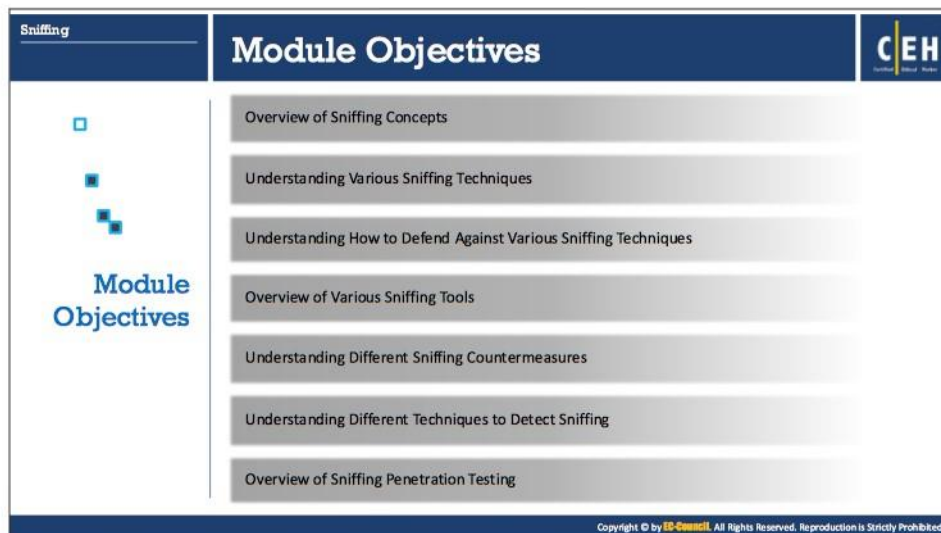




Module 08

## Sniffing

This page is intentionally left blank.



**Sniffing** **Module Objectives** **CEH**

- Overview of Sniffing Concepts
- Understanding Various Sniffing Techniques
- Understanding How to Defend Against Various Sniffing Techniques
- Overview of Various Sniffing Tools
- Understanding Different Sniffing Countermeasures
- Understanding Different Techniques to Detect Sniffing
- Overview of Sniffing Penetration Testing

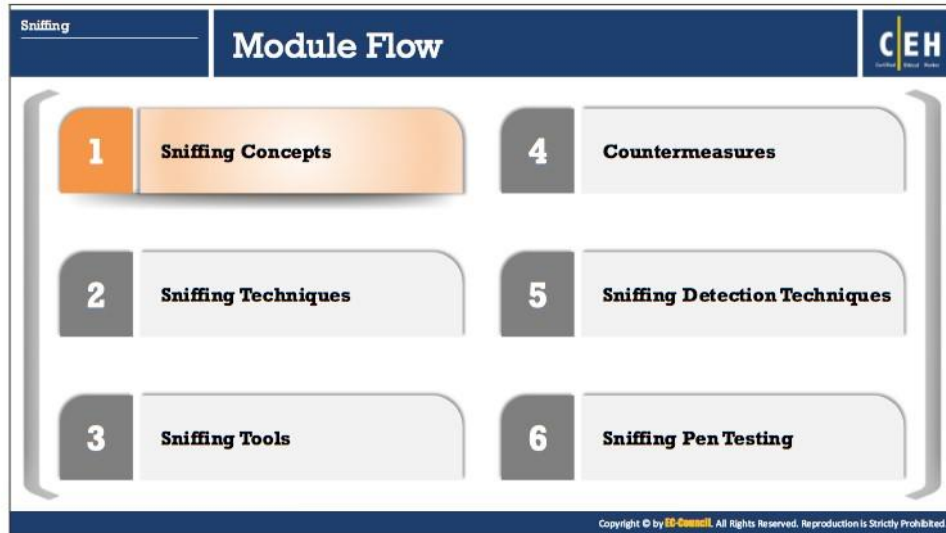
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Module Objectives

This module starts with an overview of sniffing concepts and provides an insight into MAC, DHCP, ARP, MAC spoofing, and DNS poisoning attacks. Later the module discusses various tools, countermeasures, and sniffing detection techniques. The module ends with an overview of penetration (pen) testing steps that an ethical hacker should follow to perform the security assessment of a target.

At the end of this module, you will be able to:

- Describe the sniffing concepts
- Explain different MAC attacks
- Explain different DHCP attacks
- Describe the ARP poisoning
- Explain different MAC spoofing attacks
- Describe the DNS poisoning
- Use different sniffing tools
- Apply sniffing countermeasures
- Apply various techniques to detect sniffing
- Perform sniffing penetration testing



### Sniffing Concepts

This section describes network sniffing and threats, how a sniffer works, active and passive sniffing, how an attacker hacks a network using sniffers, protocols vulnerable to sniffing, sniffing in the data link layer of the OSI model, hardware protocol analyzers, SPAN ports, wiretapping, and lawful interception.

## Network Sniffing

### Packet Sniffing

- Packet sniffing is a process of **monitoring and capturing all data packets** passing through a given network using a software application or hardware device
- It allows an attacker to observe and **access the entire network traffic** from a given point
- Packet sniffing allows an attacker to **gather sensitive information** such as Telnet passwords, email traffic, syslog traffic, router configuration, web traffic, DNS traffic, FTP password, chat sessions, account information, etc.

### How a Sniffer Works

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

The diagram shows a network topology where an attacker PC is connected to a switch. The attacker PC is labeled 'Attacker PC running NIC Card in Promiscuous Mode'. A dashed arrow points from the attacker PC to the switch, labeled 'Attacker forces switch to behave as a hub'. The switch is connected to several other devices (represented by icons of people at computers) and to the Internet. Dotted lines represent data packets being captured by the attacker PC from the switch.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Network Sniffing

Packet sniffing is a process of monitoring and capturing all data packets passing through a given network by using a software application or a hardware device. Sniffing is straightforward in hub-based networks, as the traffic on a segment passes through all the hosts associated with that segment. However, most networks today work on switches. 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 Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network.

An attacker needs to manipulate the functionality of the switch in order to see all the traffic passing through it. A packet sniffing program (also known as a sniffer) can capture data packets only from within a given subnet, which means that it cannot sniff packets from another network. Often, any laptop can plug into a network and gain access to it. Many enterprises' switch ports are open. A packet sniffer placed on a network in promiscuous mode can capture and analyze all of the network traffic. Sniffing programs turn off the filter employed by Ethernet network interface cards (NICs) to prevent the host machine from seeing other stations' traffic. Thus, sniffing programs can see everyone's traffic.

Though most networks today employ 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 relatively easy. It allows an attacker to observe and access the entire network traffic from one point. Packet sniffers can capture data packets containing sensitive information such as passwords, account information, syslog traffic, router configuration, DNS traffic, Email traffic, web traffic, chat sessions, FTP password, etc. It allows an

attacker to read passwords in clear-text, the actual emails, credit card numbers, financial transactions, etc. It also allows an attacker to sniff SMTP, POP, IMAP traffic, POP, IMAP, HTTP Basic, Telnet authentication, SQL database, SMB, NFS, and FTP traffic. An attacker can gain a lot of information by reading captured data packets and then use that information to break into the network. An attacker carries out attacks that are more effective by combining these techniques with the active transmission.

The following diagrammatic representation depicts an attacker sniffing the data packets between two legitimate network users:

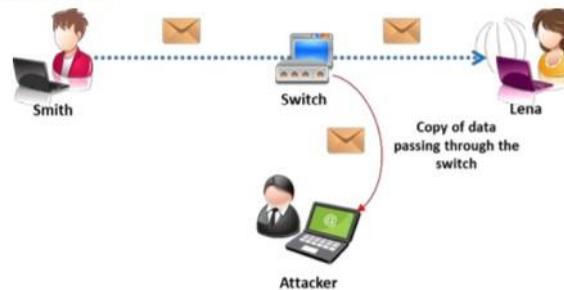


FIGURE 8.1: Packet sniffing scenario

### How a Sniffer Works

The most common way of networking computers is through an Ethernet. A computer connected to a local area network (LAN) has two addresses: a MAC Address and an Internet Protocol (IP) Address. A MAC address uniquely identifies each node in a network and is stored on the NIC itself. The Ethernet protocol uses the MAC address to transfer data to and from a system while building data frames. The Data Link Layer of the OSI model uses an Ethernet header with the MAC address of the destination machine instead of 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 there is no entry 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. The source machine's ARP cache adds this MAC address to the table. 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 differently in each. The two types of Ethernet environments are:

- **Shared Ethernet**

In a shared Ethernet environment, a single bus connects all the hosts that compete 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 and discard the unmatched frame. However, a machine running a sniffer ignores this rule and accepts all the frames. Sniffing in a shared Ethernet environment is passive and hence difficult to detect.

- **Switched Ethernet**

In a switched Ethernet environment, the hosts connect with a switch instead of a hub. The switch maintains a table that tracks each computer's MAC address and the physical port on which that MAC address is connected, and then 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 a better utilization of the available bandwidth and improved security. Hence, the process of putting a 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 following methods:

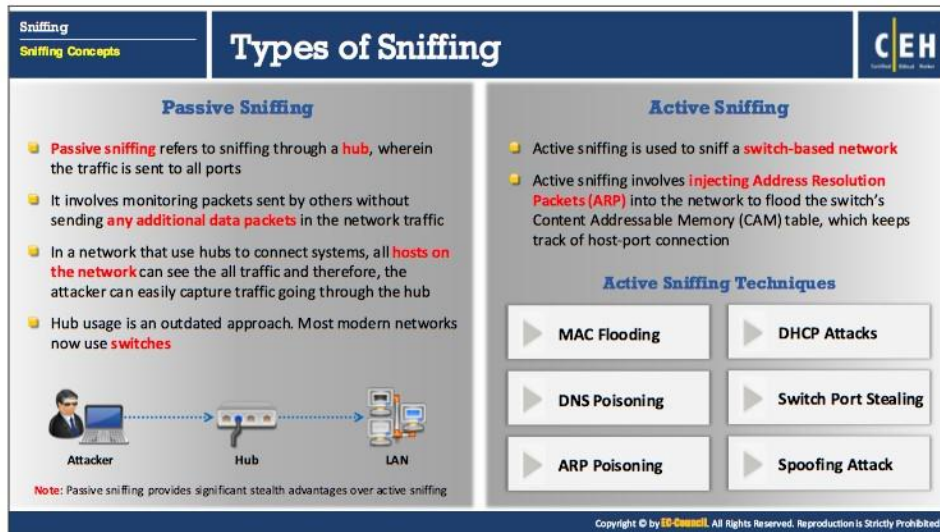
- **ARP Spoofing**

ARP is stateless. The machine can send an ARP reply even without asking for it and accepts such a reply. 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. In 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, they can intelligently route packets from one host to another. However, switches have limited memory. MAC flooding makes use of this limitation to bombard switches with fake MAC addresses until the switches can no longer keep up. Once this happens to a switch, it will enter into the fail-open mode, wherein it starts acting as a hub by broadcasting packets to all the ports on the switch. Once that happens, it becomes easy to perform sniffing. Macof is a utility that comes with the dsniff suite and helps the attacker to perform MAC flooding.

Once a switch turns into a hub, it starts **broadcasting** all packets it receives to all the computers in the network. By default, promiscuous mode is turned **off** in network machines, so the NICs accept only those packets that are addressed to a user's machine, and **discard** the packets sent to the other machines. Sniffer turns the NIC of a system to the promiscuous mode so that it listens to all the data transmitted on its segment. A sniffer can constantly monitor all the network traffic to a computer through the NIC by decoding the information encapsulated in the data packet. Attackers configure the NIC in their machines to run in promiscuous mode, so that the card starts accepting all the packets. In this way, the attacker can view all the packets that are transmitting in the network.



The infographic is titled "Types of Sniffing" and is divided into two main sections: "Passive Sniffing" and "Active Sniffing".

- Passive Sniffing:**
  - Passive sniffing refers to sniffing through a hub, wherein the traffic is sent to all ports.
  - It involves monitoring packets sent by others without sending any additional data packets in the network traffic.
  - In a network that uses hubs to connect systems, all hosts on the network can see the all traffic and therefore, the attacker can easily capture traffic going through the hub.
  - Hub usage is an outdated approach. Most modern networks now use switches.
- Active Sniffing:**
  - Active sniffing is used to sniff a switch-based network.
  - Active sniffing involves injecting Address Resolution Packets (ARP) into the network to flood the switch's Content Addressable Memory (CAM) table, which keeps track of host-port connections.

**Active Sniffing Techniques:**

- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Switch Port Stealing
- ARP Poisoning
- Spoofing Attack

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Types of Sniffing

Attackers run sniffers to convert the host system's NIC to promiscuous mode. As discussed earlier, the NIC in promiscuous mode can then capture the packets addressed to the specific network.

There are two types of sniffing. Each is used for different types of networks. The two types are:

- Passive sniffing
- Active sniffing

### Passive Sniffing

Passive sniffing involves sending no packets. It just captures and monitors the packets flowing in the network. A packet sniffer alone is not preferred 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 present in hub environments. A network that uses hubs to connect systems uses passive sniffing. In such networks, all hosts in the network can see all the traffic. Hence, it is easy to capture traffic going through the hub by using passive sniffing.

Attackers use the following passive sniffing methods to get control over the target network:

- **Compromising the physical security:** An attacker who succeeds in compromising the physical security of the target organization can walk into the organization with a laptop and try to plug into the network and capture sensitive information about the organization.
- **Using a Trojan horse:** Most Trojans have built-in sniffing capability. An attacker can install Trojans with built-in sniffing capabilities on a victim's machine to compromise it. After



compromising the victim's machine, the attacker can install a packet sniffer and perform sniffing.

Most modern networks use switches instead of hubs. A switch eliminates the risk of passive sniffing. However, a switch is still vulnerable to active sniffing.

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

### **Active Sniffing**

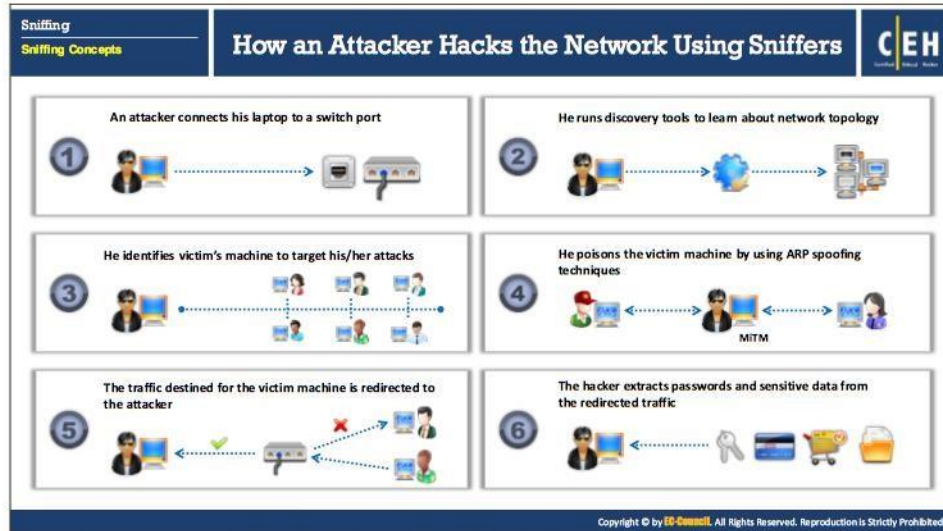
Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN. Active sniffing also refers to sniffing through a switch. In active sniffing, the switched Ethernet does not transmit information to all the systems connected through LAN as it does in a hub-based network.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

Switches examine data packets for source and destination addresses, and then transmit them to the appropriate destination. Therefore, it is cumbersome to sniff switches. However, attackers can actively inject ARP traffic into a LAN to sniff around a switched network and capture the traffic. Switches maintain their own ARP cache in a Content Addressable Memory (CAM). CAM is a special type of memory that maintains the record of which host is connected to which port. A sniffer takes all the information visible on the network and records it for future review. An attacker can see all the information in the packet, including data that should remain hidden.

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

The following is the list of different active sniffing techniques:

- MAC flooding
- DNS poisoning
- ARP poisoning
- DHCP attacks
- Switch port stealing
- Spoofing attack



### How an Attacker Hacks the Network Using Sniffers

Attackers use sniffing tools to sniff packets and monitor network traffic on the target network. The steps that an attacker follows to make use of sniffers to hack a network is illustrated below.

- **Step 1:** An attacker who decides to hack a network first discovers the appropriate switch to access the network and connects a system to one of the ports on the switch.



FIGURE 8.2: Discovering a switch to access the network

- **Step 2:** An attacker who succeeds in connecting to the network tries to determine network information such as topology of the network by using network discovery tools.



FIGURE 8.3: Using network discovery tools to learn topology

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



FIGURE 8.4: Identifying victim's machine

- **Step 4:** An attacker who identifies a target machine uses ARP spoofing techniques to send a fake (spoofed) Address Resolution Protocol (ARP) messages.



FIGURE 8.5: Attacker sending fake ARP messages

- **Step 5:** The previous step helps the attacker to divert all the traffic from the victim's computer to the attacker's computer. This is a typical man-in-the-middle (MITM) type of attack.



FIGURE 8.6: Redirecting the traffic to the attacker

- **Step 6:** Now the attacker can see all the data packets sent and received by the victim. The attacker can now extract the sensitive information from the packets, such as passwords, usernames, credit card details, PINs, etc.



FIGURE 8.7: Attacker extracting sensitive information

Sniffing		Protocols Vulnerable to Sniffing		CEH	
Sniffing Concepts					
<b>Telnet and Rlogin</b>	Keystrokes including user names and passwords are sent in clear text	<b>IMAP</b>	Passwords and data are sent in clear text		
<b>HTTP</b>	Data is sent in clear text	<b>SMTP and NNTP</b>	Passwords and data are sent in clear text		
<b>POP</b>	Passwords and data are sent in clear text	<b>FTP</b>	Passwords and data are sent in clear text		

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Protocols Vulnerable to Sniffing

The following protocols are vulnerable to sniffing. The main reason for sniffing these protocols is to acquire passwords:

- **Telnet and Rlogin**

Telnet is a protocol used for communicating with a remote host (via port no. 23) on a network by using a command line terminal. rlogin enables an attacker to log into a network machine remotely via TCP connection. Both the protocols fail to provide encryption; so the data traversing between the clients connected through any of these protocols is in plain text and vulnerable to sniff. Attackers can sniff keystrokes including usernames and passwords.

- **HTTP**

Due to vulnerabilities in the default version of HTTP, websites implementing HTTP transfer user data across the network in plain text, which the attackers can read to steal user credentials.

- **SNMP**

SNMP is a TCP/IP based protocol used for exchanging management information between devices connected on a network. The first version of SNMP (SNMPv1) does not offer strong security, which leads to transfer of data in clear text format. Attackers exploit the vulnerabilities in this version in order to acquire passwords in plain text.

- **NNTP**

Network News Transfer Protocol (NNTP) distributes, inquires, retrieves, and posts news articles using a reliable stream-based transmission of news among the ARPA-Internet

community. The protocol fails to encrypt the data which gives an attacker the opportunity to sniff sensitive information.

