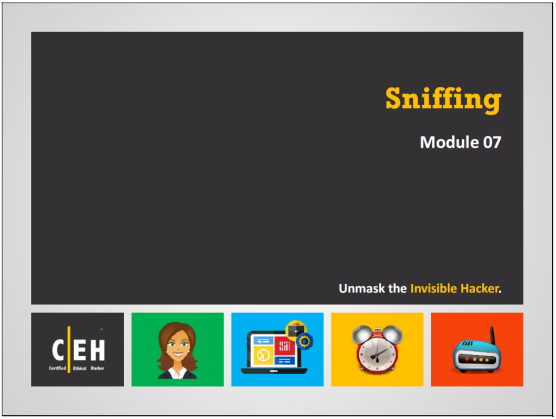
Sniffing

Module 07

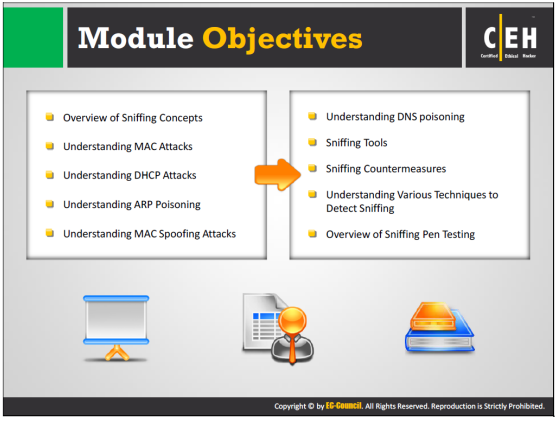


Ethical Hacking and Countermeasures v9

Module 07: Sniffing

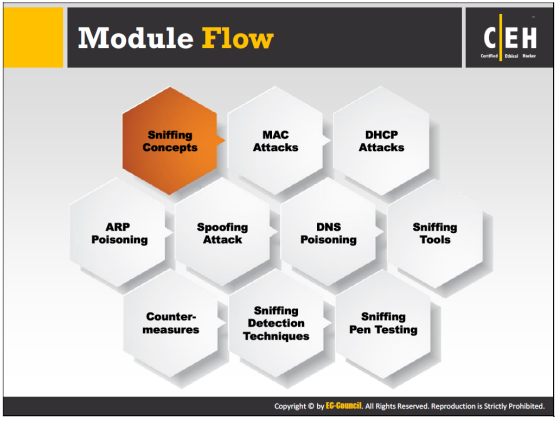
Exam 312-50

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



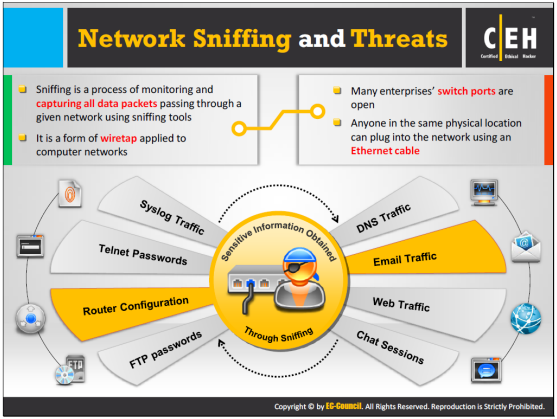
This module starts with an overview of sniffing concepts, and provides an insight into MAC, DHCP, ARP, MAC spoofing, and DNS poisoning attacks. Later the module discusses various tools, countermeasures, and sniffing detection techniques. The module ends with an overview of penetration (pen) testing steps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

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



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, lawful interception, and a wiretapping case study—PRISM.

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



Packet sniffing is a process of monitoring and capturing all data packets passing through a given network using a software application or a hardware device. Sniffing is straightforward in hub-based networks, as the traffic on a segment passes by all 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 to see all 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, 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, 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 carry out attacks that are even more effective by combining this technique with active transmission.

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

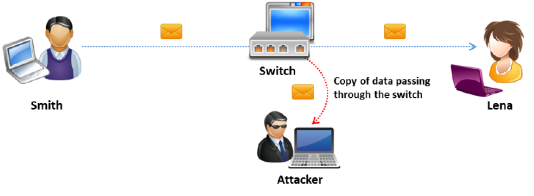
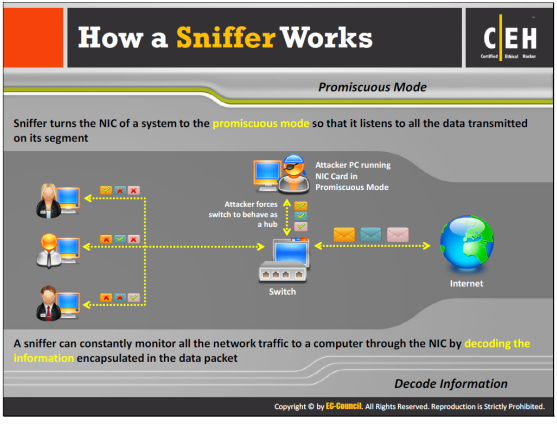


FIGURE 7.1: Packet Sniffing Scenario

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



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 rather than the IP address. The Network Layer is responsible for mapping IP network addresses to the MAC address as required by the Data Link Protocol. It initially looks for the MAC address of the destination machine in a table, usually called the ARP cache. If 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 hosts, which 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 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 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**

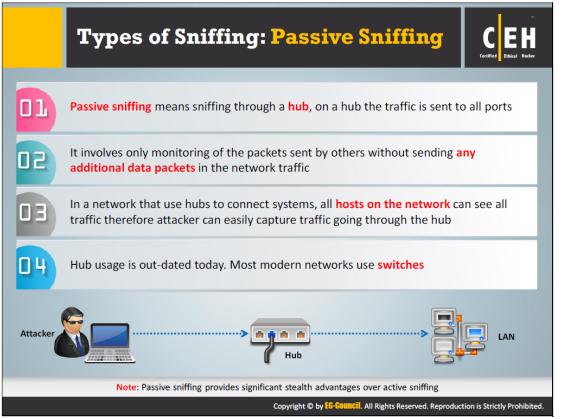
  ARP is stateless. The machine can send an ARP reply even without asking for it, and accepts such a reply. When a machine wants to sniff the traffic originating from another system, it can ARP spoof the gateway of the network. The ARP cache of the target machine will have a wrong entry for the gateway. 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 cannot keep up. Once this happens to a switch, it then enters failopen 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. Attackers configure the NIC in their machines to run in promiscuous mode, so that the card starts accepting all the packets. This way, the attacker can view all the packets transmitting in the network.

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



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 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 traffic. Hence, it is easy to capture traffic going through the hub using passive sniffing.

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

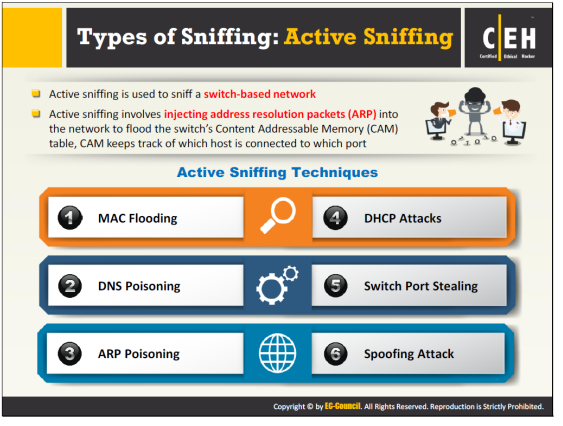
- **Compromising the physical security**: An attacker who succeeds in compromising the physical security of the target organization can walk in to the organization with a laptop and try to plug in to the network and capture sensitive information about the organization.

- **Using a Trojan horse**: Most Trojans have built-in sniffing capability. An attacker can install Trojans with built-in sniffing capabilities on a victim machine to compromise it. After compromising the victim 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.

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

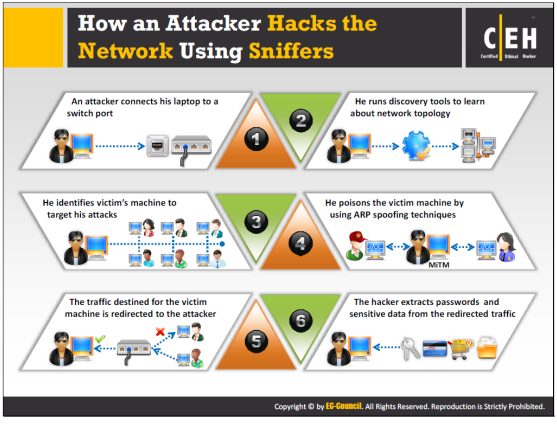


Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN. Active sniffing also refers to sniffing through a switch. In active sniffing, the switched Ethernet does not transmit information to all the systems connected through LAN as it does in a hub-based network. 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 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 just monitors the packets sent by others. Active sniffing involves sending out multiple network probes to identify access points.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**



Attackers use sniffing tools to sniff packets and monitor network traffic on the target network. A scenario that describes how an attacker makes use of sniffers to hack a network follows, and is illustrated in the slide.

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.

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.

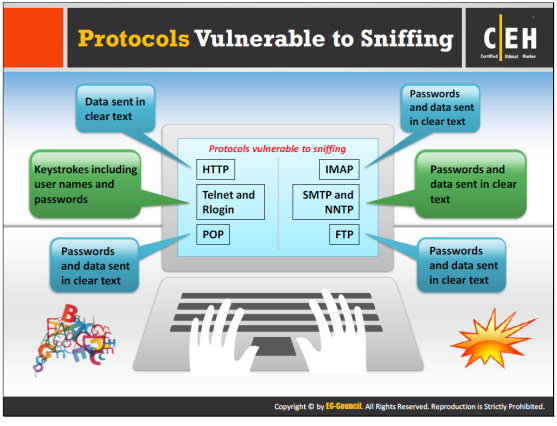
Step 3: By analyzing the network topology, the attacker identifies the victim's machine to target attacks.

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

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

Step 6: Now the attacker is able to 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, user names, credit card details, PINs, etc.

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



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 in to 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 it can be easy to sniff.

- **HTTP**

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

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

- **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 a mail from the workstation to the mailbox server via the Simple Mail Transfer Protocol (SMTP). Due to the protocol's weak security implementations, attackers can sniff the data flowing across a POP network in clear text.

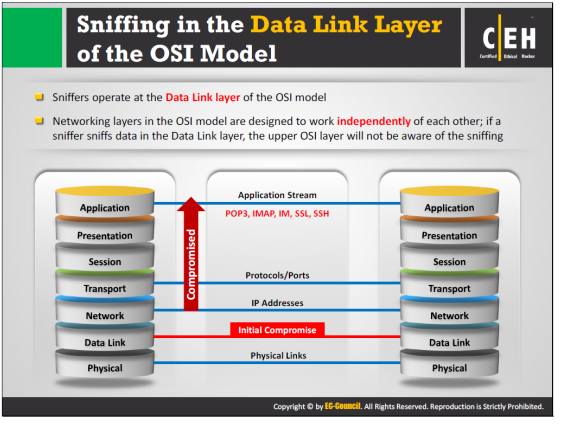
- **FTP**

  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 poor security, which allows attackers to obtain data and user credentials in clear text.

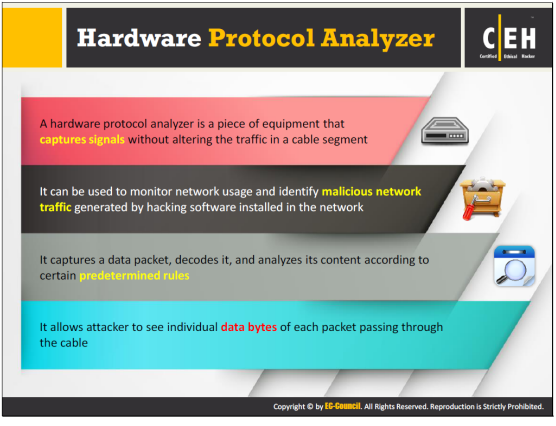
Ethical Hacking and Countermeasures Copyright © by **EC-Council**



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 can capture the packets from the Data Link layer.

