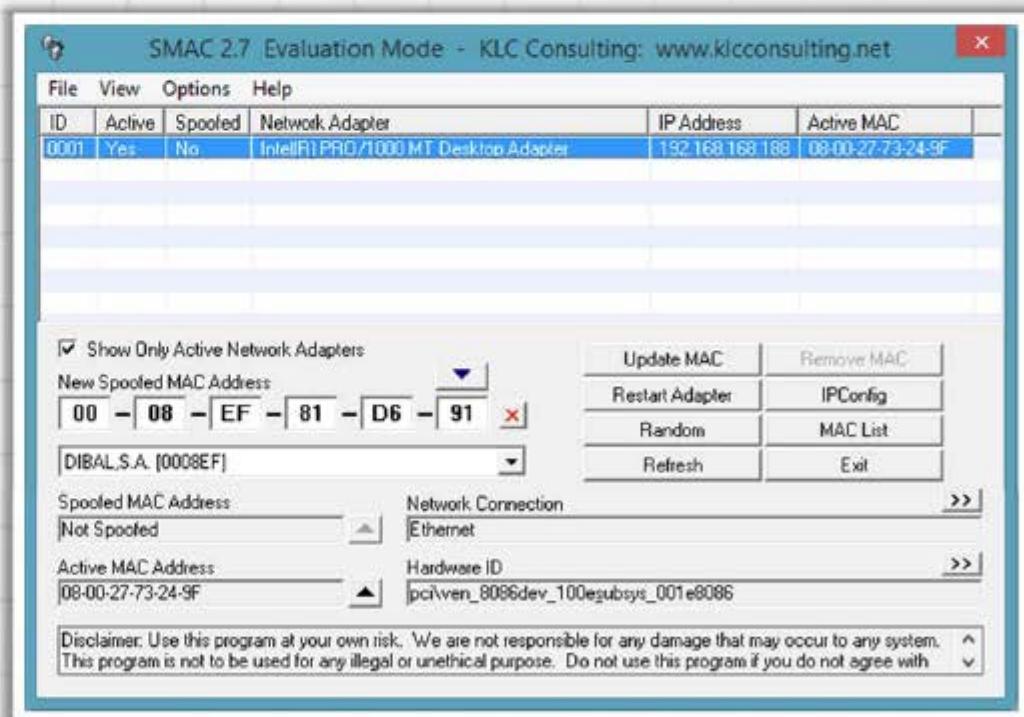


SMAC is a MAC Address Changer (Spoofing) tool that allows users to **change MAC address** for any network interface cards (NIC) on the Windows systems.



## 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.kleeeconsulting.net>

# 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	FastEthernet 3/18

10.10.10.2  
MAC B



DHCP Snooping Enabled  
Dynamic ARP Inspection Enabled  
IP Source Guard Enabled

10.10.10.1  
MAC A



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

Traffic Sent with IP  
10.10.10.2 Mac C

Received Traffic Source  
IP 10.10.10.2 Mac B



Traffic Sent with IP  
10.10.10.5 Mac B

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

# 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	FastEthernet 3/18

10.10.10.2  
MAC B



DHCP Snooping Enabled  
Dynamic ARP Inspection Enabled  
IP Source Guard Enabled

10.10.10.1  
MAC A



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

Traffic Sent with IP  
10.10.10.2 Mac C

Received Traffic Source  
IP 10.10.10.2 Mac B



Traffic Sent with IP  
10.10.10.5 Mac B

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

# Module Flow

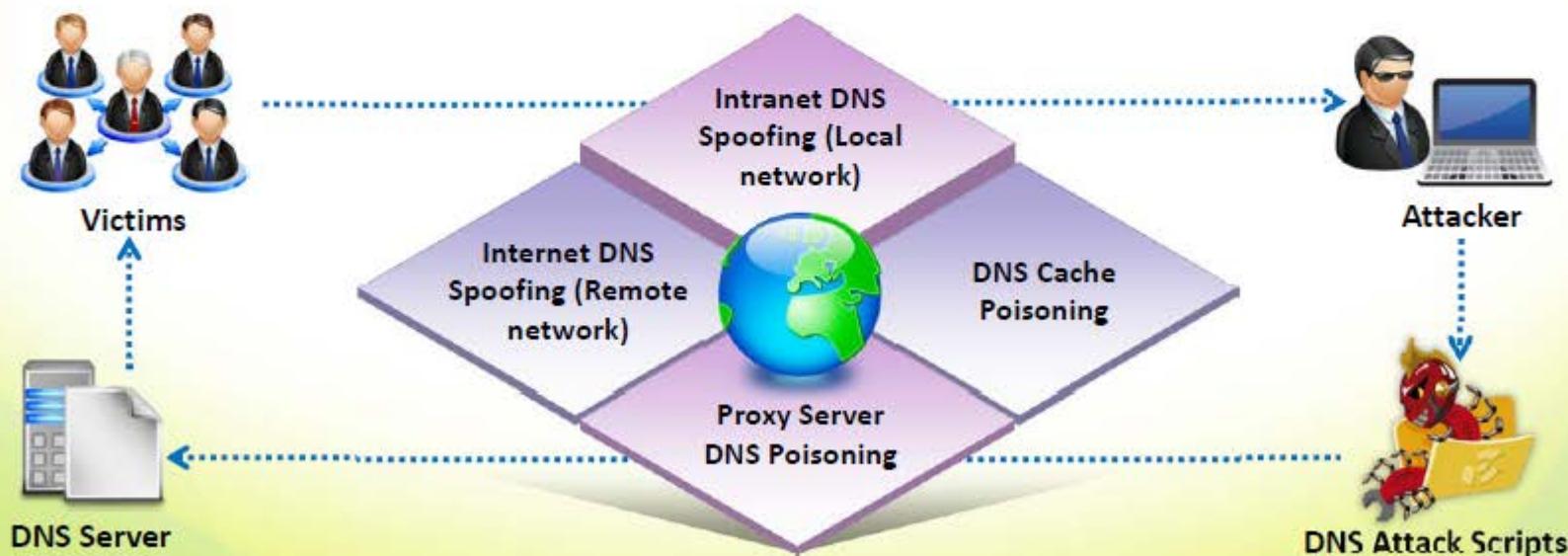


# DNS Poisoning Techniques

CEH  
Certified Ethical Hacker

- 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

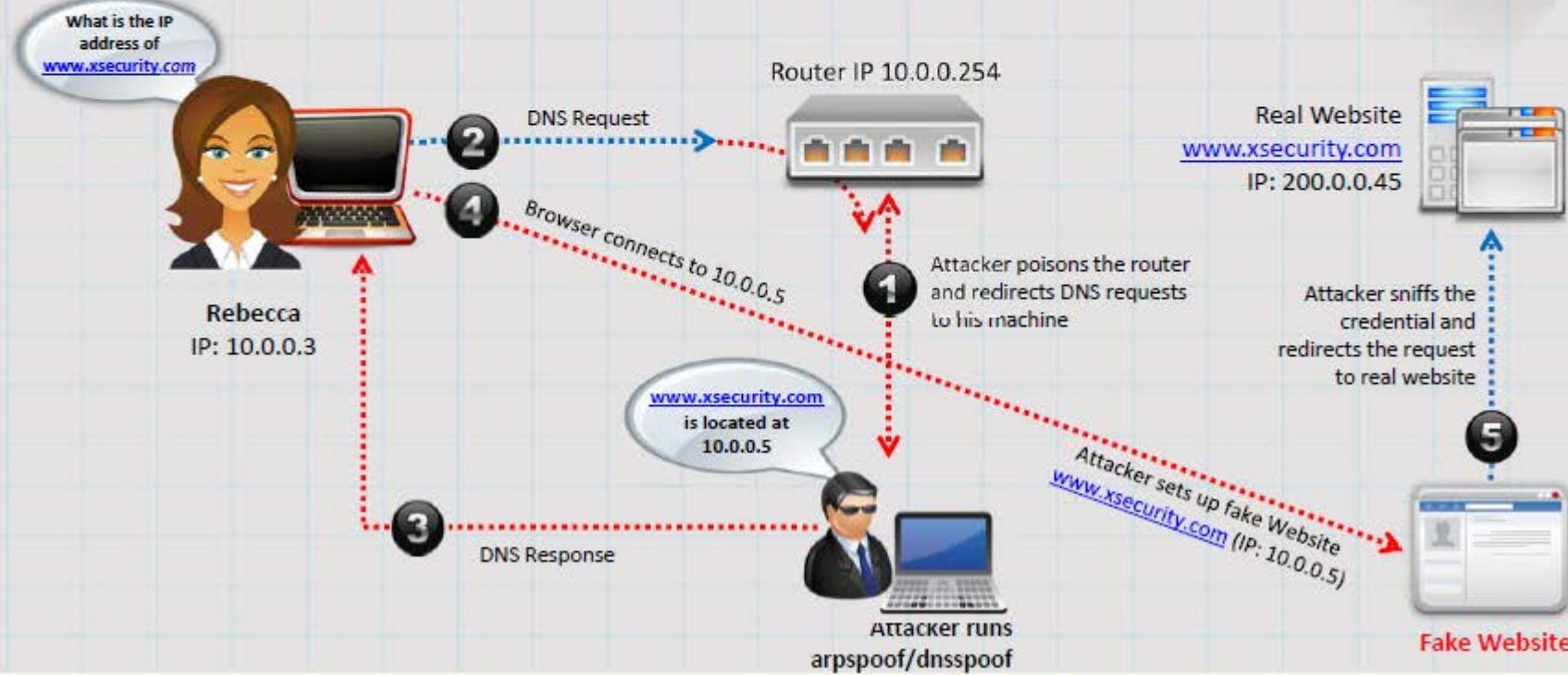
- It allows attacker to replace **IP address entries** for a target site on a given DNS server with IP address of the server he/she controls
- Attacker can create **fake DNS entries** for the server (containing malicious content) with same names as that of the target server