- **POP**

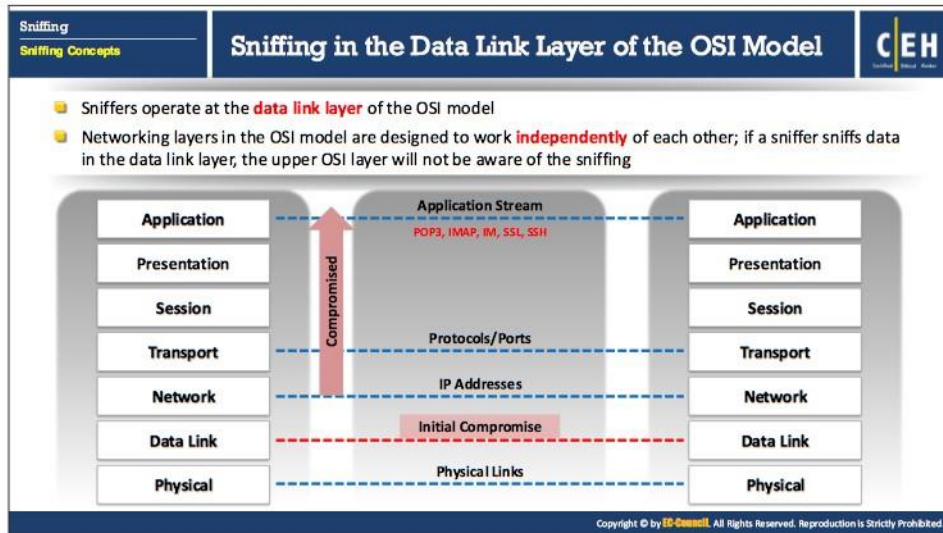
The Post Office Protocol (POP) allows a user's workstation to access mail from a mailbox server. A user can send mail from the workstation to the mailbox server via the Simple Mail Transfer Protocol (SMTP). Attackers can easily sniff the data flowing across a POP network in clear text because of the protocol's weak security implementations.

- **FTP**

File Transfer Protocol (FTP) enables clients to share files between computers in a network. This protocol fails to provide encryption; so attackers sniff data as well as user credentials by running tools like Cain & Abel.

- **IMAP**

Internet Message Access Protocol (IMAP) allows a client to access and manipulate electronic mail messages on a server. This protocol offers inadequate security, which allows attackers to obtain data and user credentials in clear text.




### Sniffing in the Data Link Layer of the OSI Model

The Open Systems Interconnection (OSI) model describes network functions as a series of seven layers. Each layer provides services to the layer above it and receives services from the layer below.

The Data Link layer is the second layer of the OSI model. In this layer, data packets are encoded and decoded into bits. Sniffers operate at the Data Link layer and can capture the packets from the Data Link layer. Networking layers in the OSI model are designed to work independently of each other; if a sniffer sniffs data in the Data Link layer, the upper OSI layer will not be aware of the sniffing.

**Sniffing**  
Sniffing Concepts


## Hardware Protocol Analyzers




- 1** A hardware protocol analyzer is a piece of equipment that **captures signals** without altering the traffic in a cable segment
- 2** It can be used to monitor network usage and identify **malicious network traffic** generated by hacking software installed in the network
- 3** It captures a data packet, decodes it, and analyzes its content based on certain **predetermined rules**
- 4** It allows the attacker to see individual **data bytes** of each packet passing through the cable

**N2X N5540A Agilent Protocol Analyzer**



<https://www.valuetronics.com>

**Keysight E2960B**



<http://www.keysight.com>

**Hardware Protocol Analyzers**

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

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 captures signals without altering the traffic segment. Its purpose is to monitor network usage and identify malicious network traffic generated by hacking software installed on the network. It captures a data packet, decodes it, and analyzes its content according to predetermined rules. It allows an attacker to see the individual data bytes of each packet passing through the network.

When compared to software protocol analysers, hardware protocol analysers are capable of capturing more data without packet drops at the time of data overload. Hardware protocol analyzers provide a wide range of network connection options varying from LAN, WAN, and wireless to circuit-based Telco network lines. They are capable of displaying bus states and low-level events such as high-speed negotiation (K/J chirps), transmission errors and retransmissions, etc. The analysers provide accurate timestamps of the captured traffic. However, hardware analyzers are more expensive and tend to be out of reach for individual developers, hobbyists, and ordinary hackers.

Hardware protocol analyzers from different companies include:

- **N2X N5540A Agilent Protocol Analyzer**

Source: <https://www.valuetronics.com>

The Agilent N2X is a test solution for testing the development and deployment of network services for converging network infrastructures. Service providers, network equipment manufacturers (NEMs), and component manufacturers can verify service attributes of the entire networks end-to-end, while also isolating problems down to individual networking devices and subsystems. Two different types of card can be configured simultaneously allowing for test scenarios that use a combination of port types.

- **Keysight E2960B**

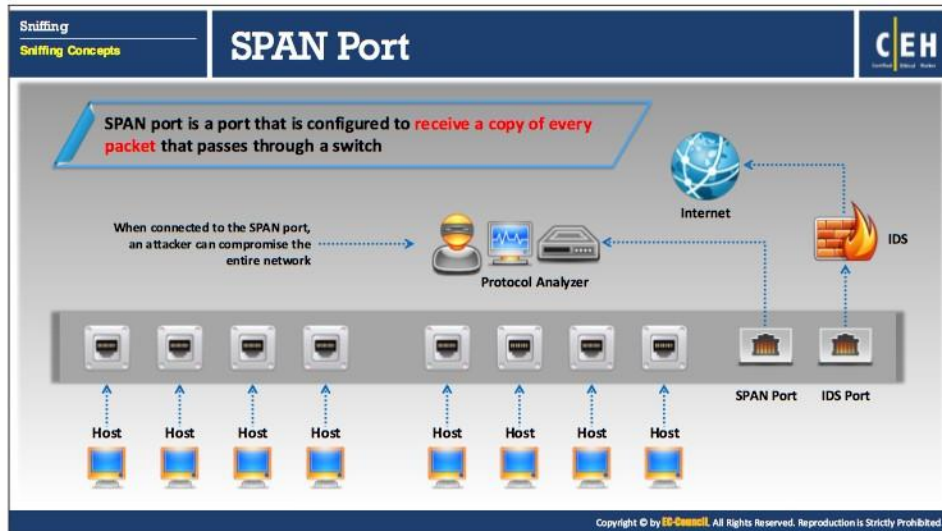
Source: <http://www.keysight.com>

Keysight E2960B tests as well as debugs. It includes a protocol analyzer that supports x1 through x16 link widths, with intuitive spreadsheet style visualization. It offers EASY flow and context-sensitive display for a clear protocol viewing. The analyzer includes unique logic capabilities such as lane view, fast ASPM sync time, and trigger an ordered set.

Some of the hardware protocol analyzers are listed below:

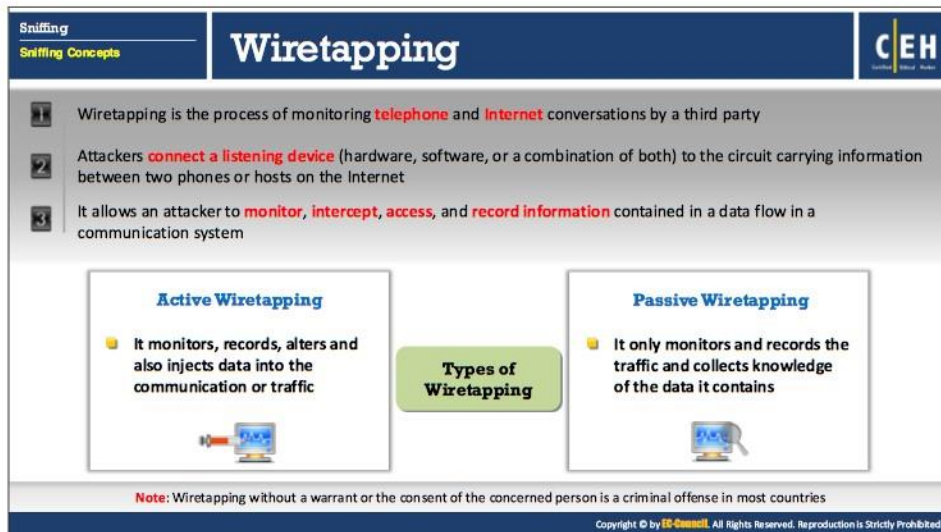
- RADCOM PrismLite Protocol Analyzer (<https://cybarcode.com>)
- STINGA Protocol Analyzer (<http://utelsystems.com>)
- NETSCOUT's OneTouch AT Network Assistant (<http://enterprise.netscout.com>)
- NETSCOUT's OptiView XG Network Analysis Tablet (<http://enterprise.netscout.com>)
- Agilent (Keysight) Technologies 8753ES (<https://www.microlease.com>)
- Agilent (Keysight) Technologies E8364B (<https://www.microlease.com>)
- U4421A Protocol Analyzer (<http://www.keysight.com>)
- U4431A MIPI M-PHY Protocol Analyzer (<http://www.keysight.com>)





### SPAN Port

Switched Port Analyzer (SPAN) is a Cisco switch feature, also known as "port mirroring," that monitors network traffic on one or more ports on the switch. SPAN port is a port that is configured to receive a copy of every packet that passes through a switch. It helps to analyze and debug data, identify errors, and investigate unauthorized network access on a network. When the port mirroring is on, the network switch sends a copy of the network packets from the source port to destination port, which studies the network packets with the help of a network analyzer. There can be one or more sources, but there should be only one destination port on the switch. Source ports are the ports whose network packets are monitored and mirrored. The user can simultaneously monitor the traffic of multiple ports, such as the traffic on all the ports of a specific VLAN.



The infographic is titled "Wiretapping" and is part of a "Sniffing Concepts" section. It defines wiretapping as monitoring telephone and Internet conversations by a third party. It lists three key actions: connecting a listening device, monitoring/intercepting/accessing/recorded information, and the types of wiretapping. The types are Active Wiretapping (which monitors, records, alters, and injects data) and Passive Wiretapping (which only monitors and records). A note states that wiretapping without a warrant is a criminal offense. The infographic includes icons for a listening device, a computer, and a magnifying glass.

**Wiretapping**

Wiretapping is the process of monitoring **telephone** and **Internet** conversations by a third party

Attackers **connect a listening device** (hardware, software, or a combination of both) to the circuit carrying information between two phones or hosts on the Internet

It allows an attacker to **monitor, intercept, access, and record information** contained in a data flow in a communication system

**Active Wiretapping**

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

**Types of Wiretapping**

**Passive Wiretapping**

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

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

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 a third party with covert intentions. In order to perform wiretapping, the attacker first selects a target person or host on the network to wiretap and then connects a listening device (hardware, software, or a combination of both) to the circuit carrying information between two phones or hosts. Typically, the attacker uses a small amount of electrical signal generated by the telephone wires to tap the conversation. This allows attackers to monitor, intercept, access, and record information contained in the data flow in a communication system.

### Wiretapping Methods

The following are ways to perform wiretapping:

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

### Types of Wiretapping

There are two types of wiretapping that an attacker can use to monitor, record, and even alter the data flow in the communication system.

**Sniffing**

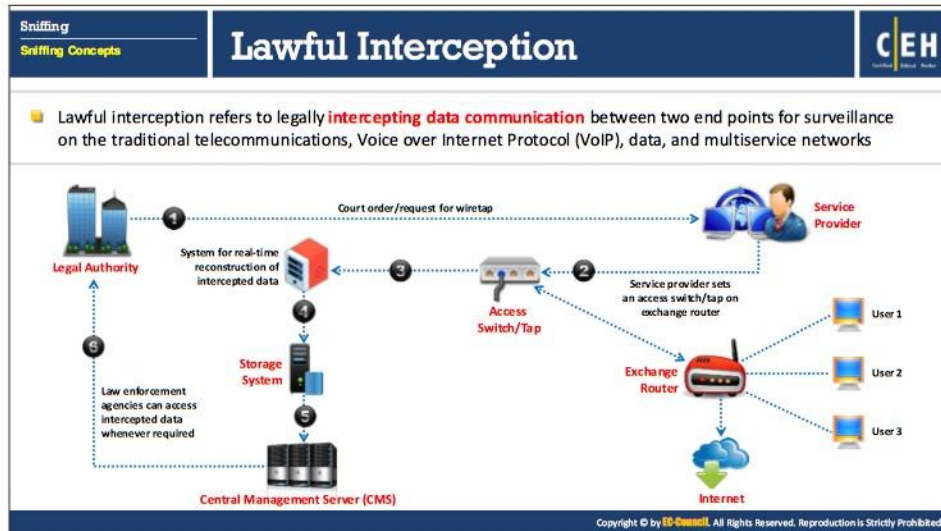
- **Active Wiretapping**

In hacking terminology, active wiretapping is an MITM attack. This allows an attacker to monitor and record the traffic or data flow in a communication system. The attacker can also alter or inject data into the communication or traffic.

- **Passive Wiretapping**

Passive wiretapping is snooping or eavesdropping. This allows an attacker to monitor and record traffic. By observing the recorded traffic flow, the attacker can snoop for a password or other information.

**Note:** Wiretapping without a warrant or the consent of the persons conducting the conversation is a criminal offense in most countries, and it is a punishable offense depending on the country's law.

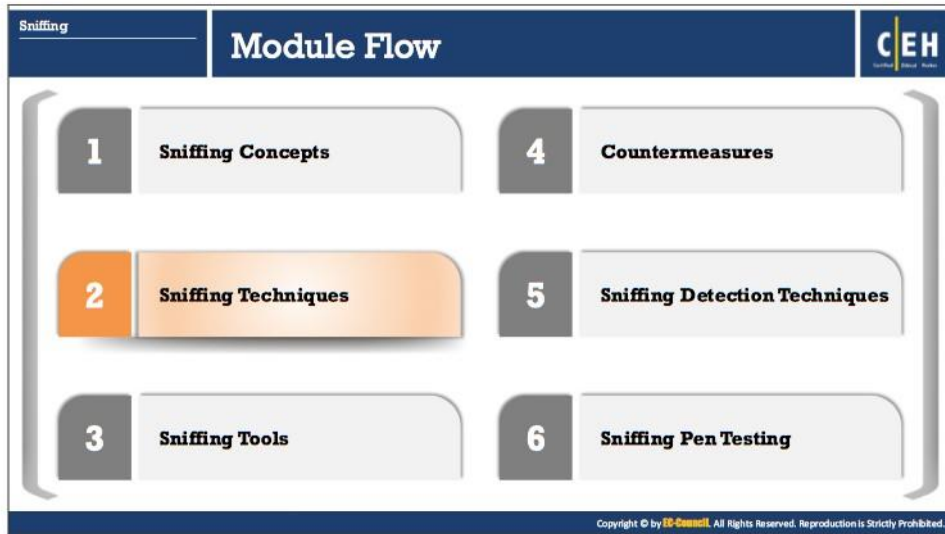


## Lawful Interception

Lawful interception refers to legally intercepting data communication between two endpoints for surveillance on the traditional telecommunications, VoIP, data, and multiservice networks. Lawful interception (LI) obtains data from a communication network for analysis or evidence. This is useful in activities like infrastructure management and protection, as well as cybersecurity-related issues. Here, the network operator or service provider legally sanctions access to private network data for monitoring private communications like telephone calls and email messages. Such operations are carried out by the Law Enforcement Agencies (LEAs).

This type of interception is necessary only to monitor messages exchanged on suspicious channels in which the users are engaged in illegal activity. Countries around the world are making strides to standardize this type of procedure for interception.

The figure above shows the Telco/ISP lawful solution provided by Decision Computer Group. The solution consists of one tap or access, and multiple systems for reconstruction of intercepted data. The tap/access switch collects traffic from the Internet service provider (ISP) network, sorts the traffic by IP domain, and serves it to the E-Detective (ED) systems that decode and reconstructs the intercepted traffic into its original format. The tool performs this with the help of supporting protocols such as POP3, IMAP, SMTP, P2P and FTP, Telnet, etc. The Centralized Management Server (CMS) manages all the ED systems.



### Sniffing Technique: MAC Attacks

Attackers use various sniffing techniques such as MAC attacks, DHCP attacks, ARP poisoning, spoofing attacks, DNS poisoning, etc. to steal and manipulate sensitive data. Attackers use these techniques to get control over the target network by reading captured data packets and then using that information to break into the network.

This section discusses MAC attacks or MAC flooding. Attackers use the MAC flooding technique to force a switch to act like hub, so that they can easily sniff the traffic.

Sniffing

Sniffing Technique:  
MAC Attacks

## MAC Address/CAM Table

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

The CAM table **stores information** such as MAC addresses available on physical ports with their associated virtual LAN (VLAN) parameters

**MAC Address**

**CAM Table**

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### MAC Address

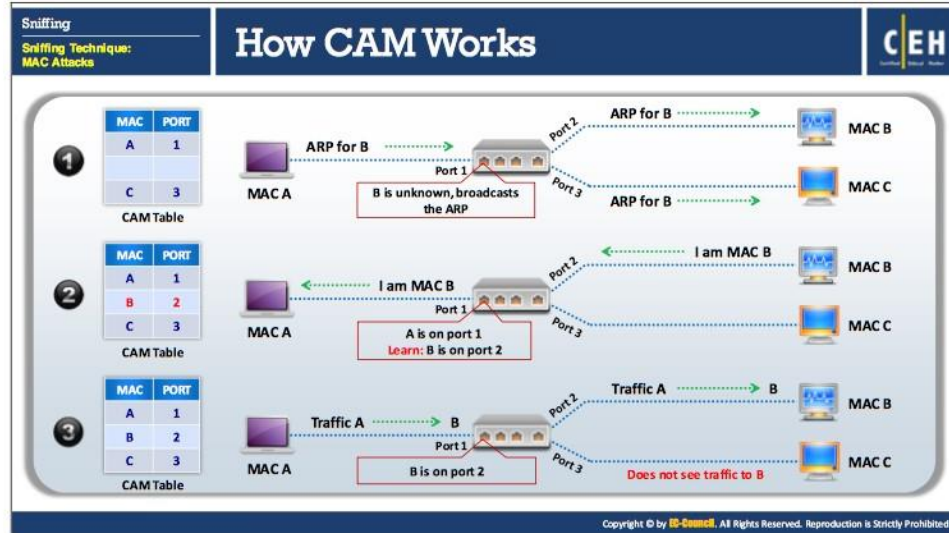
A MAC address uniquely identifies each node of a network. Each device in the network has a MAC address associated with a physical port on the network switch, which makes it possible to designate a specific single point of the network. A MAC address is used as a network address for most IEEE 802 network technologies, including Ethernet. Logically, the MAC protocol in the OSI reference model uses MAC addresses for information transfer.

A MAC address is 48 bits, which splits into two sections, each containing 24 bits. The first section contains the ID number of the organization that manufactured the adapter and is called the Organizationally Unique Identifier. The next section contains the serial number assigned to the NIC adapter and is called the NIC Specific.

