Sniffing

Module 08

Ethical Hacking and Countermeasures v8

Module 08: Sniffing

Exam 312-50

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NEWS

Public Wi-Fi Hotspots Pose Real Threat to Enterprises, Survey Finds

Source: http://searchsecurity.techtarget.com

Employees are accessing sensitive company information via unprotected public Wi-Fi hotspots, according to a new survey that found public Wi-Fi usage rose significantly over the last year.

The study, conducted by the Identity Theft Resource Center (ITRC), surveyed 377 people and found more than half (57%) used public Wi-Fi hotspots to access confidential work-related information. The online survey was commissioned by Sherman, a Conn.-based Private Communications Corporation seller of virtual private network (VPN) software.

Public Wi-Fi usage has gone up 240% in the past year, but 44% of respondents weren't aware of a way to protect their information when using a hotspot. In addition, 60% of those surveyed indicated they were either concerned or very concerned about their security when using a public hotspot. Experts have pointed out that the rapid increase in public hotspots is associated with the growing use of smartphones and tablet devices.

Security researchers have demonstrated how easy it is for an attacker to target users of open Wi-Fi hotspots, sniffing unencrypted traffic to view sensitive data, such as email and social

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

networks. A Mozilla Firefox plugin called **Firesheep** made the attacks more widely available, automating the process of monitoring and analyzing traffic.

A **VPN encrypts** information traveling between a user's computer and the provider's remote network. Large organizations often provide a VPN to protect employees, typically maintaining a VPN appliance to handle a high load of traffic, but security expert **Lisa Phifer**, president of Core Competence Inc. in Chester Springs, Pa., said they are useful for companies of all sizes.

Companies have tried other solutions with little success, Phifer said. One example is when an organization prohibits employees from adding new network names to corporate laptops. This technique does not help with employee-owned devices, however, and it is unpopular with employees.

To make sure their employees use the **VPN**, companies can stop employees from using business services on their personal laptops or mobile devices, unless they log on to a VPN.

"That doesn't stop users from doing other risky things [when not logged in]," Phifer said.

Kent Lawson, CEO and founder of Private Communications Corporation, said security experts have been warning about the growing concern of open and often poorly protected Wi-Fi threats.

"People are aware in their tummies that when they use hotspots they're doing something risky," Lawson said. "But they don't know there's a solution."

Lawson said individuals and small businesses can also use a VPN to ensure secure browsing. Critics of personal VPNs say they could slow machines down. Lawson said while the VPN is encrypting and then decrypting information as it travels between a machine and the network, the process runs in the background and does not have a noticeable affect for the ordinary worker using Wi-Fi to surf the web and check email.

"I would not recommend using a VPN if you're about to download a two-hour HD movie," he said.

Phifer said a VPN can use up battery life faster on smaller devices, but performance of applications on the device is not impacted.

Another complaint with VPNs is that the process of logging on is too time-consuming, Phifer said. In many cases, users have to log on to a hotspot and log on to their VPN before they can access the Internet.

"A great deal of it is because of the expediency," Phifer said of the tendency for users to ignore the fact that they are not protected when using public Wi-Fi. Additionally, Phifer said people do not believe five minutes on a public network will expose them to any harm.

Using **HTTPS encryption** for protection

Another option for securing information when logged on to public Wi-Fi is to use HTTPS encryption when browsing. Lawson, however, believes using HTTPS does not provide enough security.

"It's spotty. Some sites are secured and some aren't. Some only secure during login," he said.

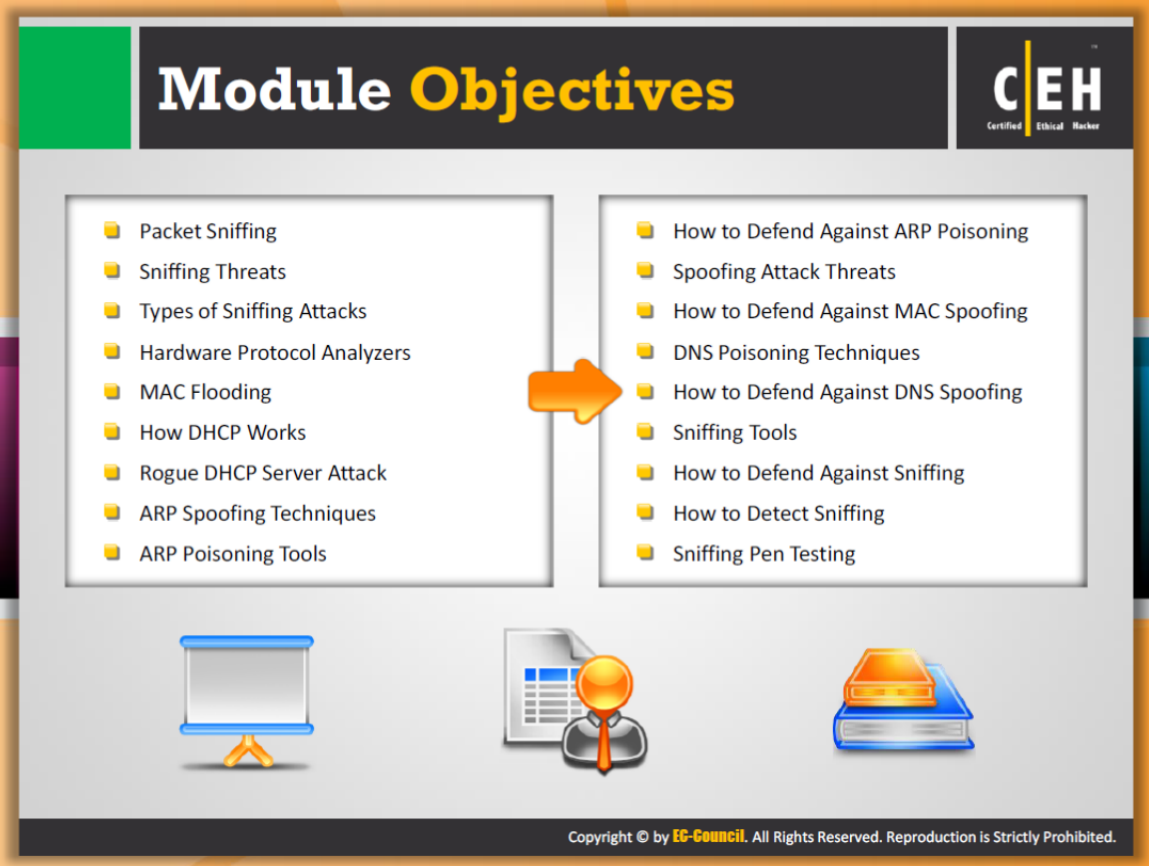
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security researchers have also developed an attack tool, the Browser Exploit Against **SSL/TLS**, that breaks the encryption.

VPN protection is limited

A VPN only addresses the lack of encryption when using public Wi-Fi, so users need to take further steps to ensure a secure browsing experience, Phifer said. In addition to a VPN, a firewall is important because it protects against others on the network viewing a user's shared files. Users should also be aware of an "evil twin," a fake access point with the same network name of a real access point. While there is not a clean fix for an evil twin, Phifer said users should be aware of where they are connecting.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



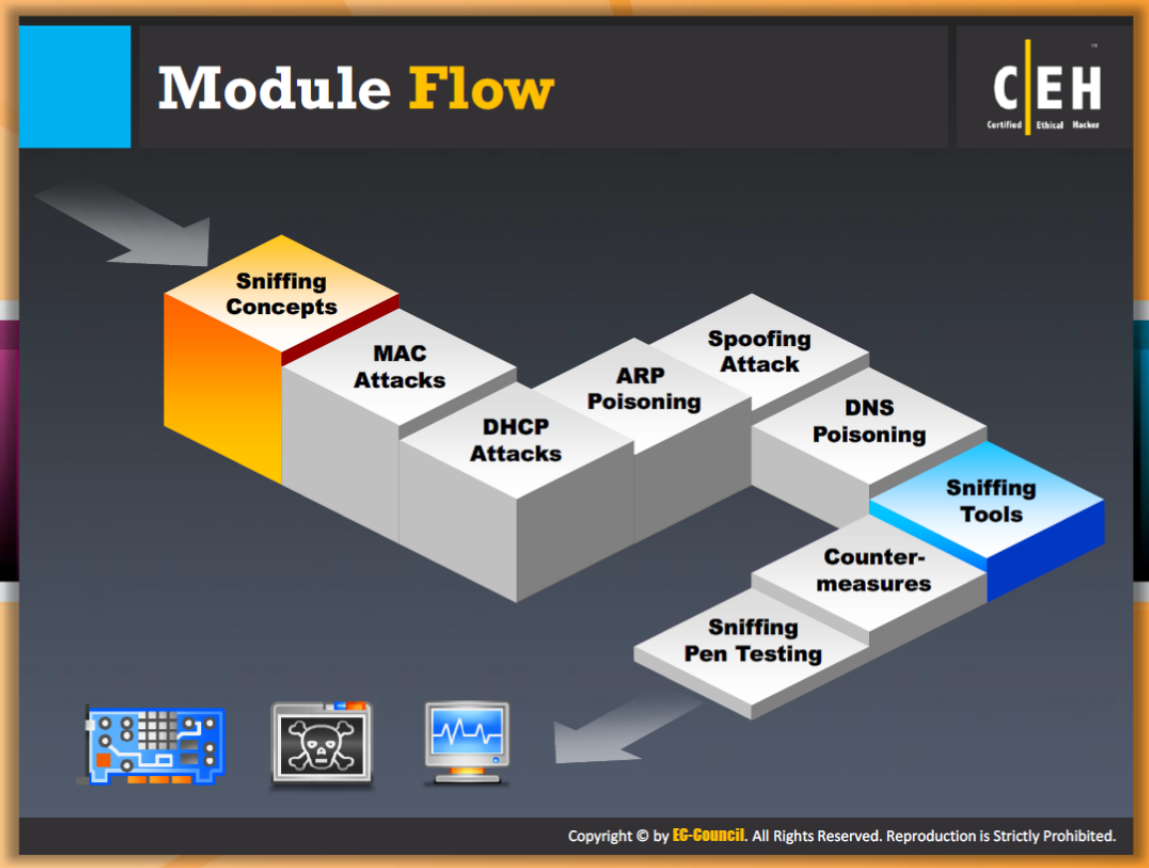
Module Objectives

This module will explain the fundamental concepts of sniffing and their use in hacking activities. The module also highlights how important it is for a network administrator to be knowledgeable about sniffers. In addition, various tools and techniques used in securing a network from anomalous traffic are explained.

The topics discussed in this module are:

- Packet Sniffing
- Sniffing Threats
- Types of Sniffing Attacks
- Hardware Protocol Analyzers
- MAC Flooding
- How DHCP Works
- Rogue DHCP Server Attacks
- ARP Spoofing Techniques
- ARP Poisoning Tools
- How to Defend Against ARP Poisoning
- Spoofing Attack Threats
- How to Defend Against MAC Spoofing
- DNS Poisoning Techniques
- How to Defend Against DNS Spoofing
- Sniffing Tools
- How to Defend Against Sniffing
- How to Detect Sniffing
- Sniffing Pen Testing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

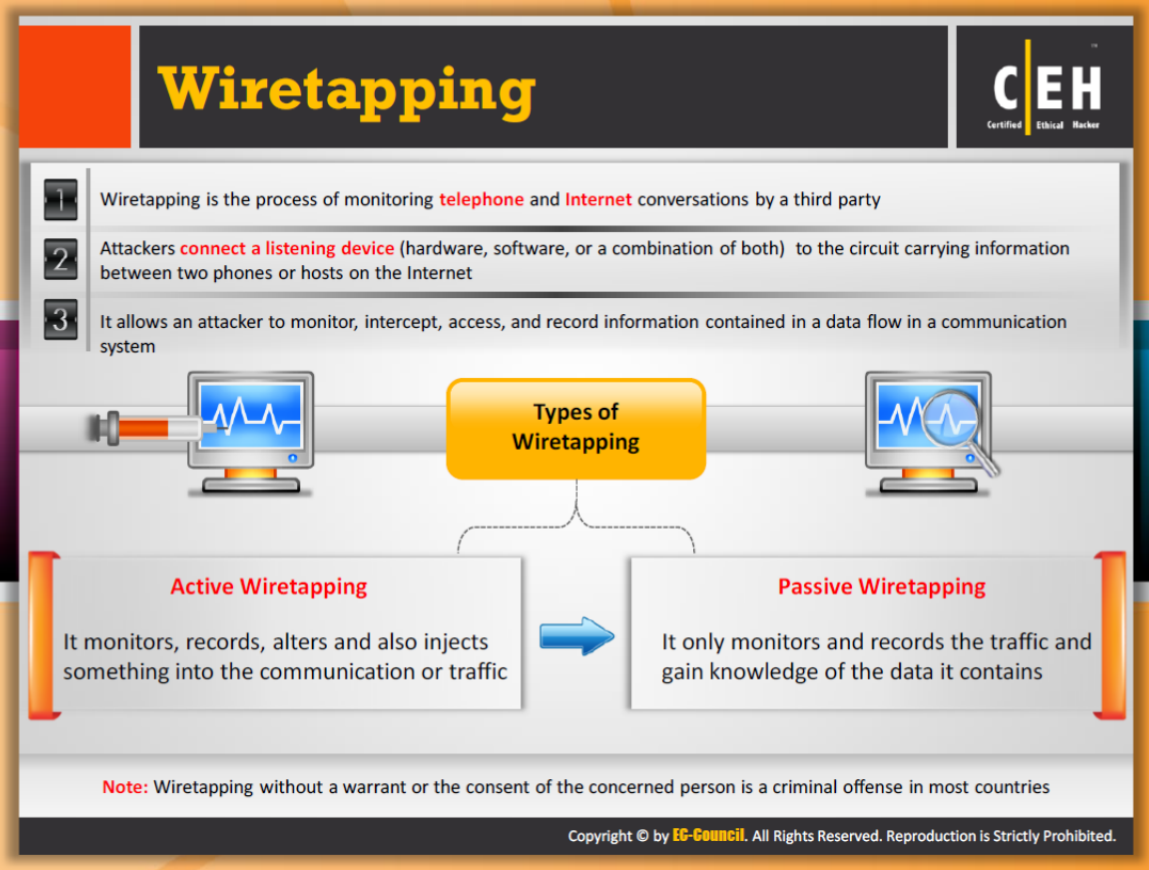


Module Flow

To begin the sniffing module, let's start by going over sniffing concepts.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Wiretapping

Wiretapping or telephone tapping is a method of **monitoring telephone** or **Internet conversations** by any third party with covert intentions. In order to perform wiretapping, first you should select a target person or host on the network to wiretap and then you should connect a listening device (hardware, software, or a combination of both) to the circuit carrying information between two phones or hosts on the Internet. Typically, the conversation is tapped with the help of a small amount of **electrical signal generated** from the telephone wires. This allows you to monitor, intercept, access, and record information contained in a data flow in a communication system.

Wiretapping Methods

Wiretapping can be performed in the following ways:

- The official tapping of telephone lines
- The unofficial tapping of telephone lines
- Recording the conversation
- Direct line wire tap
- Radio wiretap

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Wiretapping

There are two types of wiretapping using which you can monitor, record, and may even alter the data flow in the communication system.

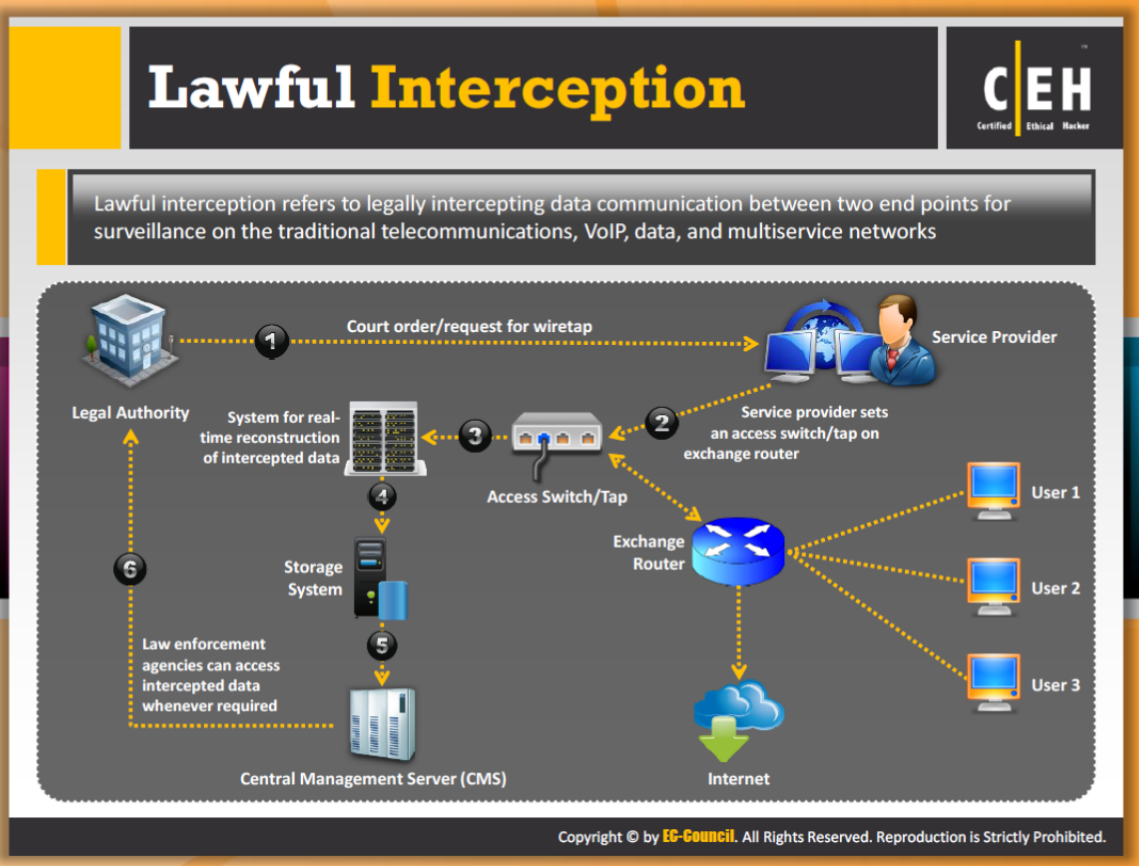
- **Active Wiretapping**

  In hacking terminology, active wiretapping is also known as a **man-in-the-middle attack**. This allows you to monitor and record the traffic or data flow in the communication system. In addition to this, it also allows you to alter or inject data into the communication or traffic

- **Passive Wiretapping**

  In hacking terminology, passive wiretapping is also called **snooping or eavesdropping**. This allows you to monitor and record traffic. By observing the recorded traffic flow, you can either snoop for a password or gain knowledge of the data it contains.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Lawful Interception

Lawful interception (LI) is a form of obtaining data from the communication network by lawful authority for analysis or evidence. These kinds of activities are mostly useful in activities like infrastructure management and protection, as well as **cyber-security-related issues**. Here, access to private network data is legally sanctioned by the network operator or service provider where private communications like telephone calls and email messages are monitored. Usually these kinds of operations are performed by the **law enforcement agencies (LEAs)**.

This type of interception is needed only to keep an eye on the messages being exchanged among the suspicious channels operating illegally for various causes.

E.g.: Terrorist activities all over the world have become a major threat so this type of lawful interception will prove more and more beneficial for us to keep an eye on these activities.

Countries around the world are making strides to standardize this procedure of interception. One of the methods that has been followed for a long time is wiretapping.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

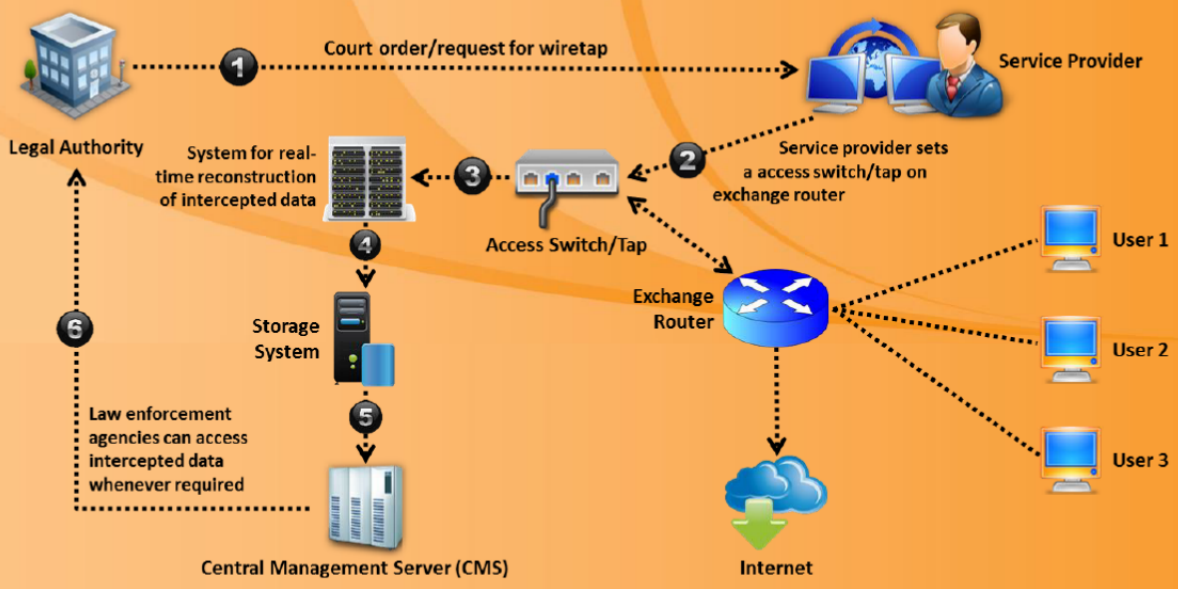
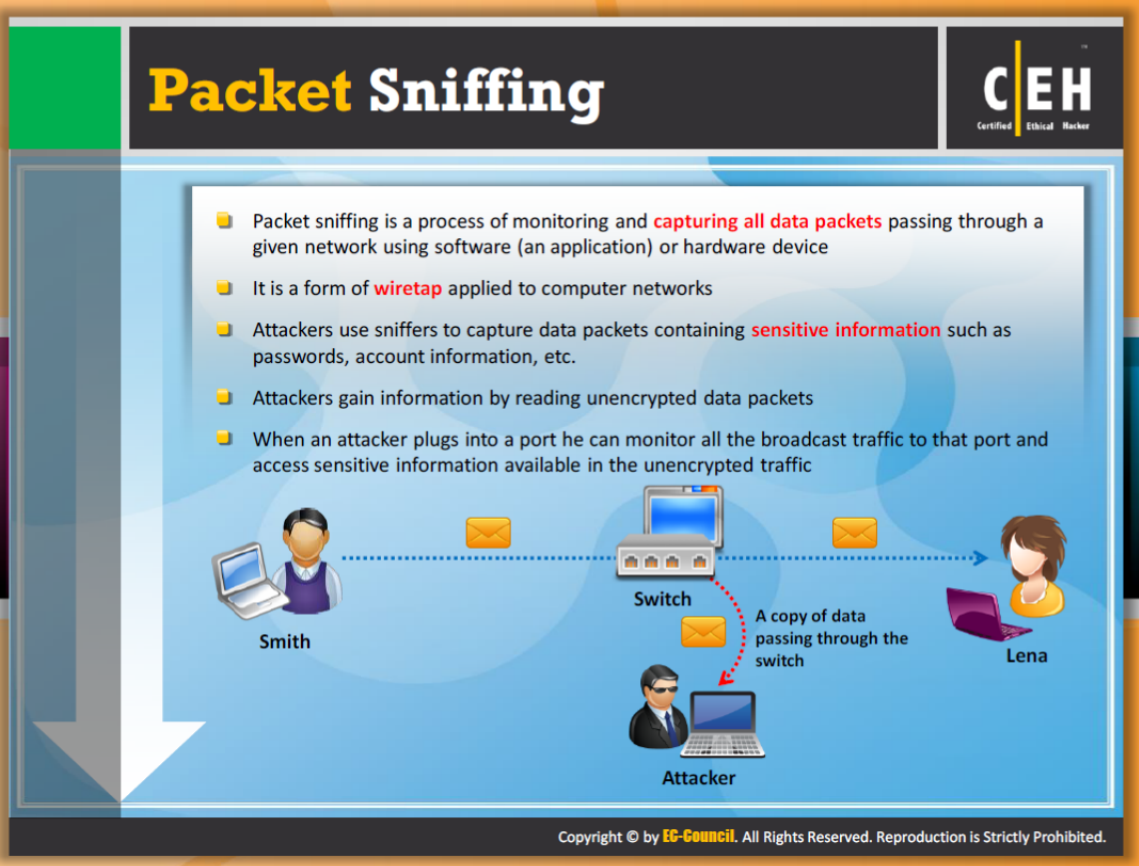


FIGURE 8.1: Telco/ISP lawful solution

The diagram shows the Telco/ISP lawful solution provided by **Decision Computer Group**. This solution consists of one tap/access and multiple systems for reconstruction of intercepted data. The tap/access switch collects traffic from the Internet service provider network and sorts the traffic by IP domain and serves to the **E-Detective (ED)** systems that decode and reconstruct the intercepted traffic into its original format. This is achieved with the help of supporting protocols such as POP3, IMAP, SMTP, P2P and FTP, Telnet, etc. All the ED systems are managed by the CMS (Centralized Management Server).

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Packet Sniffing

Like phone networks, **wiretapping** can also be applied to **computer networks**. Wiretapping in computer networks can be accomplished through packet sniffing. Packet sniffing is a process of monitoring and capturing all data packets passing through a given network using **software** (application) or **hardware device**. This is possible because the traffic on a segment passes by all hosts associated with that segment. Sniffing programs turn off the filter employed by Ethernet cards to avoid the host machine from seeing other stations' traffic. Thus, sniffing programs can see everyone's traffic.

Though most of the networks today are employing "**switch**" technology, packet sniffing is still useful. This is because installing remote sniffing programs on network components with heavy traffic flows such as servers and routers is becoming easy. It allows you to observe and access the entire network traffic from one point. Using packet sniffers, you can capture data packets containing sensitive information such as passwords, account information, etc. Therefore, it allows you to read passwords in clear-text, the actual emails, credit card numbers, financial transactions, etc. It also allows you to sniff SMTP, POP, IMAP traffic, POP, IMAP, HTTP Basic, Telnet authentication, SQL databse, SMB, NFS, FTP traffic. You can gain a lot of information by reading captured data packets and then break into the network. You can carry out even more effective attacks with the help of this technique combined with **active transmission**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following is the diagrammatic representation of how the attacker sniffs the data packets between two users:

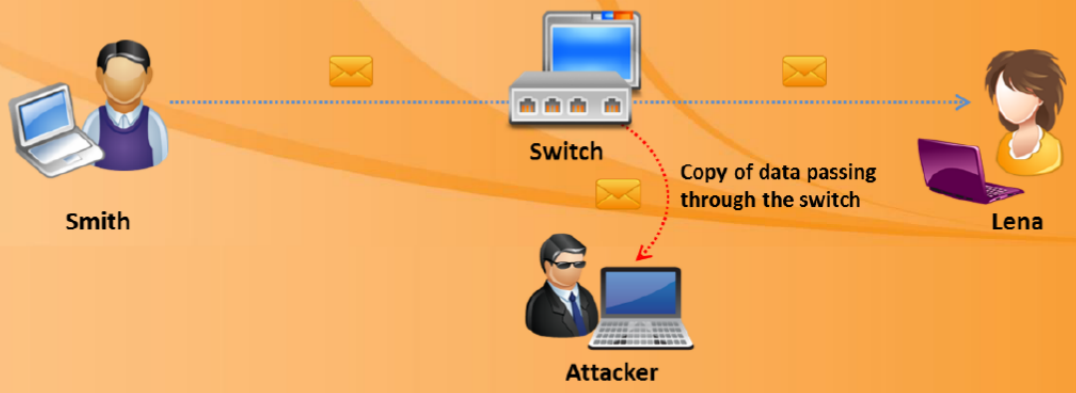
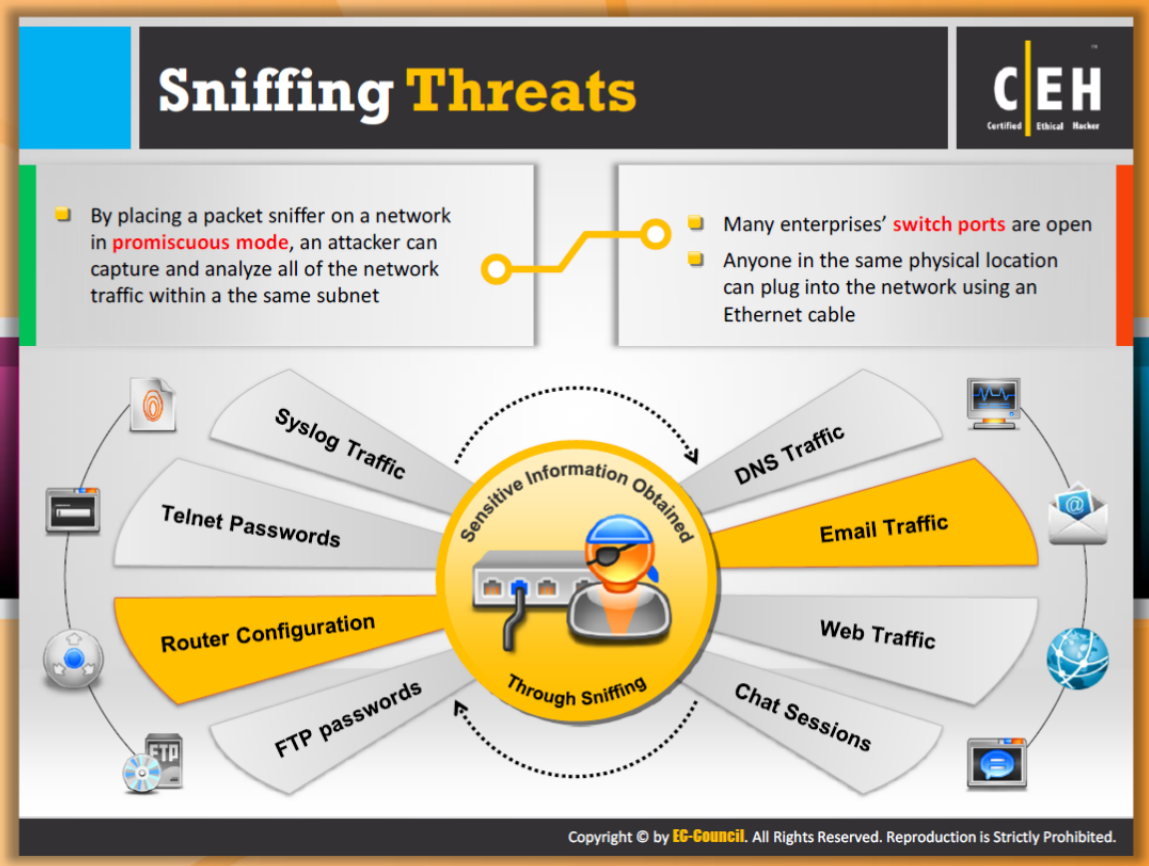


FIGURE 8.2: Packet Sniffing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Threats

Source: http://www.webopedia.com

A sniffer is a **program** and/or device that **monitors data traveling** over a network. Sniffers can be used for legitimate activities, e.g., network management, as well as for illegitimate activities, e.g., stealing information found on a network. Some of the simplest packages use a command-line interface and dump captured data onto the screen, while sophisticated ones use GUI and graph traffic statistics; they can also **track multiple sessions** and offer several configuration options.

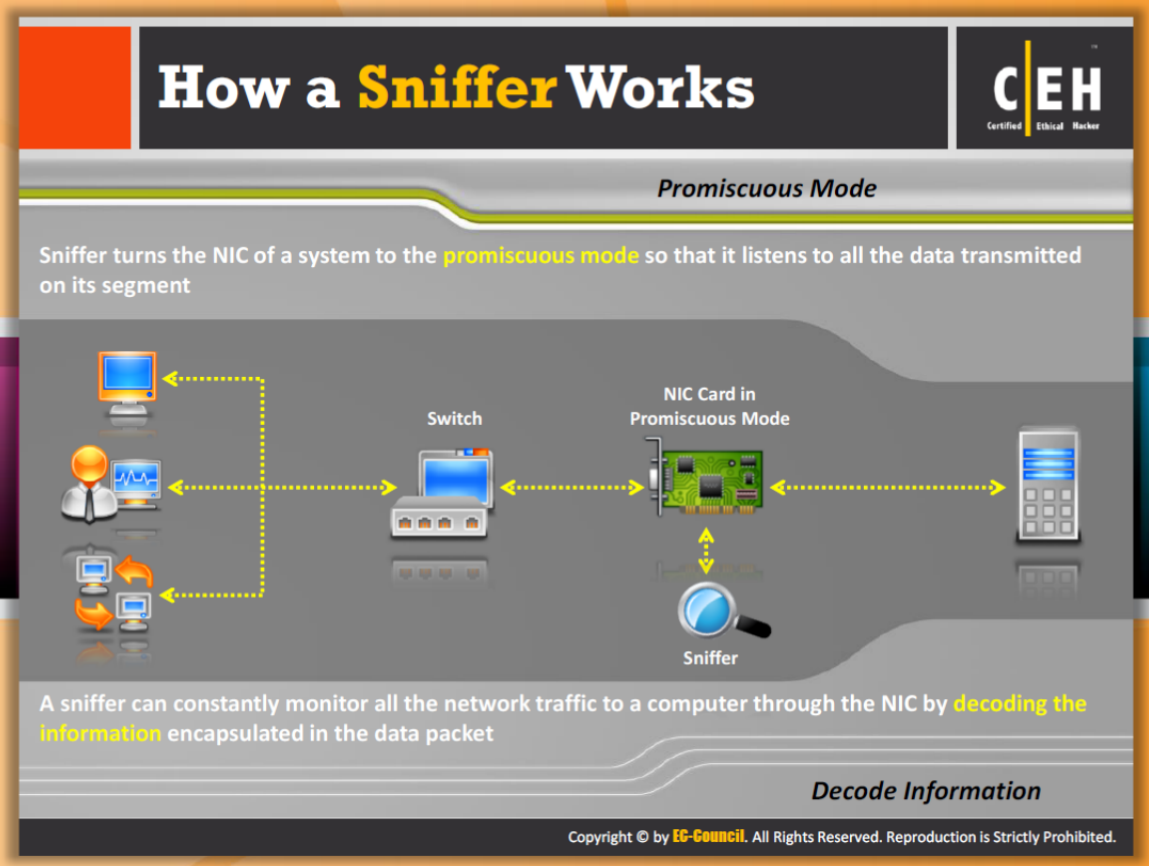
A **packet sniffer** can only capture packet information within a given subnet. Usually any laptop can plug into the network and gain access to the network. Many enterprises' switch ports are open. By placing a packet sniffer on a network in promiscuous mode, you can capture and analyze all of the network traffic. You can steal the following sensitive information by sniffing the network:

- Email traffic
- Web traffic
- Chat sessions
- FTP passwords

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Router configuration
- DNS traffic
- Syslog traffic
- Telnet passwords

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How a Sniffer Works

The most common way of networking computers is through an **Ethernet**. A computer connected to the LAN has two addresses. One is the MAC address that uniquely identifies each node in a network and is stored on the network card itself. The MAC address is used by the Ethernet protocol while building "frames" to transfer data to and from a system. The other is the IP address. This address is used by applications. The Data Link Layer uses an Ethernet header with the MAC address of the destination machine rather than the IP address. The Network Layer is responsible for mapping IP network addresses to the MAC address as required by the Data Link Protocol. It initially looks for the MAC address of the destination machine in a table, usually called the ARP cache. If no entry is found for the IP address, an ARP broadcast of a request packet goes out to all machines on the local sub-network. The machine with that particular address responds to the source machine with its MAC address. This MAC address then gets added to the source machine's ARP cache. The source machine, in all its communications with the destination machine, then uses this MAC address.

There are two basic types of Ethernet environments, and sniffers work in a little different manner in both these environments. The two types of Ethernet environments are:

Shared Ethernet

In a shared Ethernet environment, all hosts are connected to the **same bus** and

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

compete amongst each other for bandwidth. In this environment, all the other machines receive packets meant for one machine. Thus, when machine 1 wants to talk to machine 2, it sends a packet out on the network with the destination **MAC address** of machine 2 along with its own source MAC address. The other machines in the shared Ethernet (machine 3 and machine 4) compare the frame's destination MAC address with their own. If they do not match, the frame is discarded. However, a machine running a sniffer ignores this rule and accepts all frames. Sniffing in a shared Ethernet environment is totally passive and hence difficult to detect.

Switched Ethernet

An Ethernet environment in which the **hosts are connected** to a switch instead of a hub is called a switched Ethernet. The switch maintains a **table** keeping track of each computer's MAC address, and the physical port on which that MAC address is connected, and delivers packets destined for a particular machine. The switch is a device that sends packets to the destined computer only and does not **broadcast** it to all the computers on the network. This results in better utilization of the available bandwidth and improved security. Hence, the process of putting the machine **NIC** into promiscuous mode to gather packets does not work. As a result, many people think that switched networks are totally secure and immune to sniffing. However, this is not true.

Though the switch is more secure than a hub, sniffing the network is possible using the methods as follows:

- **ARP Spoofing**

  ARP is stateless. The machine can send an **ARP** reply even if one has not been asked for, and such a reply will be accepted. When a machine wants to sniff the traffic originating from another system, it can ARP spoof the **gateway** of the network. The ARP cache of the target machine will have a wrong entry for the gateway. This way, all the traffic destined to pass through the gateway will now pass through the machine that spoofed the **gateway MAC address**.

- **MAC Flooding**

  Switches keep a translation table that maps various MAC addresses to the **physical ports** on the switch. As a result of this, they can intelligently route packets from one host to another. But switches have limited memory. **MAC flooding** makes use of this limitation to bombard switches with fake MAC addresses until the switches cannot keep up. Once this happens to a switch, it then enters into what is known as "**failopen mode**," wherein it starts acting as a hub by broadcasting packets to all the ports on the switch. Once that happens, sniffing can be performed easily. MAC flooding can be performed by using macof, a utility that comes with the **dsniff suite**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

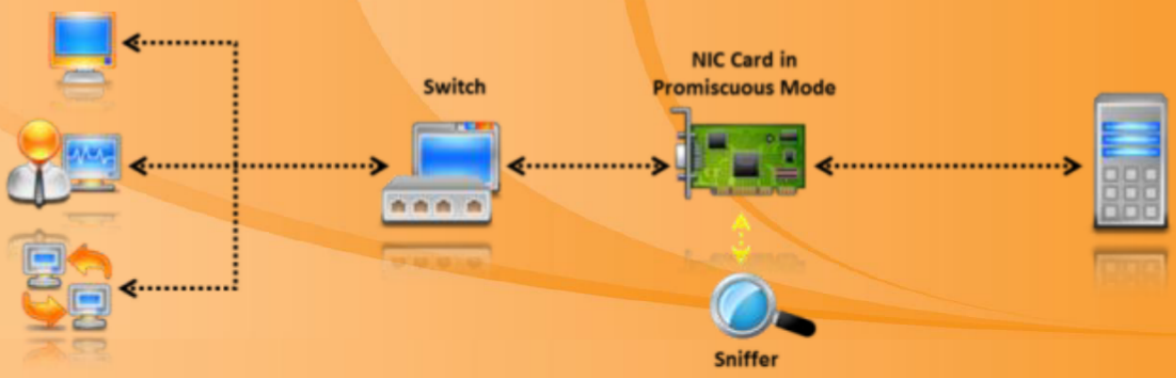
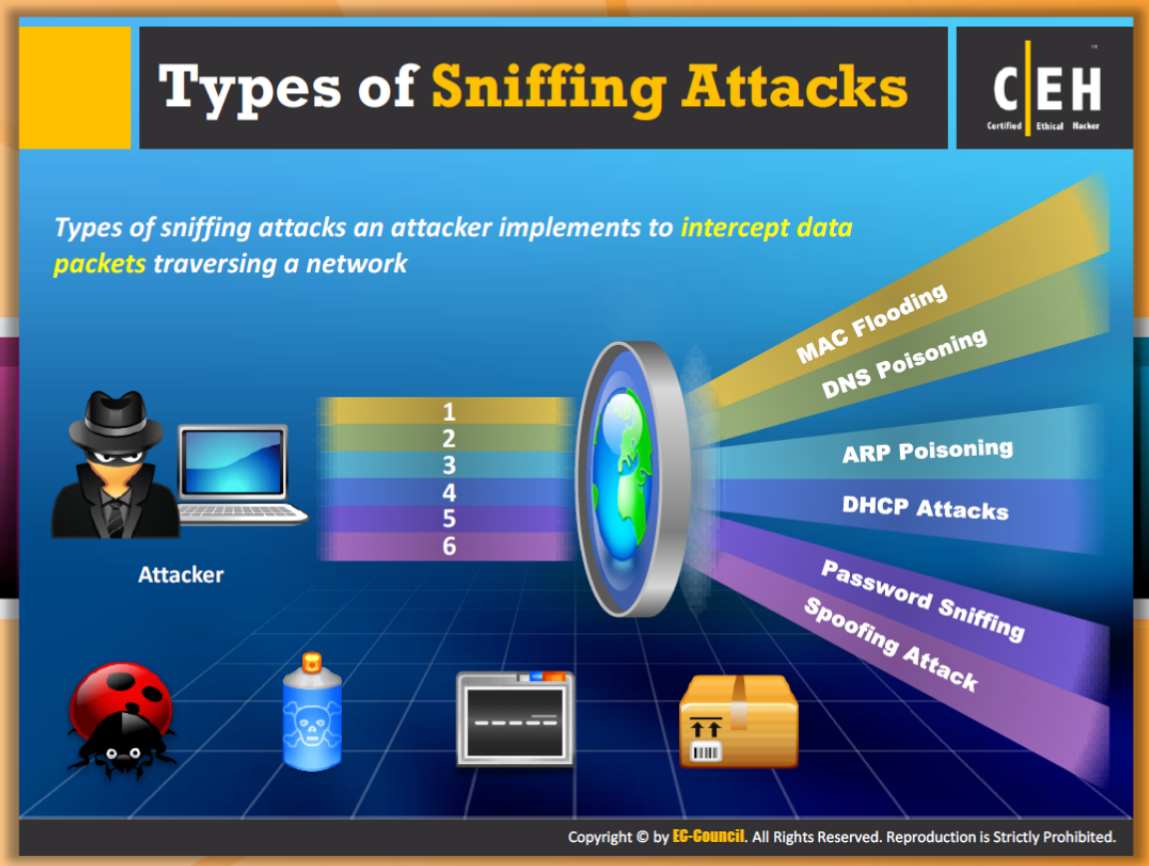


FIGURE 8.3: How a Sniffer Works

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Sniffing Attacks

Sniffers, also referred to as **network protocol analyzers**, are used for capturing data that is being transmitted on a **network,** either legitimately or illegitimately. Though the protocol analyzer is used as a troubleshooting tool, it can also be used to **break into the network**. Using sniffers you can read unencrypted data within the network. This allows you to gather information such as user names, passwords, financial account details, email messages, email attachments, FTP files, etc. Sniffing is a widely used technique for **attacking wireless networks**. Sniffing attacks can be performed in various ways. Depending on the technique used for sniffing, the attacks are categorized into different types. The following are the various types of sniffing attacks:

MAC Flooding

MAC flooding is a kind of sniffing attack that floods the network switch with data packets that interrupt the usual sender to recipient data flow that is common with **MAC addresses**. The data, instead of passing from sender to recipient, blasts out across all the ports. Thus, attackers can monitor the data across the network.

DNS Poisoning

DNS poisoning is a process in which the user is misdirected to a fake website by

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

providing fake data to the DNS server. The website looks similar to the genuine site but it is controlled by the attacker.

ARP Poisoning

ARP poisoning is an attack in which the attacker tries to associate his or her own MAC address with the victim's IP address so that the traffic meant for that IP address is sent to the attacker.

DHCP Attacks

DHCP undergoes two types of attacks. They are:

- DHCP starvation: A process of attacking a DHCP server by sending a large amount of requests to it.
- Rogue DHCP server attack: In this, an attacker sets up a rogue DHCP server to impersonate a legitimate DHCP server on the LAN; the rogue server can start issuing leases to the network's DHCP clients. The information provided to the clients by this rogue server can disrupt their network access, causing DoS.

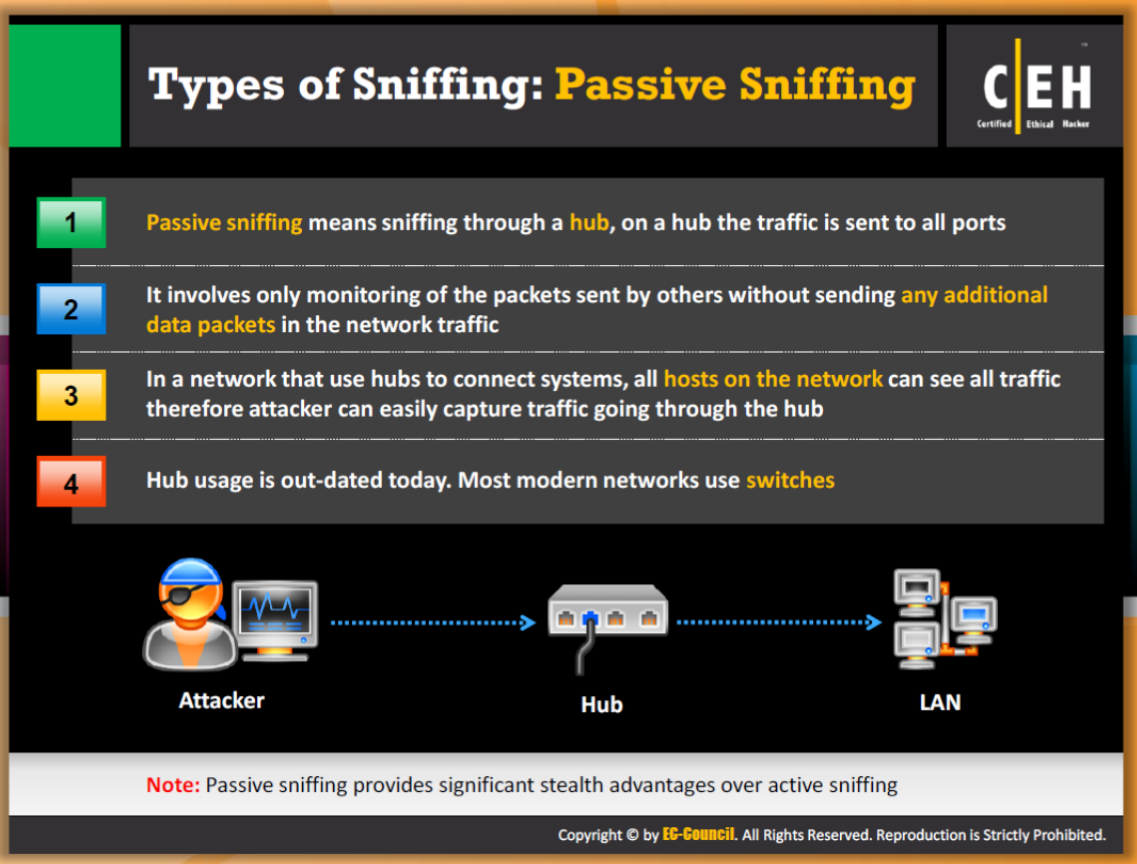
Password Sniffing

Password sniffing is a method used to steal passwords by monitoring the traffic that moves across the network and pulling out data including the data containing passwords. At times, passwords inside the systems are displayed in plain text without encryption, which makes them easy to identify by an attacker and match them with the user names. In cases where the password is encrypted, then attackers can use decryption algorithms to decrypt the password. After obtaining passwords, attackers can gain control over the network, and can even access user accounts, sensitive material, etc.

Spoofing Attacks

A spoofing attack is a situation where an attacker successfully pretends to be someone else by falsifying data and thereby gains access to restricted resources or steals personal information. The spoofing attacks can be performed in various ways. An attacker can use the victim's IP address illegally to access their accounts, to send fraudulent emails, and to set up fake websites for acquiring sensitive information such as passwords, account details, etc. Attackers can even set up fake wireless access points and simulate legitimate users to connect through the illegitimate connection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Sniffing: Passive Sniffing

A sniffer is a software tool that can **capture the packets** destined for the target system rather than the system on which the sniffer is installed. This is known as **promiscuous mode**. Sniffers can turn the **host system's network card** into promiscuous mode. A network interface card in promiscuous mode can capture the packets addressed to it as well as the data it can see. Thus, sniffing can be performed on a target system with the help of sniffers by putting the network interface card of the target organization into promiscuous mode.

Depending on the type of network, sniffing can be performed in different ways. There are two types of sniffing:

- Passive sniffing
- Active sniffing

Passive sniffing involves sending no packets. It just captures and monitors the packets sent by others. A packet sniffer alone is rarely used for an attack because this works only in a **common collision domain**. A common collision domain is the sector of the network that is not switched or bridged (i.e., connected through a hub). Common **collision domains** are usually found in hub environments. Passive sniffing is used on a network that uses **hubs to connect systems**. In such networks, all hosts in the network can see all traffic. Hence, it is easy to capture the traffic going through the hub using passive sniffing.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following is a diagram explains how **passive sniffing** is performed:

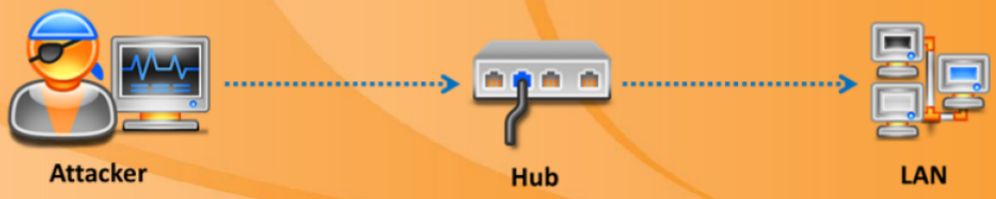


FIGURE 8.4: Passive Sniffing

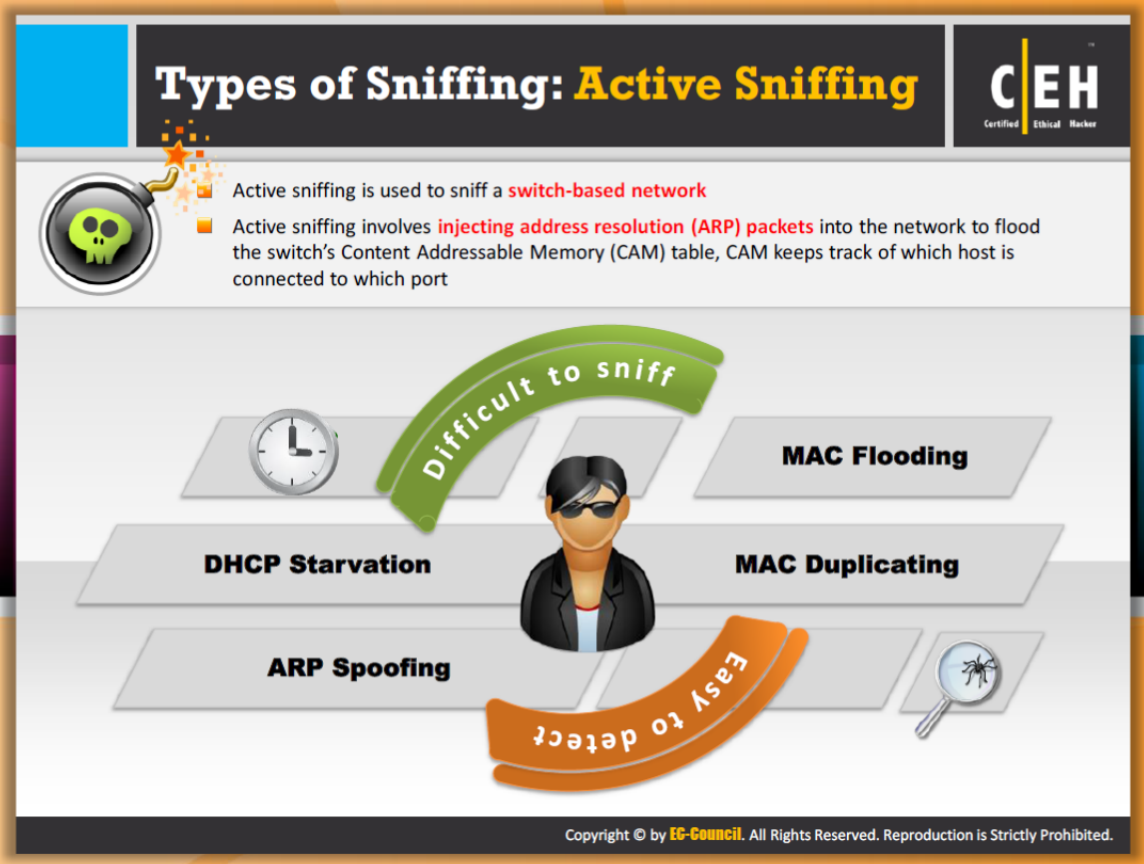
Follow the passive sniffing methods mentioned here to get control over the target network:

- Compromising the physical security: If you can compromise the physical security of the target organization, then walk in to the organization along with your laptop and try to plug in to the **network** and **capture sensitive information** about the organization.
- Using a Trojan horse: Most Trojans have built-in sniffing capability. You can install Trojans with built-in sniffing capabilities on a victim machine to compromise it. Once you compromise the victim machine, then you can install a **packet sniffer** and perform sniffing.

Most modern networks are built using **switches** instead of hubs. A switch is an advanced computer networking device**.** The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the **MAC address associated** with each frame passing through it and sends the data to the required port. Thus, a switch eliminates the risk of passive sniffing. But a switch is still vulnerable to sniffing by means of active sniffing.

Note: Passive sniffing provides significant stealth advantages over active sniffing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Sniffing: Active Sniffing

Active sniffing refers to the process of enabling sniffing of traffic on a **switched LAN** by actively injecting traffic into the LAN. Active sniffing also refers to sniffing through a switch. In active sniffing, the switched Ethernet does not transmit information to all systems that are connected to LAN as it does in a **hub-based network**. Due to this, the passive sniffer will be unable to sniff data on a switched network. It is easy to detect these programs and highly difficult to perform this type of sniffing.

In active sniffing, the data packets for source and destination addresses are first examined by the switches, and then transmitted to the appropriate destination. So it is cumbersome to sniff switches. But attackers are actively injecting traffic into a LAN for sniffing around a switched network and capture the traffic. Switches maintain their own ARP cache in a **content addressable memory (CAM)**; it is a special type of memory in which it maintains the track record of which host is connected to which port. A sniffer takes all the information that is seen on the wire and records it for future review. The users are allowed to see all the information, i.e., in the packet along with the data that should remain hidden.

