C|EH Certified Ethical Hacker

EC-Council

MODULE 08

SNIFFING

EC-COUNCIL OFFICIAL CURRICULA

This page is intentionally left blank.

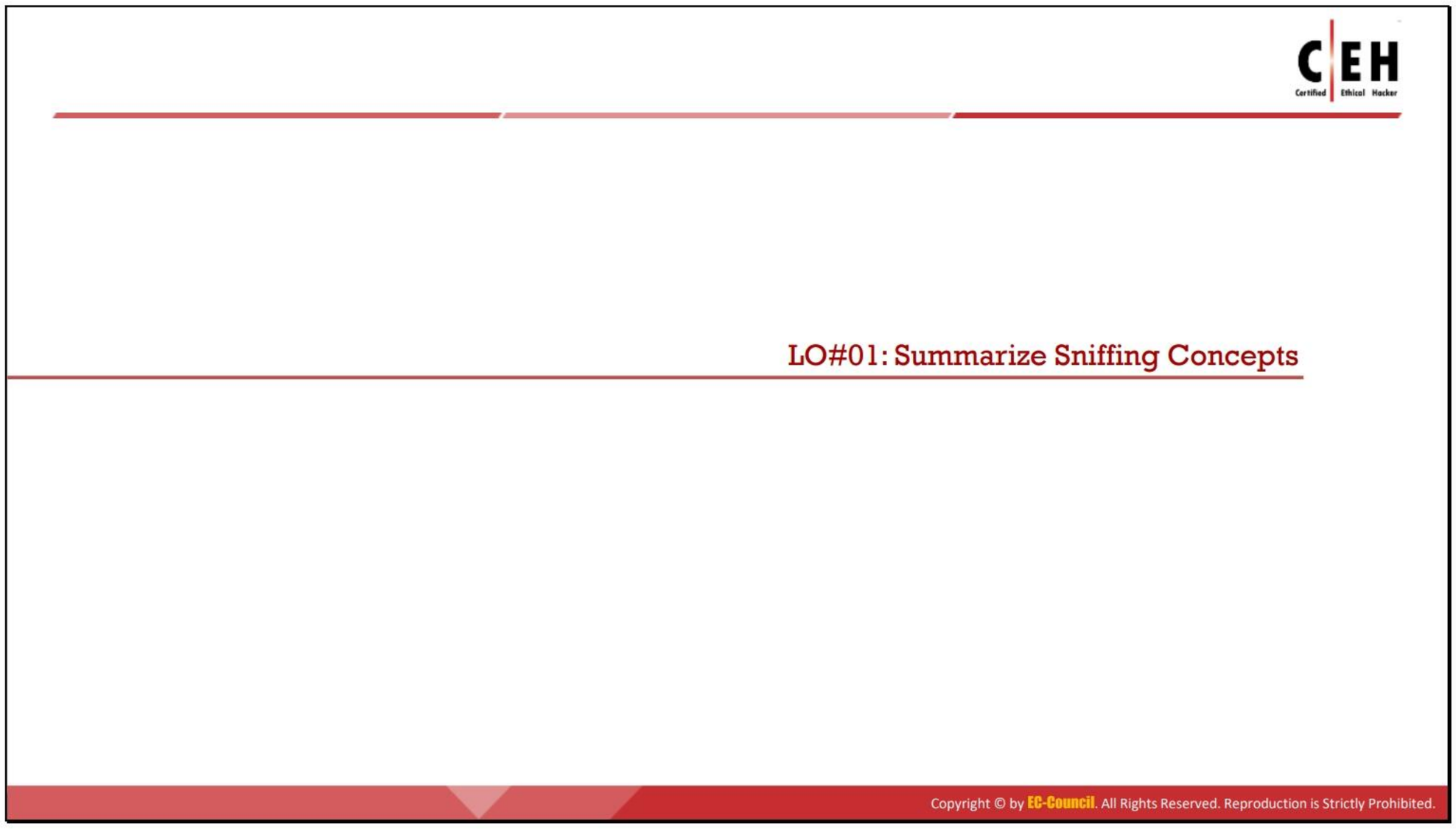
Learning Objectives

This module starts with an overview of sniffing concepts and provides an insight into MAC, DHCP, ARP, MAC spoofing, and DNS poisoning attacks. Later, the module discusses various sniffing tools, countermeasures, and detection techniques.

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

- Describe sniffing concepts
- Explain different MAC attacks
- Explain different DHCP attacks
- Describe ARP poisoning
- Explain different spoofing attacks
- Describe DNS poisoning
- Apply a defense mechanism against various sniffing techniques
- Use different sniffing tools
- Apply various sniffing countermeasures
- Apply various techniques to detect sniffing attacks

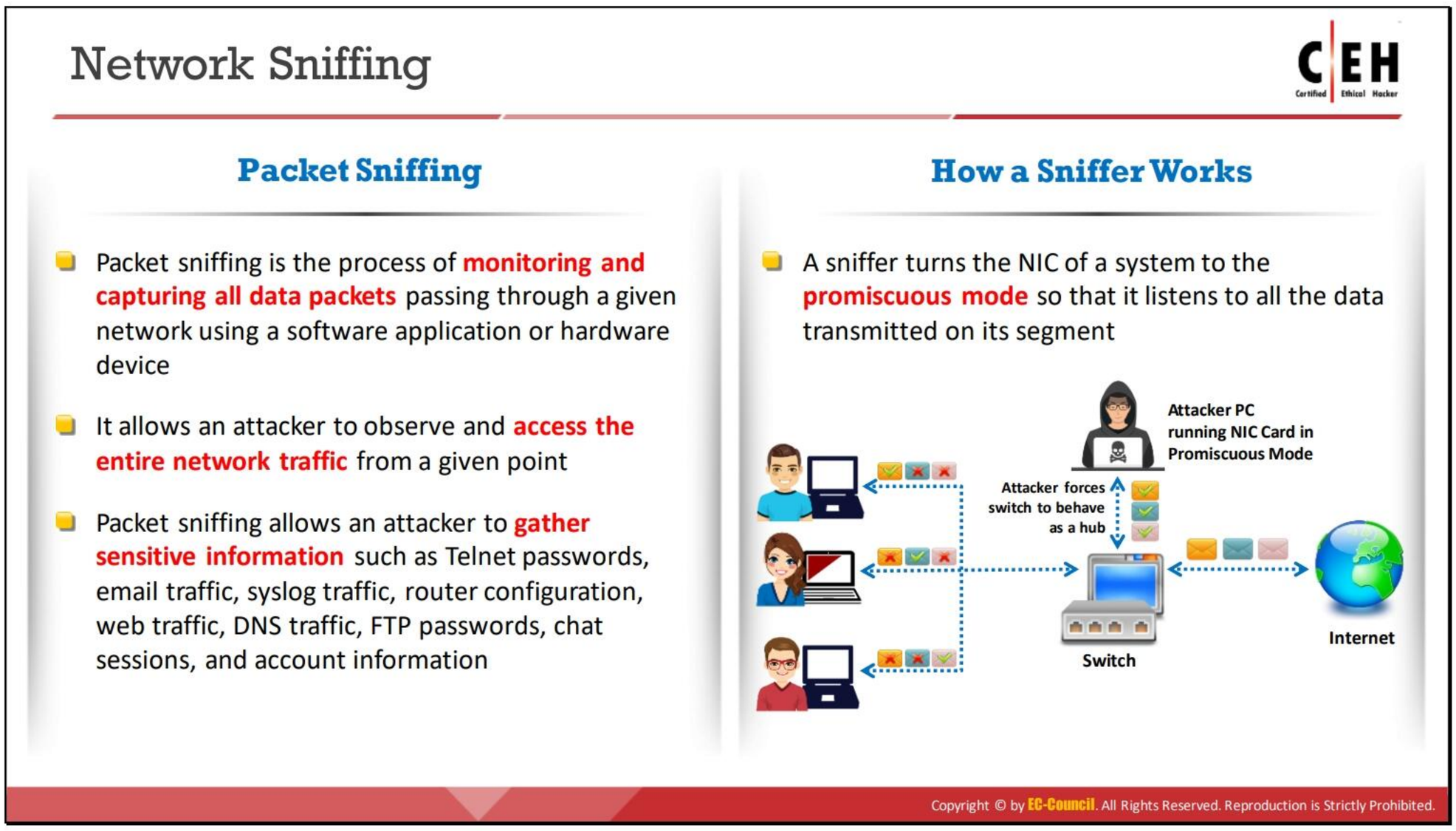
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Concepts

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

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



Network Sniffing

Packet sniffing is the process of monitoring and capturing all data packets passing through a given network using a software application or hardware device. Sniffing is straightforward in hub-based networks, as the traffic on a segment passes through all the hosts associated with that segment. However, most networks today work on switches. A switch is an advanced computer networking device. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network.

An attacker needs to manipulate the functionality of the switch to see all the traffic passing through it. A packet sniffing program (also known as a sniffer) can capture data packets only from within a given subnet, which means that it cannot sniff packets from another network. Often, any laptop can plug into a network and gain access to it. Many enterprises' switch ports are open. A packet sniffer placed on a network in promiscuous mode can therefore capture and analyze all 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 monitor all traffic.

Although most networks today employ switch technology, packet sniffing is still useful. This is because installing remote sniffing programs on network components with heavy traffic flows such as servers and routers is relatively easy. It allows an attacker to observe and access the entire network traffic from one point. Packet sniffers can capture data packets containing sensitive information such as passwords, account information, syslog traffic, router configuration, DNS traffic, email traffic, web traffic, chat sessions, and FTP passwords. This

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

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

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

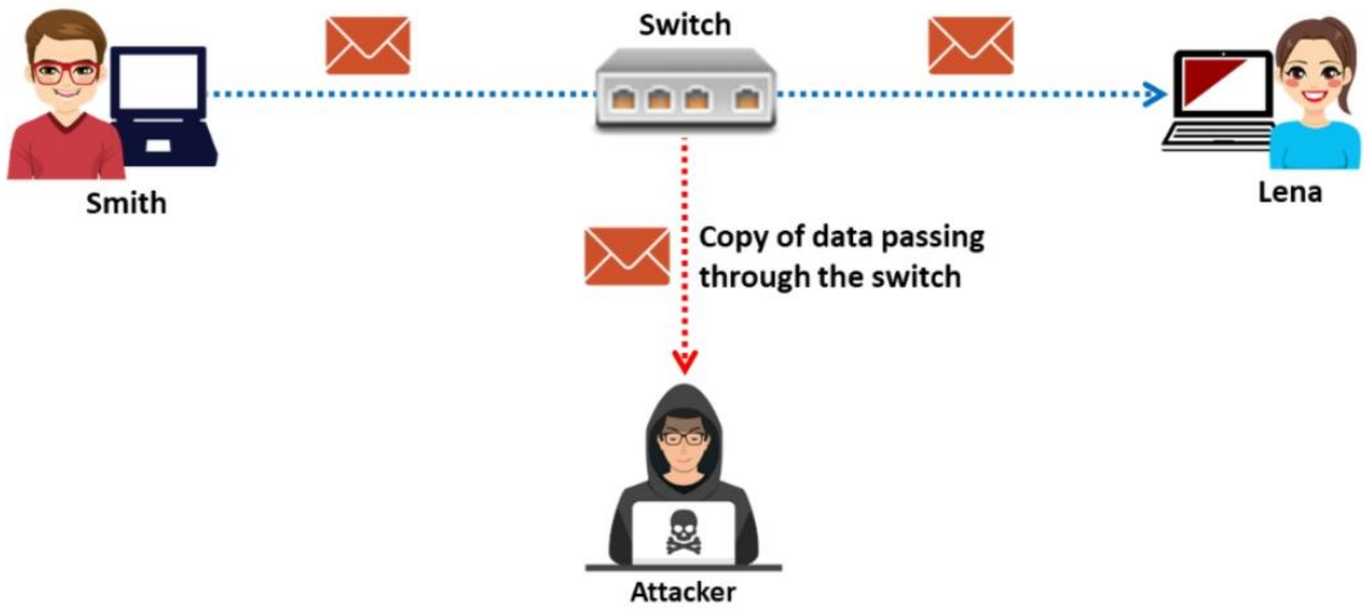


Figure 8.1: Packet sniffing scenario

How a Sniffer Works

The most common way of networking computers is through an Ethernet connection. A computer connected to a local area network (LAN) has two addresses: a MAC address and an Internet Protocol (IP) address. A MAC address uniquely identifies each node in a network and is stored on the NIC itself. The Ethernet protocol uses the MAC address to transfer data to and from a system while building data frames. The data link layer of the OSI model uses an Ethernet header with the MAC address of the destination machine instead of the IP address. The network layer is responsible for mapping IP network addresses to the MAC address as required by the data link protocol. It initially looks for the MAC address of the destination machine in a table, usually called the Address Resolution Protocol (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. These two types are:

- **Shared Ethernet**

  In a shared Ethernet environment, a single bus connects all the hosts that compete for bandwidth. In this environment, all the other machines receive packets meant for one machine. Thus, when machine 1 wants to talk to machine 2, it sends a packet out on the network with the destination MAC address of machine 2, along with its own source MAC address. The other machines in the shared Ethernet (machines 3 and 4) compare the

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

frame's destination MAC address with their own and discard the unmatched frame. However, a machine running a sniffer ignores this rule and accepts all the frames. Sniffing in a shared Ethernet environment is passive and, hence, difficult to detect.

- **Switched Ethernet**

  In a switched Ethernet environment, the hosts connect with a switch instead of a hub. The switch maintains a table that tracks each computer's MAC address and the physical port on which that MAC address is connected, and then delivers packets destined for a particular machine. The switch is a device that sends packets to the destined computer only; furthermore, it does not broadcast them 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 secure and immune to sniffing. However, this is not true.

Although a switch is more secure than a hub, sniffing the network is possible using the following methods:

- **ARP Spoofing**

  ARP is stateless. A machine can send an ARP reply even without asking for it; furthermore, it can accept 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 an incorrect entry for the gateway. Thus, all the traffic destined to pass through the gateway will now pass through the machine that spoofed the gateway MAC address.

- **MAC Flooding**

  Switches maintain 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 a limited memory. MAC flooding makes use of this limitation to bombard switches with fake MAC addresses until the switches can no longer keep up. Once this happens to a switch, it will enter fail-open mode, wherein it starts acting as a hub by broadcasting packets to all the ports on the switch. Once that happens, it becomes easy to perform sniffing. macof is a utility that comes with the dsniff suite and helps the attacker to perform MAC flooding.

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

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

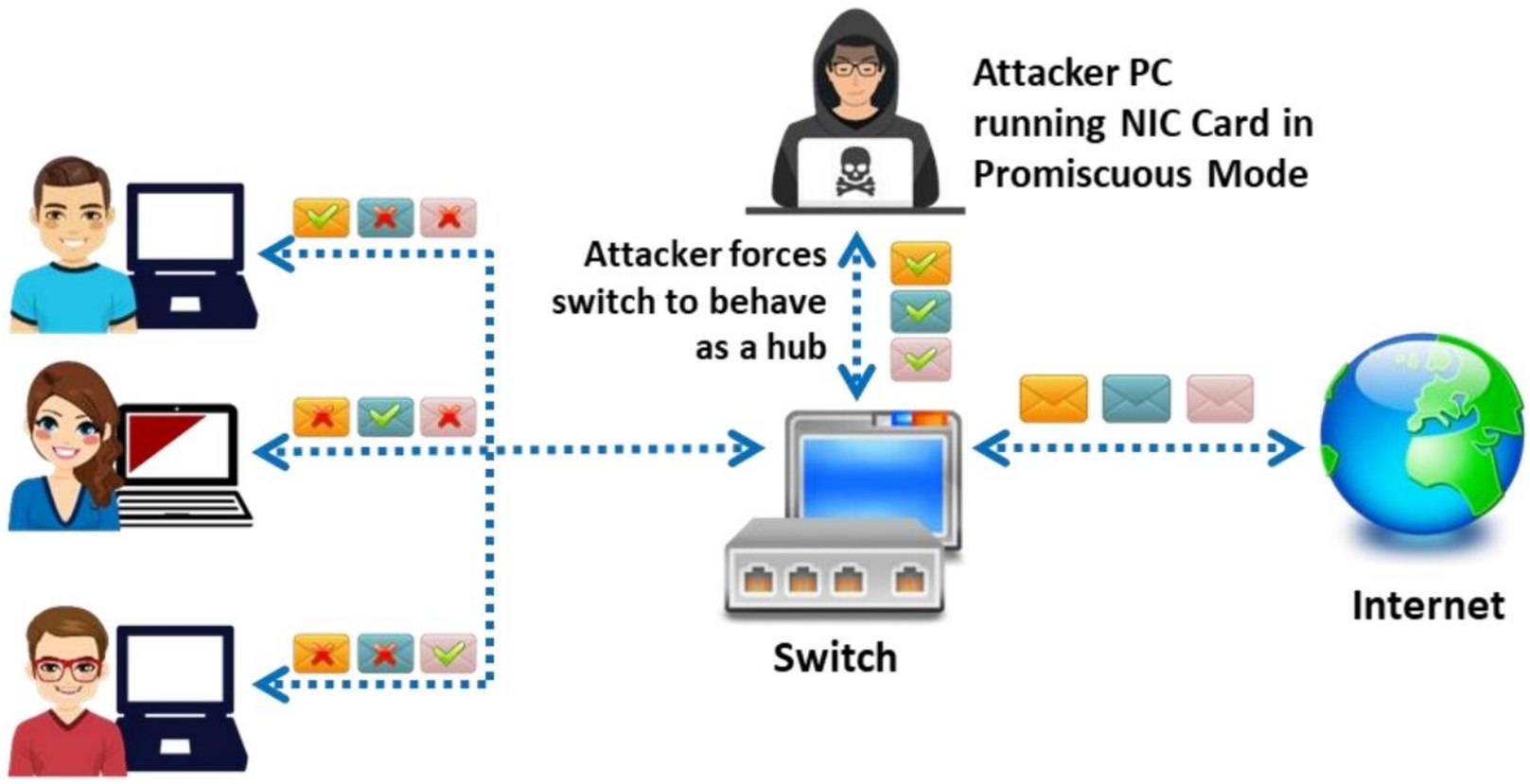
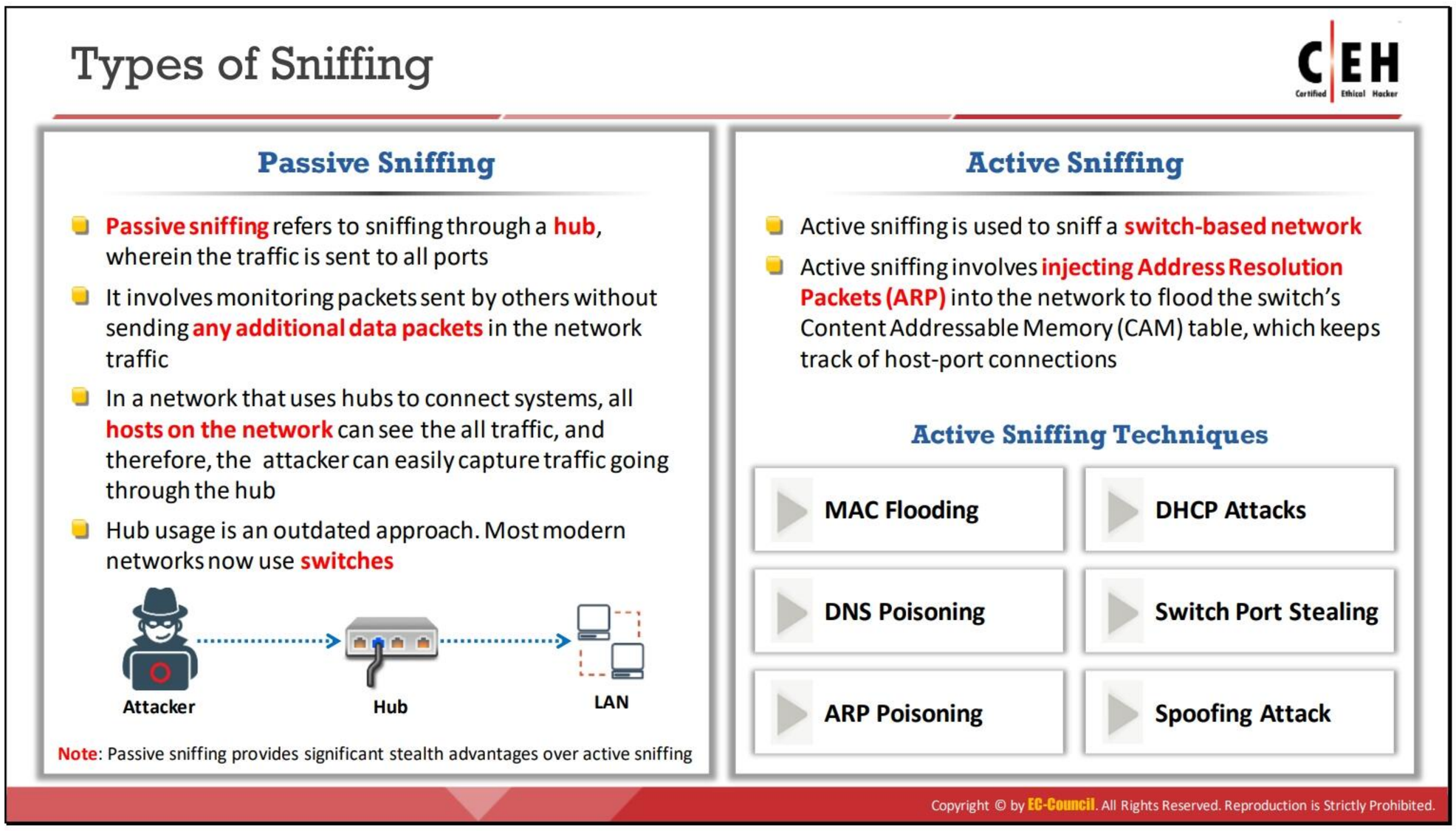


Figure 8.2: Working of a sniffer

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



Types of Sniffing

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

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

- Passive sniffing
- Active sniffing

Passive Sniffing

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

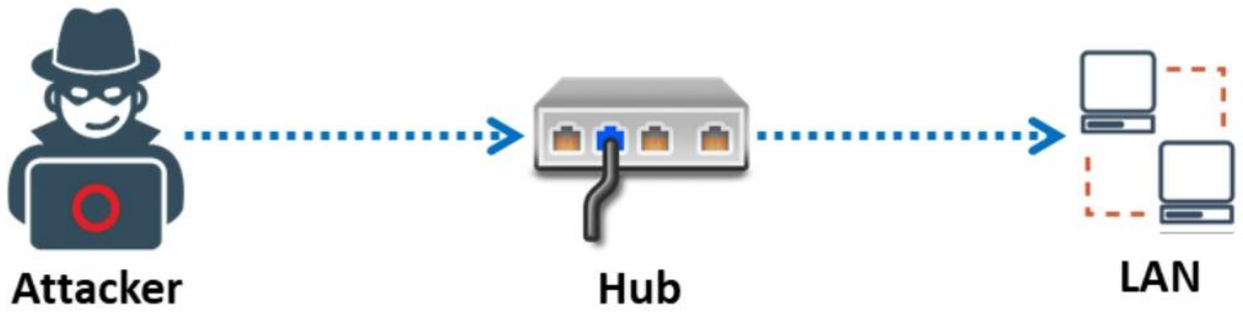


Figure 8.3: Passive sniffing

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

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

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

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

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

Active Sniffing

Active sniffing searches for traffic on a switched LAN by actively injecting traffic into it. 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.