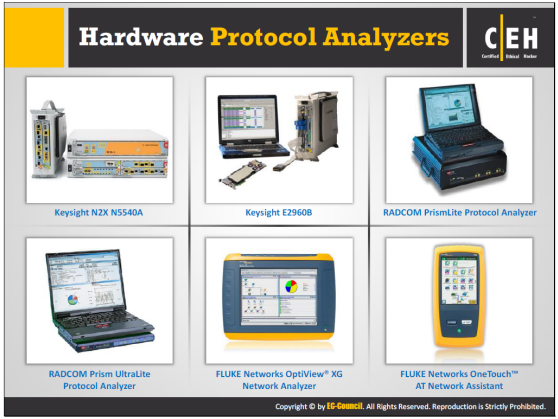
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



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 analysers 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.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**



Hardware protocol analyzers from different companies include:

Keysight N2X N5540A

Keysight N2X N5540A is a multi-port test system that verifies the performance of multi-service networks and devices. The Agilent N2X N5540A 2-slot Portable chassis provides a convenient platform for testing scenarios where portability or small size is a factor. Two different card types can be configured simultaneously, allowing for test scenarios that use a combination of port types.

Keysight E2960B

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 clear protocol viewing. The analyzer includes unique logic capabilities such as lane view, fast ASPM sync time, and trigger on ordered set.

RADCOM PrismLite Protocol Analyzer

PrismLite is designed for WAN, LAN, and ATM testing simultaneously. The Prismlite Protocol Analyzer family provides comprehensive monitoring capabilities enabling users to capture data, perform a sophisticated range of analyses, and gather statistics. The analysis processes can be performed both online and offline, with a wide range of user-defined displays, allowing the user to capture data in one time and place, and process it at any convenient time.

RADCOM Prism UltraLite Protocol Analyzer

Prism UltraLite analyzes and simulates network behavior and a wide range of communications protocols. It is a compact, portable protocol analyzer for WAN/ Fast LAN networks. Network managers and field service engineers use it to test application-specific configurations, from datacom protocols to a wide range of cellular protocols and a complete suite of VoIP protocols.

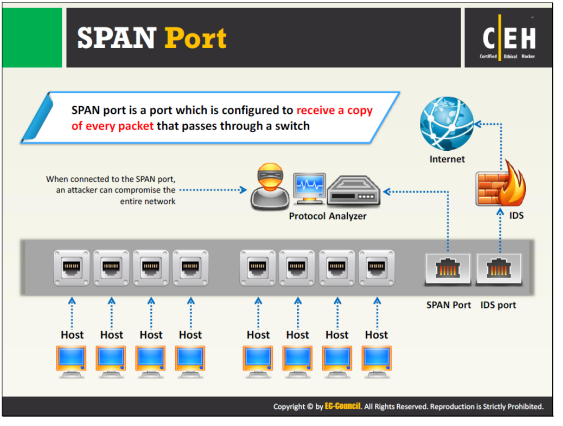
FLUKE Networks OptiView® XG Network Analyzer

OptiView® XG Network Analysis Tablet is a network analyzer and monitoring tool that automates root-cause analysis of wired and wireless network and application problems allowing the user to spend less time on troubleshooting and more time on other initiatives. The tool supports the deployment and troubleshooting of technologies like unified communications, virtualization, wireless, and 10 Gbps Ethernet.

FLUKE Networks OneTouch™ AT Network Assistant

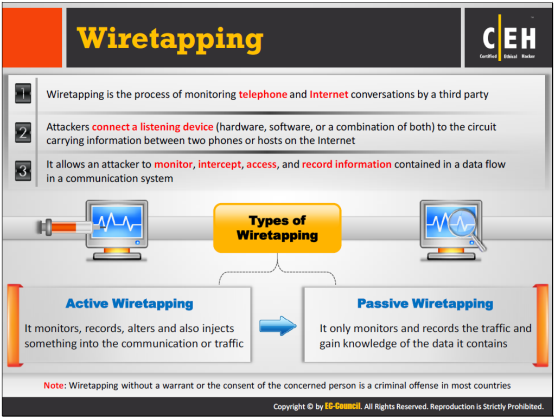
FLUKE Networks OneTouch™ AT Network Assistant performs both wired and Wi-Fi network analysis and discovery. It troubleshoots copper, fiber optic, and Wi-Fi network problems, from a client device to cloud-hosted applications. The tool troubleshoots persistent problems and validates network performance on-site in real-time. It also troubleshoots intermittent problems, identifies vulnerabilities by uploading results to the cloud for web-based performance trending, and performs root cause analysis.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**



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. It helps to analyze and debug data, identify errors, and investigate unauthorized network access on a network. When 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.

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



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.

- **Active Wiretapping**

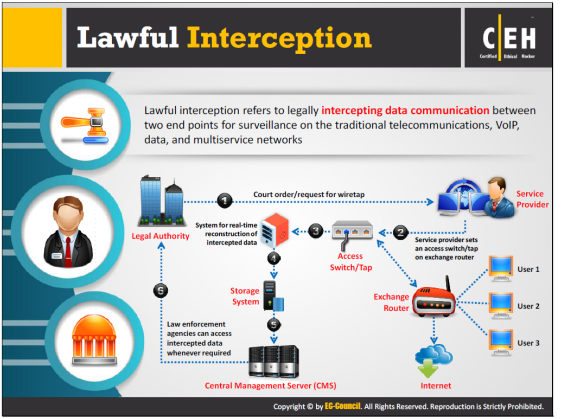
  In hacking terminology, active wiretapping is an MITM attack. This allows an attacker to monitor and record the traffic or data flow in a communication system. The attacker can also alter or inject data into the communication or traffic.

- **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.

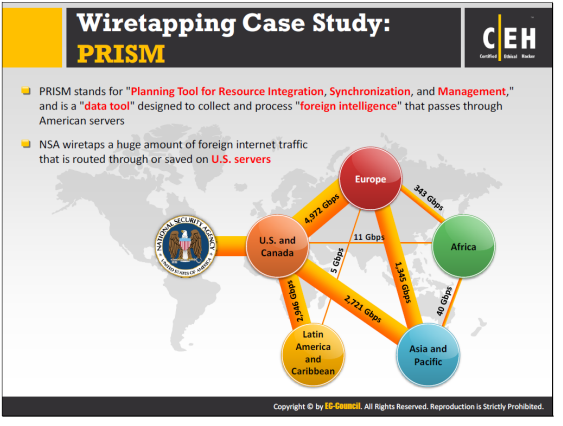
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



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 cyber-security-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. Law enforcement agencies (LEAs) perform such operations.

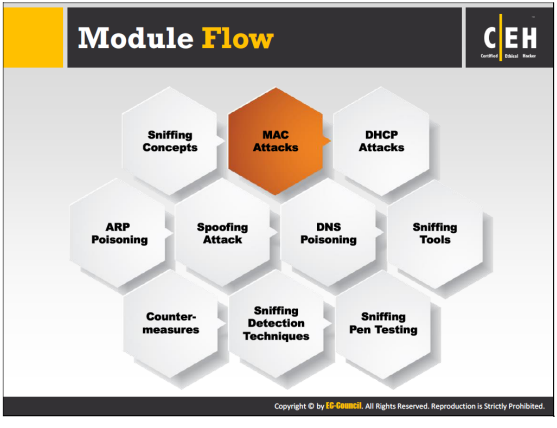
This type of interception is necessary only to monitor messages exchanged on suspicious channels in which the users are engaged in illegal activity. Countries around the world are making strides to standardize this type of procedure for interception.

The slide 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 reconstruct 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. Centralized Management Server (CMS) manages all the ED systems.



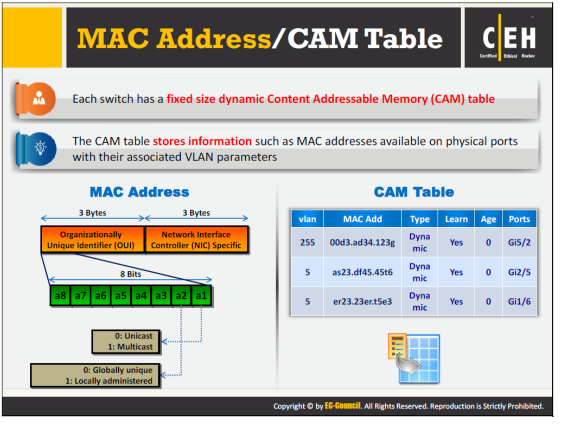
Planning Tool for Resource Integration, Synchronization, and Management (PRISM) is used by a surveillance program launched in 2007 by the National Security Agency (NSA). PRISM is a data tool to collect and process foreign intelligence from the huge amount of foreign internet traffic routed through or saved on U.S. servers. It traps communications such as E-mail, voice, video chats, file transfers, videos, photos, etc., based on demands made to companies such as Google Inc., Facebook, Skype, Apple etc. One of the operations performed by the NSA is to search for certain keywords related to terrorism, hacking, etc. If it finds a keyword in a conversation, it tracks the complete conversation.

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



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.

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



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 network.

A MAC address is useful 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.

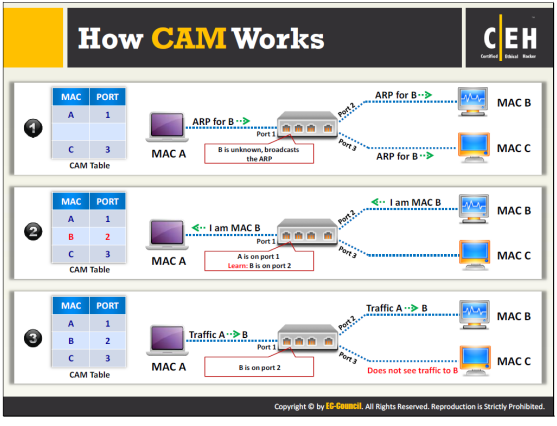
For example, consider the MAC address D4-BE-D9-14-C8-29. The first six digits, i.e., D4BED9 indicate the manufacturer (Dell, Inc.), while the next six digits 14C829 indicate the serial number of the adapter.

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, as in a hub-based network, the hub forwards the incoming traffic to all the machines in the network.

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

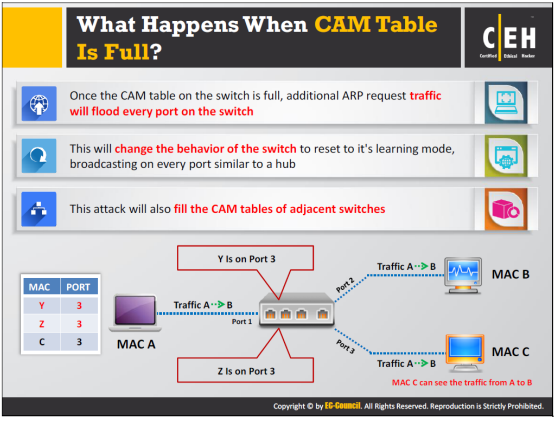


A CAM table refers to the dynamic form of content and works with the Ethernet switch. The Ethernet switch maintains the connections between the ports.

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, then the switch turns 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 is able to connect to the shared switch of the Ethernet segment can easily sniff network data.

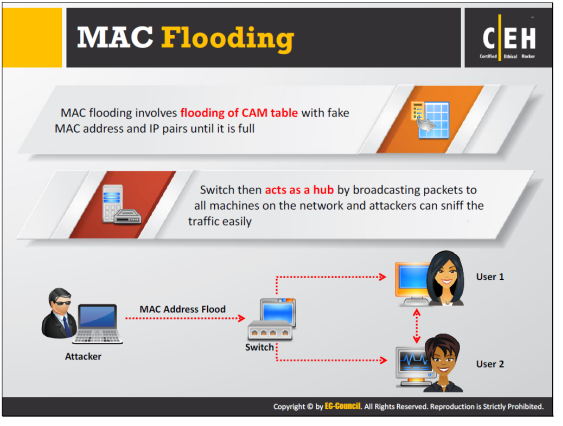
Refer the diagram in the slide for the working of CAM table. It shows three machines: Machine A, Machine B and Machine C; each holding MAC address A, B and C. The machine A holding the MAC address A wants to interact with Machine B.

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. 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. 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.



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. After this, 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, similar to a hub. The switch then works as a hub through which you an 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 slide illustrates how a CAM table can be flooded with fake MAC addresses to monitor the frames sent from victim host to another host without any CAM table entry.



MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. In a switched network, an Ethernet switch contains a CAM table that stores all the MAC addresses of devices connected in the network. 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 "**failopen mode**". In failopen mode, the switch starts behaving as 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, so that the machine would accept all the traffic entering it. This way, attackers can sniff the traffic easily and can steal sensitive information

Ethical Hacking and Countermeasures Copyright © by **EC-Council**

Mac Flooding Switches with macof

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

Command Prompt

```
macof -i eth1
18:b1:22:12:85:15 13:15:5a:6b:45:c4 0.0.0.0.25684 > 0.0.0.0.86254: S 2658741236:1235486715(0) win 512
12:a8:d8:15:4d:3b ab:4c:cd:5f:ad:ed 0.0.0.0.12387 > 0.0.0.0.78962: S 1238569742:782563145(0) win 512
13:3f:ab:14:25:95 66:ab:6d:4d:b2:85 0.0.0.0.45638 > 0.0.0.0.4568: S 123587152:456312589(0) win 512
a2:2f:85:12:ac:2f 12:85:2f:52:41:25 0.0.0.0.42358 > 0.0.0.0.35842: S 3256789512:3560742158(0) win 512
96:25:a3:5c:52:af 82:12:41:1d:ac:d6 0.0.0.0.45213 > 0.0.0.0.2358: S 3684125687:3256074125(0) win 512
a2:c2:b5:8c:6d:2a 5a:cc:f6:41:8d:df 0.0.0.0.12354 > 0.0.0.0.78521: S 1236542358:3698521475(0) win 512
55:42:ac:85:c5:96 a5:5f:ad:9d:12:aa 0.0.0.0.123 > 0.0.0.0.12369: S 8523695412:8523698742(0) win 512
a9:4d:4c:5a:5d:ad a4:ad:5f:4d:e9:ad 0.0.0.0.23685 > 0.0.0.0.45686: S 236854125:365145752(0) win 512
a3:e5:1a:25:2w:a3 25:35:a8:5d:af:fc 0.0.0.0.23685 > 0.0.0.0.85236: S 862357425:3698521456(0) win 512
```

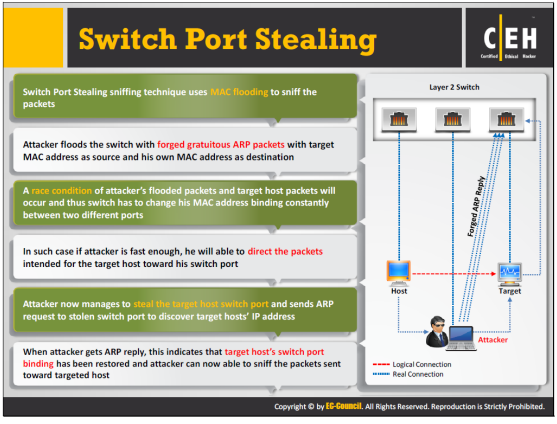
http://monkey.org

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

Macof is part of the Dsniff suite tool. It floods the local network with random MAC addresses, causing some switches to fail and open in repeating mode, facilitating sniffing. This tool floods the switch's CAM tables (131,000 per min) by sending forged MAC entries. When the MAC table fills up and the switch converts to hub-like operation, an attacker can monitor the data being broadcast.

Source: *http://monkey.org*

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



Assume 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 7.1: 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 7.2: MAC Table

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

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 7.3: ARP Cache Table

1. 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 7.4: Switch updated with a spoofed entry

2. The attacker's machine runs a sniffer that turns the machine's NIC adapter to promiscuous mode.
3. 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?)
4. The switch broadcasts this ARP request to all the machines in the network.
5. 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.
6. 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 7.5: ARP Cache updated with a spoofed entry

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

7. 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).

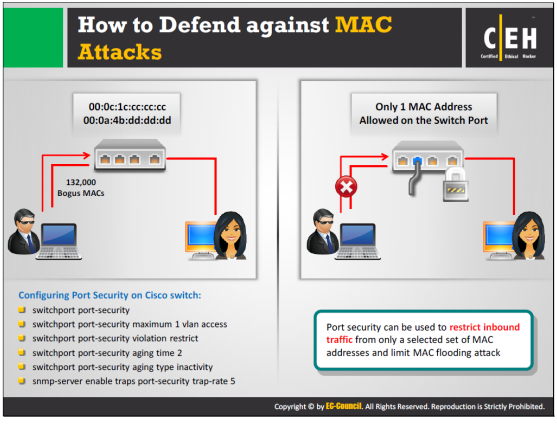
Vlan	MAC Address	Type	Learn	Age	Ports
255	Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	0	Port A
5	Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port B
5	Host C	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port C

TABLE 7.6: MAC Table updated with a spoofed entry

8. 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.

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



You can use the Cisco port security feature 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 doesn't match any of the identified secure MAC addresses

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

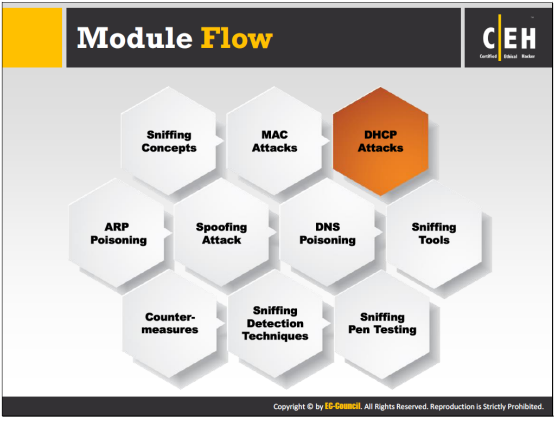
- You can configure all secure MAC addresses by using the switchport port-securing mac-address interface configuration command
- You can allow the port to dynamically configure secure MAC addresses with the MAC addresses of the connected devices
- You can configure a number of addresses and allow the rest to be dynamically configured.

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

On the left side of the slide, the attacker floods the switch CAM tables with fake MAC addresses and thus threatens security by turning a switch into a hub.

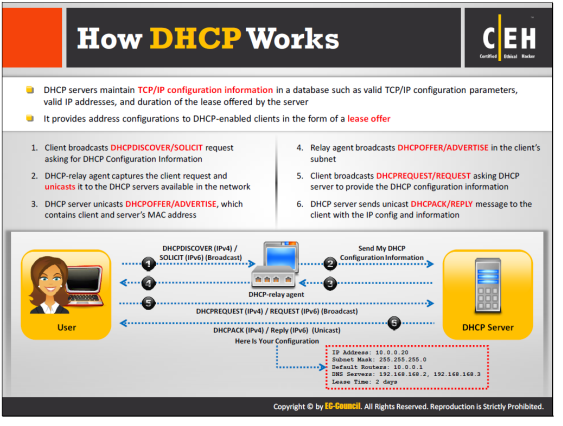
On the right side of the slide, the number of MAC addresses allowed on the switch port is limited to one; therefore, it recognizes MAC requests as flooding. Port security locks down the port and sends an SNMP trap.

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



This section discusses DHCP attacks. A DHCP attack is active sniffing 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.

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



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.

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

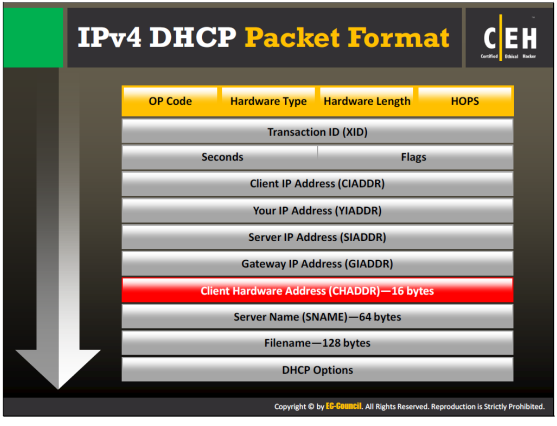
DHCP Request/Reply Messages

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

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

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.

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



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 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.

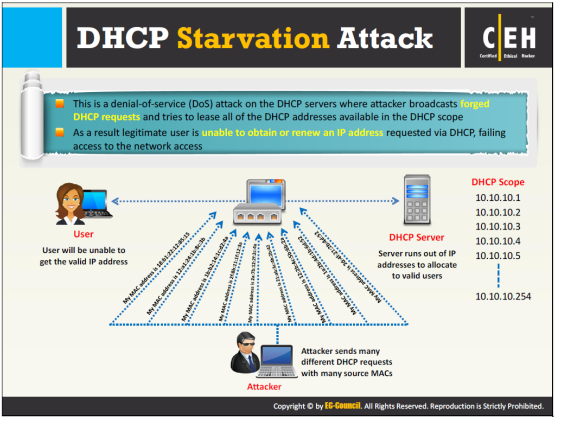
The following table details every field of the IPv4 DHCP message:

FIELD	OCTETS	DESCRIPTION
OP Code	1	This field contains message op code that represents the message type OP code “1” represents BOOTREQUEST and “2” represents BOOTREPLY
Hardware Address Type	1	Hardware address type defined at Internet Assigned Numbers Authority (IANA) (e.g., '1' = 10Mb Ethernet)
Hardware Address Length	1	Hardware address length in octets

Hops	1	In general, the 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 client began address acquisition or renewal process
Flags	2	Flags set by client. Example: If the client cannot receive unicast IP datagrams, then the broadcast flag is set
Client IP Address (CIADDR)	4	Used when the client has an IP 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 host name
File Name	128	Name of the file containing BOOTP client's boot image
DHCP Options	Variable	

TABLE 7.7: List of IPv4 DHCP Messages

Ethical Hacking and Countermeasures Copyright © by **EC-Council**



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**.

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

DHCP Starvation Attack Tools

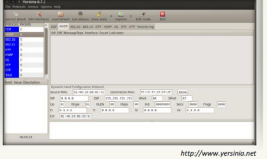
Dhcpstarv

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

http://dhcpstarv.sourceforge.net

Yersinia

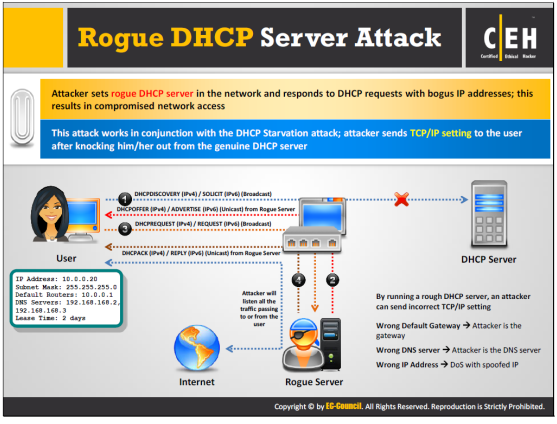
- Yersinia is a network tool designed to take advantage of some **weakeness** in different network protocols
- It pretends to be a solid framework for analyzing and testing the **deployed networks and systems**



http://www.yersinia.net

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

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



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.

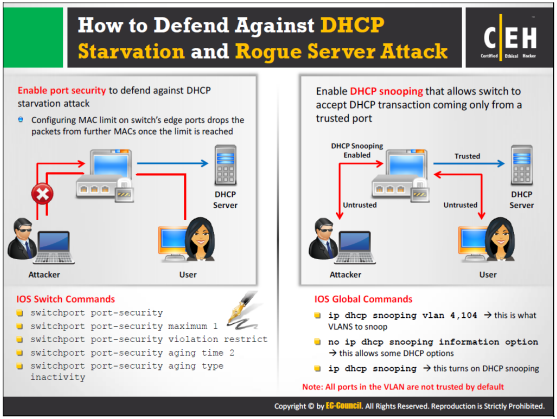
In a rogue DHCP server attack, an attacker will introduce a rogue server into the network. This rogue server has the ability to respond to clients' DHCP discovery requests. Though both the rogue and actual DHCP servers respond to the request, the client accepts the response that comes first. In a case 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 server 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 hard 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.

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



Defend Against DHCP Starvation

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 safeguards the server against a DHCP starvation attack.

IOS Switch Commands

Source: *http://www.cisco.com*

- **switchport port-security**

  switchport port-security command configures the switchport parameters to enable port security

- **switchport port-security maximum 1**

  switchport port-security maximum command configures the maximum number of secure MAC addresses for the port

  switchport port-security maximum 1 command configures the maximum number of secure MAC addresses for the port as 1

- **switchport port-security violation restrict**

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

switchport 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**

  switchport port-security aging time command configures the secure MAC address aging time on the port

  switchport port-security aging time 2 command sets the aging time as **2** minutes

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

  switchport port-security aging type command configures the secure MAC address aging type on the port

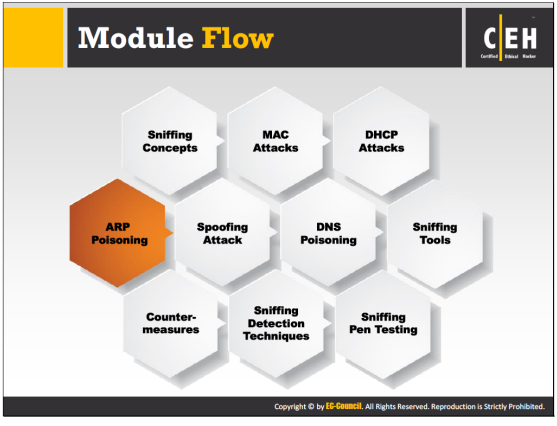
  switchport port-security aging type inactivity command sets the aging type as inactivity aging

Defend Against Rogue Server Attack

The DHCP snooping feature 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.