The following are the special techniques that are provided by sniffing programs for intercepting traffic on a switched network:

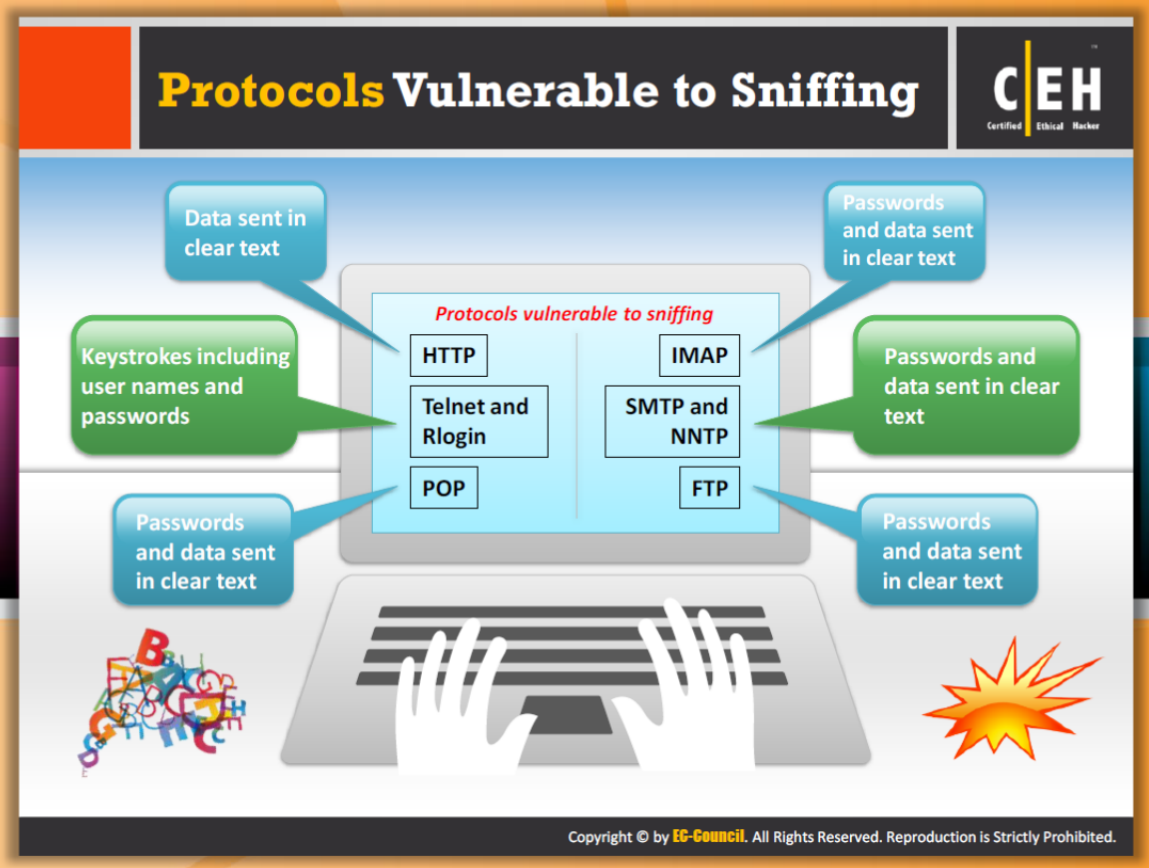
- MAC flooding

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- ARP spoofing
- DHCP starvation
- MAC duplicating

To summarize types of sniffing, passive sniffing does not send any packets; it just monitors the packets sent by others. **Active sniffing** involves sending out multiple network probes to identify access points.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

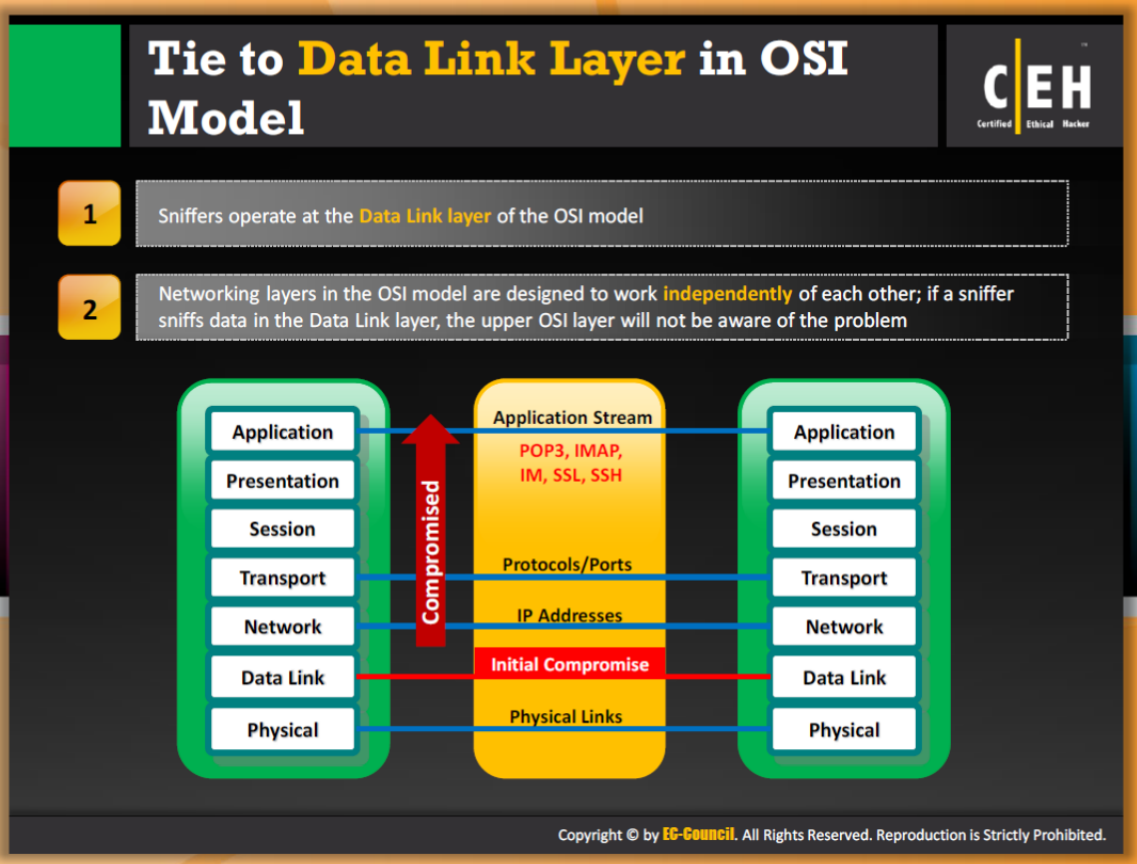


Protocols Vulnerable to Sniffing

The following are the protocols that are vulnerable to sniffing. These protocols are usually sniffed for acquiring passwords:

- **Telnet and rlogin:** With sniffing, keystrokes of a user can be captured as they are typed, including the user's user name and password. Some tools can capture all text and gather it into a terminal emulator, which can reconstruct exactly what the end user is seeing. This can produce a real-time viewer on the remote user's screen.
- **HTTP:** The default version of HTTP has many loopholes. Most of the websites use basic authentication for sending passwords across the wire in clear text. Many websites use a technique that prompts the user for a user name and password that are sent across the network in plain text. Data sent is in clear text.
- **SNMP:** SNMP traffic, i.e. SNMPv1, has no good security. SNMP passwords are sent in clear text across the network.
- **NNTP:** Passwords and data are sent in clear text across the network.
- **POP:** Passwords and data are sent in clear text across the network.
- **FTP:** Passwords and data are sent in clear text across the network.
- **IMAP:** Passwords and data are sent in clear text across the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Tie to Data Link Layer in OSI Model

The OSI model (the **Open Systems Interconnection model**) has a communication system that is divided into smaller parts. Each part is known as a layer. Each layer is engaged in providing services to its upper layer and receiving services from the layer below. The OSI has a networking framework for implementing in seven layers.

The Data Link layer is the second layer of the OSI model. In this layer, data packets are encoded and decoded into bits. Sniffers capture the packets from the Data Link layer.

- Sniffers operate at the Data Link layer of the OSI model. They do not adhere to the same rules as applications and services that reside further up the stack.
- If one layer is hacked, communications are compromised without the other layers being aware of the problem.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

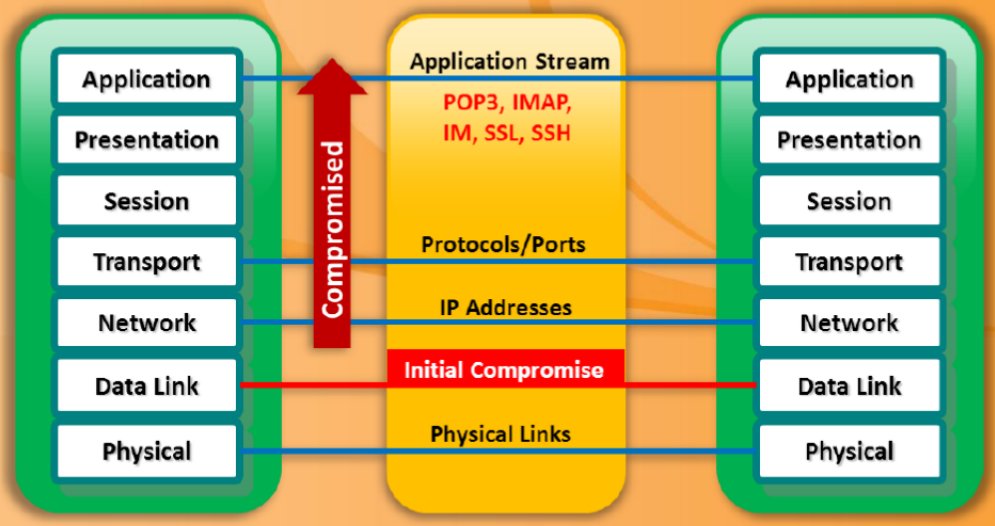
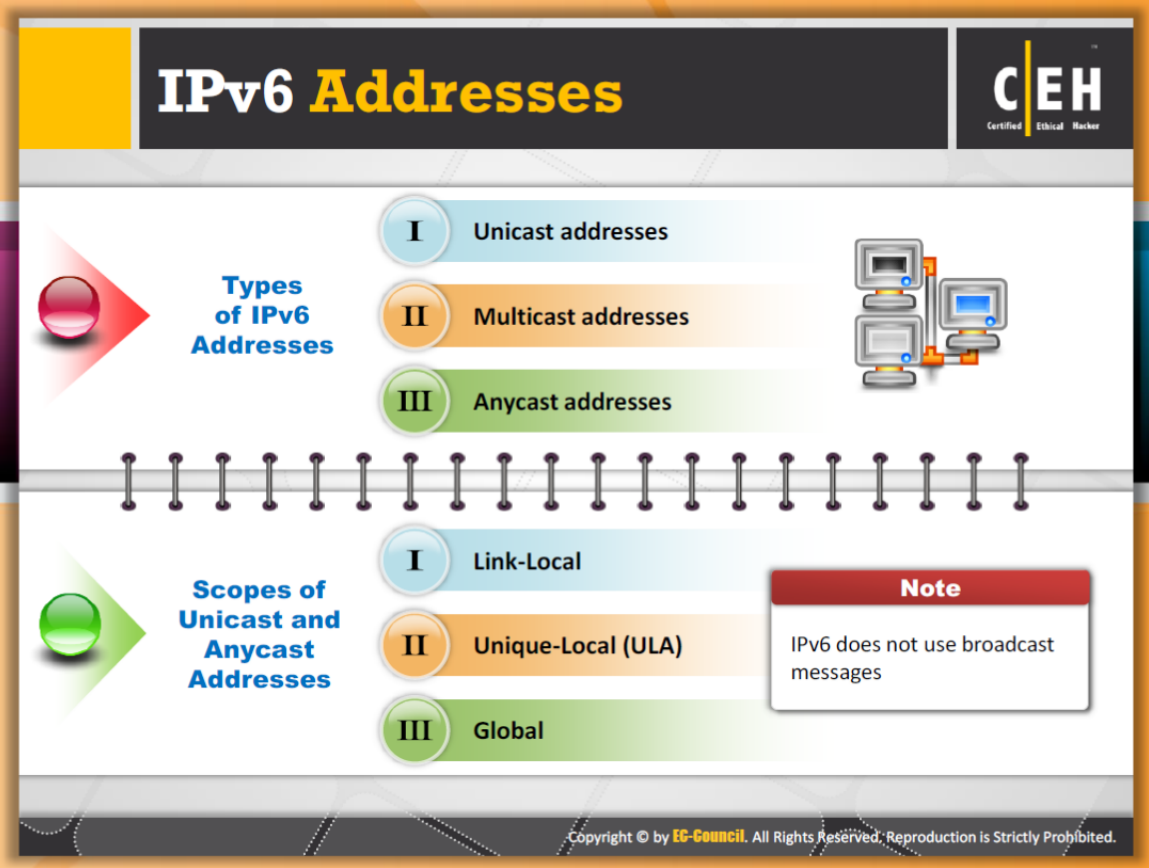


FIGURE 8.5: How Sniffer Work In Data Link Layer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv6 Addresses

IPv6 addresses are the **128-bit** identifiers for interfaces and sets of interfaces. The addresses of IPv6 are of three types. They are:

Unicast: refers to an identifier for a **single interface**. A packet sent to a unicast address is delivered to the interface identified by that address.

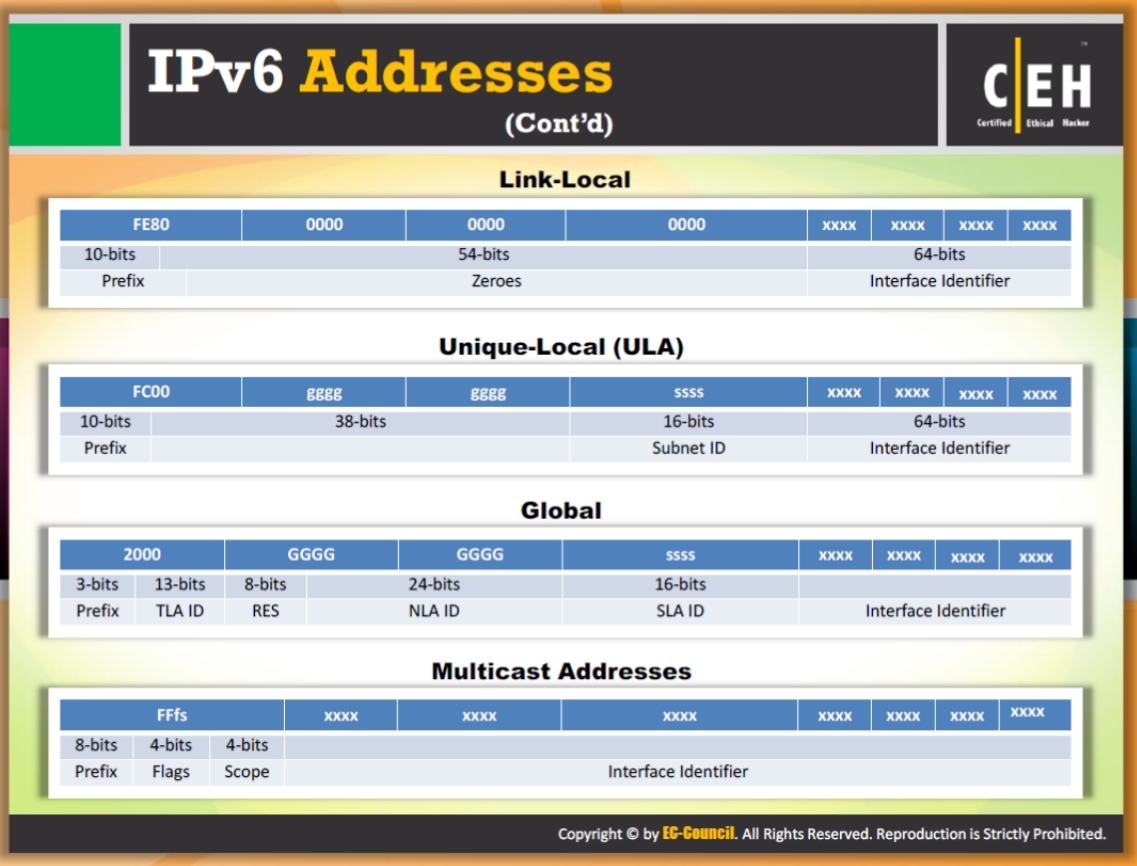
Anycast: refers to an identifier for a **set of interfaces**. A packet sent to an anycast address is delivered to the **nearest interface** identified by that address. The distance is measured based on the routing protocol.

Multicast: refers to an identifier for a **set of interfaces**. A packet sent to a **multicast address** is delivered to all the interfaces identified by that address.

When it comes to scope of the addresses, the unicast can be link-local, site-local, or global. Anycast addresses are usually assigned from the unicast address space. Hence, the scope anycast address is defined as the scope of the unicast address type that assigned the anycast address.

Note: IPv6 does not use **broadcast messages**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv6 Addresses (Cont'd)

Link-Local

FE80	0000	0000	0000	xxxx	xxxx	xxxx	xxxx
10-bits	54-bits			64-bits			
Prefix	Zeroes			Interface Identifier			

Unique-Local (ULA)

FC00	gggg	gggg	ssss	xxxx	xxxx	xxxx	xxxx
10-bits	38-bits		16-bits	64-bits			
Prefix			Subnet ID	Interface Identifier			

Global

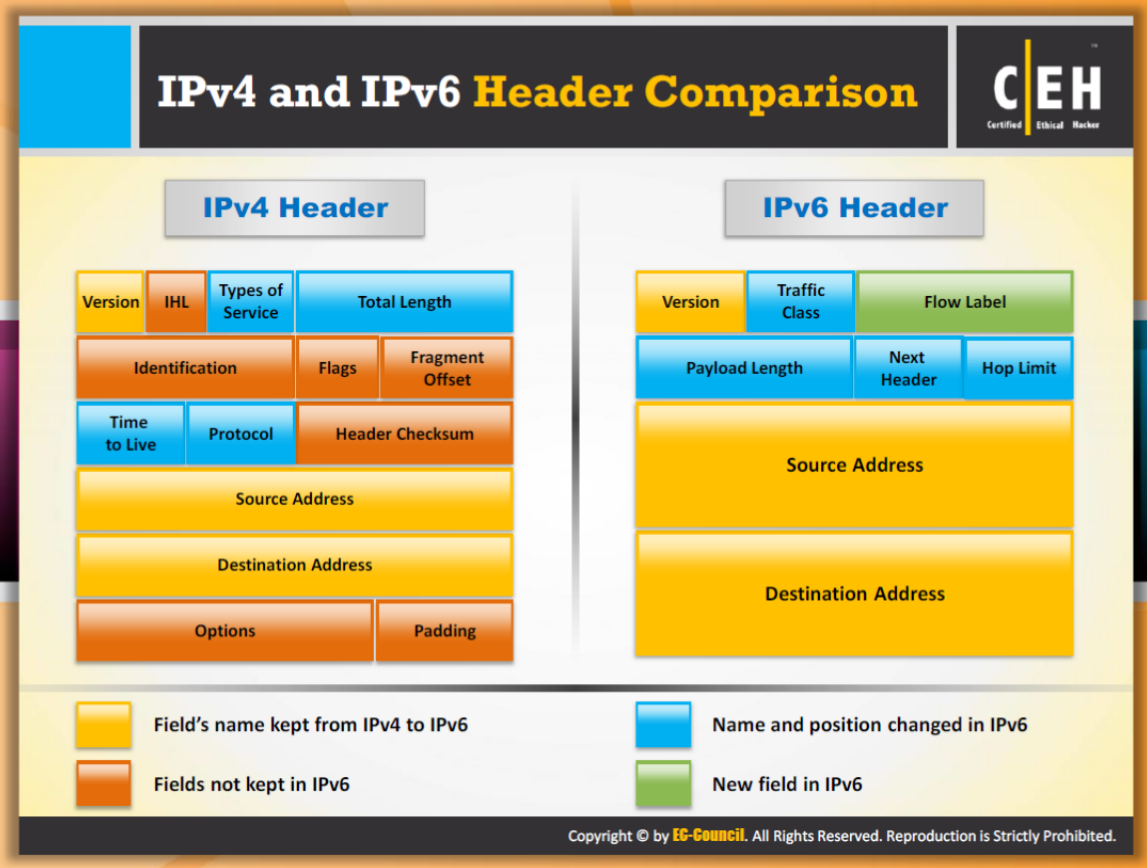
2000	GGGG	GGGG	ssss	xxxx	xxxx	xxxx	xxxx
3-bits	13-bits	8-bits	24-bits	16-bits			
Prefix	TLA ID	RES	NLA ID	SLA ID	Interface Identifier		

Multicast Addresses

FFfs	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
8-bits	4-bits	4-bits					
Prefix	Flags	Scope	Interface Identifier				

TABLE 8.1: IPv6 Addresses

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

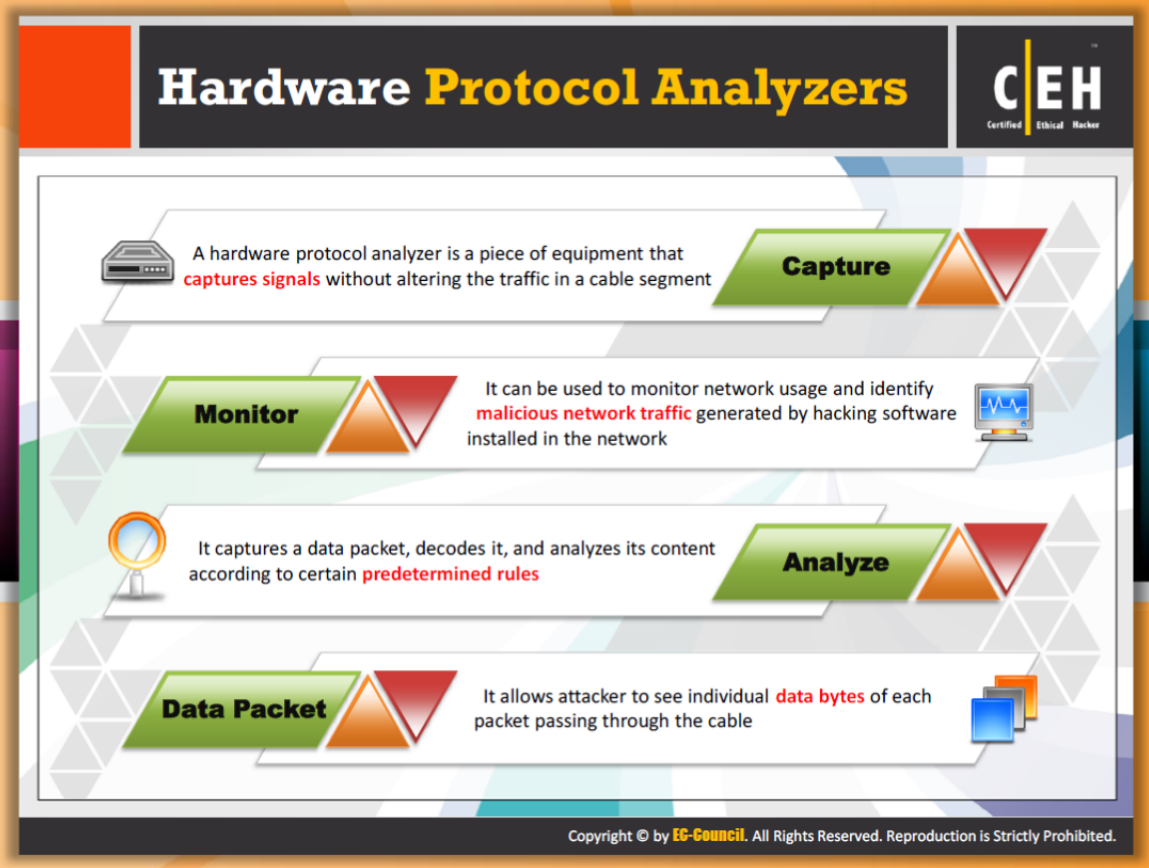


IPv4 and IPv6 Header Comparison

IPv4 Header
Version
IHL
Types of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
IPv6 Header
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
Field's name kept from IPv4 to IPv6
Name and position changed in IPv6
Fields not kept in IPv6
New field in IPv6

FIGURE 8.6: IPv4 and IPv6 Header Comparison

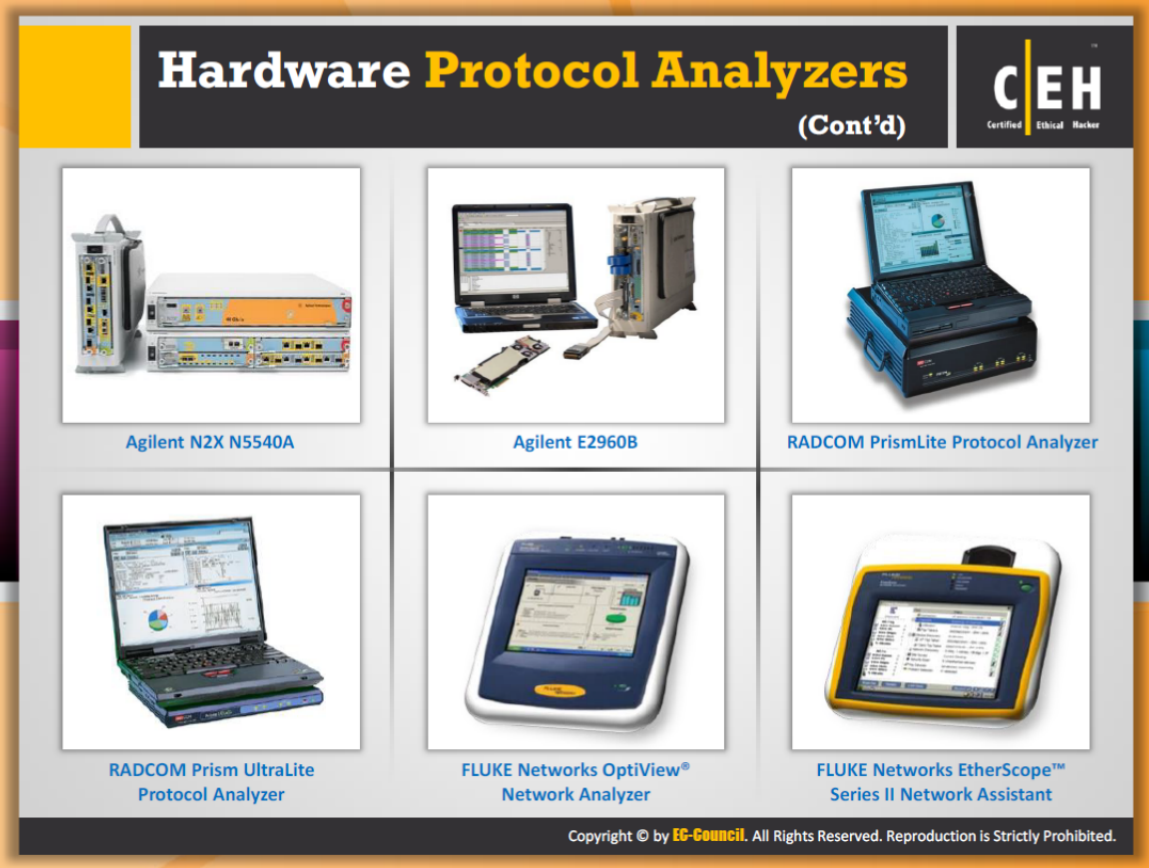
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hardware Protocol Analyzers

A hardware protocol analyzer is a device that **interprets traffic passing** over a network. It is mainly used to **capture the signals** without altering the traffic 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** and **decodes** and **analyzes** its content according to certain predetermined rules. Hardware analyzers are more expensive and out of reach for individual developers, hobbyists, and hackers.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hardware Protocol Analyzers

The hardware protocol analyzers of different companies are shown as follows.

Agilent N2X N5540A

Agilent N2X N5540A is a multi-port test system that allows you to verify the performance of multi-service networks and devices.

FIGURE 8.7: Agilent N2X N5540A

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Agilent E2960B

Agilent E2960B is a tool used for testing as well as debugging. It includes a protocol analyzer that supports x1 through x16 link widths, with intuitive spreadsheet style visualization.

FIGURE 8.8: Agilent E2960B

RADCOM Prism UltraLite Protocol Analyzer

RADCOM Prism UltraLite Protocol Analyzer allows you to monitor and troubleshoot multiple technology networks. It consists of a PrismLite, which is a portable LAN/WAN/ATM protocol analyzer and a Prism UltraLite, which is a compact protocol analyzer for WAN/Fast LAN networks. These analyzers are used for testing a wide range of protocols. Using this analyzer you can **remotely control TCP/IP**.

FIGURE 8.9: RADCOM Prism UltraLite Protocol Analyzer

FLUKE Networks OptiView® Network Analyzer

FLUKE Networks OptiView® Network Analyzer allows you to monitor every part of hardware, each and every application and connection on your network. These tools diagnose and solve the **network application performance** problems as well as protect your network from internal threats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.10: FLUKE Networks OptiView® Network Analyzer

FLUKE Networks EtherScope™ Series II Network Assistant

The Fluke ES2 EtherScope Network Assistant is a **Gigabit LAN** and **802.11 wireless LAN** analyzer. It assists network professionals with installation, validation, and troubleshooting. Install and integrate infrastructure easily by testing, validating, and fixing configuration issues during deployment. It checks the network performance at regular intervals to detect and correct emerging issues. You can identify LAN health instantaneously with the help of this analyzer.

FIGURE 8.11: FLUKE Networks EtherScope™ Series II Network Assistant

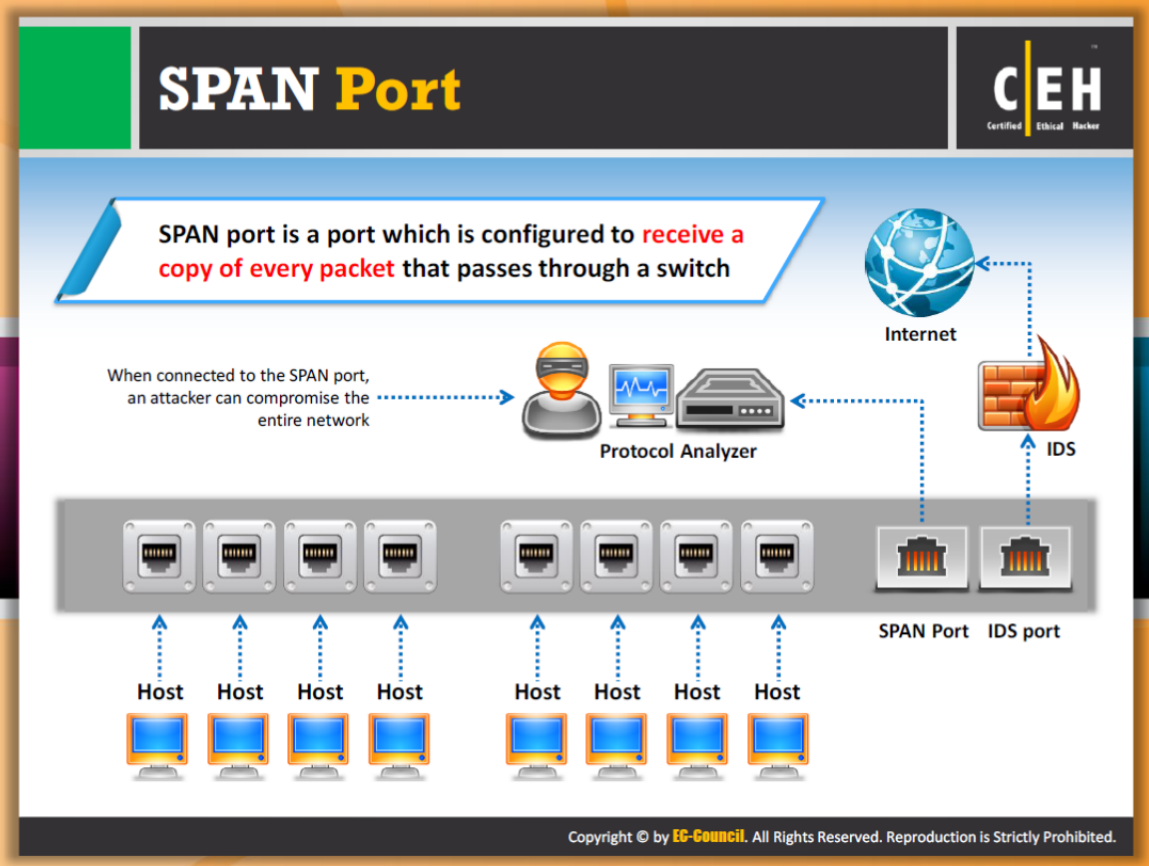
RADCOM PrismLite Protocol Analyzer

The PrismLite is designed for WAN, LAN, and ATM testing simultaneously. It is a tool that allows you to monitor, analyze, and interpret end-to-end traffic that is occurring across the **LAN/WAN network**. It helps you to maintain uninterrupted network services and maximize network performance.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.12: RADCOM PrismLite Protocol Analyzer

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SPAN Port

SPAN for Switched Port Analyzer by Cisco, also known as **port mirroring**, is a method that allows you to **monitor the network traffic** on one or more ports on the switch. It also helps you to analyze and debug data, identify errors, and investigate unauthorized network access on a network. When the port mirroring is enabled, the network switch will send a copy of the **network packets** from the source port to destination port, where the network packets are studied with the help of a **network analyzer**. There can be one or more source, but there should be only one destination port on the switch. Source ports are the ports whose network packets are monitored and mirrored. You can simultaneously monitor the traffic of multiple ports. For instance, you can monitor the traffic on all the ports of a particular **VLAN**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

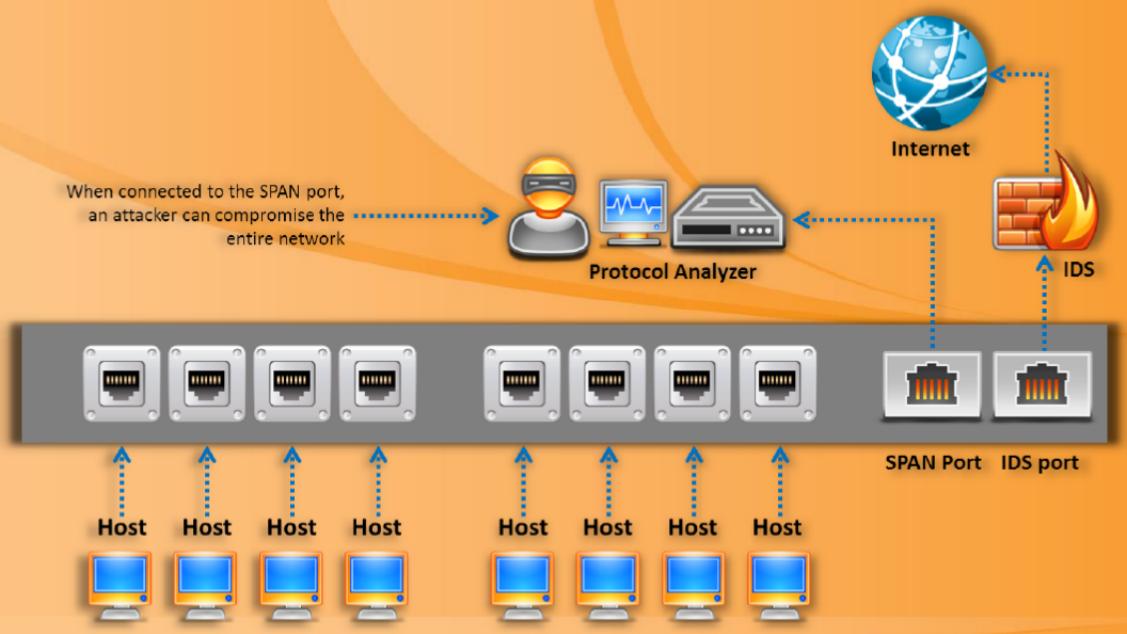
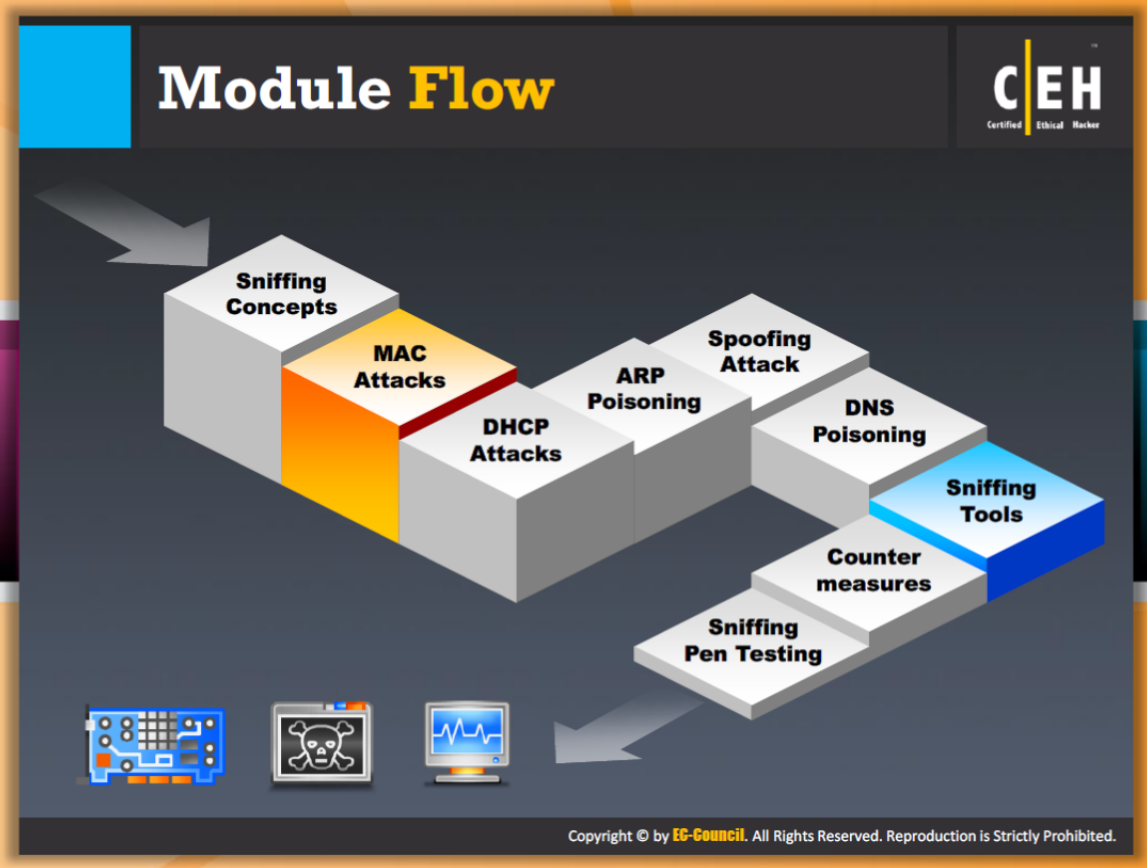


FIGURE 8.13: SPAN Port

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

MAC Attacks

As mentioned previously, sniffing is a data interception technology and a sniffer is an application or device that allows you to monitor or analyze network traffic. Sniffing used legally monitors the network traffic and maintains network security, whereas illegal sniffing aims to steal sensitive information such as passwords, files, and so on. Sniffing can be performed in many ways. MAC flooding is one of the sniffing techniques.

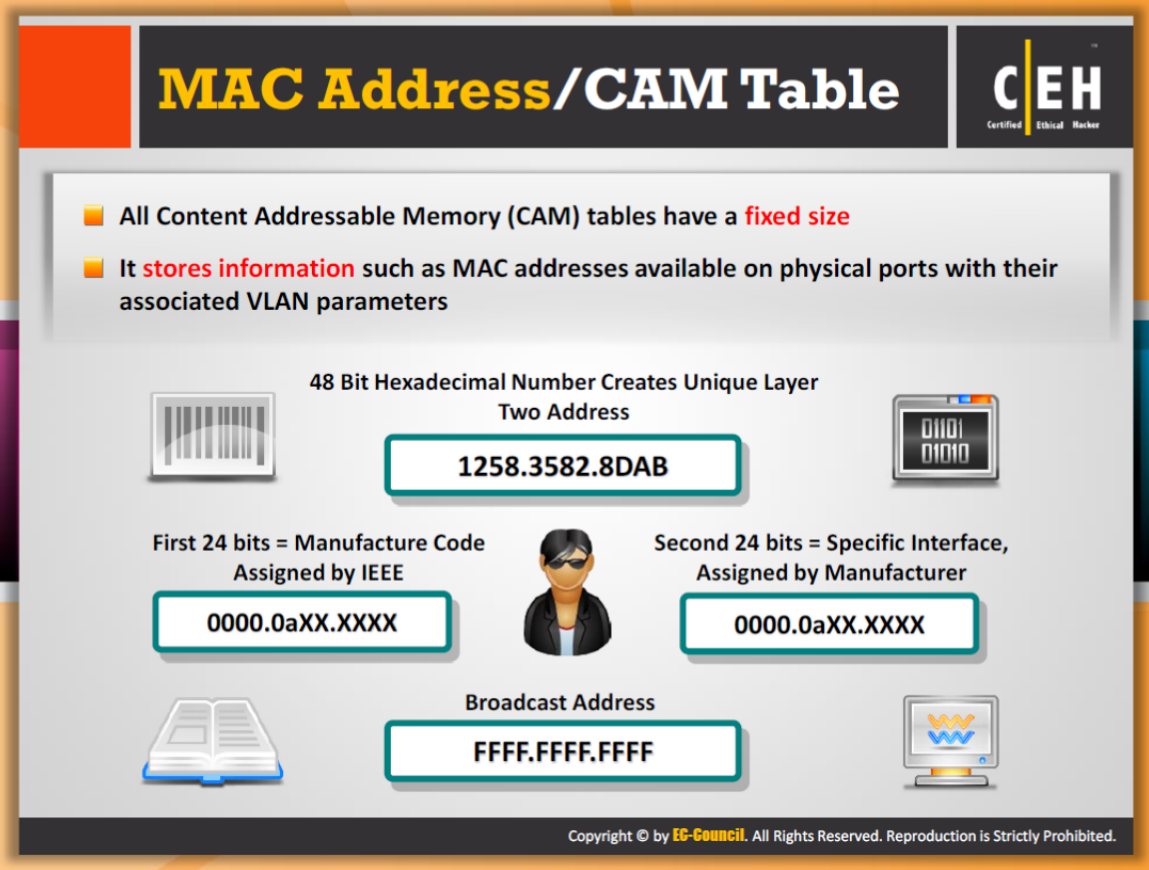
Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Spoofing Attack

This section familiarizes you with techniques used to perform MAC attacks, MAC flooding tools, and countermeasures to protect against MAC attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MAC Address/CAM Table

A media access control address (MAC address) is a **hardware address** that uniquely identifies each node of a network. Each device in the network has a MAC address associated with a **physical port** on the network switch, which makes it possible to designate a specific single point of network.

A content addressable memory (CAM) table separates a switch from hub. It stores information such as MAC addresses available on physical ports with their associated **VLAN parameters**. A CAM table is used by Catalyst switches to store MAC addresses of devices connected to switched network. Every MAC in a CAM table is assigned a switch port number. With this information, the switch knows where to send Ethernet frames. The size of CAM tables is fixed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

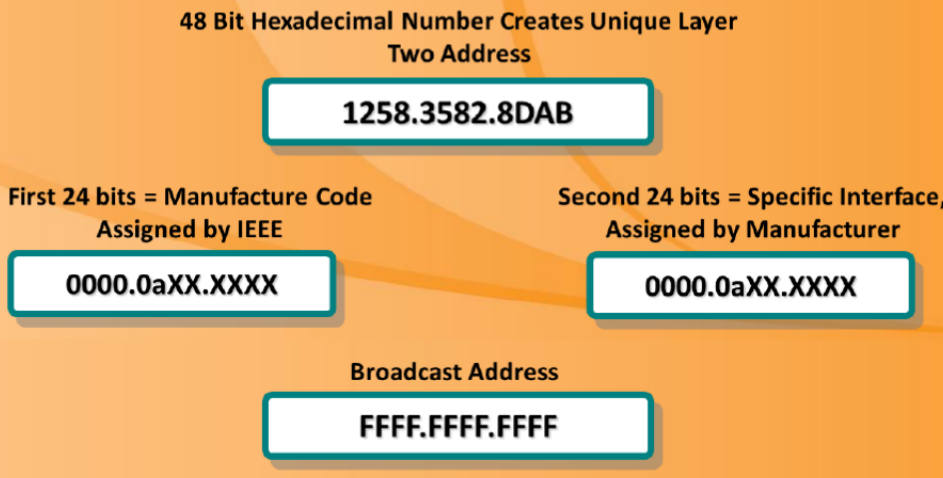
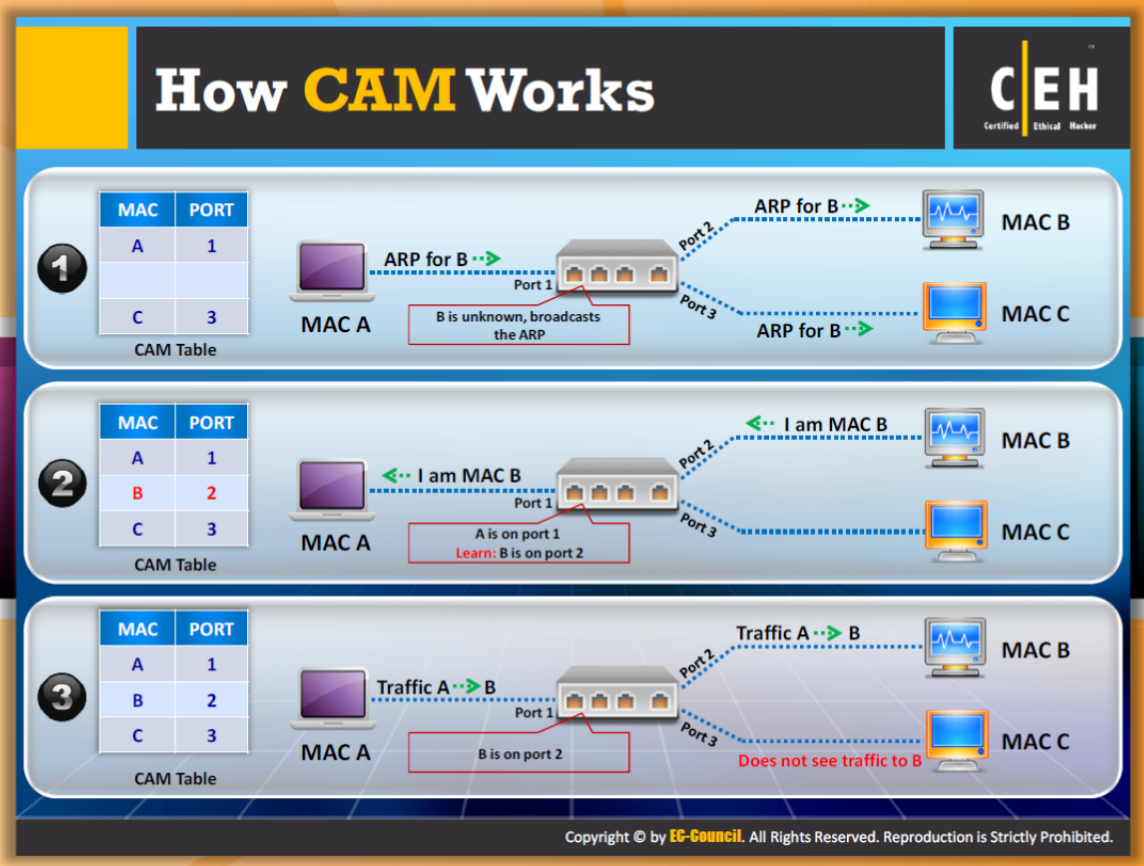


FIGURE 8.14: MAC Address/ CAM Table

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How CAM Works

Source: http://www.freetechexams.com

A CAM table is the content **addressable memory table** that refers to the dynamic form of content and is used with the help of the **Ethernet switch**. The Ethernet switch maintains the connections between the ports.

A CAM table keeps track of **MAC address locations** on a switch with a limited size. If the CAM table gets flooded with more MAC addresses beyond its size, then the switch turns into a hub. The CAM table works in this manner in order to ensure the delivery of data to the intended host. Attackers exploit this vulnerability in the CAM table to **sniff the network data**. If the attacker is able to connect to the shared switch of the Ethernet segment, then he or she can easily sniff the data.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

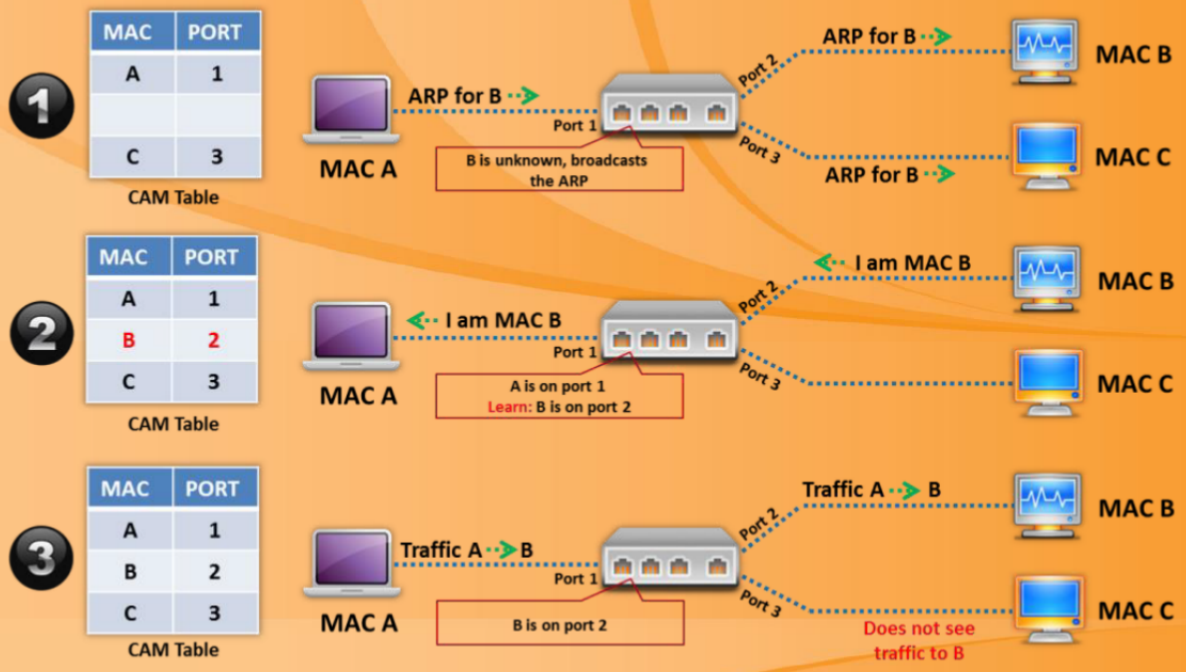
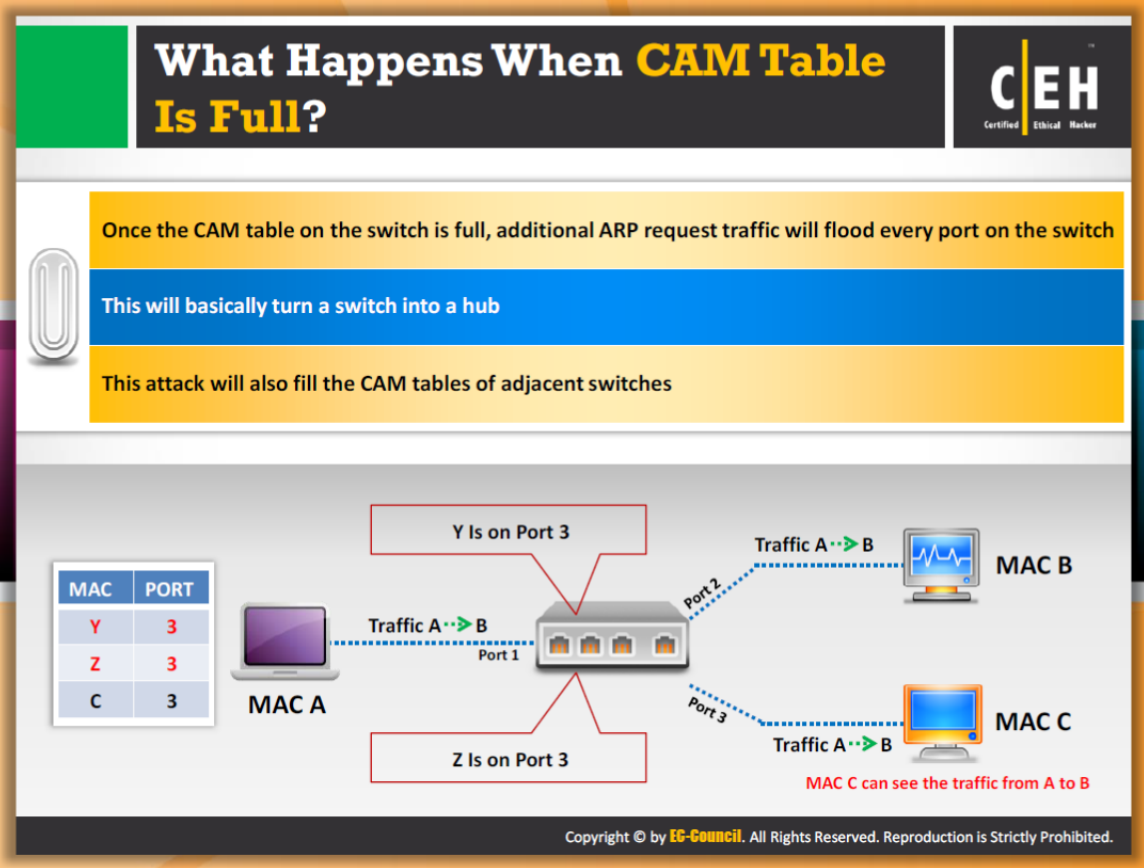


FIGURE 8.15: How CAM Works

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What Happens When a CAM Table is Full?

As we already discussed, a CAM table contains **network information** such as MAC addresses available on physical switch ports and associated VLAN parameters. But these CAM tables are limited in size. You can use this to your advantage to build the attack. You can build the attack with the help of **MAC flooding**. MAC flooding deals with bombarding the switch through fake source MAC addresses until the switch CAM table is full. Once this is done, the switch begins to flood all the incoming traffic to **all ports**. The switch then works as a hub through which you can monitor the frames sent from victim host to another host without any CAM table entry. This attack also fills the CAM tables of **adjacent switches**.

The following diagram explains how a CAM table can be flooded with fake MAC addresses to monitor the frames sent from victim host to another host without any CAM table entry:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

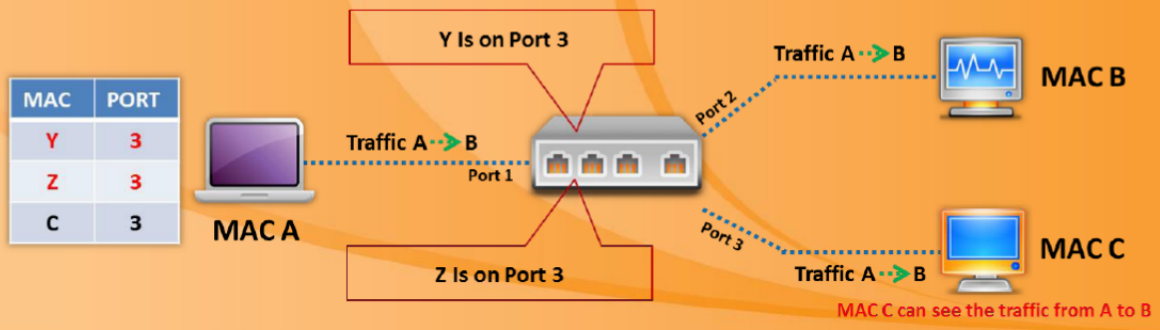
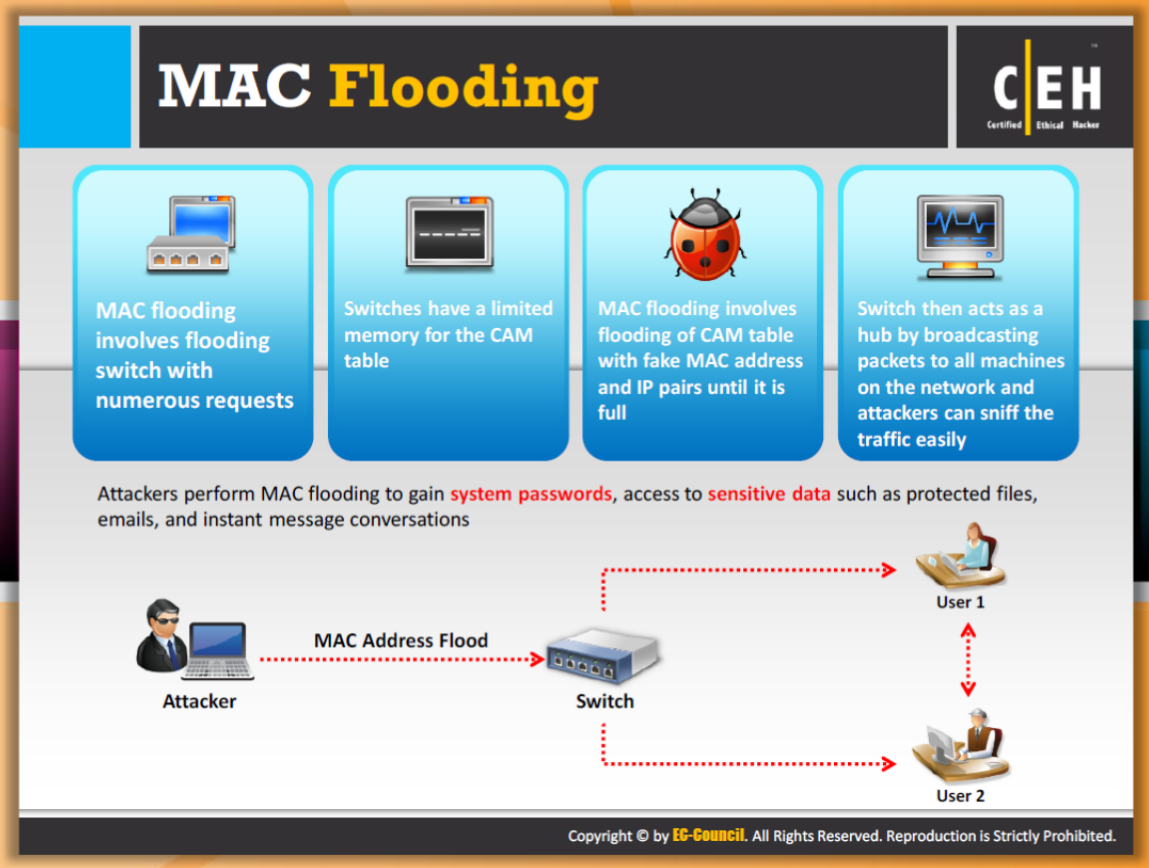


FIGURE 8.16: CAM Table Flooded with Fake MAC Address

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MAC Flooding

MAC flooding is a technique used to **compromise** the security of network switches that connect network segments or network devices. These switches map individual MAC addresses on the network to the physical ports on the switch through the means of a CAM table. Unlike a hub, which broadcasts the data across the network, the switch sends data only to the intended recipient. Thus, a switched network is more secure when compared to a hub network. But, it can still be compromised by the fact that switches have limited memory to store MAC address tables and turn into hubs when flooded with **MAC addresses** beyond their storage. The technique used to compromise a switched network based on limited storage is called MAC flooding.