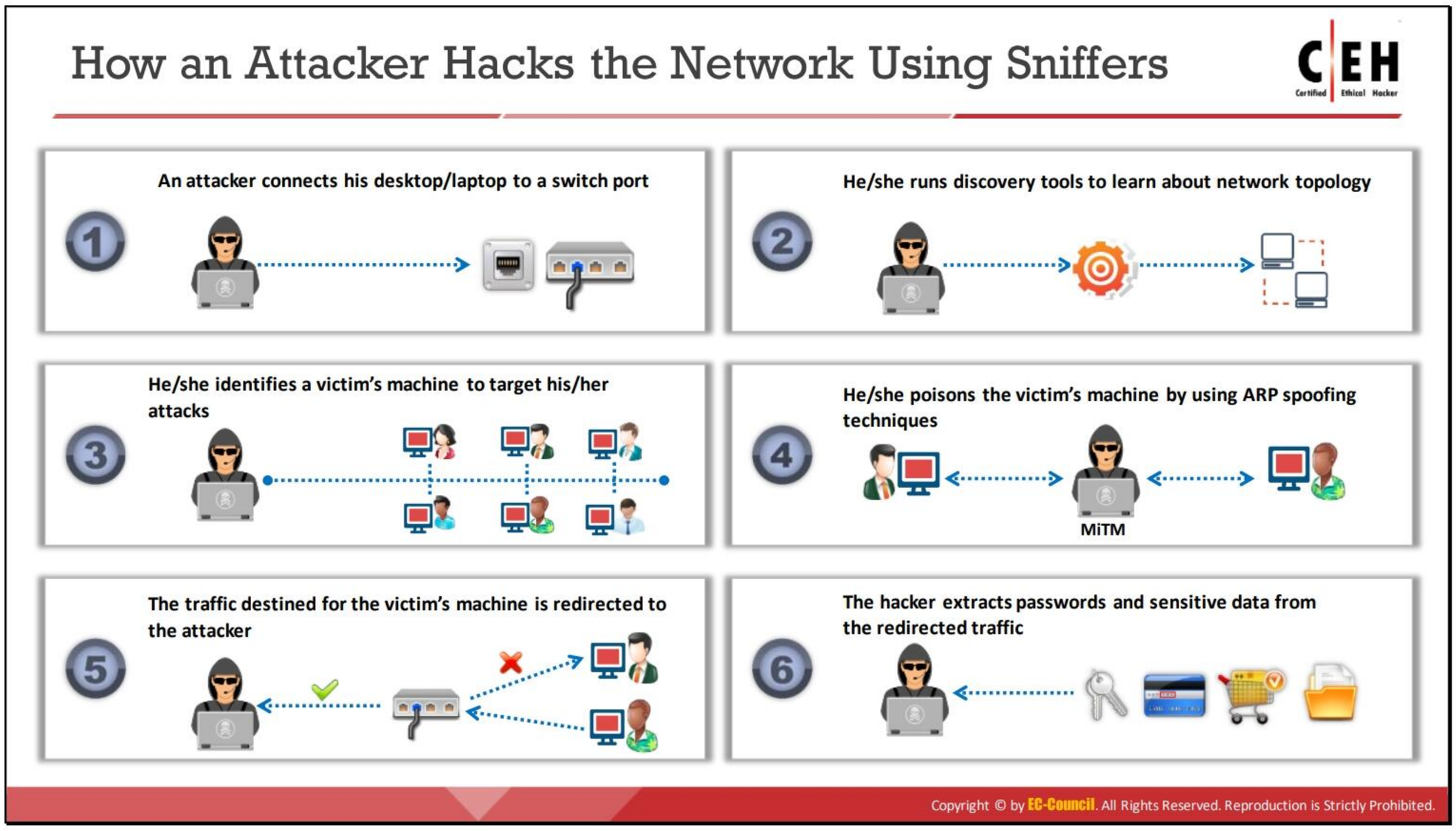
Switches examine data packets for source and destination addresses and then transmit them to the appropriate destinations. Therefore, it is cumbersome to sniff switches. However, attackers can actively inject ARP traffic into a LAN to sniff around a switched network and capture the traffic. Switches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

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

The following is a list of different active sniffing techniques:

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

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



How an Attacker Hacks the Network Using Sniffers

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

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

Figure 8.4: Discovering a switch to access the network

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

Figure 8.5: Using network discovery tools to learn topology

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

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

Figure 8.6: Identifying the victim's machine

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

Figure 8.7: Attacker sending fake ARP messages

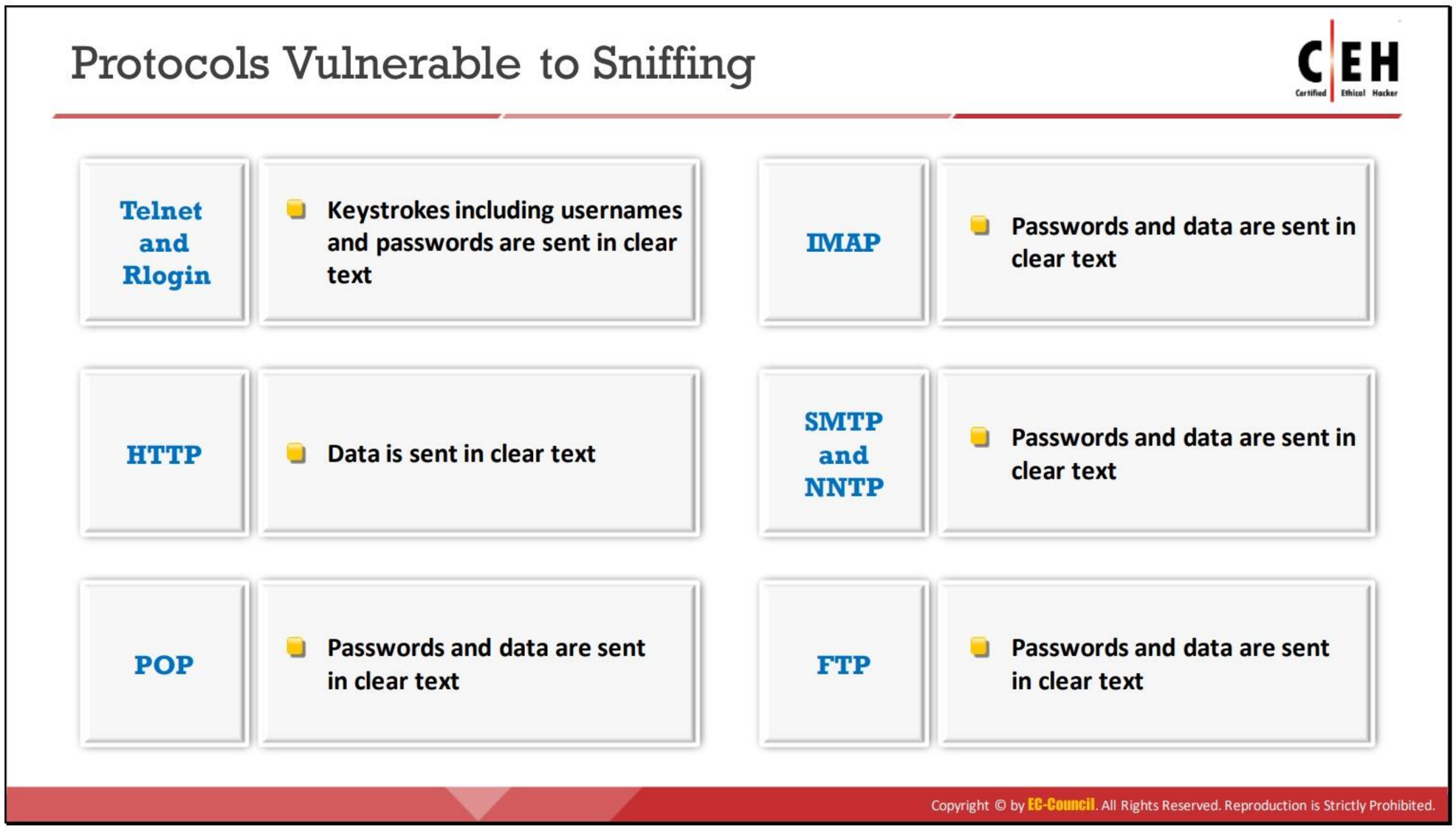
- **Step 5**: The previous step helps the attacker to divert all the traffic from the victim's computer to the attacker's computer. This is a typical man-in-the-middle (MITM) type of attack.

Figure 8.8: Redirecting the traffic to the attacker

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

Figure 8.9: Attacker extracting sensitive information

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



Protocols Vulnerable to Sniffing

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

- **Telnet and Rlogin**

  Telnet is a protocol used for communicating with a remote host (via port 23) on a network using a command-line terminal. rlogin enables an attacker to log into a network machine remotely via a TCP connection. Neither of these protocols provides encryption; therefore, data traveling between clients connected through any of these protocols are in plaintext and vulnerable to sniffing. Attackers can sniff keystrokes, including usernames and passwords.

- **HTTP**

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

- **SNMP**

  Simple Network Management Protocol (SNMP) is a TCP/IP-based protocol used for exchanging management information between devices connected on a network. The first version of SNMP (SNMPv1 and SNMPv2) does not offer strong security, which leads to the transfer of data in a cleartext format. Attackers exploit the vulnerabilities in this version to acquire passwords in plaintext.

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

- **SMTP**

  Simple Mail Transfer Protocol (SMTP) is used for transmitting email messages over the Internet. In most implementations, SMTP messages are transmitted in cleartext, which enables attackers to capture plaintext passwords. Further, SMTP does not provide any protection against sniffing attacks.

- **NNTP**

  Network News Transfer Protocol (NNTP) distributes, inquires into, retrieves, and posts news articles using a reliable stream-based transmission of news among the ARPA-Internet community. However, this protocol fails to encrypt the data, which allows attackers to sniff sensitive information.

- **POP**

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

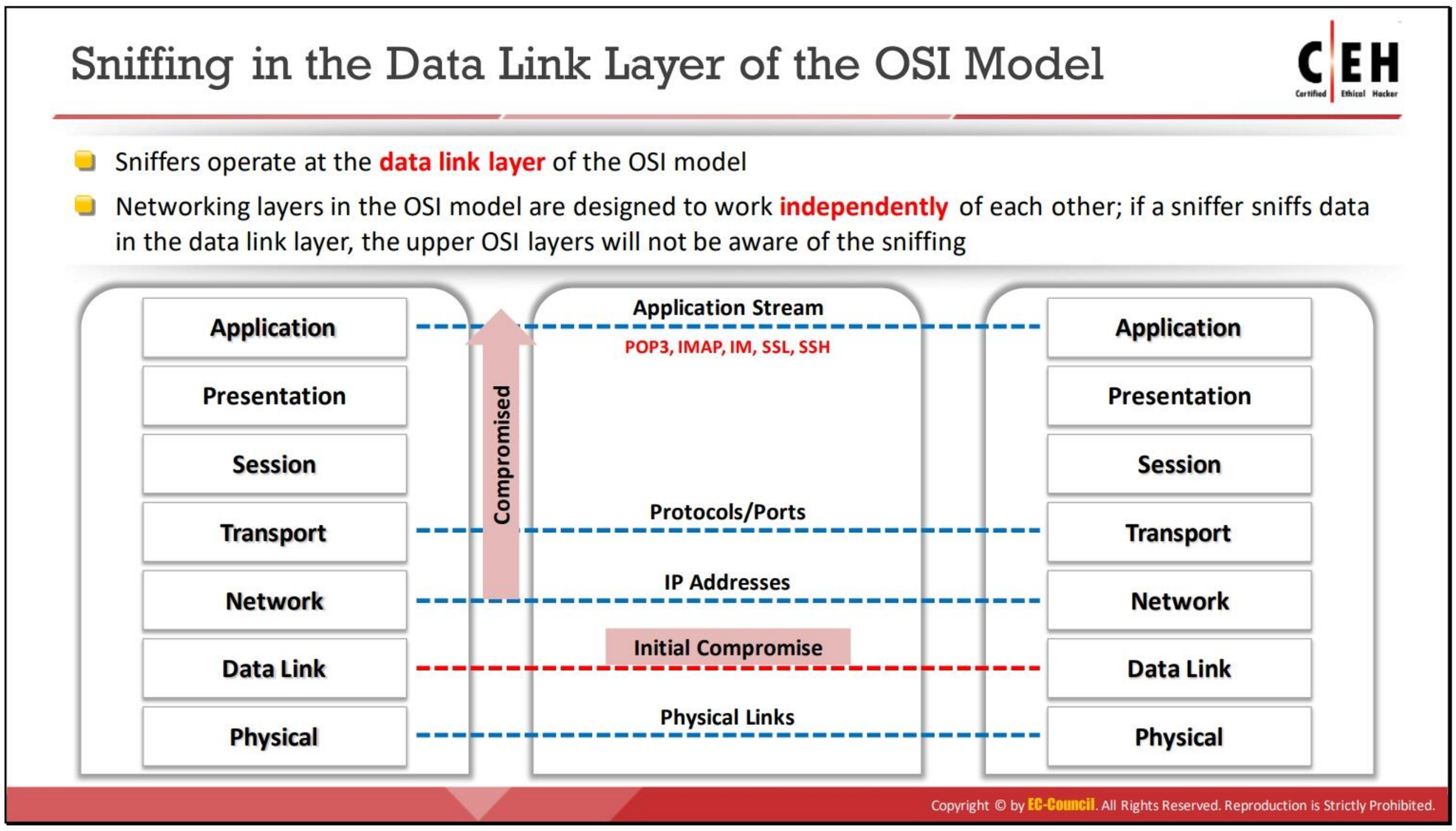
- **FTP**

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

- **IMAP**

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

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



Sniffing in the Data Link Layer of the OSI Model

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

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

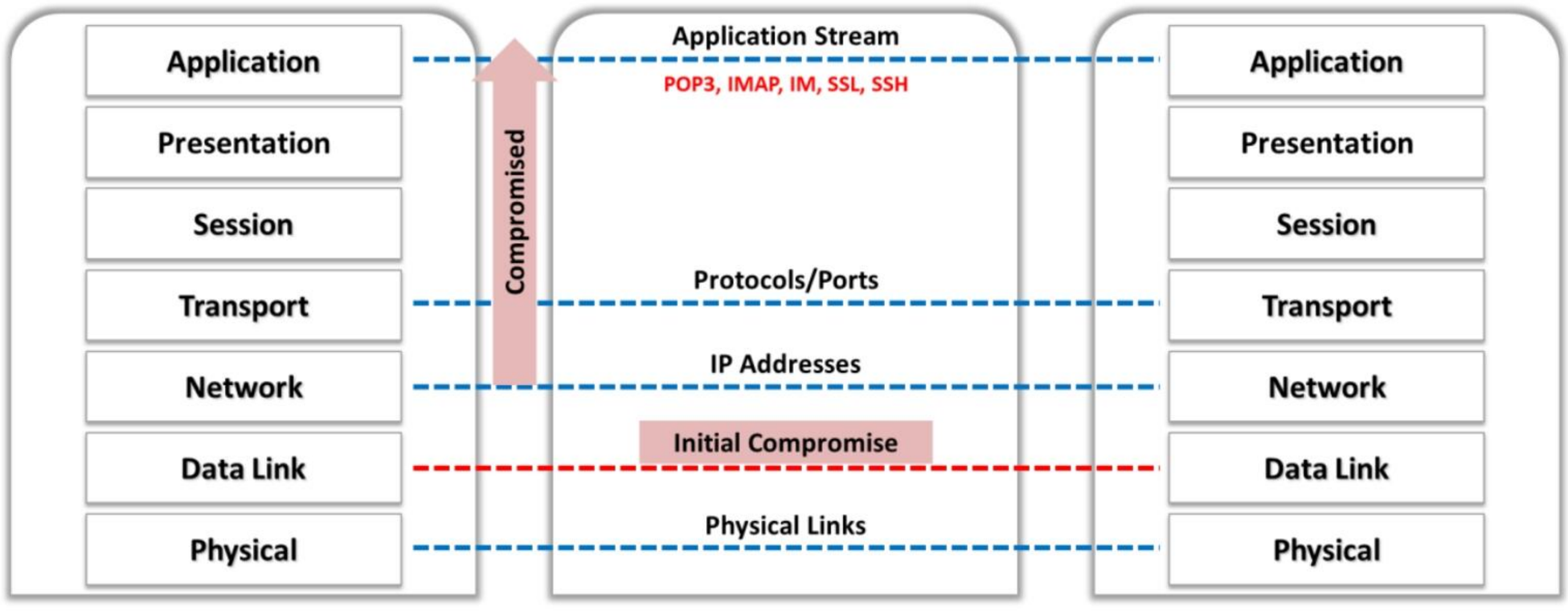
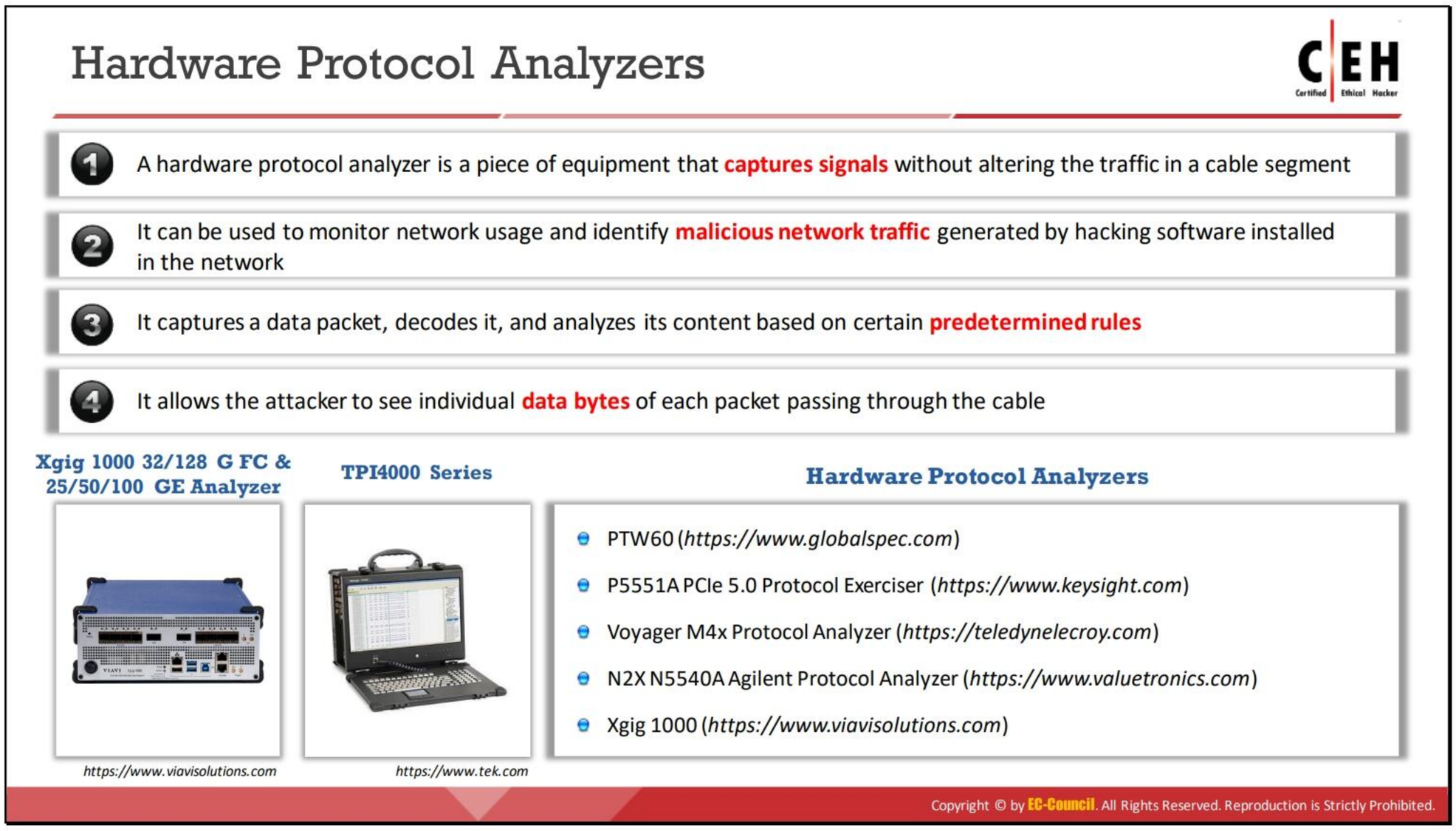


Figure 8.10: Sniffing in the data link layer of the OSI model

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



Hardware Protocol Analyzers

A hardware protocol analyzer is a device that interprets traffic passing over a network. It 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.