The MAC address contains 12-digit hexadecimal numbers, divided into three or six groups. The first six digits indicate the manufacturer, while the next six digits indicate the adapter's serial number. For example, consider the MAC address D4-BE-D9-14-C8-29. The first six digits, i.e., D4BED9 indicate the manufacturer (Dell, Inc.), while the next six digits 14C829 indicate the serial number of the adapter.

### CAM Table

The CAM (Content Addressable Memory) table is a dynamic table of fixed size. It stores information such as MAC addresses available on physical ports along with VLAN parameters associated with them. When a machine sends data to another machine in a network, the data passes through the switch. The switch searches for the destination MAC address (located in the Ethernet frame) in its CAM table, and once the MAC address is found, it forwards data to the machine through the port with which the MAC address is bound. This method of transferring data in a switched network is more secure than that of a hub-based network, in which the hub forwards the incoming traffic to all the machines in the network.



**How CAM Works**

A CAM table refers to the dynamic form of content and works with the Ethernet switch. The Ethernet switch maintains the connections between the ports. A CAM table keeps track of MAC address locations on a switch, but the table is limited in size. If the CAM table is flooded with more MAC addresses than it can hold, the switch will turn into a hub. The CAM table does this to ensure the delivery of data to the intended host. Attackers exploit this vulnerability in the CAM table to sniff network data. An attacker who can connect to the shared switch of the Ethernet segment can easily sniff network data.

Refer to the diagram below for the working of CAM table. It shows three machines: **Machine A**, **Machine B** and **Machine C**, each holding MAC address **A**, **B** and **C**. The machine A holding the MAC address **A** wants to interact with Machine B.

Machine **A** broadcasts an **ARP request** to the switch. The request contains the IP address of the target machine (Machine B), along with the source machine's (**Machine A**) MAC and IP addresses. The switch then broadcasts this ARP request to all the hosts in the network and waits for the reply.

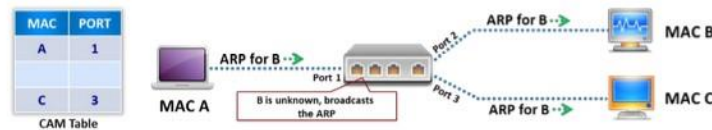


FIGURE 8.8: Working of CAM Table Step-1

Machine B possesses the target/destination IP address, so it sends an ARP reply along with its MAC address. The CAM table stores this MAC address along with the port on which this machine is connected.

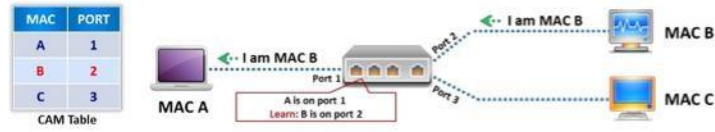


FIGURE 8.9: Working of CAM Table Step-2

Now the connection is successfully established, and Machine A forwards the traffic to Machine B, while Machine C is unable to see the traffic flowing between them.

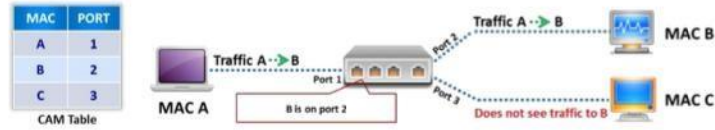


FIGURE 8.10: Working of CAM Table Step-3



**Sniffing**  
Sniffing Technique:  
MAC Attacks

## What Happens When CAM Table Is Full?

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

MAC	PORT
Y	3
Z	3
C	3

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### What Happens When CAM Table Is Full?


As discussed, a CAM table contains network information such as MAC addresses available on physical switch ports and associated VLAN parameters. The CAM table's limited size renders it susceptible to attacks from MAC flooding. MAC flooding bombards the switch with fake source MAC addresses until the CAM table is full. Hereafter, the switch broadcasts all incoming traffic to all ports. This changes the behavior of the switch to reset to its learning mode, broadcasting on every port like a hub. The switch then works like a hub through which you (the attacker) 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 figure given above illustrates how a CAM table can be flooded with fake MAC addresses to monitor the frames sent from the victim host to another host without any CAM table entry.

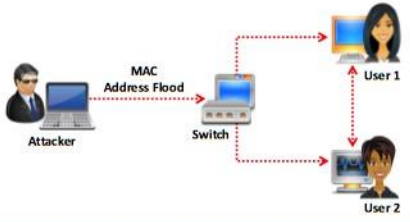
Sniffing

Sniffing Technique:  
MAC Attacks

## MAC Flooding



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



**Mac Flooding Switches with macof**

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

```

root@kali:~# macof -i eth0
1239917542(0) wan 512
62:d7:4e:10:70:48 c7:c0:12:20:22:1e 0.0.0.0.64572 > 0.0.0.0.2261: S 1387558124:1
9059418448(0) wan 512
2f:a4:84:58:3c:d5 ac:a:38:d:98:a1 0.0.0.0.22960 > 0.0.0.0.61618: S 2145102987:231
43:1b:287(0) wan 512
c41:52:32:4e:08 96:24:74:1a:3f:96 0.0.0.0.17689 > 0.0.0.0.36773: S 245668985:20
3668905(0) wan 512
40:d:01:f:7f 0e:16:54:c6:47:34 0.0.0.0.59759 > 0.0.0.0.32991: S 90668728:9086
48728(0) wan 512
ba:da:84:71:3b:20 73:a4:0a:42:85:14 0.0.0.0.11448 > 0.0.0.0.39716: S 163586221:1
80580221(0) wan 512
bc:ab:cb:17:5a:cd 7:3:97:f7:29:21:0 0.0.0.0.17812 > 0.0.0.0.45747: S 1228305696:1
                    
```

<https://www.monkey.org>

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. Attackers use the MAC flooding technique to force a switch to act as a hub, so that they can easily sniff the traffic.

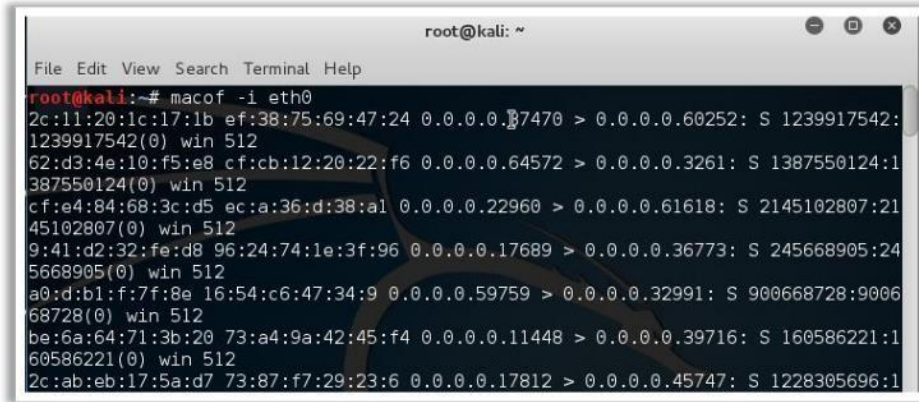
In a switched network, an Ethernet switch contains a CAM table that stores all the MAC addresses of devices connected in the network. A switch acts as an intermediate device between one or more computers in a network. It looks for Ethernet frames, which carry the destination MAC address, tally this address with the MAC address in its CAM table, and forwards the traffic to the destined machine. 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. However, the size of CAM table is fixed, and it can store only a limited number of MAC addresses in it, an attacker may send a huge number of fake MAC address to the switch. 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 “fail-open mode.” In the fail-open mode, the switch starts behaving like a hub and broadcasts the incoming traffic through all the ports in the network. The attacker then turns ON his machine’s NIC to promiscuous mode to enable the machine to accept all the traffic entering it. In this way, attackers can sniff the traffic easily and can steal sensitive information.

#### Mac Flooding Switches with macof

Source: <https://monkey.org>

Macof is a Unix/Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods the switch’s CAM tables (131,000 per min) by

sending forged MAC entries. When the MAC table fills up, and the switch converts to hub-like operation, an attacker can monitor the data being broadcast.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# macof -i eth0  
2c:11:20:1c:17:1b ef:38:75:69:47:24 0.0.0.0.37470 > 0.0.0.0.60252: S 1239917542:  
1239917542(0) win 512  
62:d3:4e:10:f5:e8 cf:cb:12:20:22:f6 0.0.0.0.64572 > 0.0.0.0.3261: S 1387550124:1  
387550124(0) win 512  
cf:e4:84:68:3c:d5 ec:a:36:d:38:a1 0.0.0.0.22960 > 0.0.0.0.61618: S 2145102807:21  
45102807(0) win 512  
9:41:d2:32:fe:d8 96:24:74:1e:3f:96 0.0.0.0.17689 > 0.0.0.0.36773: S 245668905:24  
5668905(0) win 512  
a0:d:b1:f:7f:8e 16:54:c6:47:34:9 0.0.0.0.59759 > 0.0.0.0.32991: S 900668728:9006  
68728(0) win 512  
be:6a:64:71:3b:20 73:a4:9a:42:45:f4 0.0.0.0.11448 > 0.0.0.0.39716: S 160586221:1  
60586221(0) win 512  
2c:ab:eb:17:5a:d7 73:87:f7:29:23:6 0.0.0.0.17812 > 0.0.0.0.45747: S 1228305696:1
```

FIGURE 8.11: MAC Flooding using macof

Sniffing

Sniffing Technique:  
MAC Attacks

## Switch Port Stealing

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Switch Port Stealing

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

Assume that there are three machines in a network: Host A, target's Host B and attacker's Host C.

Machine	MAC Address	IP Address	Ports
Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	Port A
Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	Port B
Host C	cc-dd-ee-ff-gg-hh	10.0.0.3	Port C

TABLE 8.2: Details of three hosts in a network

The switch's ARP cache and MAC table contains the following values:

#### MAC Table

Vlan	MAC Address	Type	Learn	Age	Ports
255	Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	0	Port A
5	Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port B
5	Host C	cc-dd-ee-ff-gg-hh	10.0.0.3	0	Port C

TABLE 8.3: MAC Table

### ARP Cache

IP	MAC
10.0.0.1	aa-bb-cc-dd-ee-ff
10.0.0.2	bb-cc-dd-ee-ff-gg
10.0.0.3	cc-dd-ee-ff-gg-hh

TABLE 8.4: ARP Cache Table

- Switch port stealing is a sniffing technique used by an attacker who spoofs both the IP address and MAC address of the target machine (Host B).

Machine	MAC Address	IP Address	Ports
Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	Port A
Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	Port B
Host C	bb-cc-dd-ee-ff-gg	10.0.0.2	Port C

TABLE 8.5: Switch updated with a spoofed entry

- The attacker's machine runs a sniffer that turns the machine's NIC adapter to promiscuous mode.
- Host A associated with the IP address (**10.0.0.1**) wants to communicate with Host B associated with the IP address (**10.0.0.2**). Therefore, host A sends an ARP request (I want to communicate with **10.0.0.2**. What is the MAC address of **10.0.0.2**?).
- The switch broadcasts this ARP request to all the machines in the network.
- Before Host B (the target machine) can respond to the ARP request, the attacker responds to the ARP request by sending an ARP reply containing the spoofed MAC and IP addresses (I am **10.0.0.2**, and my MAC address is **bb-cc-dd-ee-ff-gg**).
- The attacker can achieve this by launching an attack such as Denial of Service (DoS) on Host B, which slows down its response.
- Now the ARP cache in the switch records the spoofed MAC and IP addresses.

IP	MAC
10.0.0.1	aa-bb-cc-dd-ee-ff
10.0.0.2	bb-cc-dd-ee-ff-gg
10.0.0.2	bb-cc-dd-ee-ff-gg

TABLE 8.6: ARP Cache updated with a spoofed entry

- The spoofed MAC address of target Host B (**bb-cc-dd-ee-ff-gg**) and the port connect to the attacker's machine (**Port C**) and update the switch's CAM table. Now, a connection is established between **Host A** and the attacker's machine (**Host C**).

Vlan	MAC Address	Type	Learn	Age	Ports
255	Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	0	Port A
5	Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port B
5	Host C	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port C


TABLE 8.7: MAC Table updated with a spoofed entry

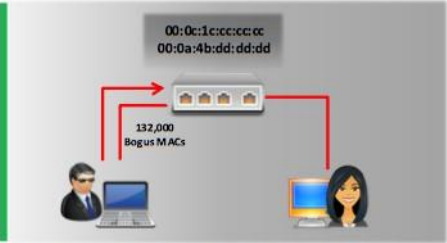
- Now, the system will forward all the packets directed towards Host B to Host C through Port C, i.e., the attacker's machine.

Thus, an attacker can sniff the packets sent to Host B.

**Sniffing**  
Sniffing Technique:  
MAC Attacks


## How to Defend against MAC Attacks





00:0c:1c:cc:cc:cc  
00:0a:4b:dd:dd:dd

132,000  
Bogus MACs



Only 1 MAC Address  
Allowed on the Switch Port

**Configuring Port Security on Cisco switch:**

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

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### How to Defend against MAC Attacks

To protect a port, this feature identifies and limits the MAC addresses of the machines that can 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 machine that is attempting to access the port does not match any of the identified secure MAC addresses

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

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

In the figure given below, the attacker floods the switch CAM tables with fake MAC addresses and thus threatens security by turning a switch into a hub.

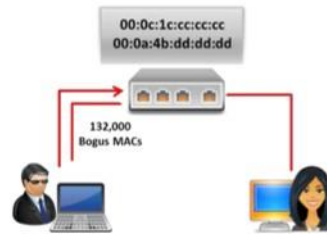


FIGURE 8.12: Flooding CAM Tables

In the figure given below, the number of MAC addresses allowed on the switch port is limited to one; therefore, it recognizes MAC requests as flooding. Port security locks down the port and sends an SNMP trap.



FIGURE 8.13: Blocking MAC Flooding

#### Configuring Port Security on Cisco switch

Source: <https://www.cisco.com>


You can use the following Cisco port security feature to defend against MAC attacks:

- **switchport port-security**  
Enables port security on the interface.
- **switchport port-security maximum 1 vlan access**  
Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 3072. The default is 1.
- **switchport port-security violation restrict**  
Sets the violation mode, the action to be taken when a security violation {restrict | shutdown} is detected.
- **switchport port-security aging time 2**  
Sets the aging time for the secure port.
- **switchport port-security aging type inactivity**  
The type keyword sets the aging type as absolute or inactive.
- **snmp-server enable traps port-security trap-rate 5**  
Controls the rate at which SNMP traps are generated.



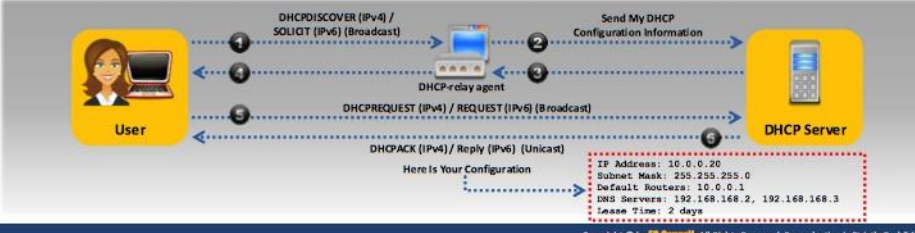
**Sniffing**  
Sniffing Technique:  
DHCP Attacks

## How DHCP Works



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

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Sniffing Technique: DHCP Attacks

This section discusses the DHCP attacks. A DHCP attack is an active sniffing technique used by the attackers to steal and manipulate sensitive data. 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.

#### How DHCP Works

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

DHCP can assign IP configuration to hosts connecting to a network. The distribution of IP configuration to hosts simplifies the administrator's work to maintain IP networks.

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

#### Working of DHCP:

1. The 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.

Module 08 Page 891

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

4. Relay agent broadcasts DHCP OFFER/ADVERTISE in the client's subnet.
5. The client broadcasts DHCP REQUEST/REQUEST asking DHCP server to provide the DHCP configuration information.
6. DHCP server sends unicast DHCP ACK/REPLY message to the client with the IP config and information.

Sniffing  
Sniffing Technique:  
DHCP Attacks

## DHCP Request/Reply Messages

DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client broadcast to locate the available DHCP servers
DHCPOffer	Advertise	Server to client in response to DHCPDISCOVER with offer of configuration parameters
DHCPRequest	Request, Confirm, Renew, Rebind	Client message to servers either (a) requesting offered parameters, (b) confirming correctness of previously allocated address, or (c) extending the lease period
DHCPAck	Reply	Server to client with configuration parameters, including committed network address
DHCPRelease	Release	Client to server relinquishing network address and canceling remaining lease
DHCPDecline	Decline	Client to server indicating network address is already in use
N/A	Reconfigure	Server tells the client that it has new or updated configuration settings. The client then sends either a renew/reply or information-request/reply transaction to get the updated information
DHCPInform	Information Request	Client to server, asking only for local configuration parameters; client already has externally configured network address
N/A	Relay-Forward	A relay agent sends a relay-forward message to relay messages to servers, either directly or through another relay agent
N/A	Relay-Reply	A server sends a relay-reply message to a relay agent containing a message that the relay agent delivers to a client
DHCPNAX	N/A	Server to client indicating client's notion of network address is incorrect (e.g., Client has moved to new subnet) or client's lease as expired

### IPv4 DHCP Packet Format

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

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, the client immediately 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 send its parameters on the usage of the network. 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 invalid. The DHCP server can put that IP address back into the pool and offer it to another client.

DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client broadcast to locate the available DHCP servers
DHCOffer	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 8.8: DHCP request/reply messages

### IPv4 DHCP Packet Format

DHCP enables 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 a client-server mode. 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 are used in 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 table details every field of the IPv4 DHCP message:

FIELD	OCTETS	DESCRIPTION
OP Code	1	This field contains message opcode that represents the message type OP code "1" represents BOOTREQUEST while "2" represents BOOTREPLY
Hardware Address Type	1	Hardware address the 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 DHCP clients set the value to "0". 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
Seconds	2	Seconds elapsed since the client began address acquisition or renewal process.
Flags	2	Flags set by the 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 address and can 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 hostname
File Name	128	Name of the file containing BOOTP client's boot image
DHCP Options	Variable	


TABLE 8.9: Fields of IPv4 DHCP message

**Sniffing**  
Sniffing Technique:  
DHCP Attacks


## DHCP Starvation Attack




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



**User**  
User will be unable to get the valid IP address



**DHCP Server**  
Server runs out of IP addresses to allocate to valid users

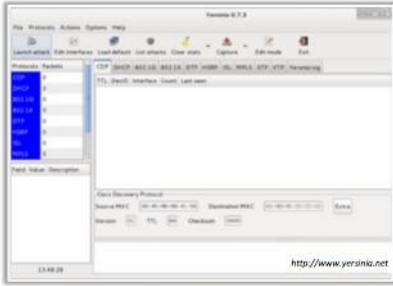


**Attacker**  
Attacker sends many different DHCP requests with many source MACs

**DHCP Scope**

- 10.10.10.1
- 10.10.10.2
- 10.10.10.3
- 10.10.10.254

#### DHCP Starvation Attack Tool: Yersinia



<http://www.yersinia.net>

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

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 requests and uses all of 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**.

### DHCP Starvation Attack Tools

DHCP starvation attack tools send a large number of requests to a DHCP server leading to exhaustion of server's address pool. After which DHCP server is not able to allocate configurations to new clients.

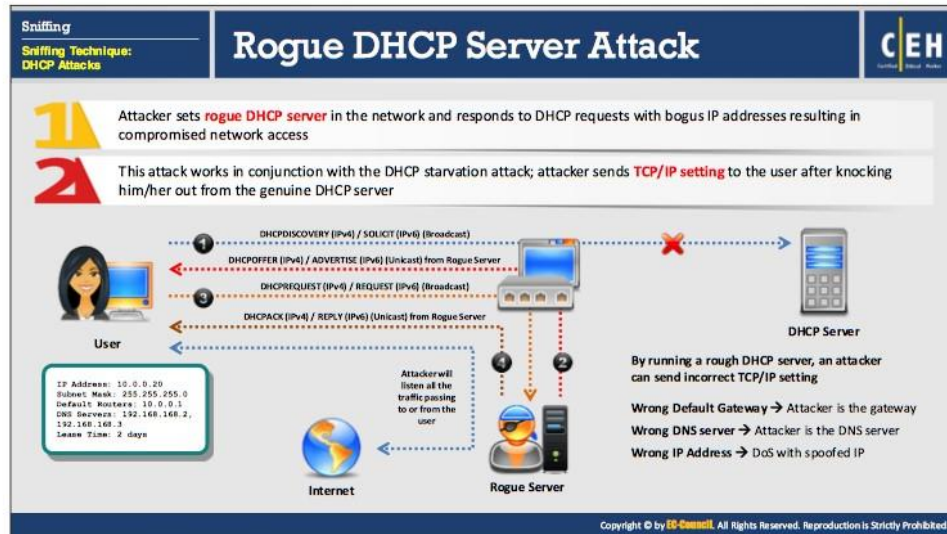
- **Yersinia**

Source: <http://www.yersinia.net>

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

Some of the DHCP starvation attack tools are listed below:

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



### Rogue DHCP Server Attack

In addition to DHCP starvation attacks, an attacker can perform MITM attacks such as sniffing. An attacker who succeeds in exhausting the DHCP Server's IP address space can set up a **Rogue DHCP Server** on the network which is not under the control of the network administrator. The Rogue DHCP server impersonates a legitimate server and offers IP addresses and other network information to other clients in the network, acting itself as a default gateway. Clients connected to the network with the addresses assigned by the Rogue Server will now become victims of MITM and other attacks, where packets forwarded from a client's machine will reach the rogue server first.

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. Although both the rogue and actual DHCP servers respond to the request, the client accepts the response that comes first. In a case where the rogue server gives the response earlier than the actual DHCP server, 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 that serves as a client's default gateway. As a result, the attacker's IP address receives all the traffic from the client. The attacker then captures all the traffic and forwards this traffic to the appropriate default gateway. The client thinks that everything is functioning correctly. This type of attack is difficult to detect by the client for long periods.


Sometimes, the client uses a rogue DHCP server instead of the standard DHCP server. The rogue server directs the client to visit fake websites in an attempt to gain their credentials.

To mitigate a rogue DHCP server attack, set the connection between the interface and the rogue server as untrusted. That action will block all ingress DHCP server messages from that interface.

**Sniffing**


**Sniffing Technique:**  
DHCP Attacks

## How to Defend Against DHCP Starvation and Rogue Server Attack



■ **Enable port security** to defend against DHCP starvation attack


- Configuring MAC limit on switch's edge ports drops the packets from further MACs once the limit is reached



**IOS Switch Commands**

- switchport port-security
- switchport port-security maximum 1
- switchport port-security violation restrict
- switchport port-security aging time 2
- switchport port-security aging type inactivity
- switchport port-security mac-address sticky

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



**IOS Global Commands**

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

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## How to Defend Against DHCP Starvation and Rogue Server Attack

### Defend Against DHCP Starvation

Enable port security to defend against DHCP starvation attack. Port security limits the maximum number of MAC addresses on the switch port. When the limit is exceeded, the switch drops subsequent MAC address requests (packets) coming from external sources which safeguard the server against a DHCP starvation attack.

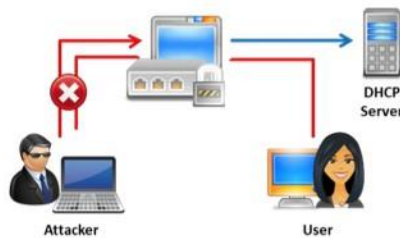


FIGURE 8.14: Defending against DHCP Starvation attack

### IOS Switch Commands

Source: <https://www.cisco.com>

- **switchport port-security**

The `switch port port-security` command configures the switch port parameters to enable port security.



- **switchport port-security maximum 1**

The `switch port port-security maximum` command configures the maximum number of secure MAC addresses for the port.

The `switch port port-security maximum 1` command configures the maximum number of secure MAC addresses for the port as 1.

- **switchport port-security violation restrict**

The `switch port port-security violation` command sets the violation mode and the necessary action in case of detection of a security violation.

The `switch port port-security violation restrict` command drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed.

- **switchport port-security aging time 2**

The `switch port port-security aging time` command configures the secure MAC address aging time on the port.

The `switch port port-security aging time 2` command sets the aging time as 2 minutes.

- **switchport port-security aging type inactivity**

The `switch port port-security aging type` command configures the secure MAC address aging type on the port.

The `switch port port-security aging type inactivity` command sets the aging type as inactivity aging.

- **switchport port-security mac-address sticky**

Enables sticky learning on the interface by entering only the mac-address sticky keywords. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses.

### Defend Against Rogue Server Attack

The DHCP snooping feature that is available on switches can mitigate against rogue DHCP servers. It is configured on the port on which the valid DHCP server is connected. Once configured, DHCP snooping does not allow other ports on the switch to respond to DHCP discover packets sent by clients. Thus, even an attacker who manages to build a rogue DHCP server and connects to the switch cannot respond to DHCP discover packets.



FIGURE 8.15: Defending against Rogue Server attack

### IOS Global Commands

Source: <https://www.cisco.com>

- **ip dhcp snooping vlan 4,104**

Enable or disable DHCP snooping on one or more VLANs.

- **no ip dhcp snooping information option**

To disable the insertion and the removal of the option-82 field, use the no IP dhcp snooping information option in global configuration command. To configure an aggregation, switch to drop incoming DHCP snooping packets with option-82 information from an edge switch, use the no IP dhcp snooping information option allow-untrusted global configuration command.

- **ip dhcp snooping**

Enable DHCP snooping option globally.

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

Sniffing

## What Is Address Resolution Protocol (ARP)?

CEH

**Sniffing Technique: ARP Poisoning**

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

The diagram illustrates the ARP process. A source machine (IP: 194.54.67.10, MAC: 00:1b:48:64:42:e4) sends an ARP\_REQUEST to three target machines. The first target machine (IP: 192.168.168.1, MAC: 00-14-20-01-23-45) responds with an ARP\_REPLY: "Hello, I am 192.168.168.1. MAC address is 00-14-20-01-23-47". The other two target machines do not respond. The source machine then establishes a connection. To the right, a Command Prompt window shows the output of the 'arp -a' command:

```
C:\Users\Test>arp -a

Interface: 192.168.01.1 --- 0x2
Internet Address      Physical Address      Type
192.168.01.254        00-50-00-00-00-00     dynamic
192.168.01.255        ff-ff-ff-ff-ff-ff     static
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22            01-00-00-00-00-00     static
224.0.0.251           01-00-00-00-00-00     static
224.0.0.252           01-00-00-00-00-00     static
224.0.0.253           01-00-00-00-00-00     static
239.255.255.250      01-00-00-00-00-00     static
255.255.255.255      ff-ff-ff-ff-ff-ff     static
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Sniffing Technique: ARP Poisoning

This section discusses the ARP poisoning technique generally used by attackers to perform sniffing on the target network. Using this method, the attacker can steal sensitive information, prevent network and web access, and perform DoS and MITM attacks such as sniffing.

#### What Is Address Resolution Protocol (ARP)?

Address Resolution Protocol (ARP) is a stateless TCP/IP protocol that maps IP network addresses to the addresses (hardware addresses) used by a data link protocol. Using this protocol, a user can easily obtain the MAC address of any device on a network. Apart from the switch, the host machines also use the ARP protocol for obtaining 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 OS also maintains the MAC address table (ARP table).

The process of obtaining the MAC address using ARP is as follows:

- The source machine generates an ARP request packet containing the source MAC address, source IP address and destination IP address, and sends it to the switch.
- On receiving the packet, the switch reads the MAC address of the source and searches for this address in its CAM table.
- The switch updates all the new entries in it. If the entry is not found in the table, the switch adds the MAC address and its respective incoming port to its CAM table and broadcasts the ARP request packet into the network.

- Each device in the network receives the broadcast ARP request packet and compares the destination IP address in the packet with its own IP address.
- Only the system whose IP address matches the destination, IP address replies with an ARP reply packet.
- The ARP reply message is then read by the switch, which adds the entry to its MAC table and forwards the message to the destination machine, i.e., the machine that sent the ARP request.
- Further, this machine updates the destination machine's IP and MAC address entries into its ARP table, and now communication can take place.

Consider an ARP example that shows two machines connected in a network. The respective hostnames, IP, and MAC addresses are:

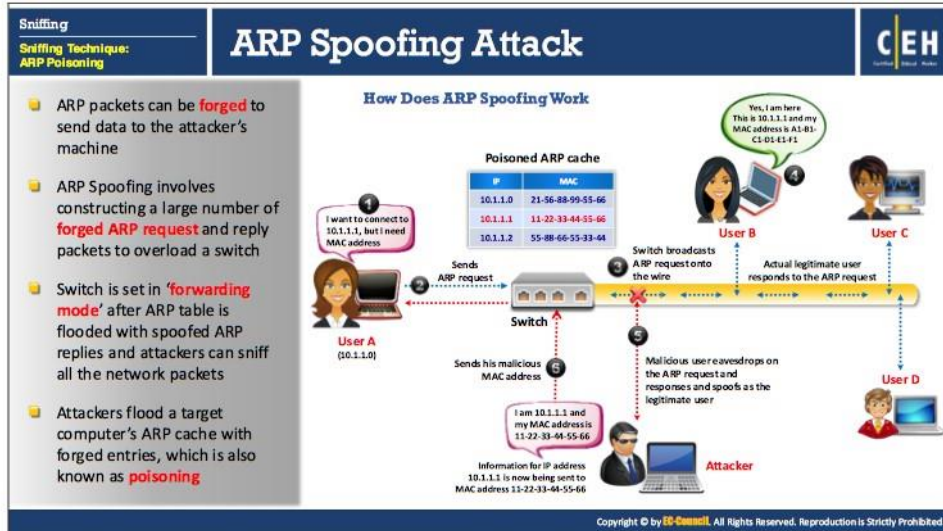
HostName	IP	MAC
A	194.54.67.10	00:1b:48:64:42:e4
B	192.54.67.15	00-14-20-01-23-47

Before communicating with host B, host A first checks for a record of host B's MAC address in the ARP cache. If host A finds the record of a MAC address, it communicates directly with host B. Otherwise, it has to access host B's MAC address by using the ARP protocol.

Host A queries all the hosts on the LAN. If the query was phrased in plain English, it might sound like this: "Hello, who is 192.54.67.15? 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. On receiving the ARP request packet, host B updates its ARP cache table with host A's IP and MAC addresses, and sends an ARP reply packet to host A that would be phrased in English as, "Hey, this is 192.54.67.15; my MAC address is 00-14-20-01-23-47."

On receiving the ARP reply, host A updates its ARP cache table with host B's IP and MAC addresses. After establishing a connection between these two hosts, they communicate with each other.



### ARP Spoofing Attack

ARP resolves IP addresses to the MAC (hardware) address of the interface to send data. ARP packets can be forged to send data to the attacker's machine. ARP Spoofing involves constructing a large number of forged ARP request and reply packets to overload a switch. If the machine sends an ARP request, it assumes that the ARP reply comes from the right machine. ARP provides no means of verifying the authenticity of the responding device. Even systems that have not made an ARP request can also accept the ARP reply coming from other devices. Attackers use this flaw in ARP to create malformed ARP replies containing spoofed IP and MAC addresses. Assuming it to be the legitimate ARP reply, the victim's computer blindly accepts the ARP entry into its ARP table. Once the ARP table is flooded with spoofed ARP replies, the attacker sets the switch in forwarding mode, which intercepts all the data that flows from the victim machine without the victim being aware of the attack. Attackers flood a target computer's ARP cache with forged entries which is also known as poisoning. ARP spoofing is an intermediary to perform attacks such as DoS, MITM, and Session Hijacking.

### How Does ARP Spoofing Work

ARP spoofing is a method of attacking an Ethernet LAN. When a legitimate user initiates a session with another user in the same Layer 2 broadcast domain, the switch broadcasts an ARP request using the recipient's IP address, while the sender waits for the recipient to respond with a MAC address. An attacker eavesdropping on this unprotected Layer 2 broadcast domain can respond to the broadcast ARP request and replies to the sender by spoofing the intended recipient's IP address. The attacker runs a sniffer and turns the machine's NIC adapter to promiscuous mode.

ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has

been forged, the destination computer (target) sends frames to the attacker's computer, where the attacker can modify the frames before sending them to the source machine (User A) in an MITM attack. In addition, the attacker can also launch a DoS attack by associating a non-existent MAC address to the IP address of the gateway, or may sniff the traffic passively and then forward it to the target destination.

**Threats of ARP Poisoning**

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

1	Packet Sniffing	6	Data Interception
2	Session Hijacking	7	Connection Hijacking
3	VoIP Call Tapping	8	Connection Resetting
4	Manipulating Data	9	Stealing Passwords
5	Man-in-the-Middle Attack	10	Denial-of-Service (DoS) Attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Threats of ARP Poisoning

With the help of ARP poisoning, an attacker can use fake ARP messages to divert all communications between two machines so that all traffic redirects via the attacker's PC.

The threats of ARP poisoning include:

- **Packet Sniffing:** Sniffs traffic over a network or a part of the network
- **Session Hijacking:** Steals valid session information and uses it to gain unauthorized access to an application
- **VoIP Call Tapping:** Uses port mirroring which allows the VoIP call tapping unit to monitor all network traffic, and picks only the VoIP traffic to record by MAC address
- **Manipulating Data:** ARP spoofing allows attackers to capture and modify data, or stops the flow of traffic
- **MITM Attack:** Attacker performs an MITM attack where the attacker resides between the victim and server
- **Data Interception:** Intercepts IP address, MAC address, and VLANs connected to the switch in a network
- **Connection Hijacking:** In a network, the hardware addresses are supposed to be unique and fixed, but a host may move when its hostname changes and uses some other protocol. In connection hijacking, an attacker can manipulate a client's connection to take complete control.
- **Connection Resetting:** The wrong routing information could be transmitted due to some hardware/software error. In such cases, if a host fails to initiate a connection, that host should inform the Address Resolution module to delete its information. Receiving data

from that host should reset a connection timeout in the ARP entry used to transmit data to that host. That entry in the ARP module is deleted if the host does not send any information for a certain time.

- **Stealing Passwords:** An attacker uses forged ARP replies and tricks target hosts into sending sensitive information such as usernames, passwords, etc.
- **Denial-of-Service (DoS) Attack:** Links multiple IP addresses with a single MAC address of the target host that will be overloaded with huge amount of traffic which is intended for different IP addresses.



**Sniffing**  
Sniffing Technique:  
ARP Poisoning

## ARP Poisoning Tools

**Ufasoft Snif**

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

**ARP Poisoning Tools**

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## ARP Poisoning Tools

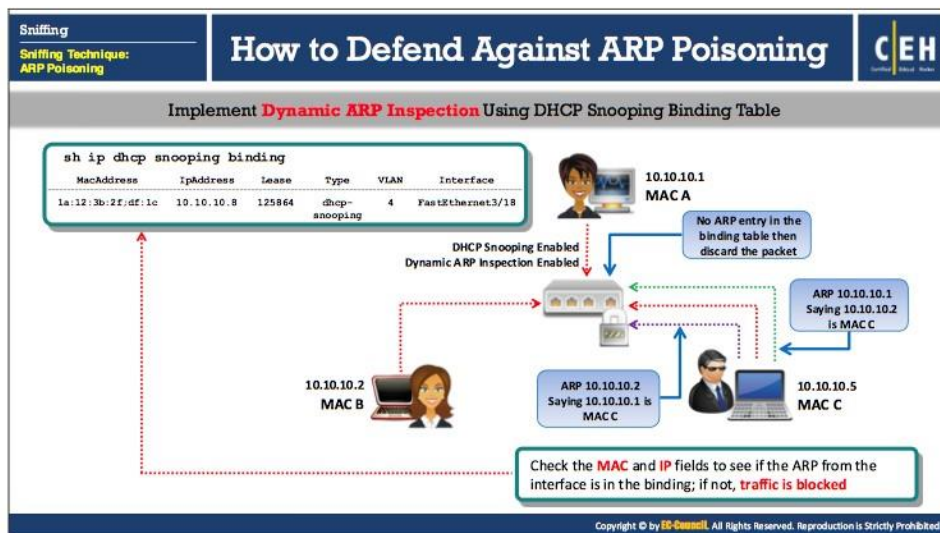
### Ufasoft Snif

Source: <http://ufasoft.com>

Ufasoft Snif is an automated ARP poisoning tool that sniffs passwords and emails messages on a wired network or Wi-Fi network. It Captures and analyzes packets going through the network. The application includes ICQ/IRC/MSN/email sniffers (formerly known as ICQ Sniffer products) and intercepts ICQ, IRC, and email messages across a LAN. It is possible to observe these messages at the same time that real users receive them. All intercepted messages are stored in files, which can later be processed and analyzed. There are two versions: IcqSnif with GUI, and console-only IcqDump. The functionality is the same, except that the user can select specific machines to ARP-spoof in the GUI version.

Some of the ARP poisoning tools are listed below:

- BetterCAP (<https://www.bettercap.org>)
- Ettercap (<https://github.com>)
- ArpSpoofTool (<https://sourceforge.net>)
- MITMf (<https://github.com>)
- Cain & Abel (<http://www.oxid.it>)
- Arpoison (<https://sourceforge.net>)
- hping3 (<http://www.hping.org>)



### How to Defend Against ARP Poisoning

Implementation of Dynamic ARP Inspection (DAI) prevents poisoning attacks. DAI is a security feature that validates ARP packets in a network. When DAI activates on a VLAN, all ports on the VLAN are considered to be untrusted by default. DAI validates the ARP packets using a DHCP snooping binding table. The DHCP snooping binding table consists of MAC addresses, IP addresses, and VLAN interfaces acquired by listening to DHCP message exchanges. Hence, you must enable DHCP snooping before enabling DAI. Otherwise, establishing a connection between VLAN devices based on ARP is not possible. Consequently, a self-imposed DoS may result on any device in that VLAN.