Typical MAC flooding involves flooding a switch with numerous requests with different fake source MAC addresses. No problem occurs until the MAC address table is full. Once the MAC address table is full, any further requests may force the switch to enter "**failopen mode**." A switch in failopen mode acts like a hub and broadcasts data to all machines on the network. Thus, attackers can sniff the traffic easily and can **steal sensitive information**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

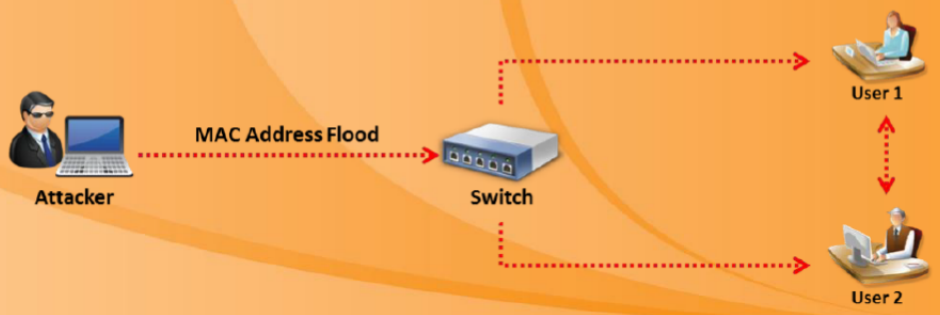
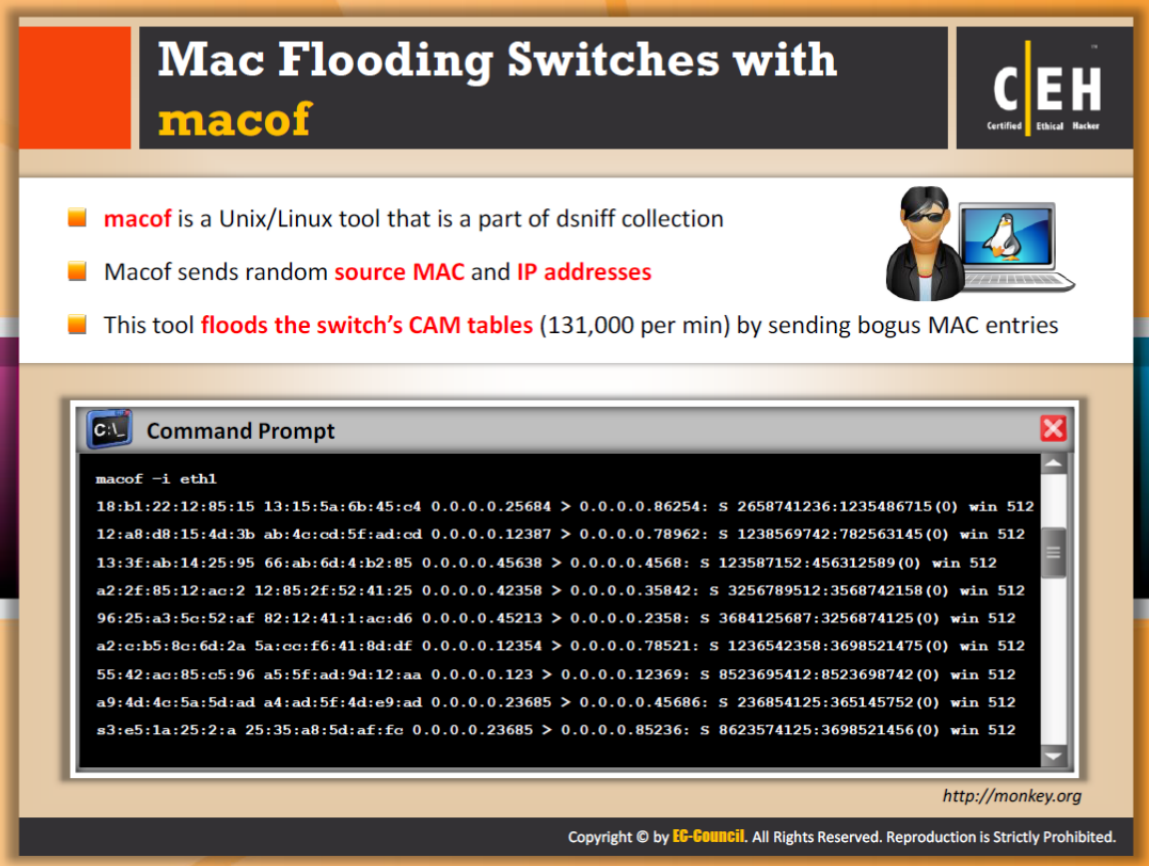


FIGURE 8.17: MAC Flooding

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Mac Flooding Switches with Macof

Source: http://monkey.org

Macof is a member of the **Dsniff suit tool** that floods the local network with random MAC addresses, causing some switches to fail and open in repeating mode, facilitating sniffing. This tool floods the switch's **CAM tables** (131,000 per min) by sending forged MAC entries. The switch regulates the flow of data between ports and monitors the MAC addresses on each port. When a switch is overloaded with huge MAC addresses, it acts like a hub and in a hub, data is broadcasted to every port without mapping. This allows you to monitor the broadcasted data.

The following screenshot shows how to use the **Macof** tool to monitor the broadcasted data:

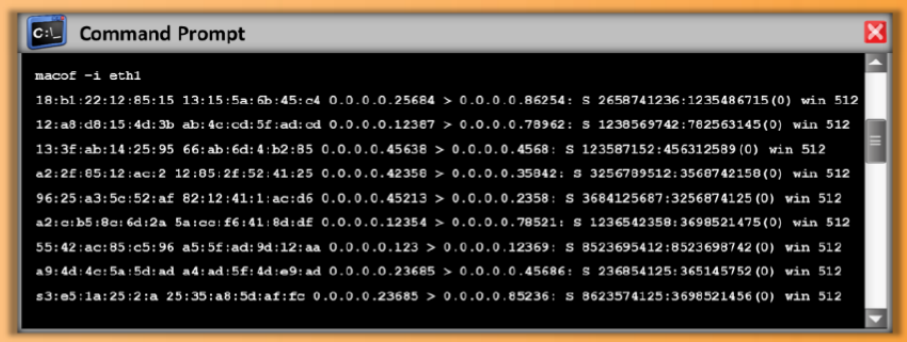
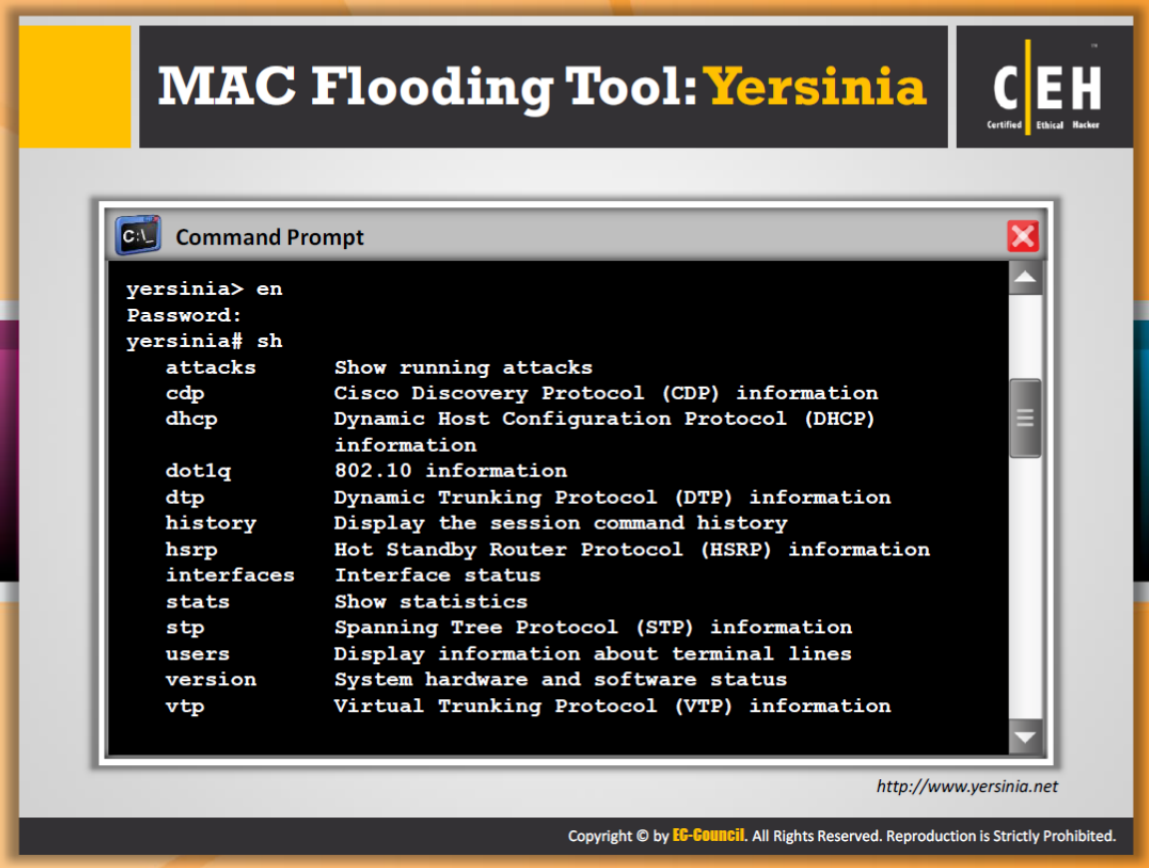


FIGURE 8.18: How Macof monitor the Broadcast Data

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MAC Flooding Tool: Yersinia

Source: http://www.yersinia.net

Yersinia is a network tool designed to take advantage of some weaknesses in different network protocols. It pretends to be a framework for analyzing and testing the **deployed networks** and **systems**. Attacks for the following network protocols are implemented:

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Hot Standby Router Protocol (HSRP)
- IEEE 802.1Q
- IEEE 802.1X
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following is the screenshot of Yersinia in network client mode:

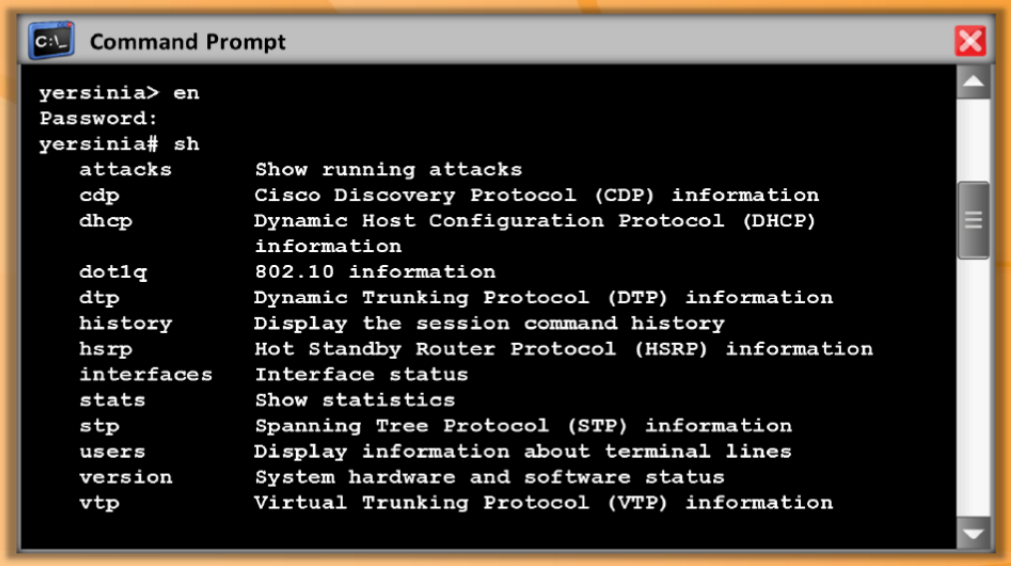
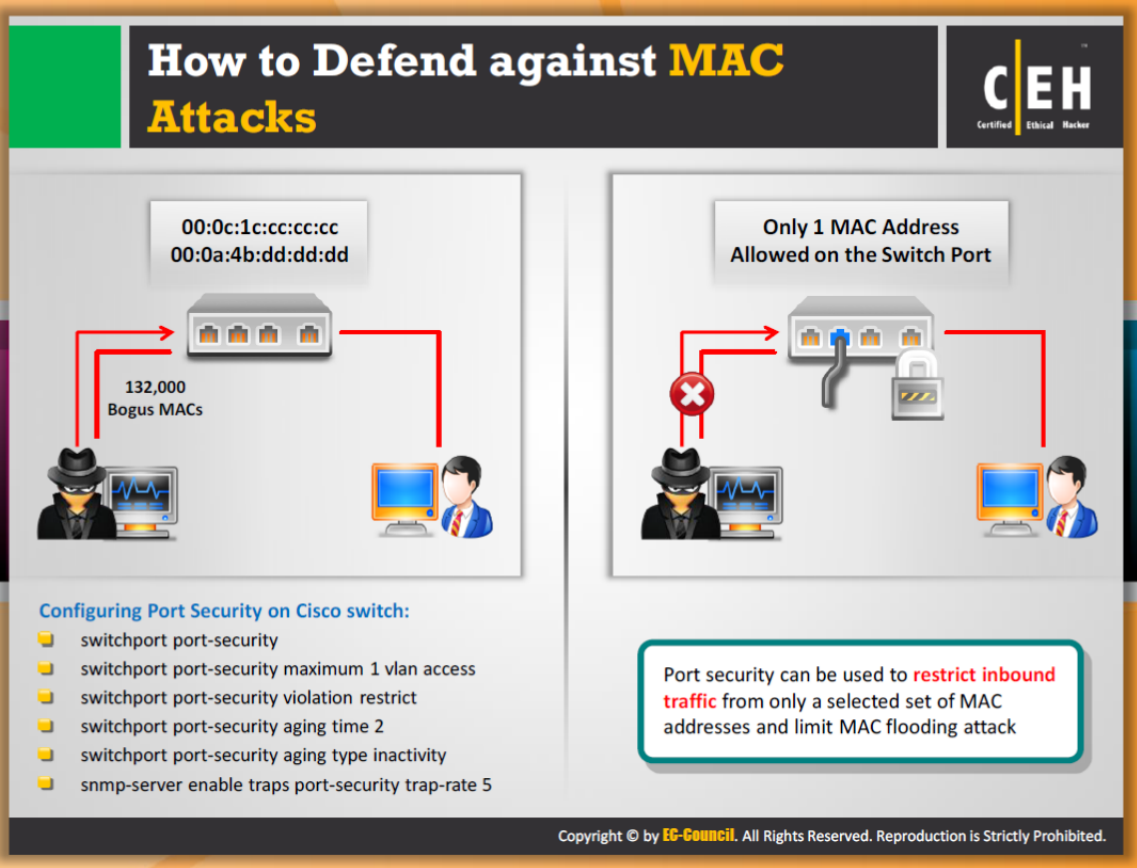


FIGURE 8.19: Working of Yersinia In Network Client Mode

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend against MAC Attacks

You can use switch port, port security feature developed by Cisco to defend against MAC attacks.

In order to protect a port, it identifies and limits the MAC addresses of the workstations that are allowed to access the port. If you assign a **secure MAC address** to a secure port, then the port will forward only the packets with source addresses that are inside the group of defined addresses.

A security violation occurs:

- When a port is configured as a secure port and the maximum number of **secure MAC** addresses is reached
- When the MAC address of the workstation that is attempting to access the port doesn't match with any of the identified secure MAC addresses

Once the maximum number of secure MAC addresses on port is set, the secure MAC addresses are included in an address table by any of the three ways:

- You can configure all secure MAC addresses by using the **switchport port-securing mac-address** interface configuration command.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can allow the port to dynamically configure secure MAC addresses with the MAC addresses of the connected devices.
- You can configure a number of addresses and allow the rest to be dynamically configured.

Port security limits MAC flooding attacks and locks down ports, sending an **SNMP trap**.

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

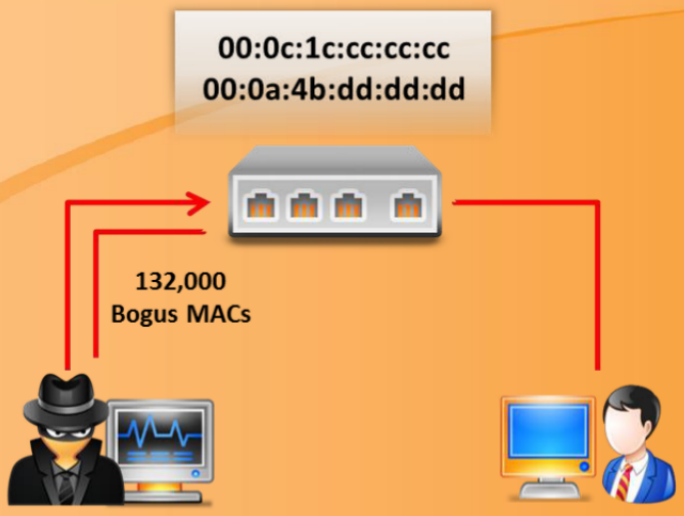


FIGURE 8.20: Attacker Flooded the Switch with Fake Make Address

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Here an attacker is flooding the switch CAM tables with fake MAC addresses and thus threatening security by turning a switch into a hub.

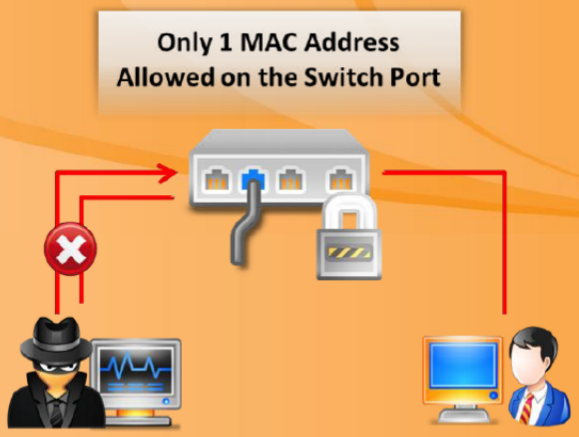
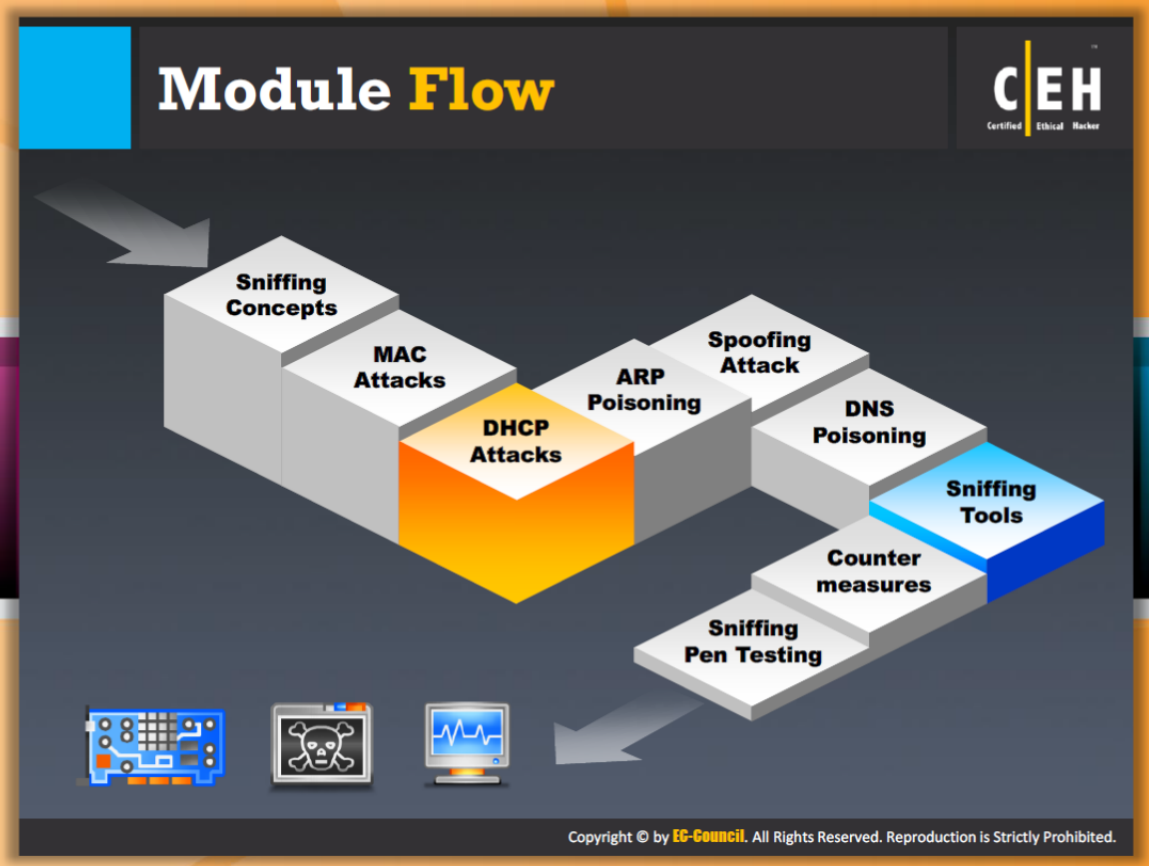


FIGURE 8.21: User Protection from MAC Flooding

The number of MAC addresses allowed on the switch port is limited to one; therefore, it recognizes MAC flooding and locks down the port and sends an SNMP trap.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



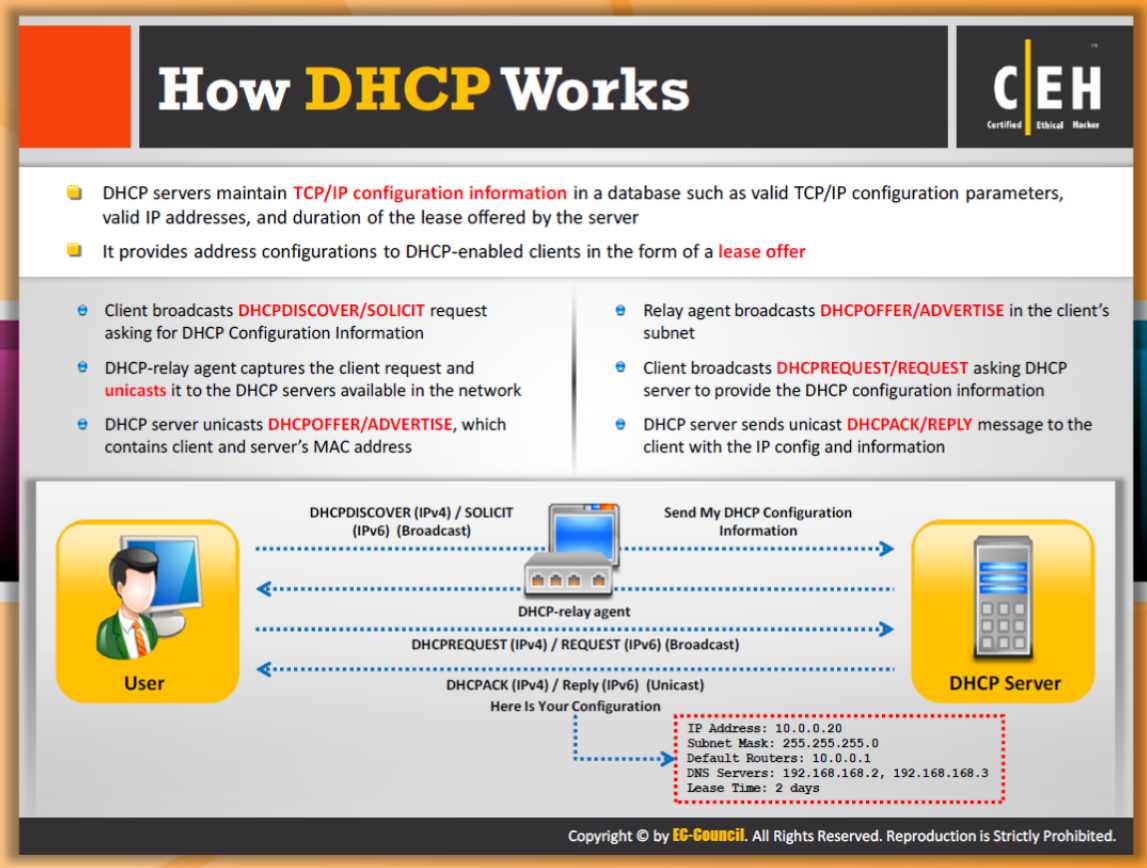
Module Flow

So far, we have discussed various sniffing concepts and MAC attacks, a violation that allows sniffing of network traffic or data. Now we will discuss DHCP attacks, another violation that allows sniffing.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

This section describes how DHCP works, DHCP starvation attacks, tools used for starvation attacks, rogue server attacks, and the ways to defend against DHCP attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How DHCP Works

Dynamic Host Configuration Protocol (DHCP) is a **client/server** protocol intended to provide an IP address to an Internet Protocol (IP) host. In addition to the IP address, the DHCP server also provides configuration-related information such as default gateway and subnet mask. When a DHCP client device boots up, it participates in **traffic broadcasting**.

You can use DHCP to assign IP configuration to hosts connecting to a network providing a framework for passing configuration information to a host on a **TCP/IP network**. A DHCP client makes a request to its server in the same subnet or a different one. The distribution of IP configuration to hosts simplifies the administrator's work to maintain IP networks.

It provides address configurations to DHCP-enabled clients in the form of a lease offer. It involves these steps:

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.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

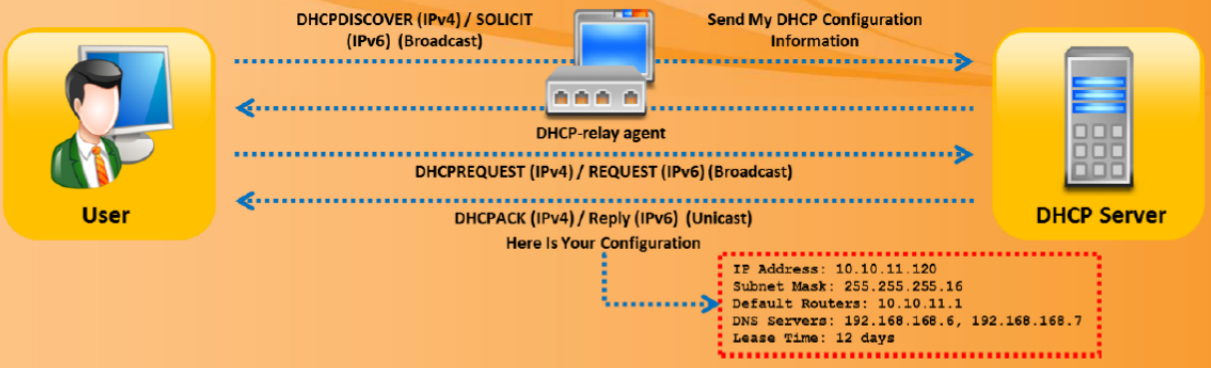


FIGURE 8.22: DHCP Working

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DHCP Request/Reply Messages

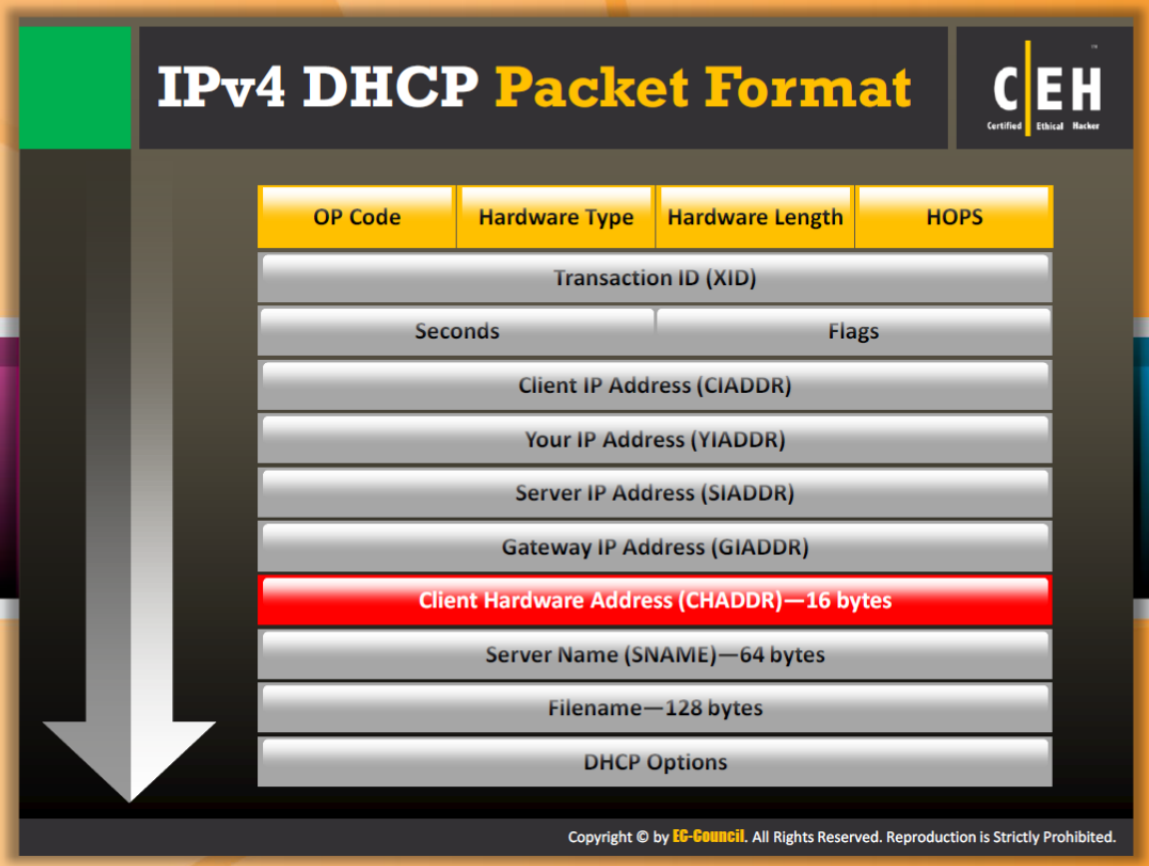
A device that already has an IP address can use the simple **request/reply exchange** to get other configuration parameters from a DHCP server. When the DHCP client receives a **DHCP offer**, immediately the client responds by sending back a DHCP request packet. Devices that are not using DHCP to acquire IP addresses can still utilize DHCP's other configuration capabilities. A client can broadcast a DHCPINFORM message to request that any available server can send its parameters for how the network is to be used. **DHCP servers** respond with the requested parameters and/or default parameters, carried in DHCP options of a DHCPACK message. If a DHCP request comes from a hardware address that is in the DHCP server's reserved pool and the request is not for the IP address that this DHCP server offered, the DHCP server's offer is considered denied. The DHCP server can put that IP address back into the pool and offer it to another client.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client Broadcast to Locate Available 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

TABLE 8.2: DHCP Request/Reply Messages

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IPv4 DHCP Packet Format

The **Dynamic Host Configuration Protocol (DHCP)** is a **network protocol** intended to enable communication on an IP network by configuring network devices. It assigns IP addresses and other information to computers so that they can communicate on the network in client-server model. DHCP has two functionalities: one is **delivering host-specific configuration** parameters and the other is **allocating network addresses** to hosts.

A series of DHCP messages is used for the communication between DHCP servers and DHCP clients. The DHCP message has the same format as that of the BOOTP message. This is because it maintains compatibility of DHCP with **BOOTP relay agents**, thus eliminating the need for changing the BOOTP client's initialization software in order to interoperate with DHCP servers. The following diagram shows the **IPv4 DHCP packet format**:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

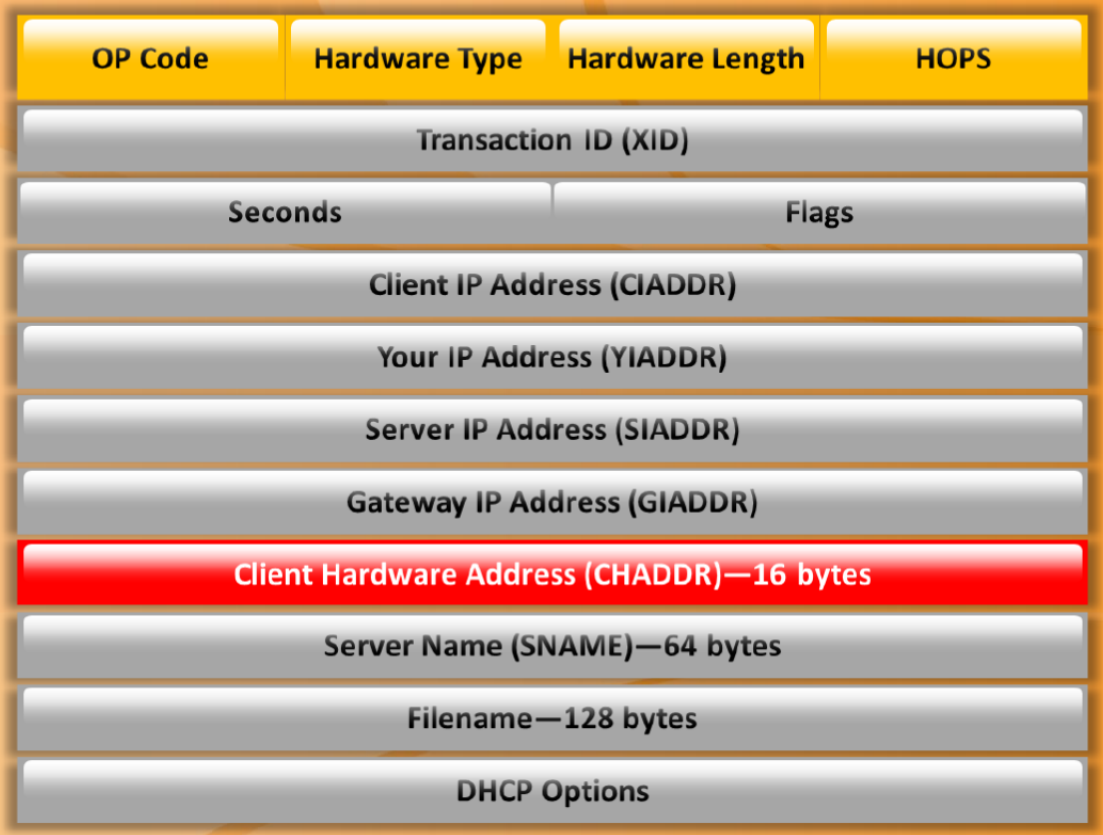


FIGURE 8.23: IPv4 DHCP Packet Format

The following table details every field of the IPv4 DHCP message:

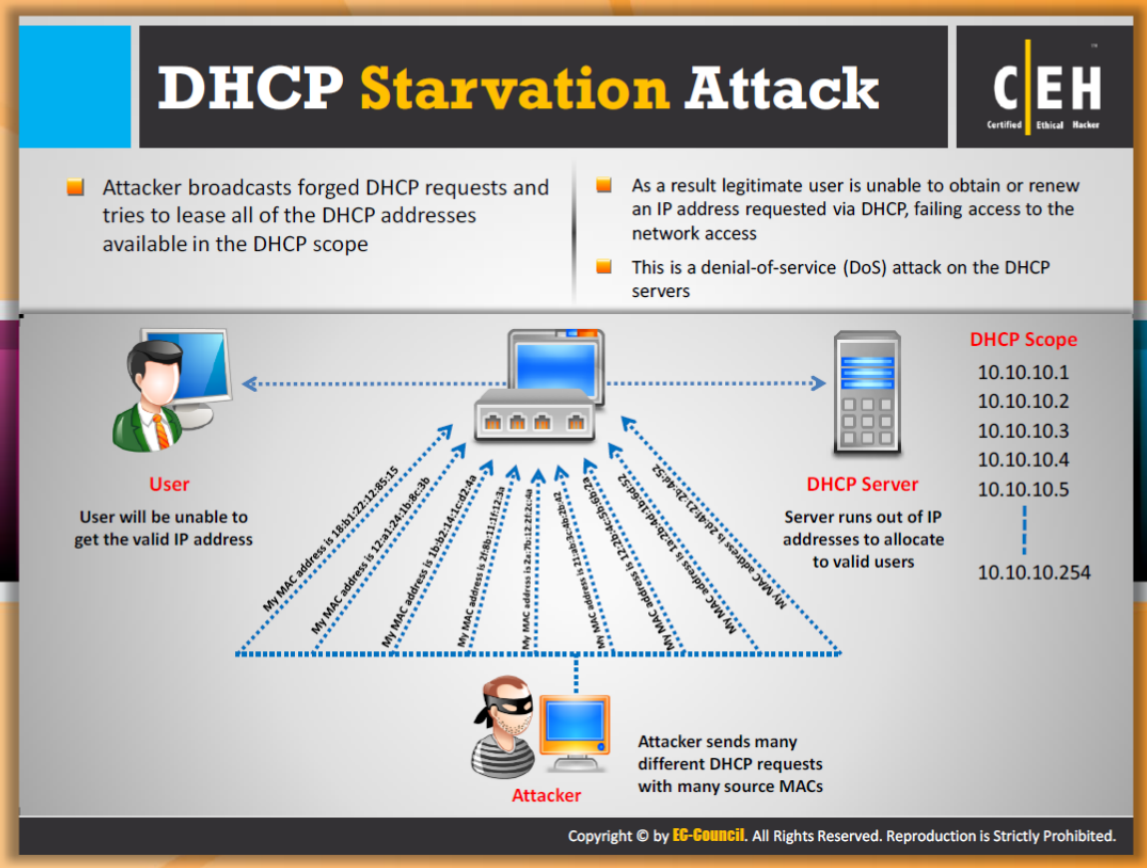
FIELD	OCTETS	DESCRIPTION
OP Code	1	This field contains message op code that represents the message type OP code "1" represents BOOTREQUEST and "2" represents BOOTREPLY
Hardware Address Type	1	Hardware address type defined at Internet Assigned Numbers Authority (IANA) (e.g., '1' = 10Mb Ethernet)
Hardware Address Length	1	Hardware address length in octets
Hops	1	In general, the value is set to "0" by the DHCP clients. But, optionally used to count the number of relay agents that forwarded the message
Transaction ID (XID)	4	A random number chosen by the client to associate the request messages and its responses between a client and a server

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Seconds	2	Seconds elapsed since client began address acquisition or renewal process
Flags	2	Flags set by client. Example: If the client cannot receive unicast IP datagrams, then the broadcast flag is set
Client IP Address (CIADDR)	4	Used when the client has an IP addess and cna respond to ARP requests
Your IP Address (YIADDR)	4	Address assigned by the DHCP server to the DHCP client
Server IP Address (SIADDR)	4	server's IP address
Gateway IP Address (GIADDR)	4	IP address of the DHCP relay agent
Client Hardware Address (CHADDR)	16	Hardware address of the client
Server Name (SNAME)	64	Optional server host name
File Name	128	Name of the file containing BOOTP client's boot image
DHCP Options	Variable	

TABLE 8.3: IPv4 DHCP message

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DHCP Starvation Attack

In a DHCP starvation attack, an attacker floods the **DHCP server** by sending a large number of DHCP request and uses all the available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to **denial of service (DoS) attacks**. Because of this issue, valid users cannot obtain or renew their IP addresses, and thus fail to access their network.

An attacker broadcasts DHCP requests with spoofed MAC addresses with the help of tools such as Gobbler.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

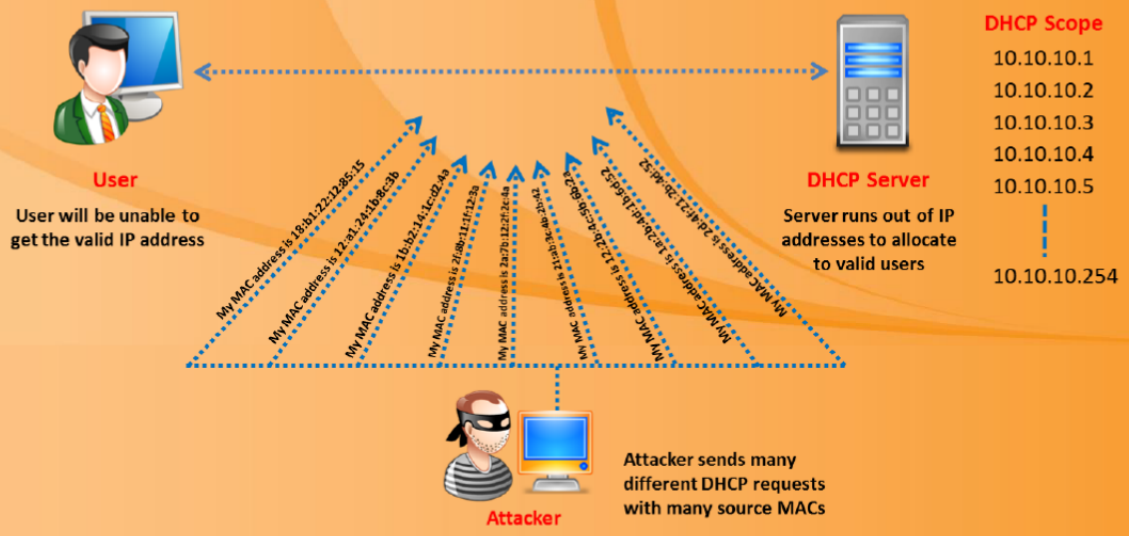
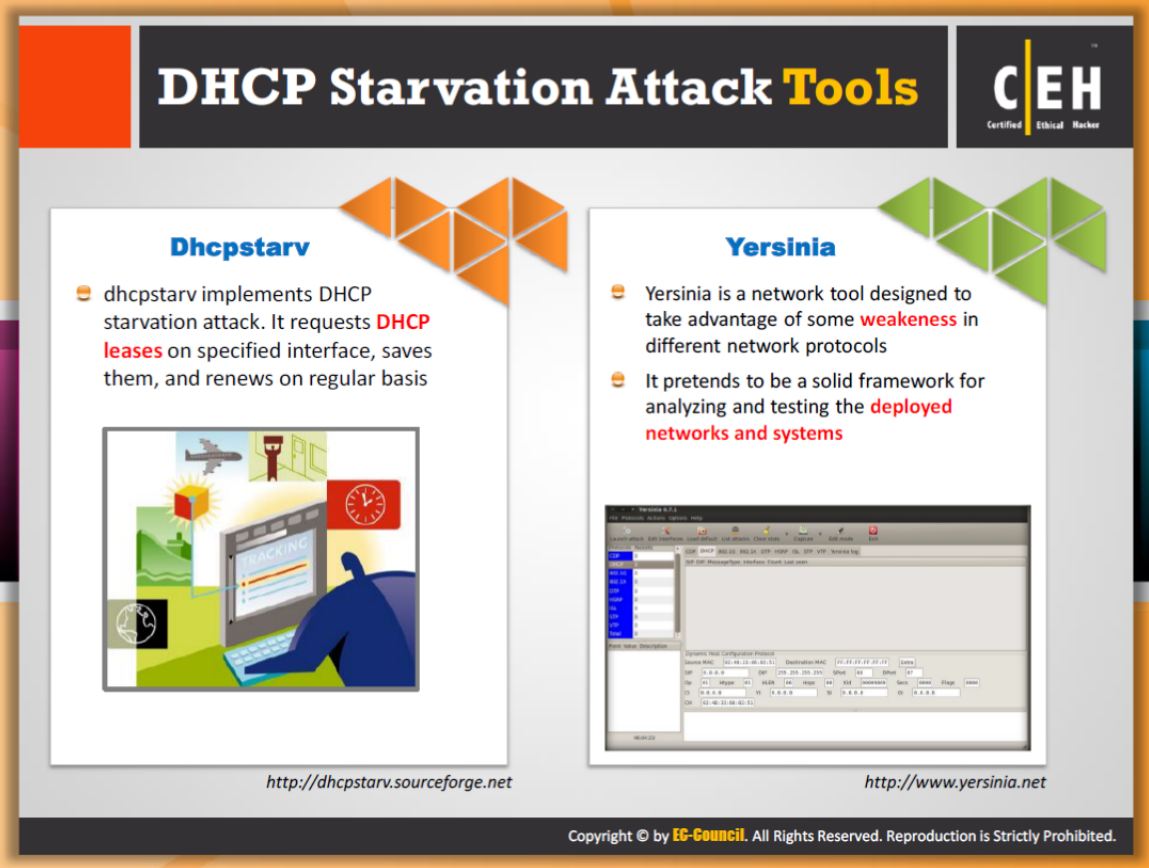


FIGURE 8.24: DHCP Starvation Attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DHCP Starvation Attack Tools

Dhcpstarv and **Yersinia** are tools used by attackers to perform DHCP starvation attacks.

Dhcpstarv

Source: http://dhcpstarv.sourceforge.net

Dhcpstarv implements a DHCP starvation attack. It requests DHCP leases on specified interfaces, saves them, and renews them on a regular basis.

Yersinia

Source: http://www.yersinia.net

Gobbler is a **DOS-based packet sniffer** with **packet-filtering capabilities** when IP addresses are host. This tool is designed especially to audit various aspects of DHCP networks. Gobbler is used to exploit DHCP and an Ethernet to allow distributed spoofed port scanning with the added bonus of being able to sniff the reply from the spoofed host. Gobbler is used as a public domain hacking tool through which automated DHCP starvation attacks are possible. Gobbler allows you to perform **OS detection** and **port scanning**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

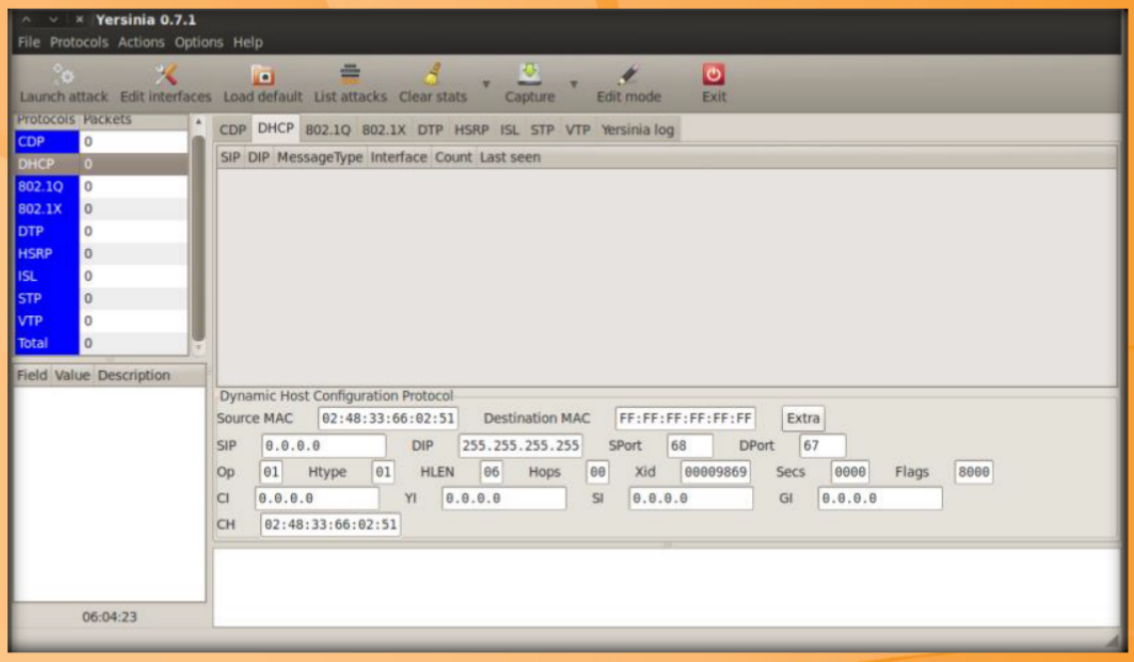
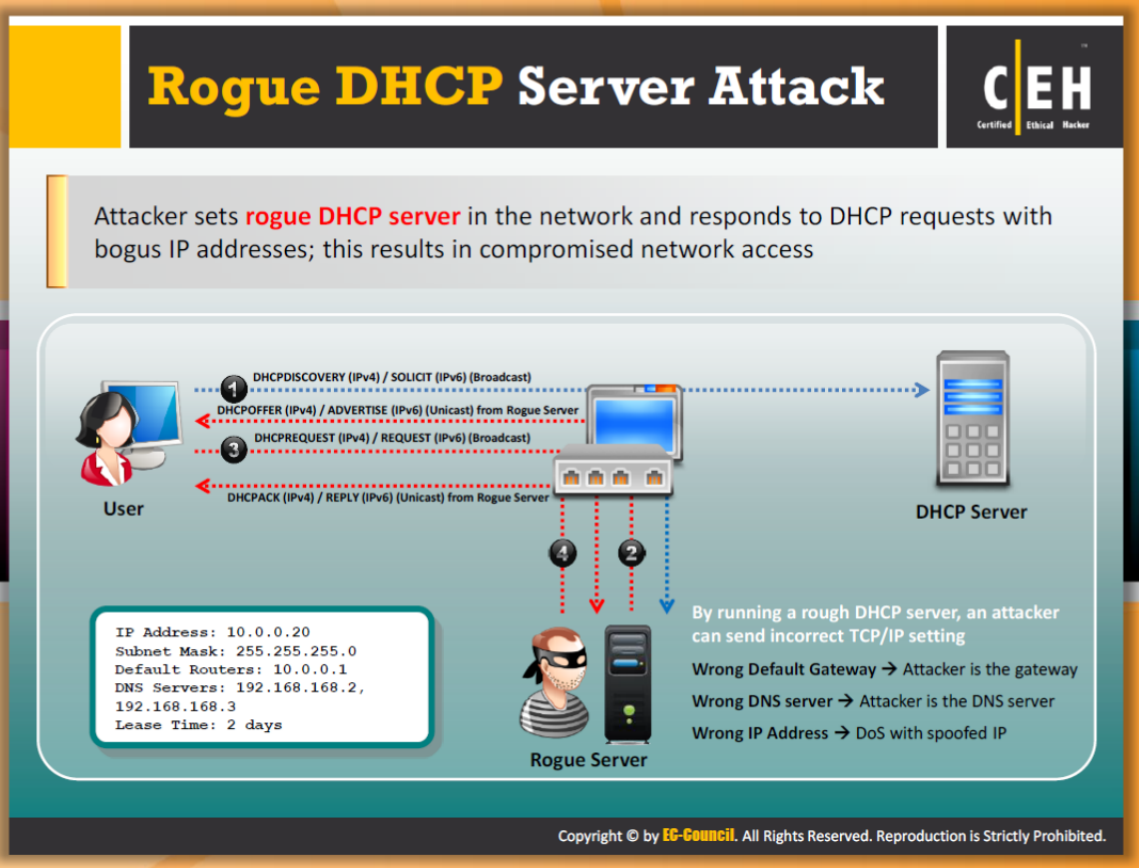


FIGURE 8.25: Working of Yersinia

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Rogue DHCP Server Attack

In a rogue DHCP server attack, an attacker will introduce a rogue server into the network. This rogue server has the ability to respond to clients' **DHCP discovery requests**. Though both the servers respond to the request, i.e., the rogue server and actual DHCP server, the server that responds first will be taken by the client. In a case where the rogue server gives the response earlier than the actual DHCP server, at that point the client takes the response of the rogue server. The information provided to the clients by this **rogue server** can disrupt their network access, causing DoS.

The DHCP response from the attacker's rogue DHCP server may assign the IP address of an attacker as a client's **default gateway**. As a result, all the traffic from the client will be sent to the attacker's IP address. The attacker then captures all the traffic and forwards this traffic to the appropriate default gateway. From the client's viewpoint, he or she thinks that everything is functioning correctly. This type of attack cannot be detected by the client for **long periods**.

Sometimes, the client, instead of using the standard DHCP server, uses a rogue DHCP server. The rogue server directs the client to visit fake websites for the purpose of gaining their credentials.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To mitigate a rogue DHCP server attack, set the interface to which that rogue server is connected to as untrusted. That action will block all ingress **DHCP server messages** from that interface.

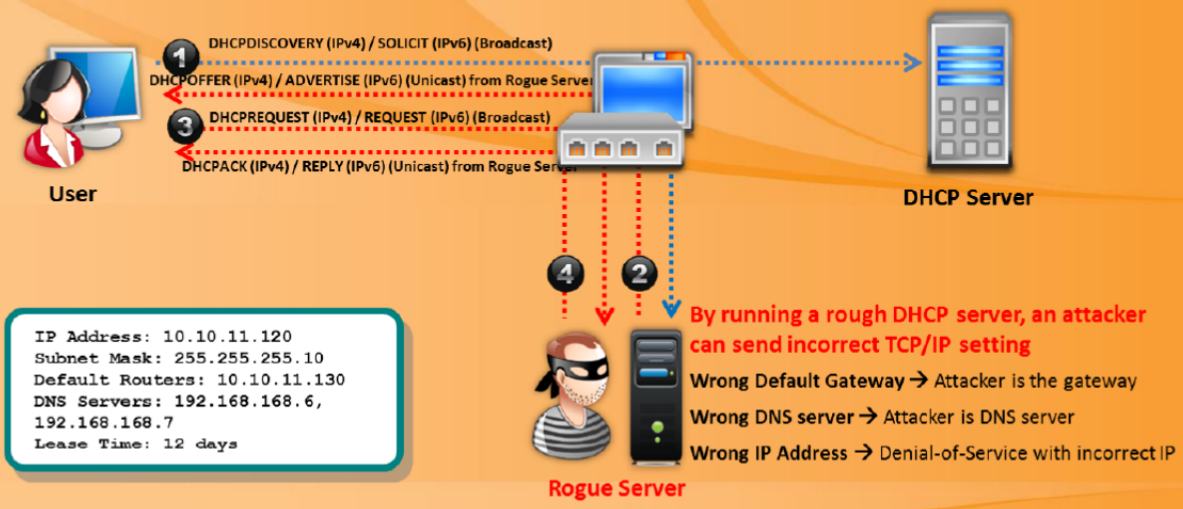
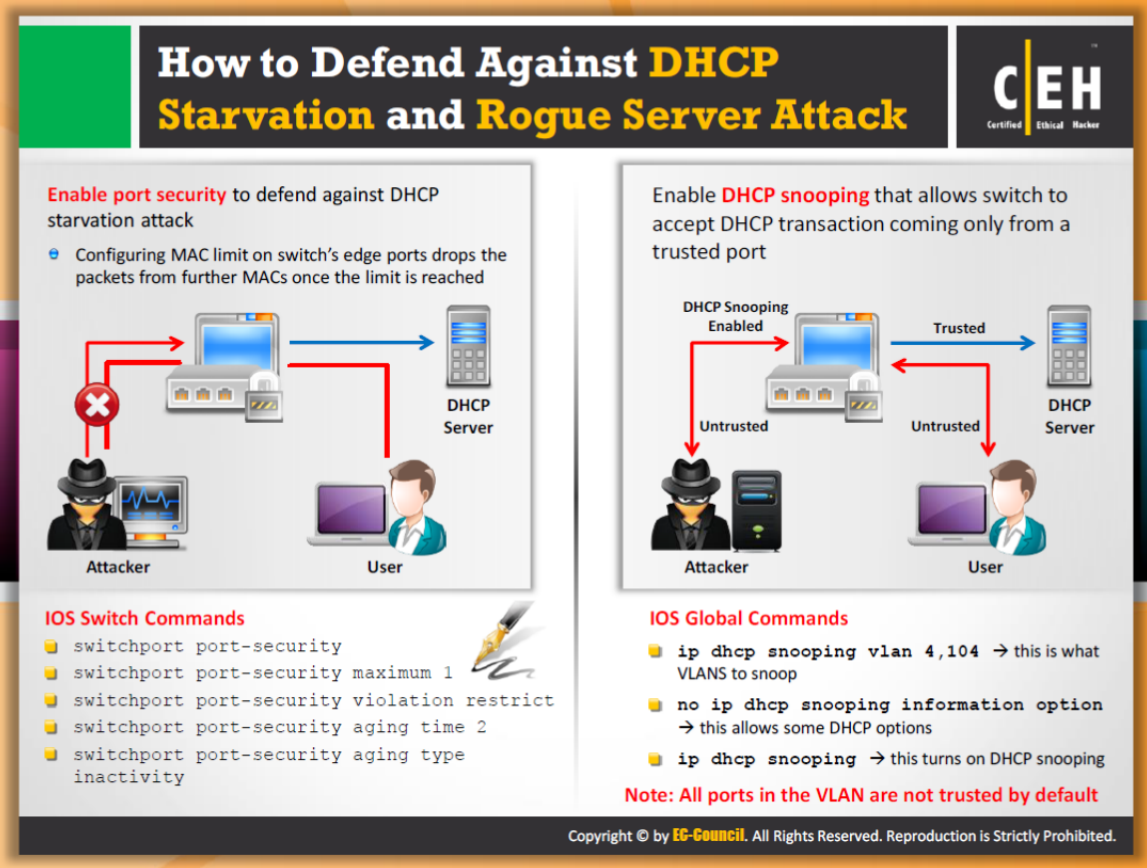


FIGURE 8.26: How Rogue DHCP Server Work

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against DHCP Starvation and Rogue Server Attacks

Defend Against DHCP Starvation

Port security is used to limit the **maximum number of MAC addresses** on the switch port, thereby preventing DHCP starvation attacks.