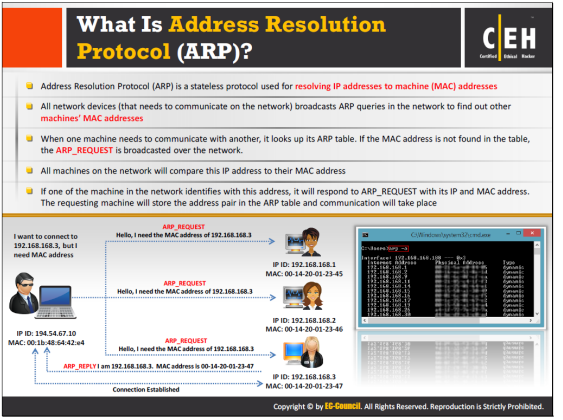
Note: All ports in the VLAN are untrusted by default.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**



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

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



Address Resolution Protocol (ARP) is a 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:

- 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 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 host names, IP, and MAC addresses are:

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

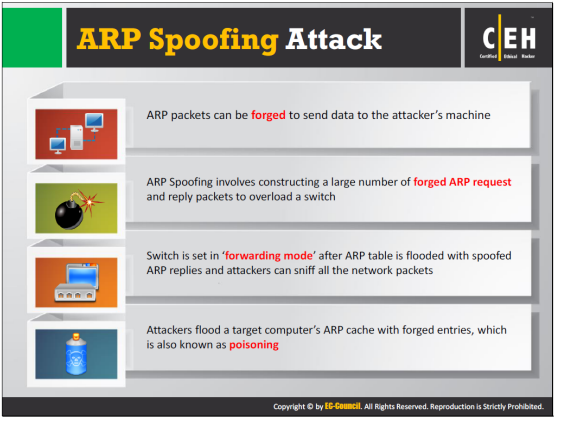
Before communicating with host B, host A first checks for a record of host B's MAC address in the ARP cache. If host A finds the record of a MAC address, it communicates directly with host B. Otherwise, it has to access host B's MAC address by using the ARP protocol.

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."

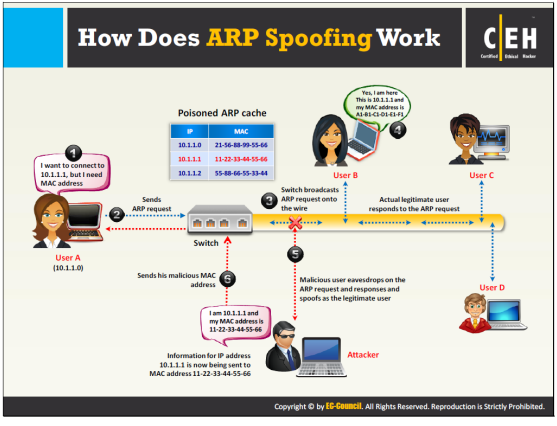
On receiving the ARP reply, host A updates its ARP cache table with host B's IP and MAC addresses. After establishing a connection between these two hosts, they communicate with each other.

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



ARP resolves IP addresses to the MAC (hardware) address of the interface to send data. If the machine sends an ARP request, it assumes that the ARP reply comes from the right machine. ARP provides no means to verify the authenticity of the responding device. Even systems that have not made an ARP request 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. ARP spoofing is an intermediary to perform attacks such as DoS, MITM, and Session Hijacking.

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



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, and 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 to the target destination.

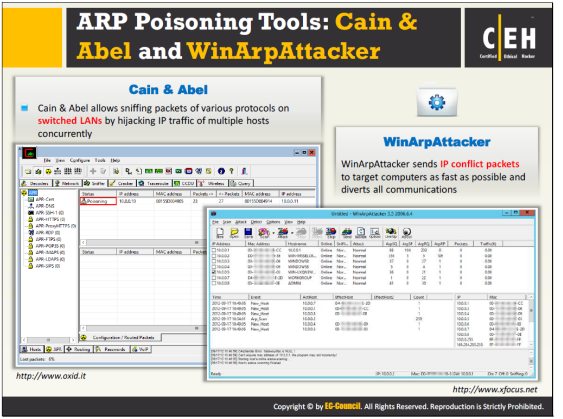
With the help of ARP poisoning, an attacker can use fake ARP messages to divert all communications between two machines so that all traffic redirects via the attacker's PC.

The threats of ARP poisoning include:

- **Packet Sniffing:** Sniffs traffic over a network or a part of 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 host name 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 the huge amount of traffic which is intended for different IP addresses

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



Cain & Abel

Source: *http://www.oxid.it*

Cain & Abel is a password recovery tool for Windows. It recovers passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols. The program does not exploit any software vulnerabilities or bugs that are not easy to fix. It covers some security aspects or weaknesses present in a protocol's standards, authentication methods, and caching mechanisms.

Features:

- APR (ARP Poison Routing) which sniffing on switched LANs and MITM attacks
- Sniffer analyzes encrypted protocols such as SSH-1 and HTTPS, and includes filters to capture credentials from a wide range of authentication mechanisms
- Routing protocols authentication monitors and routes extractors, dictionary, and brute-force crackers for all common hashing algorithms, and for several specific authentications, password or hash calculators, cryptanalysis attacks, password decoders, and some utilities related to network and system security.

WinArpAttacker

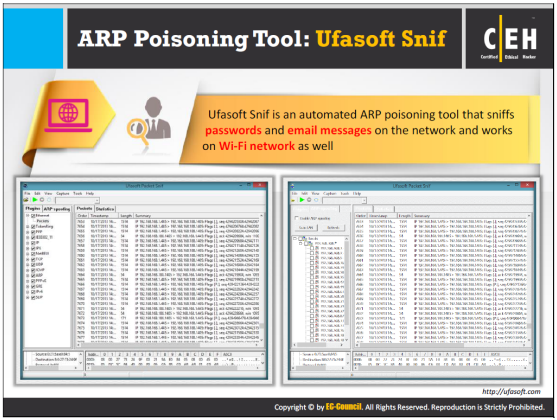
Source: *http://www.xfocus.net*

WinArpAttacker scans, attacks, detects, and protects computers on a LAN. It sends IP conflict packets to target computers as fast as possible and diverts all communications.

It can perform the following attacking actions:

- Arp Flooding
- BanGateway
- IPConflict
- SniffGateway
- SniffHosts
- SniffLan

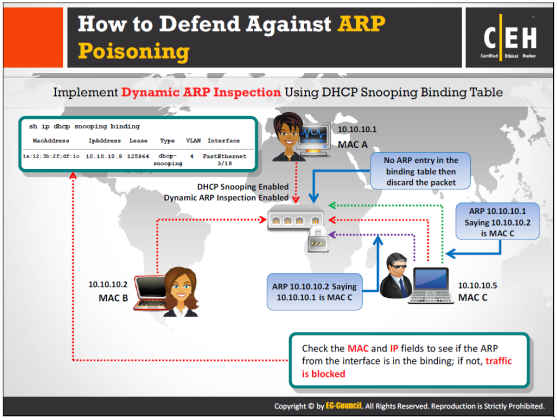
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Ufasoft Snif is an automated ARP poisoning tool that sniffs passwords and email 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 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 the user can select specific machines to ARP-spoof in the GUI version.

Source: *http://ufasoft.com*

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

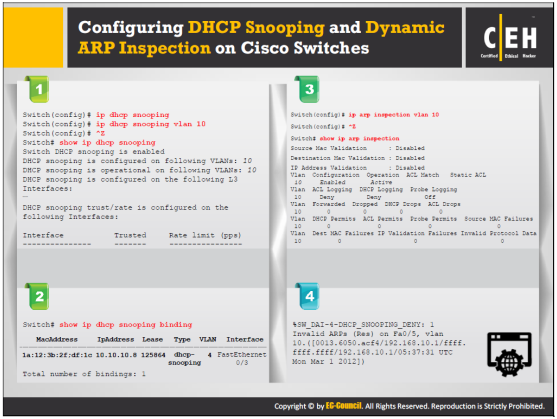


Implementation of Dynamic ARP Inspection (DAI) prevents poisoning attacks. DAI is a security feature that validates ARP packets in a network. When DAI activates on a VLAN, all ports on the VLAN are considered to be untrusted by default. DAI validates the ARP packets using a DHCP snooping binding table. 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 prior to enabling DAI. Otherwise, establishing a connection among 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 discards the ARP packet. It eliminates the risk of MITM attacks. DAI ensures the relay of only valid ARP requests and responses.

In a network, if the host systems hold static IP addresses, then DHCP snooping is not possible, or other switches in the network do not run dynamic ARP inspection. In such situations, 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 drops 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.



As discussed, DHCP snooping must be enabled prior to enabling 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, enable DHCP snooping both globally and per access VLAN. To enable DHCP snooping, execute the following commands:

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ^Z
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 10
DHCP snooping is operational on following VLANs: 10
DHCP snooping is configured on the following L3
Interfaces:
...

DHCP snooping trust/rate is configured on the
following Interfaces:

Interface            Trusted      Rate limit (pps)
---------------      -------      ----------------
```

FIGURE 7.2: Configuring DHCP Snooping on a Switch

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

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 two, apply the `ip dhcp snooping trust` command to the layer two interfaces in order to designate uplink interfaces as trusted interfaces. This informs the switch that DHCP responses 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, 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
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**

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 an MITM attack. The switch with dynamic ARP inspection enabled inspects these reply packets by comparing them with the DHCP snooping table. The switch then tries to find an entry for the source IP address 192.168.10.1 on port FastEthernet0/5. If 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
Mar 1 2012])
```

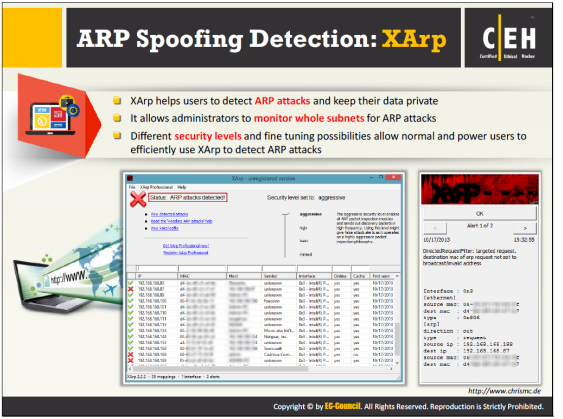
If the discarding of packets starts, then the drop count begins to increase. You can see this increase in the drop count in the dynamic ARP inspection output. To see the output, execute the command `show ip arp inspection`

```
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
```


Ethical Hacking and Countermeasures Copyright © by **EC-Council**

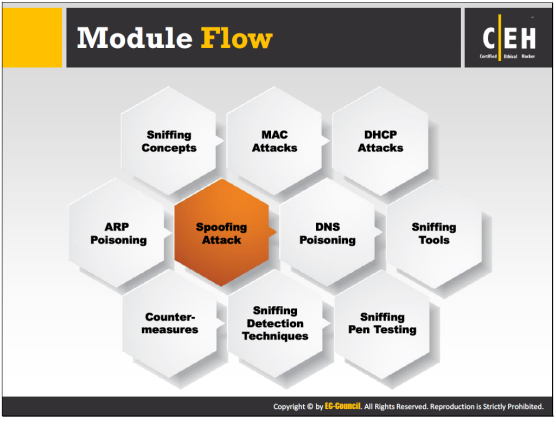
```
----  ------------ ---------     --------- ----------
10    Enabled        Active
Vlan  ACL Logging   DHCP Logging  Probe Logging
----  -----------   ------------  -------------
10        Deny           Deny          Off
Vlan  Forwarded     Dropped       DHCP Drops  ACL Drops
----  ---------     -------       ----------  ---------
10        30               5           5         0
Vlan  DHCP Permits ACL Permits Probe Permits Source MAC Failures
----  ------------ ----------- ------------- -------------------
10        30              0           0                0
Vlan  Dest MAC Failures IP Validation Failures Invalid Protocol Data
----  ----------------- ---------------------- ---------------------
10            0                   0                     0
```


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



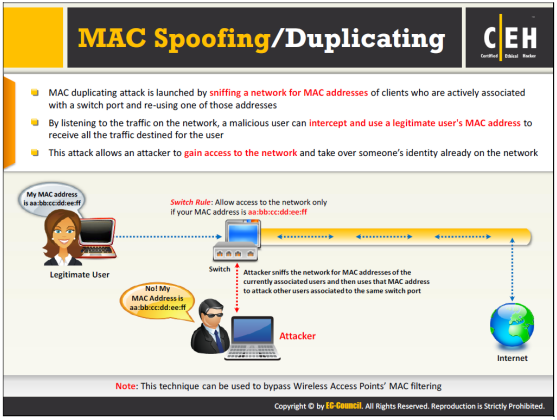
XArp is a security application that detects ARP-based attacks. It detects critical network attacks that firewalls cannot cover. It uses advanced techniques to detect ARP attacks like ARP spoofing. The detection mechanism relies on two techniques: inspection modules and discoverers. Inspection modules look at ARP packets and check their correctness and validity in respect to databases they 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.