To validate the ARP packet, the DAI performs IP address-to-MAC address binding inspection stored in the DHCP snooping database before forwarding the packet to its destination. If any invalid IP address binds a MAC address, the DAI will discard the ARP packet. It eliminates the risk of MITM attacks. DAI ensures the relay of only valid ARP requests and responses.

If the host systems in a network hold static IP addresses, the DHCP snooping will not be possible, or other switches in the network cannot run dynamic ARP inspection. In such situations, you have to perform static mapping that associates an IP address to a MAC address on a VLAN to prevent an ARP poisoning attack.

Implement software that runs custom scripts to monitor ARP tables. This script can compare the current ARP table to the list of known MAC addresses and IP addresses. If there is a mismatch in the list of valid MAC/IP pairs, the switch will drop the packet. Such scripts are helpful to defend against ARP poisoning attacks by monitoring the MAC/IP pairs on important LAN machines like servers, gateways, etc.

Implementation of cryptographic protocols as HTTP Secure (HTTPS), Secure Shell (SSH), Transport Layer Security (TLS), and various other networking cryptographic protocols prevents against ARP spoofing attack by encrypting data before transmission and authenticating it after it is received.

**Sniffing**  
Sniffing Technique:  
ARP Poisoning

## Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

1

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ^Z
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 10
DHCP snooping is operational on following VLANs: 10
DHCP snooping is configured on the following L3
Interfaces:
.....
DHCP snooping trust/rate is configured on the following
Interfaces:
Interface          Trusted      Rate limit (pps)
-----

```

3

```
Switch(config)# ip arp inspection vlan 10
Switch(config)# ^Z
Switch# show ip arp inspection
Source Mac Validation      : Disabled
Destination Mac Validation: Disabled
IP Address Validation      : Disabled
Vlan Configuration        Operation  ACL Match  Static ACL
10      Enabled      Active
Vlan ACL Logging          DHCP Logging  Probe Logging
10      Deny          Deny          Off
Vlan Forwarded           Dropped      DHCP Drops  ACL Drops
10      0              0            0            0
Vlan DHCP Permits        ACL Permits  Probe Permits Source MAC Failures
10      0              0            0            0
Vlan Dest MAC Failures   IP Validation Failures Invalid Protocol Data
10      0              0            0            0

```

2

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

```

4

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs
(Req) on Fa0/5, vlan
10, {{0013.6050.acf4/192.168.10.1/ffff.ffff.fff
f/192.168.10.1/05:37:31 UTC Mon Oct 30 2017}}

```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

As discussed, DHCP snooping must be enabled before enabling the dynamic ARP inspection (DAI). 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.

To configure DHCP snooping on a Cisco switch, make sure to enable DHCP snooping both globally and per access VLAN. To enable DHCP snooping, execute the following commands:

#### Configuring DHCP Snooping in Global configuration mode

```
Switch(config)# ip dhcp snooping
```

#### Configuring DHCP Snooping for a VLAN

```
Switch(config)# ip dhcp snooping vlan 10
```

```
Switch(config)# ^Z
```

#### To view the DHCP snooping status

```
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 switch is functioning only at layer 2, apply the `ip dhcp snooping trust` command to the layer 2 interfaces in order to designate uplink interfaces as trusted interfaces. This informs the switch that DHCP responses can arrive on those interfaces.

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

```
Switch(config)# show ip dhcp snooping binding
```

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

MAC Address	IP Address	Lease (sec)	Type	VLAN	Interface
1a:12:3b:2f:df:1c	10.10.10.8	125864	dhcp-snooping	4	FastEthernet0/3

Total number of bindings: 1

After establishing a DHCP snooping binding table, the user can start configuring dynamic ARP inspection for the VLAN. To enable dynamic ARP inspection for multiple VLANs, specify a range of VLAN numbers.

#### Command to configure ARP Inspection for a VLAN

```
Switch(config)# ip arp inspection vlan 10
```

```
Switch(config)# ^Z
```

#### Command to configure ARP Inspection for a range of VLANs

```
Switch(config)# ip arp inspection vlan 10, 11, 12, 13
```

Or

```
Switch(config)# ip arp inspection vlan 10-13
```

#### To view the ARP Inspection status

```
Switch(config)# 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. Even more, security can be attained by enabling one or more of these additional validation checks. To do so, execute the command `ip arp inspection validate` followed by the address type.

Assume that an attacker with source IP address 192.168.10.1 connects to VLAN 10 on interface FastEthernet0/5 and sends ARP replies, pretending to be the default router for the subnet in an attempt to initiate a MITM attack. The switch with dynamic ARP enabled inspection 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 there is no entry, 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
Oct30 2017])
```

If the discarding of packets starts, then the drop count begins to increase. 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(config)# 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    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
```

Sniffing

**Sniffing Technique:**  
ARP Poisoning

## ARP Spoofing Detection Tools

**XArp**

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

IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last seen
192.168.0.60	78-31-a1-c9-ea-38		LinkSystem	0x10-Realtek...	yes	no	16-01-2018 15:43:47	16-01-2018
192.168.0.69	64-00-aa-2b-e1-33	SEC2304-001	LinkSystem	0x10-Realtek...	yes	yes	16-01-2018 15:43:12	16-01-2018
192.168.0.76	00-15-56-96-02-03	192.168.0.76	Microsoft C...	0x10-Realtek...	yes	yes	16-01-2018 15:43:12	16-01-2018
192.168.0.75	64-00-aa-2b-e1-33		LinkSystem	0x10-Realtek...	yes	no	16-01-2018 15:43:12	16-01-2018
192.168.0.82	00-90-40-ae-36-03	RD03W-021	LinkSystem	0x10-Realtek...	yes	yes	16-01-2018 15:43:12	16-01-2018
192.168.0.83	ea-49-58-88-f5-17	CRT130-007	LinkSystem	0x10-Realtek...	yes	yes	16-01-2018 15:43:12	16-01-2018
192.168.0.83	78-31-a1-c9-ea-38		LinkSystem	0x10-Realtek...	yes	yes	16-01-2018 15:43:12	16-01-2018
192.168.0.84	10-7a-34-a7-06	85W-033	LinkSystem	0x10-Realtek...	yes	yes	16-01-2018 15:43:12	16-01-2018
192.168.0.85	64-00-aa-2b-e1-33		LinkSystem	0x10-Realtek...	yes	yes	16-01-2018 15:43:12	16-01-2018
192.168.0.86	64-00-aa-2b-e1-33		LinkSystem	0x10-Realtek...	yes	yes	16-01-2018 15:43:12	16-01-2018
192.168.0.87	00-90-40-ae-36-03	192.168.0.87	Grandstream	0x10-Realtek...	yes	yes	16-01-2018 15:43:12	16-01-2018

- Capsa Network Analyzer**  
<http://www.colasoft.com>
- ArpON**  
<http://arpon.sourceforge.net>
- ARP AntiSpoof**  
<https://sourceforge.net>
- ARPStraw**  
<https://github.com>
- shARP**  
<https://github.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### ARP Spoofing Detection Tools

- **XArp**

Source: <http://www.xarp.net>

XArp is a security application that detects ARP-based attacks. It detects critical network attacks that firewalls cannot cover. It uses advanced techniques to detect ARP attacks like ARP spoofing. The detection mechanism relies on two techniques: inspection modules and discoverers. Inspection modules look at ARP packets and check their correctness and validity with respect to the databases they have built up. Discoverers actively validate IP-MAC mappings and actively detect attackers. The mechanism detects ARP attacks and keeps data private. It even monitors whole subnets for ARP attacks. This application screens the whole subnet for ARP attacks using different security levels and fine-tuning possibilities. A local network that is subject to ARP attacks inspects every ARP packet and reports attacks against remote machines.

Some of the ARP spoofing detection tools are listed below:


- Capsa Network Analyzer (<http://www.colasoft.com>)
- ArpON (<http://arpon.sourceforge.net>)
- ARP AntiSpoof (<https://sourceforge.net>)
- ARPStraw (<https://github.com>)
- shARP (<https://github.com>)

Module 08 Page 913


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

**Sniffing**  
Sniffing Technique:  
Spoofing Attacks

## MAC Spoofing/Duplicating



- MAC duplicating attack is launched by **sniffing a network for MAC addresses** of clients who are actively associated with a switch port and re-using one of those addresses
- By listening to the traffic on the network, a malicious user can **intercept and use a legitimate user's MAC address** to receive all the traffic destined for the user
- This attack allows an attacker to **gain access to the network** and take over someone's identity on the network



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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Sniffing Technique: Spoofing Attacks

Besides ARP spoofing, an attacker can also use MAC spoofing and IRDP spoofing to sniff the traffic of a target network. This section describes spoofing techniques that help attackers to steal sensitive information.

#### MAC Spoofing/Duplicating

MAC duplicating refers to spoofing a 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 a MAC address with the MAC address of the legitimate client. 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 the identity of someone on the network.

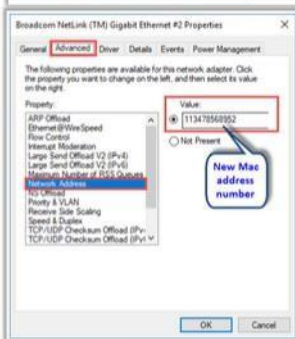


**Sniffing**  
Sniffing Technique:  
Spoofing Attacks

## MAC Spoofing Technique: Windows

**In Windows 10 OS**

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



1. Click **Start** and search for **Control Panel** and open it, then navigate to **Network and Internet** → **Networking and Sharing Center**
2. Click on the **Ethernet** and then click on the **Properties** in the **Ethernet Status** window
3. In the **Ethernet Properties** window, click on the **Configure** button and then click on the **Advanced** tab
4. Under the "Property" section, browse for **Network Address** and click on it
5. On the right side, under "Value", type in the new MAC address you would like to assign and click **OK**  
**Note:** Enter the MAC address number without "-" in between
6. Type "**ipconfig/all**" or "**net config rdr**" in command prompt to verify the changes
7. If the changes are visible then **reboot** the system, else try method 2 (change MAC address in the registry)

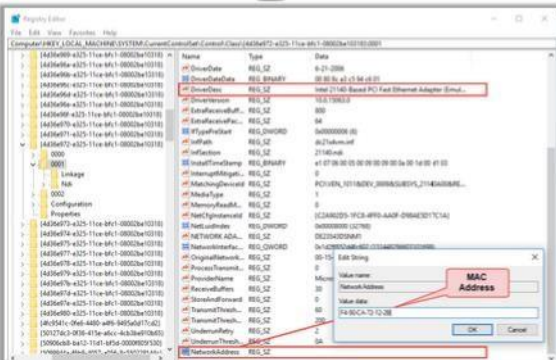
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


**Sniffing**  
Sniffing Technique:  
Spoofing Attacks

## MAC Spoofing Technique: Windows (Cont'd)

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

- 1. Press **Win + R** to open Run, type **regedit32** to start the registry editor  
**Note:** Do not type **Regedit** to start registry editor
- 2. Go to **"HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}"** and double click on it to expand the tree
- 3. 4-digit sub keys representing network adapters will be found (starting with 0000, 0001, 0002, etc.)
- 4. Search for the proper "DriverDesc" key to find the desired interface
- 5. Edit, or add, the string key "NetworkAddress" (data type "REG\_SZ") to contain the new MAC address
- 6. **Disable** and then **re-enable** the network interface that was changed or reboot the system





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### MAC Spoofing Technique: Windows

There are two methods for MAC spoofing in Windows 10 OS:

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

1. Click on **Start** and search for **Control Panel** and open it, then navigate to **Network and Internet** → **Networking and Sharing Center**.
2. Click on the **Ethernet** and then click on the **Properties** in the **Ethernet Status** window.

3. In the **Ethernet Properties** window, click on the **Configure** button and then on the **Advanced** tab.
4. Under the **"Property"** section, browse for **Network Address** and click on it.
5. On the right side, under **"Value"**, type in the new MAC address you would like to assign and click **OK**.

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

6. Type **"ipconfig/all"** or **"net config rdr"** in the command prompt to verify the changes.
7. If the changes are visible, then **reboot** the system, else try method 2 (change MAC address in the registry).

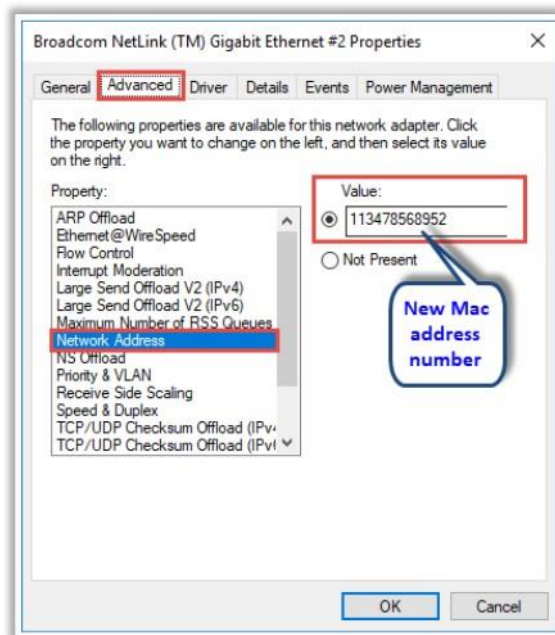


FIGURE 8.16: Ethernet Properties dialogue box

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

1. Press **Win + R** to open Run, type **regedt32** to start the registry editor.
2. **Note:** Do not type **Regedit** to start registry editor. Go to **"HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}"** and double click on it to expand the tree.
3. 4-digit sub keys representing network adapters will be found (starting with 0000, 0001, 0002, etc.).

4. Search for the proper "DriverDesc" key to find the desired interface.
5. Edit, or add, the string key "NetworkAddress" (data type "REG\_SZ") to contain the new MAC address.
6. Disable and then re-enable the network interface that was changed or reboot the system.

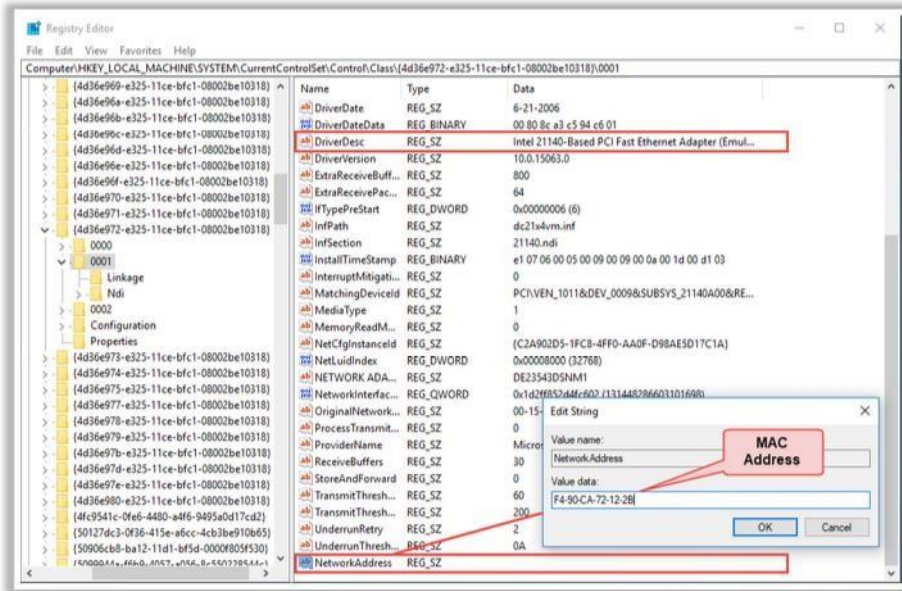


FIGURE 8.17: Registry Editor

### MAC Spoofing Tools

- **Technitium MAC Address Changer**

Source: <https://technitium.com>


Technitium MAC Address Changer (TMAC) allows you to change (spoof) Media Access Control (MAC) Address of your Network Interface Card (NIC) instantly. It has a very simple user interface and provides ample information regarding each NIC in the machine. Every NIC has a MAC address hard coded in its circuit by the manufacturer. This hard coded MAC address is used by windows drivers to access Ethernet Network (LAN). This tool can set a new MAC address to your NIC, bypassing the original hard coded MAC address.

Some of the MAC spoofing tools are listed below:

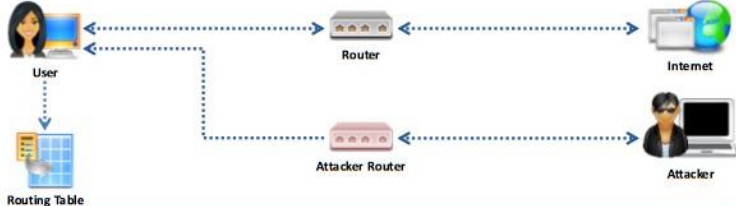
- **MAC Address Changer** (<http://www.novirusthanks.org>)
- **Change MAC Address** (<https://lizardsystems.com>)
- **GhostMAC** (<http://ghostmac.fevermedia.ro>)
- **Spoof-Me-Now** (<https://sourceforge.net>)
- **SMAC** (<http://www.klcconsulting.net>)
- **SpoofMAC** (<https://github.com>)
- **Win7 MAC Address Changer** (<http://www.zokali.com>)

**Sniffing**  
Sniffing Technique:  
Spoofing Attacks

## IRDP Spoofing



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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### IRDP Spoofing

The 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 advertisement messages. Since IRDP does not require any authentication, the target host will prefer the default route defined by the attacker to the default route provided by the DHCP server. The attacker accomplishes this by setting the preference level and the lifetime of the route at high values 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 the case of a Windows system configured as a DHCP client, the Windows checks the received router advertisements for entries. If there is only one, 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, it ignores the advertisement.

An attacker can use this to send spoofed router advertisement messages so that all the data packets travel through the attacker's system. Thus, the attacker can sniff the traffic and collect valuable information from the data packets. Attackers can use IRDP spoofing to launch MITM, DoS, and passive sniffing attacks.

- **Passive Sniffing:** In a switched network, the attacker spoofs IRDP traffic to re-route the outbound traffic of target hosts through the attacker's machine.
- **MITM:** Once sniffing starts, the attacker acts as a proxy between the victim and destination. The attacker plays an MITM role and tries to modify the traffic.
- **DoS:** IRDP spoofing allows remote attackers to add wrong route entries into victims routing table. The wrong address entry causes DoS.

Prevent IRDP spoofing attacks by disabling IRDP on hosts, if the OS permits it.

**Sniffing**  
 Sniffing Technique:  
 Spoofing Attacks

## How to Defend Against MAC Spoofing

CEH

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

```

sh ip dhcp snooping binding
-----
MacAddress      IpAddress      Lease      Type      VLAN      Interface
-----
2a:33:4c:2f:4a:1c  10.10.10.9    185235    dhcp-    4         FastEthernet3/18
                
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### How to Defend Against MAC Spoofing

Performing security assessments is the primary aim of an ethical hacker. An ethical hacker attacks a target network or organization with the knowledge and authorization of its management, to find loopholes in the security architecture. But the job does not end there. Finding those loopholes is a minor task. The most crucial task of ethical hacking is to apply the appropriate countermeasures to security loopholes in order to fix them.