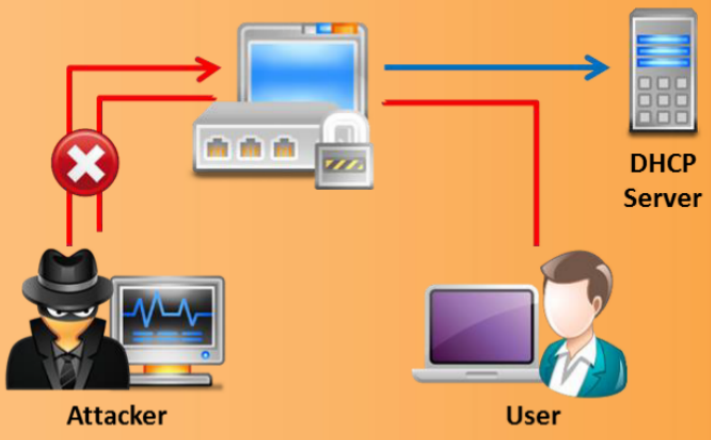


FIGURE 8.27: Defend Against DHCP Starvation

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

Defend Against Rogue Servers

Rogue DHCP servers can be mitigated by the DHCP snooping feature. **DHCP snooping** is a feature available on switches. In order to defend against rogue DHCP servers, configure DHCP snooping on the port on which the valid dhcp server is connected. Once you configure DHCP snooping, it does not allow other ports on the switch to respond to **DHCP discover** packets sent by clients. Thus, even if an attacker manages to build a rogue dhcp server and connects to the switch, he or she cannot respond to DHCP discover packets.

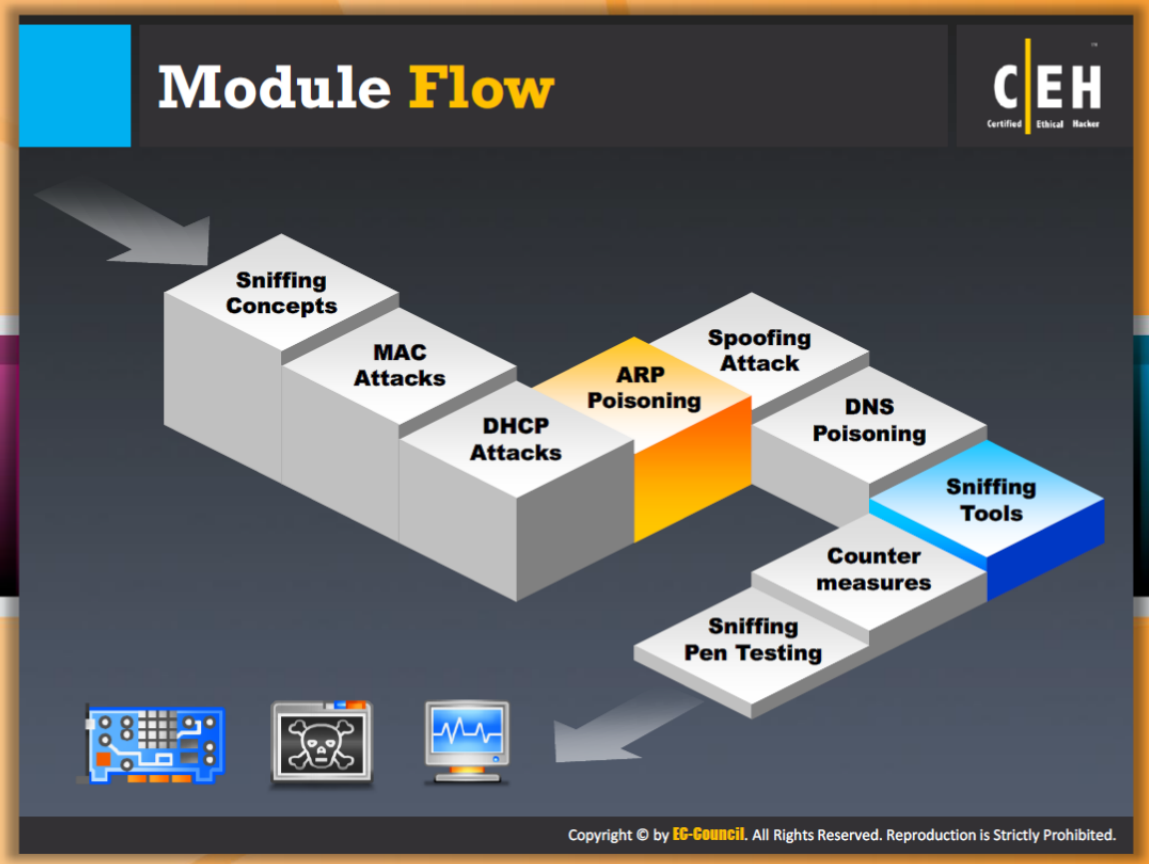
IOS Global Commands

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

FIGURE 8.28: Defend Against DHCP Starvation

Note: All ports in the **VLAN** are untrusted by default.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

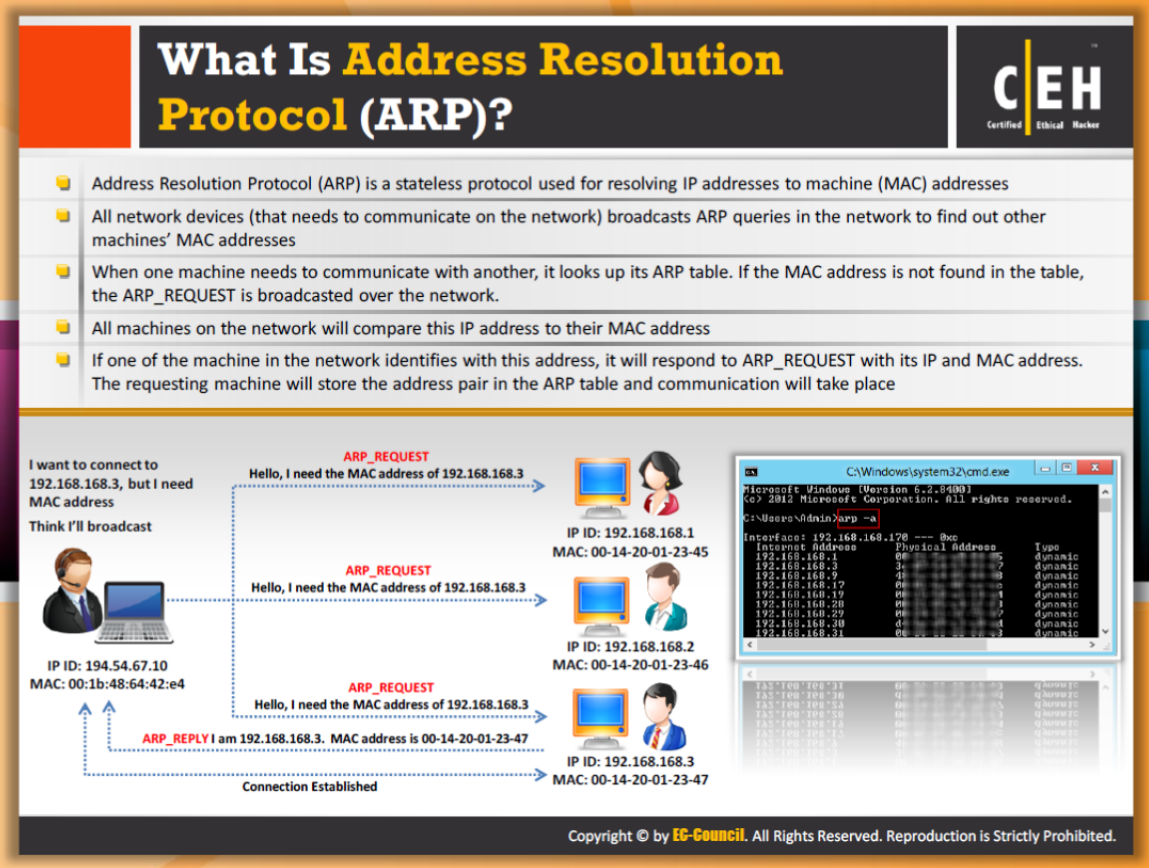
So far, we have discussed two sniffing techniques: MAC attacks and DHCP attacks. Now, we will discuss ARP poisoning. In an ARP poisoning attack, an attacker modifies the MAC address in the ARP cache due to which the corresponding IP address is pointed to another machine. Using this technique, the attacker can steal sensitive information, prevent network and web access, and perform DOS and man-in-the-middle attacks.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This section describes Address Resolution (ARP) protocol, various ARP spoofing techniques, ARP spoofing attacks, threats of ARP poisoning, various ARP poisoning tools, and ways to defend against ARP poisoning.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Address Resolution Protocol (ARP)?

ARP (Address Resolution Protocol) is a **TCP/IP protocol** that maps IP network addresses to the addresses (**hardware addresses**) used by a data link protocol. Using this protocol, you can easily get the MAC address of any device within a network. Apart from the switch, the host machines also use the **ARP protocol** for getting **MAC addresses**. ARP is used by the host machine when a machine wants to send a packet to another device where it has to mention the destination MAC address in the packet sent, so in order to write the destination MAC address in the packet the host machine should know the MAC address of the destination machine. The MAC address table (**ARP table**) is maintained even by the operating system. The following process is performed by ARP for obtaining the MAC address:

- An ARP request packet is generated by source machine with source MAC address, source IP address, and destination IP address and sends it to switch.
- The incoming packet will be received by the switch after which it reads the MAC address of the source and checks its MAC address table; if the entry is found for the packet at incoming port, then it checks its MAC address with the source MAC address and updates it. If it does not find the entry, then the switch adds an entry for the incoming port with the MAC address.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Each and every ARP request packet is broadcasted in the network, so switch the broadcast ARP REQUEST packet in network. (Broadcasts are those packets that are sent to everyone in network except the sender.)
- Each and every device in the network, after receiving the ARP packet, will compare their respective IP address with the destination IP address in that packet.
- Only the system whose IP address matches the destination IP address will reply with ARP reply packet.
- The ARP reply message is then read by the switch and in turn adds the entry in its ARP table, and communication will take place.

To explain the ARP protocol in detail, consider an example that shows two host computers on a LAN; the host names, IP addresses, and MAC addresses are as follows:

HostName	IP	MAC
A	194.54.67.10	00:1b:48:64:42:e4
B	192.168.168.3	00-14-20-01-23-47

Before communicating with host B, host A will first check whether or not host B's MAC address has been recorded in the ARP cache. After checking the entire ARP cache, if it found that the MAC address has been recorded, then you can communicate directly. Otherwise, host A has to access host B's MAC addresses through ARP protocol. Host A asks all the hosts on the LAN in the following way:

Hello, who is 192.168.168.3? This is 194.54.67.10. My MAC address is 00:1b:48:64:42:e4. I need your MAC address." Here, host A sends the Broadcast - Request data packet to host B. As soon as host B receives "the ARP Broadcast: Request packet" from host A, it then immediately saves the corresponding relation between host A's IP address and MAC address to its ARP cache. Then an “ARP Non-Broadcast: Reply packet" is sent to host A, saying: "Hey, this is 192.168.168.3; my MAC address is 00-14-20-01-23-47." Once the reply from host B is received by host A, it will save the corresponding relation between host B's IP address and MAC address to its ARP cache. Then, a communication is established between these two hosts; as a result they communicate with each other.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

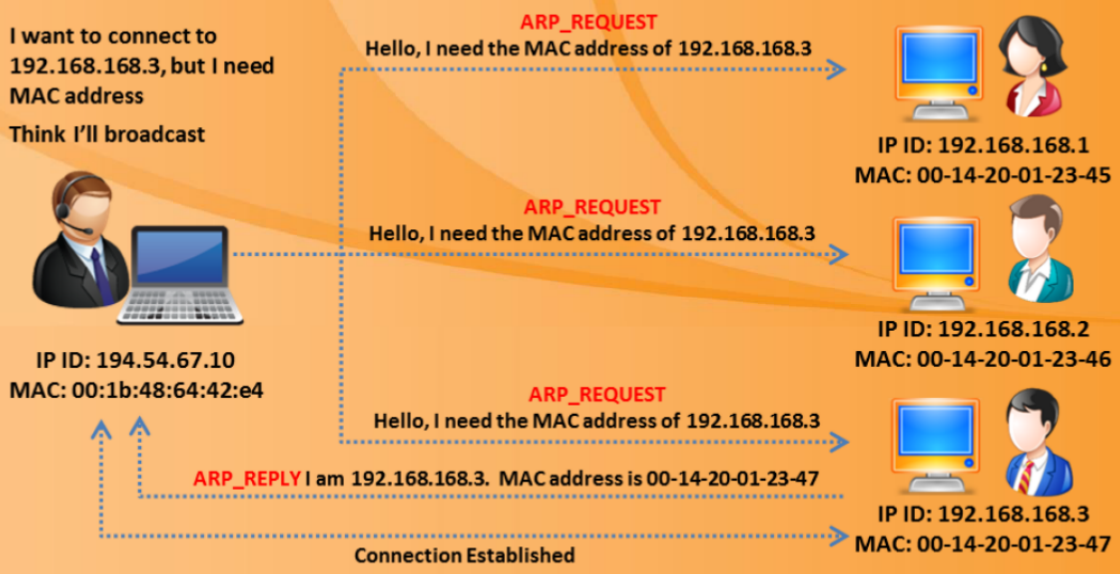
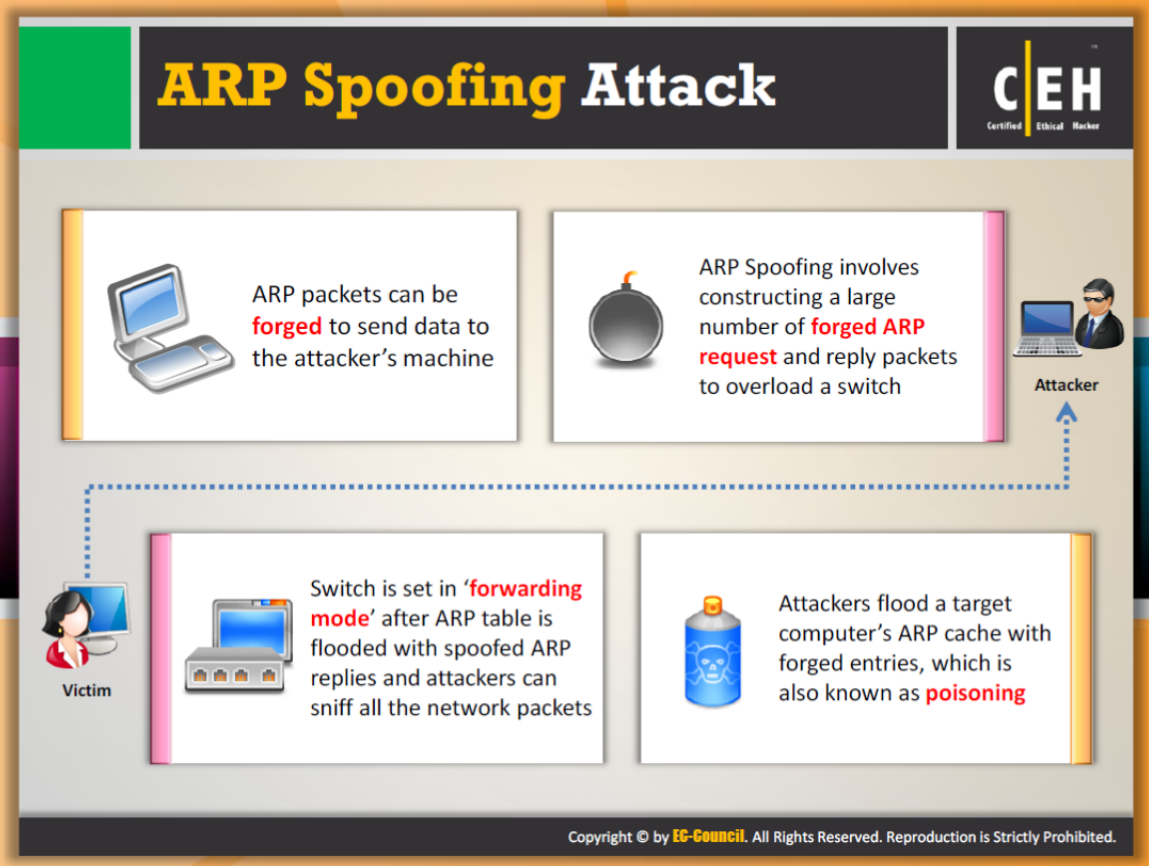


FIGURE 8.29: How ARP Works

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Spoofing Techniques

A host computer saves and updates the local ARP cache when it receives an "**ARP request**" or "**ARP Reply**" packet. Any host on a LAN can counterfeit ARP packets freely because ARP protocol doesn't require authentication. Attackers can use this inherent flaw as an advantage and can compromise the host or network.

Assume there are three host computers on a LAN whose host names, IP addresses, and MAC addresses are as follows:

Host Name	IP	MAC
PC01	10.0.0.8	h3-79-k3-46-v8-64
PC02	10.0.0.6	78-e6-d4-34-h2-25
Router/Gateway	10.0.0.4	c6-24-s8-45-n4-92

The ability to associate any IP address with any MAC address provides attackers with the ability to launch many attack vectors such as denial of service, man-in-the-middle, and MAC flooding.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

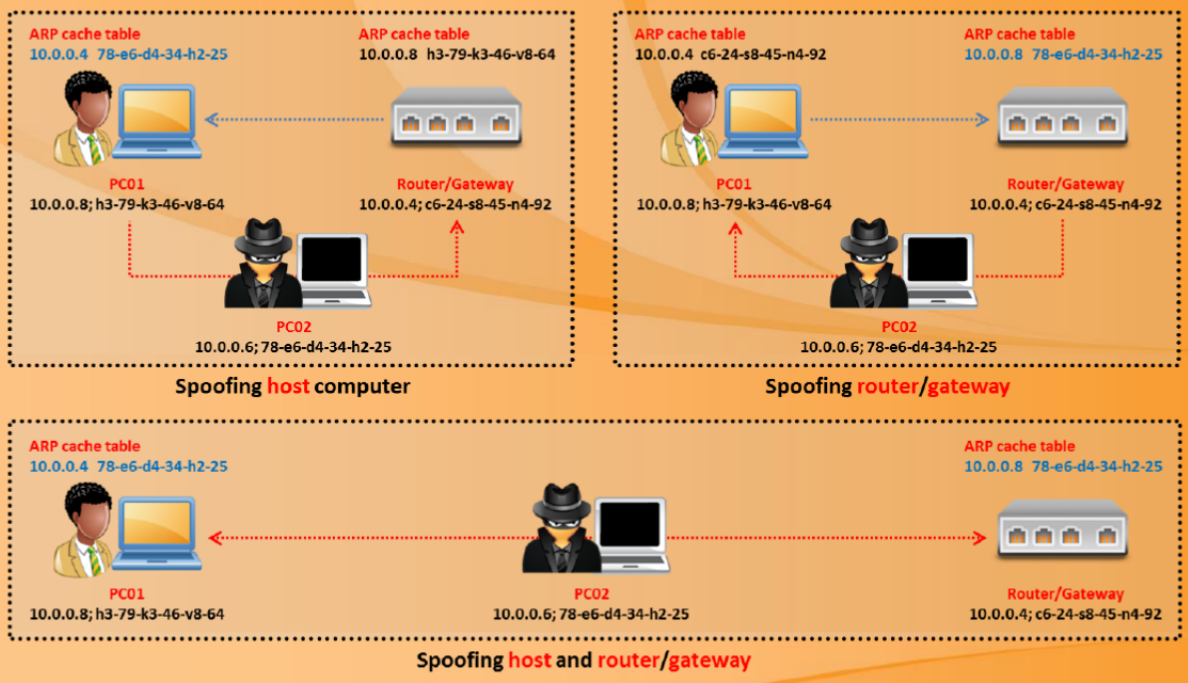
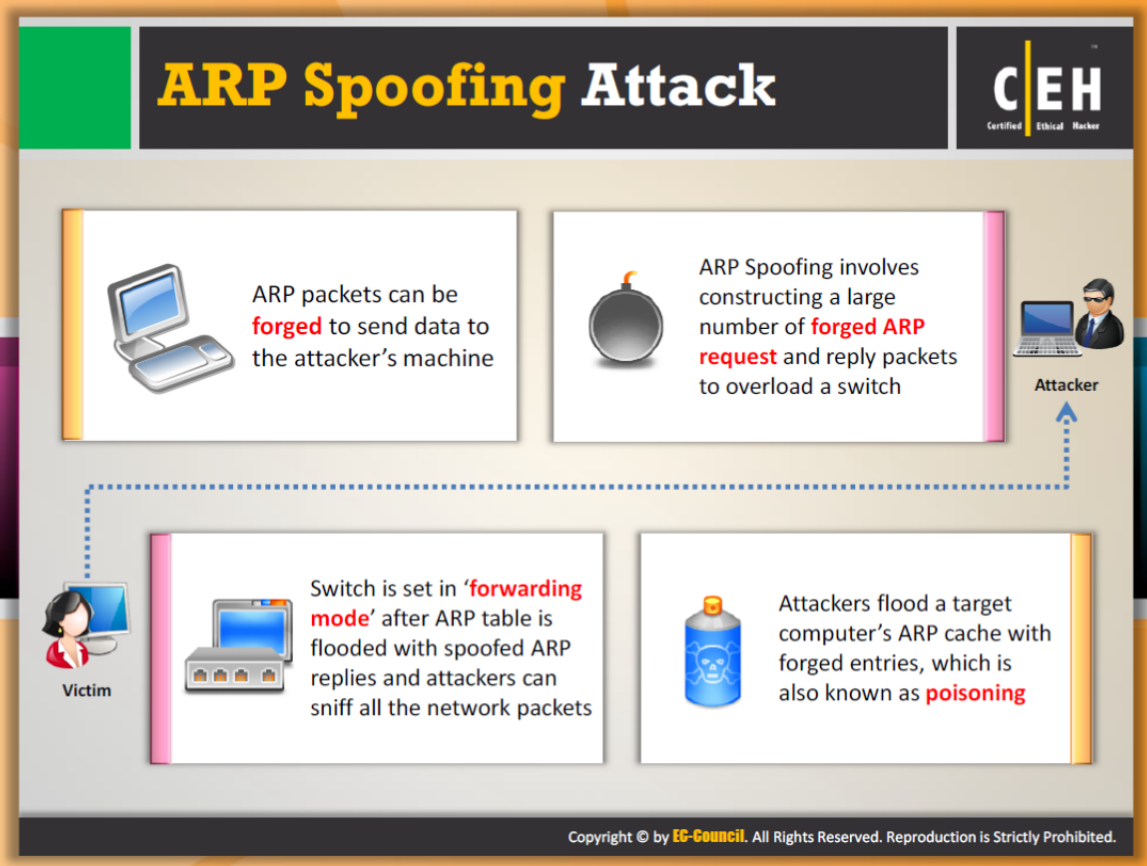


FIGURE 8.30: ARP Spoofing Techniques

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Spoofing Attack

ARP resolves IP addresses to the MAC (hardware) address of the interface to send data. If the machine sends an **ARP request**, it normally considers that the ARP reply comes from the right machine. ARP provides no means to verify the authenticity of the responding device. In fact, many operating systems implement ARP so trustingly that devices that have not made an ARP request still accept ARP replies from other devices.

An attacker can craft a malicious ARP reply that contains **arbitrary IP** and **MAC addresses**. Since the victim's computer blindly accepts the ARP entry into its ARP table, an attacker can force the victim's computer to think that any IP is related to the MAC address he or she wants. An attacker can then broadcast his or her **fake ARP reply** to the victim's entire network.

An attacker may abuse ARP poisoning for capturing the packets between two systems in the network. For instance, the attacker may want to see all the traffic between the victim's computer, 192.168.1.21, and the Internet router, 192.168.1.25. The attacker begins by sending a malicious ARP reply (for which there was no previous request) to the router, associating his or her computer's MAC address with 192.168.1.21. The router confuses the attacker's computer with the victim's computer. Then, he or she sends a malicious ARP reply to the computer, associating his or her MAC address with 192.168.1.25. The victim's machine thinks the attacker's computer is the router. Finally, the attacker enables the operating system feature called IP forwarding to forward any network traffic it receives from the victim's computer to the

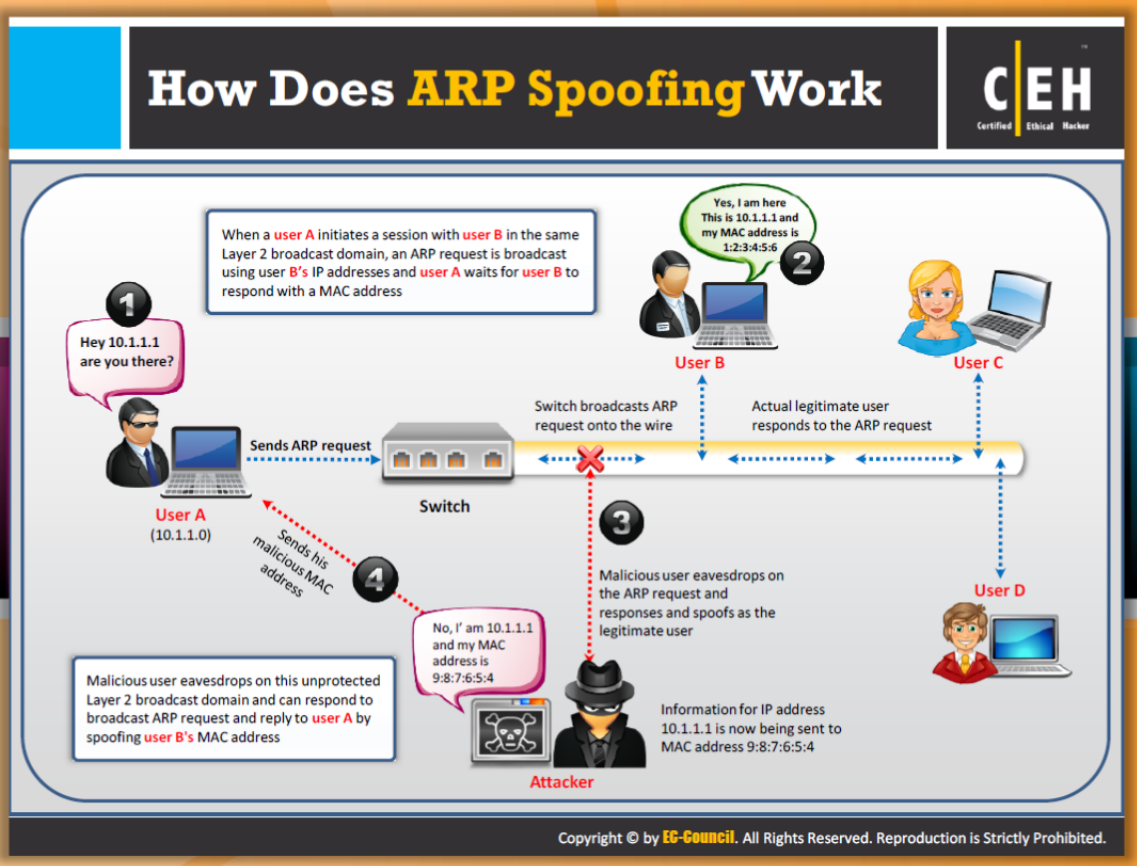
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

router. Now, when the victim is online, the system forwards the network traffic to the attacker's system, and from there it transfers it to the real router. Since the attacker is still forwarding the traffic to the Internet router, the victim remains unaware that the attacker is intercepting the network traffic and perhaps sniffing clear text passwords.

MAC flooding is an ARP cache poisoning technique aimed at network switches. When the switches in the network are flooded with requests, they change to "hub" mode. In hub mode, the switch becomes too busy to enforce its port security features and, therefore, broadcasts all network traffic to every computer in the network.

When the switch is working as a hub, the attacker can overload many vendors' switches and can packet sniff the traffic by flooding a switch's ARP table with spoofed ARP replies.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How Does ARP Spoofing Work?

Source: http://www.trapezenetworks.com

ARP spoofing is defined as when a legitimate user initiates a session with another user in the same Layer 2 **broadcast domain**, an address resolution protocol (**ARP**) **request** is broadcasted using the recipient's IP address, and the sender waits for the recipient to respond with a MAC address. A malicious user eavesdropping on this unprotected **Layer 2 broadcast** domain can respond to the **broadcast ARP request**, and reply to the sender by spoofing the intended recipient's MAC address.

ARP spoofing is a method of attacking an **Ethernet LAN**. ARP spoofing is carried out by changing the MAC address of the attacker's computer to the MAC address of the target computer. This can be done by updating the target ARP cache with a forged ARP request and reply packet. As the ARP reply has been forged, the target computer sends frames to the attacker's computer where the attacker can modify the frames before sending them elsewhere in a man-in-the-middle attack. In addition, the attacker can also launch a **DoS attack** by associating a nonexistent MAC address to the IP address of the gateway or may sniff the traffic passively and then forward to the target destination.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

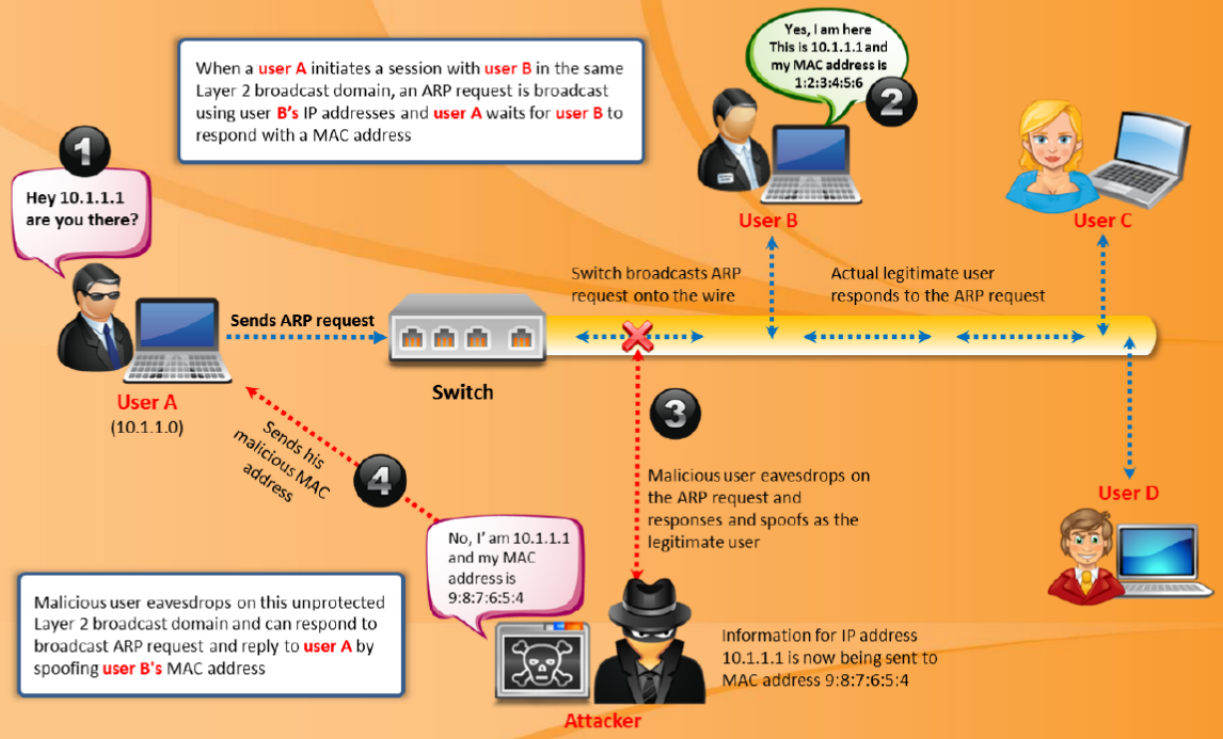


FIGURE 8.31: Working of ARP Spoofing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

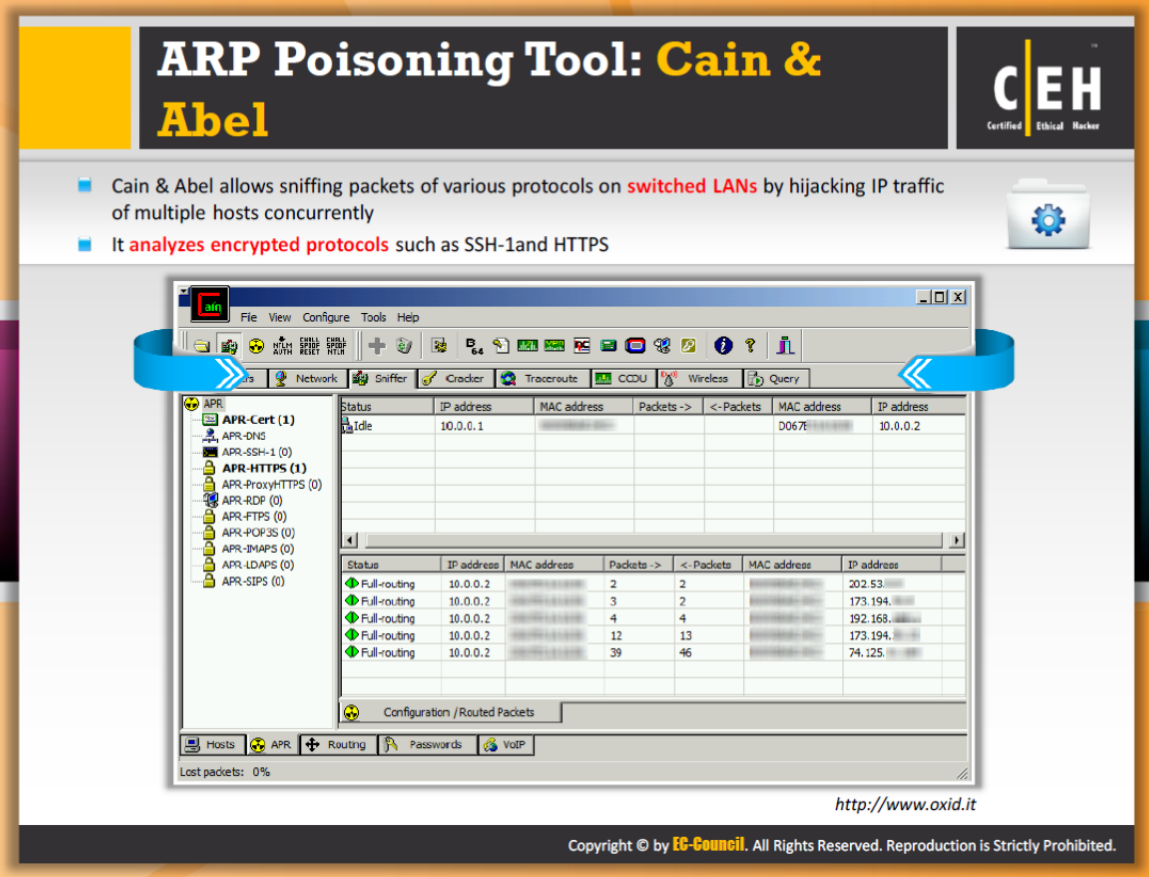
Threats of ARP Poisoning

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

The threats of ARP poisoning include:

- Packet sniffing
- Session hijacking
- VoIP call tapping
- Manipulating data
- Man-in-the-middle attack
- Data interception
- Connection hijacking
- Connection resetting
- Stealing passwords
- Denial-of-service (DoS) attack

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Poisoning Tool: Cain & Abel

Source: http://www.oxid.it

Cain & Abel is a password recovery tool for **Microsoft operating systems**. It contains a new feature APR (ARP poison routing) that enables sniffing on switched LANs and man-in-the-middle attacks. The sniffer can also analyze encrypted protocols such as **SSH-1** and **HTTPS**, and contains filters to capture credentials from a wide range of authentication mechanisms.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

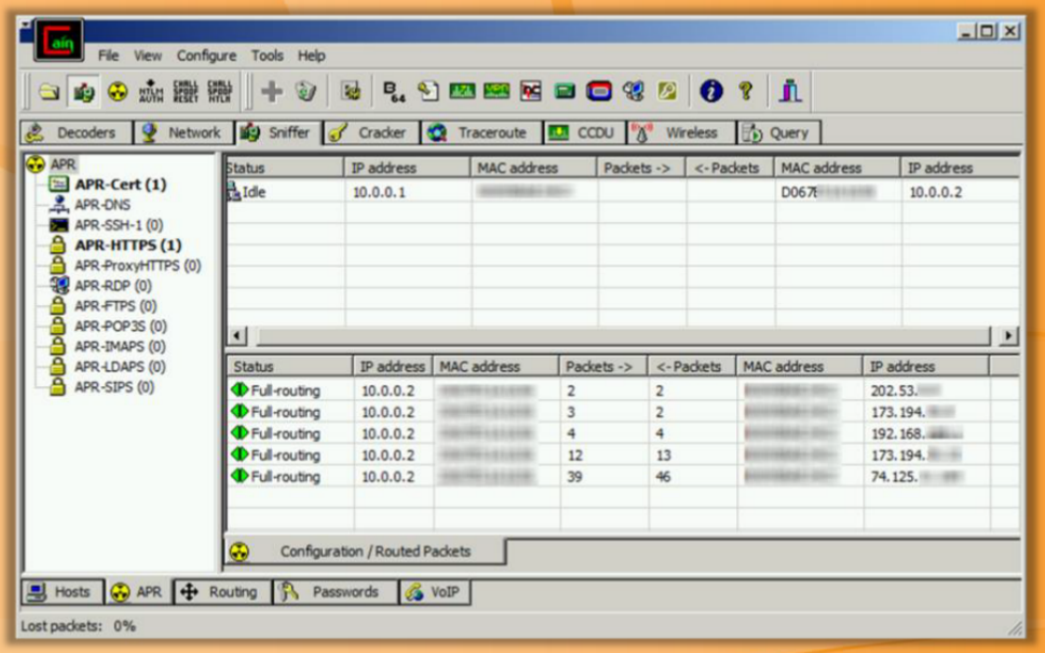
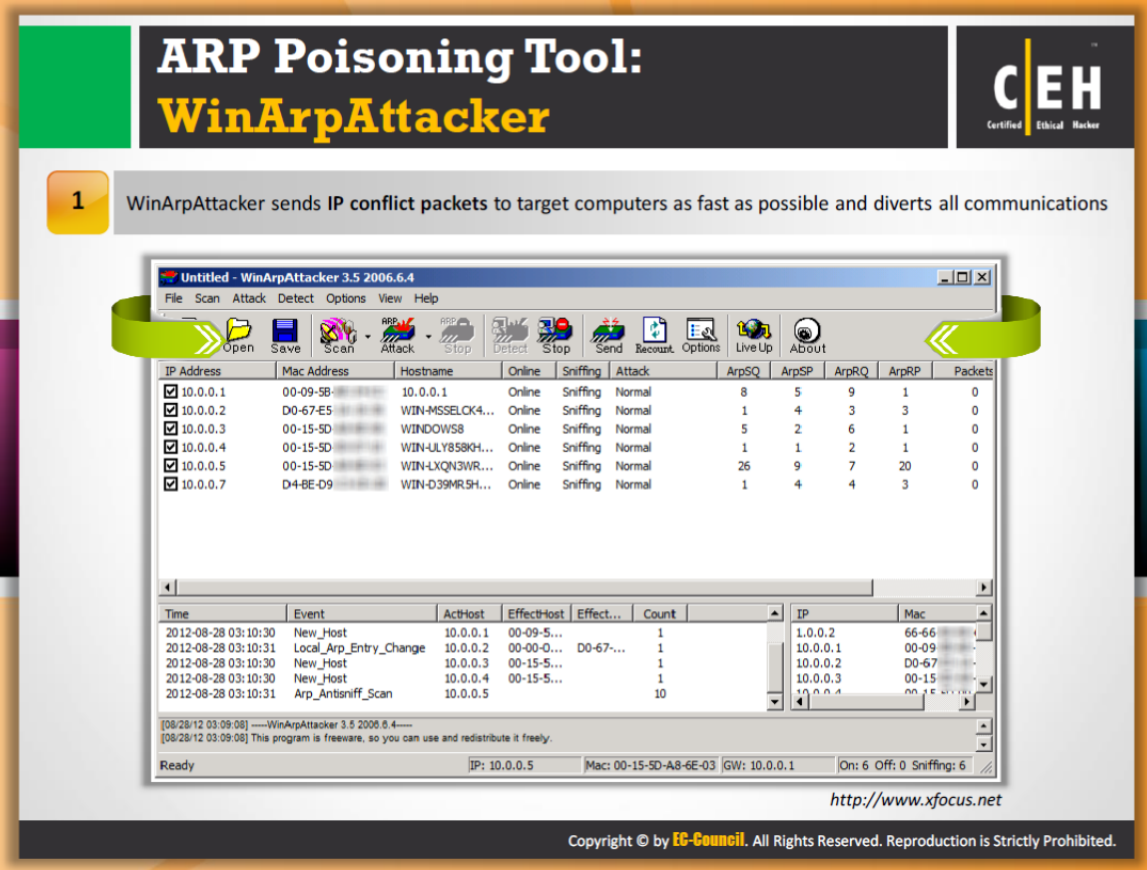


FIGURE 8.32: ARP poison routing using Cain & Abel

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Poisoning Tool: WinArpAttacker

Source: http://www.xfocus.net

WinArpAttacker is a program that can scan and attack computers on a **local area network**. It can scan and show the active hosts on the LAN. It can perform attacking actions such as **ARP flooding**, in which it sends IP conflict packets to target computers and diverts all communications.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

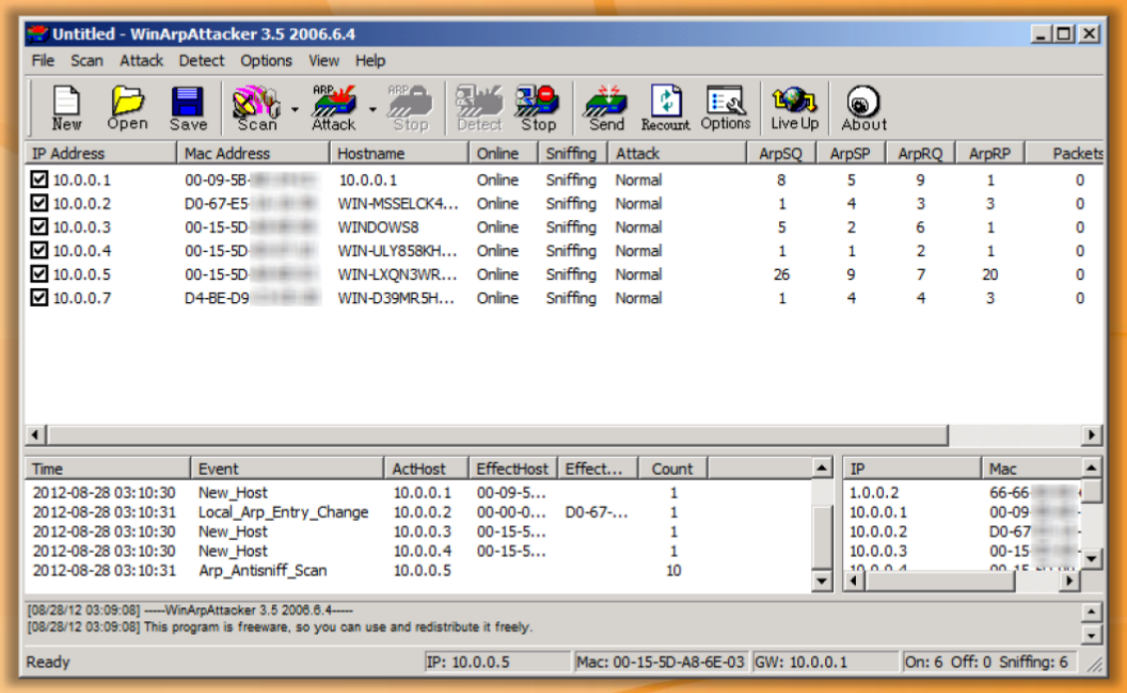
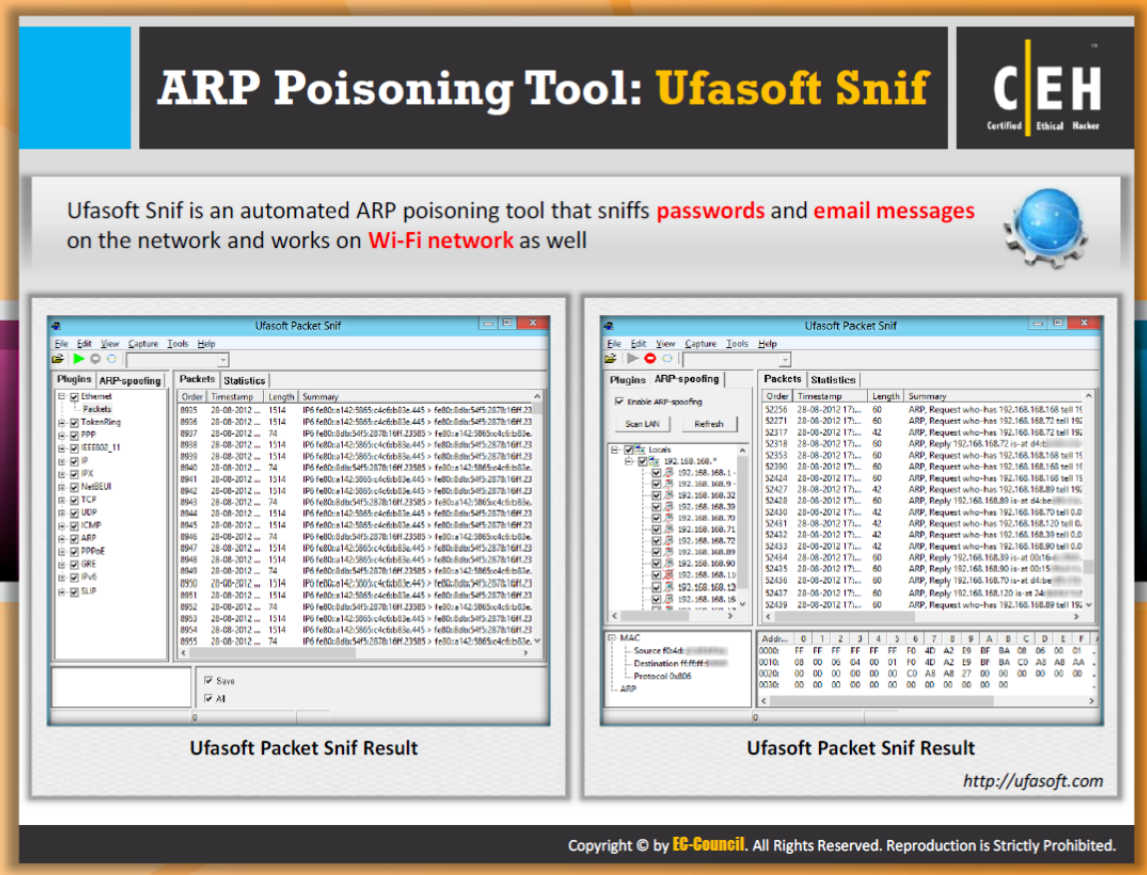


FIGURE 8.33: WinArpAttacker Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Poisoning Tool: Ufasoft Snif

Source: http://ufasoft.com

Ufasoft Snif is an automated ARP poisoning tool that sniffs passwords and email messages on the network and Wi-Fi network, as well. It is designed for capturing and analysis of the packets going through the network. Including **ICQ/IRC/MSN/email Sniffers** (formerly ICQ Sniffer products), this software is designed to intercept ICQ, IRC, and email messages across a LAN. It is possible to **observe** these messages at the same time that real users will receive them. All intercepted messages are stored in files, which can be later processed and analyzed. There are two versions: **IcqSnif** with GUI and console-only **IcqDump**. The functionality is the same, except it is possible to select which machines to **ARP-spoof** exactly in the GUI version. The software is based on the reliable and well-known Ufasoft Sniffer engine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

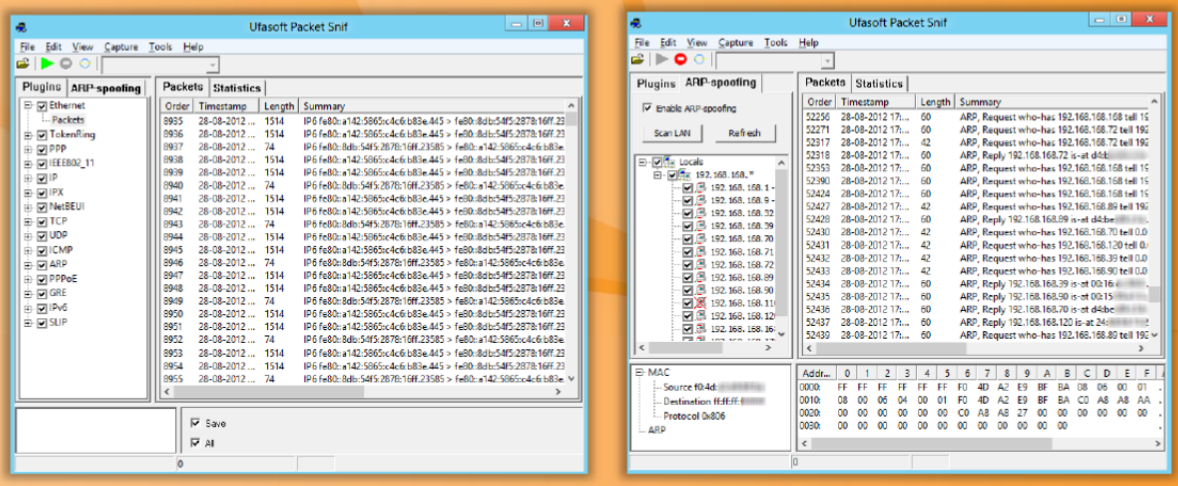
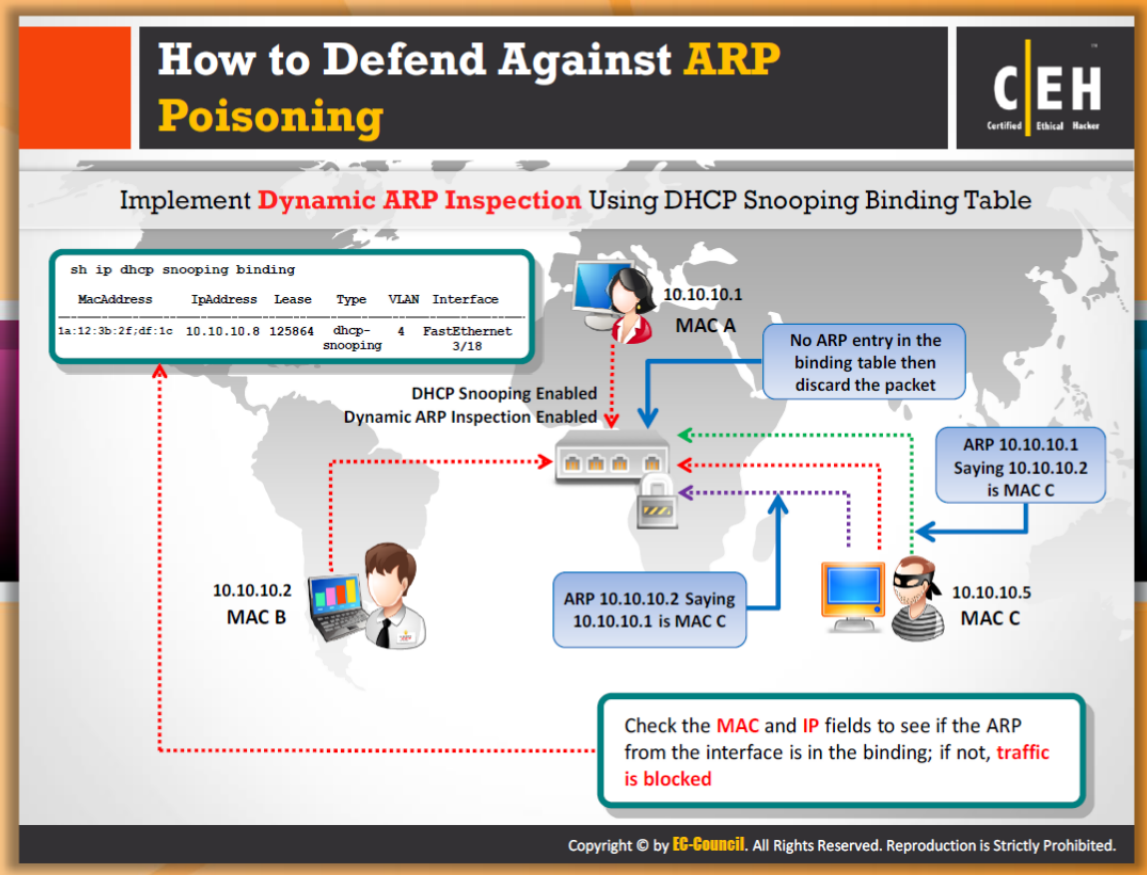


FIGURE 8.34: Ufasoft Packet Snif

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against ARP Poisoning

ARP poisoning attacks can be prevented by implementing **dynamic ARP inspection (DAI)**. DAI is a security feature that allows you to validate Address Resolution Protocol (ARP) packets in a network. When DAI is enabled on a **VLAN**, all ports on the VLAN considered to be untrusted by default. DAI validates the ARP packets using a DHCP snooping binding table. Hence, you must enable DHCP snooping prior to enabling DAI. If you fail to enable **DHCP snooping** before enabling DAI, then no connection among VLAN devices will be established based on ARP. Consequently, a self-imposed denial-of-service may result on any device in that VLAN.