# Intranet DNS Spoofing

CEH  
Certified Ethical Hacker

- 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

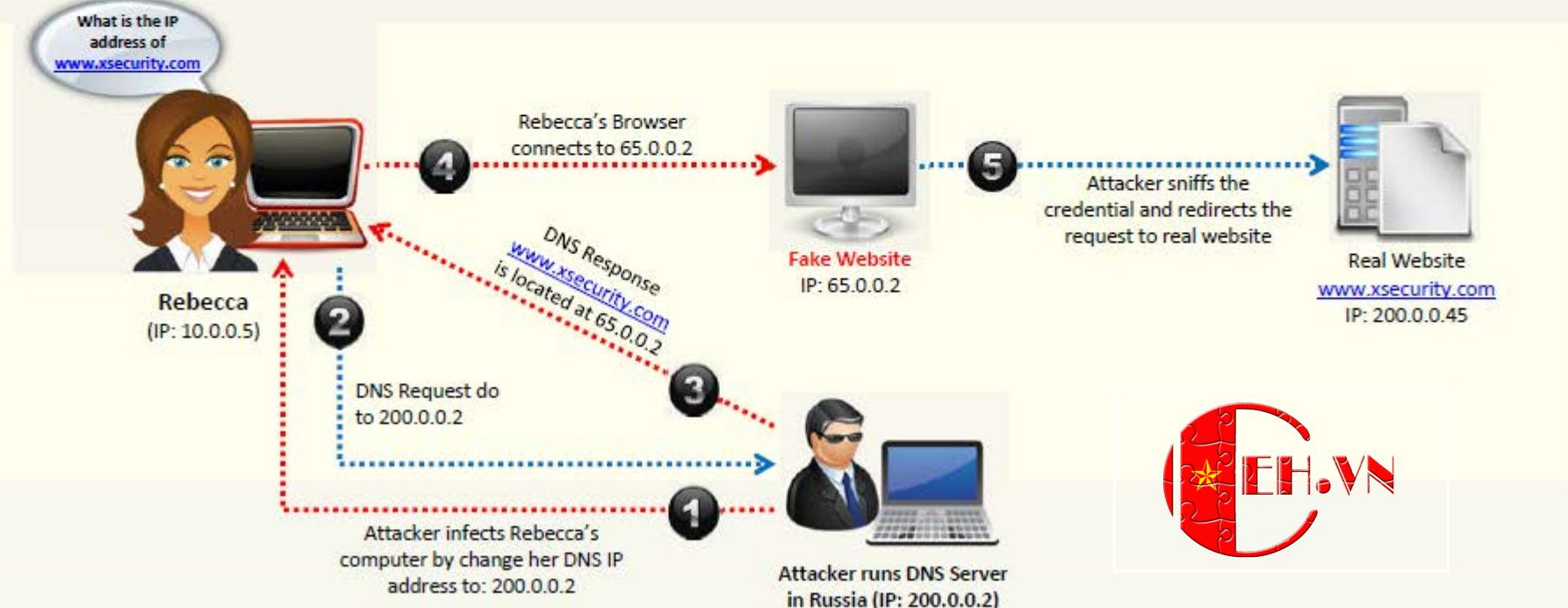


# Internet DNS Spoofing

CEH  
Certified Ethical Hacker



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

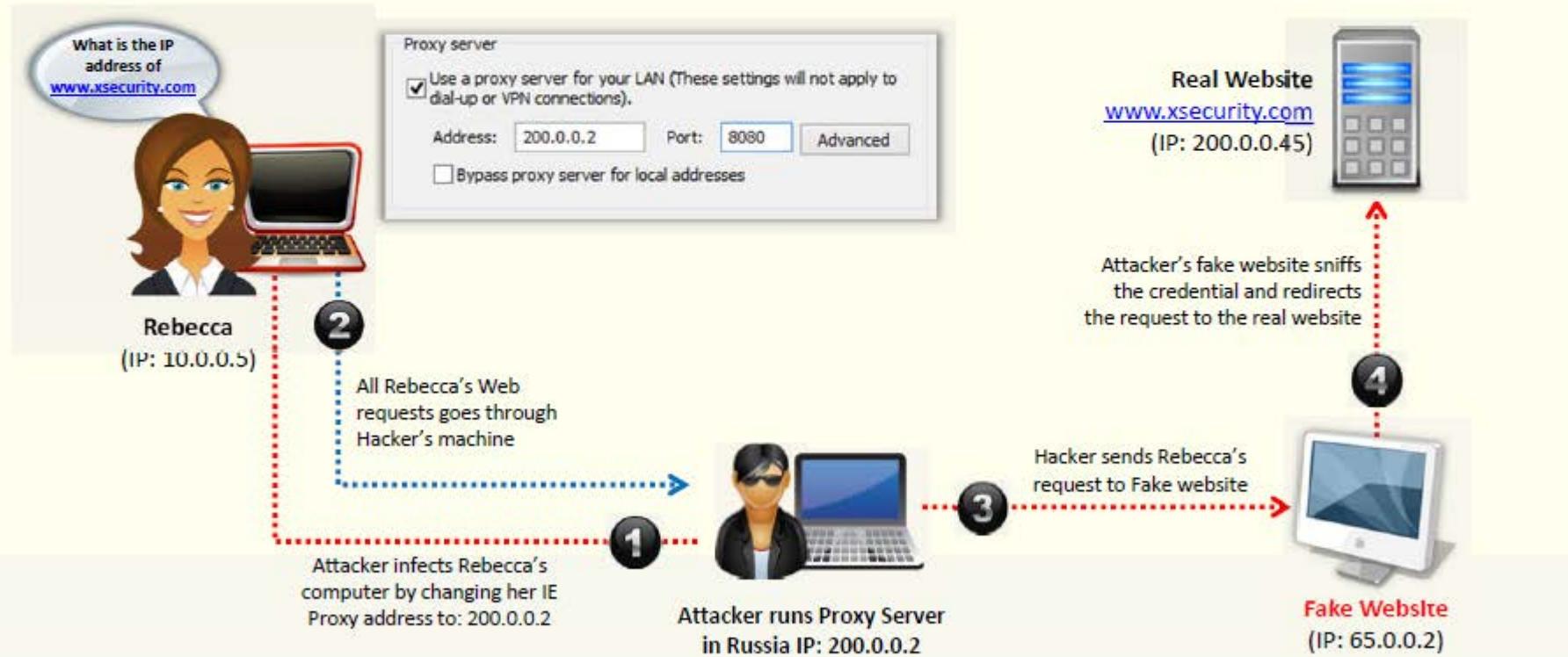


# Proxy Server DNS Poisoning

CEH  
Certified Ethical Hacker



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



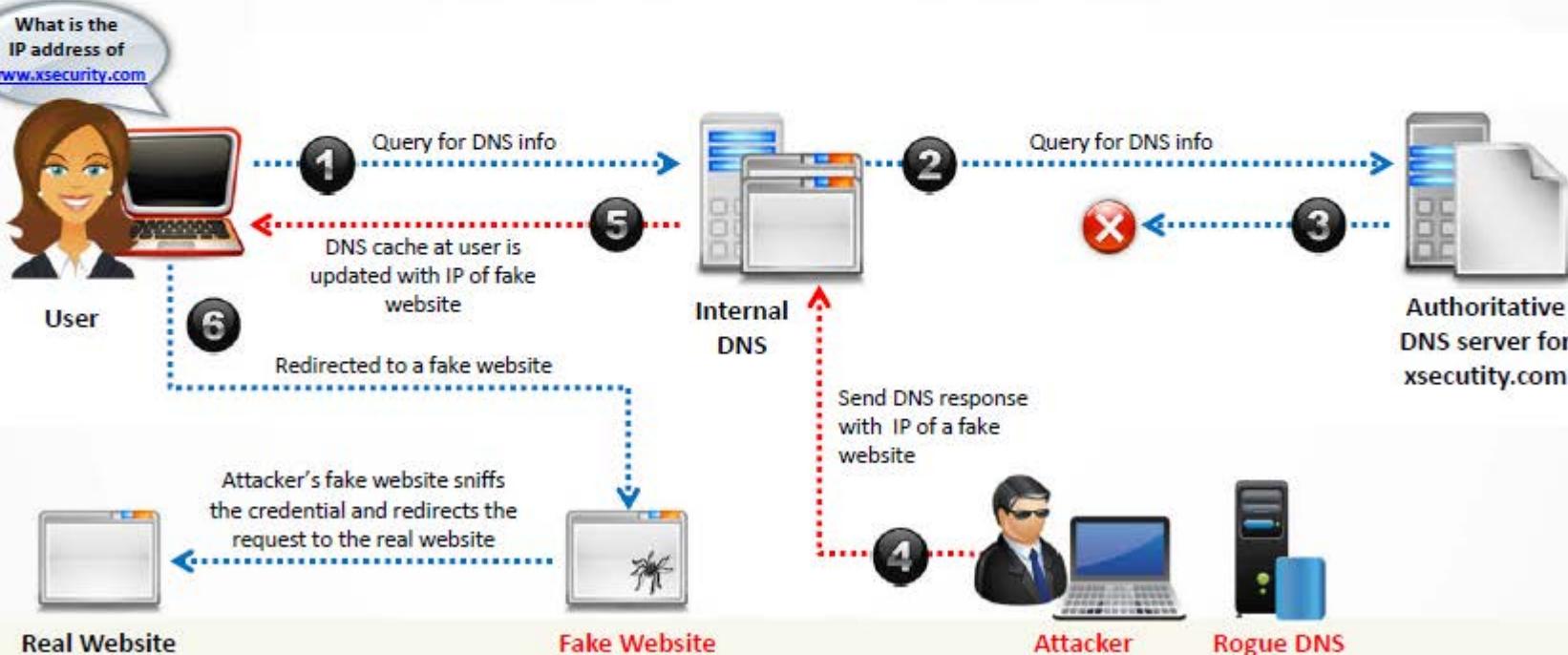
# DNS Cache Poisoning

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



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

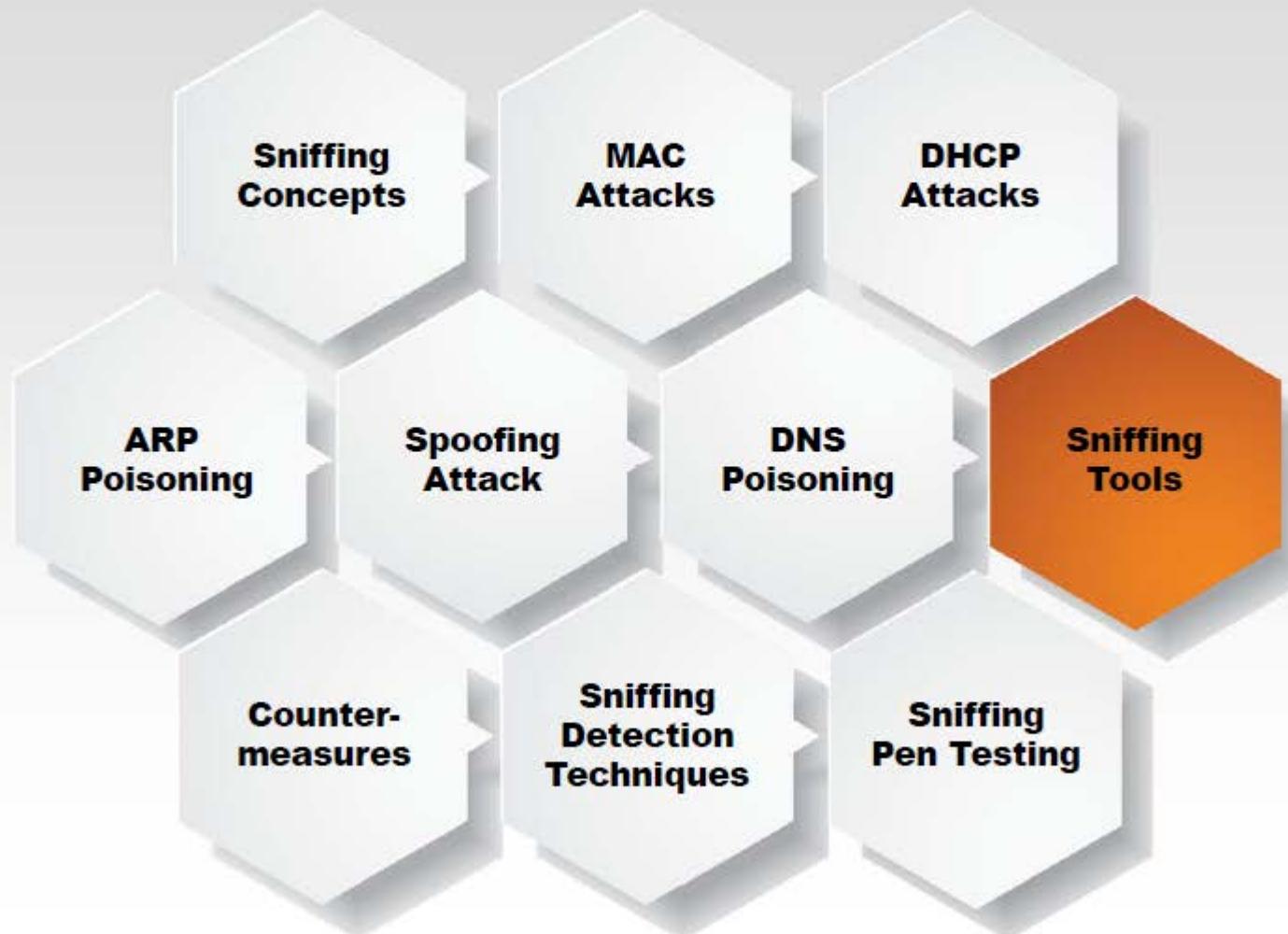


Use DNS Non-Existent Domain (NXDOMAIN) Rate Limiting



Secure your internal machines

# Module Flow



# Sniffing Tool: Wireshark



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

01

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

02

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

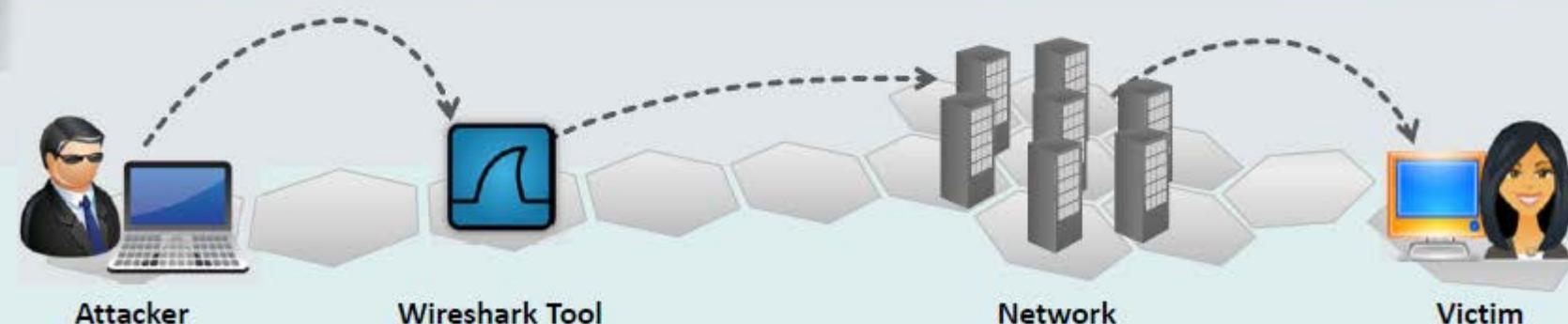
03

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

04

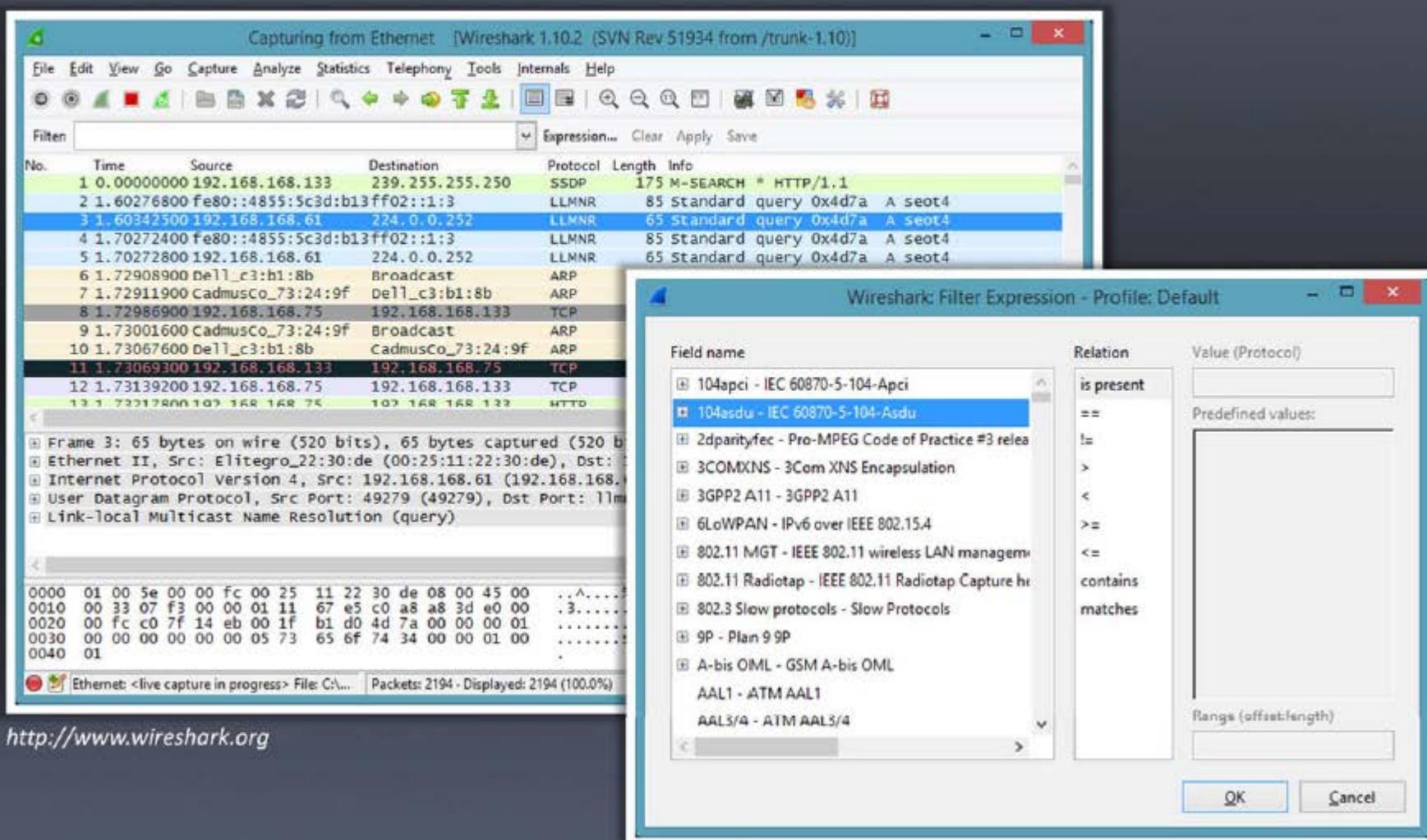
A **set of filters** for customized data display can be refined using a display filter

05



# Sniffing Tool: Wireshark

**(Cont'd)**



# Follow TCP Stream in Wireshark



The screenshot shows two windows from the Wireshark application. On the left is the main packet list window titled "Ethernet (Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1,10))". A