Once you test the network for MAC spoofing attacks and collect security loopholes, you should apply countermeasures to protect the network again from MAC spoofing. Many MAC spoofing countermeasures can be applied to specific network architectures and loopholes. Apply the appropriate countermeasures to your network.

To detect MAC spoofing, it is necessary to know all the MAC addresses in the 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. Making changes to Port security interface configuration is another way to prevent MAC spoofing attacks. Once you enable the port security command, it allows you to specify the MAC address of the system connected to the specific port. It also allows for specific action to be taken if a port security violation occurs.

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


- **DHCP Snooping Binding Table:** The DHCP snooping process filters 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:** The system checks the IP to MAC address binding for each ARP packet in a network. While performing a Dynamic ARP inspection, the system will automatically drop invalid IP to MAC address bindings.
- **IP Source Guard:** IP Source Guard is a security feature in switches that restricts the IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database. It prevents spoofing attacks when the attacker tries to spoof or use the IP address of another host.
- **Encryption:** Encrypt the communication between the access point and computer to prevent MAC spoofing.
- **Retrieval of MAC Address:** You should always retrieve the MAC address from the NIC directly instead of retrieving it from the OS.
- **Implementation of IEEE 802.1X suites:** It is a type of network protocol for port-based Network Access Control (PNAC), and its main purpose is to enforce access control at the point where a user joins the network.
- **AAA (Authentication, Authorization and Accounting):** Use of AAA (Authentication, Authorization and Accounting) server mechanism in order to filter MAC addresses subsequently.

**Sniffing**  
Sniffing Technique:  
DNS Poisoning

## DNS Poisoning Techniques



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



The diagram illustrates the flow of a DNS poisoning attack. On the left, a group of 'Victims' is shown. A 'DNS Server' is connected to them. In the center, a globe represents the 'Internet DNS Spoofing (Remote network)'. Above it is 'Intranet DNS Spoofing (Local network)'. To the right is 'DNS Cache Poisoning'. Below the globe is 'Proxy Server DNS Poisoning'. On the right side, an 'Attacker' is shown with a laptop, connected to 'DNS Attack Scripts'. Dotted lines indicate the flow of information and the redirection of traffic from victims to the attacker's server.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Sniffing Technique: DNS Poisoning

This section describes DNS poisoning techniques to sniff the DNS traffic of a target network. Using this technique, an attacker can obtain the ID of the DNS request by sniffing and can send a malicious reply to the sender before the actual DNS server.

#### DNS Poisoning Techniques

DNS is the protocol that translates a domain name (e.g., [www.eccouncil.org](http://www.eccouncil.org)) into an IP address (e.g., 208.66.172.56). The protocol uses DNS tables that contain the domain name and its equivalent IP address stored in a distributed large database. In DNS spoofing, also known as DNS poisoning, the attacker tricks a DNS server into believing that it has received authentic information when in reality, it has not received any. The attacker tries to redirect the victim to a malicious server instead of the legitimate server. The attacker does this by manipulating the DNS table entries in the DNS. It results in substitution of a false IP address at the DNS level where web addresses are converted into numeric IP addresses.

When the victim tries to access a website, the attacker manipulates the entries in the DNS table so that the victim's system redirects the URL to the attacker's server. The attacker replaces IP address entries for a target site on a given DNS server with IP address of the server (malicious server) he/she controls. The attacker can create fake DNS entries for the server (containing malicious content) with the same names as that of the target server. Thus, the victim connects to the attacker's server without realizing it. Once the victim connects to the attacker's server, the attacker can compromise the victim's system and steal data.

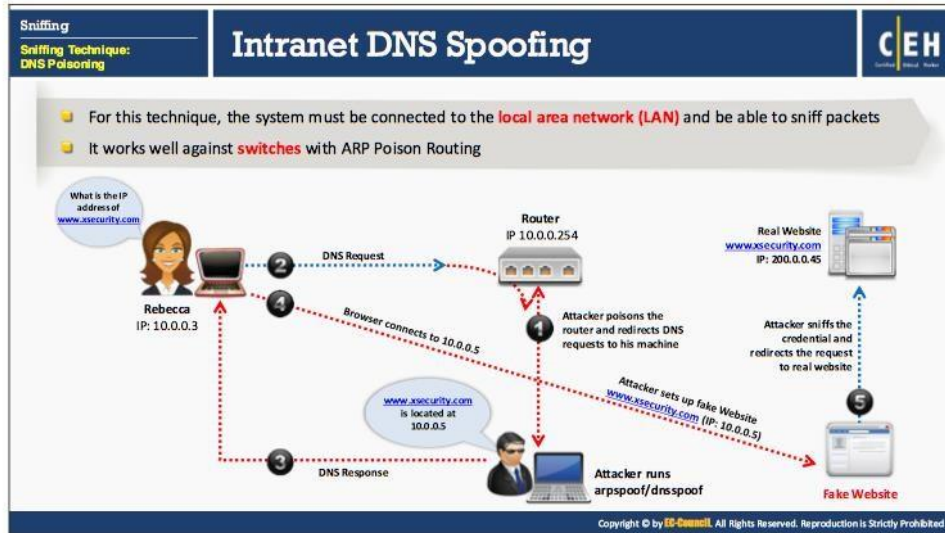


Similarly, an attacker can compromise a target system by conducting a DNS poisoning attack. To launch a DNS poisoning attack, follow these steps below:

- 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 your system the DNS server.
- 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 the victim.
- When the victim clicks on the Trojanned file, it will replace the victim's DNS entry in TCP/IP properties with that of your machine.
- You will become the DNS server for the victim, whose DNS requests will go through you.
- When the victim tries to open a password-protected website, the browser resolves instead to a fake website. Then, sniff the password and send her to the real website

DNS poisoning is possible using the following techniques:

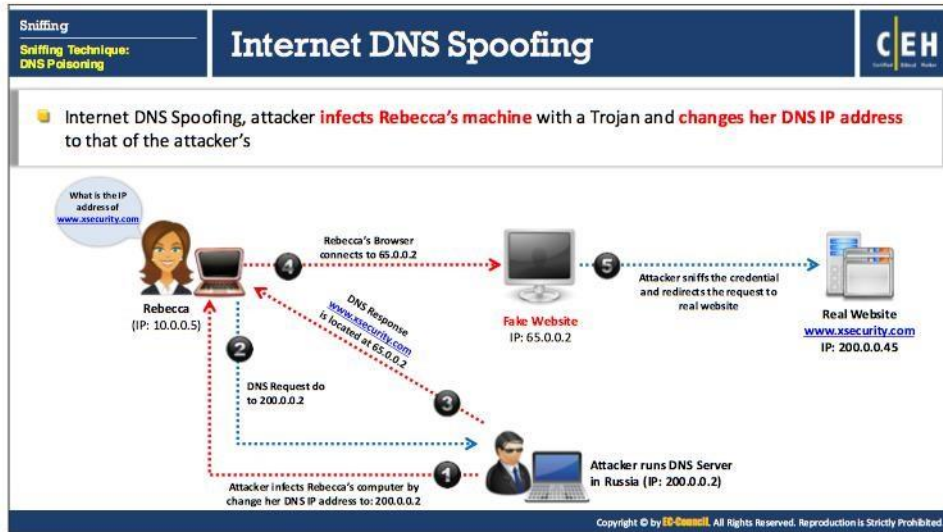
- Intranet DNS Spoofing
- Internet DNS Spoofing
- Proxy Server DNS Poisoning
- DNS Cache Poisoning



### Intranet DNS Spoofing

An attacker can perform an intranet DNS spoofing attack on a switched LAN with the help of the ARP poisoning technique. To perform this attack, the attacker must be connected to the LAN and be able to sniff the traffic or packets. An attacker who succeeds in sniffing the ID of the DNS request from the intranet can send a malicious reply to the sender before the actual DNS server.

In the diagram above, the attacker poisons the router by running arpspoof/dnsspoof 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. The attacker owns the website and 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. The attacker retrieves the required information and then redirects the client to the real website.

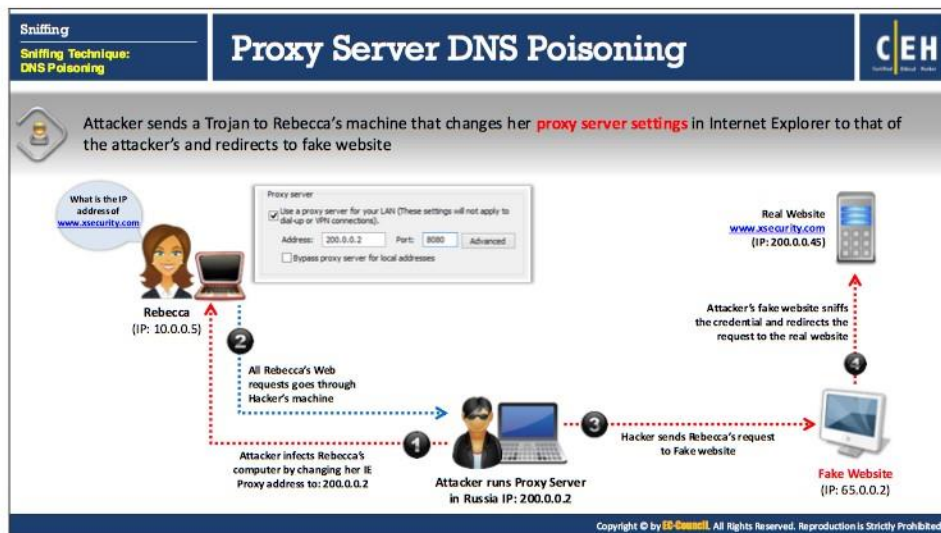


### Internet DNS Spoofing

Internet DNS poisoning is also known as remote DNS poisoning. Attackers can perform DNS spoofing attacks on a single or multiple victims anywhere in the world. In order to perform this attack, the attacker sets up a rogue DNS server with a static IP address.

Attackers perform Internet DNS spoofing with the help of Trojans when the victim's system connects to the Internet. It is an MITM attack in which 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 resolves to the attacker's system. Thus, the victim's traffic redirects to the attacker's system. At this point, the attacker can easily sniff the victim's confidential information.

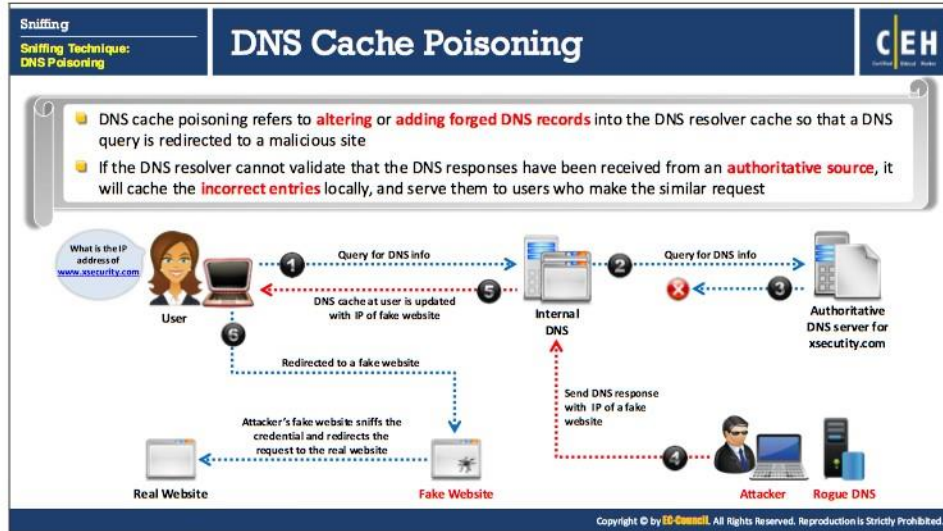
The figure in the slide above illustrates an attacker performing Internet DNS spoofing. The attacker infects Rebecca's machine with a Trojan and changes her DNS IP address to that of the attacker's.



### Proxy Server DNS Poisoning

In the proxy server DNS poisoning technique, the attacker sets up a proxy server on the attacker's system. The attacker also configures a fraudulent DNS and makes its IP address a primary DNS entry in the proxy server. The attacker changes the proxy server settings of the victim with the help of a Trojan. The proxy serves as a primary DNS and redirects the victim's traffic to the fake website where the attacker can sniff the confidential information of the victim and then redirect the request to the real website.

In the above figure, an attacker sends a Trojan to Rebecca's machine that changes her proxy server settings in Internet Explorer to that of the attacker's and redirects it to a fake website.



### DNS Cache Poisoning

DNS cache poisoning refers to altering or adding forged DNS records into the DNS resolver cache so that a DNS query is redirected to a malicious site. The DNS system uses cache memory to hold the recently resolved domain names. The attacker populates it with recently used domain names and their respective IP address entries. When a user request is received, the DNS resolver first checks the DNS cache; if the system finds the domain name that the user requested in the cache, the resolver will quickly send its respective IP address. Thus, it reduces the traffic and time of DNS resolving.

Attackers target this DNS cache and make changes or add entries to the DNS cache. If the DNS resolver cannot validate that the DNS responses have come from an authoritative source, it will cache the incorrect entries locally and serve them to users who make the same request. The attacker replaces the user-requested IP address with the fake IP address and when the user requests that domain name, the DNS resolver checks the entry in the DNS cache and picks the matched (poised) entry. Then it redirects the victim to the attacker's fake server instead of the intended server.

Sniffing		How to Defend Against DNS Spoofing		CEH	
Sniffing Technique: DNS Poisoning					
1	Implement <b>Domain Name System Security Extension (DNSSEC)</b>	8	Restrict <b>DNS recusing service</b> , either full or partial, to authorized users		
2	Use <b>Secure Socket Layer (SSL)</b> for securing the traffic	9	Use <b>DNS Non-Existent Domain (NXDOMAIN)</b> Rate Limiting		
3	Resolve all DNS queries to <b>local DNS server</b>	10	Secure your <b>internal machines</b>		
4	Block DNS requests being sent to <b>external servers</b>	11	Use <b>static ARP and IP table</b>		
5	Configure firewall to restrict <b>external DNS lookup</b>	12	Use <b>Secure Shell (SSH) encryption</b>		
6	Implement <b>intrusion detection system (IDS)</b> and deploy it correctly	13	Do not allow <b>outgoing traffic</b> to use <b>UDP port 53</b> as a <b>default source port</b>		
7	Configure <b>DNS resolver</b> to use a new random source port for each outgoing query	14	<b>Audit the DNS server</b> regularly to remove vulnerabilities		

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

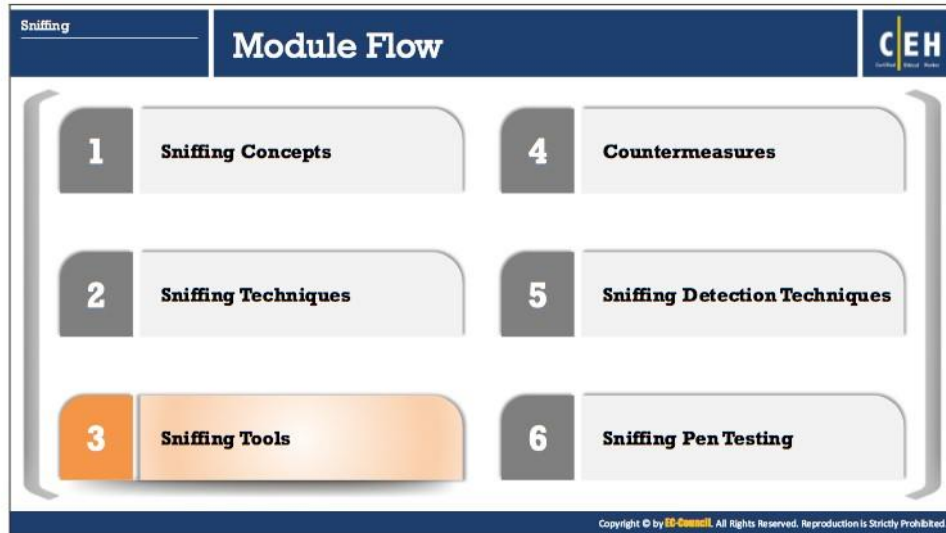
### How to Defend Against DNS Spoofing

Major DNS implementations have reported attacks using DNS spoofing, and this vulnerability still affects a large number of organizations. This is because of lack of information when performing DNS queries which allow attackers to spoof DNS responses. You have seen how an attacker carries out different types of DNS spoofing attacks. Let us know how to defend a network from these types of attacks.

Countermeasures that help prevent DNS spoofing attacks:

- Implement Domain Name System Security Extension (DNSSEC)
- Use Secure Socket Layer (SSL) for securing the traffic
- Resolve all DNS queries to local DNS server
- Block DNS requests being sent to external servers
- Configure firewall to restrict external DNS lookup
- Implement intrusion detection system (IDS) and deploy it correctly
- Configure DNS resolver to use a new random source port for each outgoing query
- Restrict DNS recusing service, either full or partial, to authorized users
- Use DNS Non-Existent Domain (NXDOMAIN) Rate Limiting
- Secure your internal machines
- Use static ARP and IP table
- Use Secure Shell (SSH) encryption

- Do not allow outgoing traffic to use UDP port 53 as a default source port
- Audit the DNS server regularly to remove vulnerabilities
- Use sniffing detection tools
- Do not open suspicious files
- Always use trusted proxy sites
- If a company handles its own resolver, it should be kept private and well protected
- Randomize source and destination IP addresses
- Randomize Query ID
- Randomize case in the name requests
- Use Public Key Infrastructure (PKI) to protect server
- Maintain a single or a specific range of IP addresses to log in to the systems
- Implement packet filtering for both inbound and outbound traffic



## Sniffing Tools

System administrators use automated tools to monitor their network, but attackers misuse these tools to sniff network data. This section describes tools that an attacker can use for sniffing.