Source: *http://www.chrismc.de*



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.

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



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.

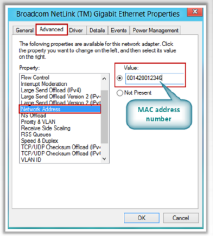
The diagram in slide shows how an attacker performs a MAC spoofing/duplicating attack.

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

MAC Spoofing Technique: Windows

In Windows 8 OS

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



1. Go to **Right bottom** of the screen → **Settings** → **Control Panel** → **Network and Internet** → **Networking and Sharing Center**
2. Click on the **Ethernet** and then click on the **Properties** in the Ethernet Status window
3. In the Ethernet properties window click on the **Configure** button and then on the **Advanced** tab
4. Under the "**Property:**" section, browse for **Network Address** and click on it
5. On the right side, under "**Value:**", type in the new MAC address you would like to assign and click **OK**

   Note: Enter the MAC address number without "-" in between
6. Type "**ipconfig/all**" or "**net config rdr**" in command prompt to verify the changes
7. If the changes are visible then **reboot** the system, else try method 2 (change MAC address in the registry)

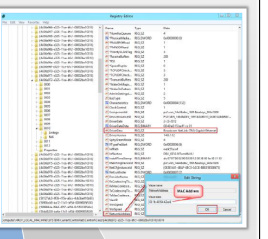
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Spoofing Technique: Windows (Cont'd)

Method 2: Steps to change MAC address in Registry

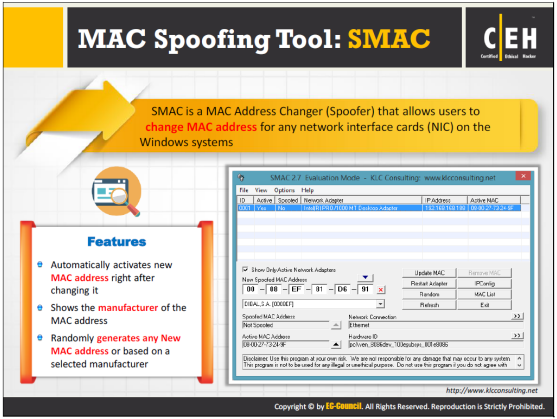
- Go to **Start** → **Run**, type **regedt32** to start registry editor

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



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

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



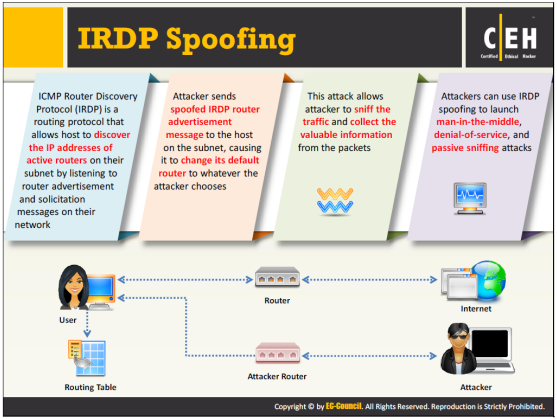
SMAC is a MAC address changer that changes MAC addresses for any Virtual PC, VMs, or Windows systems. It does not rely on the hardware address on the NIC, but changes only software-based MAC addresses. It changes only software-based MAC addresses, but not the hardware burned-in MAC addresses. The new MAC addresses sustain reboots. It features MAC address lookup. It displays either all or only active network adapters, and randomly generates new MAC addresses or those based on a selected manufacturer. It also restores the original MAC address by removing the spoofed MAC address.

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

Features:

- Automatically activates new MAC address right after changing it
- Shows the manufacturer of the MAC address
- Randomly generates any New MAC address or based on a selected manufacturer
- Allows a user to pre-load MAC addresses list and can choose the new MAC address from a list

Source: *http://www.klcconsulting.net*



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, 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.

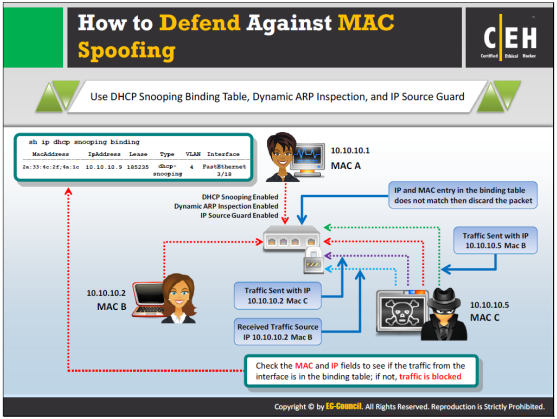
An attacker can use this to send spoofed router advertisement messages so that all the data packets travel through the attacker's system. Thus, the attacker can sniff the traffic and collect valuable information from the data packets. Attackers can use IRDP spoofing to launch MITM, DoS, and passive sniffing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

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



Performing security assessments is the main 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 here. Finding those loopholes is a minor task. The major, critical 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 MAC spoofing. Many MAC spoofing countermeasures are can be applied to specific network architectures and loopholes. Apply the appropriate countermeasures to your network.

To detect MAC spoofing, it is important 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 specifying an action to take if a port security violation occurs.

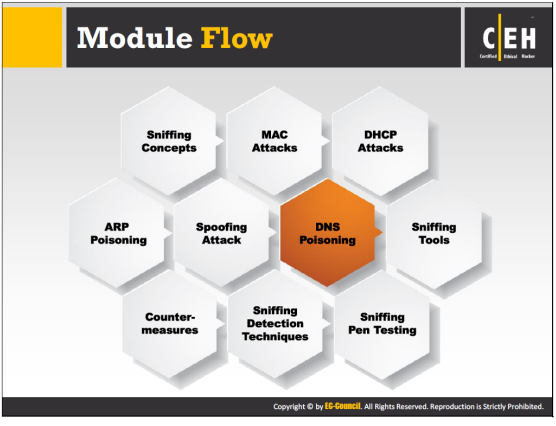
You can also implement the following techniques to defend against MAC address spoofing attacks:

- **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.

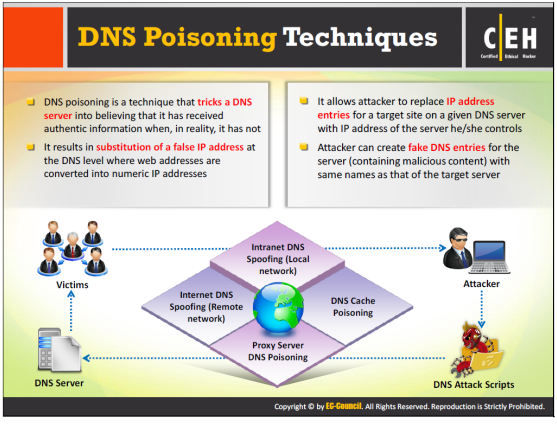
- **Dynamic ARP Inspection:** The system checks the IP to MAC address binding for each ARP packet in a network. While performing a Dynamic ARP inspection, the system drops invalid IP to MAC address bindings.
- **IP Source Guard:** IP Source Guard is a security feature in switches that restricts the IP 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 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.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**



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.

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



DNS is the protocol that translates a domain name (e.g., 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 poisoning, also called DNS spoofing, 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.

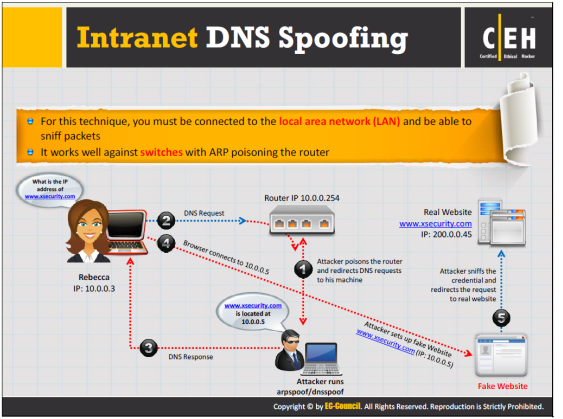
When the victim tries to access a website, the attacker manipulates the entries in the DNS table so that the victim's system redirects the URL to the attacker's server. The attacker changes the IP address of the website to the IP address of a malicious server. Thus, the victim connects to the attacker's server without realizing it. Once the victim connects to the attacker's server, the attacker can compromise the victim's system and steal data.

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

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

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

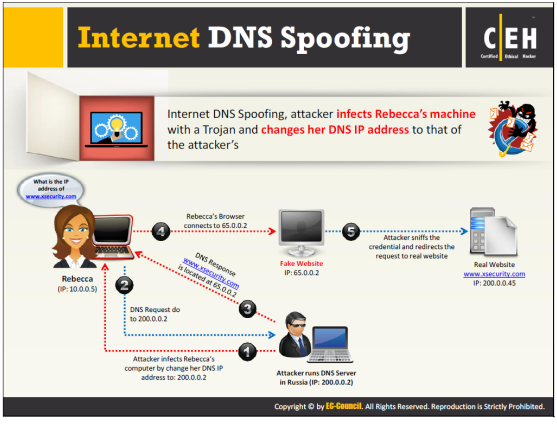


An attacker can perform an intranet DNS spoofing attack on a switched LAN with the help of the ARP poisoning technique. To perform this attack, the attacker must be connected to the LAN and be able to sniff the traffic or packets.

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.

The diagram in the slide describes how an attacker performs Intranet DNS spoofing.

In the diagram, 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.

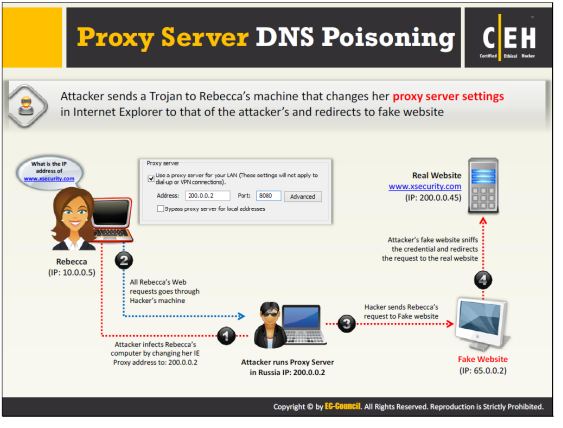


Internet DNS poisoning is also known as remote DNS poisoning. Attackers can perform DNS spoofing attacks on a single or multiple victims anywhere in the world. In order to perform this attack, the attacker sets up a rouge DNS server with a static IP address.

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. Now the attacker can easily sniff the victim's confidential information.

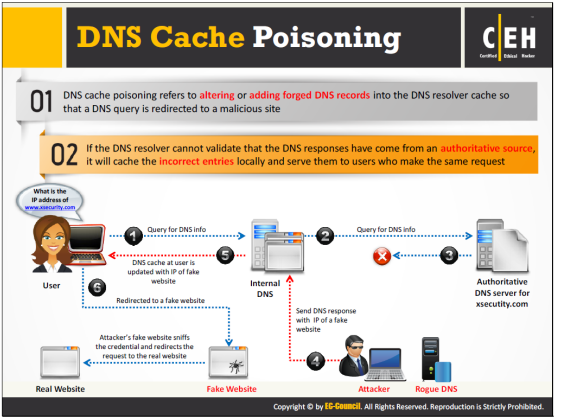
The slide illustrates an attacker performs Internet DNS spoofing.

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



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.