In order to validate the ARP packet, the DAI performs IP to **MAC address** binding inspection stored in the DHCP snooping database before forwarding the packet to its appropriate destination. If any invalid IP to MAC address binding is encountered, then the DAI discards the respective ARP packet. Thus, it eliminates the risk of man-in-the-middle attacks. DAI ensures that only valid ARP requests and responses are relayed.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

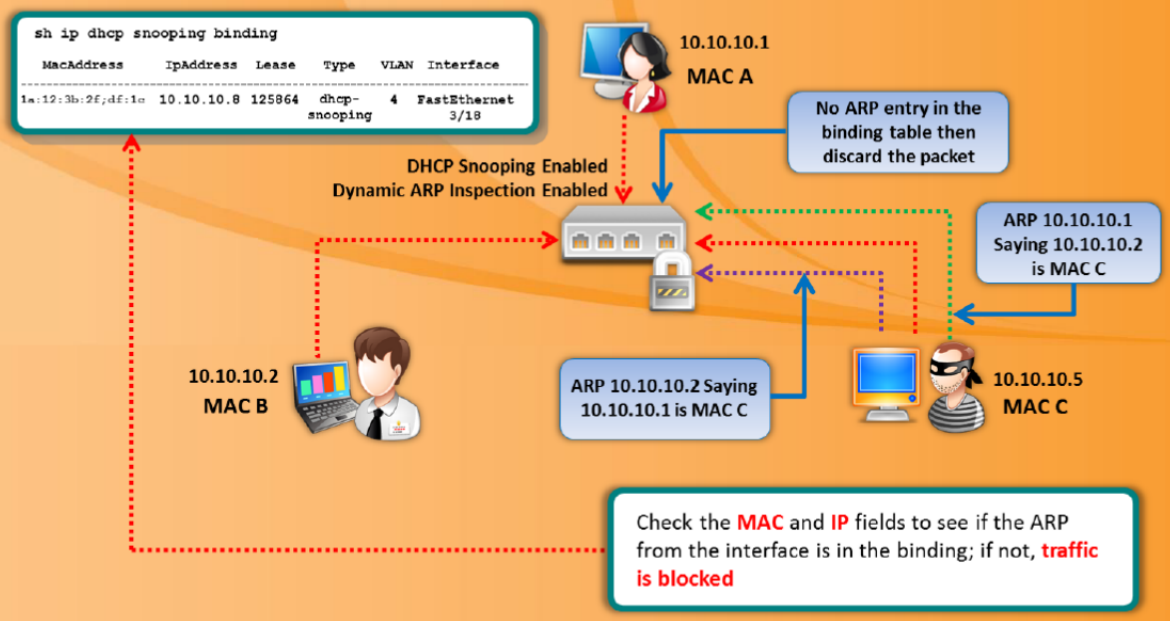
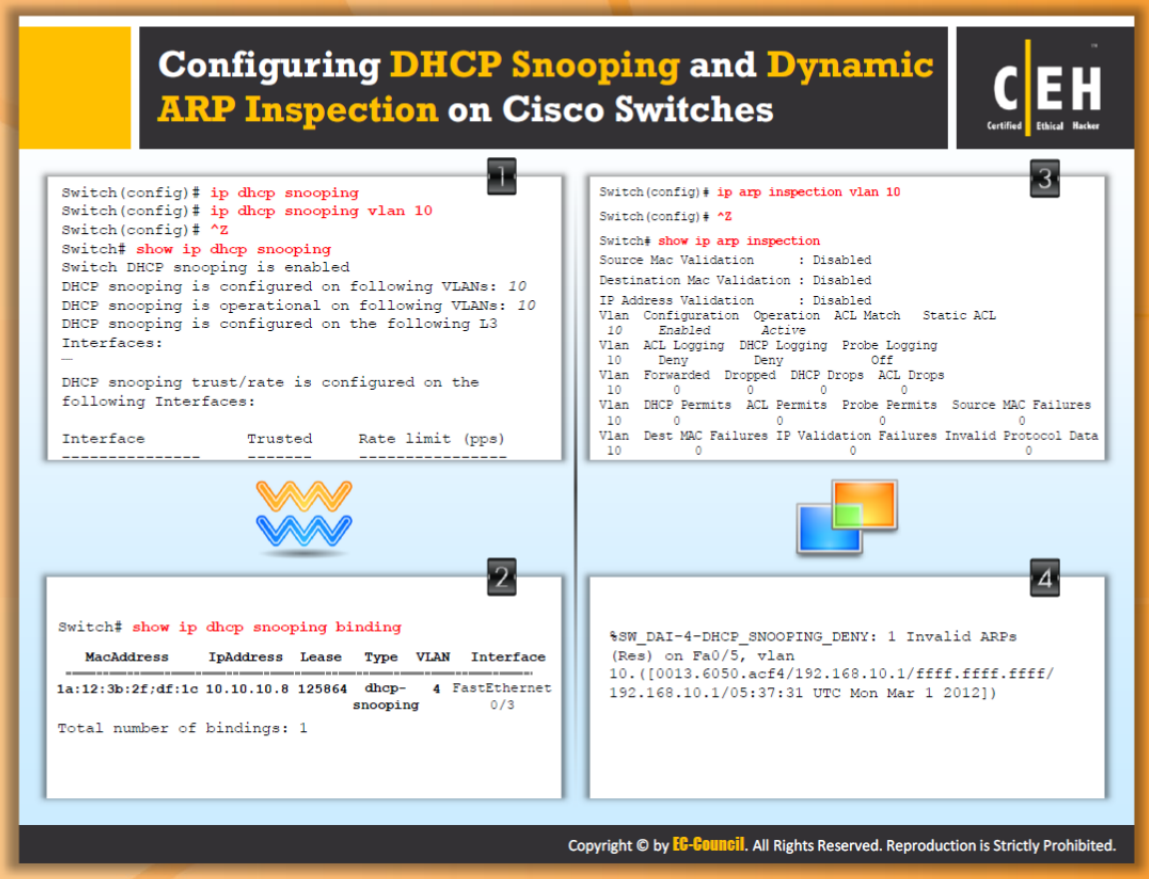


FIGURE 8.35: Working of Dynamic ARP Inspection (DAI)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

As we discussed previously, DHCP snooping must be enabled prior to **enabling dynamic ARP inspection (DAI)**. Therefore, first we need to configure DHCP snooping. DHCP snooping is a security feature that builds and maintains a DHCP snooping binding table and filters untrusted DHCP messages. A Cisco switch with DHCP snooping enabled can inspect **DHCP traffic** flow at a layer two segment and track IP addresses to switch ports mapping.

In order to configure DHCP snooping on a Cisco switch, you need to enable DHCP snooping both globally and per access VLAN. To enable DHCP snooping, execute the following commands:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

FIGURE 8.36: Configuring DHCP Snooping

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)

--- --- ---

If the access switch is functioning only at layer two, then you have to apply the **ip dhcp snooping trust** command to the layer two interfaces in order to designate uplink interfaces as trusted interfaces. This informs the switch that DHCP responses are allowed to arrive on those interfaces.

The DHCP snooping binding table contains the trusted DHCP clients and their respective IP addresses. If you want to see the DHCP snooping table, then execute the following command:

Switch# show ip dhcp snooping binding

It displays the DHCP snooping table. The DHCP snooping table contains the MAC addresses, respective IP addresses, as well as total number of bindings. The following is the DHCP snooping binding table:

MacAddress IpAddress Lease(sec) Type VLAN Interface

--- --- --- --- --- ---

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
1a:12:3b:2f;df:1c   10.10.10.8     125864  dhcp-snooping   4     FastEthernet0/3
Total number of bindings: 1
```

Once you have DHCP snooping binding table, you can start configuring dynamic ARP inspection for the VLAN. If you want to enable dynamic ARP inspection for multiple VLANS, then you need to specify a range of VLAN numbers.

```
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
```

From this ip arp inspection result, it is clear that the source MAC, destination MAC, and IP address are disabled. You can attain even more security by enabling one or more of these additional validation checks. To do so, you need to execute the command `ip arp inspection validate` followed by the address type.

Assume that an attacker with source IP address 192.168.10.1 is connected to VLAN 10 on interface FastEthernet0/5 and sending ARP replies, pretending to be the default router for the subnet in an attempt to initiate a man-in-the-middle attack. The switch with dynamic ARP

inspection enabled inspects these reply packets by comparing them with the DHCP snooping table. The switch then tries to find an entry for the source IP address 192.168.10.1 on port FastEthernet0/5. If no entry is found, then the switch discards these packets.

```
%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])
```

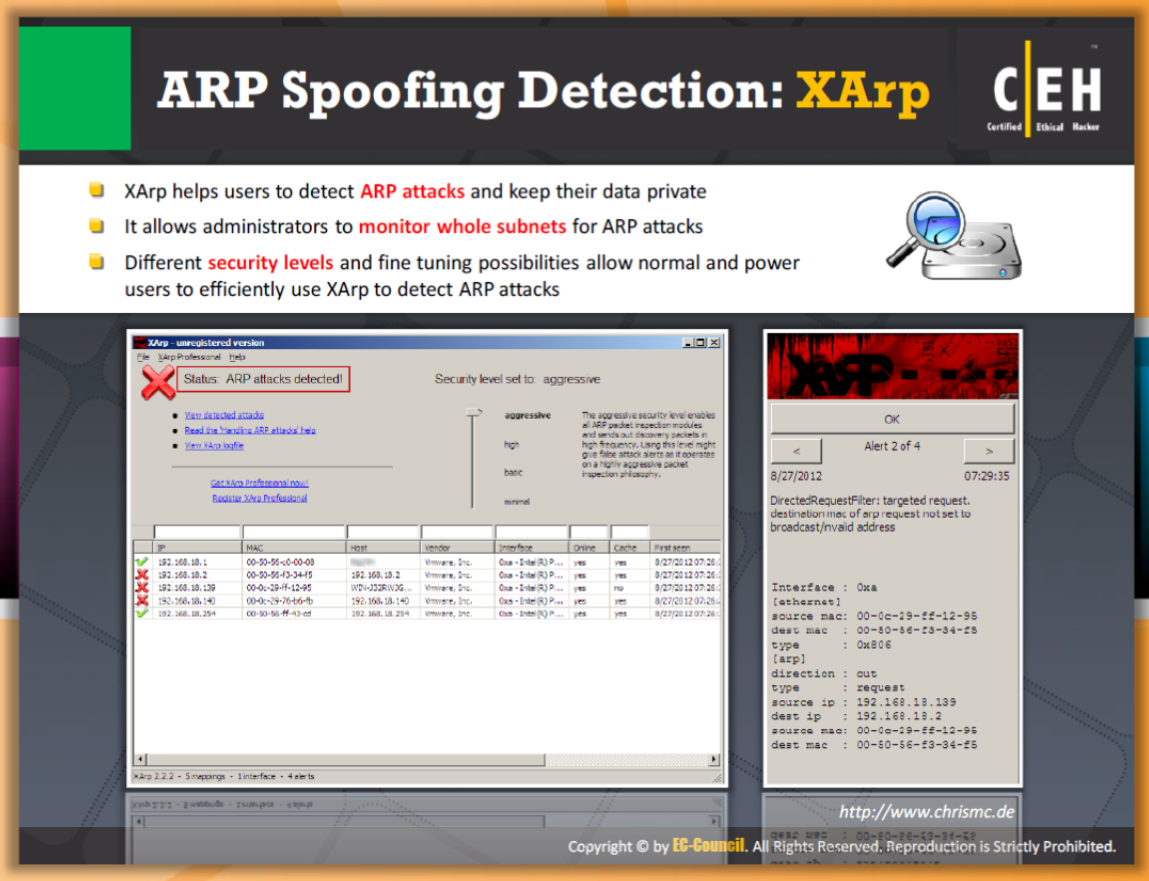
The drop count begins to increase if any packets are discarded. You can see this increase in the drop count in the dynamic ARP inspection output. To see the output, execute the command `show ip arp inspection:`

```
Switch# show ip arp inspection
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
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        30               5           5         0
Vlan  DHCP Permits ACL Permits Probe Permits Source MAC Failures
----  ------------ ----------- ------------ -------------------
10        30              0          0                0
Vlan  Dest MAC Failures IP Validation Failures Invalid Protocol Data
----  ----------------- ---------------------- --------------------
10             0                    0                     0
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ARP Spoofing Detection: XArp

Source: http://www.chrismc.de

XArp is a security application designed to detect **ARP-based attacks**. The **detection mechanism** is based on two techniques: **inspection modules** and **discoverers**. Inspection modules look at each ARP packet and check its correctness and validity in respect to databases they built up. Discoverers actively validate IP-MAC mappings and help to **detect attackers actively**. It helps users to detect ARP attacks and keep their data private. It even allows administrators to monitor whole subnets for ARP attacks. Administrators can use this application to screen the whole subnet for ARP attacks using different security levels and **fine-tuning possibilities**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

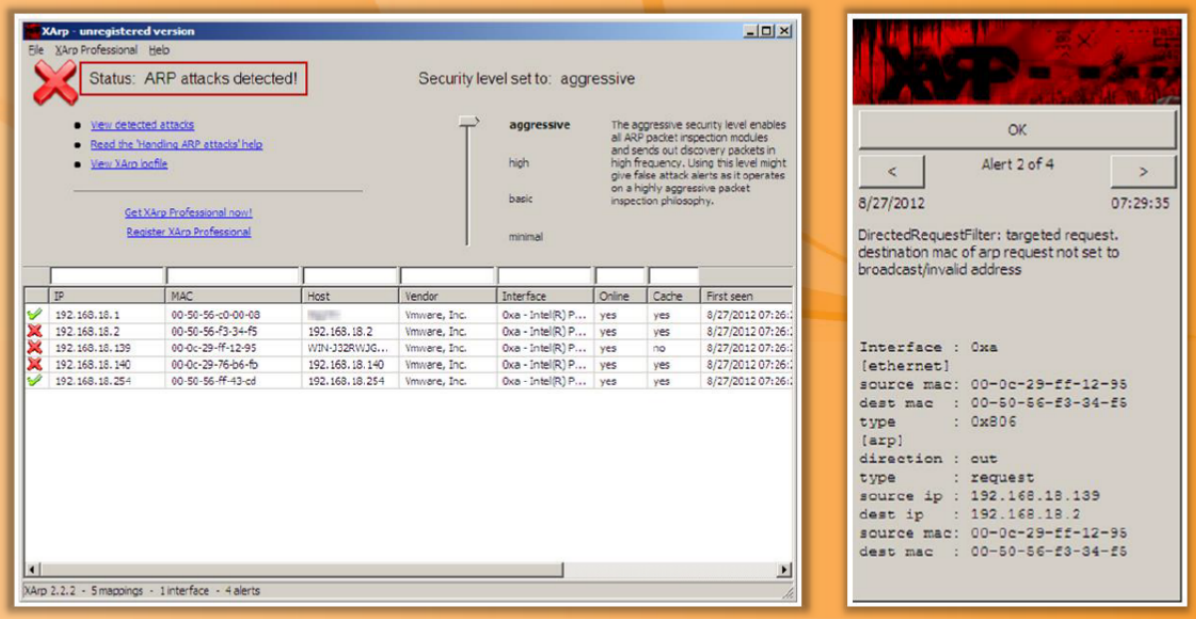
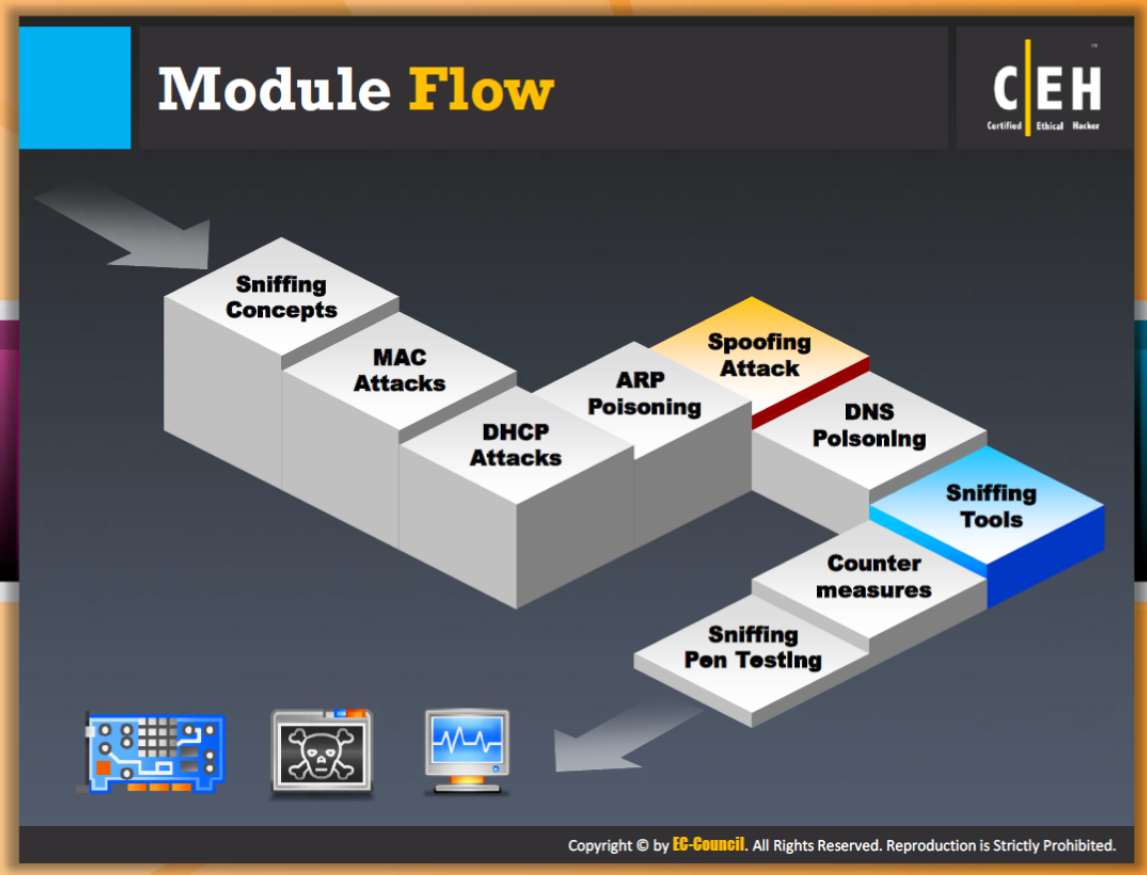


FIGURE 8.37: XArp Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

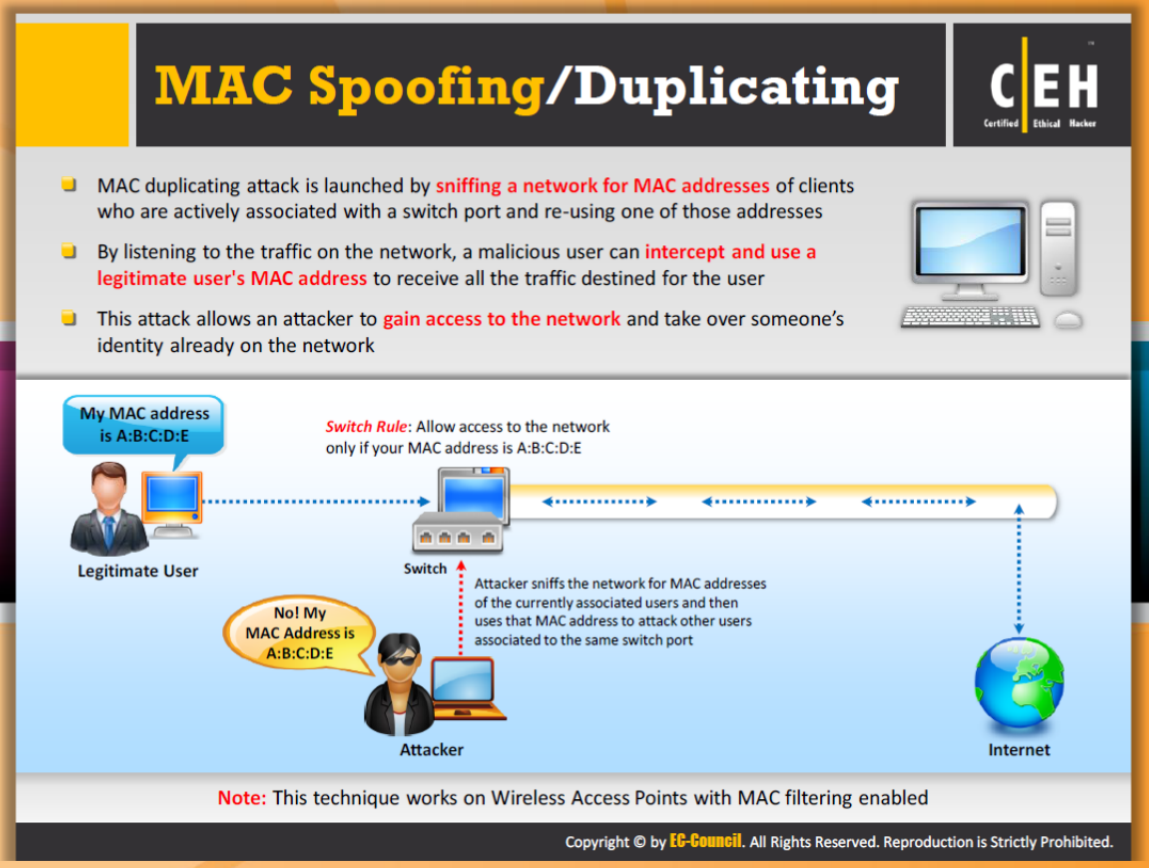


Module Flow

So far, we have discussed sniffing concepts, MAC attacks, DHCP attacks, and ARP poisoning. Now we will discuss spoofing attacks, a means to sniff the network data. This section highlights the threats of spoofing attacks and describes MAC spoofing/duplicating, various spoofing techniques, IRDP spoofing, and a way to defend against MAC spoofing.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Spoofing Attack Threats

Spoofing may refer to any threat that allows an attacker to pretend to be someone who is legitimate or authorized. MAC spoofing and IRDP are the two major threats of spoofing attacks.

MAC Spoofing

Intrusion detection systems generally use MAC addresses for **authorization**. These physical MAC addresses are permanent by design but can be changed on most hardware. MAC spoofing is the means of forging the source MAC address. This can be done by changing the information in the packet's header. Though it is intended for the purpose of legitimately requiring connectivity after hardware failure, it is associated with severe security risks. Through **MAC spoofing**, attackers can gain access to the network by taking over the identity of a legitimate user of the network.

IRDP Spoofing

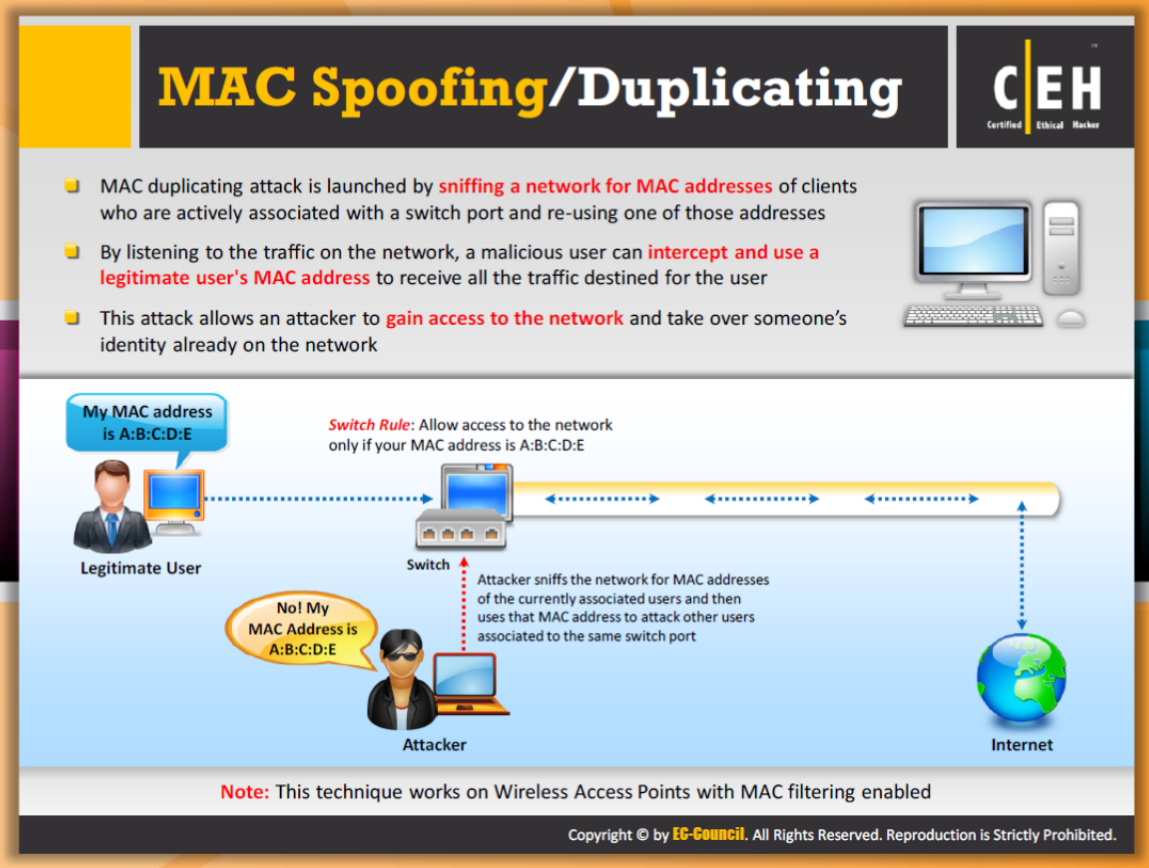
IRDP **(ICMP Router Discovery Protocol)** is an extension to the ICMP protocol. It allows hosts to discover routers on their networks by listening for "**router advertisement**" broadcasts. When a host receives router advertisement messages, the routing table of the respective host

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

may change. Hosts with IRDP can be easily spoofed to change their routes, as IRDP does not check for authenticity of router advertisement messages.

An attacker can replace the default route of the data flow with the route of attacker's choice by sending spoofed IRDP router advertisement messages to the host. This may led to denial-of-service, sniffing, and/or man-in-the-middle attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MAC Spoofing/Duplicating

A Media Access Control address (MAC address) is a **unique identifier** assigned to network interfaces for communications on the **physical network segment**. In general terms, duplicating refers to the process of making an exact copy of the original, with characteristics that are the same as the original. This is also the case with the MAC address. **MAC duplicating** refers to spoofing the MAC address with the MAC address of a legitimate user on the network.

A MAC duplicating attack involves sniffing a network for MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port. Then the attacker spoofs his or her own MAC address with the MAC address of the legitimate client. Once if the spoofing is successful, then the attacker can receive all the traffic destined for the client. Thus, an attacker can gain access to the network and take over someone's identity who is already on the network.

The following diagram explains how to perform a **MAC spoofing/duplicating attack**:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

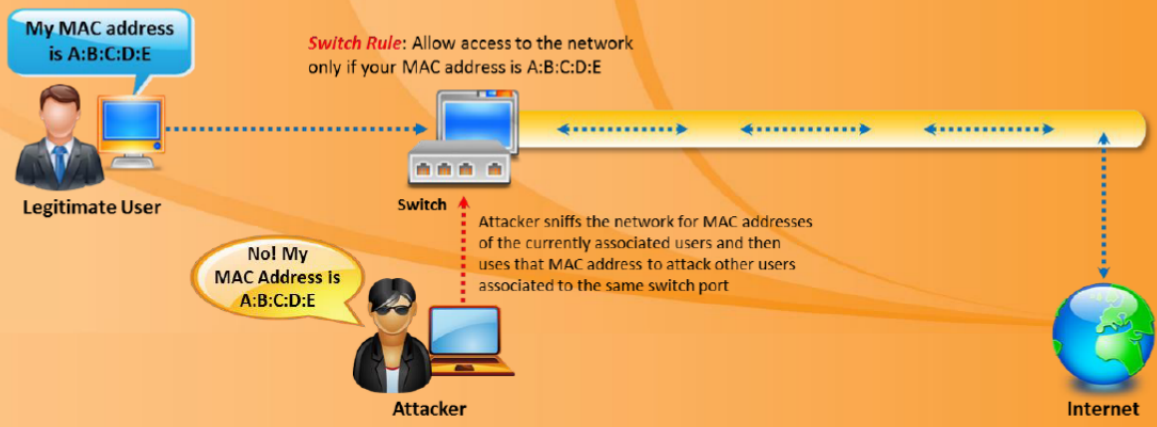
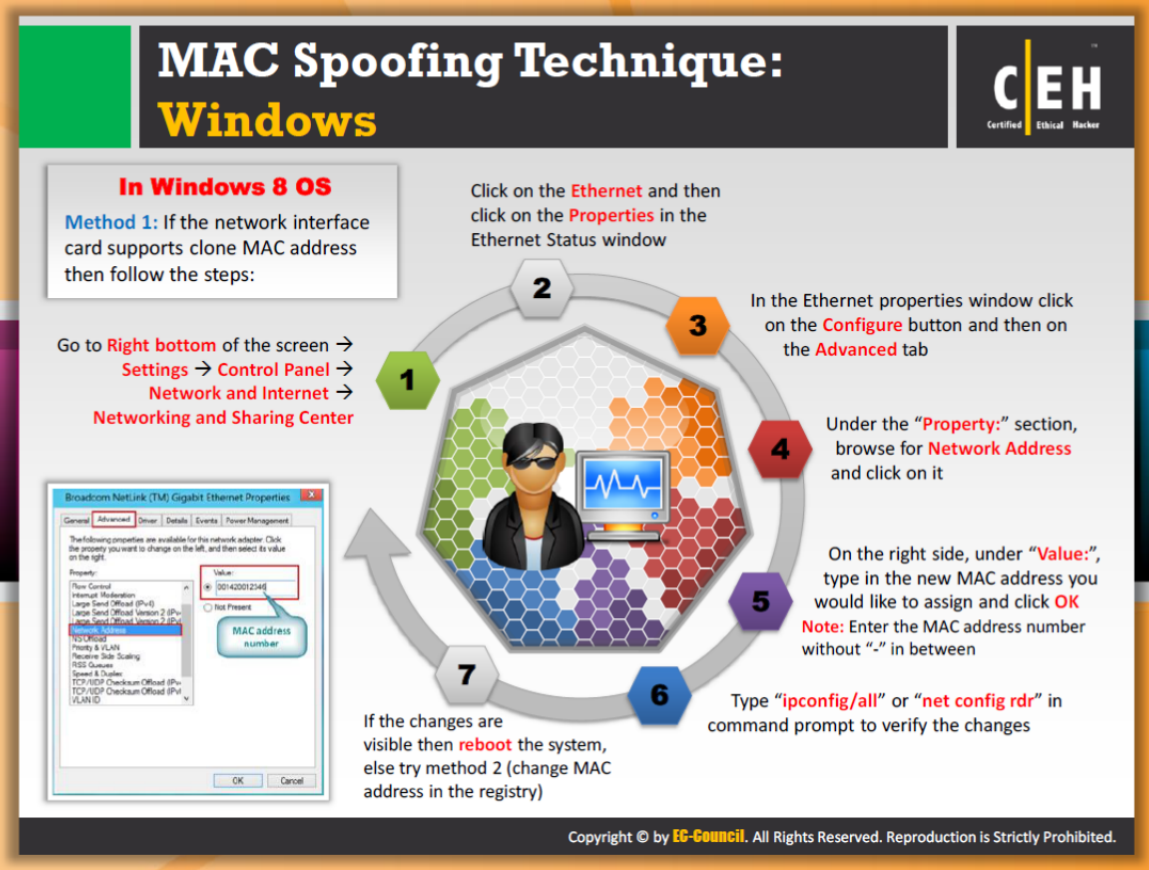


FIGURE 8.38: How to Perform MAC Spoofing

Note: This technique works on Wireless Access Points with MAC filtering enabled.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MAC Spoofing Technique: Windows

In Windows 8 OS

MAC spoofing can be performed in many ways. Changing the router's MAC address is one way. But this can be applied only on a few routers, as not all routers support changing their MAC address. The routers that support MAC addresses changes are referred to as "clone MAC addresses." Another way is changing a MAC address on a Cisco router by using the MAC-address command in interface configuration mode.

Method 1:

This method depends on the type of network interface card (NIC). Follow the steps here to perform MAC spoofing if the network interface card supports cloning MAC address:

- From the lower-right of the screen, select **Settings → Control Panel → Network and Internet → Networking and Sharing Center**.
- Click the Ethernet and then click **Properties** in the Ethernet Status window.
- In the Ethernet properties window, click the **Configure** button and then the **Advanced** tab.
- Under the **Property** section, browse for **Network Address** and click it.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- On the right side, under **Value**, type the new MAC address you would like to assign and click **OK**.

Note: Enter the MAC address number without "-" in between.

- Type "ipconfig/all" or "net config rdr" in the command prompt to verify the changes.
- If the changes are visible, then reboot the system; if not, try method 2 (change the MAC address in the registry).

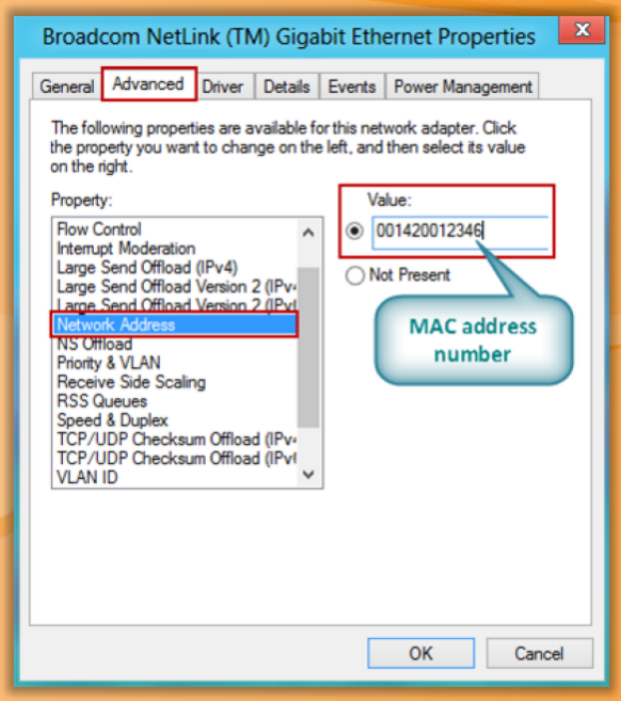
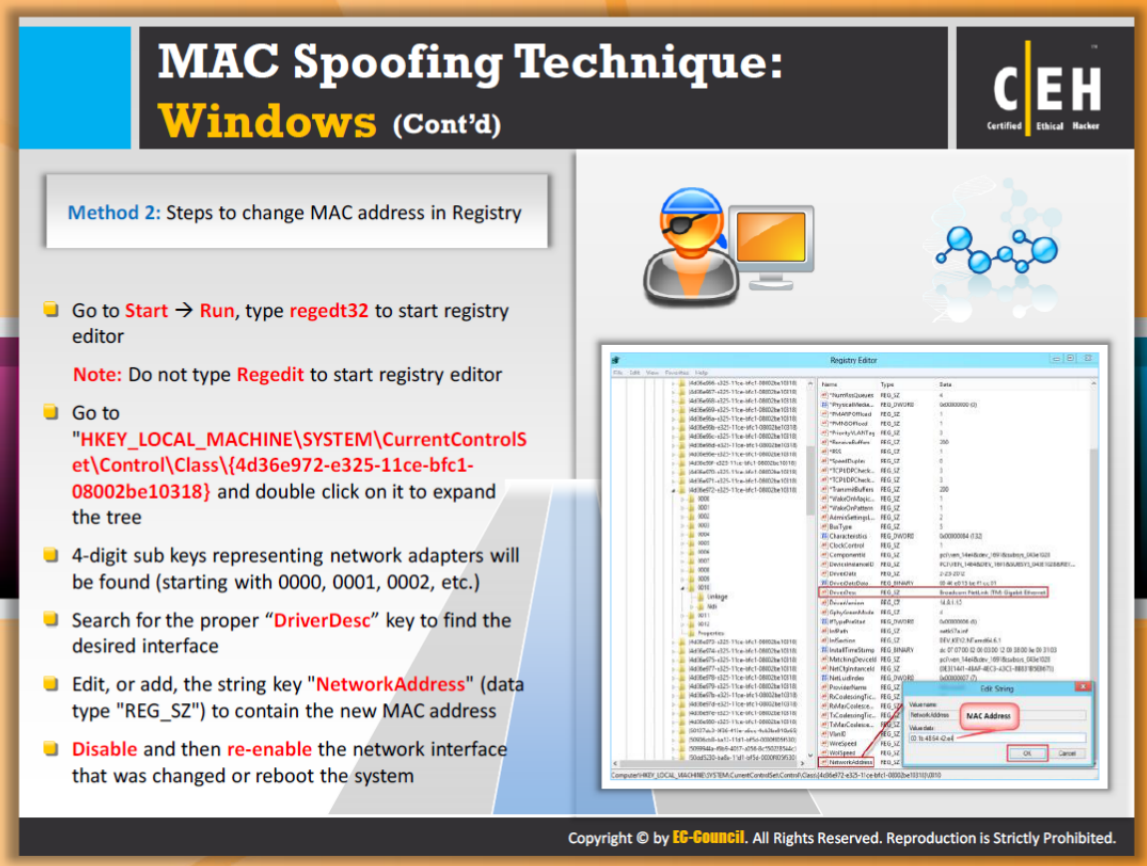


FIGURE 8.39: MAC Spoofing Technique In Windows

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MAC Spoofing Technique: Windows (Cont'd)

In Windows 8 OS

Method 2:

MAC spoofing can also be performed by editing the registry. This method is preferred when the network interface card (NIC) doesn't support cloning MAC addresses. Follow these steps to change the MAC address by editing the registry:

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

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

- Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318} and double-click it to expand the tree.
- Four-digit subkeys representing network adapters will be found (starting with 0000, 0001, 0002, etc.).
- Search for the proper "DriverDesc" key to find the desired interface.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- 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.

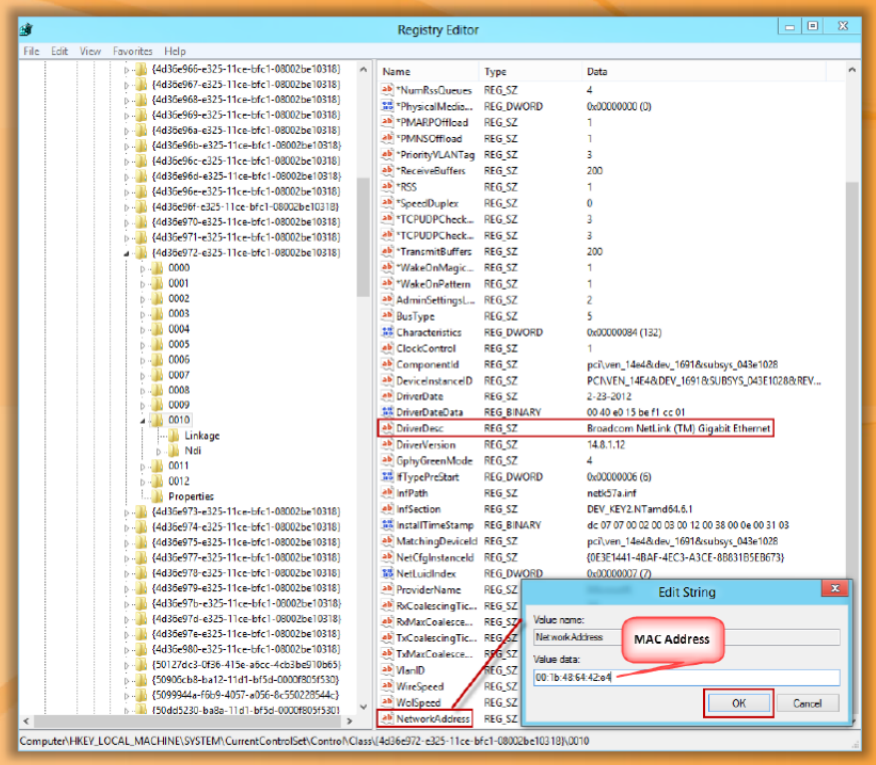
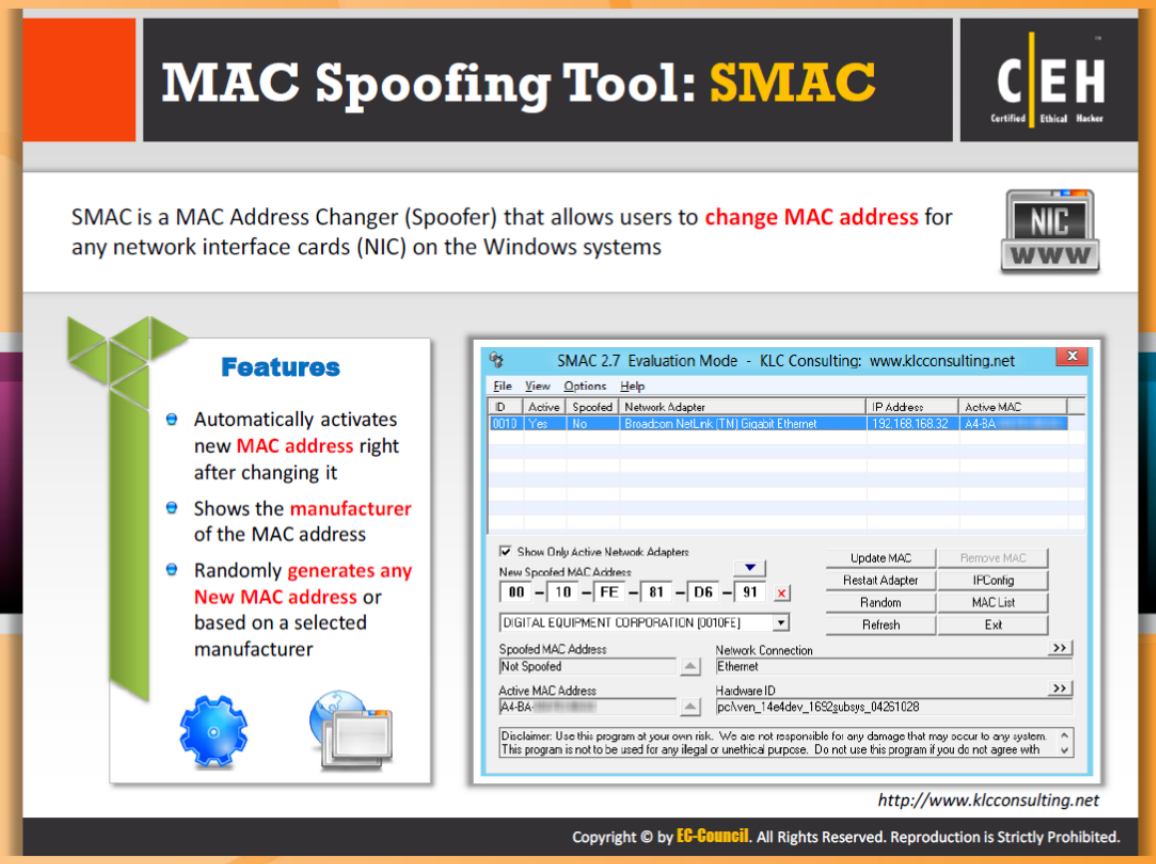


FIGURE 8.40: MAC Spoofing Technique In Registry Editor

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MAC Spoofing Tool: SMAC

Source: http://www.klcconsulting.net

SMAC is a MAC address changer (spoofer) that allows you to change MAC addresses for any NICs) on Windows VISTA, XP, 2003, and 2000 systems. It changes only **software-based MAC addresses**; it doesn't change hardware burned-in MAC addresses. The new MAC addresses sustain reboots. It features MAC address lookup. It allows you to see either all or only active network adapters, and randomly generate new MAC addresses or those based on a selected manufacturer. It also allows you to restore the original MAC address by removing the **spoofed MAC address**.

You can find information about NIC that includes Device ID, Active Status, NIC description, NIC Manufacturer, Spoofed status (Yes/No), IP Address, Active MAC addresses, Spoofed MAC Address, NIC Hardware ID, NIC Configuration ID, and so on. This tool helps you to protect your identity on Wi-Fi networks. It also helps you in troubleshooting network problems, testing intrusion detection/prevention systems (**IDS/IPSs**), testing incident response plans, build high-availability solutions, recovering (MAC-address-based) software licenses, and etc.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

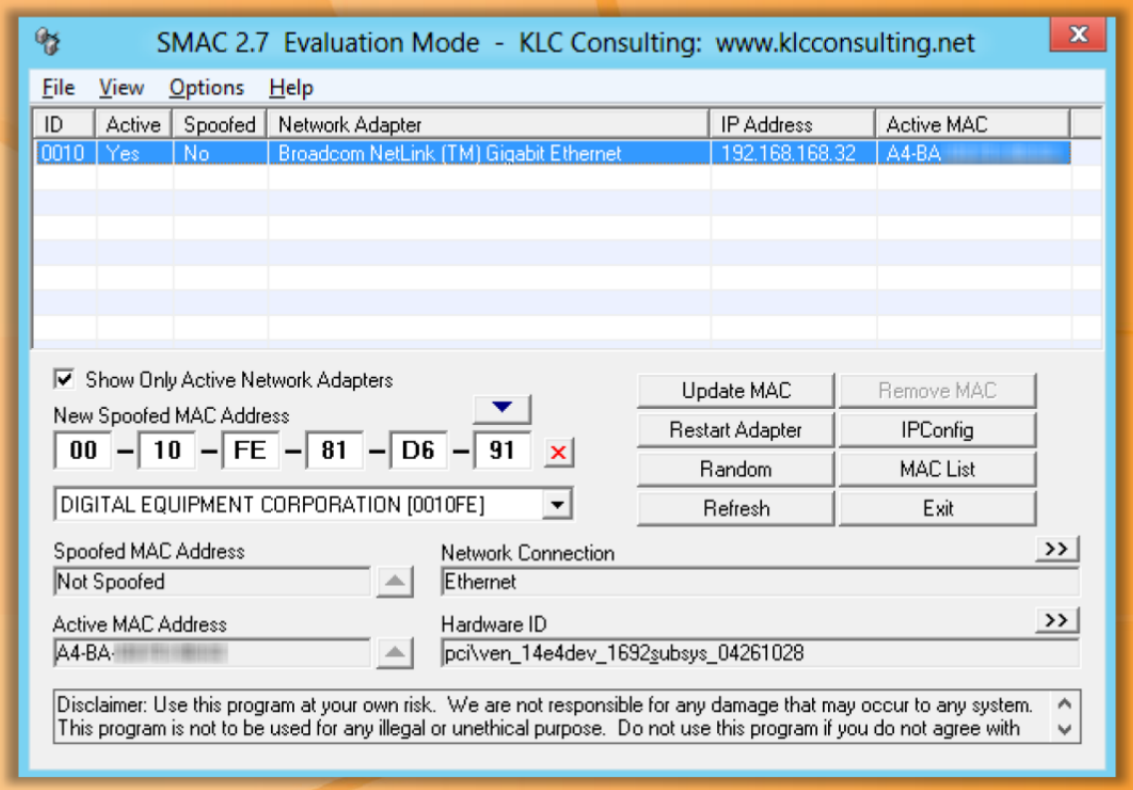
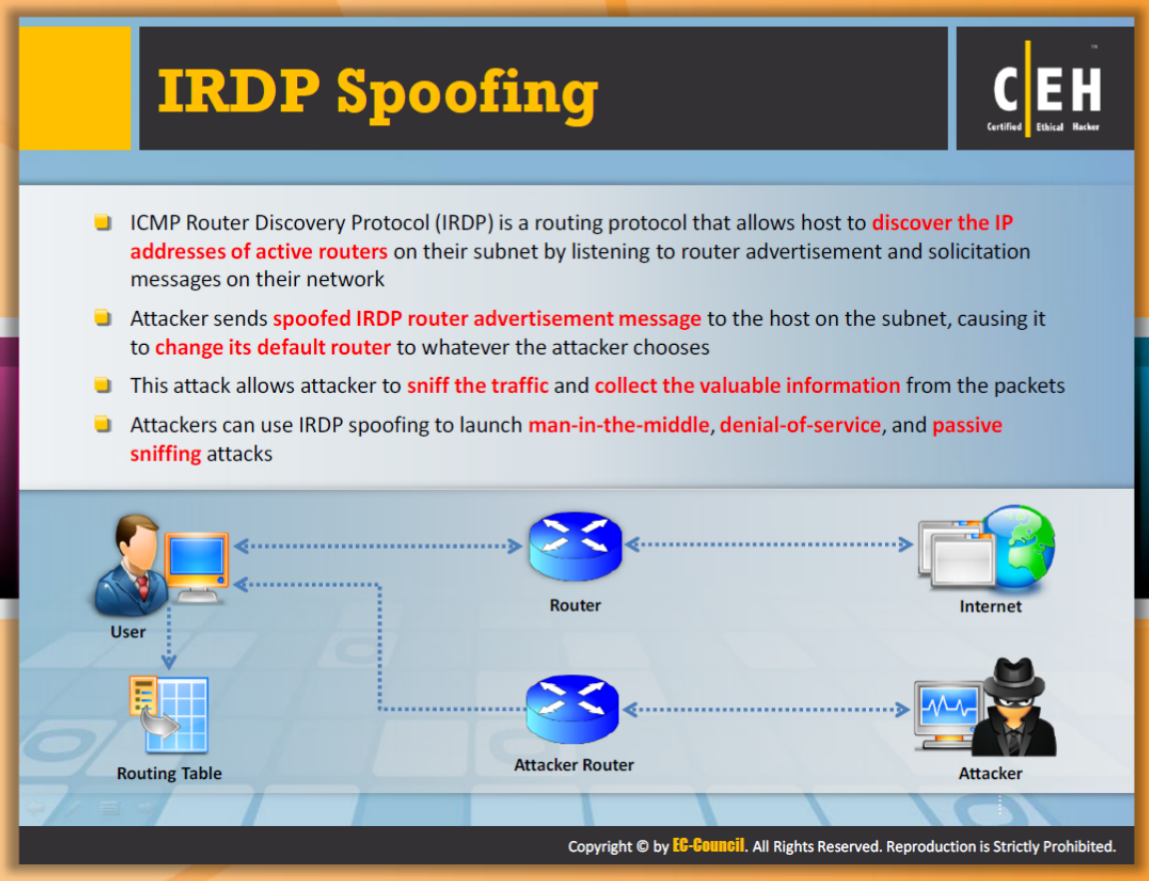


FIGURE 8.41: SMAC Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IRDP Spoofing

ICMP Router Discovery Protocol (IRDP) is a **routing protocol** that allows a host to discover the IP addresses of active routers on its subnet by listening to router advertisement and solicitation messages on its network. The attacker can add default route entries on a system remotely by spoofing router advertisements. The default route defined by the attacker will be preferred over the default route provided by the **DHCP server**. The attacker accomplishes this by setting the preference level and the lifetime of his or her route at high values in order to ensure that the **target hosts** will choose it as the preferred route. This attack succeeds if the attacker launching the attack is on the same network as the victim. In case of a Windows system configured as a DHCP client, Windows checks the received router advertisements for entries. If only one entry is there, then it checks whether the IP source address is within the subnet. If the address is **within the subnet**, then it adds the default route entry; otherwise, the advertisement is ignored.

An attacker can use this to his or her advantage and send spoofed router advertisement messages such that all the data packets travel throughthe **attacker's system**. Thus, the attacker can sniff the data. The following figure shows how attackers perform IRDP spoofing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

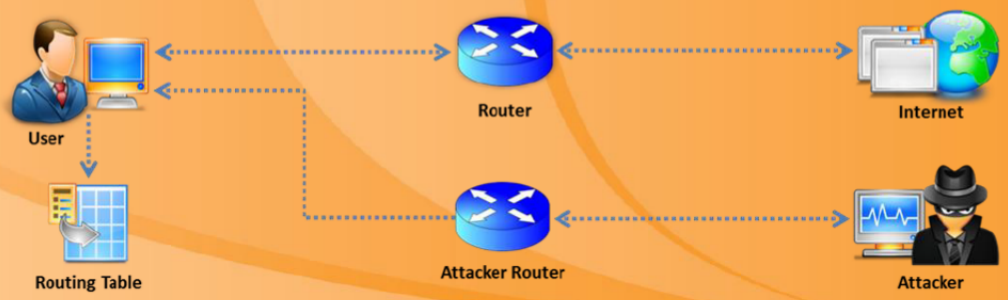
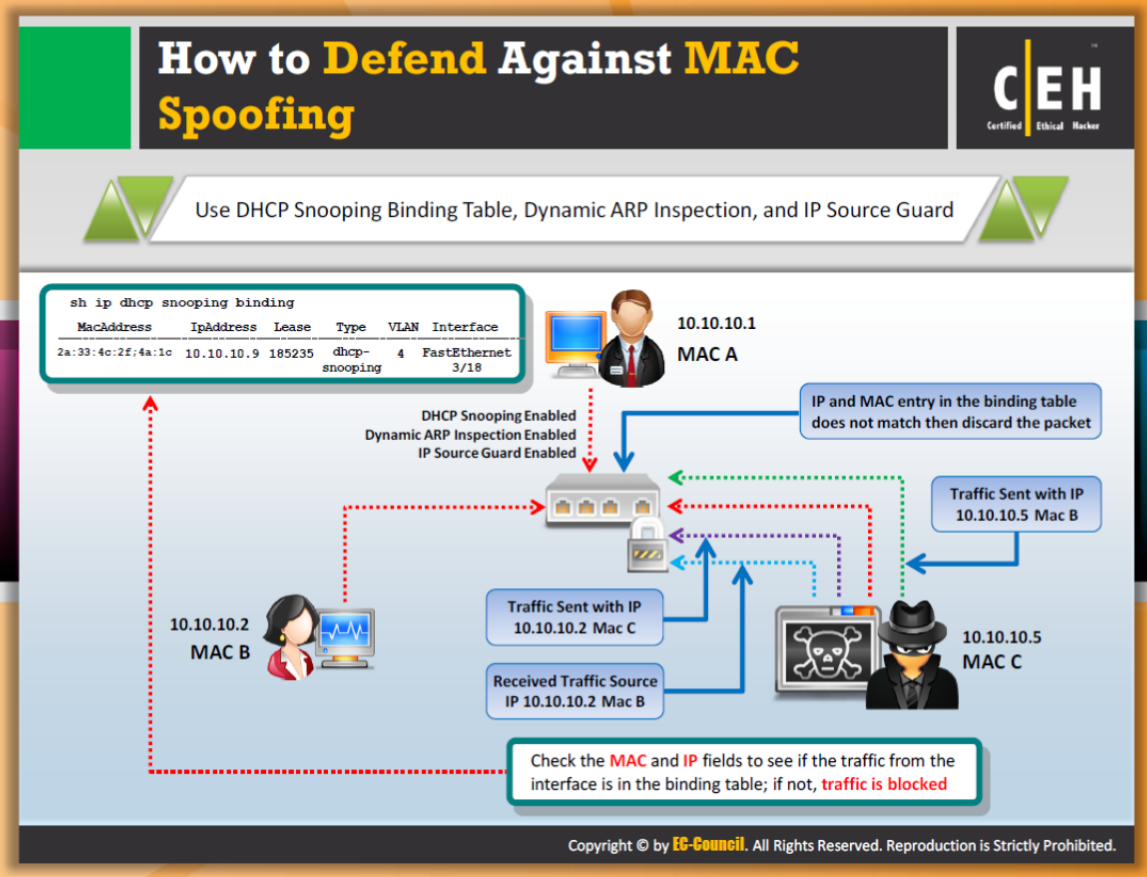


FIGURE 8.42: ICMP Router Discovery Protocol (IRDP) Working

You can avoid this ARDP spoofing attack by disabling IRDP on your hosts if the operating system permits it.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against MAC Spoofing

Performing security assessments is the main aim of an **ethical hacker**. As an ethical hacker, you have to perform various attacks against the target network or organization with permissions to find loopholes in the security architecture. But here your job is not done. Finding the security loopholes of the target organization is just a minor task. The major and the critical task of ethical hacking is to apply the appropriate countermeasures to the found **security loopholes** in order to fix them.

Once you test the network against MAC spoofing attacks and collect security loopholes, you should apply countermeasures to protect the network again **MAC spoofing**. There are many MAC spoofing countermeasures available that are suitable in various situations. Depending on your network security architecture and the loopholes found, you should apply the appropriate countermeasure to your network.

The best way to defend against **MAC address** spoofing is to place the server behind the router. This is because routers depend only on IP addresses, whereas switches depend on MAC addresses for communication in a network. Port security interface configuration is another way to mitigate MAC spoofing attacks. Once the port security command is enabled, it allows you to specify the MAC address of the system connected to the specific port. It also allows specifying an action to take if a port security violation occurs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

You can also implement the following techniques to defend against MAC address spoofing attacks:

- **DHCP Snooping Binding Table:** DHCP snooping filters the **untrusted** DHCP messages and helps to build and bind a DHCP binding table. This table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information to correspond with untrusted interfaces of a switch. It acts as a firewall between untrusted hosts and DHCP servers. It also helps in differentiating between trusted and untrusted interfaces.
- **Dynamic ARP Inspection:** It **checks the IP to MAC address** binding for each ARP packet in a network. If any IP to MAC invalid address bindings are found, then they are dropped by the Dynamic ARP inspection.
- **IP Source Guard:** IP Source Guard is a **security feature** that helps you restrict the IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database. It helps you to avoid the spoofing attacks when the attacker tries to spoof or use the IP address of another host.
- **Encryption:** Communication should be encrypted between **access point and computer** to avoid MAC spoofing.
- **Retrieval of MAC Address:** You should always retrieve the MAC address from the NIC directly instead of retrieving it from the operating system.