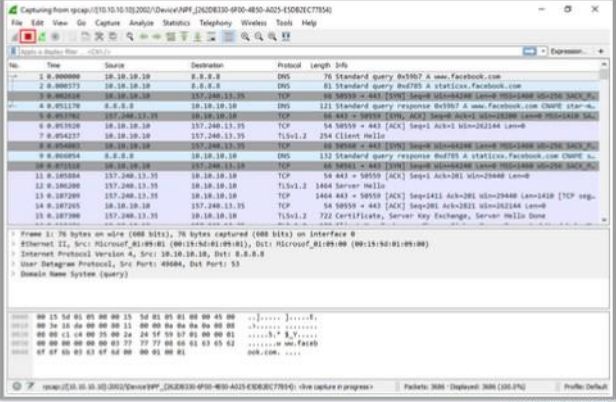


Sniffing

Sniffing Tool: Wireshark

CEH

- It lets you **capture and interactively browse the traffic** running on a computer network
- Wireshark uses **Winpcap** to capture packets on its own supported networks
- It **captures live network traffic** from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI networks
- A **set of filters** for customized data display can be refined using a display filter



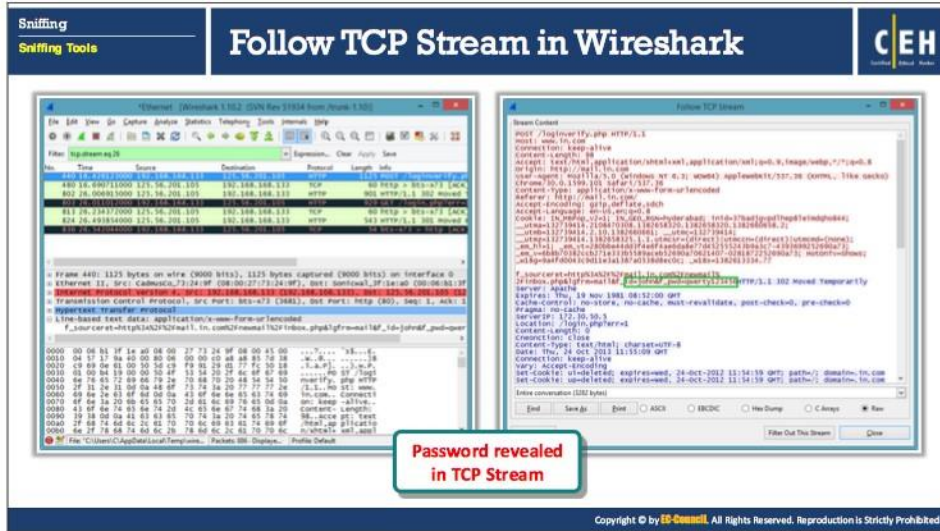
The screenshot shows the Wireshark interface with a list of captured packets. The list includes columns for No., Time, Source, Destination, Protocol, Length, and Info. The details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query).

<https://www.wireshark.org>  
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wireshark

Source: <https://www.wireshark.org>

Wireshark lets you capture and interactively browse the traffic running on a computer network. This tool uses Winpcap to capture packets on its own supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI networks. The captured files can be programmatically edited via command-line. A set of filters for customized data display can be refined using a display filter.



### Follow TCP Stream in Wireshark

Source: <https://www.wireshark.org>

Wireshark displays data from the TCP port with a feature known as "Follow TCP stream." The tool sees TCP data in the same way as that of the application layer. Use this tool to find passwords in a Telnet session or make sense of a data stream.

To see the TCP stream, select a TCP packet in the packet list of a stream/connection 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 tool displays the streaming content in the same sequence as it appeared on the network. It displays the captured data in ASCII, EBCDIC, HEX Dump, C Arrays, or Raw formats.

The infographic is titled "Display Filters in Wireshark" and is part of a "Sniffing Tools" series. It explains that display filters are used to change the view of packets in captured files. It lists five categories of filters with examples:

- 1 Display Filtering by Protocol**: Example: Type the protocol in the filter box; arp, http, tcp, udp, dns, ip
- 2 Monitoring the Specific Ports**:
  - `tcp.port==23`
  - `ip.addr==192.168.1.100 machine`
  - `ip.addr==192.168.1.100 && tcp.port=23`
- 3 Filtering by Multiple IP Addresses**:
  - `ip.addr == 10.0.0.4 or`
  - `ip.addr == 10.0.0.5`
- 4 Filtering by IP Address**:
  - `ip.addr == 10.0.0.4`
- 5 Other Filters**:
  - `ip.dst == 10.0.1.50 && frame.pkt_len > 400`
  - `ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30`
  - `ip.src==205.153.63.30 or ip.dst==205.153.63.30`

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Display Filters in Wireshark

Source: <https://wiki.wireshark.org>

Wireshark features display filters that filter traffic on the target network by protocol type, IP address, port, etc. Display filters are used to change the view of packets in the captured files. To set up a filter, type the protocol name, such as arp, http, tcp, udp, dns, ip, etc. in the filter box of Wireshark. Wireshark can use multiple filters at a time.

Some of the display filters in Wireshark are listed below:

- **Display Filtering by Protocol**  
Example: Type the protocol in the filter box; arp, http, tcp, udp, dns, ip
- **Monitoring the Specific Ports**
  - `tcp.port==23`
  - `ip.addr==192.168.1.100 machine`
  - `ip.addr==192.168.1.100 && tcp.port=23`
- **Filtering by Multiple IP Addresses**
  - `ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5`
- **Filtering by IP Address**
  - `ip.addr == 10.0.0.4`
- **Other Filters**
  - `ip.dst == 10.0.1.50 && frame.pkt_len > 400`
  - `ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30`
  - `ip.src==205.153.63.30 or ip.dst==205.153.63.30`

Sniffing		Additional Wireshark Filters		CEH	
Sniffing Tools					
1	<code>tcp.flags.reset==1</code> Displays all TCP resets	6	<code>!(arp or icmp or dns)</code> Masks out arp, icmp, dns, or other protocols and allows you to view traffic of you interest		
2	<code>udp contains 33:27:58</code> Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset	7	<code>tcp.port == 4000</code> Sets a filter for any TCP packet with 4000 as a source or destination port		
3	<code>http.request</code> Displays all HTTP GET requests	8	<code>tcp.port eq 25 or icmp</code> Displays only SMTP (port 25) and ICMP traffic		
4	<code>tcp.analysis.Retransmission</code> Displays all retransmissions in the trace	9	<code>ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16</code> Displays only traffic in the LAN (192.168.x.x), between workstations and servers -- no Internet		
5	<code>tcp contains traffic</code> Displays all TCP packets that contain the word 'traffic'	10	<code>ip.src != xxx.xxx.xxx.xxx &amp;&amp; ip.dst != xxx.xxx.xxx.xxx &amp;&amp; sip</code> Filter by a protocol ( e.g. SIP ) and filter out unwanted IPs		

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Additional Wireshark Filters

Source: <https://wiki.wireshark.org>

Some of the Wireshark filters are listed below:

- `tcp.flags.reset==1`  
Displays all TCP resets
- `udp contains 33:27:58`  
Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset
- `http.request`  
Displays all HTTP GET requests
- `tcp.analysis.retransmission`  
Displays all retransmissions in the trace
- `tcp contains traffic`  
Displays all TCP packets that contains the word 'traffic'
- `!(arp or icmp or dns)`  
Masks out arp, icmp, dns, or other protocols and allows you to view traffic of your interest
- `tcp.port == 4000`  
Sets a filter for any TCP packet with 4000 as a source or destination port


- `tcp.port eq 25 or icmp`  
Displays only SMTP (port 25) and ICMP traffic
- `ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16`  
Displays only traffic in the LAN (192.168.x.x), between workstations and servers -- no Internet
- `ip.src != xxx.xxx.xxx.xxx && ip.dst != xxx.xxx.xxx.xxx && sip`  
Filter by a protocol ( e.g. SIP ) and filter out unwanted IPs

**Sniffing**  
Sniffing Tools

## Sniffing Tools: SteelCentral Packet Analyzer and Capsa Network Analyzer


**SteelCentral Packet Analyzer**

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



**Capsa Network Analyzer**

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### SteelCentral Packet Analyzer

Source: <https://www.riverbed.com>

SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. This tool comes integrated with Riverbed AirPcap adapters to analyze and troubleshoot 802.11 wireless networks. As it captures terabytes of packet data traversing the network, this tool reads that traffic and displays it in a GUI. It can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (physical, virtual, or embedded on SteelHeads) without a large file transfer; to identify anomalous network issues or diagnose and troubleshoot complex network and application performance issues down to the bit level. This tool can also:

- Isolate and identify traffic of interest through an extensive collection of network analysis metrics called “Views”
- Baseline and monitor long-duration network traffic with a flexible trigger-alerting mechanism called “Watches”
- Integrated with Wireshark and works with Wireshark’s capture and display filters and prodigious dissector library for deep packet analysis
- Analyze all types of data on the network including VDI
- Streamline transaction troubleshooting workflow

## Capsa Network Analyzer

Source: <http://www.colasoft.com>

Capsa Network Analyzer is a network-monitoring tool that captures all the data transmitted over the network and provides a wide range of analysis statistics in an intuitive and graphic way. The tool helps 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 to detect network vulnerabilities. An attacker can use this tool to sniff packets from the target network.

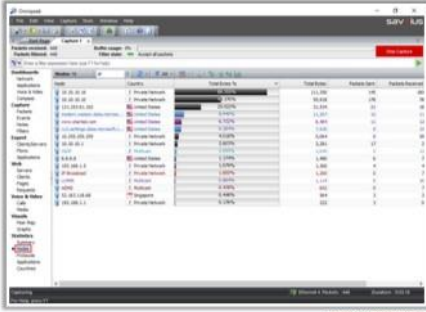
### Features:

- Real-time capture and save data transmitted over local networks, including wired networks and 802.11a/b/g/n wireless networks.
- Identify and analyze more than 1040 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 a summary and decoding information about these packets.
- View network statistics at a single glance, allowing easy capture and interpretation of network utilization data.
- Monitor Internet, email, and instant messaging traffic, helping keep employee productivity to a maximum level.
- 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 of them.
- Visualize the entire network in an ellipse that shows the connections and traffic between each host.

**Sniffing Tools: OmniPeek and Observer Analyzer**

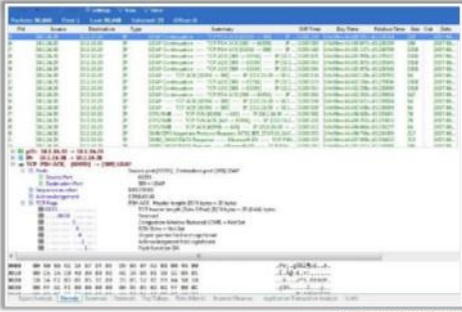
**OmniPeek**

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



**Observer Analyzer**

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



<https://www.savvius.com> <https://www.viavisolutions.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### OmniPeek

Source: <https://www.savvius.com>

OmniPeek network analyzer provides real-time visibility and expert analysis of each part of the target network. This tool will analyze, drill down, and fix performance bottlenecks across multiple network segments. Analytic plug-ins provide targeted visualization and search abilities within OmniPeek. The Google Maps plug-In enhances the analysis capabilities of the 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 can monitor a network in real time, and shows the source location of that traffic. Attackers can use this tool to analyze a network and inspect the packets in the network.

### Observer Analyzer

Source: <https://www.viavisolutions.com>

Observer Analyzer monitors unified communications (UC) deployments, network performance, applications, and troubleshooting on complex networks including VM environments. It provides the complete package needed to achieve peak performance:

- Total visibility into network and application health
- High-level to granular views
- Detailed HTTP tracking for client browser and OS type
- Customized Key Performance Indicators (KPIs)
- In-depth troubleshooting with root-cause analysis
- Application performance analytics
- Expert Analysis alerts you to potential problems and solution strategies.



The screenshot shows a webpage titled "Additional Sniffing Tools" with a dark blue header. On the left, there is a sidebar with "Sniffing" and "Sniffing Tools" links. The main content area contains a grid of 15 tool cards, each with an icon, the tool name, and a URL. The tools listed are: PRTG Network Monitor, Colasoft Packet Builder, RSA NetWitness Investigator, tcpdump, NetFlow Analyzer, CommView, NetResident, ntopng, SmartSniff, Free Network Analyzer, CSniffer, EtherApe, Network Probe, WebSiteSniffer, and Kismet. A footer at the bottom of the grid reads: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

### Additional Sniffing Tools

Many other tools can monitor network traffic, and capture and analyze packet data. Some of the sniffing tools are listed below:

- PRTG Network Monitor (<https://www.paessler.com>)
- Colasoft Packet Builder (<http://www.colasoft.com>)
- RSA NetWitness Investigator (<https://community.rsa.com>)
- tcpdump (<http://www.tcpdump.org>)
- NetFlow Analyzer (<https://www.manageengine.com>)
- CommView (<https://www.tamos.com>)
- NetResident (<https://www.tamos.com>)
- ntopng (<http://www.ntop.org>)
- SmartSniff (<http://www.nirsoft.net>)
- Free Network Analyzer (<https://freenetworkanalyzer.com>)
- CSniffer (<https://www.mcafee.com>)
- EtherApe (<http://etherape.sourceforge.net>)
- Network Probe (<http://www.objectplanet.com>)
- WebSiteSniffer (<http://www.nirsoft.net>)
- Kismet (<https://www.kismetwireless.net>)
- Ettercap (<https://github.com>)

- Alchemy Eye (<http://www.alchemy-lab.com>)
- BetterCAP (<https://www.bettercap.org>)
- Nast (<https://sourceforge.net>)
- IPgrab (<http://ipgrab.sourceforge.net>)
- Netstumbler (<http://www.netstumbler.com>)
- EffeTech HTTP Sniffer (<http://www.effetech.com>)
- SniffPass (<http://www.nirsoft.net>)
- netsniff-ng toolkit (<http://netsniff-ng.org>)
- Ace Password Sniffer (<http://www.effetech.com>)
- MaaTec Network Analyzer (<http://www.maatec.com>)
- AIM Sniffer (<http://www.effetech.com>)
- WinDump (<https://www.winpcap.org>)



### Packet Sniffing Tools for Mobile

- **Wi.cap. Network Sniffer Pro**

Source: <https://play.google.com>

This tool is a mobile network packet sniffer for ROOT ARM droids. It works on the rooted Android mobile devices.

**Features:**

- Parallel packet captures for various type of connections such as Wi-Fi, 3G, LTE, etc.
- Real-time packet information
- Flexible packet filtering
- Active network operations
- Supports Wireshark format such as cap, pcap, etc.

- **FaceNiff**

Source: <http://faceniff.ponury.net>

FaceNiff is an Android app that can sniff and intercept web session profiles over the Wi-Fi connected to the mobile. This app works on rooted android devices. The Wi-Fi connection should be over Open, WEP, WPA-PSK, or WPA2-PSK networks while sniffing the sessions.

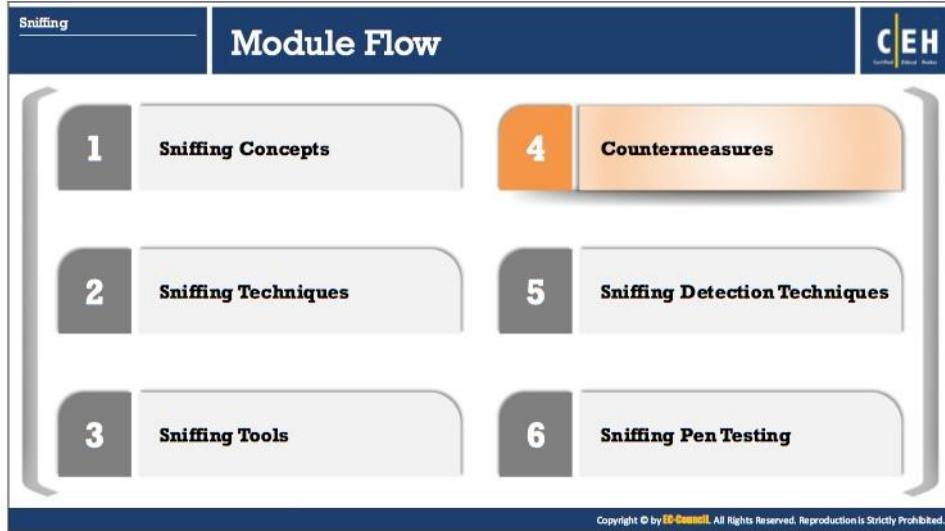
- **Packet Capture**

Source: <https://play.google.com>

Packet capture is a network traffic sniffer app with SSL decryption. It is a powerful debugging tool, especially when developing an app.

**Features:**

- Capture network packets and record them
- SSL decryption using man-in-the-middle technique
- No root required
- Show packet in either hex or text



## Countermeasures

The previous section describes how an attacker carries out sniffing with different techniques and tools. This next section describes countermeasures and possible defensive techniques used to defend a target network against sniffing attacks.

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Countermeasures	How to Defend Against Sniffing (Cont'd)	CEH	
08	Use HTTPS instead of HTTP to protect user names and passwords	12	Always encrypt the wireless traffic with a strong encryption protocol such as WPA and WPA2
09	Use switch instead of hub as switch delivers data only to the intended recipient	13	Retrieve MAC directly from NIC instead of OS; this prevents MAC address spoofing
10	Use Secure File Transfer Protocol (SFTP), instead of FTP for secure transfer of files	14	Use tools to determine if any NICs are running in the promiscuous mode
11	Use PGP and S/MIME, VPN, IPsec, SSL/TLS, Secure Shell (SSH) and One-time passwords (OTP)	15	Use a concept of ACL or Access Control List to allow access to only a fixed range of trusted IP addresses in a network

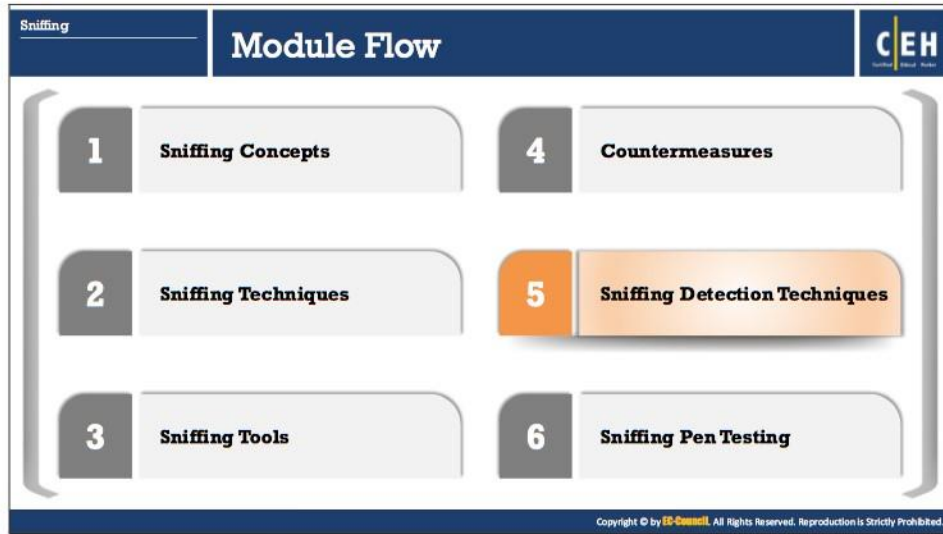
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### How to Defend Against Sniffing

Listed below are some of the countermeasures to be followed to defend against sniffing:

- Restrict the physical access to the network media to ensure that a packet sniffer cannot be installed.
- Use end-to-end encryption to protect confidential information.
- Permanently add the MAC address of the gateway to the ARP cache.