search filter "tcp.stream eq 26" is applied. The list contains several captured frames, with frame 440 selected. The details pane below shows the selected frame's information, including source and destination addresses, protocol (HTTP), and payload. The bytes pane at the bottom displays the raw hex and ASCII data of the selected frame. On the right is a "Follow TCP Stream" dialog box. It shows the "Stream Content" pane with the full HTTP POST request and response. The request is for "/loginverify.php" with various headers like Host, Connection, and Content-Length. The response is a 302 Moved Temporarily redirect with headers like Server, Expires, Cache-Control, Pragma, and Location. Below the content panes are several buttons: Find, Save As, Print, ASCII, EBCDIC, Hex Dump, C Arrays, and Row. A red callout box points to the "Row" button with the text "Password revealed in TCP Stream".

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



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 your interest



# Sniffing Tool: SteelCentral Packet Analyzer



The image displays three separate windows of the SteelCentral Packet Analyzer software, each showing different network monitoring and analysis features:

- Top Left Window:** Shows a timeline graph of "Traffic Over Time - Bits" with data points from 12:02:59 to 12:03:28. Below it, two bar charts show "Top Ten MAC Sources" and "Top Ten MAC Destinations".
- Top Right Window:** Shows a "Network Topology" diagram with nodes representing IP addresses like 10.0.0.3, 10.0.0.255, 224.0.2.22, and 224.0.2.232. A callout box provides details for node 10.0.0.3.
- Bottom Window:** Shows four bar charts under "Protocol Distribution": "MAC Overview" (11.48M), "Transport Protocols" (TCP: 12.13M, UDP: 11.48M), "TCP Protocols" (HTTP: 12.13M, HTTPS: 11.48M), and "UDP Protocols" (DNS: 11.48M, TFTP: 11.48M).

<http://www.riverbed.com>

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

# 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

```
Command Prompt
C:\> tcpdump -i eth0
13:13:48.437836 10.20.21.03.router > RIP2-
ROUTERS.MCAST.NET.router: RIPv2
13:13:48.437836 10.20.21.23 > 10.20.21.55: icmp: RIP2-
ROUTERS.MCAST.NET.udp
13:13:54.947195 vmtl.endicott.juggyboy.com.router > RIP2-
ROUTERS.MCAST.NET.rou
13:13:58.313192 :: > ff02::1:ff00:11: icmp6: neighbor sol: who has fe80::
13:13:59.313573 fe80::26f:5a00:100:11 > ipv6-allrouters: icmp6:
router so
13:14:05.179268 :: > ff02::1:ff00:14: icmp6: neighbor sol: who has fe80::
13:14:06.179453 fe80::26f:5a00:100:14 > ipv6-allrouters: icmp6:
router so
13:14:18.473315 10.20.21.55.router > RIP2-
ROUTERS.MCAST.NET.router: RIPv2
13:14:18.473950 10.20.21.23 > 10.20.21.55: icmp: RIP2-
ROUTERS.MCAST.NET.udp
13:14:20.628769 10.20.21.64.filenet-bms >
btvdns01.srv.juggyboy.com.domain: 49
13:14:24.982405 vmtl.endicott.juggyboy.com.router > RIP2-
ROUTERS.MCAST.NET.rou
```