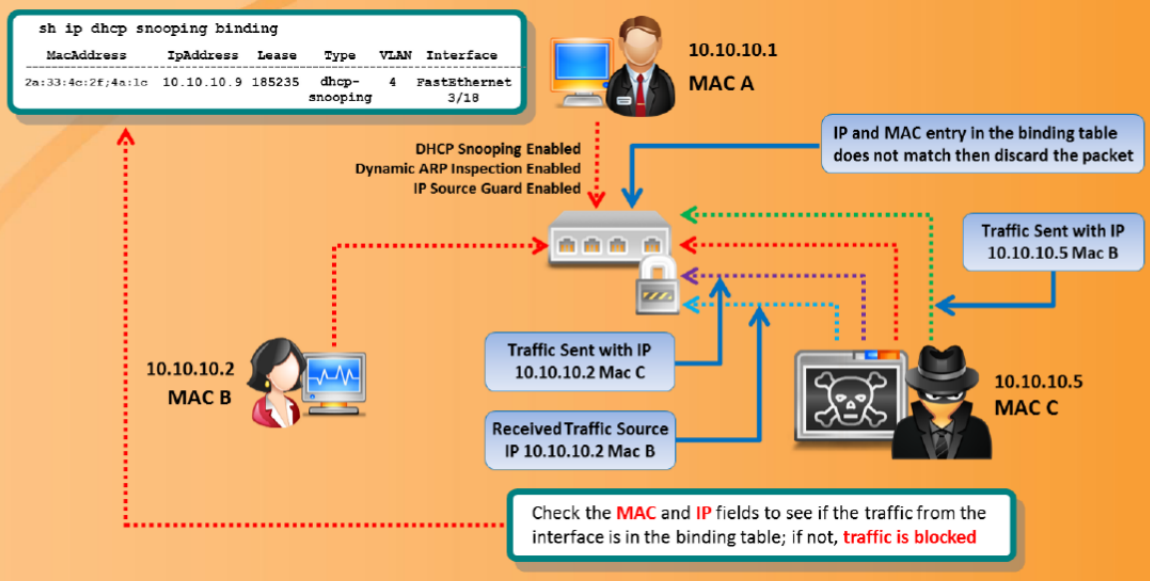
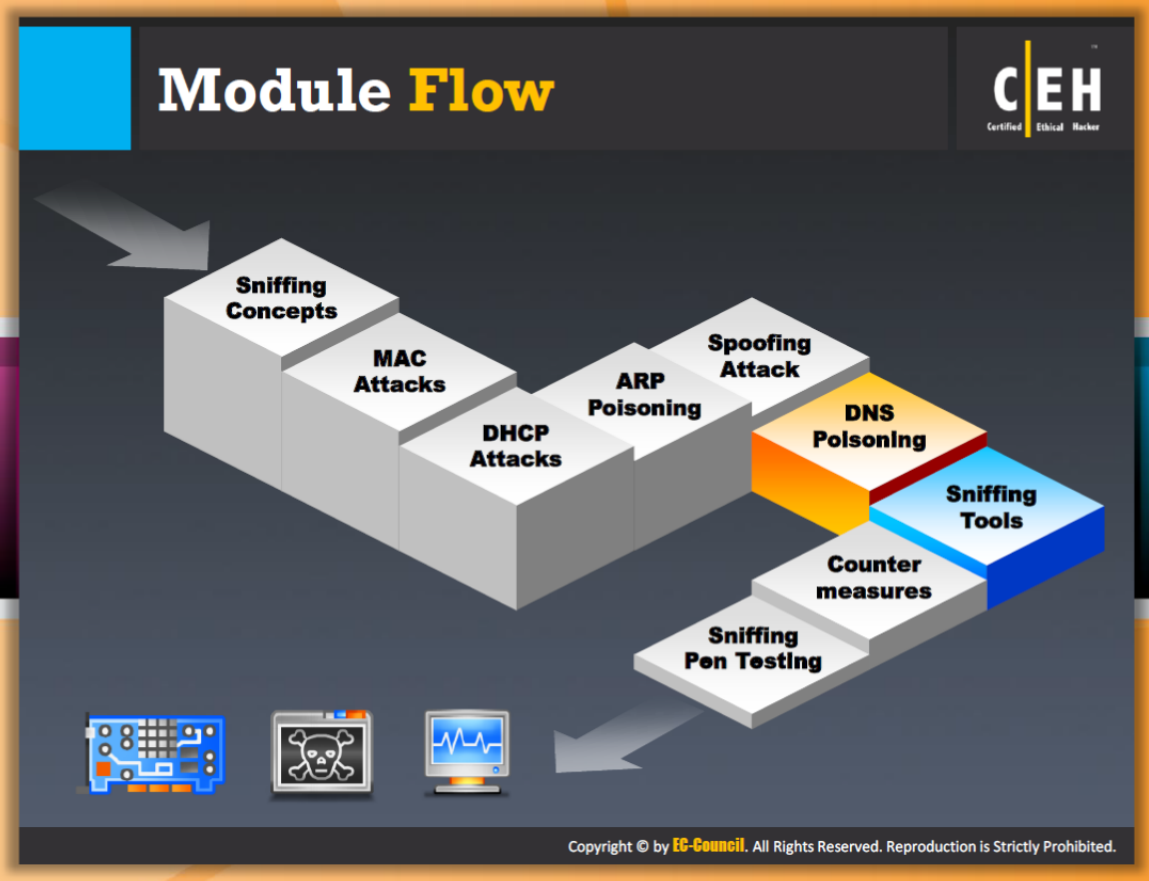


FIGURE 8.43: How to Defend Against MAC Spoofing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

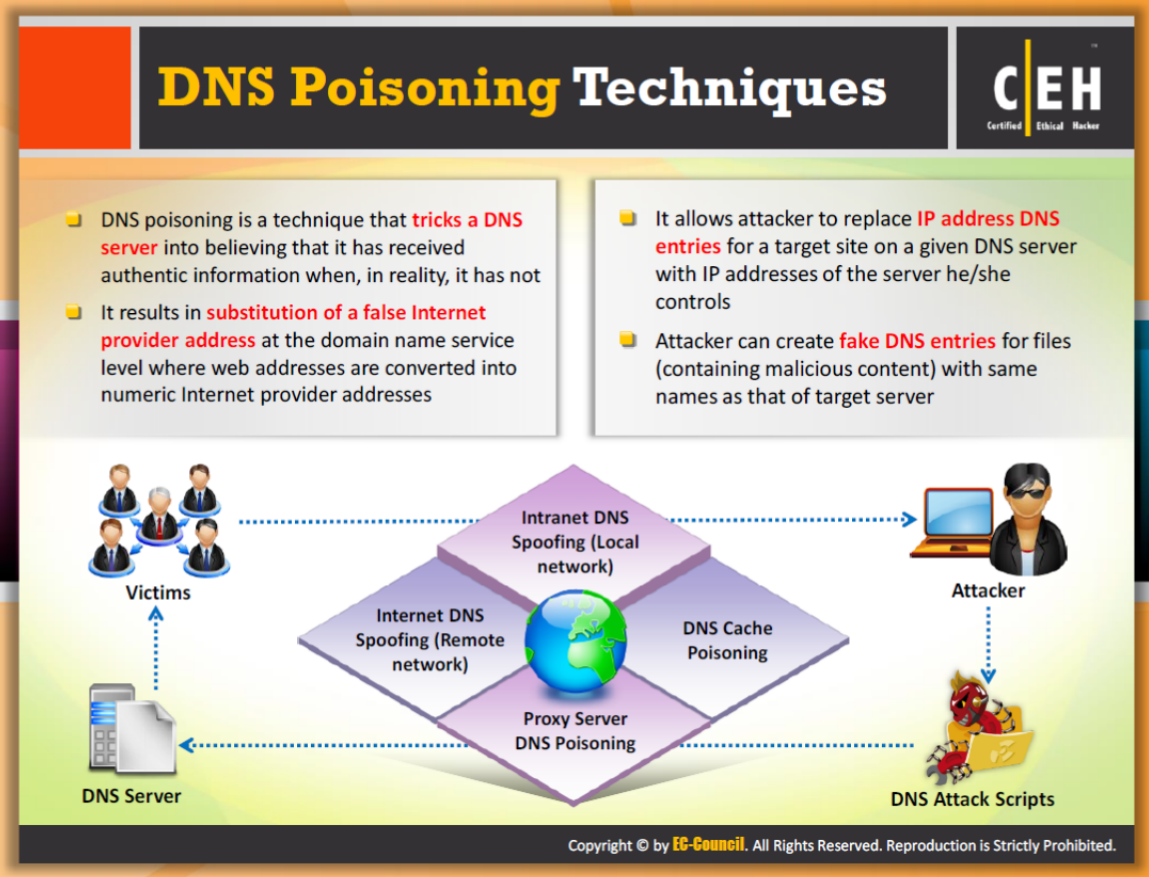
Once you check the network against MAC spoofing attacks and apply the countermeasures to protect it, next you should test and protect the network against DNS poisoning.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This section will familiarize you with various DNS poisoning techniques and the countermeasures to defend against DNS poisoning.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Poisoning Techniques

DNS (Domain Name Service) is the protocol that **translates** domain name (e.g., www.eccouncil.org) into IP address (e.g., 208.66.172.56). To maintain DNS, it uses DNS tables that contain the domain name and its equivalent IP address stored in a distributed large database. DNS poising, also called **DNS spoofing**, is an attack in which the attacker tries to redirect the victim to a malicious server instead of the legitimate server. The attacker can commit this type of attack by manipulating the DNS table entries in the DNS system. Suppose the victim wants to access the website ABC.com, The **attacker manipulates** the entries in the DNS table in such a way that the victim is being redirected to attacker's server. This can be done by changing the IP address of ABC.com to the attacker's malicious server IP address. Thus, the victim connects to the attacker's server without his or her knowledge. Once the victim connects to the attacker's server, the attacker can **compromise** the victim's system and **steal data**. In a similar manner, you can also compromise the target system by conducting a DNS poisoning attack.

To launch a DNS poisoning attack, follow these steps:

- Set up a fake website on your computer.
- Install treewalk and modify the file mentioned in the readme.txt to your IP address. Treewalk will make you the DNS server.

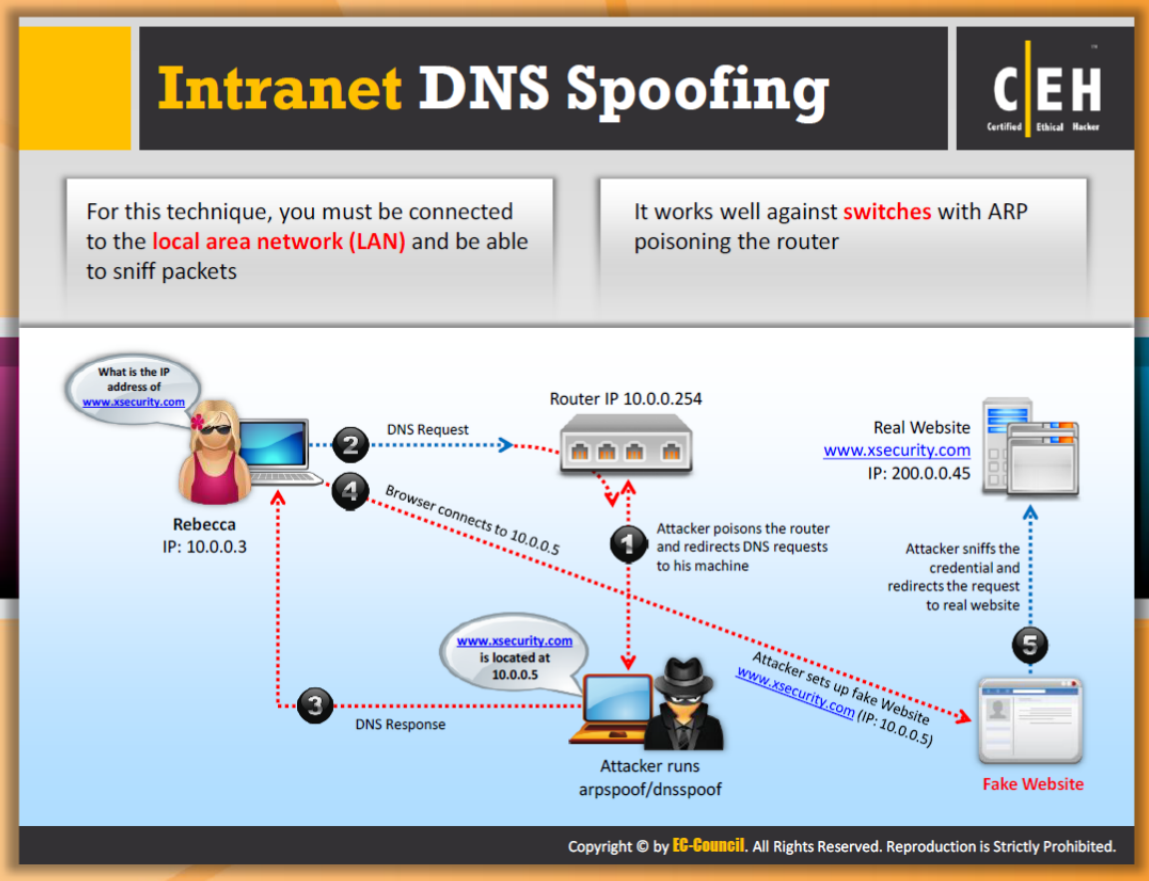
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Modify the file dns-spoofing.bat and replace the IP address with your IP address.
- Trojanize the dns-spoofing.bat file and send it to Jessica (ex: chess.exe).
- When the host clicks the Trojanned file, it will replace Jessica's DNS-entry in her TCP/IP properties to that of your machine.
- You will become the DNS server for Rebecca and her DNS requests will go through you.
- When Rebecca types XSECURITY, the website she resolves to is the fake XSECURITY website. Then, sniff the password and send her to the real website.

There are four types of DNS poisoning attacks using which you can compromise the target system:

- Intranet DNS spoofing (local network)
- Internet DNS spoofing (remote network)
- Proxy server DNS poisoning
- DNS cache poisoning

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Intranet DNS Spoofing

When an attacker performs **DNS poisoning** on a **local area network (LAN)**, it is called intranet DNS spoofing. An attacker can perform intranet DNS spoofing attack with the help of the ARP poisoning technique. This is usually conducted on a switched LAN. To perform this attack, you must be connected to the LAN and be able to sniff the traffic or packets.

Once the attacker succeeds in sniffing the **ID** of the **DNS request** from the intranet, he or she can send a malicious reply to the sender before the actual DNS server.

You can perform an intranet DNS spoofing attack as per the scenario explained in the following diagram:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

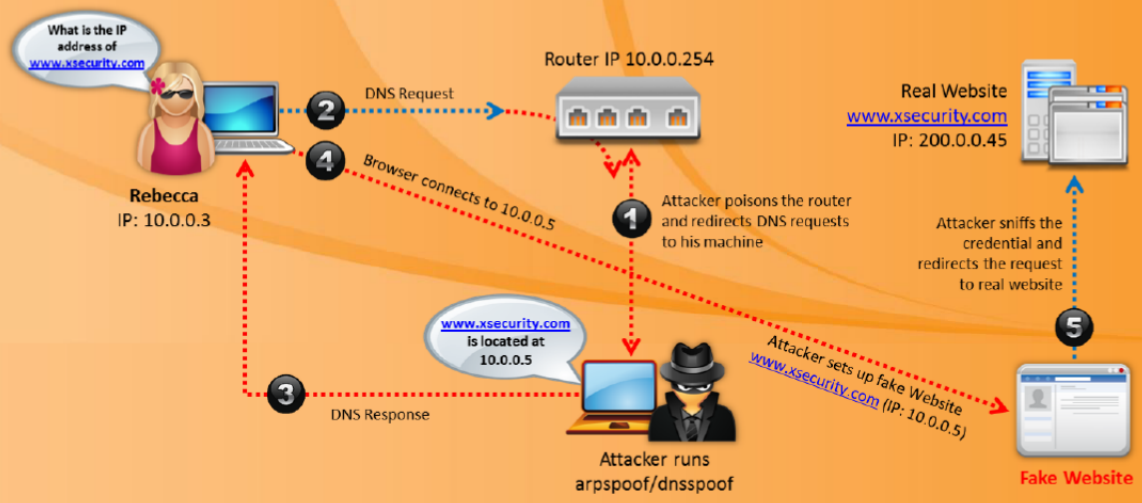
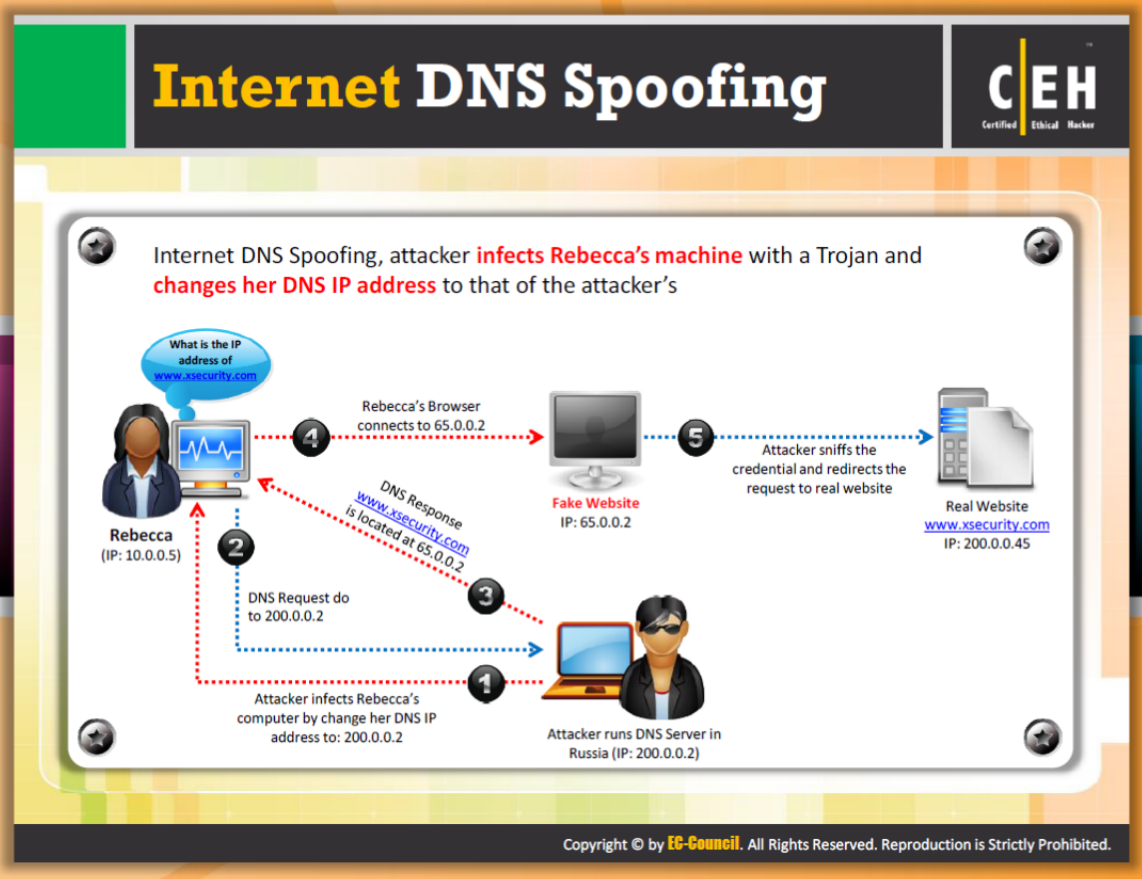


FIGURE 8.44: Working of Intranet DNS Spoofing

It is clear from the diagram that first the attacker poisons the router by running arpspoof/dnsspoof in order to redirect DNS requests of clients to the attacker's machine. When a client (Rebecca) sends a DNS request to the router, the poisoned router sends the DNS request packet to the attacker's machine. Upon receiving the DNS request, the attacker sends a fake DNS response that redirects the client to a fake website set up by the attacker. As the website is owned by the attacker, attacker can see all the information submitted by the client to that website. Thus, the attacker can sniff sensitive data such as passwords, etc. submitted to the fake website. Once the attacker retrieves the required information, he or she then redirects the client to the real website.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Internet DNS Spoofing

Internet DNS poisoning is also known as **remote DNS poisoning**. This attack can be performed either on a single or multiple victims anywhere in the world. In order to perform this attack, you need to set up a rouge **DNS server** with a static IP address.

Internet DNS spoofing is performed when the victim's system is connected to the Internet. It is done with the help of Trojans. It is one of the **MITM** types of attacks, where the attacker changes the primary DNS entries of the victim's computer. The attacker replaces the victim's DNS IP address with the fake IP address that refers to the attacker's system; thus all traffic will be redirected to the attacker's system. Now the attacker can easily sniff the victim's confidential information.

The following diagram explains how to perform Internet **DNS spoofing** in detail:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

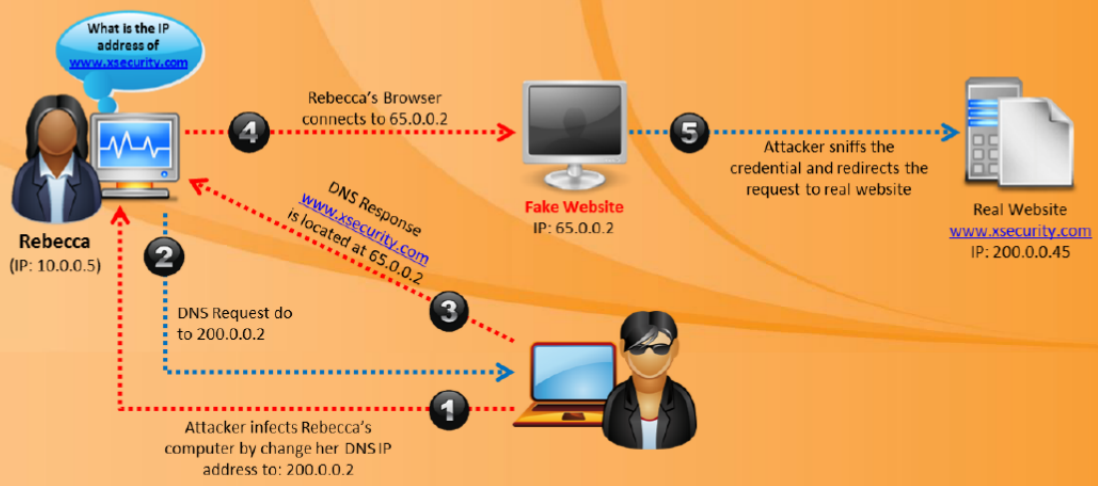
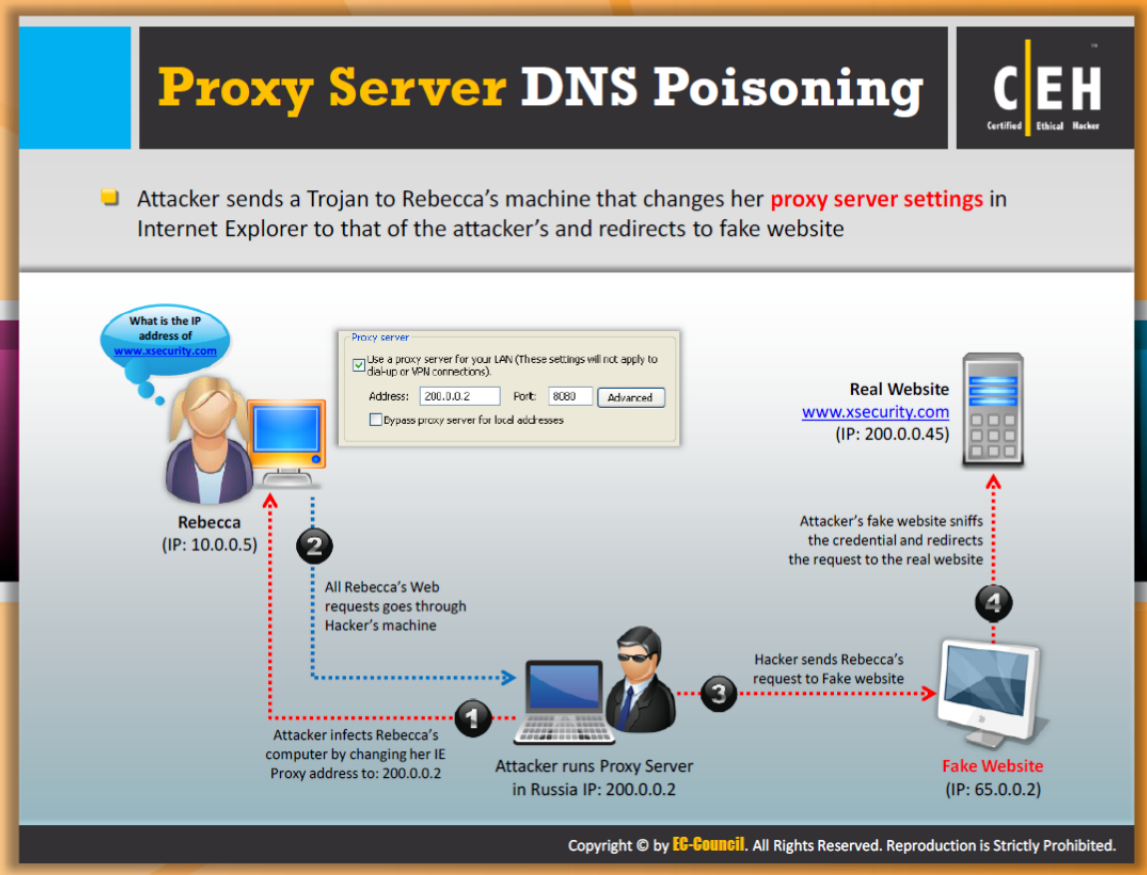


FIGURE 8.45: Working of Internet DNS Spoofing

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Proxy Server DNS Poisoning

In the proxy server DNS poisoning technique, the attacker changes the **proxy server** setting of the victim to that of the attacker. This is done with the help of a **Trojan**. This redirects the victim's request to the attacker's fake website where the attacker can sniff the **confidential information** of the victim.

The following diagram helps you to understand how an attacker performs proxy server DNS poisoning:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

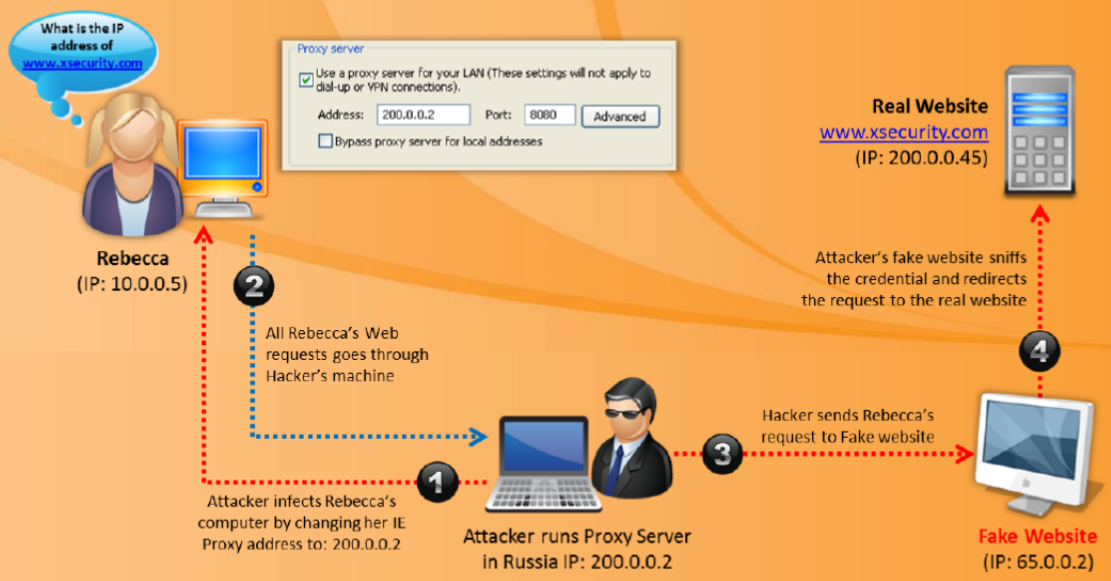
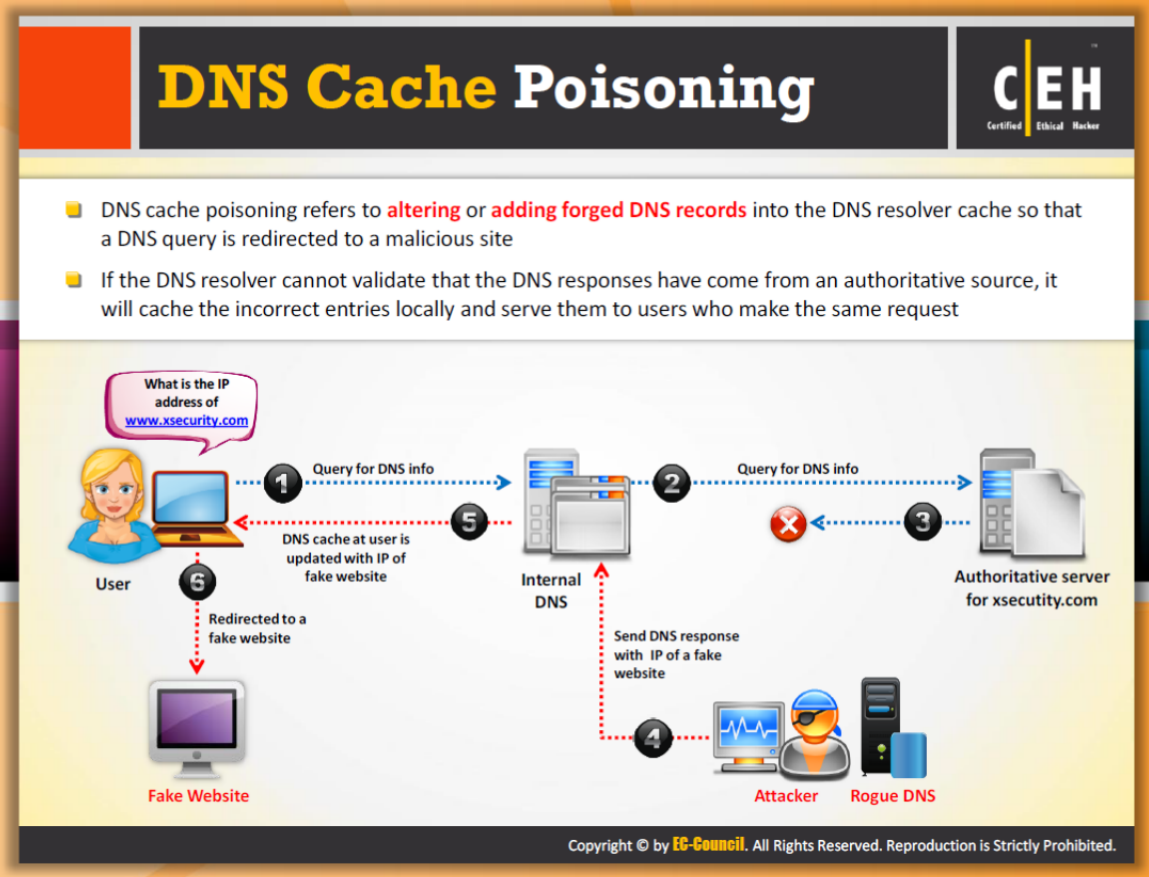


FIGURE 8.46: Working of Proxy Server DNS Poisoning

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Cache Poisoning

The DNS system uses cache memory to hold the recently resolved **domain names**. It is populated with recently used domain names and respective IP address entries. When the user request comes, the DNS resolver first checks the **DNS cache**; if the domain name that the user requested is found in the cache, then the resolver sends its respective IP address quickly. Thus, it reduces the traffic and time of **DNS resolving**.

Attacker target this DNS cache and make changes or add entries to the **DNS cache**. The attacker replaces the user-requested IP address with the **fake IP address**. Then, after when user requests that domain name, the DNS resolver checks the entry in the DNS cache and picks the matched (poised) entry. Thus, the victim is redirected to the attacker's fake server instead of the authorized server.

The following figure shows scenarios of how an attacker poisons the DNS cache:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

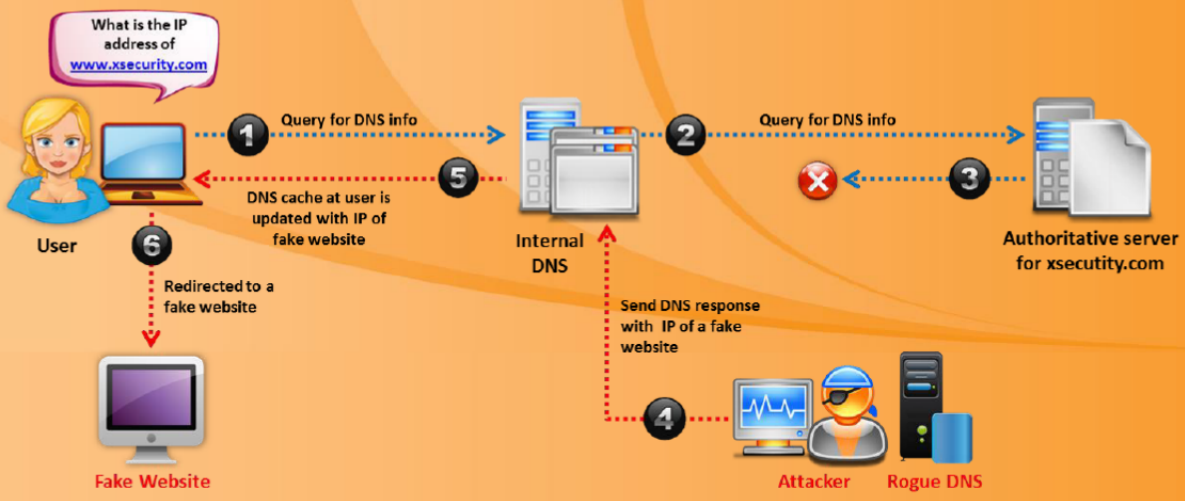
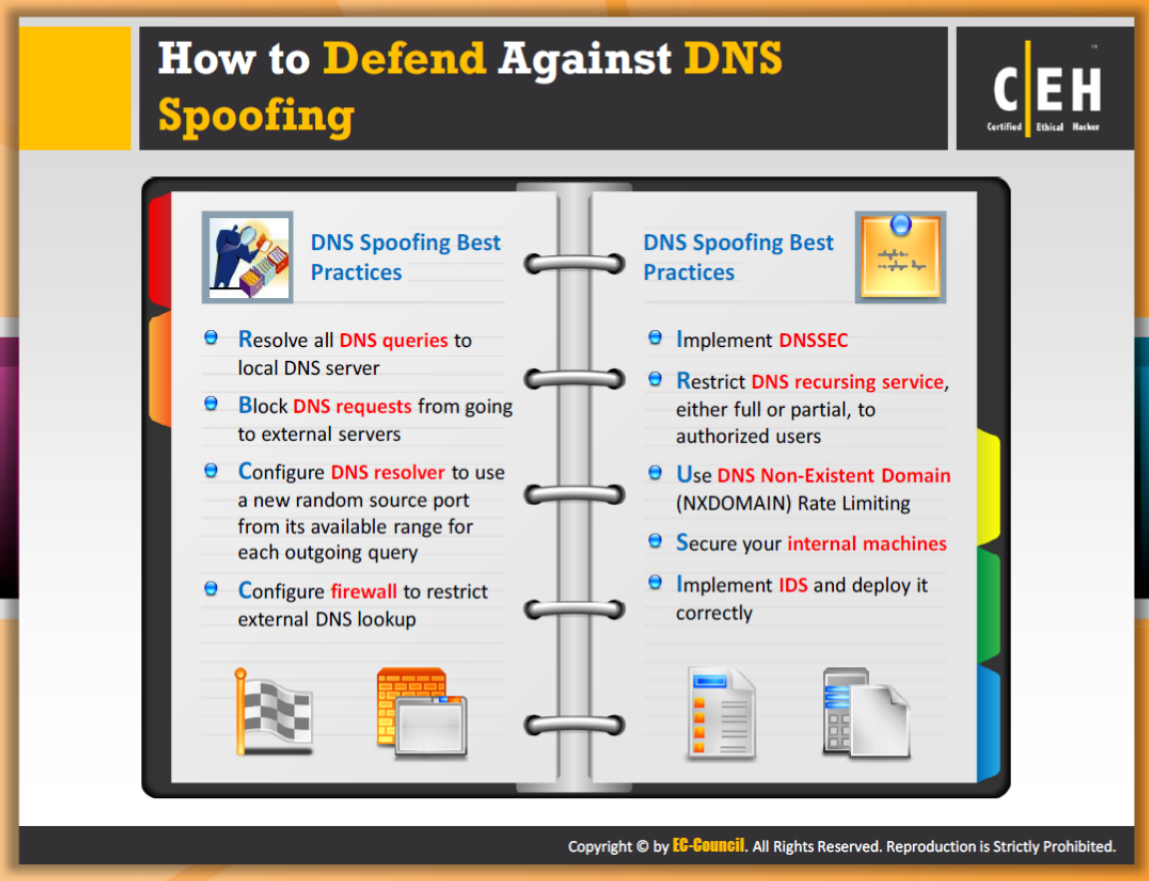


FIGURE 8.47: How an Attacker Poisons the DNS Cache

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against DNS Spoofing

You have learned how an attacker carries out different types of DNS spoofing attacks. Let's see what you should do to defend your network from these types of attacks.

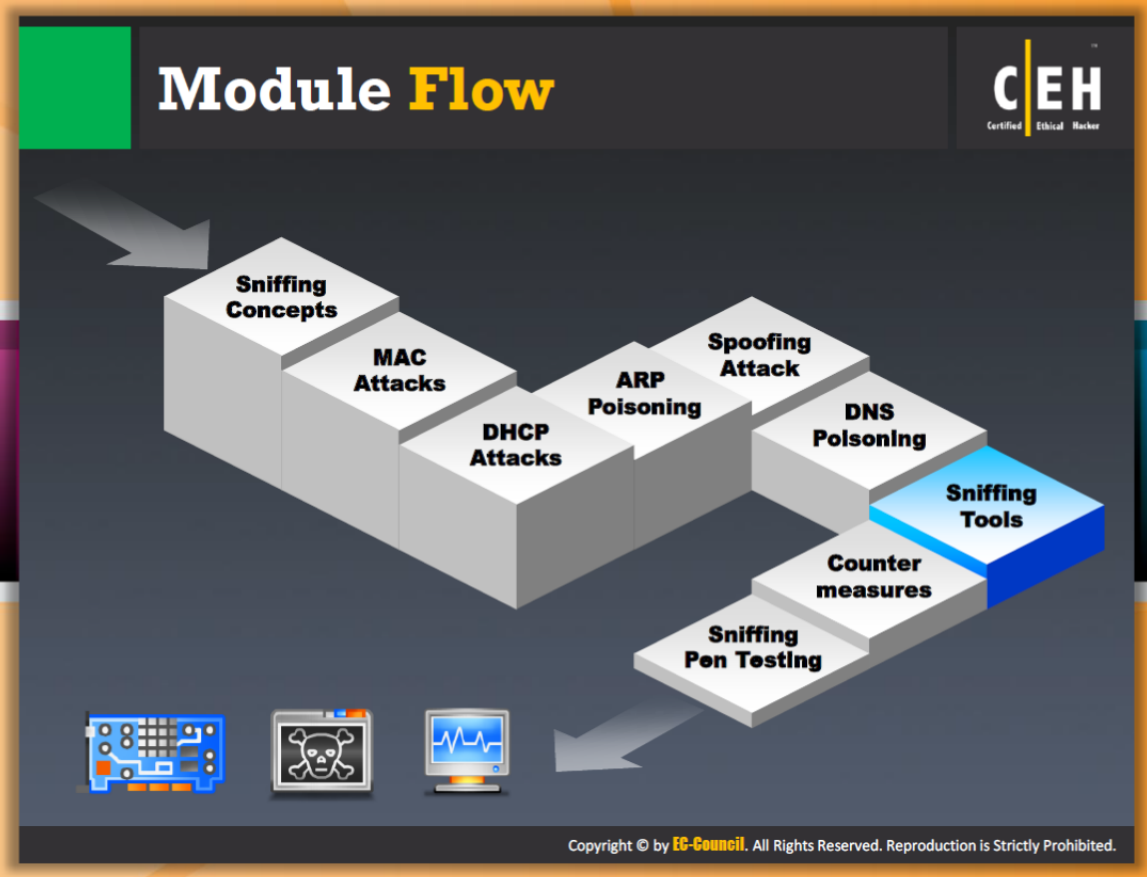
Here are the some countermeasures that will help you to avoid DNS spoofing attacks:

- Resolve all DNS queries to local DNS servers
- Block DNS requests from going to external servers
- Implement DNSSEC
- Configure the DNS resolver to use a new random source port from its available range for each outgoing query
- Configure the firewall to restrict external DNS lookup
- Restrict the DNS recursing service, either full or partial, to authorized users
- Use **DNS Non-Existent Domain (NXDOMAIN)** rate limiting
- Secure your internal machines
- Implement IDS and deploy it correctly
- Use static ARP and IP table

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use SSH encryption
- Use sniffing detection tools
- Do not open suspicious files
- Always use trusted proxy sites
- Audit your DNS server regularly to remove vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

So far, we have discussed sniffing concepts and various techniques to sniff network traffic or data. Administrators use sniffing tools to monitor their network and attackers misuse sniffing tools to sniff the network data.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This section will introduce you to some useful tools that attackers may use to sniff the target network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Tool: Wireshark

Source: http://www.wireshark.org

Wireshark allows you to capture and interactively browse the traffic running on a target computer network. It uses **Winpcap** to capture packets, so it can only capture packets on networks supported by Winpcap. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. Captured files can be programmatically edited via the command line. A set of filters for customized data display can be refined using a **display filter**.

You can use this tool for sniffing target network traffic covertly. It allows you to put the network interface controllers that support into promiscuous mode. Thus, you can see all traffic visible on that interface.

Features:

- Allows you to capture live or offline network data for analysis
- Allows you to browse the captured network data via a GUI or via the **TTY-mode TShark** utility

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Runs on multiple platforms such as Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- Supports many read/write capture file formats
- Reads live data from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)

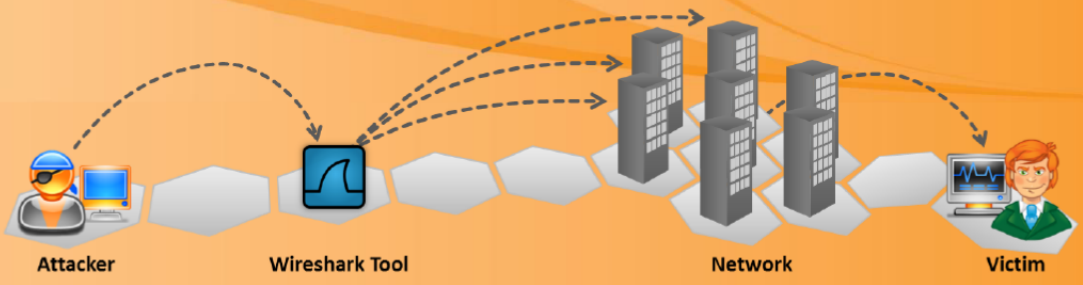
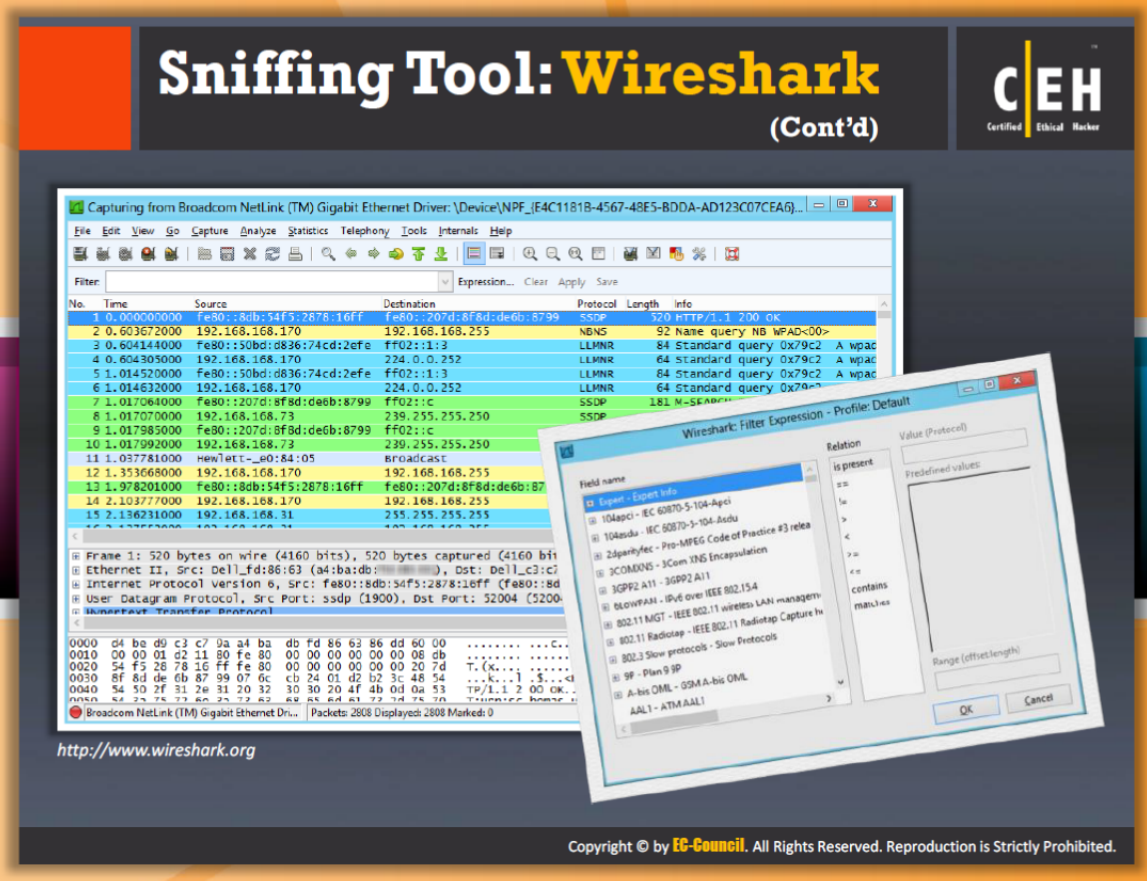


FIGURE 8.48: Working of Wireshark

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Tool: Wireshark (Cont'd)

Source: http://www.wireshark.org

The following Wireshark screenshots show details such as source, destination, protocol used, length, etc. of the captured packets on the network.

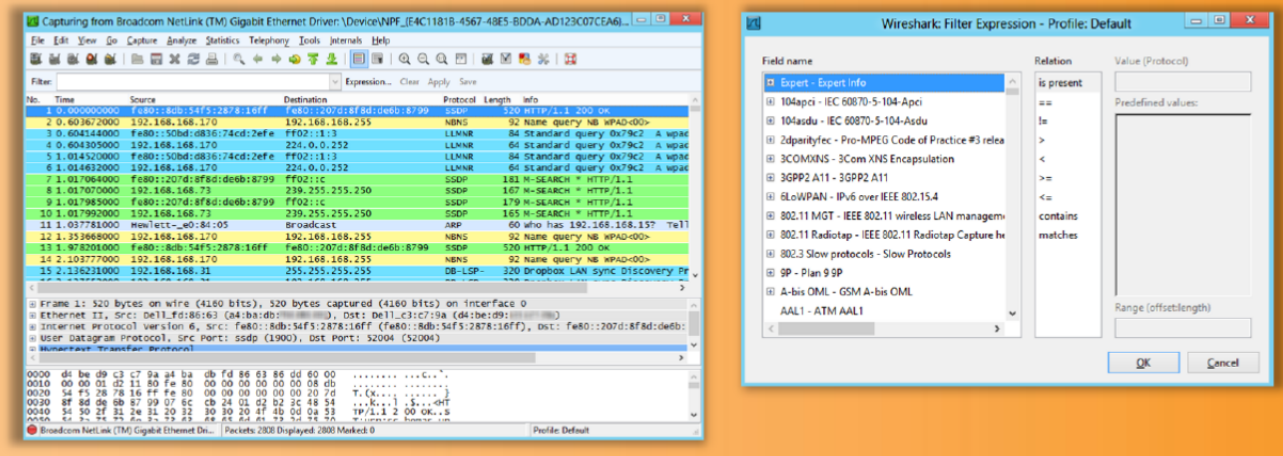
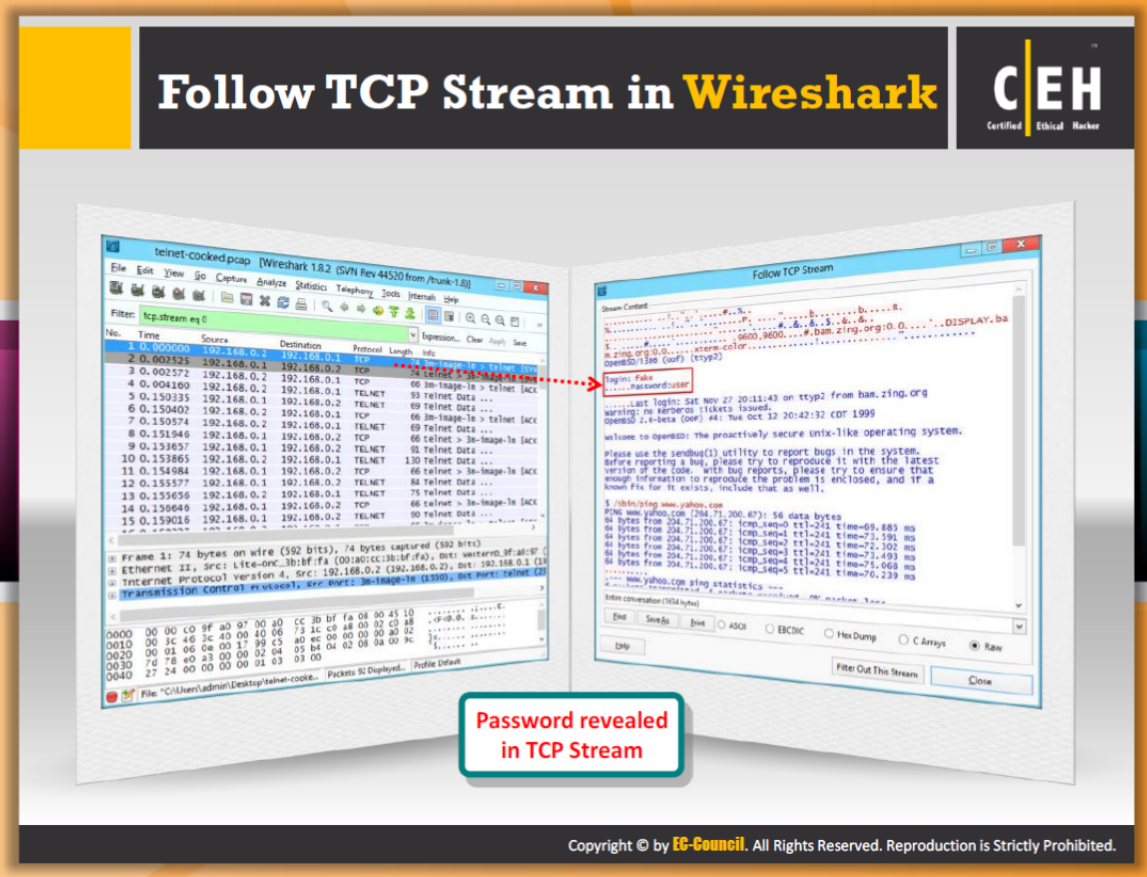


FIGURE 8.49: Wireshark Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Follow TCP Stream in Wireshark

Source: http://www.wireshark.org

Wireshark allows you to see the data from **TCP port** with its feature known as "**Follow tcp stream**". With this tool you can see the tcp data in the same way as that of the application layer. Using this you can find passwords in a Telnet or make sense of a data stream.

To see the **TCP stream**, select a TCP packet in the packet list of the stream/connection you are interested in and then select the Follow TCP Stream menu item from the **Wireshark** Tools menu. Wireshark displays all the data from TCP stream by setting an appropriate display filter. The stream content is displayed in the same sequence as it appeared on the network. It allows you to see the captured data in ASCII, EBCDIC, HEX Dump, C Arrays, Raw formats.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

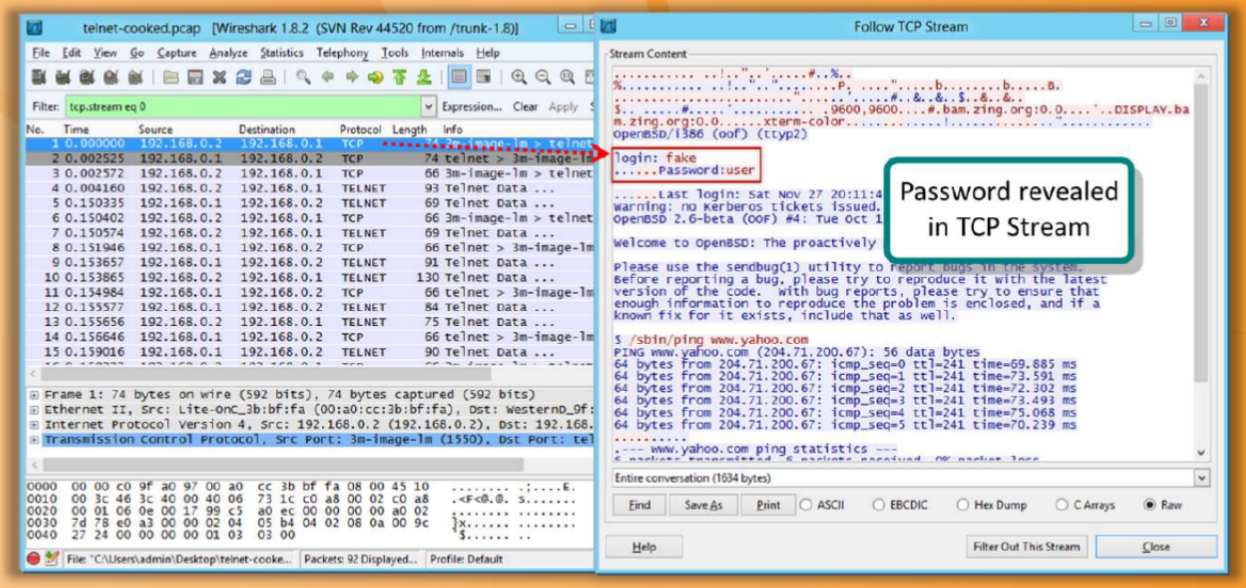
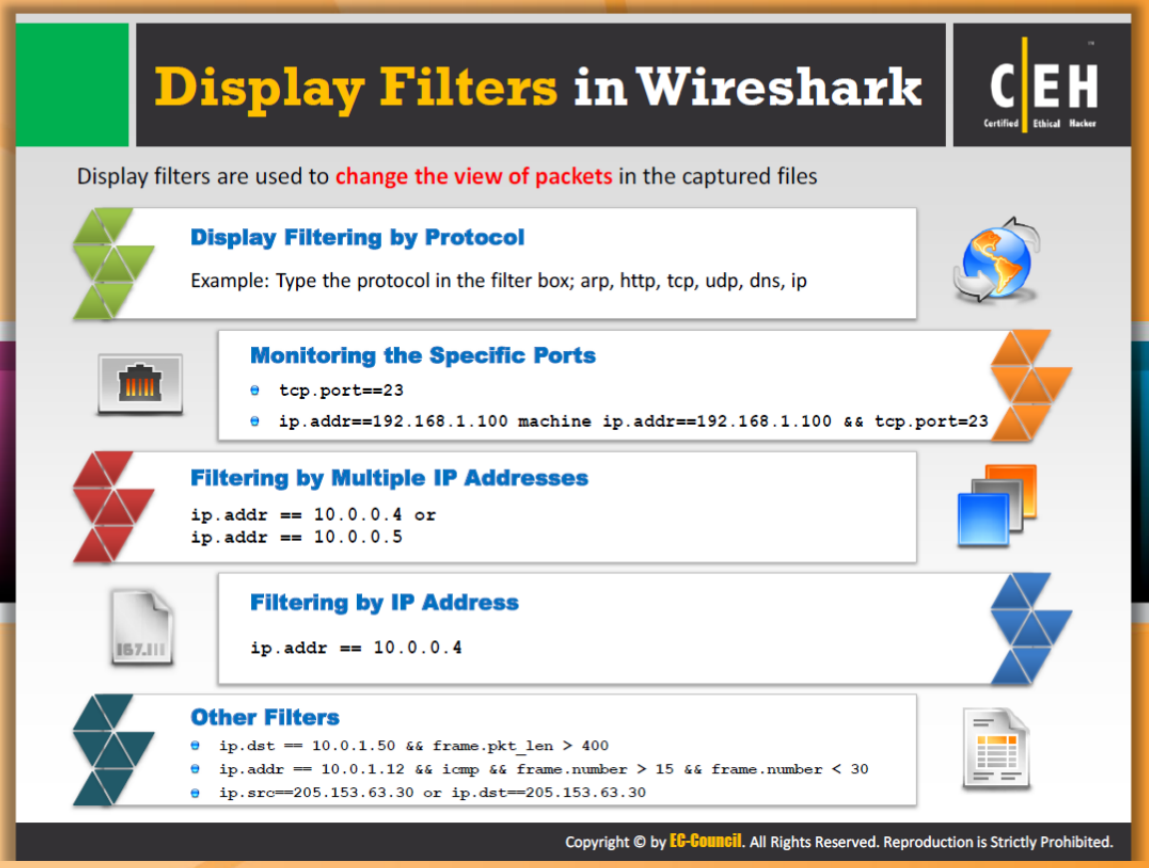


FIGURE 8.50: Wireshark TCP Streaming Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Display Filters in Wireshark

Source: http://wiki.Wireshark.com

Wireshark features display filters that allow you to filter the traffic on the **target network** by protocol type, IP address, port, etc. If you filter by protocol type, it first captures the traffic, then filters and displays only the traffic coming from the selected protocol. This is useful when you want to monitor the traffic coming from a specific protocol rather than monitoring all the traffic. To set a filter, type the protocol name, such as arp, http, tcp, udp, dns, ip ,etc. in the filter box of Wireshark. You can set multiple filters at a time to sort out data you want.