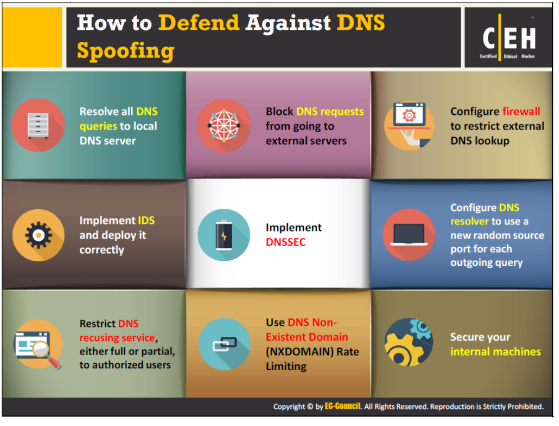
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



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, and then the resolver sends its respective IP address quickly. 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. 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.

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

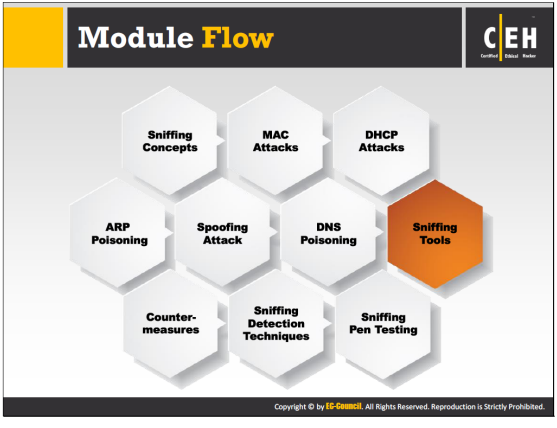


Major DNS implementations have reported attacks using DNS spoofing, and this vulnerability still affects a large number of organizations. This is because of lack of information when performing DNS queries, which allows attackers to spoof DNS responses. You have seen how an attacker carries out different types of DNS spoofing attacks. Let us see 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
- Use static ARP and IP table
- Use SSH encryption
- Use sniffing detection tools
- Do not open suspicious files
- Always use trusted proxy sites
- Audit the DNS server regularly to remove vulnerabilities

Ethical Hacking and Countermeasures Copyright © by **EC-Council**



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 make use for sniffing.

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

Sniffing Tool: Wireshark

CEH Certified Ethical Hacker

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

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

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

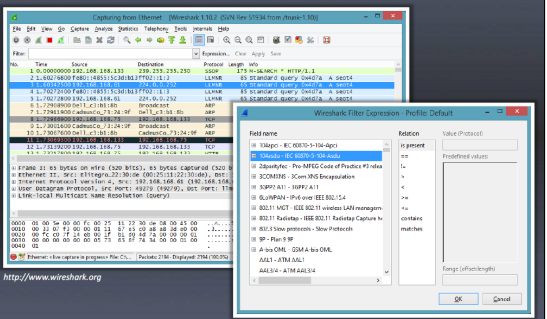
04 Captured files can be programmatically edited via **command-line**

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

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

Sniffing Tool: Wireshark (Cont'd)

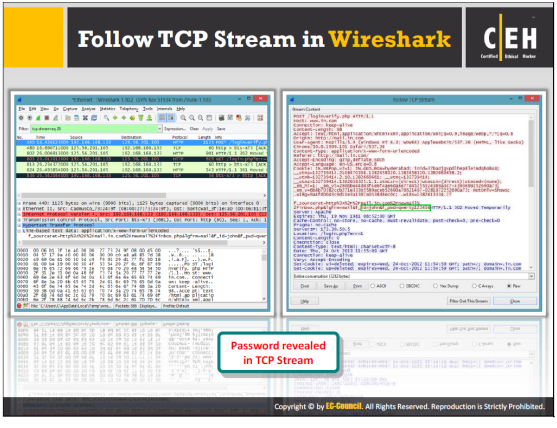
CEH Certified Ethical Hacker



http://www.wireshark.org

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

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

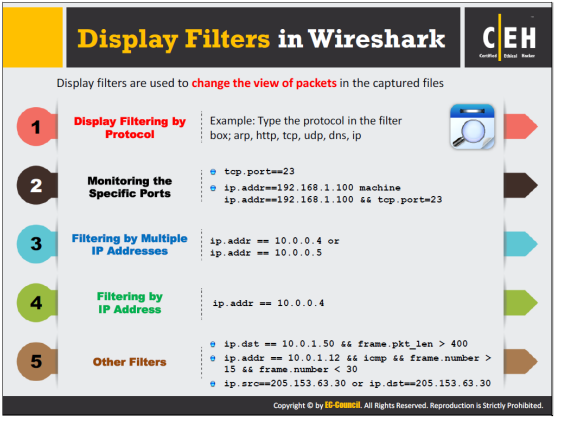


Wireshark displays data from the TCP port with a feature known as "**Follow tcp stream**". The tool sees TCP data in the same way as that of the application layer. Use this tool to find passwords in a Telnet session or make sense of a data stream.

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 stream 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.

Source: *http://www.wireshark.org*

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



Wireshark features display filters that filter traffic on the target network by protocol type, IP address, port, etc. To set 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.

Source: *http://wiki.Wireshark.com*

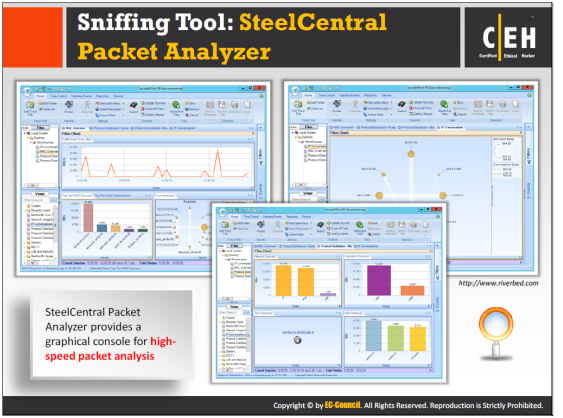
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Wireshark Filters

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

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

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

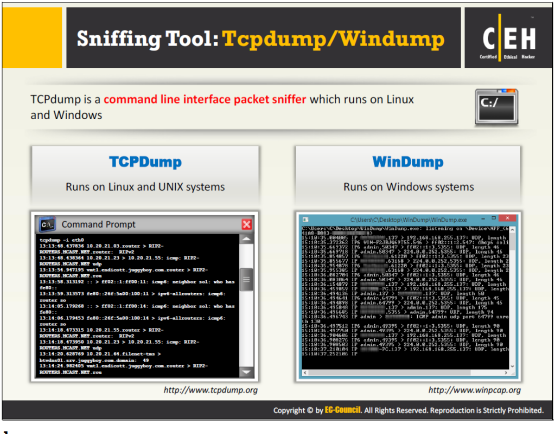


SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. This tool comes integrated with Riverbed AirPcap adapters to analyze and troubleshoot 802.11 wireless networks. As it captures terabytes of packet data traversing the network, this tool reads that traffic and displays 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

Source: *http://www.riverbed.com*



Tcpdump

Source: *http://www.tcpdump.org*

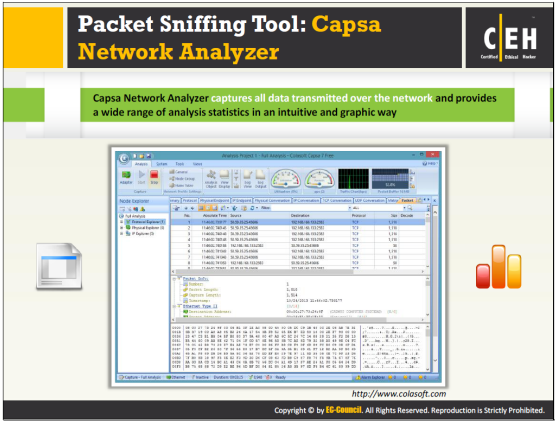
Tcpdump is a command-line packet analyzer. This tool can intercept and display TCP/IP and other packets transmitted or received over a network. It runs on Linux and other UNIX-like operating systems.

WinDump

Source: *http://www.winpcap.org*

WinDump is the Windows version of tcpdump. It can watch, diagnose, and save network traffic to disk according to various complex rules. It has almost the same functionality as that of tcpdump except that it runs on Windows systems. It captures network traffic using the WinPcap library and drivers. This tool supports 802.11b/g wireless capture and troubleshooting through the Riverbed AirPcap adapter.

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



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

Features:

- Real-time capture and save data transmitted over local networks, including wired networks and 802.11a/b/g/n wireless networks
- Identify and analyze more than 500 network protocols, as well as network applications based on the protocols
- Monitor network bandwidth and usage by capturing data packets transmitted over the network and providing summary and decoding information about these packets
- View network statistics at a single glance, allowing easy capture and interpretation of network utilization data
- Monitor Internet, email, and instant messaging traffic, helping keep employee productivity to a maximum
- Diagnose and pinpoint network problems in seconds by detecting and locating suspicious hosts

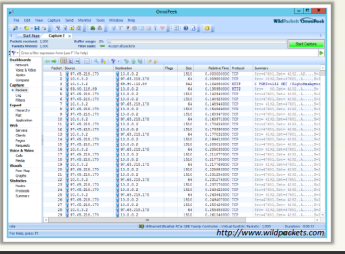
- Map out the details, including traffic, IP address, and MAC, of each host on the network, allowing for easy identification of each host and the traffic that passes through each
- Visualize the entire network in an ellipse that shows the connections and traffic between each host

Source: *http://www.colasoft.com*

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

Network Packet Analyzer: OmniPeek Network Analyzer

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

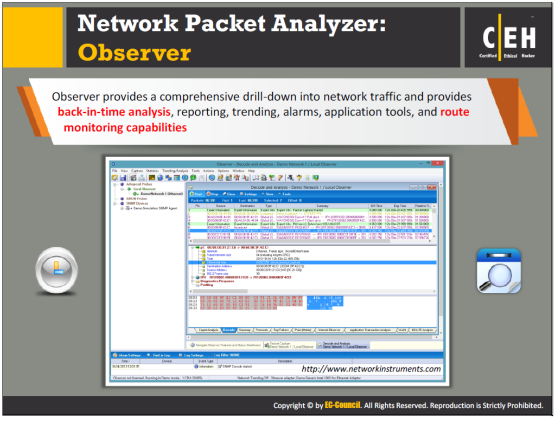


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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 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.

Source: *http://www.wildpackets.com*

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



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

Source: *http://www.netinst.com*

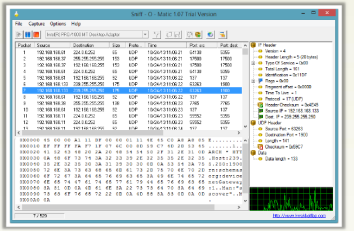
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network Packet Analyzer: Sniff-O-Matic

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

Features

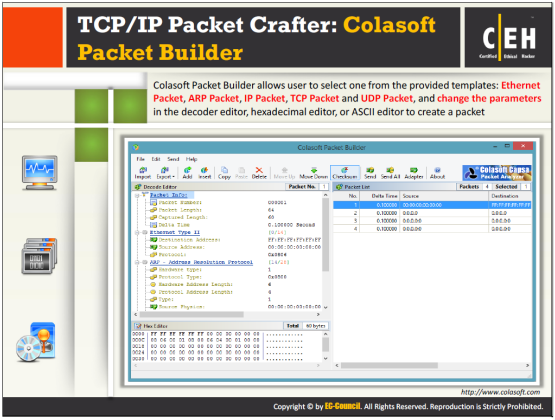
- Capture IP packets on your LAN without packet loss
- Monitor network activity in real time
- Filters to show only the packets you want
- Realtime checksum calculation
- Save and load captured packets
- Traffic charts with filter info



http://www.kwokkeflap.com

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

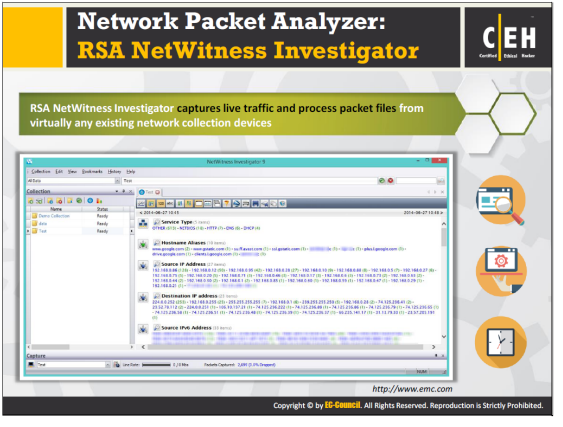
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Colasoft Packet Builder is a network packet crafter, packet generator, and packet editor tool. Attackers can use this tool to create custom network packets or create malicious network packets to carry out an attack on a target network. This tool can pen test a user's network for vulnerabilities to attacks by creating custom packets. The decoding editor of this tool can edit specific protocol field values in the network packets. Any of the templates of Ethernet Packet, ARP Packet, IP Packet, TCP Packet, and UDP Packet can create custom packets.