<http://www.tcpdump.org>

## WinDump

Runs on Windows systems

```
C:\> C:\Users\C\Desktop\WinDump\WinDump.exe: listening on \Device\NPF_{6A410B-BB83-4...
15:18:35.004005 IP [REDACTED].137 > 192.168.168.255.137: UDP, length
15:18:35.372362 IP6 [REDACTED]!F2JBQ69755.546 > FF02::1:2.547: dhcp6 soli
15:18:35.669372 IP admin.50347 > FF02::1:3.5355: UDP, length 46
15:18:35.669718 IP admin.50347 > 224.0.0.252.5355: UDP, length 46
15:18:35.854857 IP6 [REDACTED].61220 > FF02::1:3.5355: UDP, length 23
15:18:35.855677 IP [REDACTED].63168 > 224.0.0.252.5355: UDP, length 23
15:18:35.954878 IP6 [REDACTED].61220 > FF02::1:3.5355: UDP, length 23
15:18:35.955385 IP [REDACTED].63168 > 224.0.0.252.5355: UDP, length 23
15:18:36.082704 IP6 admin.50347 > FF02::1:3.5355: UDP, length 46
15:18:36.083064 IP admin.50347 > 224.0.0.252.5355: UDP, length 46
15:18:36.154879 IP [REDACTED].137 > 192.168.168.255.137: UDP, length
15:18:36.459859 IP [REDACTED]-PC.137 > 192.168.168.255.137: UDP, length
15:18:36.494136 IP admin.137 > [REDACTED].137: UDP, length 50
15:18:36.494641 IP admin.64799 > FF02::1:3.5355: UDP, length 45
15:18:36.494898 IP admin.64799 > 224.0.0.252.5355: UDP, length 45
15:18:36.495848 IP [REDACTED].137 > admin.137: UDP, length 175
15:18:36.496685 IP [REDACTED].5355 > admin.64799: UDP, length 94
15:18:36.496743 IP admin > [REDACTED]: ICMP admin udp port 64799 unrec
th 138
15:18:36.497512 IP6 admin.49395 > FF02::1:3.5355: UDP, length 90
15:18:36.497750 IP admin.49395 > 224.0.0.252.5355: UDP, length 90
15:18:36.908466 IP [REDACTED].137 > 192.168.168.255.137: UDP, length
15:18:36.908626 IP6 admin.49395 > FF02::1:3.5355: UDP, length 90
15:18:36.908833 IP admin.49395 > 224.0.0.252.5355: UDP, length 90
15:18:37.218184 IP [REDACTED]-PC.137 > 192.168.168.255.137: UDP, length
15:18:37.252186 IP [REDACTED]
```

<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**



The screenshot shows the OmniPeek Network Analyzer application running. The main window displays a list of captured network packets. The packet list includes columns for ID, Source, Destination, Flags, Size, Relative Time, Protocol, and Summary. The summary column provides detailed information about each packet, such as source and destination ports and specific data bytes. To the left of the main window, there is a sidebar titled 'Dashboards' containing links to various monitoring tools: Network, Voice & Video, Adapters, CoS/packets, Capture, Padlets, Log, Filters, Expert, Hierarchy, Mat, Application, Web, Servers, Clerks, Pages, Requests, Voice & Video, Call, Media, and Visuals. The 'Capture' link is currently selected. At the top of the application window, there is a menu bar with File, Edit, View, Capture, Send, Monitor, Tools, Window, and Help. Below the menu bar, there are several status indicators: 'Packets received: 2,000', 'Packets filtered: 2,000', 'Buffer usage: 2%', 'Filter state: Accept all packets', and a 'Start Capture' button. The bottom of the window shows a status bar with 'idle', 'vethernet (Health) PCIe GBE Family Controller - Virtual Switch', and 'Duration: 0:00:12'. The URL 'http://www.wildpackets.com' is displayed at the very bottom right.

# 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**

The screenshot displays the Network Observer software interface. The main window shows a list of captured network packets with columns for ID, Type, Source, Destination, and Summary. A specific packet is selected, and its details are shown in the center pane, including fields like Ethernet Type, Source MAC, Destination MAC, and Length. Below this, the packet's bytes are displayed in a hex dump format. The bottom of the window features tabs for 'Decode', 'Summary', 'Protocols', etc., and a status bar indicating the URL <http://www.networkinstruments.com>.



# 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

The screenshot shows the Sniff-O-Matic 1.07 Trial Version interface. The main window displays a list of captured network packets. The columns include: Packet, Source, Destination, Size, Proto, Time, Port src, and Port dest. A specific UDP packet (Packet 7) is selected, highlighted in blue. To the right of the list, a detailed pane shows the IP Header and UDP Header fields for the selected packet. Below the list, there is a hex dump of the packet data. At the bottom right, there is a small waveform plot and a URL: <http://www.kwakkelflap.com>.

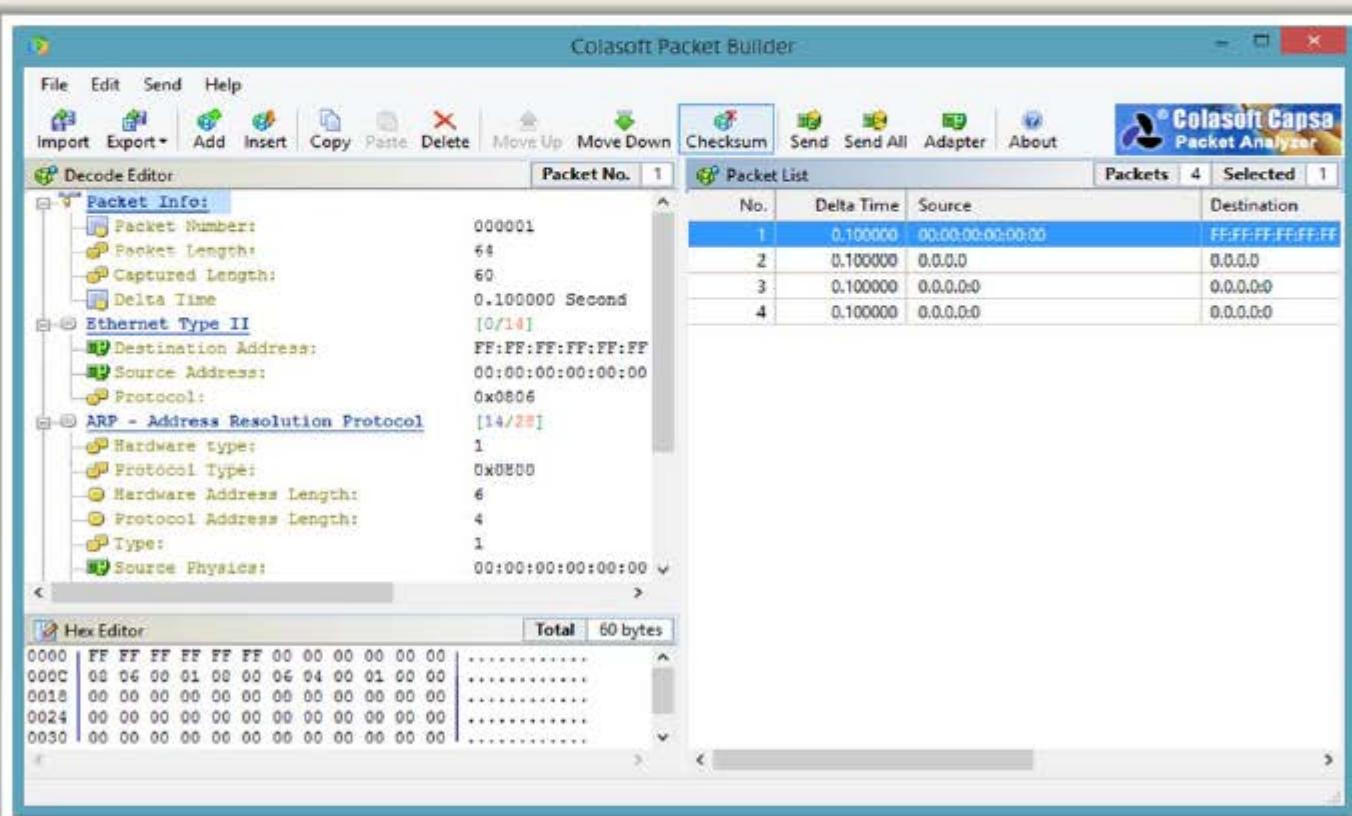
Packet	Source	Destination	Size	Proto	Time	Port src	Port dest
1	192.168.168.61	224.0.0.252	65	UDP	10/24/13 11:06:21	64138	5365
2	192.168.168.37	255.255.255.255	153	UDP	10/24/13 11:06:21	17500	17500
3	192.168.168.37	192.168.168.255	153	UDP	10/24/13 11:06:21	17500	17500
4	192.168.168.61	224.0.0.252	65	UDP	10/24/13 11:06:21	64138	5365
5	192.168.168.61	192.168.168.255	92	UDP	10/24/13 11:06:22	137	137
6	192.168.168.133	239.255.255.250	175	UDP	10/24/13 11:06:22	63263	1900
7	192.168.168.133	239.255.255.250	175	UDP	10/24/13 11:06:22	63263	1900
8	192.168.168.61	192.168.168.255	92	UDP	10/24/13 11:06:22	137	137
9	192.168.168.38	255.255.255.255	138	UDP	10/24/13 11:06:23	7768	7768
10	192.168.168.61	192.168.168.255	92	UDP	10/24/13 11:06:23	137	137
11	192.168.168.11	224.0.0.252	65	UDP	10/24/13 11:06:23	55552	5365
12	192.168.168.11	224.0.0.252	65	UDP	10/24/13 11:06:23	55552	5365
13	192.168.168.11	192.168.168.255	92	UDP	10/24/13 11:06:24	137	137