Following are the various ways to filter traffic on network using **Wireshark**.

Using Wireshark, traffic can be filtered in various ways. To filter the traffic on network by protocol, IP address, or ports, type the respective command in the filter box:

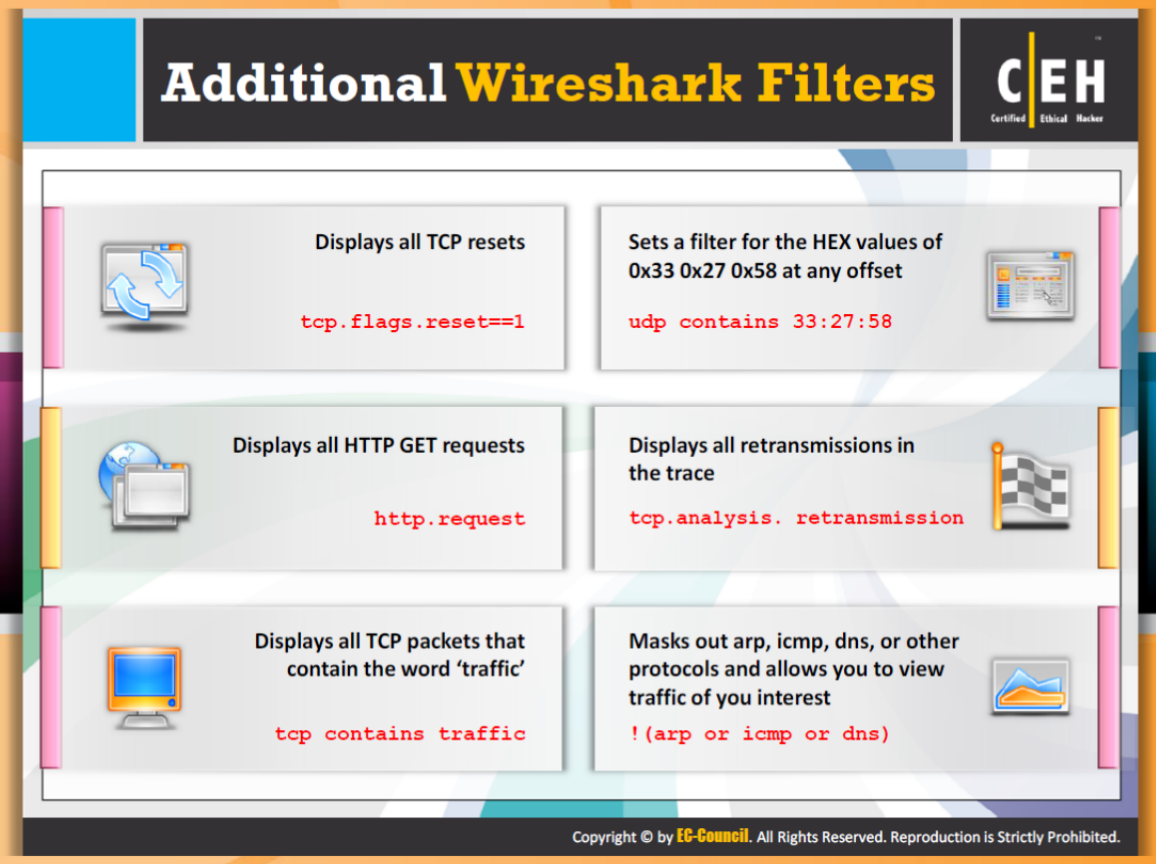
- **Filtering by Protocol:** arp, http, tcp, udp, dns
- **Filtering By IP Address:** ip.addr == 10.0.0.4
- **Filtering By Multiple IP Addresses:** ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5
- **Monitoring Specific Ports:** tcp.port==443
- **Multiple filtering:**

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- ip.addr==192.168.1.100 machine ip.addr==192.168.1.100 && tcp.port=443

- **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.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



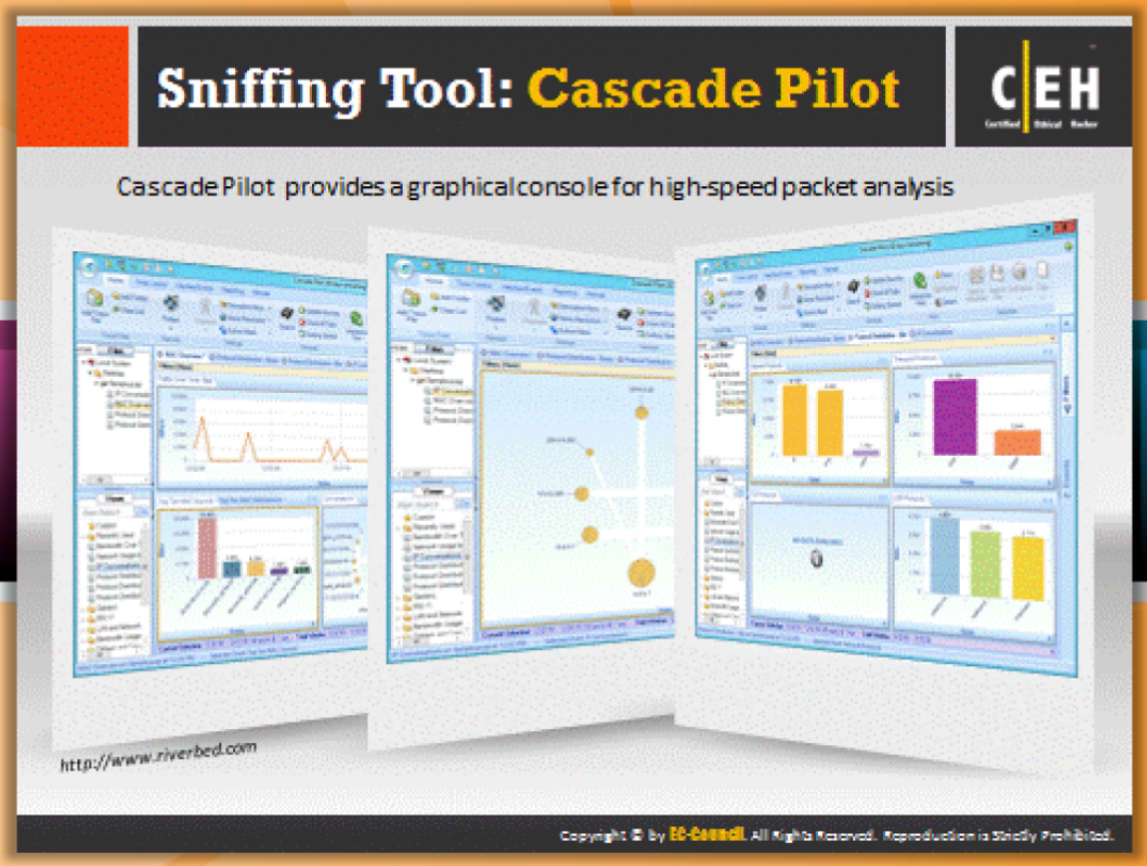
Additional Wireshark Filters

Source: http://wiki.Wireshark.com

In addition to the filters discussed previously, **Wireshark features additional** filters that allow you to filter the traffic by specific TCP reset field, http request, specific keyword, etc. The additional Wireshark filters and the respective entry in the filter field are as follows:

- **Filtering by TCP resets:** tcp.flags.reset==1
- **Filtering by HTTP GET requests:** http.request
- **Filtering by TCP packets that contain the word 'traffic':** tcp contains traffic: this type of filter can be used when you want to search specific string or user ID
- **Sets a filter for the HEX values of 0x33 0x27 0x58 at any** offset: udp contains 33:27:58
- **Filtering by retransmissions in the trace:** tcp.analysis.retransmission: This filtering helps you when tracking down slow application performance and packet loss

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Tool: Cascade Pilot

Source: http://www.riverbed.com

Cascade Pilot is a **packet analysis** tool that helps you to analyze **multi-terabyte** packet recordings on remote Cascade Shark appliances, Virtual Cascade Shark, and Steelhead WAN optimization products without having to transfer large packet capture files across the network. Attackers can use this tool to analyze traffic streams to capture sensitive data packets. Besides packet analysis and capture, it can also be used for performance monitoring, flow collection, packet inspection, etc. It allows you to isolate and identify the **traffic of interest**. It also allows you to see and analyze long-duration local and **remote traffic** statistics by moving back in time. The following are screenshots taken while performing traffic analysis of a network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

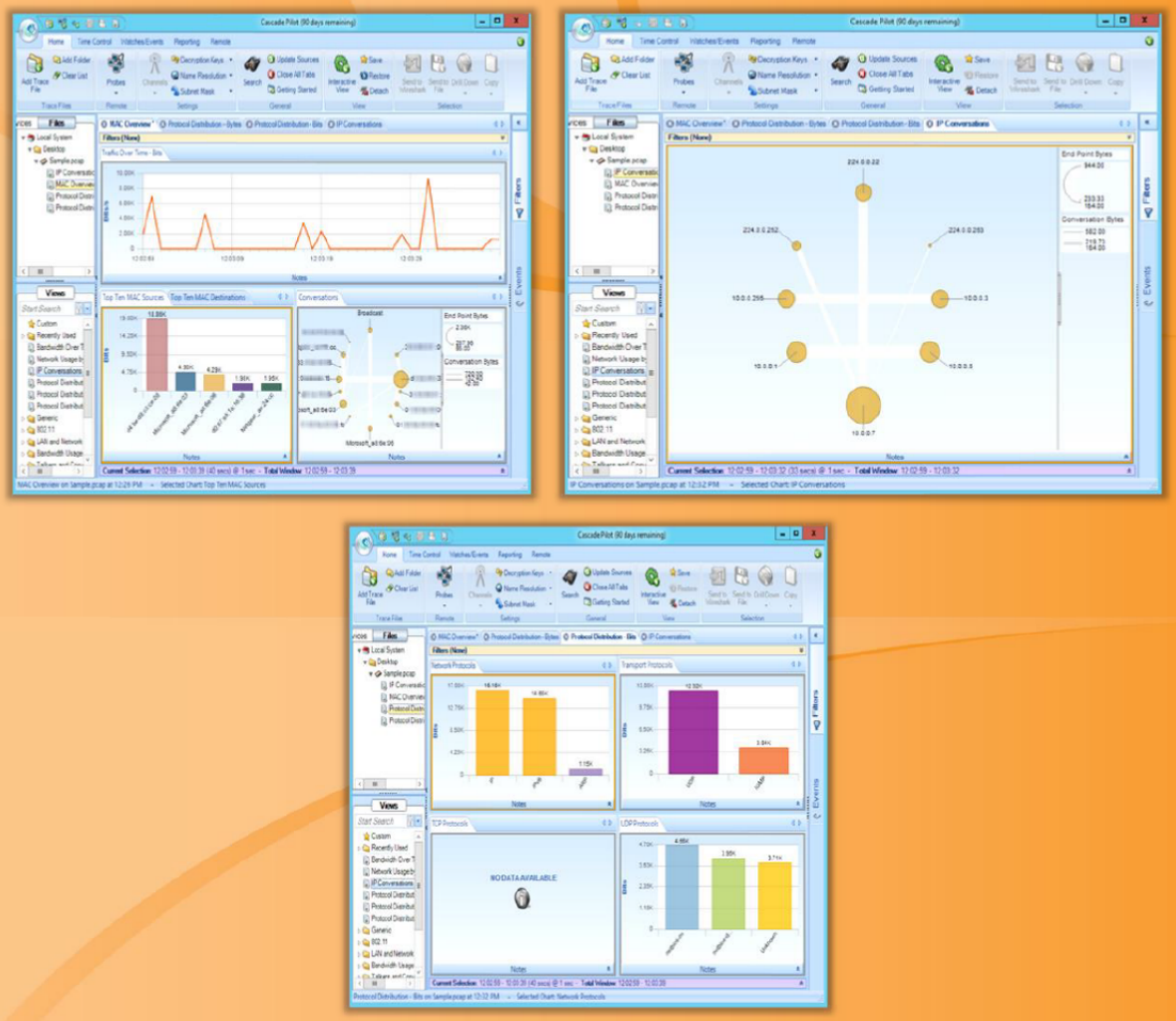
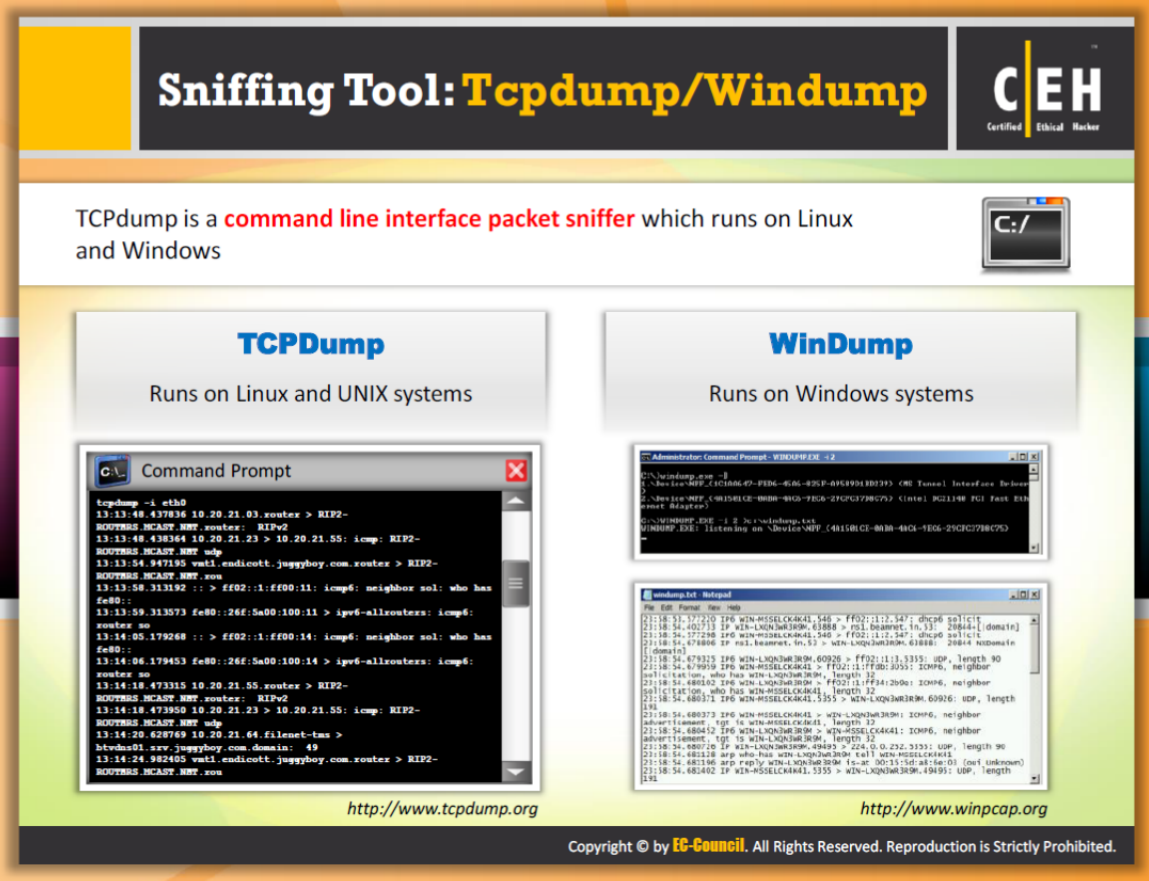


FIGURE 8.51: Cascade Pilot Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Tool: Tcpdump/Windump

Tcpdump

Source: http://www.tcpdump.org

Tcpdump is a command-line **packet analyzer**. This tool allows you to intercept and display TCP/IP and other packets being transmitted or received over a network. It runs on Linux and other **UNIX-like operating systems**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

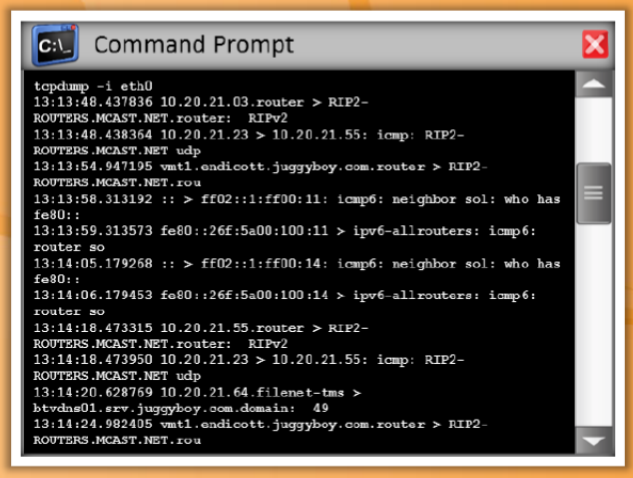


FIGURE 8.52: Tcpdump

Windump

Source: http://www.winpcap.org

WinDump is the **Windows version** of tcpdump , the command-line network analyzer for UNIX. It can be used to watch, diagnose, and save network traffic to disk according to various complex rules. It has almost the same functionality as that of tcpdump except that it runs on Windows systems.

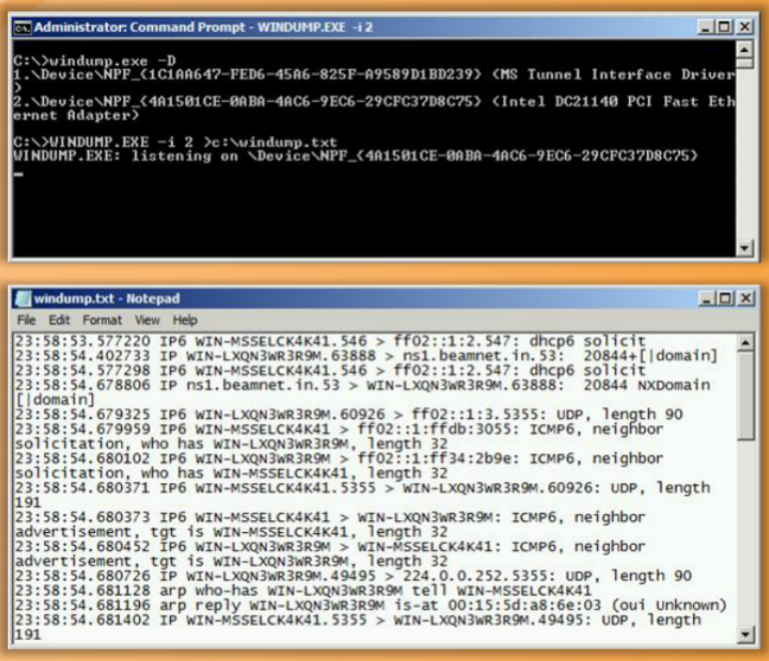
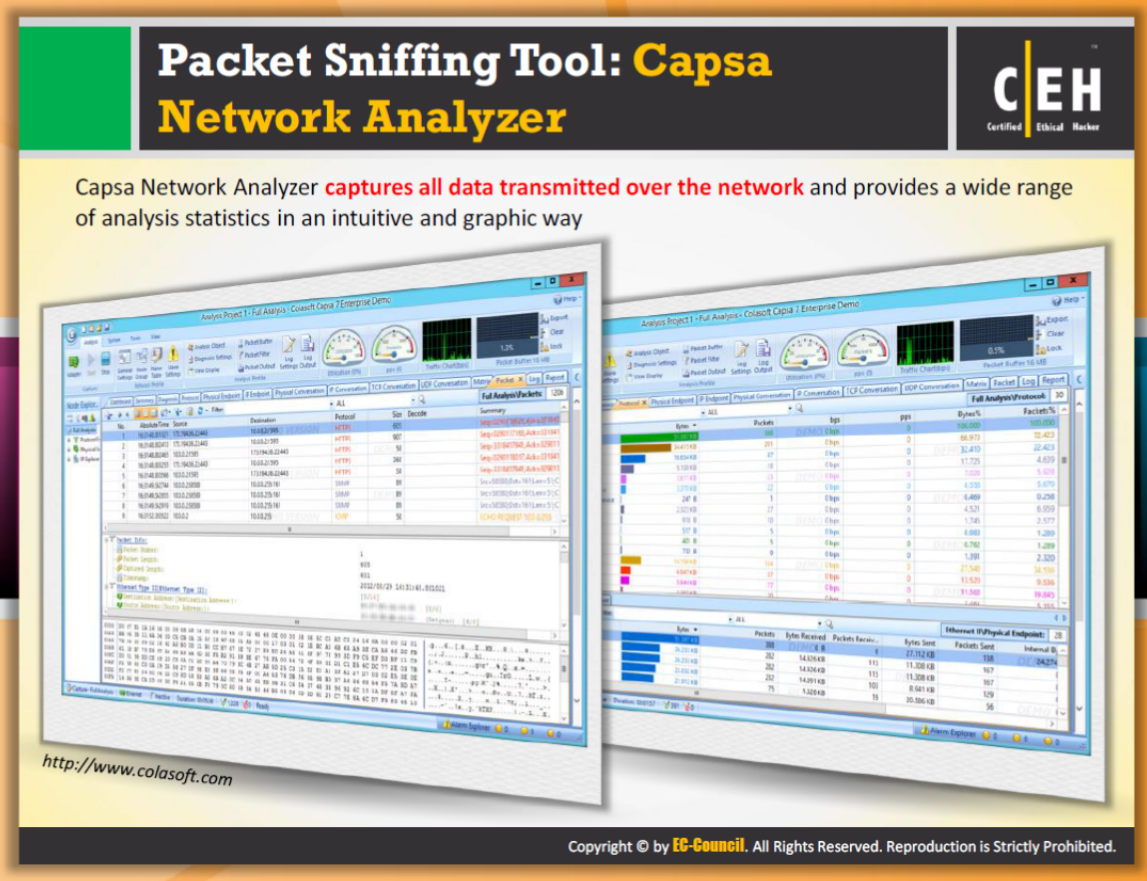


FIGURE 8.53: Windump

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Packet Sniffing Tool: Capsa Network Analyzer

Source: http://www.colasoft.com

Capsa Network Analyzer is a **network monitoring tool** that captures all **data transmitted** over the network and provides a wide range of analysis statistics in an intuitive and graphic way. It is even used to analyze and troubleshoot the problem that has occurred (if any) in the network. It is also able to perform **reliable network** forensics, advanced protocol analyzing, in-depth packet decoding, and automatic expert diagnosing. It helps you detect network **vulnerabilities**. Attacker can use this tool to sniff packets from the target network.

Features:

- Real-time capture and save data transmitted over local networks, including wired network and wireless network like **802.11a/b/g/n**
- Identify and analyze more than **300 network protocols**, as well as network applications based on the protocols
- Monitor network bandwidth and usage by capturing data packets transmitted over the network and providing summary and decoding information about these packets
- View network statistics at a single glance, allowing easy capture and interpretation of network utilization data

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Monitor Internet, email, and instant messaging traffic, helping keep employee productivity to a maximum
- Diagnose and pinpoint network problems in seconds by detecting and locating suspicious hosts
- Map out the details, including traffic, IP address, and MAC, of each host on the network, allowing for easy identification of each host and the traffic that passes through each
- Visualize the entire network in an ellipse that shows the connections and traffic between each host

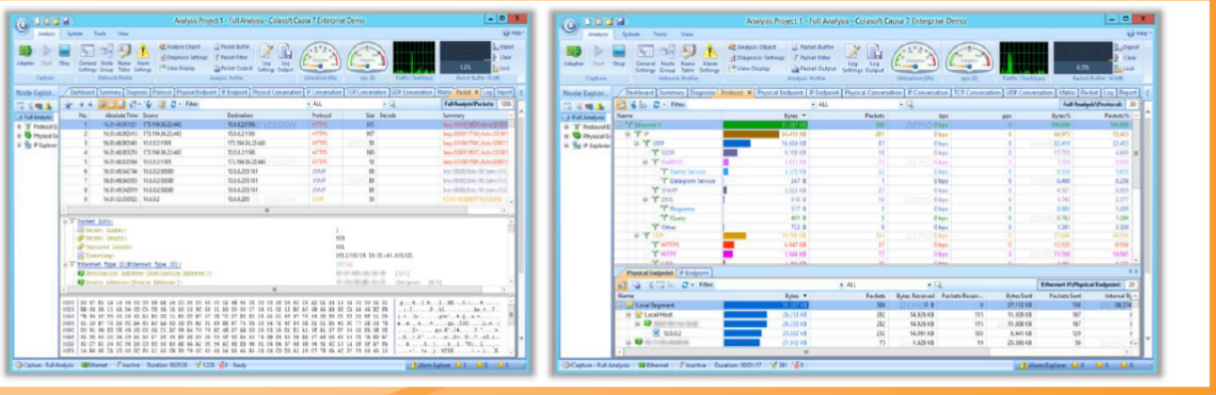
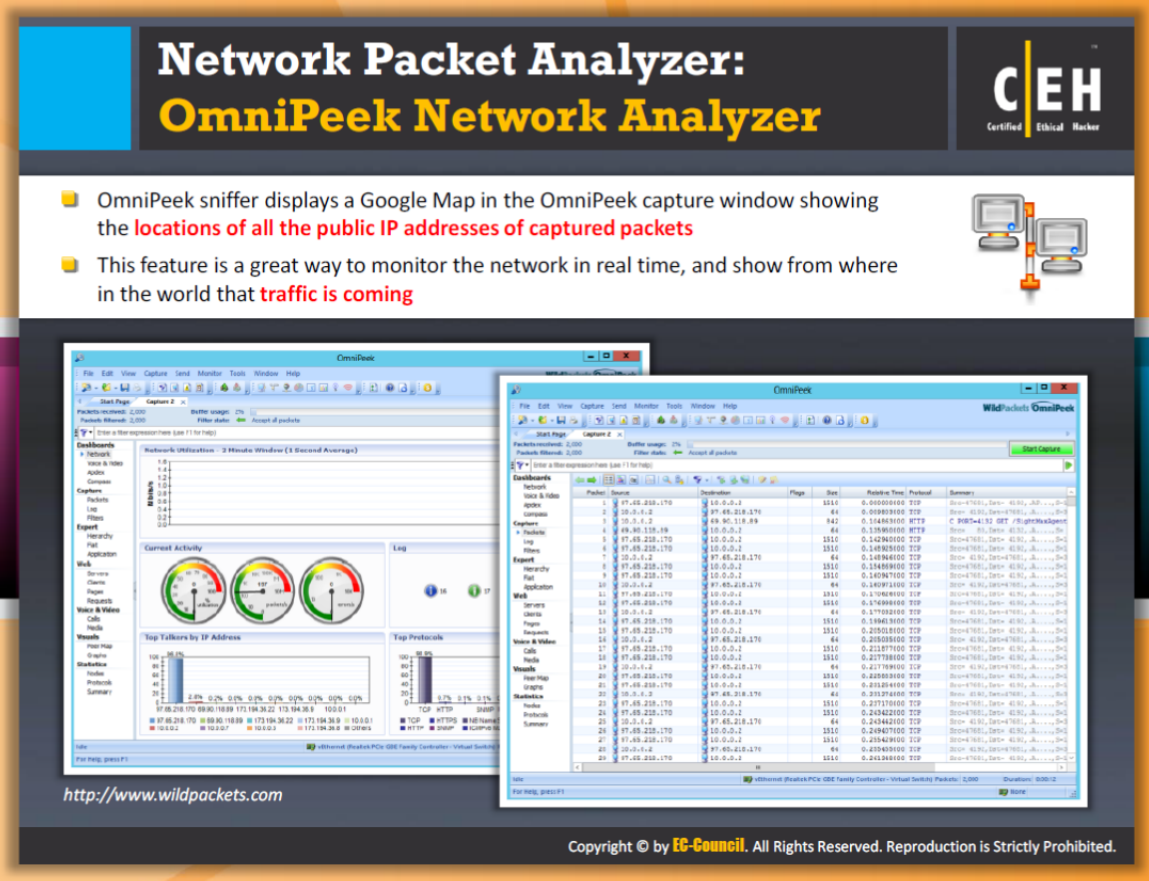


FIGURE 8.54: Capsa Network Analyzer Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Packet Analyzer: OmniPeek Network Analyzer

Source: http://www.wildpackets.com

OmniPeek Network Analyzer gives you **real-time visibility** and expert analysis of each part of the target network. This tool allows you to analyze, drill down, and fix the performance bottlenecks across multiple network segments. Analytic **plug-ins provide** targeted visualization and search abilities within OmniPeek. **Google Map** Plug-In enhances the analysis capabilities of OmniPeek. It displays a Google map in the OmniPeek capture window that shows the locations of all the public IP addresses of captured packets. This feature allows you to monitor the network in real time, and shows from where in the world that traffic is coming. Attackers can use this tool to analyze the network and inspect the packets in the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

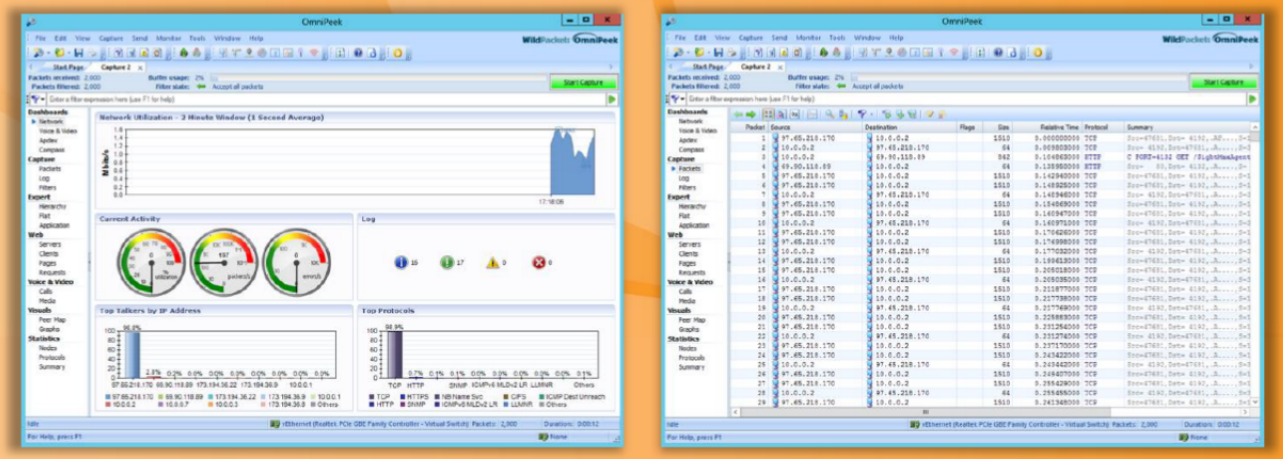
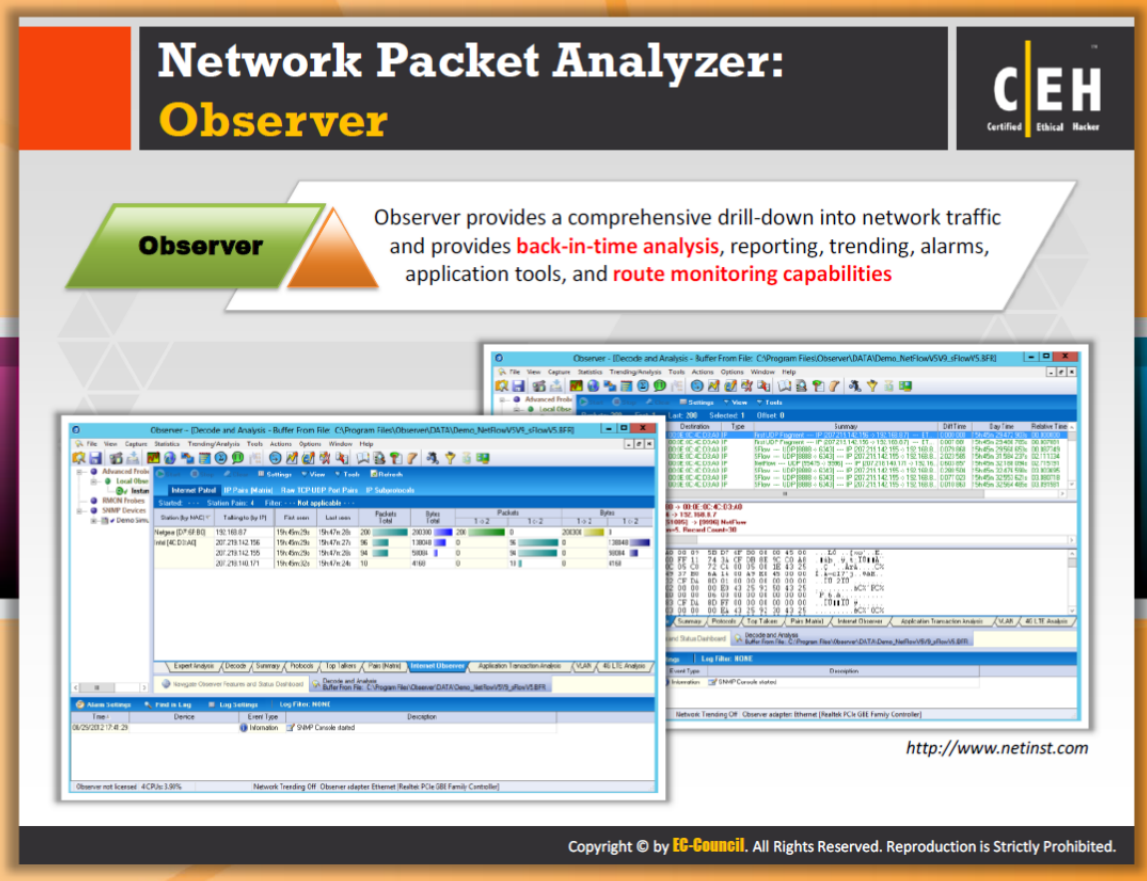


FIGURE 8.55: OmniPeek Network Analyzer Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Packet Analyzer: Observer

Source: http://www.netinst.com

Observer Standard provides **first-level network** analysis including **real-time packet captures** and decodes, filtering, real-time statistics, triggers and alarms, trending, and more across multiple topologies (LAN, wireless, and gigabit). You can use this tool to perform **network analysis** and **capture network packets**. It allows you to perform network monitoring across topologies, locations, and technologies.

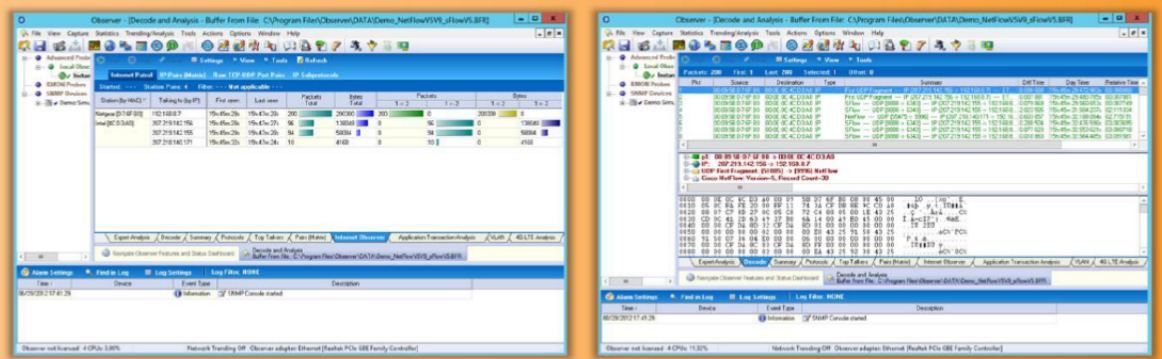
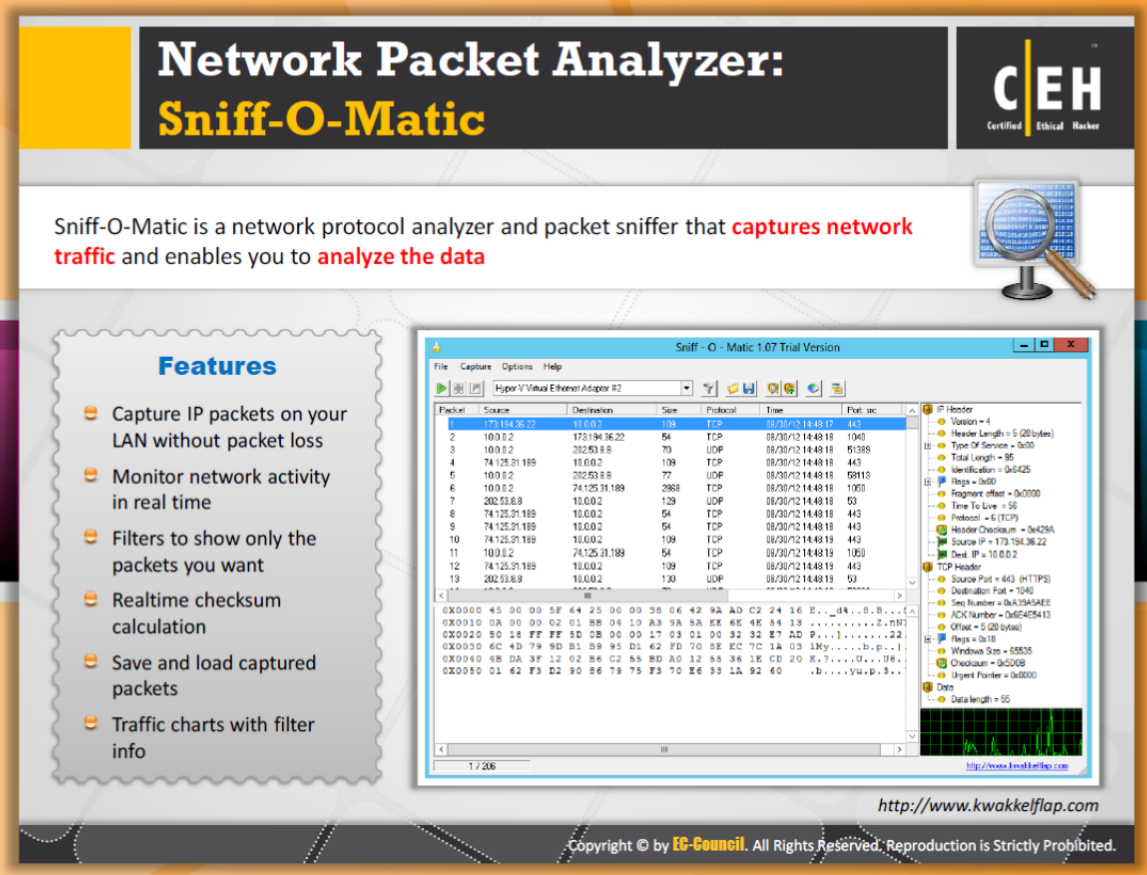


FIGURE 8.56: Observer Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Packet Analyzer: Sniff-O-Matic

Source: http://www.kwakkelflap.com

Sniff-O-Matic is a network **protocol analyzer** and a **packet sniffer**. It allows you to capture network traffic and enables you to analyze the data. It gives detailed information about packets in a tree structure or raw data view of the packet data. It allows you perform many more activities such as:

- Capture IP packets on your LAN without packet loss
- Monitor network activity in real time
- Filter to show only the packets you want
- Real-time checksum calculation
- Save and load captured packets
- Autostart capturing and continuous capture

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

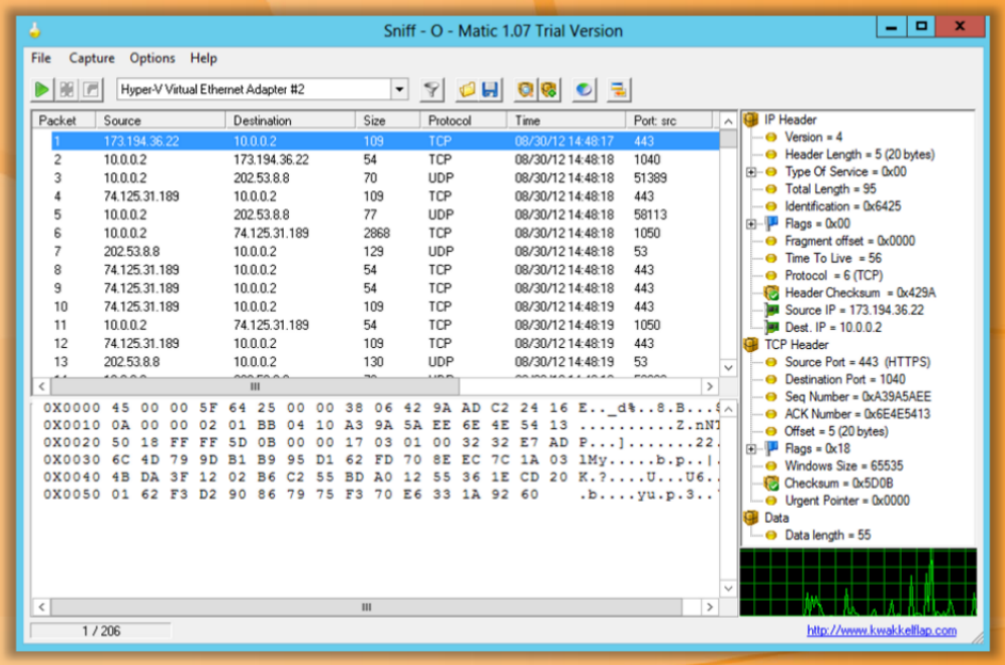
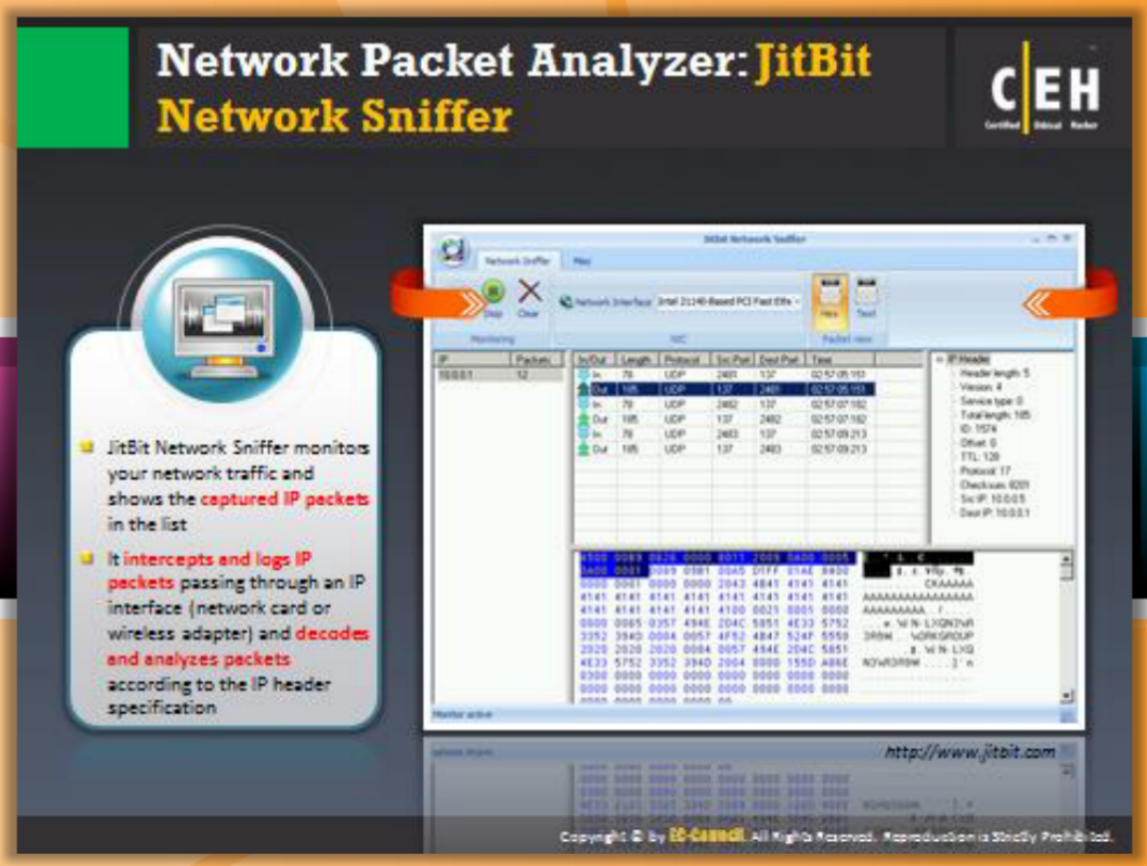


FIGURE 8.57: Sniff-O-Matic Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Packet Analyzer: JitBit Network Sniffer

Source: http://www.jitbit.com

JitBit Network Sniffer is a **network sniffer** tool that allows you to monitor target network traffic and capture and view IP packets. It shows the captured IP packets in the list. You can view packet contents in text or **HEX format**. With the help of this tool, you can intercept and log the IP packets passing through **NIC or wireless adapter**. It decodes and analyzes packets according to the IP header specification. It allows you to filter content suspected of network traffic. The attacker can use this tool to analyze the traffic and capture the IP packets over the target network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

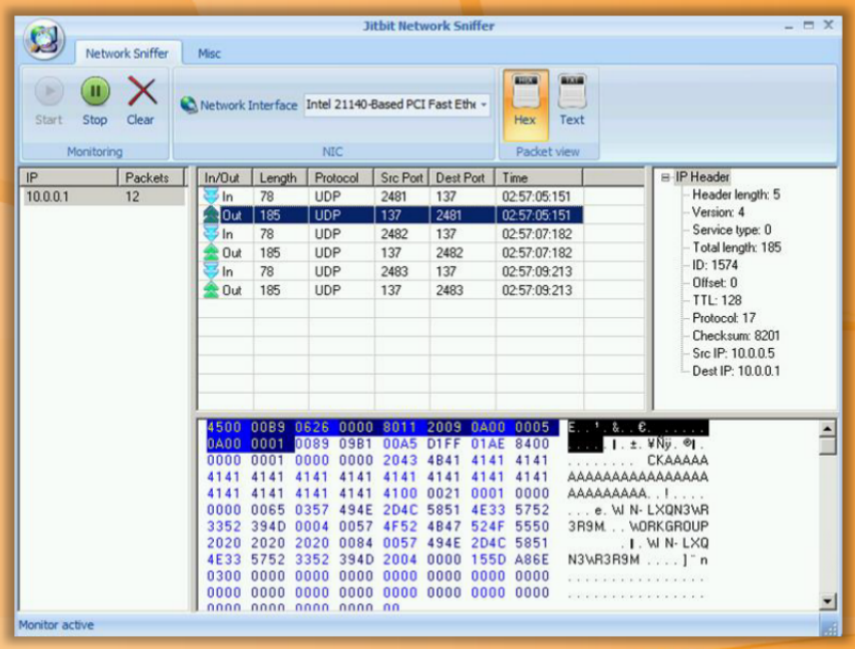


FIGURE 8.58: JitBit Network Sniffer Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Chat Message Sniffer: MSN Sniffer 2

Source: http://www.msnsniffer.com

MSN Sniffer 2 is an MSN chat-capturing and **impact-analysis tool**. It captures **MSN chats** across all computers in the same **LAN** and **analyzes** and saves in a database for future analysis. It allows you to capture the chat messages of each conversations in real time. You can see all captured chat messages in a chat history file. Installing this tool on any one computer of the target network will capture all the MSN chat messages traveling on the network.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

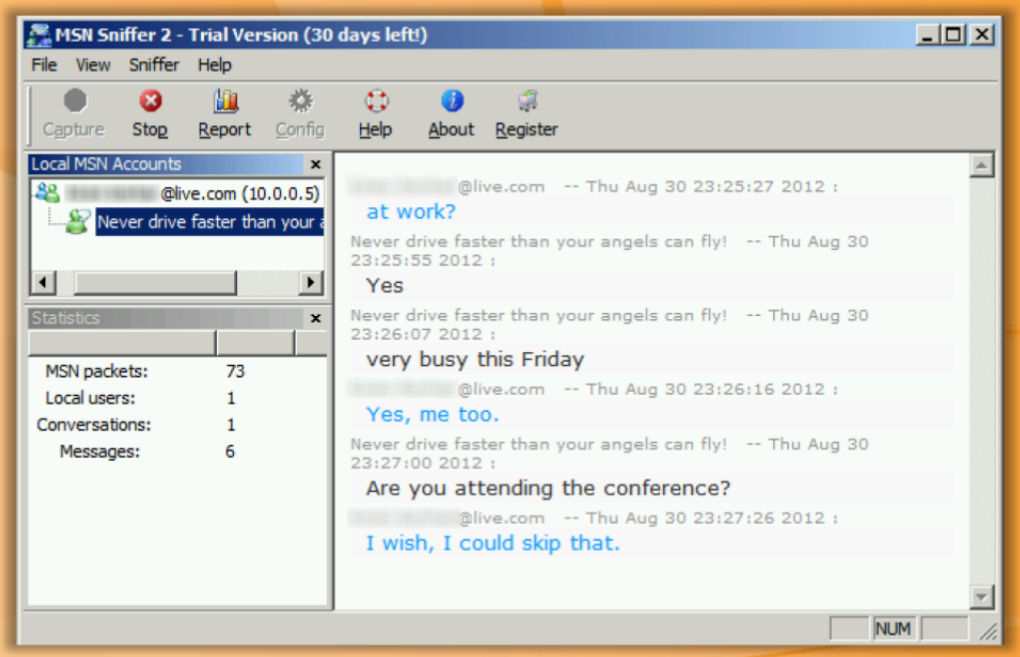
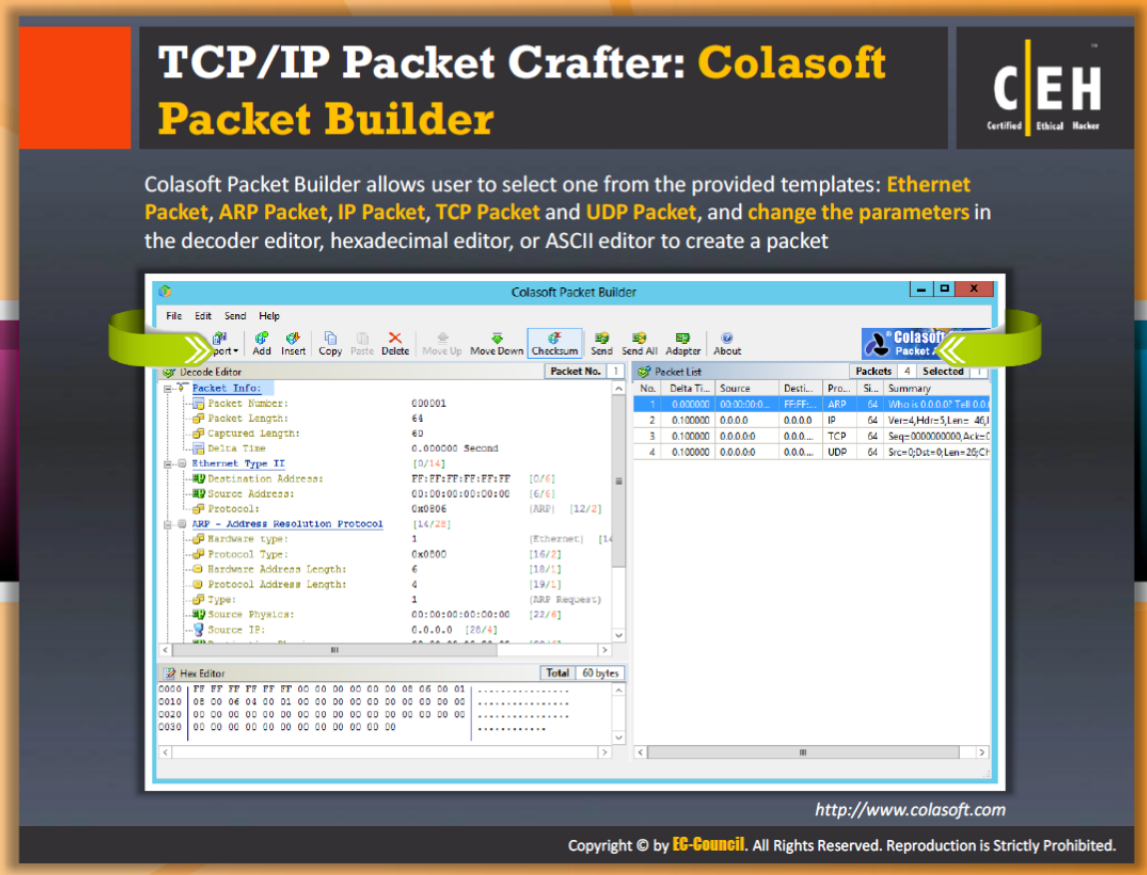


FIGURE 8.59: MSN Sniffer 2 Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



TCP/IP Packet Crafter: Colasoft Packet Builder

Source: http://www.colasoft.com

Colasoft Packet Builder is a **network packet crafter**, packet generator, or packet editor tool. It is used to create custom network packets. Attackers can use this tool to create **malicious network** packets to carry out the attack on the target network. You can also use this tool to pen test your own network against possible attacks by **creating custom packets**. The decoding editor of this tool allows you to edit specific protocol field values in the network packets. You can use any of the templates of Ethernet Packet, ARP Packet, IP Packet, TCP Packet, and UDP Packet to create custom packets.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

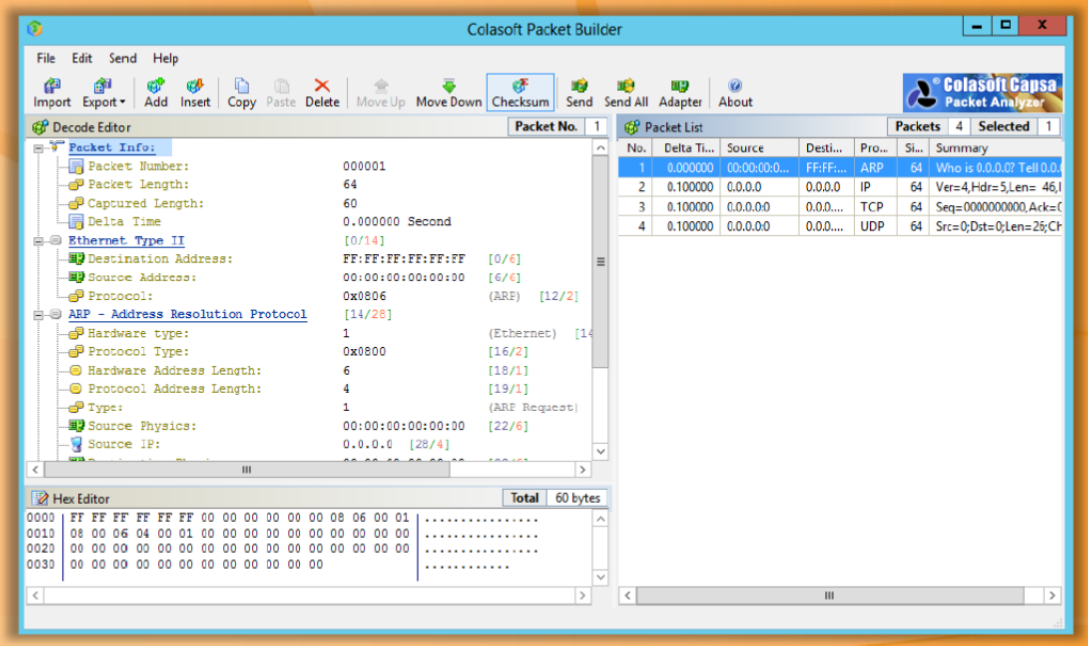


FIGURE 8.60: Colasoft Packet Builder Screenshot

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Sniffing Tools

In addition to the tools discussed so far, there are many other tools that are intended for the same purpose, i.e., monitoring network traffic and capturing and analyzing the packet data, etc. A list of sniffing tools along with their sources from which you can download the tools follows:

- Ace Password Sniffer available at http://www.effetech.com
- RSA NetWitness Investigator available at http://www.emc.com
- Big-Mother available at http://www.tupsoft.com
- EtherDetect Packet Sniffer available at http://www.etherdetect.com
- dsniff available at http://monkey.org
- EffeTech HTTP Sniffer available at http://www.effetech.com
- Ntop available at http://www.ntop.org
- Ettercap available at http://ettercap.sourceforge.net
- SmartSniff available at http://www.nirsoft.net
- EtherApe available at http://etherape.sourceforge.net

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Sniffing Tools (Cont'd)

The following is the continuation of the list of sniffing tools mentioned on the previous slide:

- Network Probe available at http://www.objectplanet.com
- Snort available at http://www.snort.org
- Sniff'em available at http://www.sniff-em.com
- MaaTec Network Analyzer available at http://www.maatec.com
- Alchemy Network Monitor available at http://www.mishelpers.com
- CommView available at http://www.tamos.com
- NetResident available at http://www.tamos.com
- Kismet available at http://www.kismetwireless.net
- AIM Sniffer available at http://www.effetech.com
- Netstumbler available at http://www.netstumbler.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Sniffing Tools (Cont'd)

The following is the continuation of the list of sniffing tools mentioned on the previous slide:

- IE HTTP Analyzer available at http://www.ieinspector.com
- MiniStumbler available at http://www.netstumbler.com
- PacketMon available at http://www.analogx.com
- NADetector available at http://www.nsauditor.com
- Microsoft Network Monitor available at http://www.microsoft.com
- NetworkMiner available at http://www.netresec.com
- PRTG Network Monitor available at http://www.paessler.com
- Network Security Toolkit available at http://www.networksecuritytoolkit.org
- Ethereal available at http://www.ethereal.com
- KSniffer available at http://ksniffer.sourceforge.net

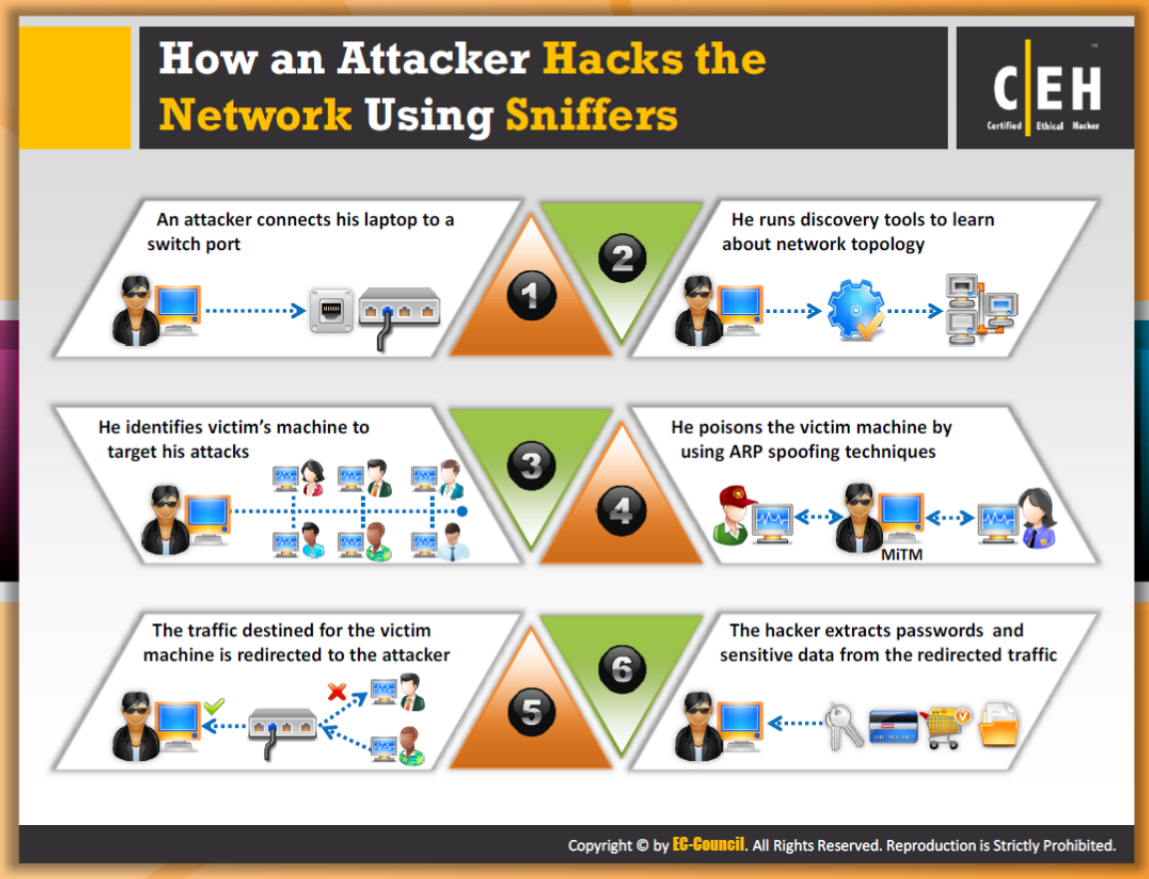
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Sniffing Tools (Cont'd)

The following is the continuation of the list of sniffing tools mentioned on the previous slide:

- IPgrab available at http://ipgrab.sourceforge.net
- WebSiteSniffer available at http://www.nirsoft.net
- ICQ Sniffer available at http://www.etherboss.com
- URL Helper available at http://www.urlhelper.com
- WebCookiesSniffer available at http://www.nirsoft.net
- York available at http://thesz.diecru.eu
- IP Traffic Spy available at http://www.networkdls.com
- SniffPass available at http://www.nirsoft.net
- Cocoa Packet Analyzer available at http://www.tastycocoabytes.com
- vxSniffer available at http://www.cambridgevx.com

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How an Attacker Hacks the Network Using Sniffers

You know that attackers use sniffing tools to **sniff packets** and **monitor network traffic** on the target network. A scenario that describes how an attacker makes use of sniffers to hack particular networks follows.