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

Hardware protocol analyzers from different manufacturers include the following.

- **Xgig 1000 32/128 G FC & 25/50/100 GE Analyzer**

  Source: *https://www.viavisolutions.com*

  The VIAVI Xgig 1000 32/128 G Fiber Channel (FC) and 25/50/100 G Ethernet (GE) platform is a hardware product that addresses 8G/16G/32G/128G FC and 10/25/50/100 GE in an integrated, portable platform with reconfigurable ports. It provides a platform to perform inline, nonintrusive capture and analysis and inline jamming (error injection). It uses the industry's first true analog pass-through adapter while keeping the linear

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

nature of signal-over-copper connections. The platform offers unmatched visibility to the OSI physical layer with features such as auto negotiation, link training, and forward error correction (FEC).

Figure 8.11: Xgig 1000 32/128 G FC and 25/50/100 GE Analyzer

- **TPI4000 Series**

Source: *https://www.tek.com*

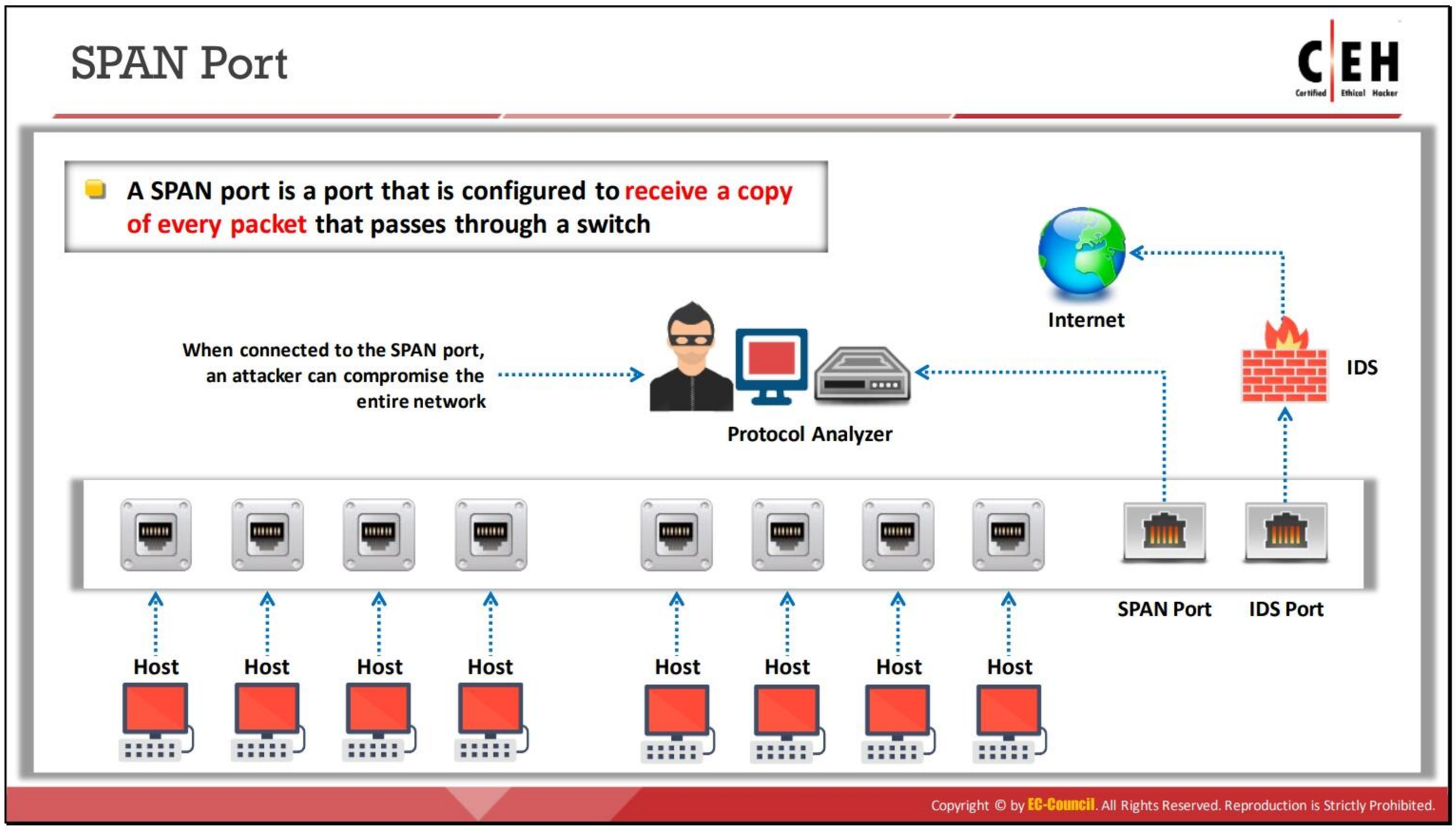
Each of the TPI4000 protocol analyzers captures and displays link data, even at full line rates. Views of primitives as well as the frame delimiter, frame header, and payload data are also provided. The Protocol Database Editor allows the user to define the additional decoding of protocols to further enhance existing functions. Deep, bit-level triggering and pre- and post-filtering capabilities ensure that relevant data can be extracted from multi-gigabit data streams.

Figure 8.12: TPI4000 protocol analyzer

Some examples of hardware protocol analyzers are listed below:

- PTW60 (*https://www.globalspec.com*)
- P5551A PCIe 5.0 Protocol Exerciser (*https://www.keysight.com*)
- Voyager M4x Protocol Analyzer (*https://teledynelecroy.com*)
- N2X N5540A Agilent Protocol Analyzer (*https://www.valuetronics.com*)
- Xgig 1000 (*https://www.viavisolutions.com*)

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



SPAN Port

Switched Port Analyzer (SPAN) is a Cisco switch feature, also known as "port mirroring," that monitors network traffic on one or more ports on the switch. A SPAN port is a port that is configured to receive a copy of every packet that passes through a switch. It helps to analyze and debug data, identify errors, and investigate unauthorized network access. When port mirroring is on, the network switch sends a copy of the network packets from the source port to the 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 for which 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 virtual local area network (VLAN).

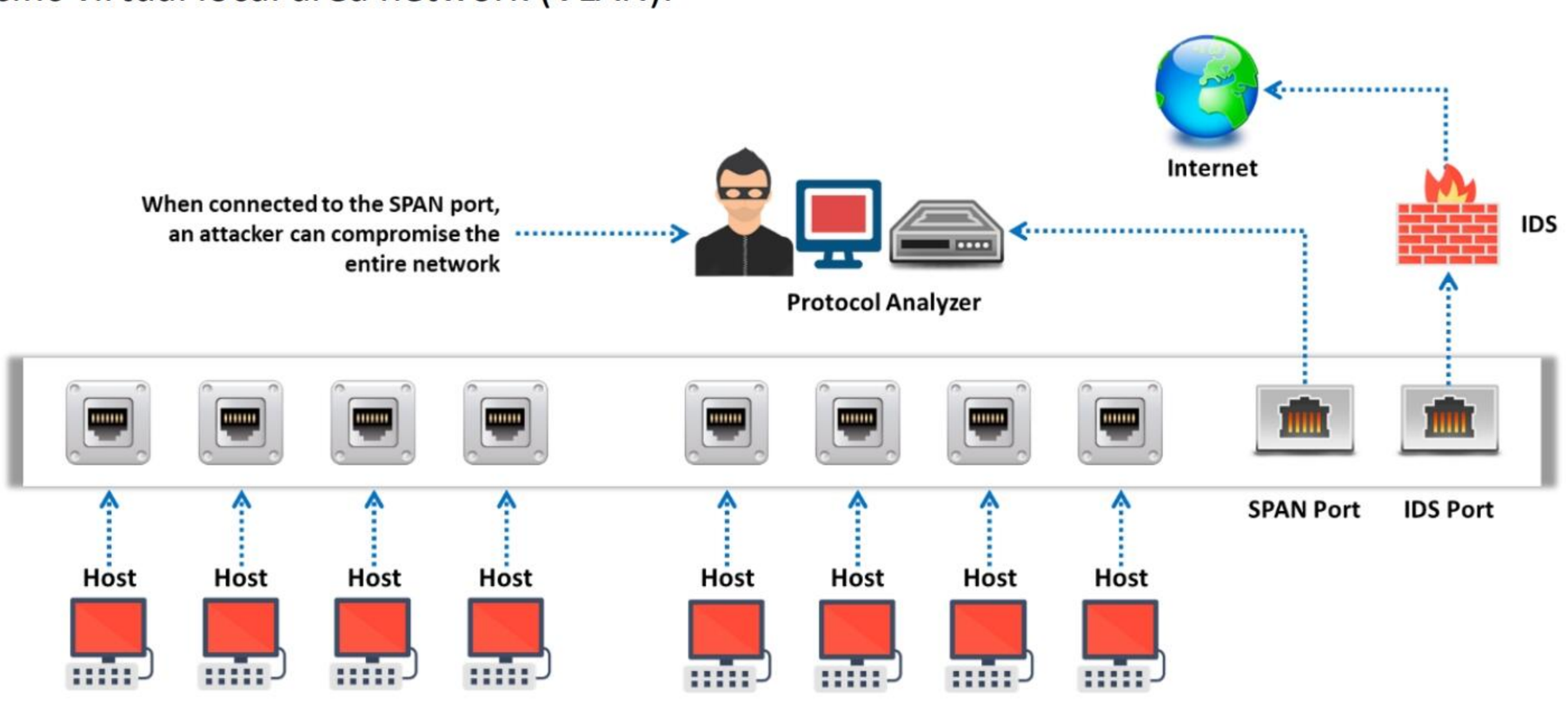
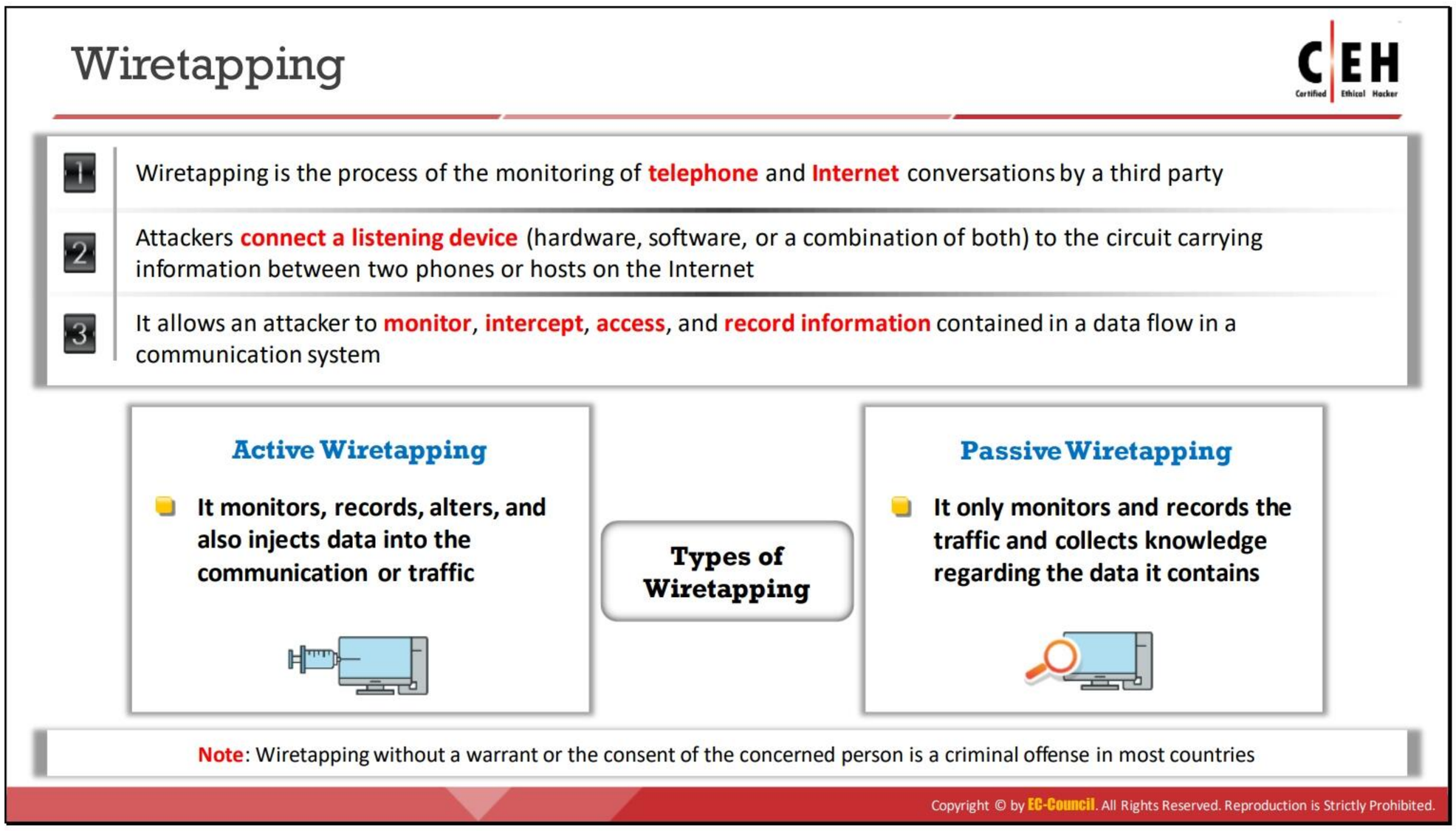


Figure 8.13: Working of SPAN

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



Wiretapping

Wiretapping, or telephone tapping, refers to the monitoring of telephone or Internet conversations by a third party with covert intentions. 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 the two target phones or hosts. Typically, the attacker uses a small amount of the electrical signals 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

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

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**

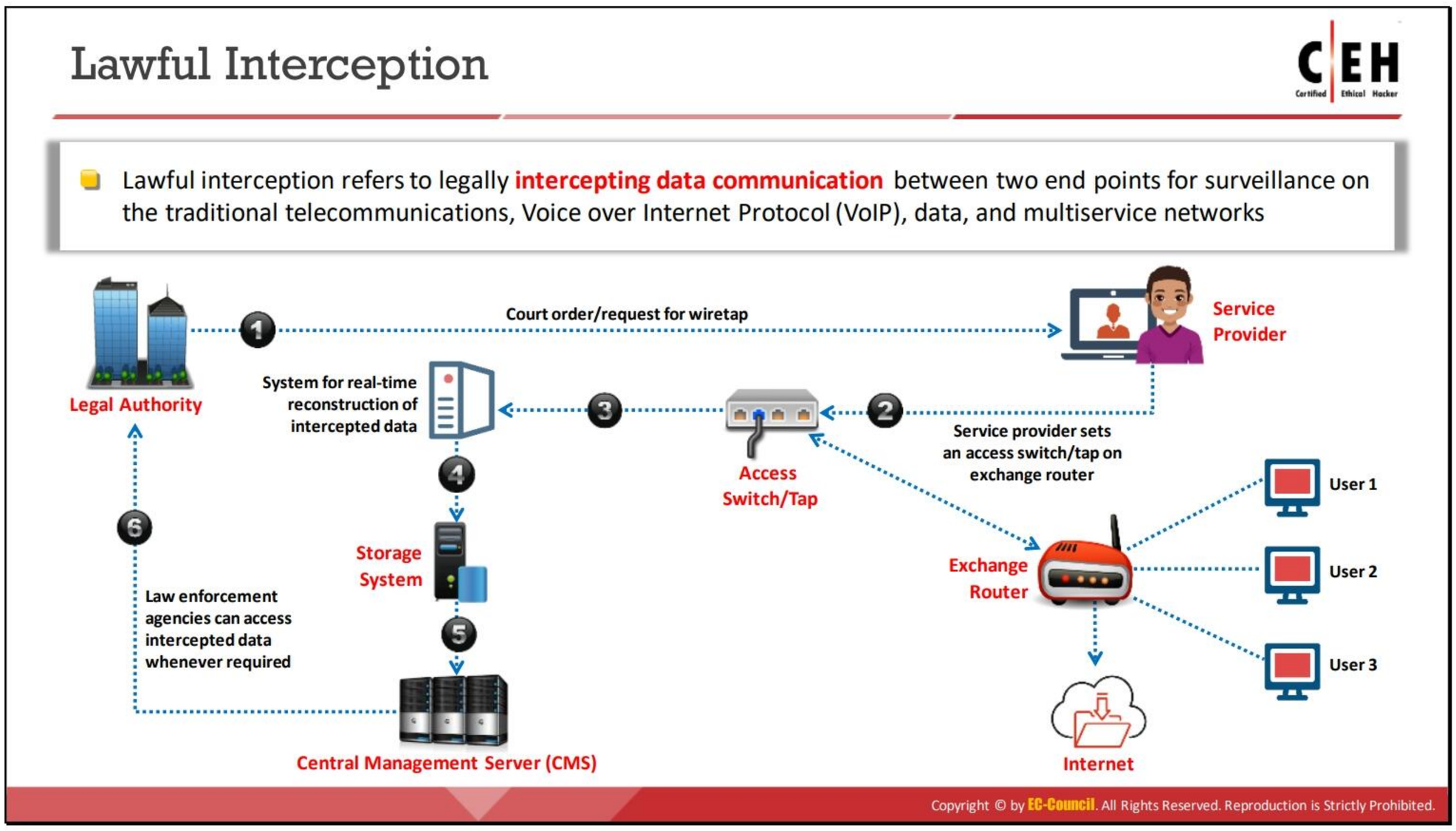
  In hacking terminology, active wiretapping is an MITM attack. This allows an attacker to monitor and record the traffic or data flow in a communication system. The attacker can also alter or inject data into communication or traffic.

- **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 people conducting the conversation is a criminal offense in most countries, and is punishable depending on the country's law.

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



Lawful Interception

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

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

The figure shows the telco/ISP lawful solution provided by the Decision Computer Group. The solution consists of one tap/access switch and multiple systems for the 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 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, and telnet. The Centralized Management Server (CMS) manages all the ED systems.