<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

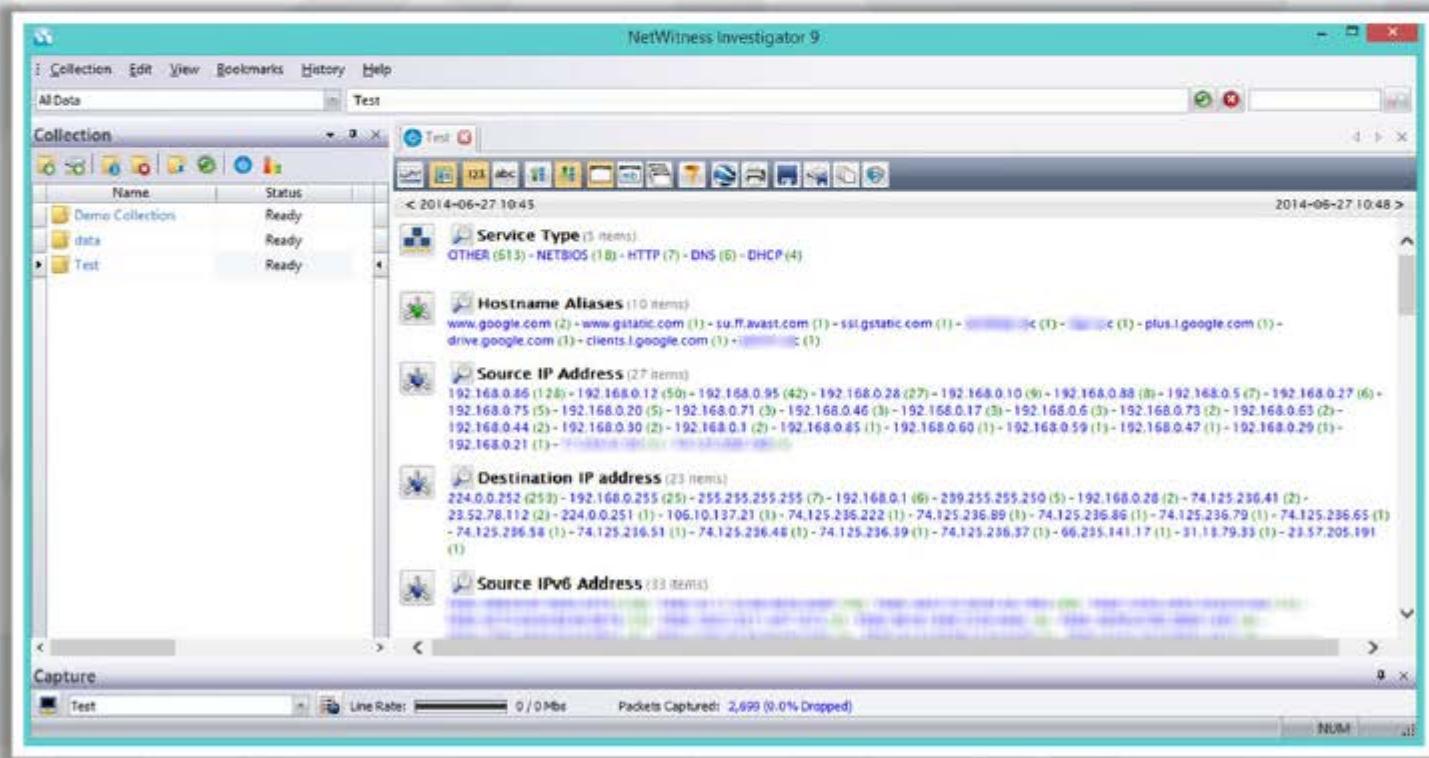


<http://www.colasoft.com>

# **Network Packet Analyzer: RSA NetWitness Investigator**

CEH  
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



**Ace Password Sniffer**

<http://www.effetech.com>



**IPgrab**

<http://ipgrab.sourceforge.net>



**Big-Mother**

<http://www.tupsoft.com>



**EtherDetect Packet Sniffer**

<http://www.etherdetect.com>



**dsniff**

<http://monkey.org>



**EffeTech HTTP Sniffer**

<http://www.effetech.com>



**ntopng**

<http://www.ntop.org>



**Ettercap**

<http://ettercap.sourceforge.net>



**SmartSniff**

<http://www.nirsoft.net>



**EtherApe**

<http://etherape.sourceforge.net>

# Additional Sniffing Tools

(Cont'd)



**Network Probe**

<http://www.objectplanet.com>



**WebSiteSniffer**

<http://www.nirsoft.net>



**ICQ Sniffer**

<http://www.etherboss.com>



**MaaTec Network Analyzer**

<http://www.maatec.com>



**Alchemy Network Monitor**

<http://www.mishelpers.com>



**CommView**

<http://www.tamos.com>



**NetResident**

<http://www.tamos.com>



**Kismet**

<http://www.kismetwireless.net>



**AIM Sniffer**

<http://www.effetech.com>



**Netstumbler**

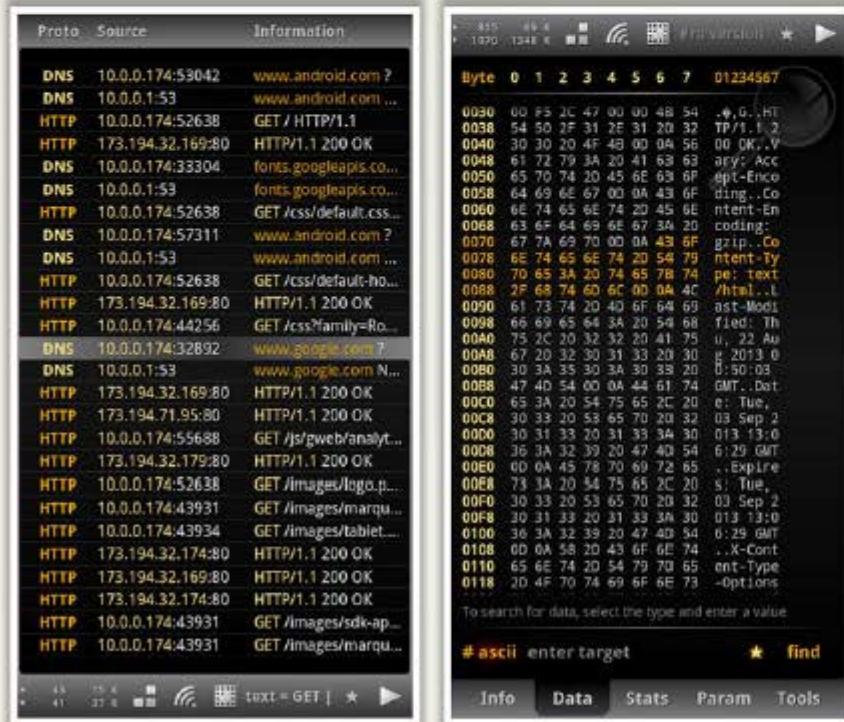
<http://www.netstumbler.com>

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



## Wi.cap. Network Sniffer Pro

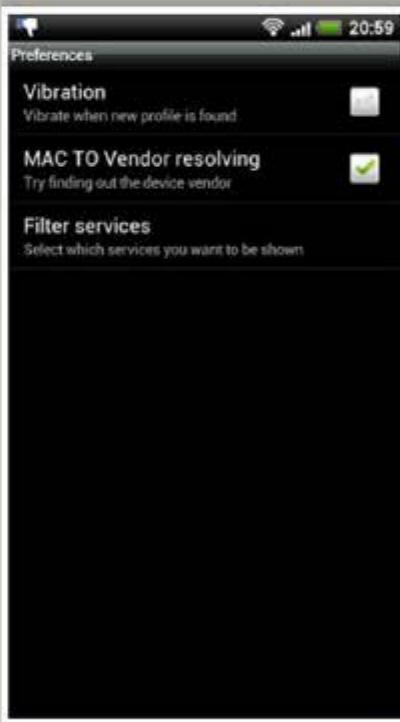
Mobile network packet sniffer for **ROOT ARM droids**