- Use static IP addresses and 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 the 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 connection, etc. to protect wireless network users against sniffing attacks.
- Use HTTPS instead of HTTP to protect usernames and passwords.
- Use switch instead of the hub as switch delivers data only to the intended recipient.
- Use Secure File Transfer Protocol (SFTP), instead of FTP for secure transfer of files.
- Use PGP and S/MIME, VPN, IPSec, SSL/TLS, Secure Shell (SSH), and One-time passwords (OTP).
- Always encrypt the wireless traffic with a strong encryption protocol such as WPA and WPA2.
- Retrieve MAC directly from NIC instead of OS; this prevents MAC address spoofing.
- Use tools to determine if any NICs are running in the promiscuous mode.
- Use a concept of ACL or Access Control List to allow access to only a fixed range of trusted IP addresses in a network.
- Change default passwords to complex passwords.
- Avoid broadcasting SSID (Session Set Identifier).
- Implement MAC filtering mechanism on your router.



## Sniffing Detection Techniques

It is very difficult to detect passive sniffers, especially when they are running on a shared Ethernet. This section discusses some detection techniques.

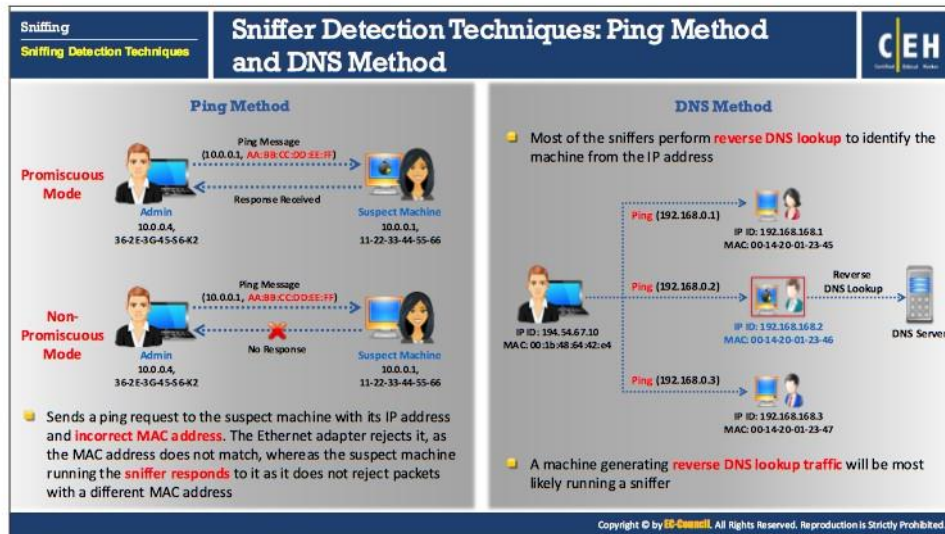


The infographic is titled "How to Detect Sniffing" and is part of a "Sniffing Detection Techniques" series. It is presented in a three-column layout. The first column, "Promiscuous Mode", lists two points: checking machines in promiscuous mode and the ability to intercept and read every network packet. The second column, "IDS", lists two points: running IDS to detect MAC address changes and receiving alerts for suspicious activities. The third column, "Network Tools", lists two points: using tools like Capsa Network Analyzer to detect strange packets and the ability to collect, consolidate, and analyze traffic data. Each column includes a small icon representing the concept: a server for promiscuous mode, a monitor for IDS, and a network diagram for network tools. A copyright notice for EC-Council is at the bottom.

Promiscuous Mode	IDS	Network Tools
<ul style="list-style-type: none"><li>You will need to <b>check which machines are running</b> in the promiscuous mode</li><li>Promiscuous mode allows a network device to <b>intercept and read each network packet</b> that arrives in its entirety</li></ul>	<ul style="list-style-type: none"><li><b>Run IDS</b> and notice if the <b>MAC address</b> of certain machines has changed (Example: router's MAC address)</li><li>IDS can alert the administrator about <b>suspicious activities</b></li></ul>	<ul style="list-style-type: none"><li>Run network tools such as <b>Capsa Network Analyzer</b> to monitor the network for detecting strange packets</li><li>Enables to <b>collect, consolidate, centralize, and analyze traffic data</b> across different network resources and technologies</li></ul>

### How to Detect Sniffing

It is not easy to detect a sniffer on a network as it only captures data and runs in promiscuous mode. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer leaves no trace since it does not transmit data. To find sniffers, check for systems that are running in promiscuous mode which is a NIC mode 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 helps to detect non-standalone sniffers. There are many tools, such as the Nmap that are available to use for the detection of promiscuous mode. Run IDS and notice if the MAC address of certain machines has changed (Example: router's MAC address). IDS can detect sniffing activities on a network. It notifies or alerts the administrator when a suspicious activity such as sniffing or MAC spoofing occurs. Network tools such as Capsa Network Analyzer monitors the network for strange packets such as packets with spoofed addresses. This tool can collect, consolidate, centralize, and analyze traffic data across different network resources and technologies.



### Sniffer Detection Techniques

#### ▪ Ping Method

To detect a sniffer on a network, identify the system on the network running in promiscuous mode. 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.

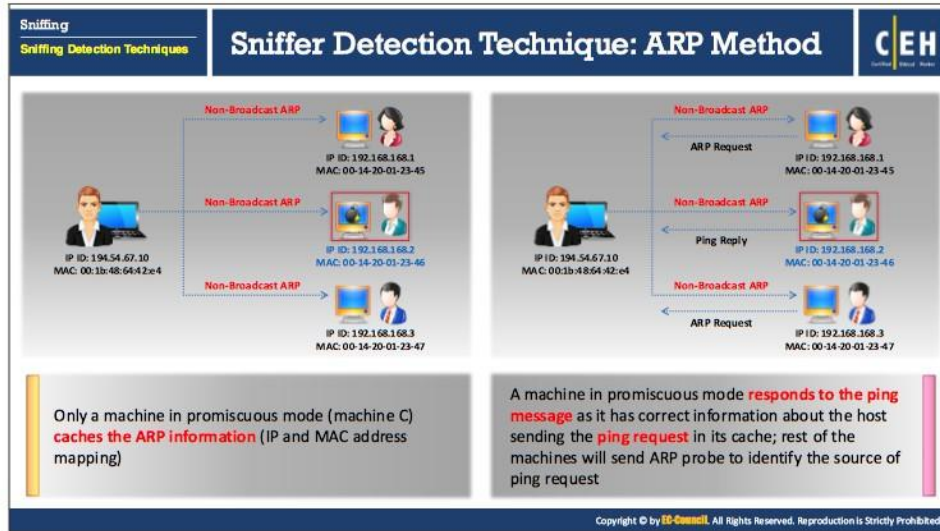
Just send a ping request to the suspected machine with its IP address and incorrect MAC address. The adapter will reject it since the MAC address does not match, whereas the suspect machine running the sniffer responds to it, as it does not reject packets with a different MAC address. Thus, this response will identify the sniffer in the network.

#### ▪ DNS Method

The reverse DNS lookup is the opposite of the DNS lookup method. Sniffers using reverse DNS lookup increase network traffic. This increase in network traffic can be an indication of the presence of a sniffer on the network.

Users can perform a reverse DNS lookup remotely or locally. Monitor the organization's DNS server to identify incoming reverse DNS lookups. The method of sending ICMP requests to a non-existing IP address can also 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, configure the detector in promiscuous mode. Send an ICMP request to a non-existing IP address, and view the response. If the system receives a response, the user can identify the responding machine as performing reverse DNS lookups on the local machine. A machine generating reverse DNS lookup traffic will be most likely running a sniffer.



### Sniffer Detection Techniques: ARP Method

This technique sends a non-broadcast ARP to all the nodes in the network. The node that runs in promiscuous mode on the network will cache the local ARP address. Then it will broadcast a ping message on the network with the local IP address but a different MAC Address. In this case, only the node that has the MAC address (cached earlier) will be able to respond to your broadcast ping request. A machine in promiscuous mode replies to the ping message as it has correct information about the host that is sending ping request in its cache; rest of the machines will send ARP probe to identify the source of the ping request. This will detect the node on which the sniffer is running.

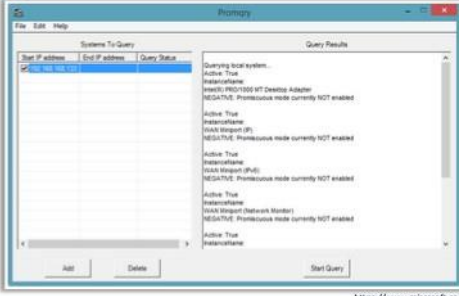
Sniffing  
Sniffing Detection Techniques

## Promiscuous Detection Tools

CEH  
Certified Ethical Hacker

### PromqryUI

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



<https://www.microsoft.com>

### Nmap

- Nmap's NSE script allows you to check if a target on a local Ethernet has its network card in **promiscuous mode**
- Command to detect NIC in promiscuous mode:**  
`nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]`



<https://nmap.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Promiscuous Detection Tools

- **PromqryUI**

Source: <https://www.microsoft.com>

The PromqryUI tool detects which network interface card is running in promiscuous mode. It can determine accurately if a 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. A version of PromqryUI is available as a command line tool. PromqryUI can:

- Query the local computer's network interfaces
- Query a single remote computer's interfaces
- Query a range of remote computers' interfaces

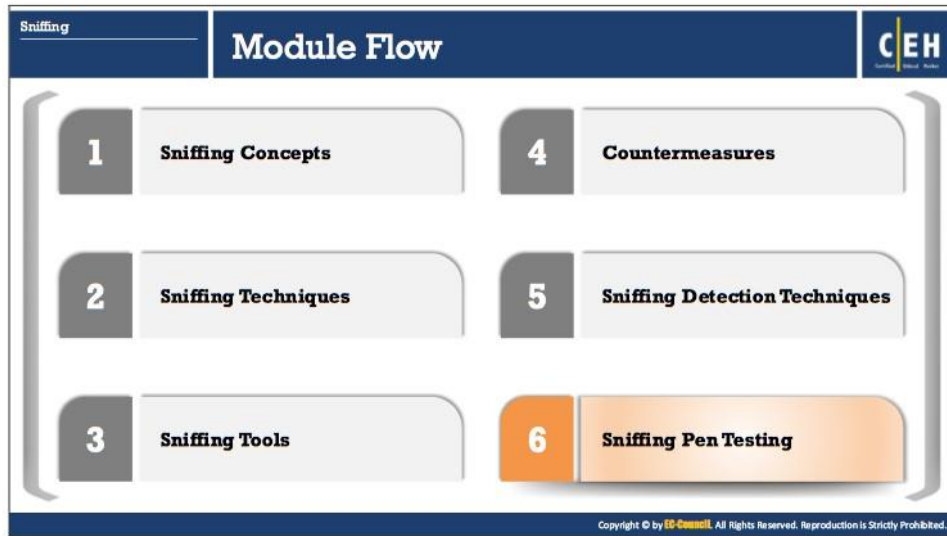
- **Nmap**

Source: <https://nmap.org>

Nmap's NSE script allows you to check if a target on a local Ethernet has its network card in promiscuous mode.

Command to detect NIC in promiscuous mode:

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



**Sniffing**  
Sniffing Pen Testing

## Sniffing Penetration Testing

CEH

- Sniffing pen test is used to check if the **data transmission** from an organization is **secure from sniffing and interception attacks**
- Sniffing pen test helps administrators to:
  - Audit the network traffic** for malicious content
  - Implement security mechanism** such as SSL and VPN to secure the network traffic
  - Identify rogue sniffing application** in the network
  - Discover rogue DHCP and DNS servers** in the network
  - Discover the presence of **unauthorized networking devices**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

**Sniffing**  
Sniffing Pen Testing

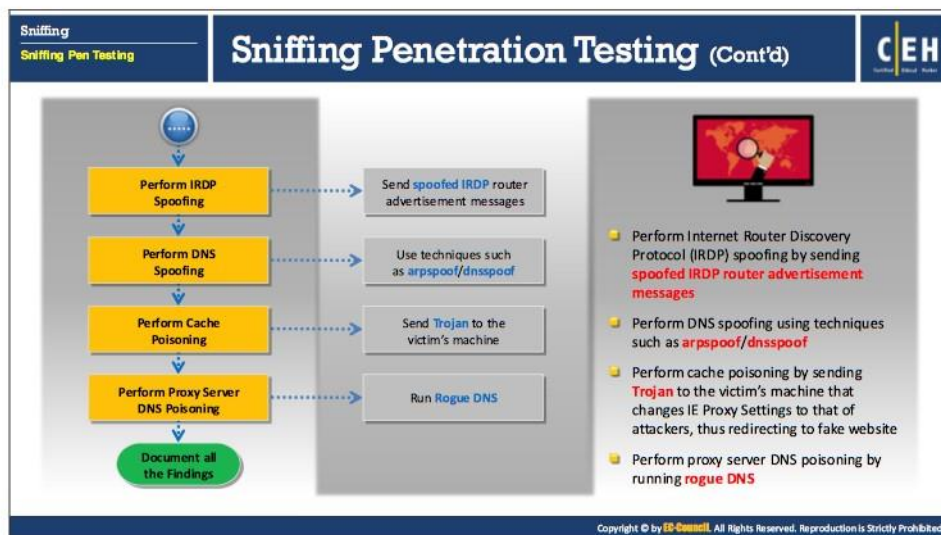
## Sniffing Penetration Testing (Cont'd)

CEH

The flowchart starts with a 'START' button, followed by a sequence of attack types: Perform MAC Flooding Attack, Perform DHCP Starvation Attack, Perform Rogue Server Attack, Perform ARP Poisoning, and Perform MAC Spoofing. Each attack type is linked to specific tools or actions: Yersinia and macof for MAC flooding; Yersinia for DHCP starvation; Run rogue DHCP server for Rogue Server Attack; Ufasoft Snif, BetterCAP, Ettercap, etc. for ARP poisoning; and Technitium MAC Address Changer for MAC spoofing. A list of tools and actions is also provided on the right side of the diagram.

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Sniffing Penetration Testing

Conducting a security assessment to identify vulnerabilities can protect a network from sniffing attacks. This section describes the pen testing process that simulates sniffing attacks. It involves series of steps during which the pen tester uses different techniques and tools to sniff the target network.

You have learned how the attacker sniffs the conversation in a target network to gain confidential information. This section describes how to test a target network for sniffing attacks. A pen tester should simulate the actions of an attacker performing a sniffing attack to check the target network for sniffing. Pen testing will determine whether the network is vulnerable to any type of sniffing or interception attacks.

Sniffing pen test helps administrators to:

- Audit the network traffic for malicious content
- Implement security mechanism such as SSL and VPN to secure the network traffic
- Identify rogue sniffing application in the network
- Discover rogue DHCP and DNS servers in the network
- Discover the presence of unauthorized networking devices

A pen test simulates sniffing attacks that an attacker might carry out. A pen tester should try all possible ways of sniffing the network. This ensures the full scope pen test, which will reveal the maximum possible vulnerabilities in the network.

Follow specific pen testing steps to perform the test successfully. Let us begin with the sniffing pen testing steps:

- **Step 1: Perform MAC Flooding Attack**

Flood the switch with many Ethernet frames, each containing different source MAC addresses. Check whether the switch enters into the fail-open mode, in which the switch broadcasts data to all ports rather than just to the port intended to receive the data. If this happens, the attackers have the ability to sniff network traffic. You can use tools such as Yersinia and macof for detection.

- **Step 2: Perform 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. If this happens, the attackers will have the chance to sniff network traffic or DHCP requests of clients by building a rogue DHCP server. Test for DHCP starvation attacks by using tools such as Yersinia and Hyenae.

- **Step 3: Perform 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 ARP Poisoning**

Try to compromise the ARP table and change the MAC address so that the IP address points to another machine. If this is successful, the attackers can also do the same thing and steal information by changing the MAC address to their own system. To perform ARP poisoning, use tools such as Ufasoft Snif, BetterCAP, and Ettercap.

- **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 this succeeds, an attacker can bypass the access control lists on routers or servers by pretending to be another device on the network. If the network allows this kind of attack, then attackers can also break into the network and steal data. To prevent this, use tools such as Technitium MAC Address Changer (TMAC).

- **Step 6: Perform IRDP Spoofing**

Perform Internet Router Discovery Protocol (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. If the router changes its default path, then it is vulnerable to DoS attacks, passive sniffing, and/or MITM attacks.

- **Step 7: Perform DNS Spoofing**

Perform DNS spoofing using techniques such as arpspoof/dnsspoof. The DNS spoofing attack misdirects the victim to another address that is under the control of the attacker. The attacker intercepts the DNS request of the victim and sends a response with a spoofed



IP address before the actual response arrives at the victim's system. The spoofed DNS redirects the victim to the attacker's site. To prevent this kind of attack, maintain proper IDS/IPS across the network.

- **Step 8: Perform Cache Poisoning**

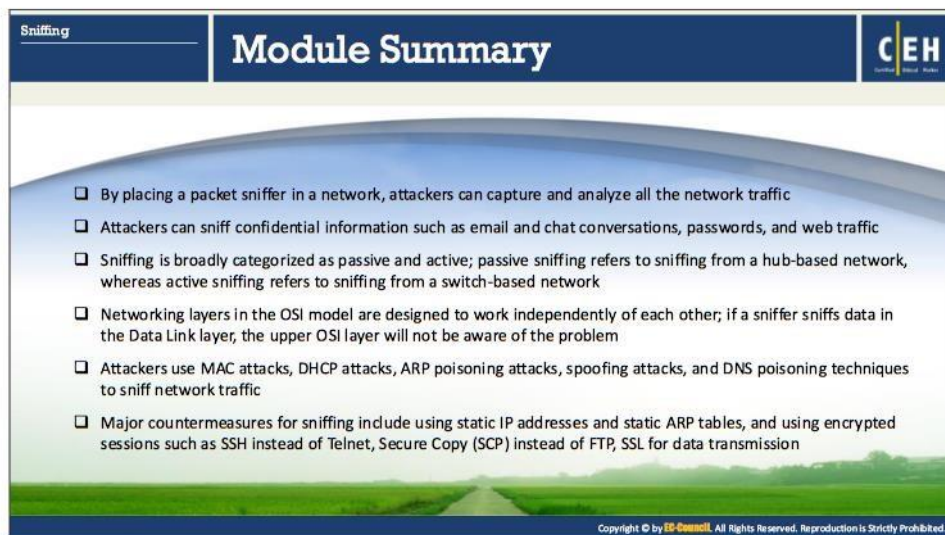
Perform cache poisoning by sending a Trojan to the victim's machine that changes proxy server settings in IE, thus redirecting to a fake website.

- **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 a rogue DNS as the primary DNS entry in the proxy server system. 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 the victim and the website being visited.

- **Step 10: Document all the Findings**

After performing all these tests, document all findings and tests conducted. Analyze the target's security and plan countermeasures to cover any security gaps.



The slide features a dark blue header with the word "Sniffing" on the left and the "CEH" logo on the right. The main title "Module Summary" is centered in a large, white font. Below the title, a list of six bullet points is presented against a background of a road stretching into a green field under a blue sky. The text is white for readability. At the bottom right of the slide, there is a small copyright notice.

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Module Summary

This module familiarized you with topics related to sniffing such as sniffing concepts, attacks, tools, and detection techniques. The end of this module described sniffing countermeasures and the steps involved in full-scope pen testing.