Step1: Once an attacker decides to **hack a network**, he or she first finds out the appropriate switch to access the network and connects his or her system to one of the ports on the switch, as shown in following figure:

FIGURE 8.61: Step 1 Find the Appropriate Switch to Hack the Network

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 2: Once the attacker succeeds in getting connected to the network, he or she tries to determine network information such as **topology** of the network by using some network discovery tools, as shown in following figure:

FIGURE 8.62: Step 2 Gain the Network Information

Step 3: By analyzing the network topology. the attacker identifies the victim's machine to target his or her attacks:

FIGURE 8.63: Step 3 Analyze the Network Topology

Step 4: Once the attacker knows his or her target machine, then he or she uses ARP spoofing techniques to send fake ("spoofed") Address Resolution Protocol (ARP) messages, as follows:

FIGURE 8.64: Step 4 Use the ARP Spoofing Techniques

Step 5: The previous step helps the attacker to divert all the traffic of the victim's computer to his or her computer. This is a typical man-in-the-middle (MITM) type of attack, as shown in following figure:

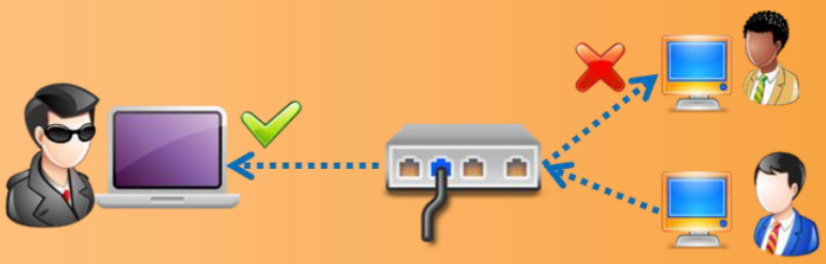


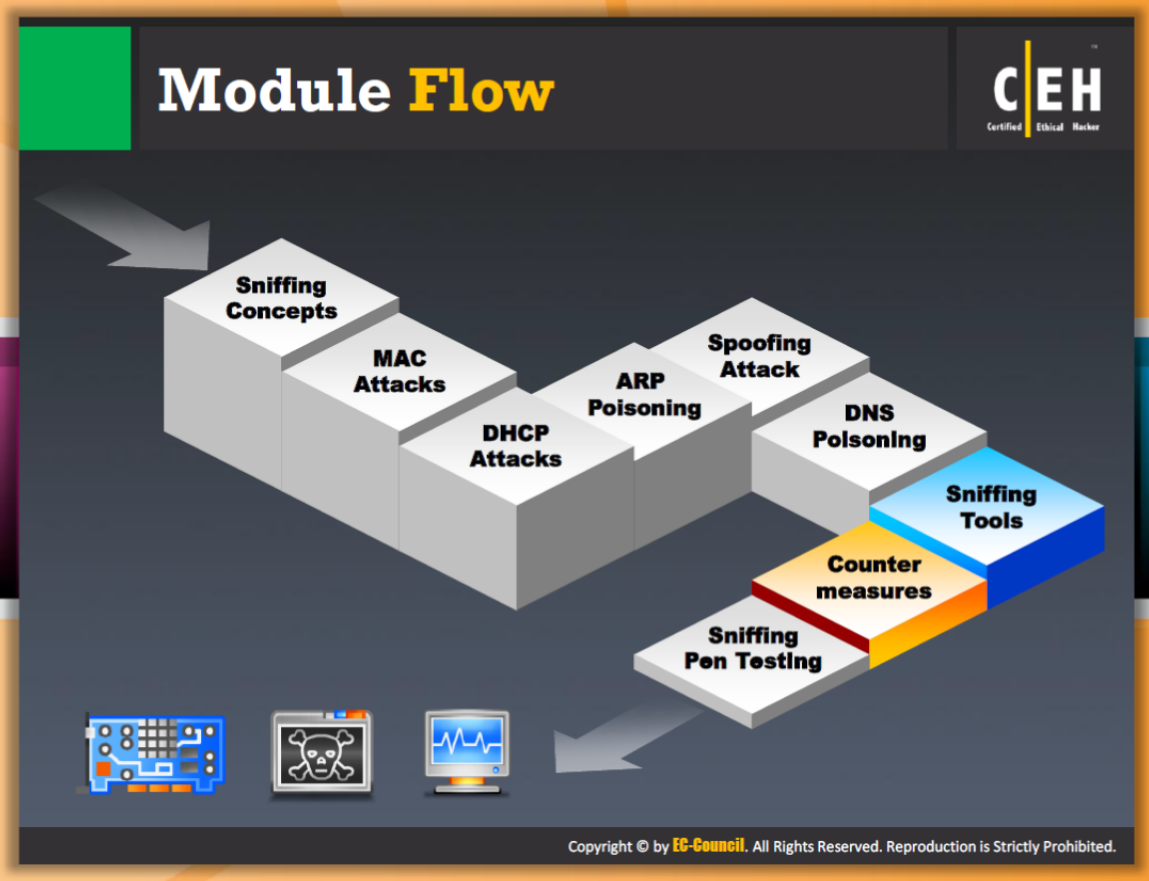
FIGURE 8.65: Step 5 Divert the Traffic

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 6: Now the attacker is able to see all the data packets sent and received by the victim. He or she can now extract the sensitive information from the packets such as passwords, user names, credit card details, PINs, etc.; thus, the **attacker succeeds** in sniffing packets from the target network.

FIGURE 8.66: Step 6 Attacker Succeeds in Sniffing Packets

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

So far, we have discussed how attackers carry out different types of sniffing attacks on the target network and the different types of sniffing tools that attackera can use to sniff the packets and monitor the traffic of target network. Now it's time to learn the actions you can protect you against sniffing attacks.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This section covers various countermeasures that can be applied to protect a network against sniffing.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against Sniffing

Here are some countermeasures that can help you avoid sniffing attacks:

- Restrict the physical access to the **network media** to ensure that a packet sniffer cannot be installed
- Use encryption to protect confidential information
- Permanently add the MAC address of the gateway to the ARP cache
- Use static **IP addresses** and **static ARP tables** to prevent attackers from adding the spoofed ARP entries for machines in the network
- Turn off network identification broadcasts and if possible, restrict the network to authorized users in order to protect network from being discovered with sniffing tools
- Use IPv6 instead of IPv4 protocol
- Use encrypted sessions such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, SSL for email connections, etc. to protect wireless network users against sniffing attacks

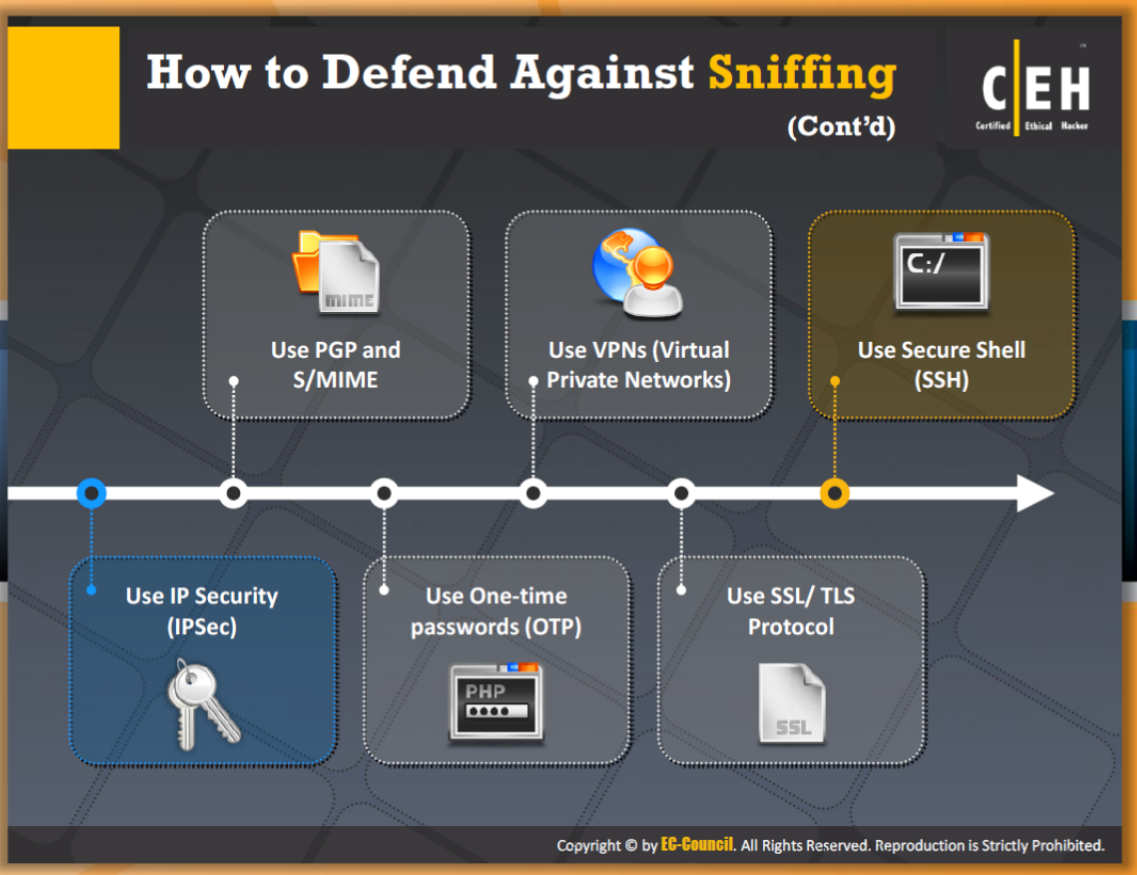
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against Sniffing (Cont'd)

The list of sniffing countermeasures continues as follows:

- Use **HTTPS** instead of HTTP to protect user names and passwords
- Use switches instead of hubs as switches deliver data only to the intended recipient
- Use crossover cables as they restrict unauthorized hosts from being accidentally or intentionally plugged into hubs and switches
- Password authenticate the **shared folders and services**
- Always encrypt the communication between the wireless PC and access point to prevent MAC spoofing
- Retrieve MAC directly from NIC instead of the OS; this prevents **MAC address spoofing**
- Use antisniff tools to determine if any NICs are running in promiscuous mode

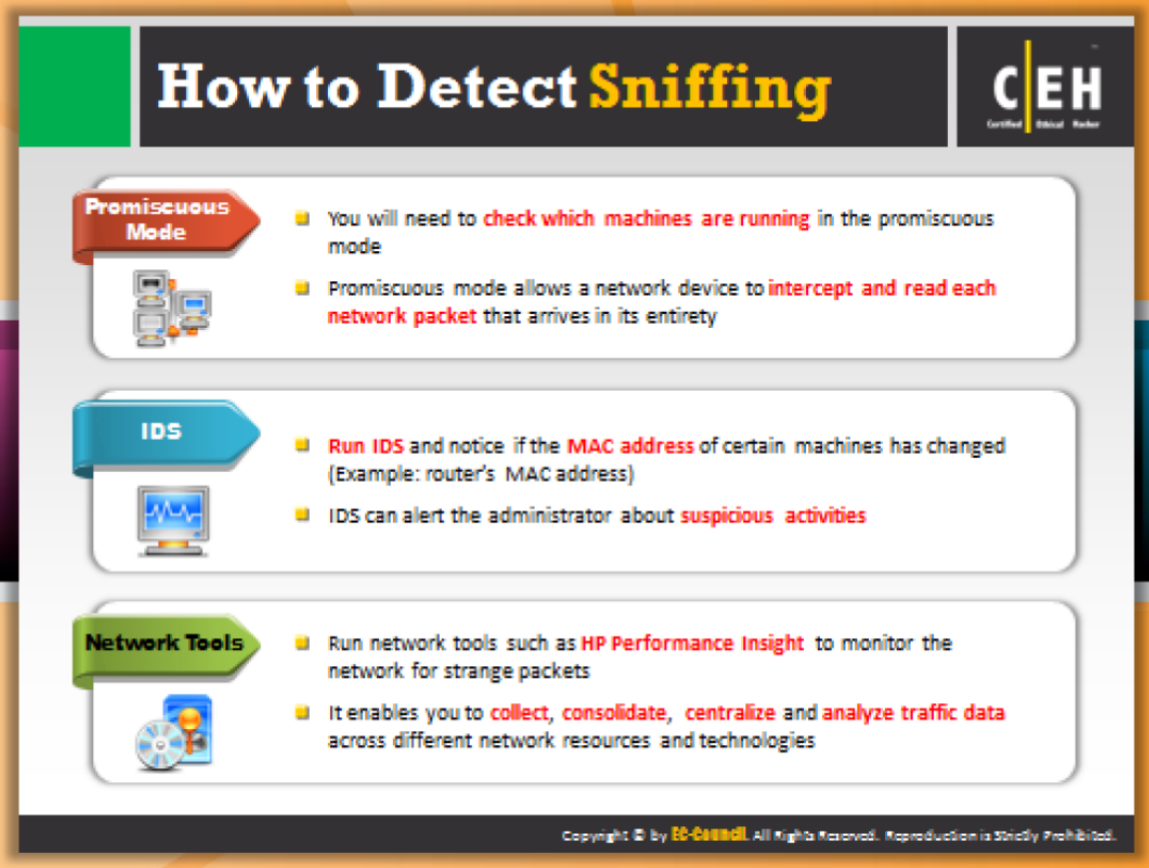
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Defend Against Sniffing (Cont'd)

- Use IP security (IPSec)
- Use PGP and S/MIME
- Use one-time passwords (OTPs)
- Use VPNs (virtual private networks)
- Use SSL/TLS Protocol
- Use Secure Shell (SSH)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How to Detect Sniffing

Promiscuous Mode

It is not easy to detect a sniffer on the network as it only captures data and runs in promiscuous mode. The sniffer leaves no trace, since it does not transmit data. To find such sniffers, check for the systems that are running in promiscuous mode. Promiscuous mode is a mode of the network interface card of the system that allows all packets (traffic) to pass, without validating its destination address. Standalone sniffers are difficult to detect, because they do not transmit data traffic. The reverse DNS Lookup method can be used to detect non-standalone sniffers.

There are a lot of tools available to detect promiscuous mode on the system, such as Nmap.

IDS

An intrusion detection system (IDS) is a security mechanism that helps you to detect sniffing activities on the network. If you run IDS on your network, then it notifies or alerts you when a suspicious activity such as sniffing, MAC spoofing, etc. occurs.

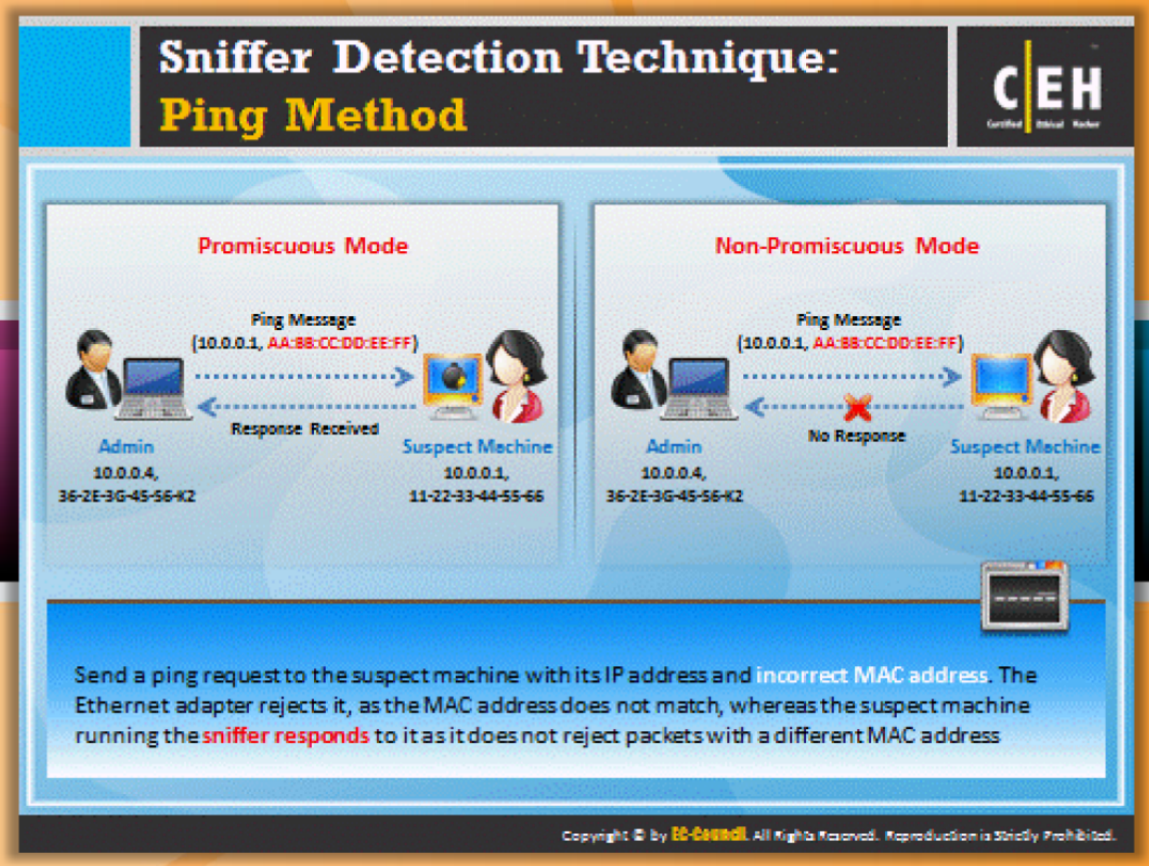
Network Tools

You can also run network tools such as HP Performance Insight to monitor the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

network for strange packets such as packets with spoofed addresses. This tool enables you to collect, consolidate, centralize, and analyze traffic data across different network resources and technologies

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffer Detection Technique: Ping Method

To detect the sniffer on a **particular network**, you need to identify the system on the network running in **promiscuous mode**. Let's see how the ping method is useful in detecting a system that runs in promiscuous mode, which in turns helps to detect sniffers installed on the network.

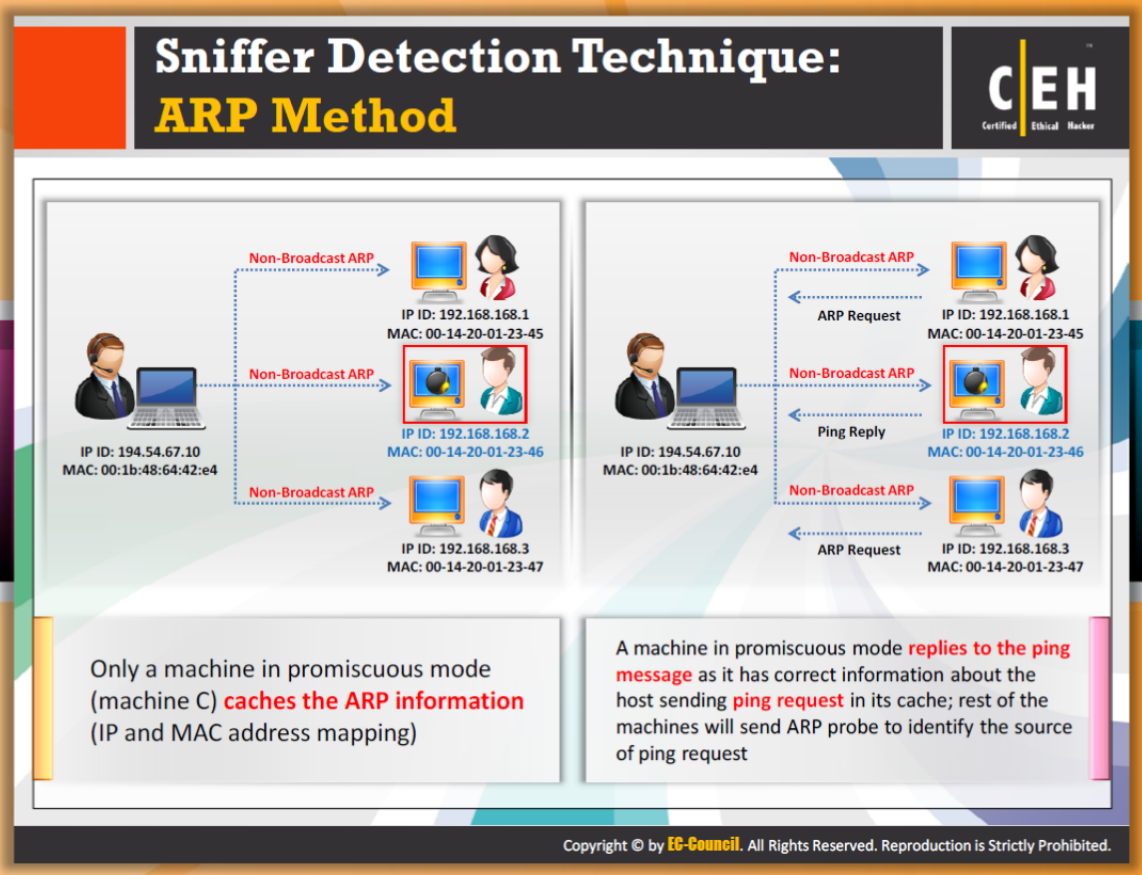
The idea behind this method is that you just need to send a ping request to the suspect machine with its IP address and incorrect **MAC address**. The Ethernet adapter in the network is rejected as the MAC address does not match, whereas the suspect machine running the sniffer responds to it as it does not reject packets with a different MAC address. Thus, this response will help you to identify the sniffer in the network.

See the difference between ping responses of a system that runs in promiscuous mode and a system that runs in non-promiscuous mode.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.67: Sniffer Detection Technique by Using Ping Method

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

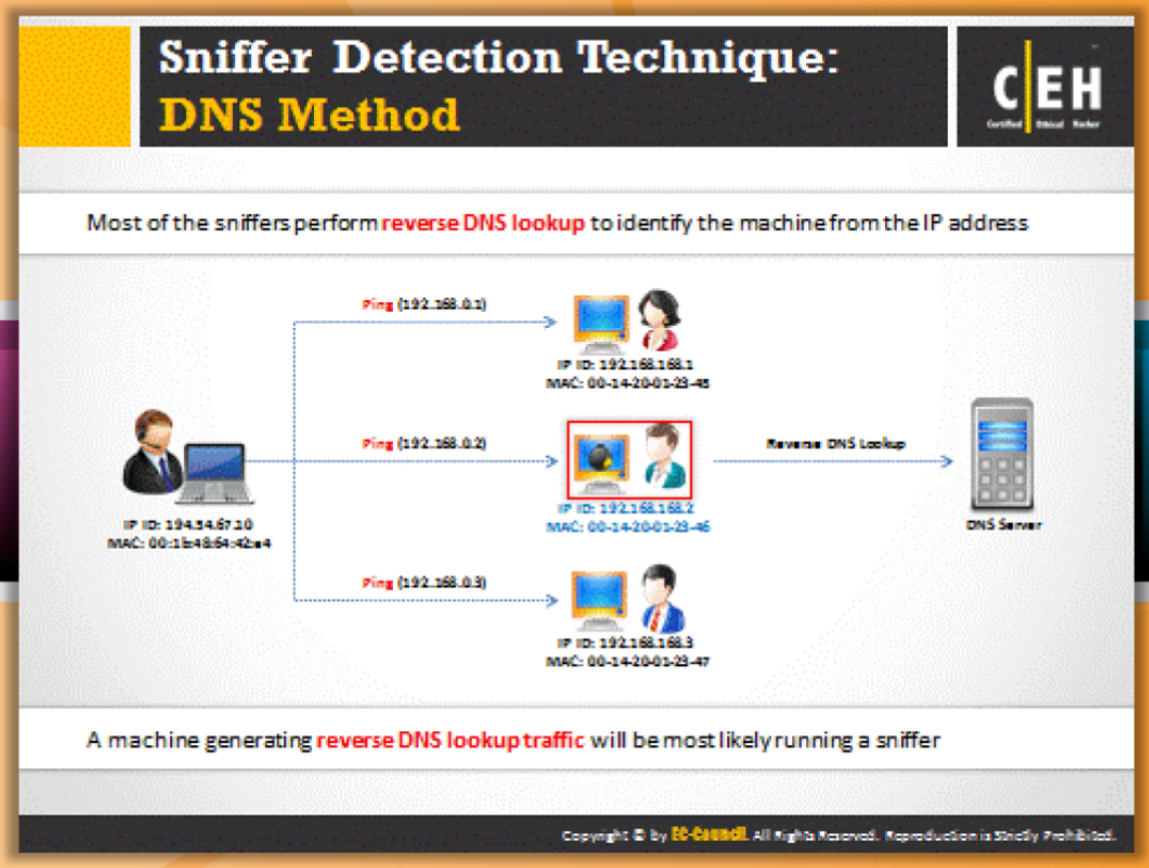


Sniffer Detection Technique: ARP Method

In this technique, you need to send a **non-broadcast ARP** to all the nodes in the network. The node that runs in promiscuous mode on the network will cache your ARP address. Now you broadcast the ping message on the network with your **IP address** but a different Mac Address. In this case, only the node that has your MAC address (that was cached earlier) will be able to respond to your broadcast ping request, as shown in the following figure. Thus, you can detect the node on which the sniffer is running.

FIGURE 8.68: Sniffer Detection Technique by Using ARP Method

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffer Detection Technique: DNS Method

The **reverse DNS lookup** is the opposite of the **DNS lookup method**. Sniffers use reverse DNS lookup and increase network traffic. This increase in network traffic can be an indication of the presence of a sniffer on the network. The computers on this network are in promiscuous mode.

Reverse DNS lookup can be carried out either remotely or locally. The organization's **DNS server** has to be monitored to identify incoming reverse DNS lookups. The method of sending ICMP requests to a non-existing IP address can be used to monitor reverse DNS lookups. The computer performing the reverse DNS lookup would respond to the ping, thus identifying it as hosting a sniffer.

For local reverse DNS lookups, the detector should be configured in promiscuous mode. Send an **ICMP request** to a non-existing IP address, and view the response. If a response is received, the responding machine can be identified as performing reverse DNS lookup on the local machine.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

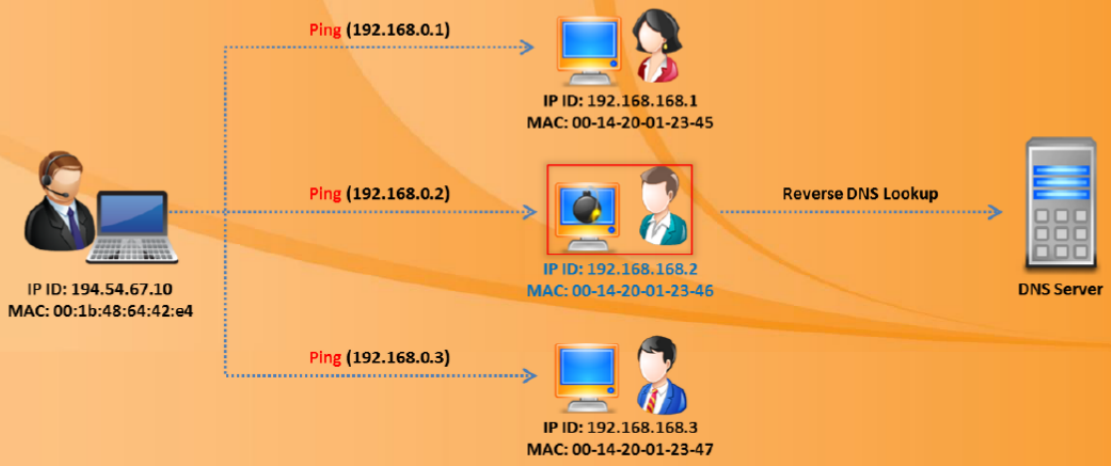
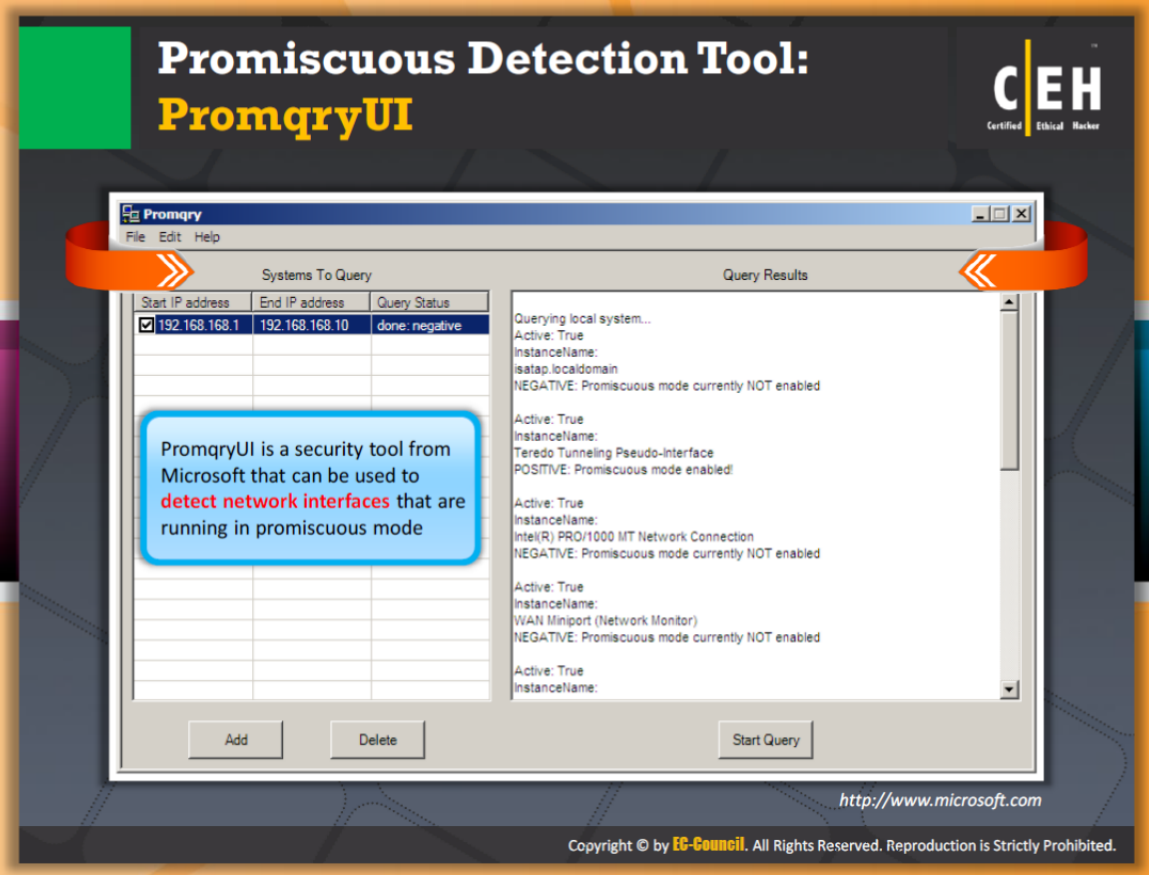


FIGURE 8.69: Sniffer Detection Technique by Using DNS Method

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Promiscuous Detection Tool: PromqryUI

Source: http://www.microsoft.com

The PromqryUI tool allows you to detect which **network interface card** is running in promiscuous mode. It can determine accurately if a modern managed Windows system has network interfaces in promiscuous mode. If a system has network interfaces in promiscuous mode, it may indicate the presence of a network sniffer running on the system.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

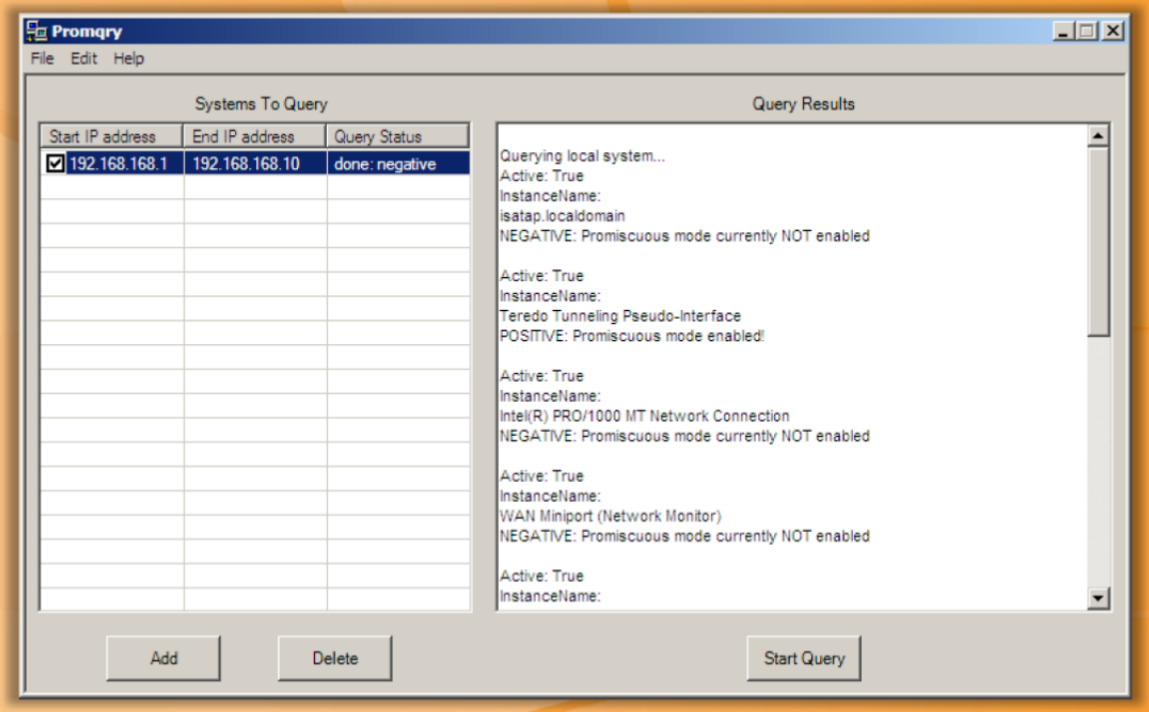
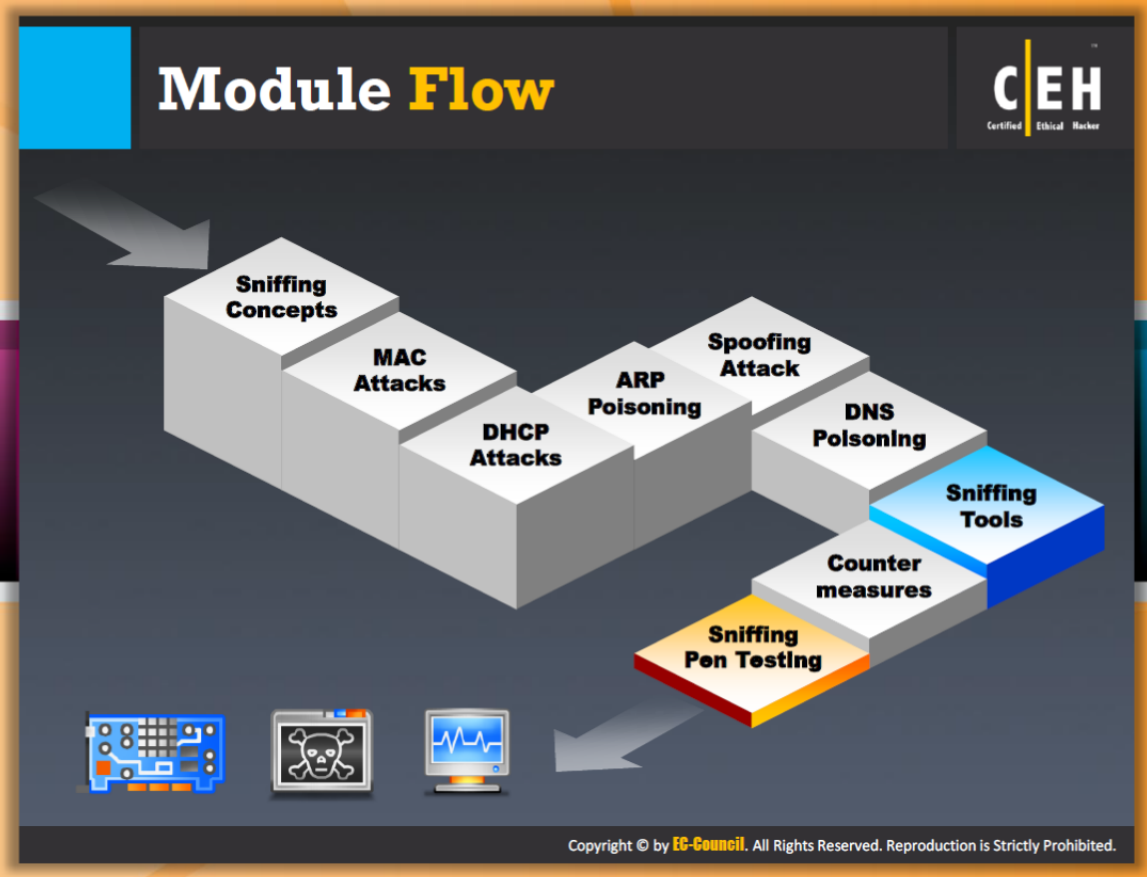


FIGURE 8.70: Promiscuous Detection By Using PromqryUI

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Flow

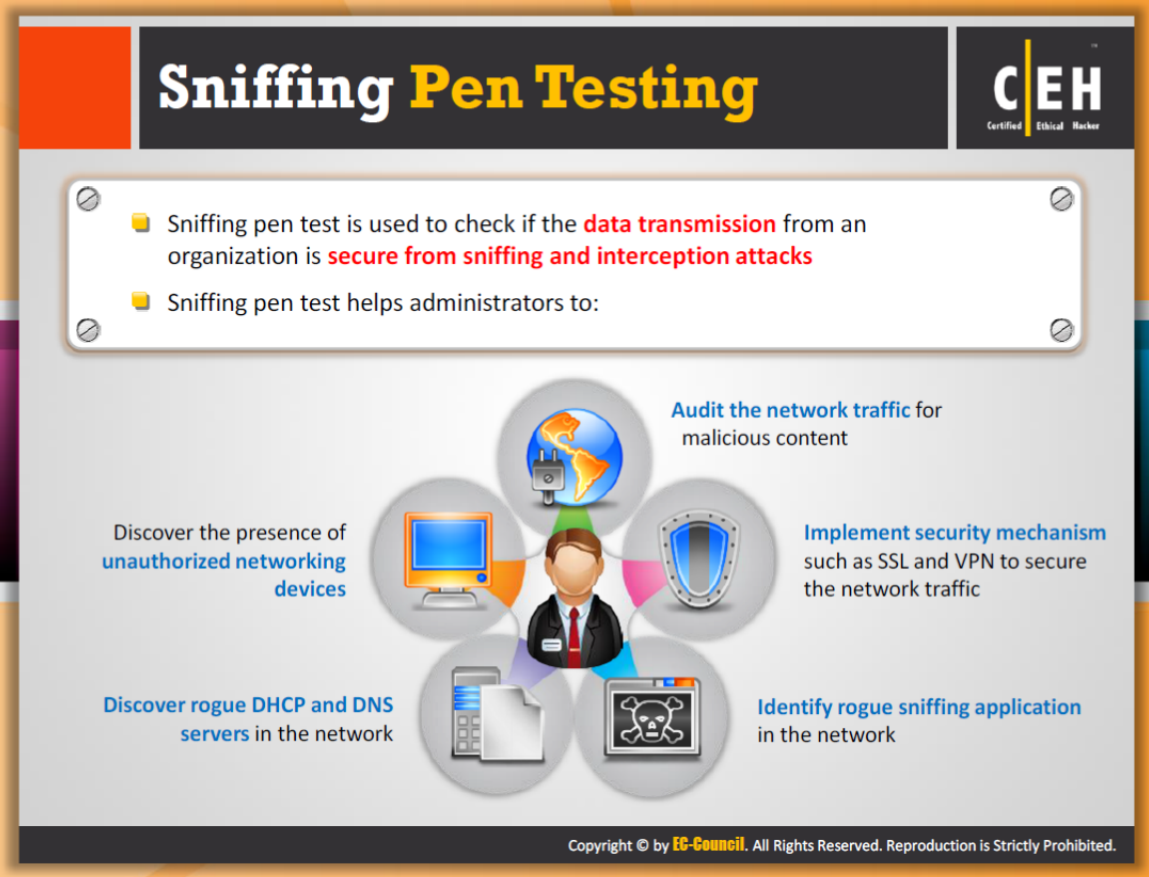
So far, we have discussed all the necessary concepts, attack techniques, and tools to perform sniffing pen testing. We also discussed the countermeasures to be applied in order to enhance the security of a target organization. Now it's time to conduct sniffing pen testing on the target organization.

Sniffing Concepts	DNS Poisoning
MAC Attacks	Sniffing Tools
DHCP Attacks	Countermeasures
ARP Poisoning	Sniffing Pen Testing
Spoofing Attack	

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This section highlights the need for sniffing pen testing and the steps involved in it.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

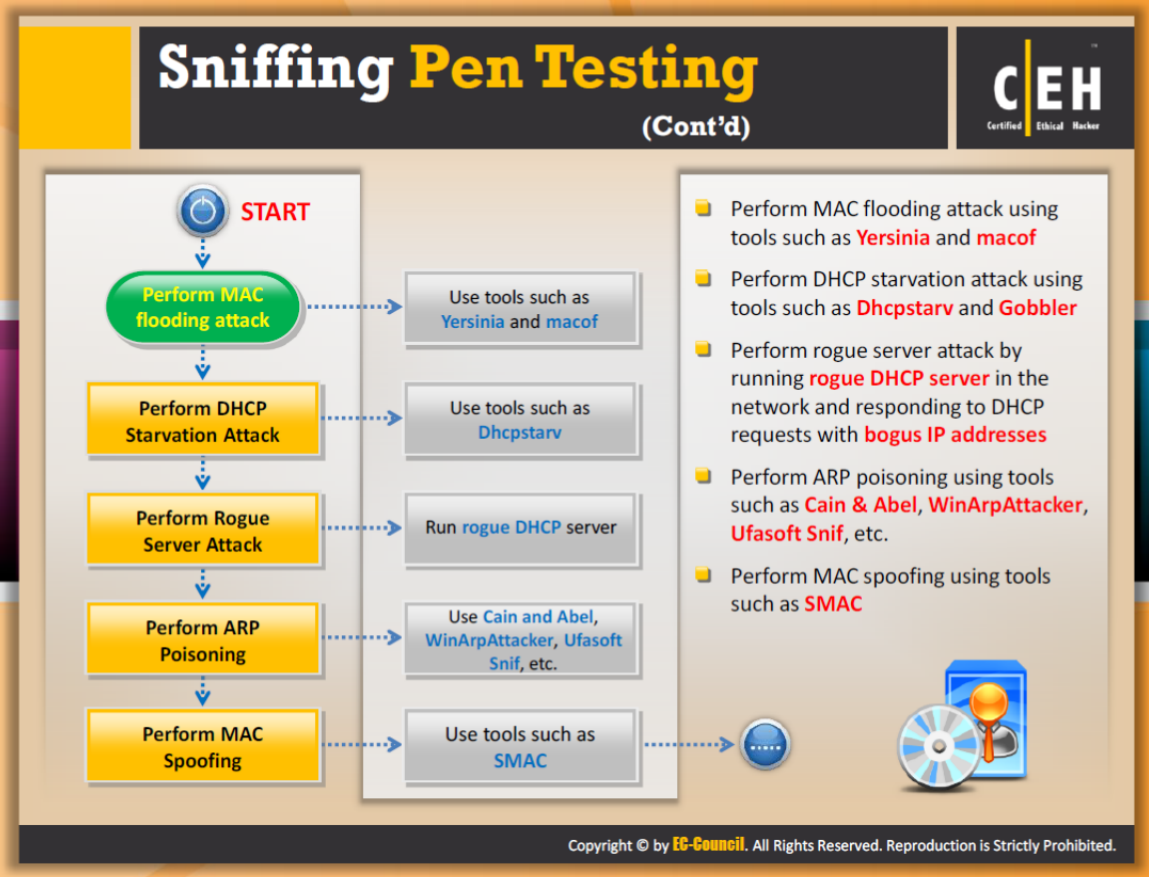


Sniffing Pen Testing

You have learned how the attacker sniffs the conversation in the target network in order to gain **confidential information**. Now in this section, you will learn how to test a target network for sniffing attacks. As a **penetration tester**, you should simulate the actions of an attacker performing a sniffing attack to test your target network against sniffing. Sniffing penetration testing will help you to determine whether your network is vulnerable to any type of sniffing or interception attacks. Sniffing pen testing helps administrator 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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Pen Testing (Cont'd)

While doing pen testing you need to keep in mind that you have to simulate sniffing attacks just as an attacker would. Try all possible ways of sniffing the network. This ensures the full scope of the test.

You need to follow certain pen testing steps that help you to perform the pen test successfully and correctly. Let's begin with the sniffing pen testing steps:

Step 1: Perform a MAC flooding attack

Flood the switch with many Ethernet frames, each containing different source **MAC addresses**. Check whether the switch enters into **failopen mode**, a mode in which the switch broadcasts data to all ports rather than just to the port intended to receive the data. If this happens, then attackers have the probability to sniff your network traffic. You can do this by using tools such as Yersinia and macof.

Step 2: Perform a DHCP starvation attack

Broadcast the DHCP requests with spoofed MAC addresses. At a certain point, this may exhaust the DHCP server's address space available for a period of time. If this happens, then attackers have the chance to sniff network traffic or DHCP requests of your clients by building a rogue

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DHCP server. You can test for **DHCP starvation attacks** using tools such as Dhcpstarv and Gobbler.

Step 3: Perform a rogue server attack

Perform rogue server attacks by running a **rogue DHCP server** in the network and responding to DHCP requests with bogus IP addresses.

Step 4: Perform an ARP poisoning attack

Try to compromise the ARP table and change the MAC address so that the IP address points to another machine. If you can do this task successfully, then attackers can also do the same thing and steal your information by changing the MAC address to their own system. This can be done by using tools such as Cain & Abel, WinArpAttacker, and Ufasoft snif.

Step 5: Perform MAC spoofing

Try to spoof the MAC address on the network card. Try to change the factory-assigned MAC address of a networked device. If you are able to do this, then there is a possibility to bypass access control lists on routers or servers by pretending to be another device on the network. If your network entertains this kind of attack, then attackers can also break into your network and steal data. You can do this by using tools such as **SMAC**.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Pen Testing (Cont'd)

The steps mentioned as follows are the continuation of sniffing pen testing steps mentioned on the previous slide:

Step 6: Perform IRDP spoofing

Perform IRDP spoofing by sending spoofed **IRDP router** advertisement messages to the host on the subnet. Check whether the router changes its default router to the malicious route suggested by the advertisement messages or not. If the router changes its default path, then it is vulnerable to DoS attacks, passive sniffing, and/or **man-in-the-middle attacks**.

Step 7: Perform DNS spoofing

Perform **DNS spoofing** using techniques such as arpspoof/dnsspoof. The DNS spoofing attack is about misdirecting the victim to another address that is under control of the attacker. In this attack, the attacker intercepts the DNS request of the victim and sends a response with a spoofed IP address before the actual response arrives to the victim system. The victim is thereby redirected to the attacker's site. To avoid this kind of attack, proper **IDS/IPS** should be maintained.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 8: Perform cache poisoning

Perform cache poisoning by sending a Trojan to the victim's machine that changes proxy server settings in IE to that of attackers, thus redirecting to a **fake website**.

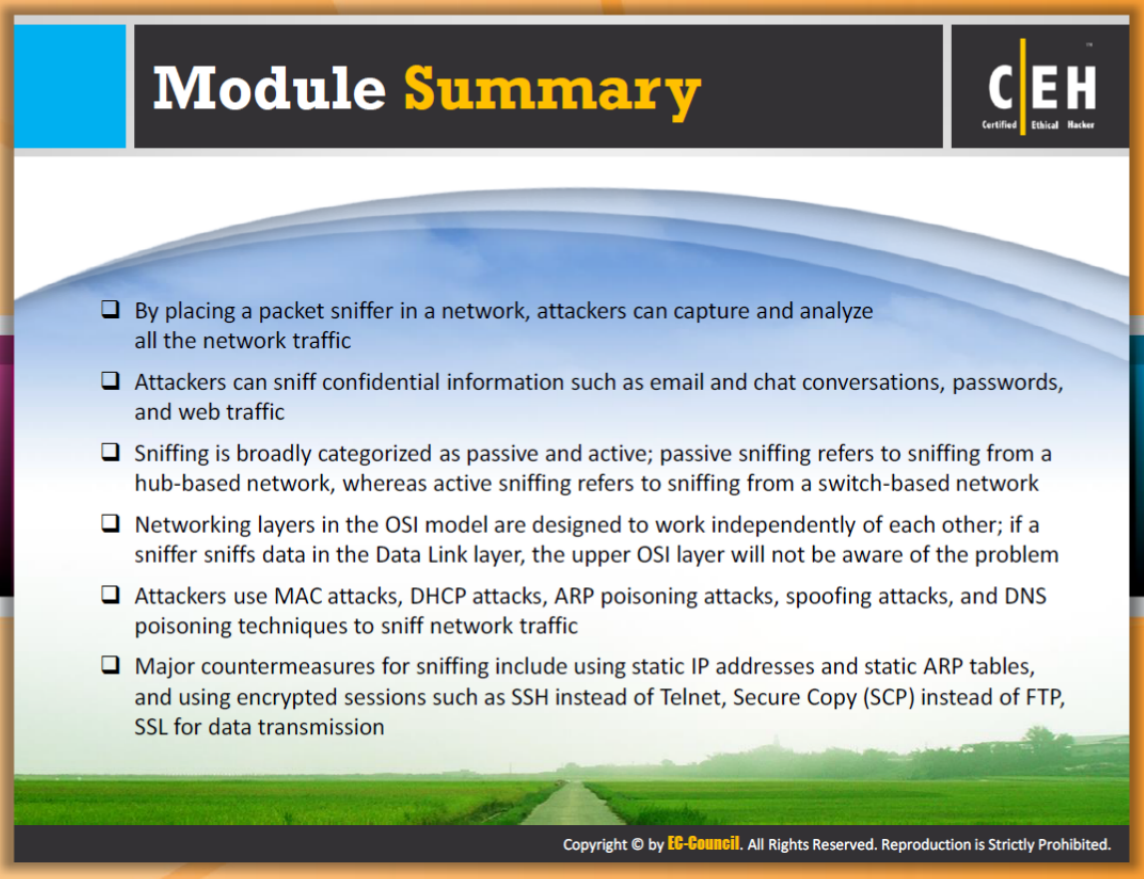
Step 9: Perform Proxy Server DNS Poisoning

Perform proxy server **DNS poisoning** to test for sniffing. In this type of attack, the attacker sets up a proxy server and sets a rogue DNS as the primary DNS entry in the proxy server system. Then the attacker lures the victim to use the attacker's **proxy server**. If the victim uses the attacker's proxy server, the attacker can sniff all the traffic between victim and the website he or she communicates with.

Step 10: Document all findings

Once you perform all tests, document all the findings and the tests conducted. This helps you to analyze the target's security and plan respective countermeasures to cover the security gaps, if any.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



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.
- Sniffers operate at the Data Link layer of the OSI model and do not adhere to the same rules as applications and services that reside further up the stack.
- 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, and SSL for data transmission.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.