<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/MIME, 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

CEH  
Certified Ethical Hacker



## 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



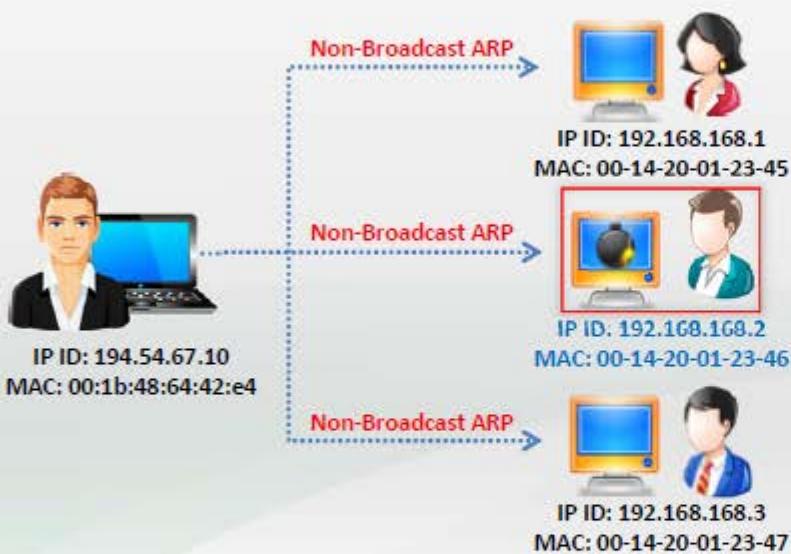
## Non-Promiscuous Mode



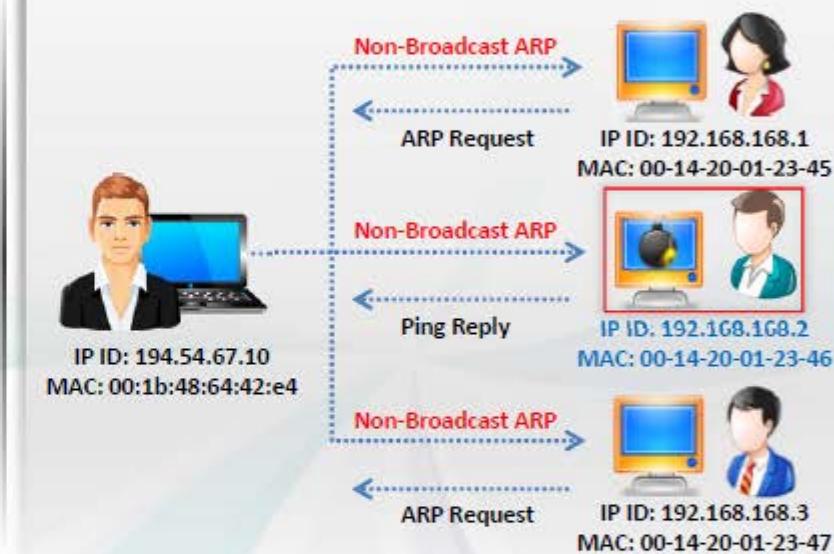
Send a ping request to the suspect machine with its IP address and **incorrect MAC address**. The Ethernet adapter rejects it, as the MAC address does not match, whereas the suspect machine running the **sniffer responds** to it as it does not reject packets with a different MAC address

# Sniffer Detection Technique: ARP Method

CEH  
Certified Ethical Hacker



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

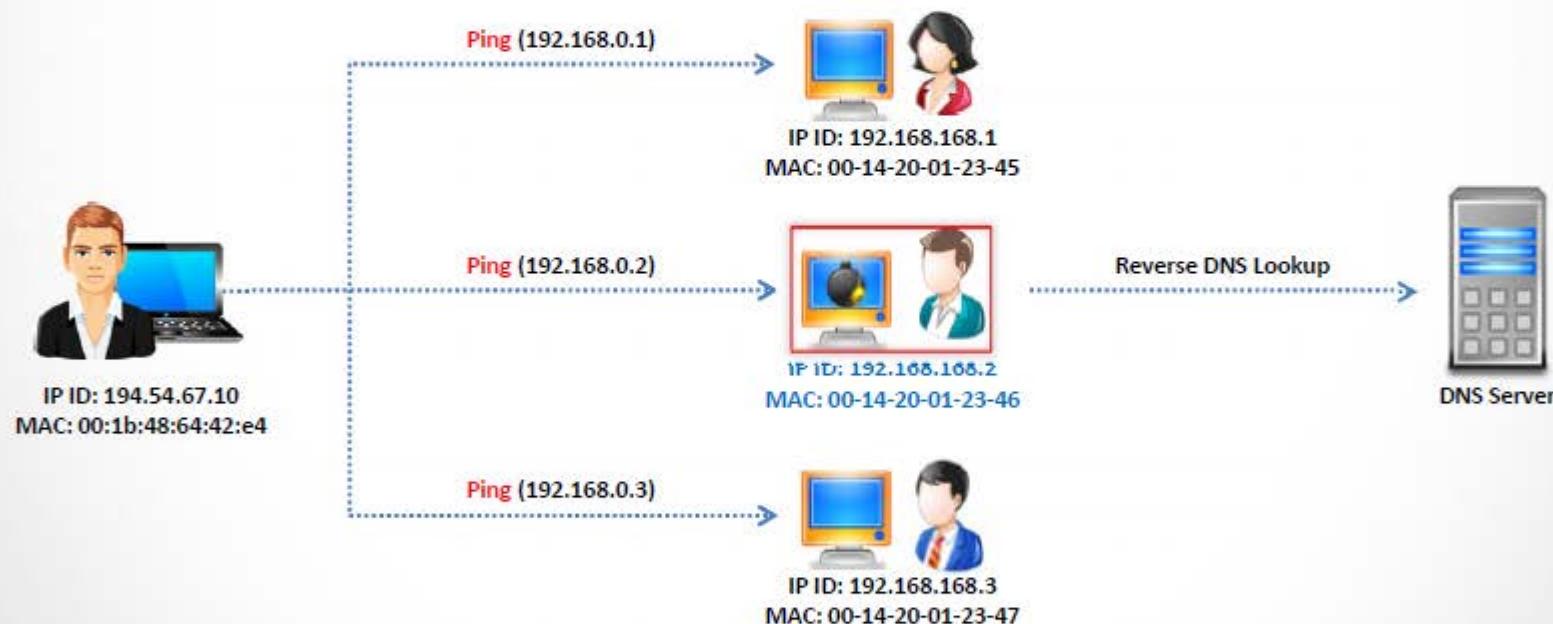


A machine in promiscuous mode **replies to the ping message** as it has correct information about the host sending **ping request** in its cache; rest of the machines will send ARP probe to identify the source of ping request

# 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



The screenshot shows the Promqry UI application window. On the left, under 'Systems To Query', there is a table with one row selected, showing 'Start IP address' as 192.168.168.133 and 'Query Status' as 'Active: True'. A blue callout box contains the text: 'PromqryUI is a security tool from Microsoft that can be used to detect network interfaces that are running in promiscuous mode'. On the right, under 'Query Results', the application displays five network interface entries, each with 'Active: True', 'InstanceName', and 'NEGATIVE: Promiscuous mode currently NOT enabled'. At the bottom of the window are 'Add', 'Delete', and 'Start Query' buttons.

Start IP address	End IP address	Query Status
192.168.168.133		Active: True

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

Query Results

Querying local system...