Source: *http://www.colasoft.com*

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



RSA NetWitness Investigator is the primary interactive analysis application of the NetWitness AppSuite. This network packet analyzer provides in-depth context and content of network sessions in real-time threat analysis and performs unprecedented free-form contextual analysis of raw network data for complete situational awareness.

Features:

- Real-time patented analytics of OSI Layers 2-7
- Effectively analyze data starting from application layer entities such as users, email, files etc.
- Content of the starting points
- Captures network traffic in real-time from any wired or wireless interface and many more

Source: http://www.emc.com

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

Many other tools can monitor network traffic and capture and analyze packet data.

Ace Password Sniffer

Source: *http://www.effetech.com*

Ace Password Sniffer is a password recovery utility that captures passwords through http, ftp, SMTP, pop3, and telnet. Network administrators can use it to capture passwords of other users. Ace Password Sniffer supports password monitoring through FTP, POP3, HTTP, SMTP, and Telnet, including some web mail passwords. Ace Password Sniffer works passively and does not generate any network traffic. Therefore, it is very hard for others to detect this tool. When connected to a network through a switch, the sniffer can run on the gateway or proxy server, which can monitor all network traffic. This can recover network passwords and monitor password abuse.

IPgrab

Source: *http://ipgrab.sourceforge.net*

IPgrab is a packet sniffing tool, based on the Berkeley packet capture library, that prints complete data-link, network, and transport layer header information for all captured packets.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**

Big-Mother

Source: *http://www.tupsoft.com*

Big Mother is an eavesdropping program that uses a switch sniffer to capture and analyze communication traffic over a network.

EtherDetect Packet Sniffer

Source: *http://www.etherdetect.com*

EtherDetect Packet Sniffer can capture full packets, organized by TCP connections or UDP threads; passively monitor a network, with no need to install program on target PCs; and view packets in Hex format and syntax highlighting viewer.

dsniff

Source: *http://monkey.org*

dsniff is a collection of tools for network auditing and penetration testing. It passively monitors a network for data like passwords, e-mail, files, etc. Tools like arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker. sshmitm and webmitm implement active MITM attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.

EffeTech HTTP Sniffer

Source: *http://www.effetech.com*

EffeTech HTTP Sniffer is an HTTP packet sniffer, protocol analyzer and file reassembly software application that runs on Windows. The sniffer captures IP packets containing HTTP protocol, rebuilds the HTTP sessions, and reassembles files sent through HTTP protocol. Its smart real-time analyzer enables on-the-fly content viewing while allowing an attacker to capture, analyze, parse and decode HTTP protocol.

ntopng

Source: *http://www.ntop.org*

ntopng is a network traffic probe that shows network usage. ntopng is a portable tool that can run on UNIX, MacOSX, and on Win32. ntopng users use a web browser to navigate through ntop (that acts as a web server) traffic information and get a dump of the network status.

Ettercap

Source: *http://ettercap.sourceforge.net*

Ettercap is a comprehensive suite for MITM attacks. It features sniffing of live connections, content filtering and so on. It supports active and passive dissection of many protocols and includes features for network and host analysis.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**

SmartSniff

Source: *http://www.nirsoft.net*

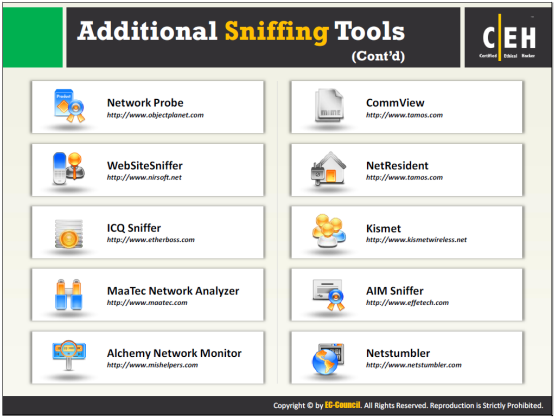
SmartSniff is a network monitoring utility that can capture TCP/IP packets that pass through a network adapter, and can view the captured data as sequence of conversations between clients and servers. Smartsniff displays the TCP/IP conversations in ASCII mode (for text-based protocols, like HTTP, SMTP, POP3 and FTP.) or as a hex dump (for non-text base protocols, like DNS).

EtherApe

Source: *http://etherape.sourceforge.net*

EtherApe is a graphical network monitor/ packet sniffer for UNIX. It can filter traffic and can read packets from a file as well as live from the network.

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



Other sniffing tools include:

Network Probe

Source: *http://www.objectplanet.com*

Network Probe is a network monitor and protocol analyzer that monitors network traffic in real-time, and can find the sources of any network slow-downs in a matter of seconds.

WebSiteSniffer

Source: *http://www.nirsoft.net*

WebSiteSniffer is a packet sniffer tool that captures all Web site files downloaded by a Web browser, and stores them on a hard drive. WebSiteSniffer can choose which type of Web site files to capture: HTML, Text, XML, CSS, Video/Audio, Image, or Flash files, as well as Scripts.

ICQ Sniffer

Source: *http://www.etherboss.com*

EtherBoss Monitor is a network utility to capture and log ICQ chat from computers within the same LAN. It supports messaging through ICQ server with the format of plain text, RTF, or HTML. All intercepted messages are organized and displayed. It provides a feature-rich report system to export captured ICQ conversations as HTML files for later analysis and reference.

MaaTec Network Analyzer

Source: *http://www.maatec.com*

The MaaTec Network Analyzer can capture, save, and analyze network traffic on a LAN or a DSL internet connection. It can be used for network troubleshooting, to analyze an existing network infrastructure, or for long-term network monitoring.

Alchemy Network Monitor

Source: *http://www.mishelpers.com*

Alchemy Network Monitor is a tool that monitors servers or network devices and notifies when a problem occurs. Compatible with any type of server, it monitors servers using a variety of protocols and services, including ICMP ping, NT event log, HTTP(s) and FTP URLs, disk space control, NT service state monitoring, Oracle Server, Microsoft SQL Server and virtually any SQL-compatible database server monitoring, SMTP, POP3, IMAP, NNTP and TELNET protocols, as well as some others.

CommView

Source: *http://www.tamos.com*

CommView is a network monitor and analyzer that presents a full picture of the traffic flowing through a PC or LAN segment. This application captures every packet on the wire to display important information such as a list of packets and network connections, vital statistics, protocol distribution charts, etc. It can examine, save, filter, import and export captured packets, view protocol decodes down to the lowest layer with full analysis of over 70 protocols.

NetResident

Source: *http://www.tamos.com*

NetResident is a network content analysis application that monitors, stores, and reconstructs a wide range of network events and activities, such as e-mail messages, Web pages, downloaded files, instant messages, and VoIP conversations. NetResident uses advanced monitoring technology to capture the data on the network, saves the data to a database, reconstructs it, and displays the content in an easy-to-understand format.

Kismet

Source: *http://www.kismetwireless.net*

Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card that supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plugins, which allow sniffing other media such as DECT. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of non-beaconing networks via data traffic.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**

AIM Sniffer

Source: *http://www.effetech.com*

AIM Sniffer is a network utility to capture and log AIM (AOL Instant Messenger) chat from computers within the same LAN. It supports not only messaging through AIM server but also direct connection messaging. All intercepted messages are well organized by AIM user with buddies and shown instantly on the main window. It provides rich-features report system to export captured AIM conversations as HTML files for later analyzing and reference.

Netstumbler

Source: *http://www.netstumbler.com*

NetStumbler is a tool for Windows that detects Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g.

IE HTTP Analyzer

Source: *http://www.ieinspector.com*

HTTP Analyzer is a sniffer or viewer that monitors and inspects HTTP/HTTPS traffic in real-time. It can trace and display a wide range of information, including header, content, cookies, query strings, post data, request and response stream, and redirection URLs. It has a request builder that enables the user to handcraft a HTTP/HTTPS Request, and capture HTTP traffic. It also provides cache information and session clearing, as well as HTTP status code information and several filtering options.

York

Source: *http://thesz.diecru.eu*

York logs source, destination [fqdn or ip address], protocol and packet size of all network traffic on a network. The network card will be set to promiscuous mode. York captures HTTP, FTP, POP3, SMTP, SMB, VNC, and AIM passwords/hash and HTTP cookies like 'GX'; and logs them as l0phtcrack files. It captures and stores transmitted HTTP and FTP files. It displays captured pictures in a slideshow or in full screen.

PacketMon

Source: *http://www.analogx.com*

AnalogX PacketMon can capture IP packets that pass through a network interface— whether they originated from the machine with PacketMon or a completely different machine on the network. After receiving the packet, the built-in viewer displays the header as well as the contents, and can even export the results to a standard comma-delimited file. PacketMon has a rule system that can filter the packets it captures.

NADetector

Source: *http://www.nsauditor.com*

NADetector monitors and analyzes network traffic and displays statistical information pertaining to each IP address pair and protocol, helping network administrators and users troubleshoot network problems. NADetector can collect statistical information about network

Ethical Hacking and Countermeasures Copyright © by **EC-Council**

traffic that passes through network adapters and displays incoming, outgoing and summary traffic statistics. This information is useful, especially for understanding the different IP addresses and data amounts involved with a given network utilizing task.

Microsoft Message Analyzer

Source: *http://www.microsoft.com*

Microsoft Message Analyzer is a tool for capturing, displaying, and analyzing protocol messaging traffic and other system messages. Message Analyzer can also import, aggregate, and analyze data from log and trace files. It is the successor to Microsoft Network Monitor 3.4 and a key component in the Protocol Engineering Framework (PEF) created by Microsoft for the improvement of protocol design, development, documentation, testing, and support. Message Analyzer can capture data live or load archived message collections from multiple data sources simultaneously.

NetworkMiner

Source: *http://www.netresec.com*

NetworkMiner is a Network Forensic Analysis Tool (NFAT) for Windows (but also works in Linux/Mac OS X/FreeBSD). NetworkMiner acts as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can also parse PCAP files for off-line analysis, to regenerate/reassemble transmitted files and certificates from PCAP files.

PRTG Network Monitor

Source: *http://www.paessler.com*

PRTG Network Monitor is a network monitoring application for Windows. It is suitable for small, medium, and large networks and capable of LAN, WAN, WLAN, and VPN monitoring. It can also monitor physical or virtual web, mail, and file servers, Linux systems, Windows clients, routers, and many more. PRTG monitors network availability and bandwidth usage, as well as various other network parameters such as quality of service, memory load, and CPU usages. It provides system administrators with live readings and periodical usage trends to optimize the efficiency, layout, and setup of leased lines, routers, firewalls, servers, and other network components.

Network Security Toolkit

Source: *http://www.networksecuritytoolkit.org*

Network Security Toolkit (NST) is a bootable ISO image (Live DVD) based on Fedora 20, providing easy access to best-of-breed open source network security applications, and should run on most Windows platforms. An advanced Web User Interface (WUI) performs system/network administration, navigation, automation, network monitoring, host geo-location, network analysis and configuration of many network and security applications found within the NST distribution.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**

IP Traffic Spy

Source: *http://www.networkdls.com*

IP Traffic Spy can watch the data transmitted back and forth from one computer and others on the internet or network. To accomplish this, the tool reads the raw TCP/IP packets processed by a network adapter and displays them in a user-friendly fashion.

KSniffer

Source: *http://ksniffer.sourceforge.net*

KSniffer is a network statistics collector. It can watch all network traffic over any network interfaces connected to the host machine.

KSniffer supports most TCP/IP protocols, (TCP, IP, UDP, ICMP, ARP, and RARP, as well as minimal IPX). KSniffer collects the # of packets, and # of bytes for each protocol. It also displays the activity in terms of kbits/sec, kbytes/sec and packets/sec. KSniffer can also watch port specific traffic for monitoring things like http, ftp, telnet, etc. traffic.