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

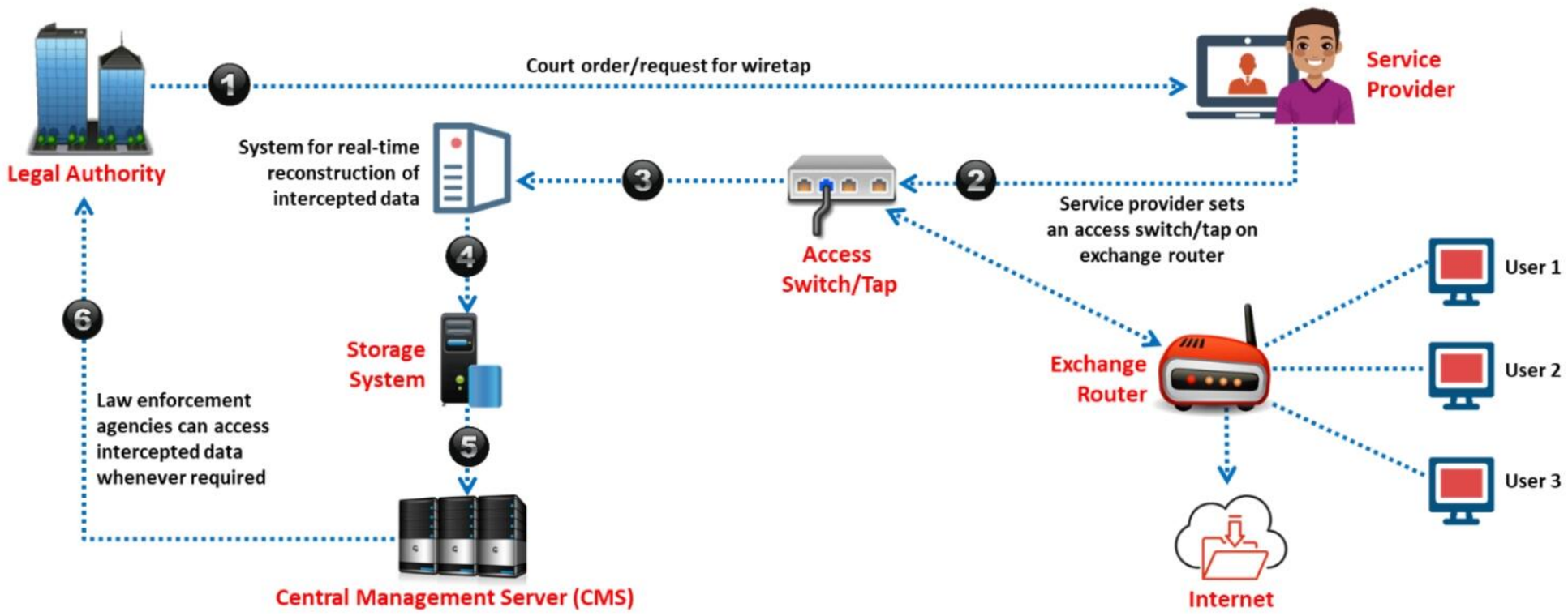
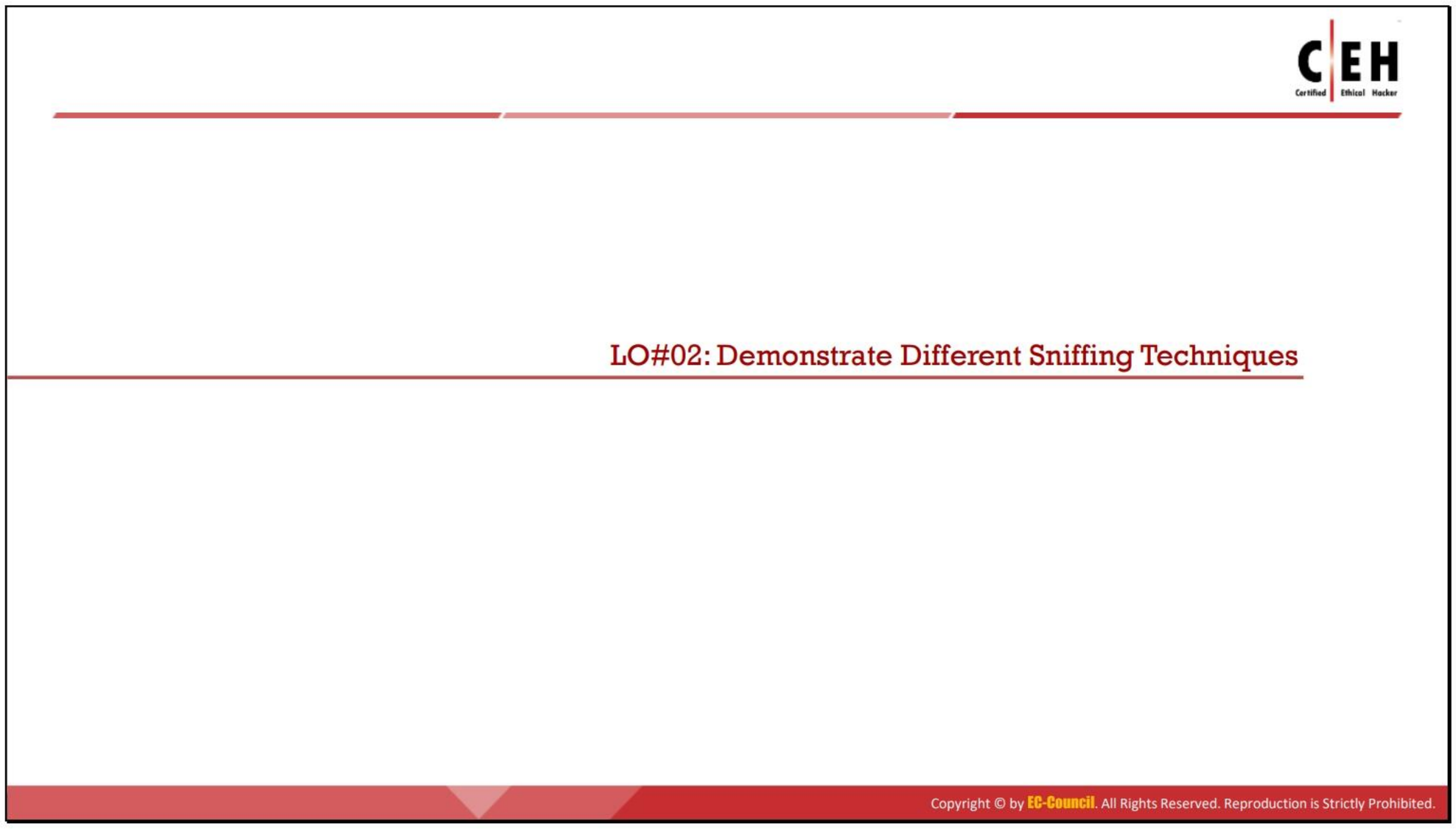


Figure 8.14: Telco/ISP lawful solution

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

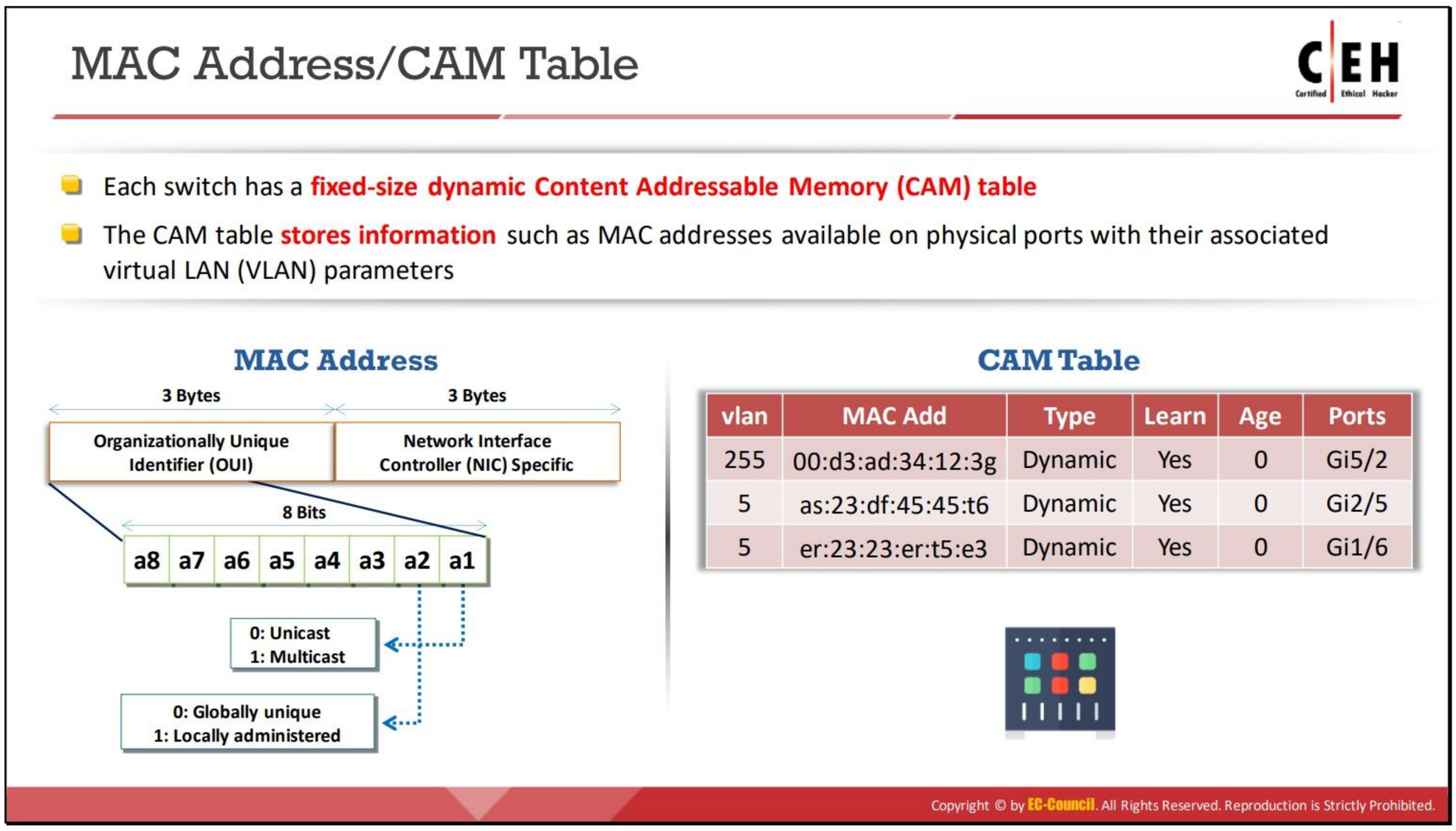


Sniffing Technique: MAC Attacks

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

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

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



MAC Address

A MAC address uniquely identifies each node of a network. Each device in the network has a MAC address associated with a physical port on the network switch, which makes it possible to designate a specific single point of the network. MAC addresses are used as network addresses 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 comprises 48 bits that are split 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 (OUI). 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.), and the next six digits, 14C829, indicate the serial number of the adapter.

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

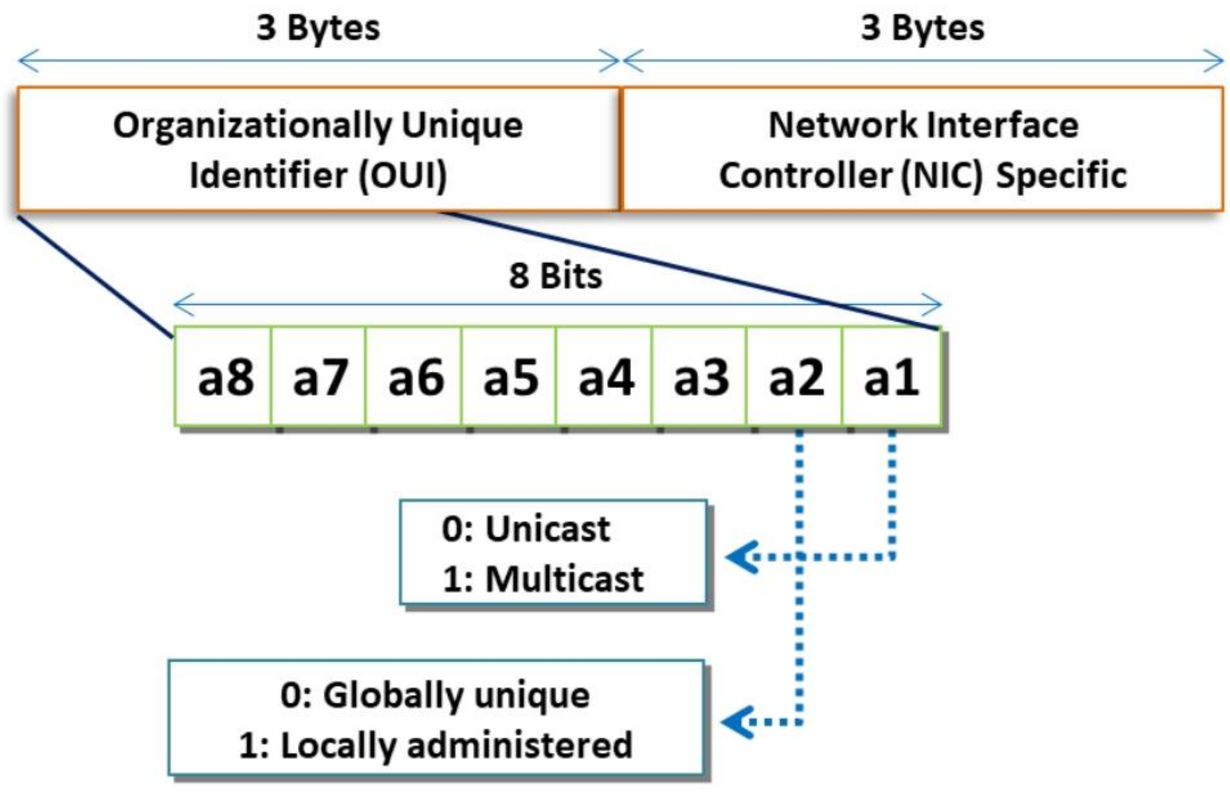


Figure 8.15: MAC address

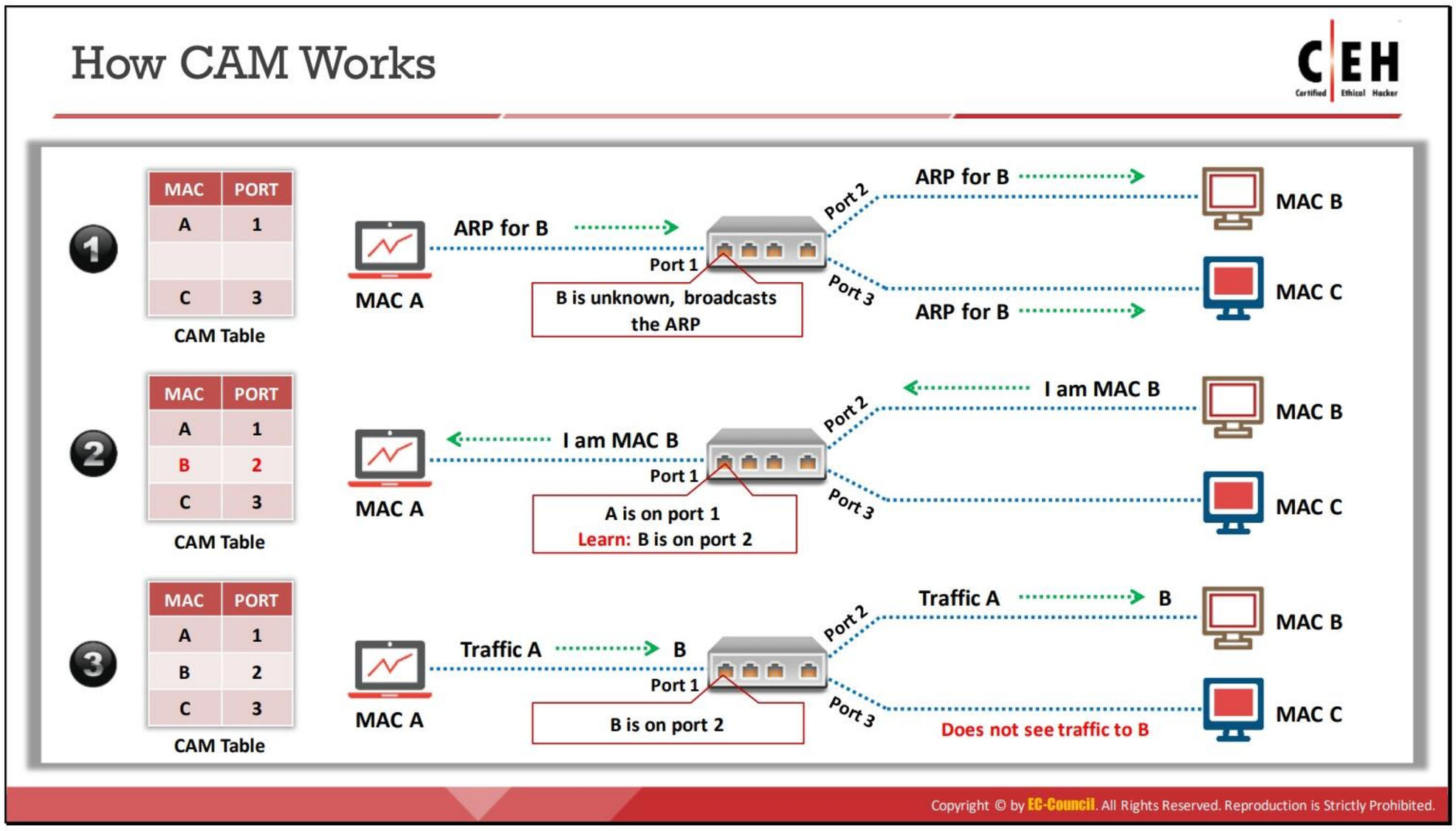
CAM Table

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

vlan	MAC Add	Type	Learn	Age	Ports
255	00:d3:ad:34:12:3g	Dynamic	Yes	0	Gi5/2
5	as:23:df:45:45:t6	Dynamic	Yes	0	Gi2/5
5	er:23:23:er:t5:e3	Dynamic	Yes	0	Gi1/6

Table 8.1: CAM table

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



How CAM Works

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

Refer to the diagrams of the working of the CAM table. Three machines are shown: **Machine A**, **Machine B**, and **Machine C**, each holding MAC addresses **A**, **B**, and **C**. Machine A, holding the MAC address A, wants to interact with Machine B.

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

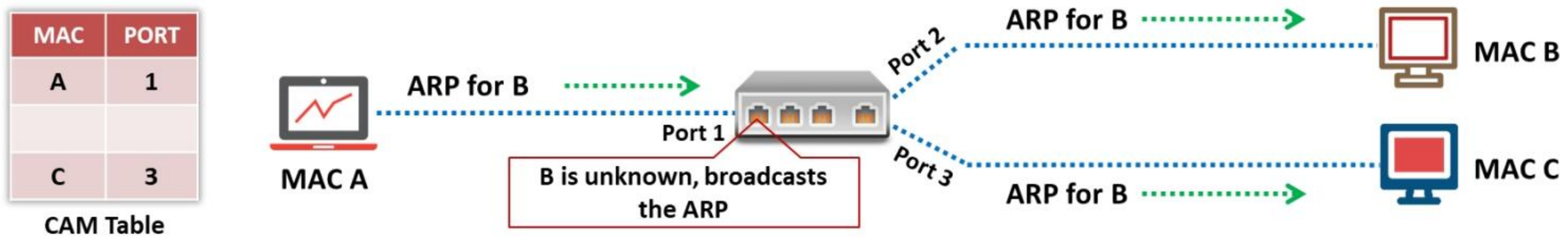


Figure 8.16: Working of CAM table step-1

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

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

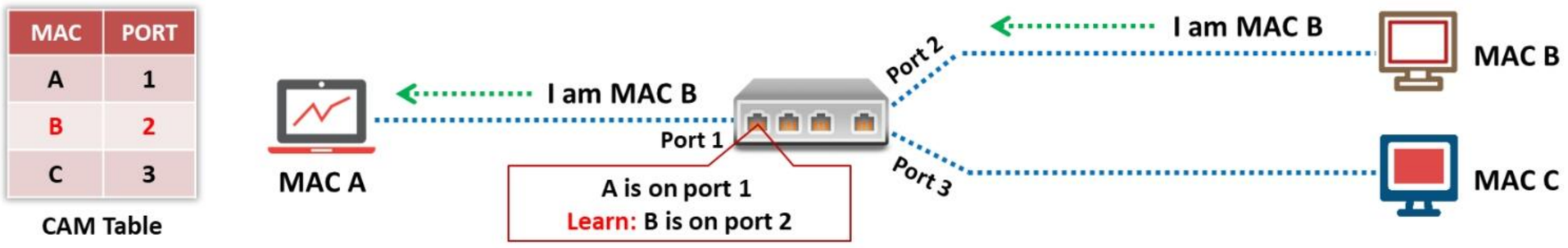


Figure 8.17: Working of CAM table step-2

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

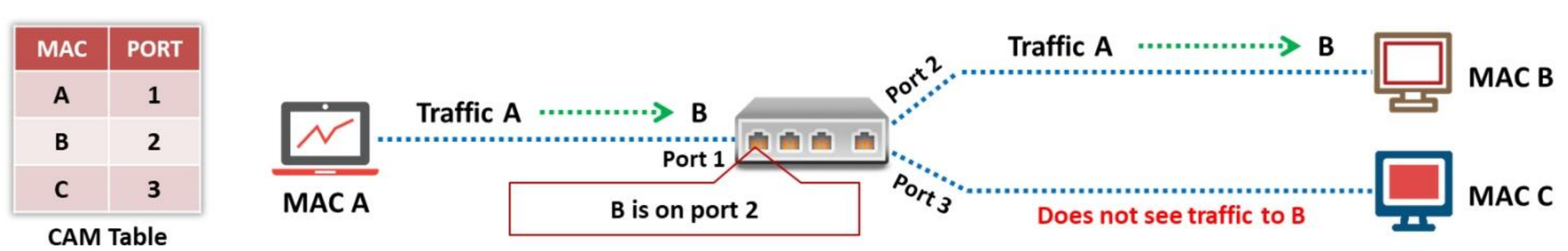
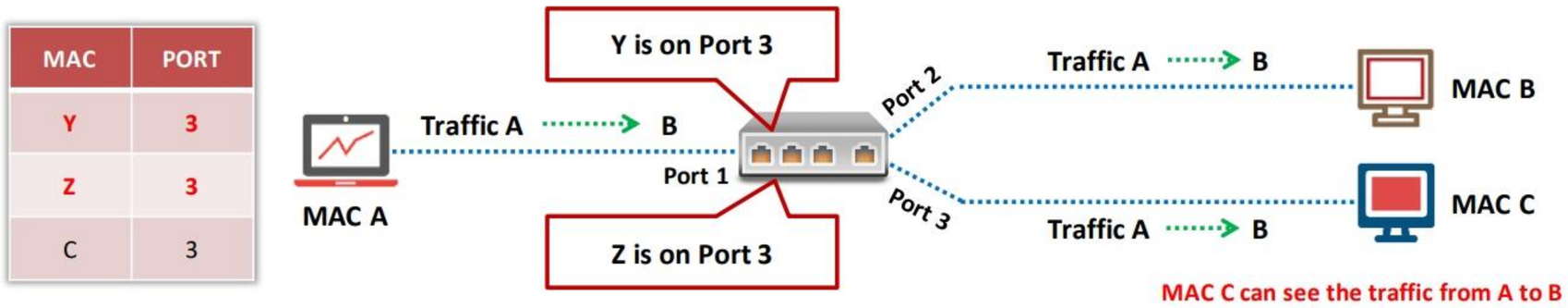


Figure 8.18: Working of CAM table step-3

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

What Happens When a CAM Table Is Full?