Active: True  
InstanceName: Intel(R) PRO/1000 MT Desktop Adapter  
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True  
InstanceName: WAN Miniport (IP)  
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True  
InstanceName: WAN Miniport (IPv6)  
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True  
InstanceName: WAN Miniport (Network Monitor)  
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True  
InstanceName:

Add Delete Start Query

<http://www.microsoft.com>

# 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]`



```
root@root:~# nmap --script=sniffer-detect 10.0.0.2
Starting Nmap 6.46 ( http://nmap.org ) at 2015-04-07 09:31 EDT
Nmap scan report for 10.0.0.2
Host is up (0.00038s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
1027/tcp  open  IIS
1028/tcp  open  unknown
1030/tcp  open  iadl
1034/tcp  open  zincite-a
1051/tcp  open  optima-vnet
1053/tcp  open  remote-as
1070/tcp  open  gmrudateserv
1433/tcp  open  ms-sql-s
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  oklogin
2107/tcp  open  msmq-mgmt
2179/tcp  open  vncdcp
2383/tcp  open  ms-clap4
3309/tcp  open  ms-wbt-server
MAC Address: D4:BE:D9:C3:C3:CC (Dell)

Host script results:
| sniffer-detect: Likely in promiscuous mode (tests: "11111111")

Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
root@root:~#
```



# 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

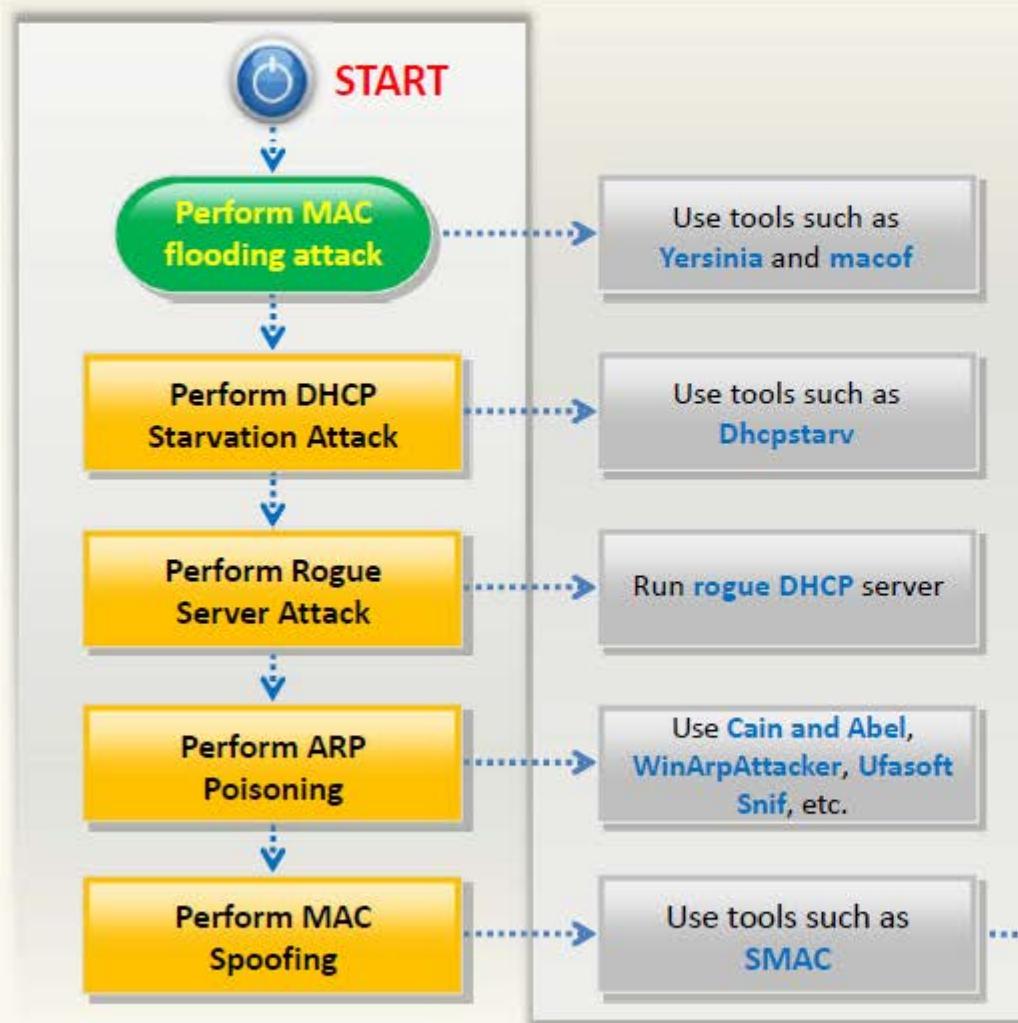


**Discover the presence of unauthorized networking devices**



# Sniffing Pen Testing

(Cont'd)

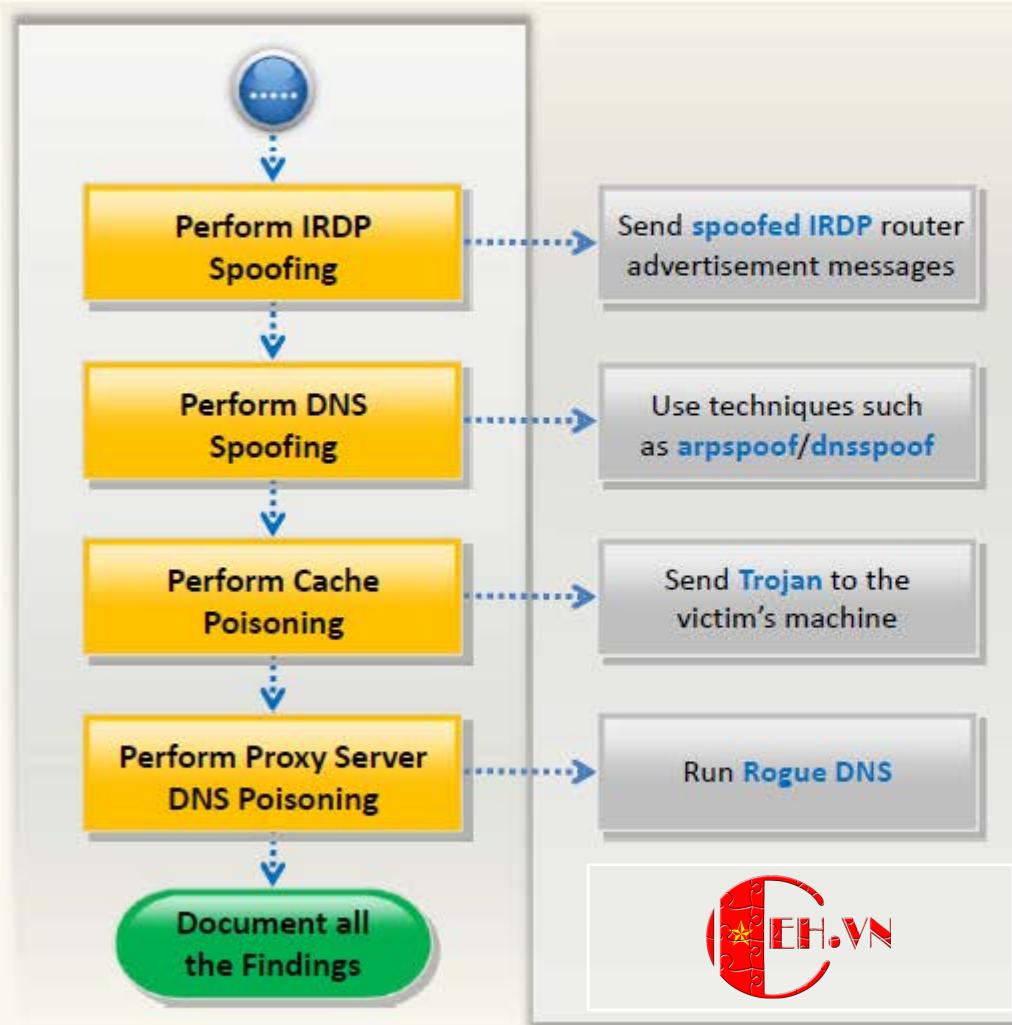


- Perform MAC flooding attack using tools such as **Yersinia** and **macof**
- Perform DHCP starvation attack using tools such as **Dhcpstarv** and **Yersinia**
- Perform rogue server attack by running **rogue DHCP server** in the network and responding to DHCP requests with **bogus IP addresses**
- 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