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

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:

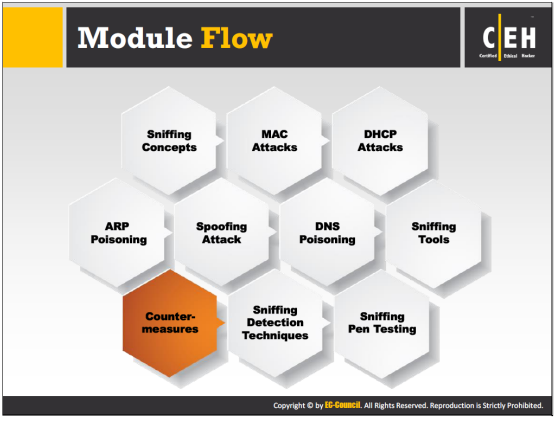
- Parallel packet captures for various type of connections such as Wi-Fi, 3G, LTE, etc.
- Real-time packet information
- Flexible packet filtering
- Active network operations
- Supports Wireshark format such as cap, pcap, etc.,

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.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**



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.

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

How to Defend Against Sniffing

01	Restrict the physical access to the network media to ensure that a packet sniffer cannot be installed
02	Use encryption to protect confidential information
03	Permanently add the MAC address of the gateway to the ARP cache
04	Use static IP addresses and static 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 in order 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

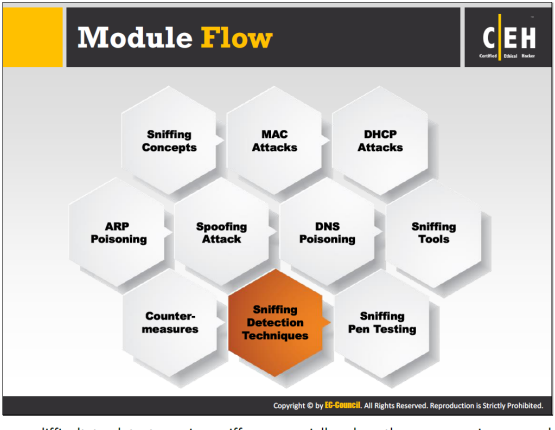
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against Sniffing (Cont'd)

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

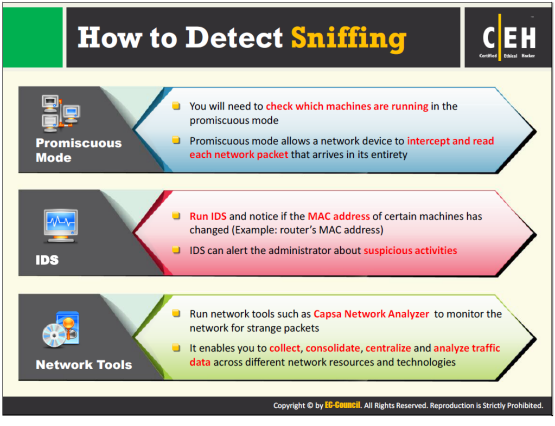
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

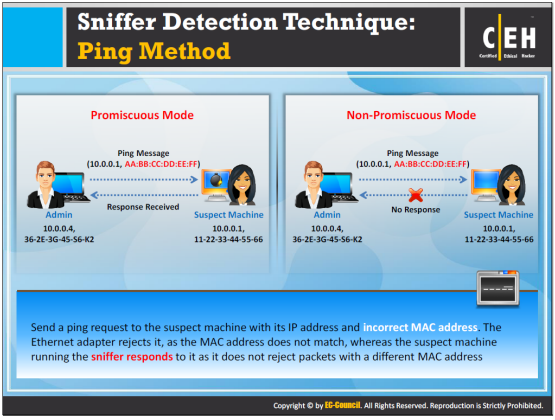


It is very difficult to detect passive sniffers, especially when they are running on a shared Ethernet. This section discusses some detection techniques.

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



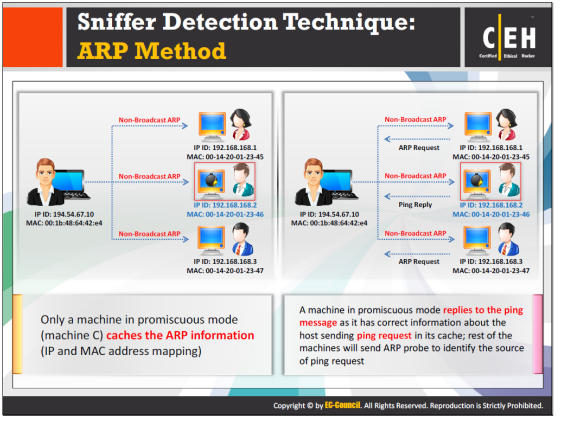
It is not easy to detect a sniffer on a network as it only captures data and runs in promiscuous mode. The sniffer leaves no trace, since it does not transmit data. To find sniffers, check for systems that are running in promiscuous mode, which is a NIC mode that allows all packets (traffic) to pass, 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 available to detect promiscuous mode, such as **Nmap**. IDS can detect sniffing activities on a network. It notifies or alerts when a suspicious activity such as sniffing or MAC spoofing occurs. Network tools such as **HP Performance Insight** monitor 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.



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.

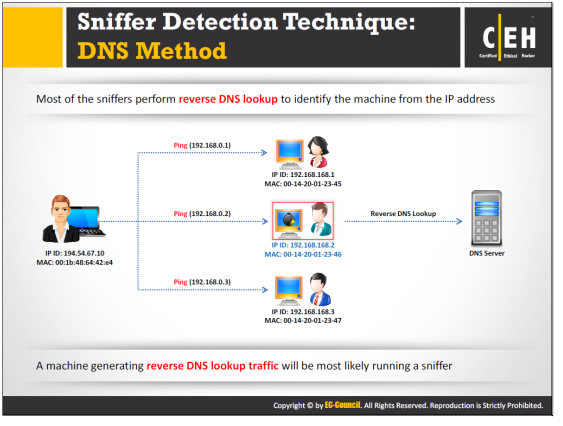
Just send a ping request to the suspect machine with its IP address and incorrect MAC address. The Ethernet adapter rejects it, as the MAC address does not match, whereas the suspect machine running the sniffer responds to it, as it does not reject packets with a different MAC address. Thus, this response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

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



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 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 that MAC address (cached earlier) will be able to respond to your broadcast ping request. This will detect the node on which the sniffer is running.

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



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. The computers on this network are in promiscuous mode.

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.

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

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

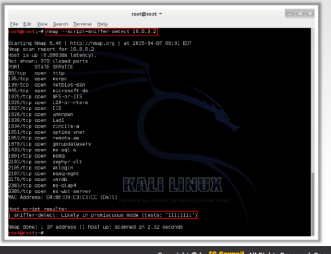
Source: *http://www.microsoft.com*

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

Promiscuous Detection Tool: Nmap

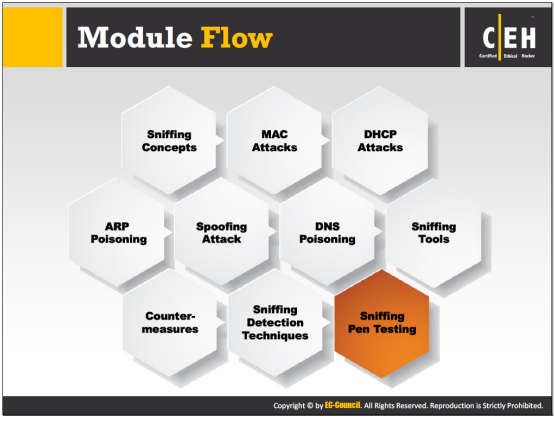
- Nmap's NSE script allows you to check if a target on a local Ethernet has its network card in **promiscuous** mode
- **Command to detect NIC in promiscuous mode:**

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



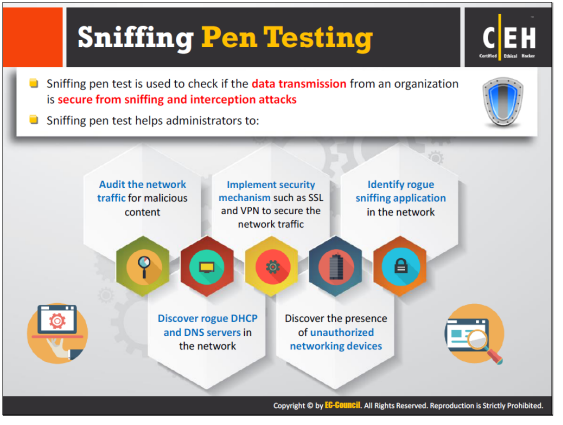
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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



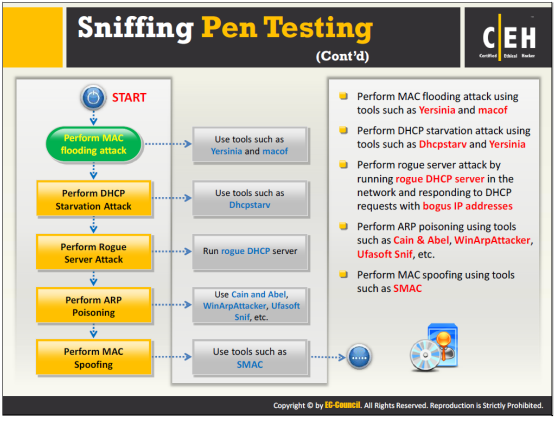
Conducting a security assessment to identify vulnerabilities can protect a network from sniffing attacks. This section describes the pen testing process that simulates sniffing attacks. It involves series of steps during which the pen tester uses different techniques and tools to sniff the target network.

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



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 test the target network for sniffing. Pen testing will determine whether the network is vulnerable to any type of sniffing or interception attacks.

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



A pen test simulates sniffing attacks that an attacker might conduct. 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 failopen mode, in which the switch broadcasts data to all ports rather than just to the port intended to receive the data. If this happens, then attackers have the ability to sniff network traffic. Use tools such as **Yersinia** and **macof**.

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, then attackers have the chance to sniff network traffic or DHCP requests of clients by building a rogue DHCP server. Test for DHCP starvation attacks using tools such as **Dhcpstarv** and **Gobbler**.

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.

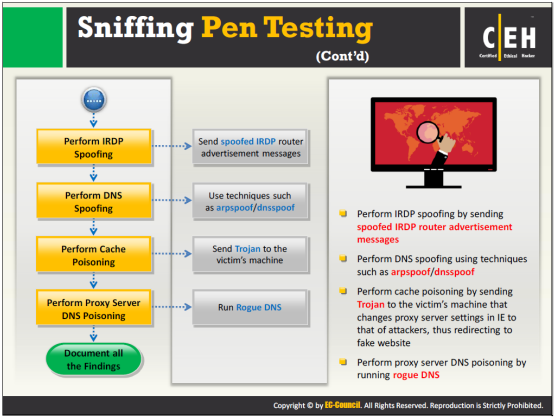
Step 4: Perform ARP Poisoning

Try to compromise the ARP table and change the MAC address so that the IP address points to another machine. If this is successful, then 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 **Cain & Abel**, **WinArpAttacker**, and **Ufasoft snif**.

Step 5: Perform MAC Spoofing

Try to spoof the MAC address on the network card. Try to change the factory-assigned MAC address of a networked device. If this succeeds, then an attacker could bypass 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. Use tools such as **SMAC**.

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



Step 6: Perform IRDP Spoofing

Perform IRDP spoofing by sending spoofed IRDP router advertisement messages to the host on the subnet. Check whether the router changes its default router to the malicious route suggested by the advertisement messages. 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 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 to the victim 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 sets a rogue DNS as the primary DNS entry in the proxy server system. Then the attacker lures the victim to use the attacker's proxy server. If the victim uses the

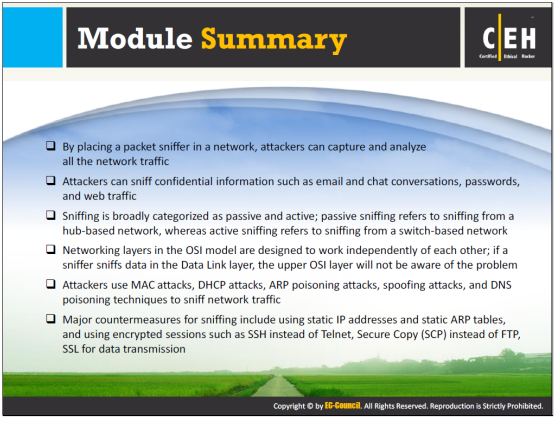
Ethical Hacking and Countermeasures Copyright © by **EC-Council**

attacker's proxy server, the attacker can sniff all the traffic between victim and the website being visited.

Step 10: Document all the Findings

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

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



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

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