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



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

What Happens when a CAM Table is Full?

As discussed, a CAM table contains network information such as MAC addresses available on physical switch ports and associated VLAN parameters. A CAM table's limited size renders it susceptible to attacks from MAC flooding, which bombards the switch with fake source MAC addresses until the CAM table is full. Thereafter, the switch broadcasts all incoming traffic to all ports. This causes the switch to reset to its learning mode, causing the switch to broadcast on every port similar to a hub, thereby enabling the attacker to monitor the frames sent from the victim host to another host without any CAM table entry. This attack also fills the CAM tables of adjacent switches.

The figure illustrates how a CAM table can be flooded with fake MAC addresses to monitor the frames sent from the victim host to another host without any CAM table entry.

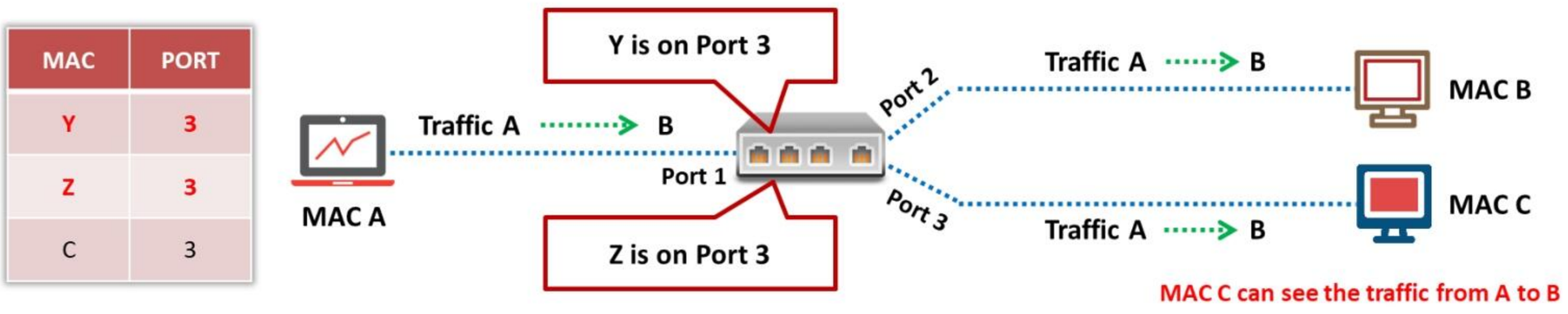
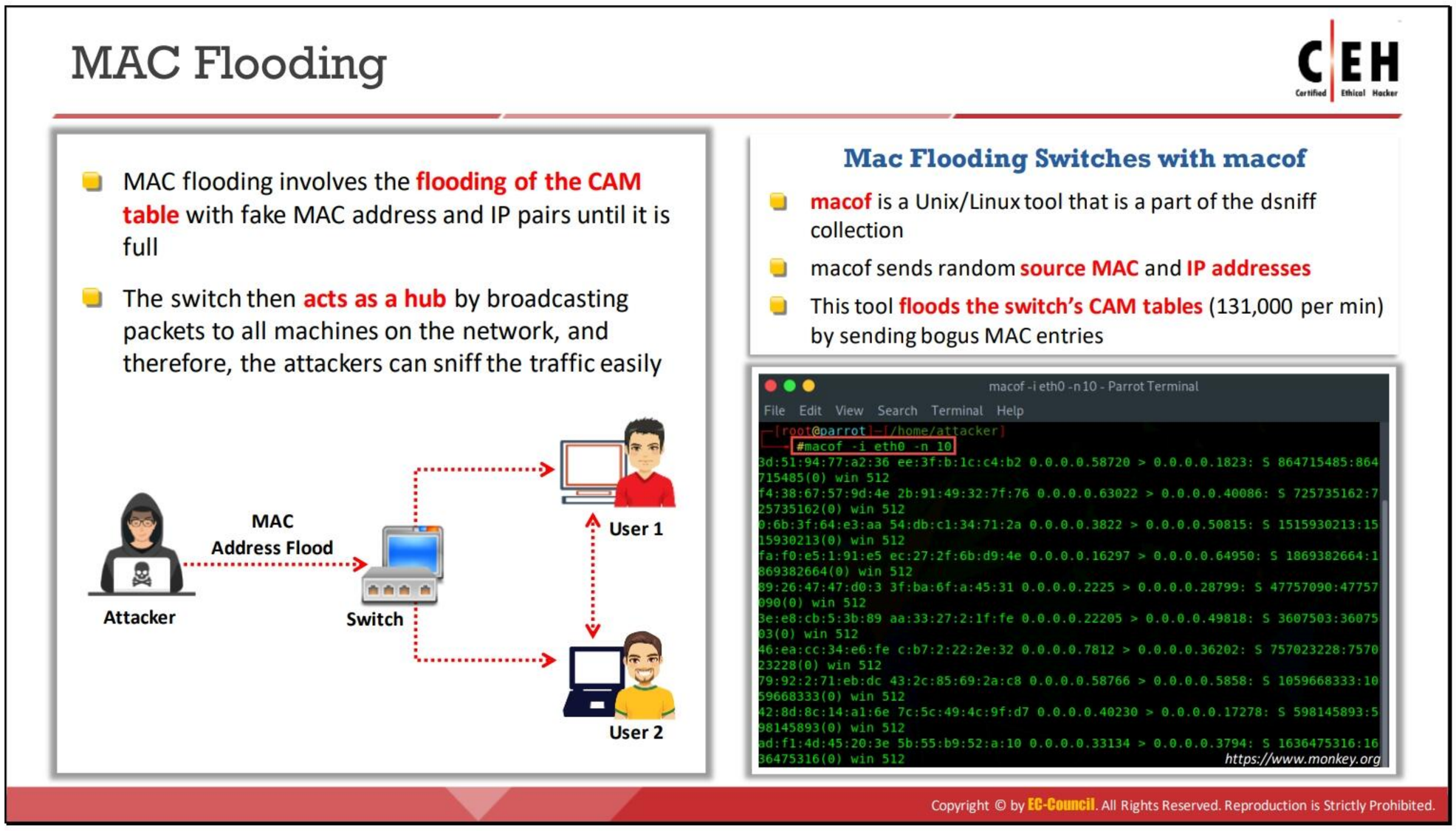


Figure 8.19: Flooding a CAM table

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



MAC Flooding

MAC flooding is a technique used to compromise the security of network switches that connect network segments or devices. Attackers use the MAC flooding technique to force a switch to act as a hub so that they can easily sniff the traffic.

In a switched network, an Ethernet switch contains a CAM table that stores all the MAC addresses of devices connected in the network. A switch acts as an intermediate device between one or more computers in a network. It looks for Ethernet frames, which carry the destination MAC address; then, it tallies this address with the MAC address in its CAM table and forwards the traffic to the destined machine. Unlike a hub, which broadcasts data across the network, a switch sends data only to the intended recipient. Thus, a switched network is more secure compared to a hub network. However, the size of the CAM table is fixed, and as it can store only a limited number of MAC addresses in it, an attacker may send numerous fake MAC address to the switch. No problem occurs until the MAC address table is full. Once the MAC address table is full, any further requests may force the switch to enter fail-open mode. In the fail-open mode, the switch starts behaving like a hub and broadcasts incoming traffic through all the ports in the network. The attacker then changes his/her machine's NIC to promiscuous mode to enable the machine to accept all the traffic entering it. Thus, attackers can sniff the traffic easily and steal sensitive information.

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

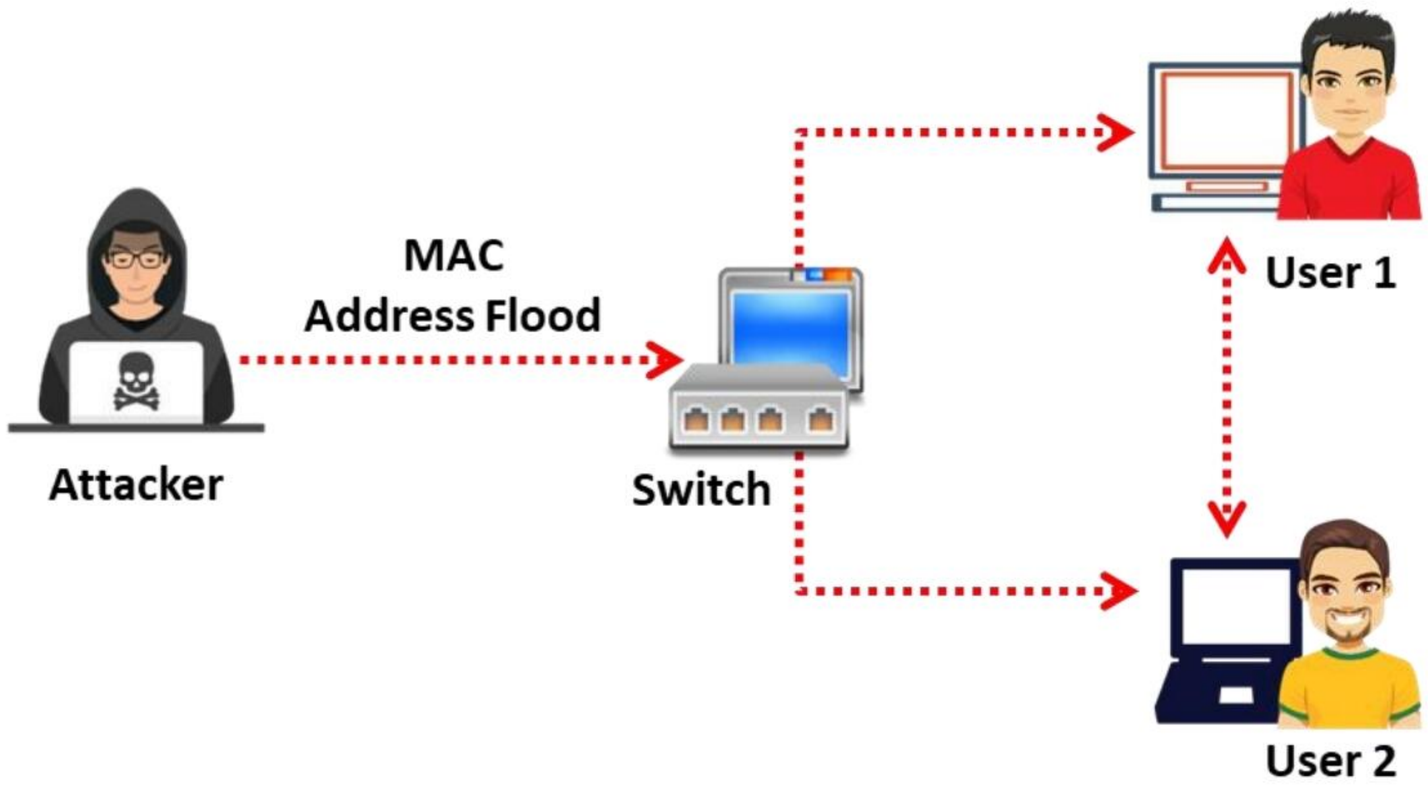


Figure 8.20: MAC flooding

Mac Flooding Switches with macof

Source: *https://monkey.org*

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

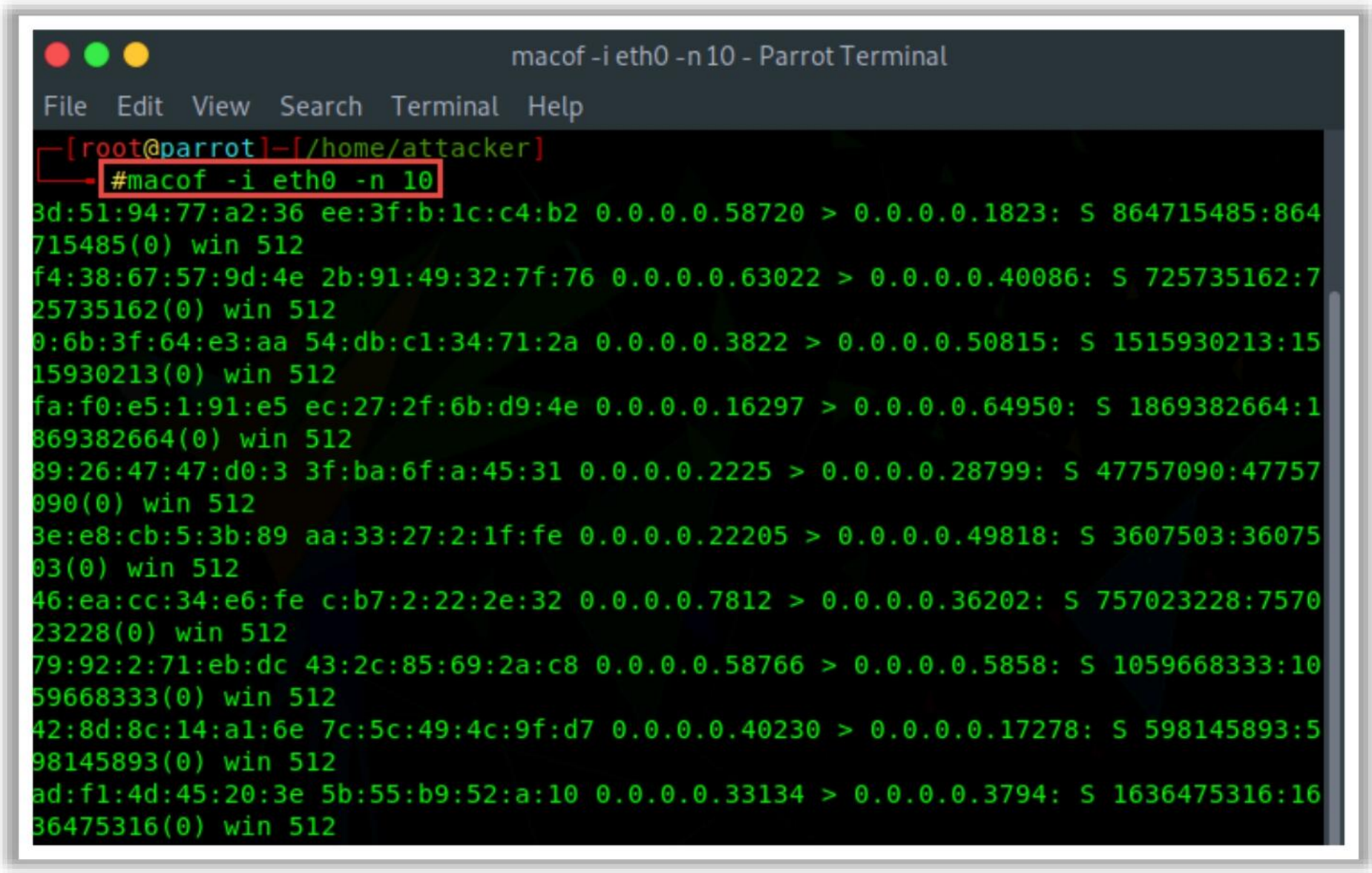
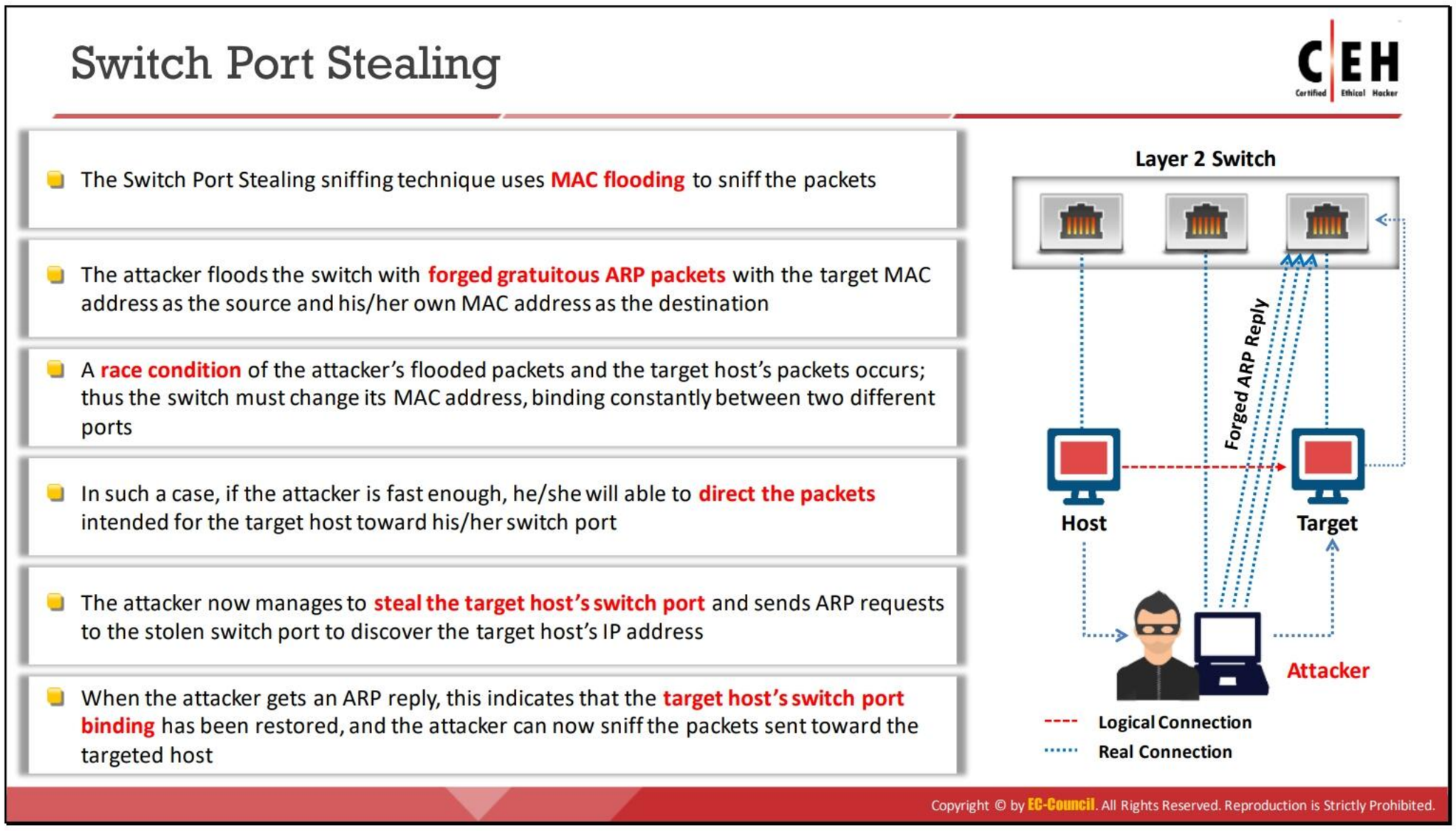


Figure 8.21: MAC flooding using macof

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



Switch Port Stealing

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

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

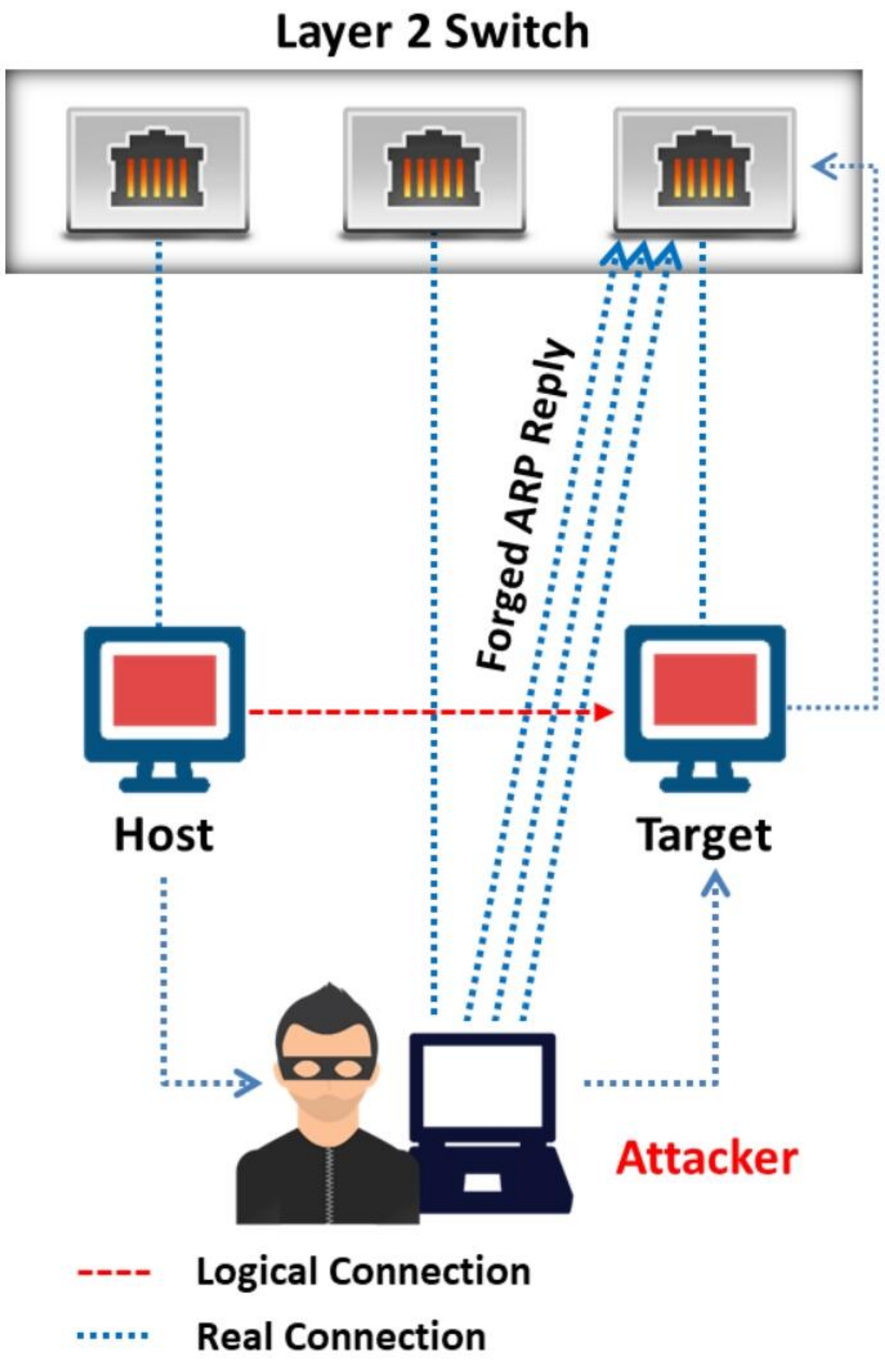


Figure 8.22: Switch port stealing

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

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

Table 8.2: Details of three hosts in a network

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

MAC Table

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

Table 8.3: MAC table

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 8.4: ARP cache table

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

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

Table 8.5: Switch updated with a spoofed entry

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 8.6: ARP cache updated with a spoofed entry

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**).

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

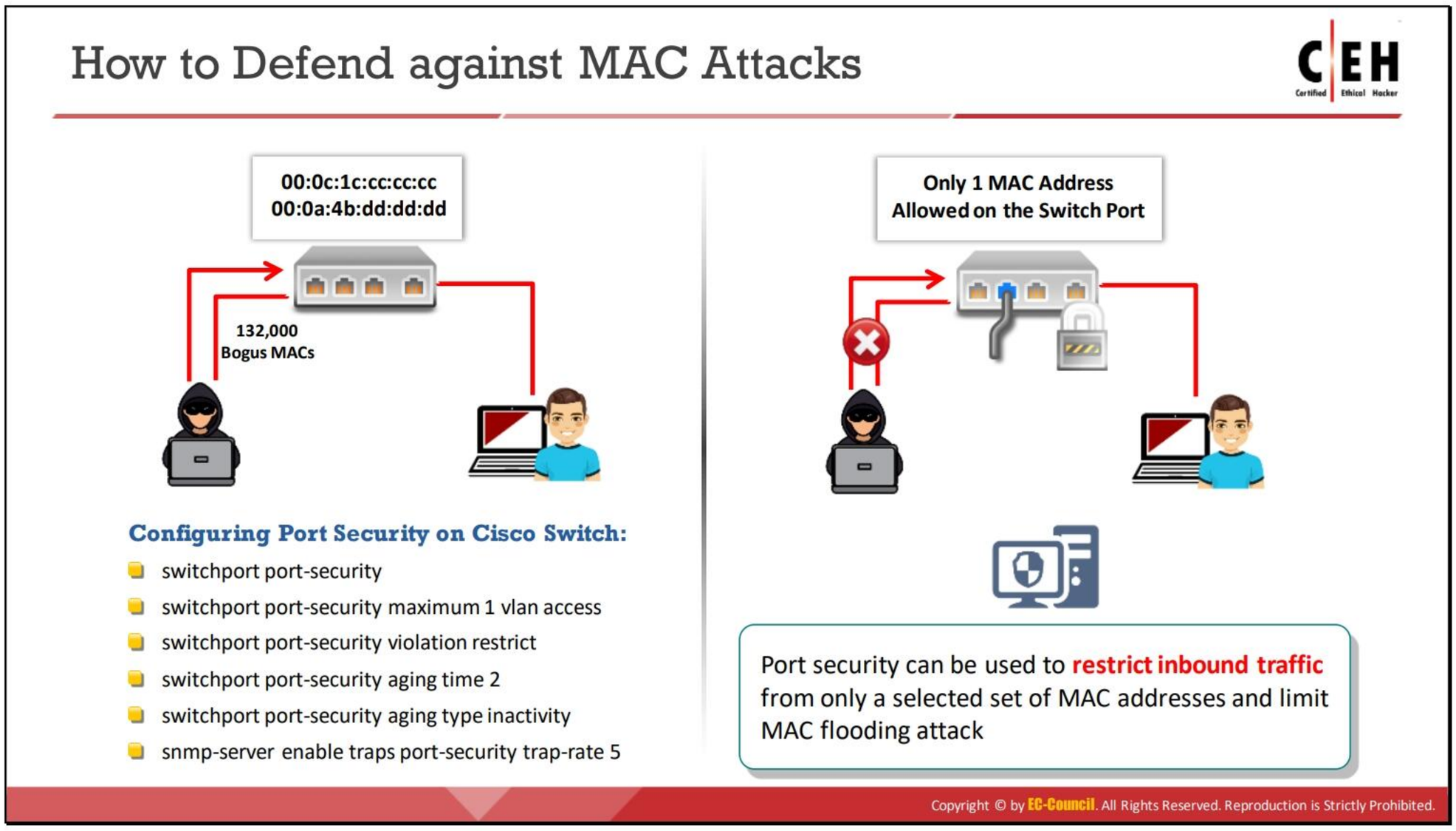
VLAN	MAC Address	Type	Learn	Age	Ports
255	Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	0	Port A
5	Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port B
5	Host C	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port C

Table 8.7: MAC Table updated with a spoofed entry

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.



How to Defend against MAC Attacks

Port security is a feature that 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 inside the group of defined addresses.

A security violation occurs

- When a port is configured as a secure port, and the maximum number of secure MAC addresses is reached
- When the MAC address of the machine that is attempting to access the port does not match any of the identified secure MAC addresses

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

- You can configure all secure MAC addresses by using the switch port, port-securing the 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.

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

As shown in the figure, the attacker floods the switch CAM tables with fake MAC addresses and thus threatens security by turning a switch into a hub.

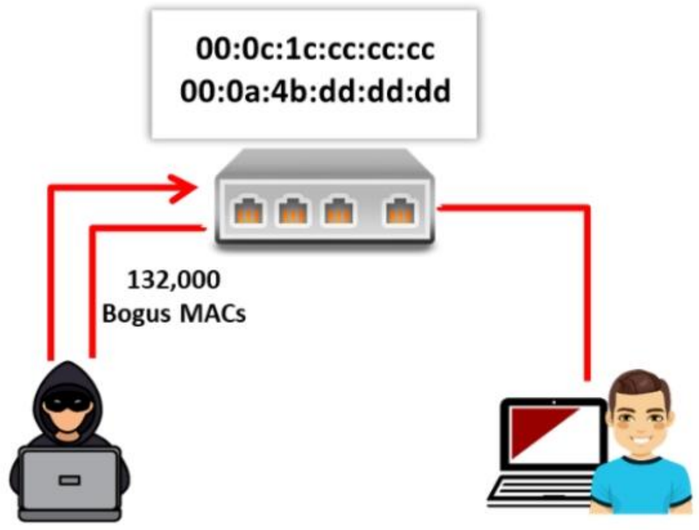


Figure 8.23: Flooding CAM tables

As shown in the figure, the number of MAC addresses allowed on the switch port is limited to one; therefore, the MAC requests are recognized as flooding. Port security locks down the port and sends an SNMP trap.

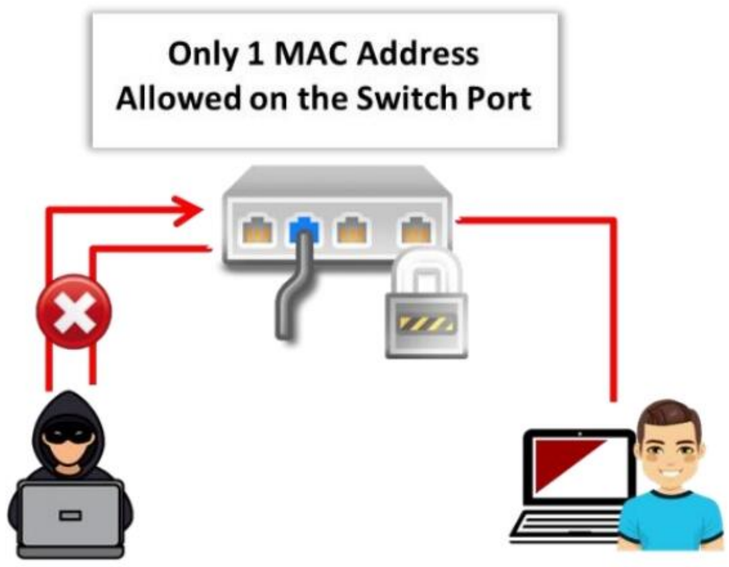


Figure 8.24: Blocking MAC flooding

Configuring Port Security on Cisco Switch

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

Steps to restrict traffic through a port by limiting and identifying MAC addresses of the stations allowed to access the port:

1. **`interface interface_id`**

   Enters interface configuration mode and enters the physical interface to configure, for example, gigabitethernet 3/1.

2. **`switchport mode access`**

   Sets the interface mode as access; an interface in the default mode (dynamic desirable) cannot be configured as a secure port.

3. **`switchport port-security`**

   Enables port security on the interface.

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

4. **`switchport port-security maximum value`**

   Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 3072; the default is 1.

5. **`switchport port-security violation {restrict | shutdown}`**

   Sets the violation mode, the action to be taken when a security violation {restrict | shutdown} is detected.

6. **`switchport port-security limit rate invalid-source-mac`**

   Sets the rate limit for bad packets.

7. **`switchport port-security mac-address mac_address`**

   Enters a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses.

8. **`switchport port-security mac-address sticky`**

   Enables sticky learning on the interface.

9. **`end`**

   Returns to privileged EXEC mode.

10. **`show port-security address`**

    `or`
    `show port-security address interface interface_id`

    Verifies your entries.

Some additional commands to configure the Cisco port security feature:

- **`switchport port-security maximum 1 vlan access`**

  Sets the maximum number of secure MAC addresses for the interface. The range is 1 to 3072. The default is 1.

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

  Sets the aging time for the secure port.

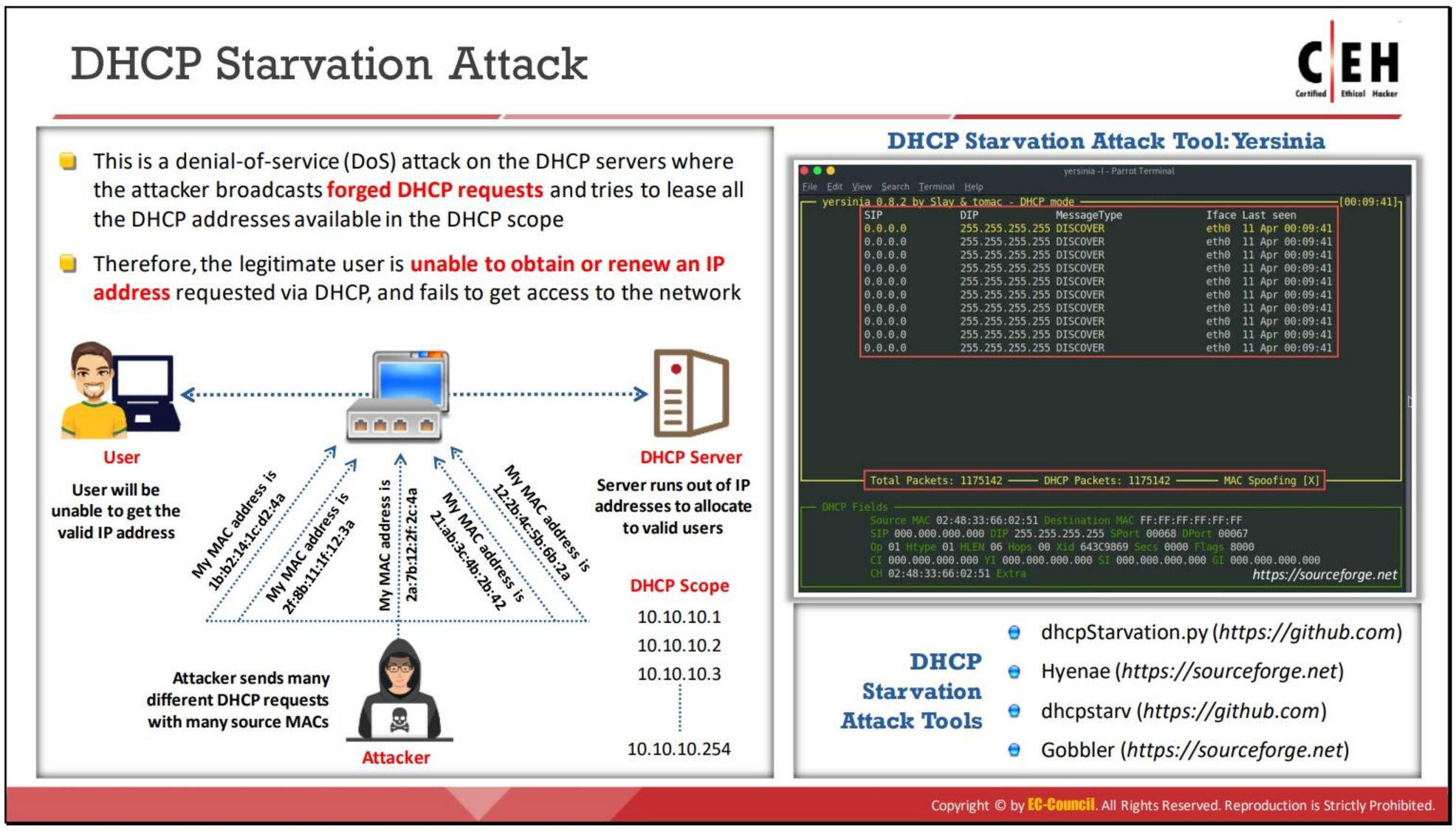
- **`switchport port-security aging type inactivity`**

  The type keyword sets the aging type as absolute or inactive.

- **`snmp-server enable traps port-security trap-rate 5`**

  Controls the rate at which SNMP traps are generated.

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



Sniffing Technique: DHCP Attacks

This section discusses various Dynamic Host Configuration Protocol (DHCP) attacks. A DHCP attack is an active sniffing technique used by the attackers to steal and manipulate sensitive data. This section describes how DHCP works, DHCP starvation attacks, tools used for starvation attacks, rogue server attacks, and different ways to defend against DHCP attacks.

How DHCP Works

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

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

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

Working of DHCP:

1. The client broadcasts a DHCPDISCOVER/SOLICIT request asking for DHCP configuration Information.
2. A DHCP-relay agent captures the client request and unicasts it to the DHCP servers available in the network.

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

3. A DHCP server unicasts DHCPOFFER/ADVERTISE, which contains the client's and server's MAC addresses.
4. The relay agent broadcasts DHCPOFFER/ADVERTISE in the client's subnet.
5. The client broadcasts DHCPREQUEST/REQUEST asking the DHCP server to provide the DHCP configuration information.
6. The DHCP server sends a unicast DHCPACK/REPLY message to the client with the IP configuration and information.

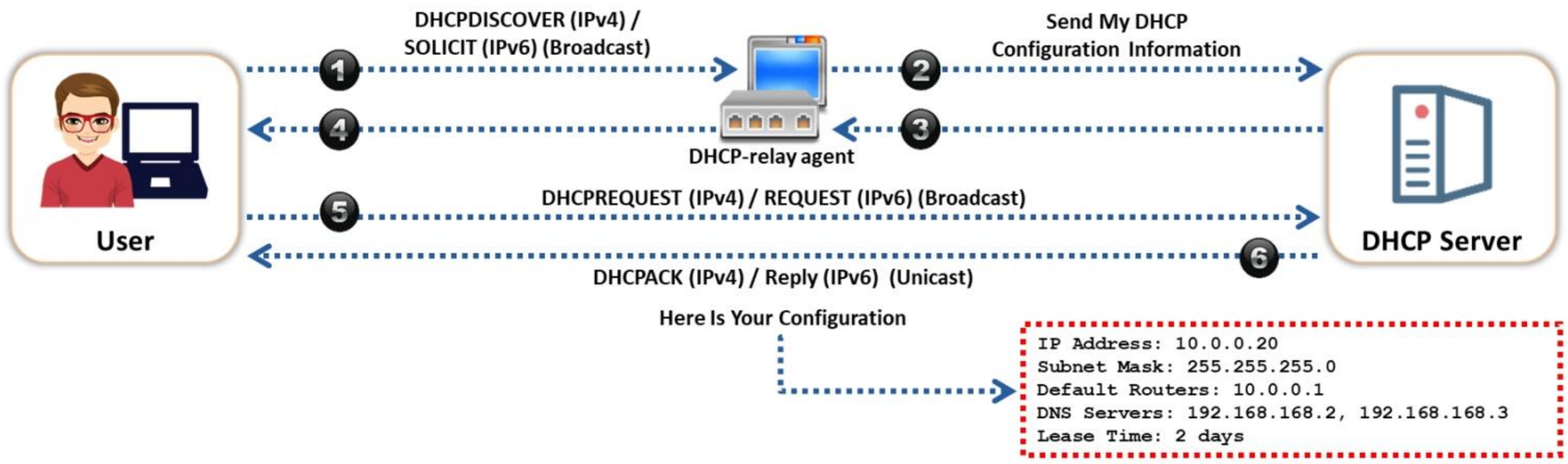


Figure 8.25: Working of DHCP

DHCP Request/Reply Messages

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

DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client broadcast to locate the available DHCP servers
DHCPOffer	Advertise	Server to client in response to DHCPDiscover with the offer of configuration parameters
DHCPRequest	Request, Confirm, Renew, Rebind	Client to servers either (a) requesting offered parameters, (b) confirming the correctness of the previously allocated address, or (c) extending the lease period
DHCPAck	Reply	Server to client with configuration parameters, including the committed network address

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

DHCPRelease	Release	Client to server relinquishing the network address and canceling the remaining lease
DHCPDecline	Decline	Client to server indicating that the network address is already in use
N/A	Reconfigure	Server to client saying 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; the client already has the 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 that the client's notion of the network address is incorrect (e.g., the client has moved to a new subnet) or the client's lease has expired

Table 8.8: DHCP request/reply messages

IPv4 DHCP Packet Format

DHCP enables communication on an IP network by configuring network devices. It assigns IP addresses and other information to computers so that they can communicate on the network in the client–server mode. DHCP has two functionalities: delivering host-specific configuration parameters and allocating network addresses to hosts.

A series of DHCP messages is used in communication between DHCP servers and DHCP clients. DHCP messages have the same format as that of Bootstrap Protocol (BOOTP) messages. This is because DHCP maintains its compatibility with BOOTP relay agents, thus eliminating the need to change the BOOTP client's initialization software to interoperate with DHCP servers.

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

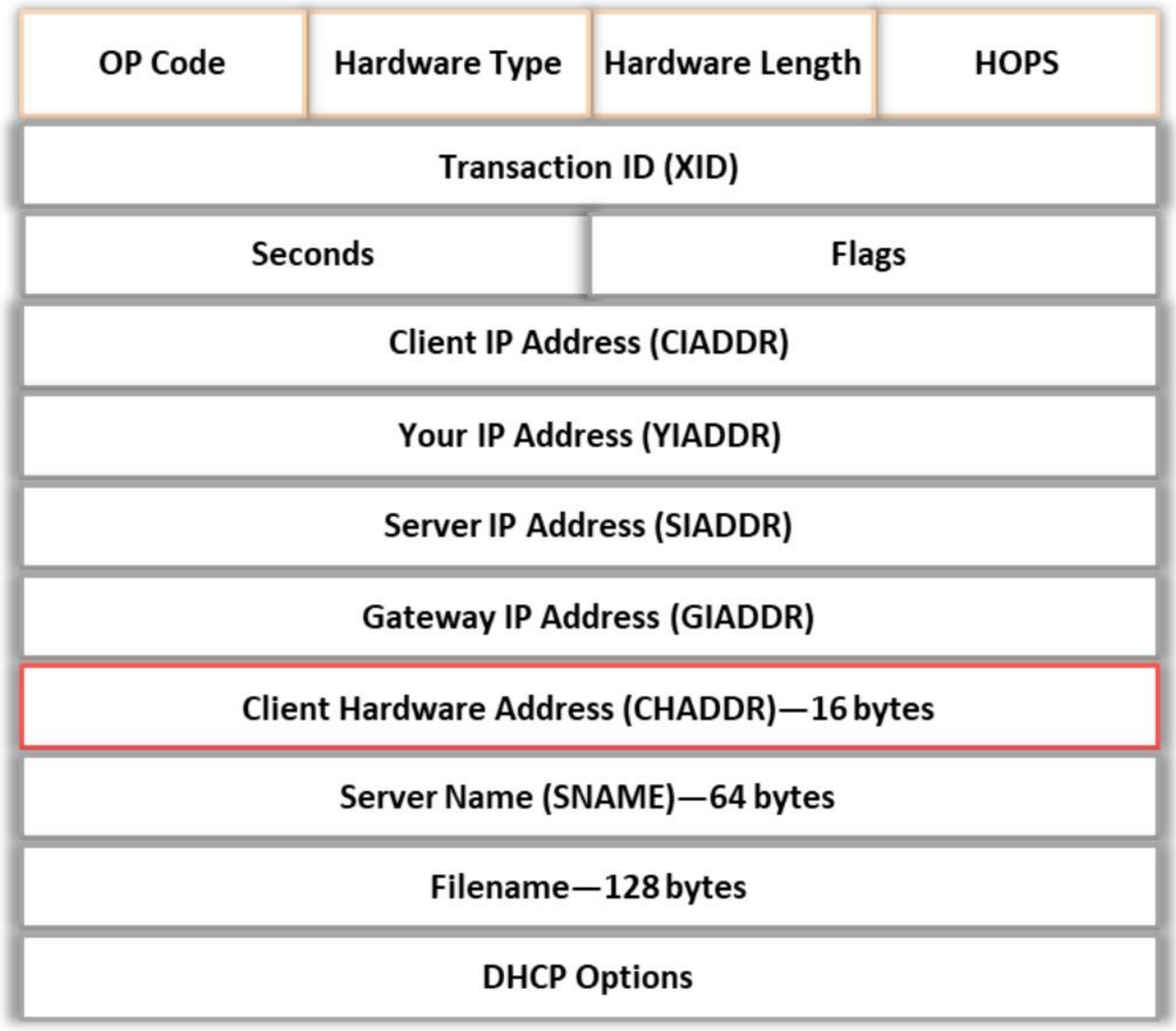


Figure 8.26: IPv4 DHCP packet format

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

FIELD	OCTETS	DESCRIPTION
Opcode	1	This field contains the message opcode that represents the message type: opcode “1” represents messages sent by the client, while “2” represents responses sent by the server
Hardware Address Type	1	Hardware address type defined at the Internet Assigned Numbers Authority (IANA) (e.g., “1” = 10 Mb Ethernet)
Hardware Address Length	1	Hardware address length in octets
Hops	1	In general, the DHCP clients set the value to “0”; however, optionally used to count the number of relay agents that forwarded the message
Transaction ID (XID)	4	A random number is chosen by the client to associate the request messages and their responses between a client and a server
Seconds	2	Seconds elapsed since the client began the address acquisition or renewal process
Flags	2	Flags set by the client; For 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	The address assigned by the DHCP server to the DHCP client

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

Server IP Address (SIADDR)	4	Server's IP address
Gateway IP Address (GIADDR)	4	The IP address of the DHCP relay agent
Client Hardware Address (CHADDR)	16	The hardware address of the client
Server Name (SNAME)	64	Optional server hostname
File Name	128	Name of the file containing BOOTP client's boot image
DHCP Options	Variable	

Table 8.9: Fields of IPv4 DHCP message

DHCP Starvation Attack

In a DHCP starvation attack, an attacker floods the DHCP server by sending numerous 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 a DoS attack. Because of this issue, valid users cannot obtain or renew their IP addresses; thus, they fail to access their network. An attacker broadcasts DHCP requests with spoofed MAC addresses with the help of tools such as Yersinia, Hyenae, and Gobbler.

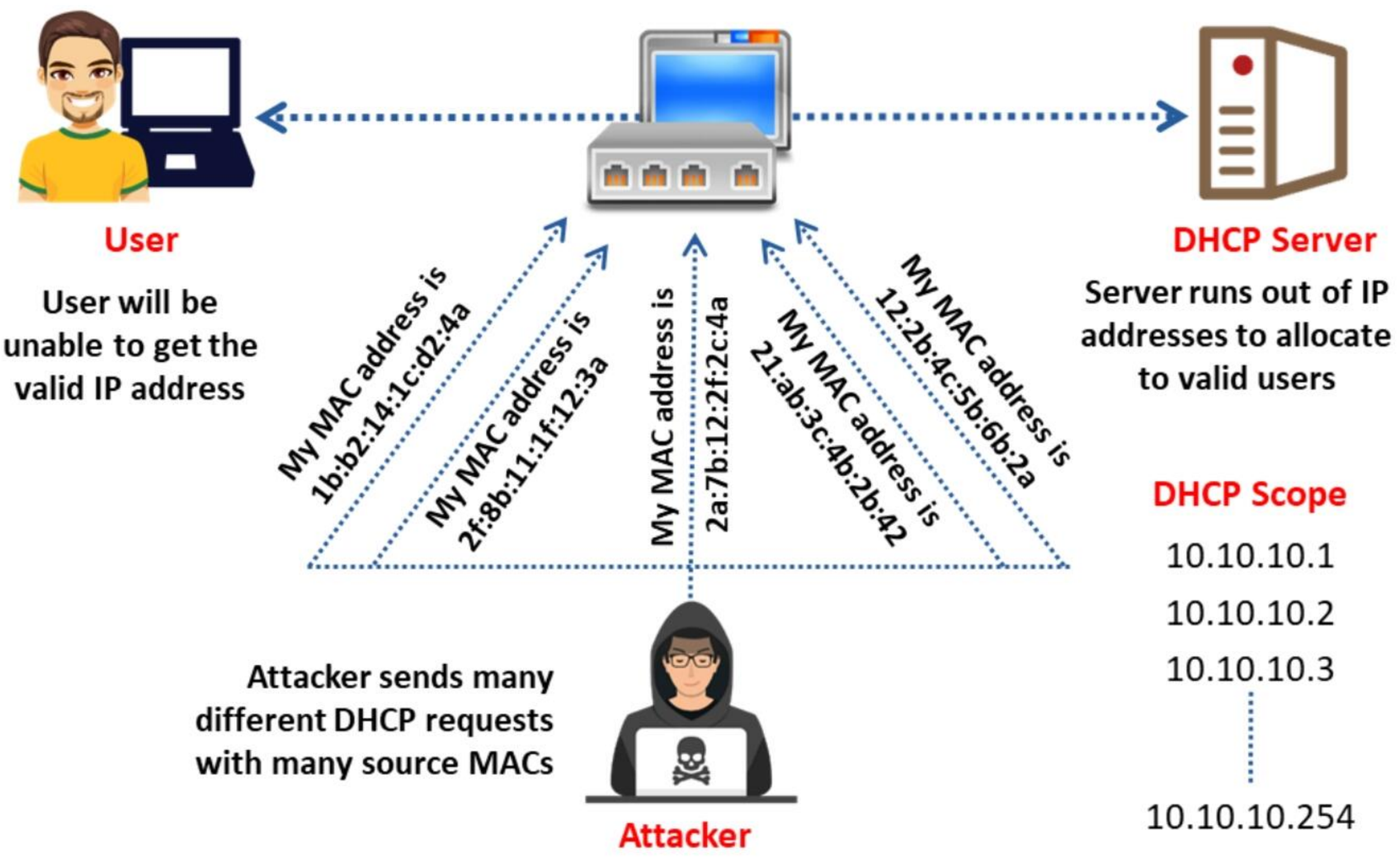


Figure 8.27: DHCP starvation attack

DHCP Starvation Attack Tools

DHCP starvation attack tools send a large number of requests to a DHCP server, leading to exhaustion of the server's address pool. Subsequently, the DHCP server is unable to allocate configurations to new clients.

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

- **Yersinia**

  Source: *https://sourceforge.net*

  Yersinia is a network tool designed to take advantage of weaknesses in different network protocols like DHCP. It pretends to be a solid framework for analyzing and testing the deployed networks and systems. As shown in the screenshot, attackers use Yersinia to perform a DHCP starvation attack on the target system.

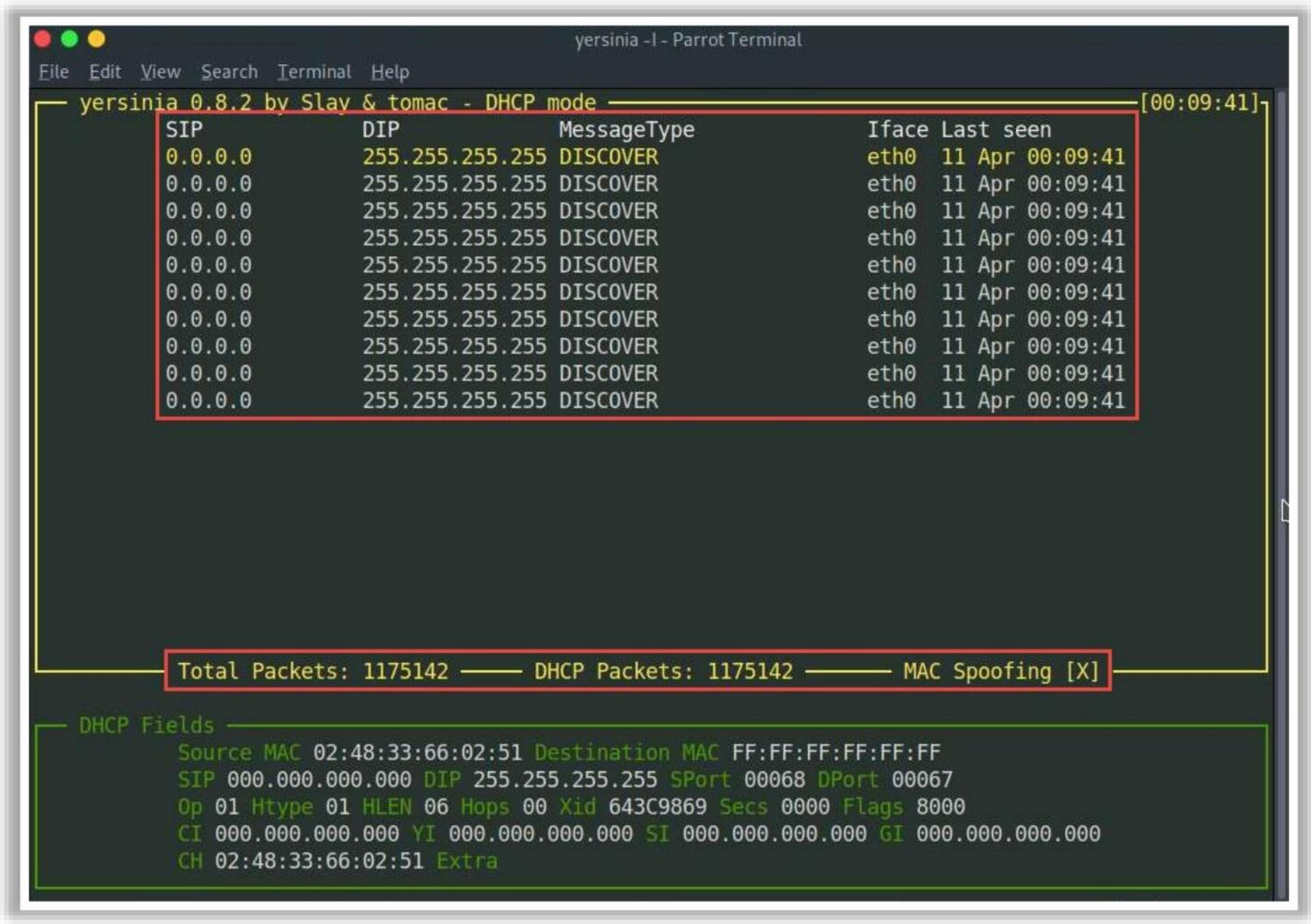
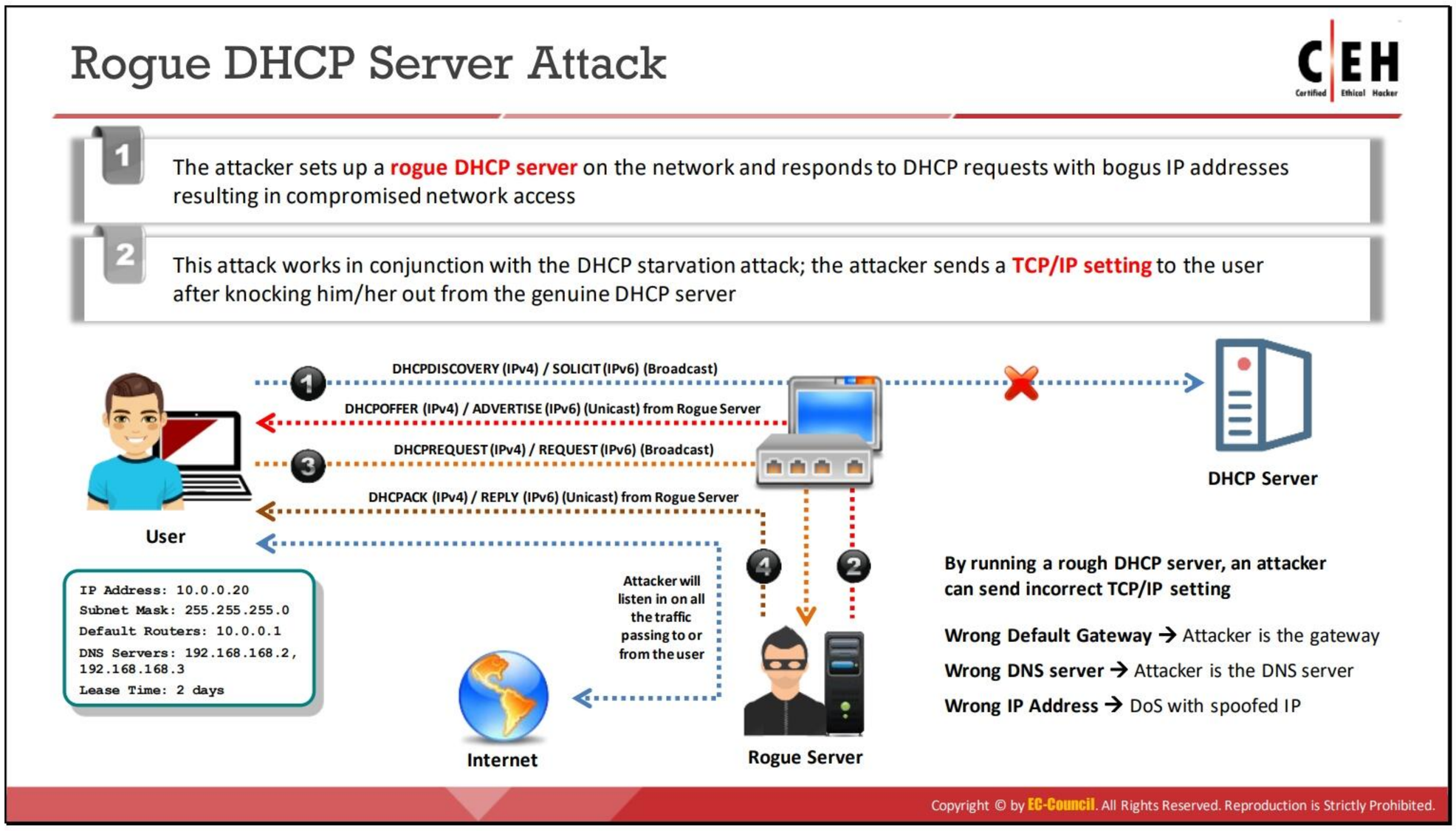


Figure 8.28: Screenshot of Yersinia

Some examples of DHCP starvation attack tools are listed below:

- dhcpStarvation.py (*https://github.com*)
- Hyenae (*https://sourceforge.net*)
- dhcpstarv (*https://github.com*)
- Gobbler (*https://sourceforge.net*)
- DHCPig (*https://github.com*)

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



Rogue DHCP Server Attack

In addition to DHCP starvation attacks, an attacker can perform MITM attacks such as sniffing. An attacker who succeeds in exhausting the DHCP server's IP address space can set up a **rogue DHCP server** on the network, which is not under the control of the network administrator. The rogue DHCP server impersonates a legitimate server and offers IP addresses and other network information to other clients in the network, acting 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, whereby 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 can respond to clients' DHCP discovery requests. Although both the rogue and actual DHCP servers respond to the request, the client accepts the response that comes first. In the case where the rogue server responds 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 a DoS attack.

The DHCP response from the attacker's rogue DHCP server may assign the IP address that serves as a client's default gateway. As a result, the attacker's IP address receives all the traffic from the client. The attacker then captures all the traffic and forwards it to the appropriate default gateway. The client thinks that everything is functioning correctly. This type of attack is difficult for the client to detect for long periods.

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

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

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

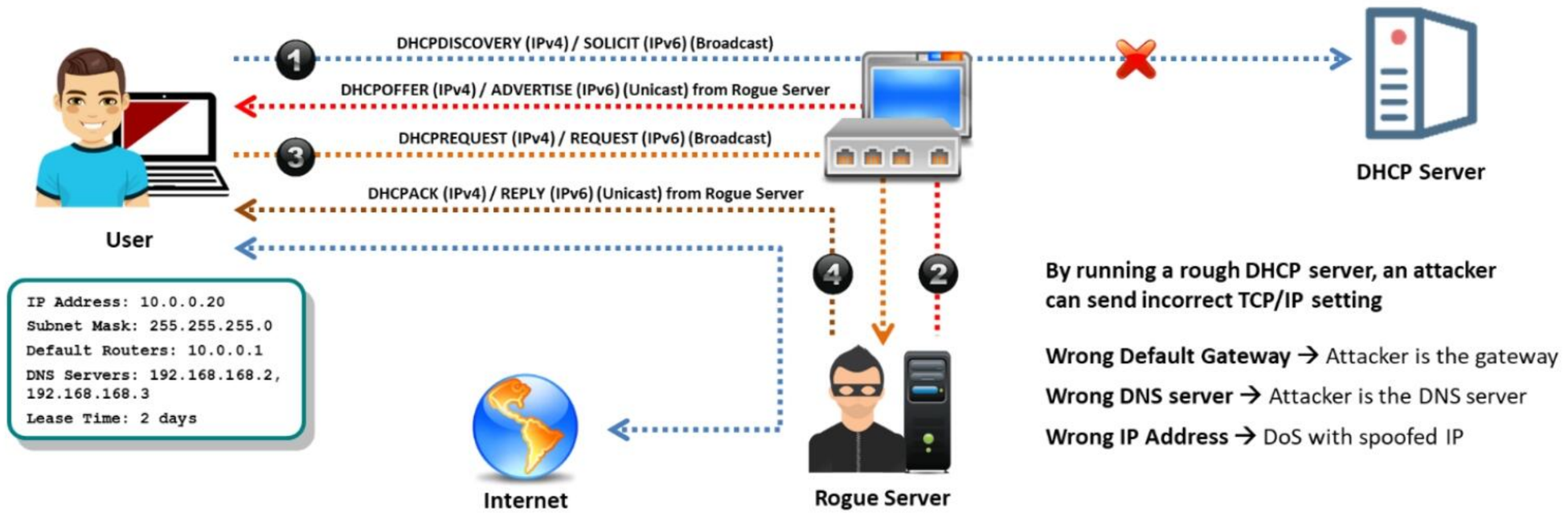


Figure 8.29: Rogue DHCP server attack

DHCP Attack Tools

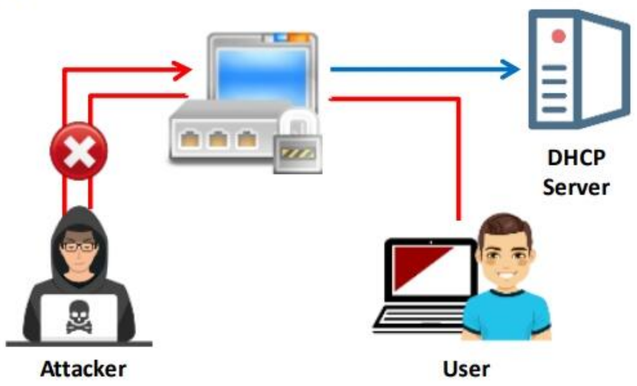
Some additional DHCP attack tools are listed below:

- mitm6 (*https://github.com*)
- DHCPwn (*https://github.com*)
- DHCPig (*https://github.com*)

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

How to Defend Against DHCP Starvation and Rogue Server Attacks

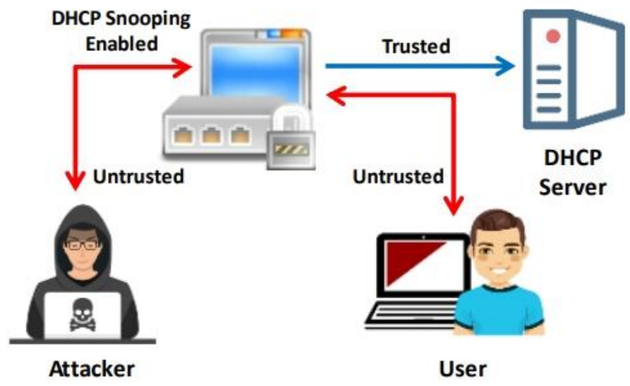
- **Enable port security** to defend against DHCP starvation attacks
  - Configuring the MAC limit on the switch's edge ports drops the packets from further MACs once the limit is reached



IOS Switch Commands

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

- Enable **DHCP snooping**, which allows the switch to accept a DHCP transaction directed from a trusted port



IOS Global Commands

- **`ip dhcp snooping`** → this turns on DHCP snooping
- **`ip dhcp snooping vlan 4,104`** → this configures VLANs to snoop
- **`ip dhcp snooping trust`** → this configures interface as trusted

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

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

How to Defend Against DHCP Starvation and Rogue Server Attacks (Cont'd)

MAC Limiting Configuration on Juniper Switches

- **`set interface ge-0/0/1 mac-limit 3 action drop`**
- **`set interface ge-0/0/2 mac-limit 3 action drop`**
- **`show`**

```
interface ge-0/0/1.0 {
mac-limit 3 action drop;
}
interface ge-0/0/2.0 {
mac-limit 3 action drop;
}
```

- **`show ethernet-switching table`**

Configuring DHCP Filtering on a Switch

- Enable DHCP filtering for the switch:

```
config
<IP address> dhcp filter
exit
exit
```

- Enable DHCP filtering for an interface:

```
config
interface 0/11
<IP address> dhcp filter trust
exit
exit
```

- Show the DHCP filtering configuration:

```
show <IP address> dhcp filtering
```

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

How to Defend Against DHCP Starvation and Rogue Server Attacks

Defend Against DHCP Starvation

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

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

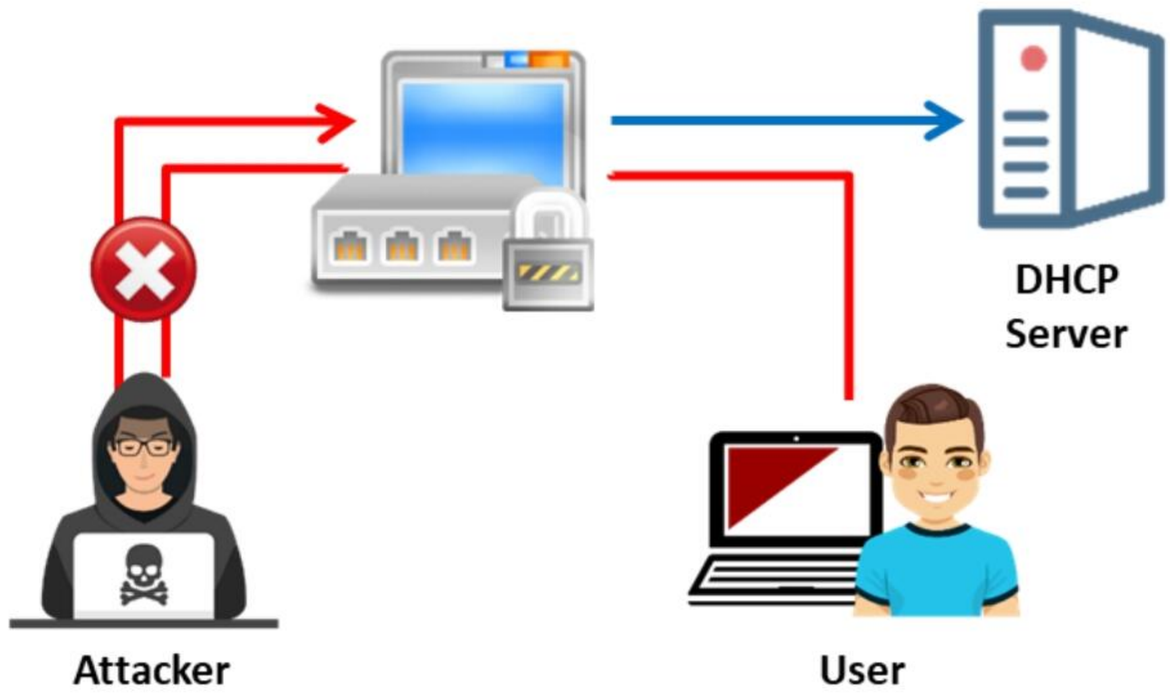


Figure 8.30: Defending against a DHCP starvation attack

Internetwork Operating System (IOS) Switch Commands

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

- **`switchport port-security`**

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

- **`switchport port-security maximum 1`**

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

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

- **`switchport port-security violation restrict`**

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

  The **`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`**

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

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

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

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

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

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

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

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

Defend Against Rogue Server Attack

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

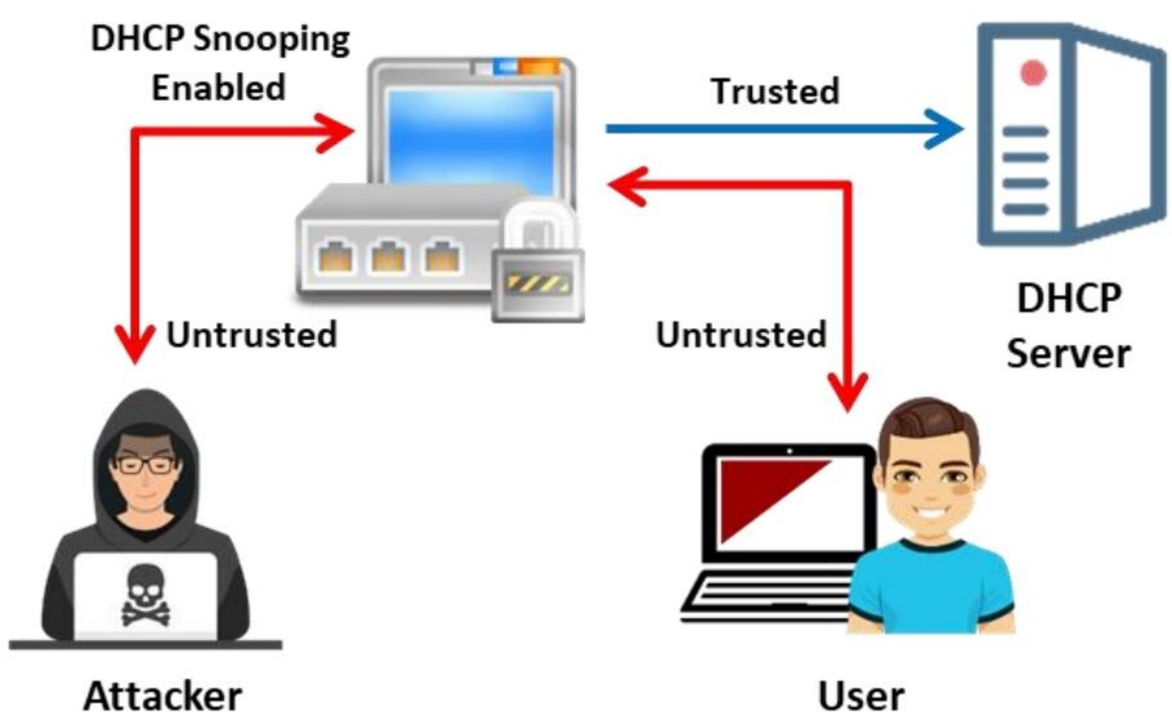


Figure 8.31: Defending against a rogue server attack

IOS Global Commands

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

Steps to configure DHCP snooping:

1. **`ip dhcp snooping`**

   Enables DHCP snooping globally.

2. **`ip dhcp snooping vlan number [number] | vlan {vlan range}]`**

   Enables or disables DHCP snooping on one or more VLANs. For example:

   `ip dhcp snooping vlan 4,104`

3. **`ip dhcp snooping trust`**

   Configures the interface as trusted or untrusted.

4. **`ip dhcp snooping limit rate`**

   Configures the number of DHCP packets per second (pps) that an interface can receive.

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

5. **`end`**

   Exits configuration mode.

6. **`show ip dhcp snooping`**

   Verifies the configuration.

Additional DCHP snooping command:

- **`no ip dhcp snooping information option`**

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

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

MAC Limiting Configuration on Juniper Switches

Source: *https://www.juniper.net*

Consider that three devices are connected to an enterprise switch and are trusted devices with the interfaces **ge-0/0/1**, **ge-0/0/2**, and **ge-0/0/3**. Further, consider a DHCP server with the interface **ge-0/0/8** connected in the background, resulting in a total of 4 interfaces connected to the switch.

- Run the following commands on the switch terminal to apply quick MAC limiting:

```
set interface ge-0/0/1 mac-limit 3 action drop
set interface ge-0/0/2 mac-limit 3 action drop
```

Alternatively, follow the steps below to apply a MAC limiting configuration.

- **Step 1**: Run the following command to configure a MAC limit of 3 on the first device's interface **ge-0/0/1** and specify the action if the limit is exceeded:

```
set interface ge-0/0/1 mac-limit 3 action drop
```

- **Step 2:** Run the following command to configure a MAC limit of 3 on **the** second device's interface **ge-0/0/2** and specify the action if the limit is exceeded:

```
set interface ge-0/0/2 mac-limit 3 action drop
```

- **Step 3**: Execute the following commands to view the outcome of the above MAC limiting configurations:

```
show
interface ge-0/0/1.0 {
    mac-limit 3 action drop;
}
interface ge-0/0/2.0 {
```


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

```
        mac-limit 3 action drop;
    }
```

- **Step 4:** Run the following command to verify the MAC limiting process on the specific switch:

```
show ethernet-switching table
```

Configuring DHCP Filtering on a Switch

Source: *https://docs.oracle.com*

DHCP filtering allows the administrators to determine whether traffic is being forwarded between trusted nodes. When DHCP filtering is applied, the corresponding switch checks the legitimacy of packets/messages before forwarding them to the client. With such filtering, the client can receive the port number and IP address from the legitimate DHCP server.

- Run the following commands to enable DHCP filtering for the switch:

```
config
      <IP address> dhcp filter
      exit
exit
```

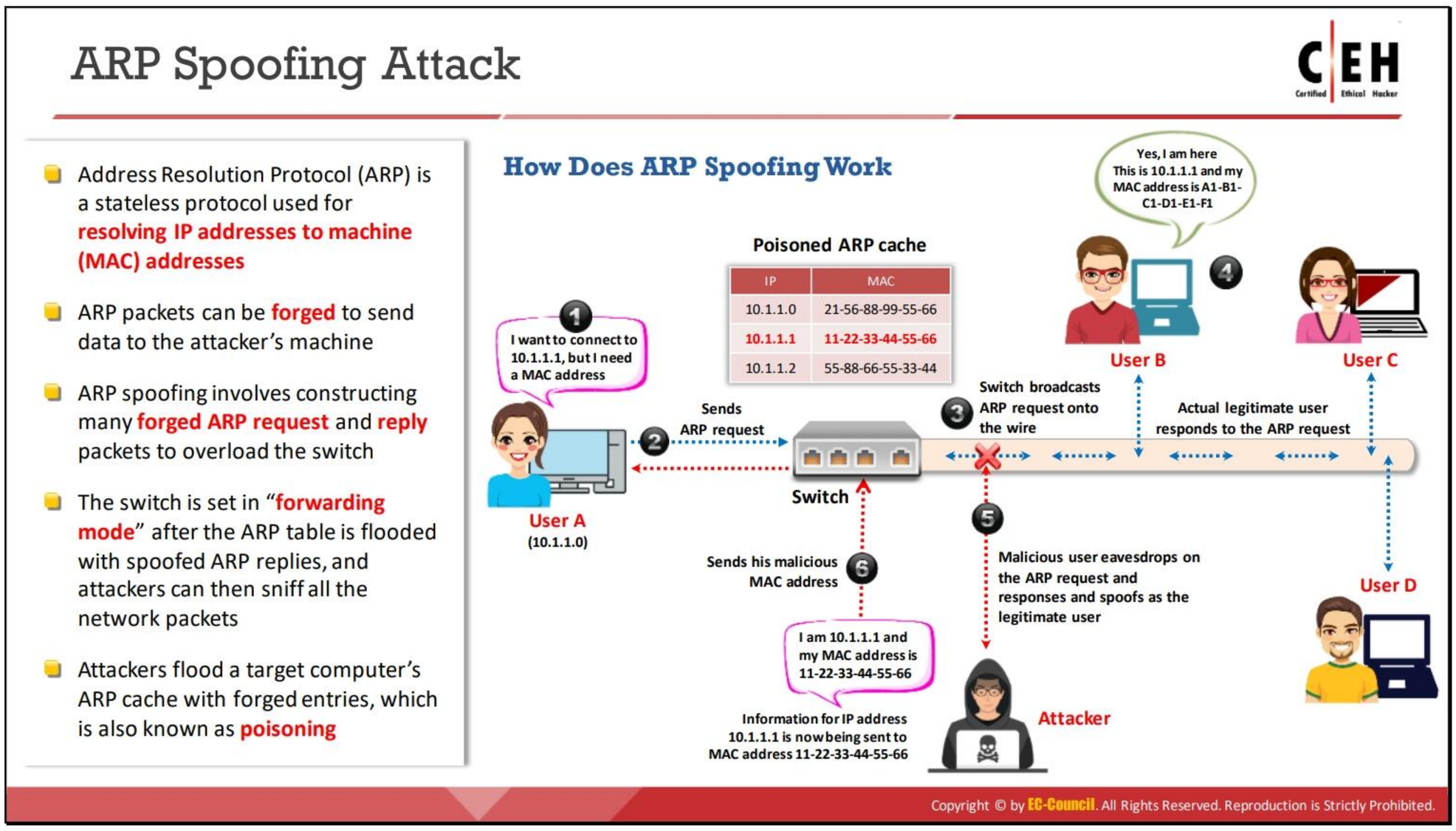
- Run the following commands to enable DHCP filtering for an interface:

```
config
      interface 0/11
            <IP address> dhcp filter trust
            exit
      exit
```

- Run the following command to show the DHCP filtering configuration:

```
show <IP address> dhcp filtering
```


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



Sniffing Technique: ARP Poisoning

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

What Is Address Resolution Protocol (ARP)?

The ARP is a stateless TCP/IP protocol that maps IP network addresses to the addresses (hardware addresses) used by a data link protocol. Using this protocol, a user can easily obtain the MAC address of any device on a network. Apart from the switch, the host machines also use the ARP protocol for obtaining MAC addresses. ARP is used by the host machine when it wants to send a packet to another device, and the host machine must mention the destination MAC address in the packet sent. Therefore, 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 an ARP table, which is generated from responses received to ARP requests. This table maps IP addresses to the corresponding MAC addresses.

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

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

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

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

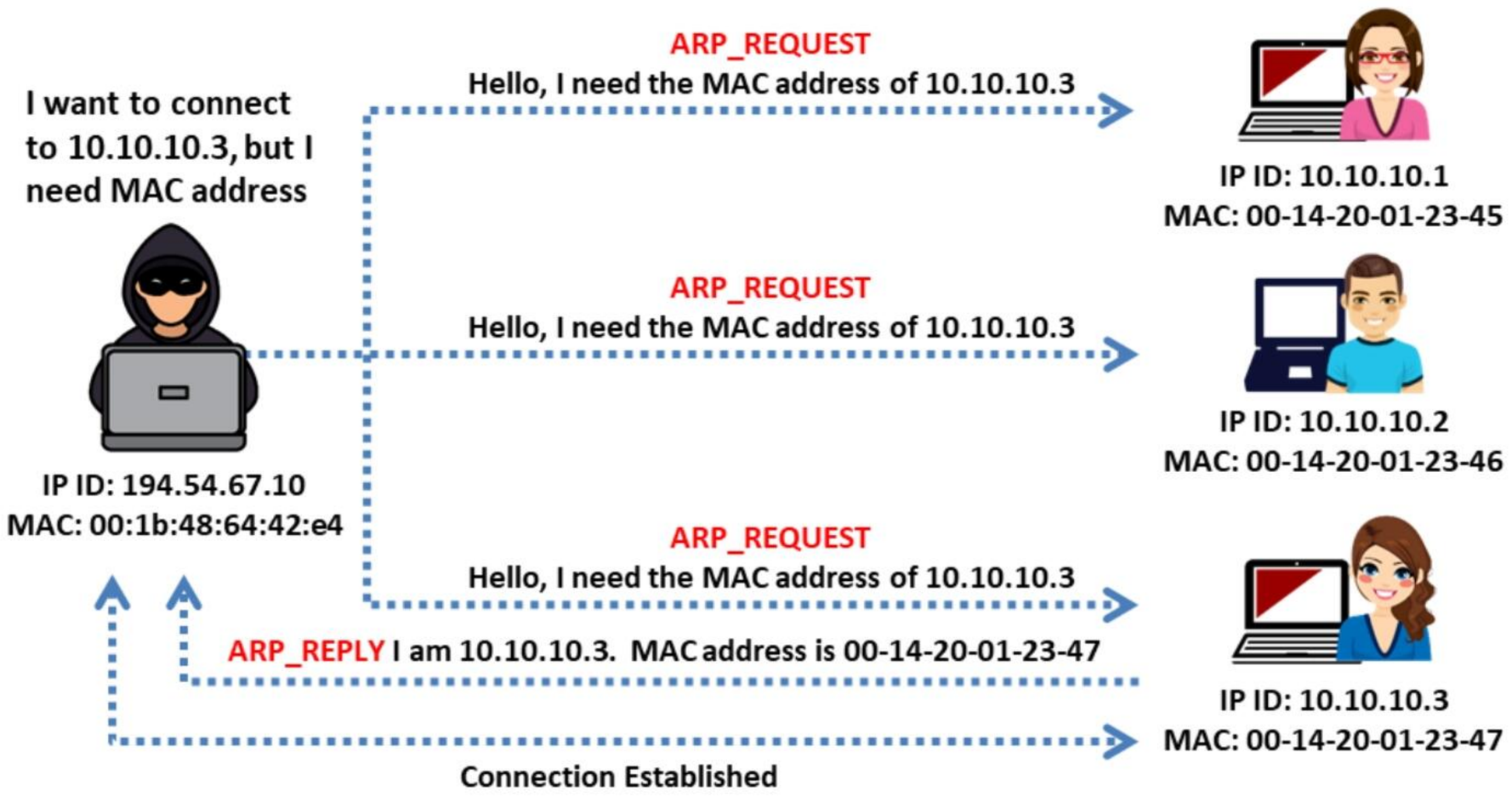


Figure 8.32: Working of ARP protocol

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

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

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

Host A queries all the hosts on the LAN. If the query were 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 a 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

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

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, these two hosts can communicate with each other.

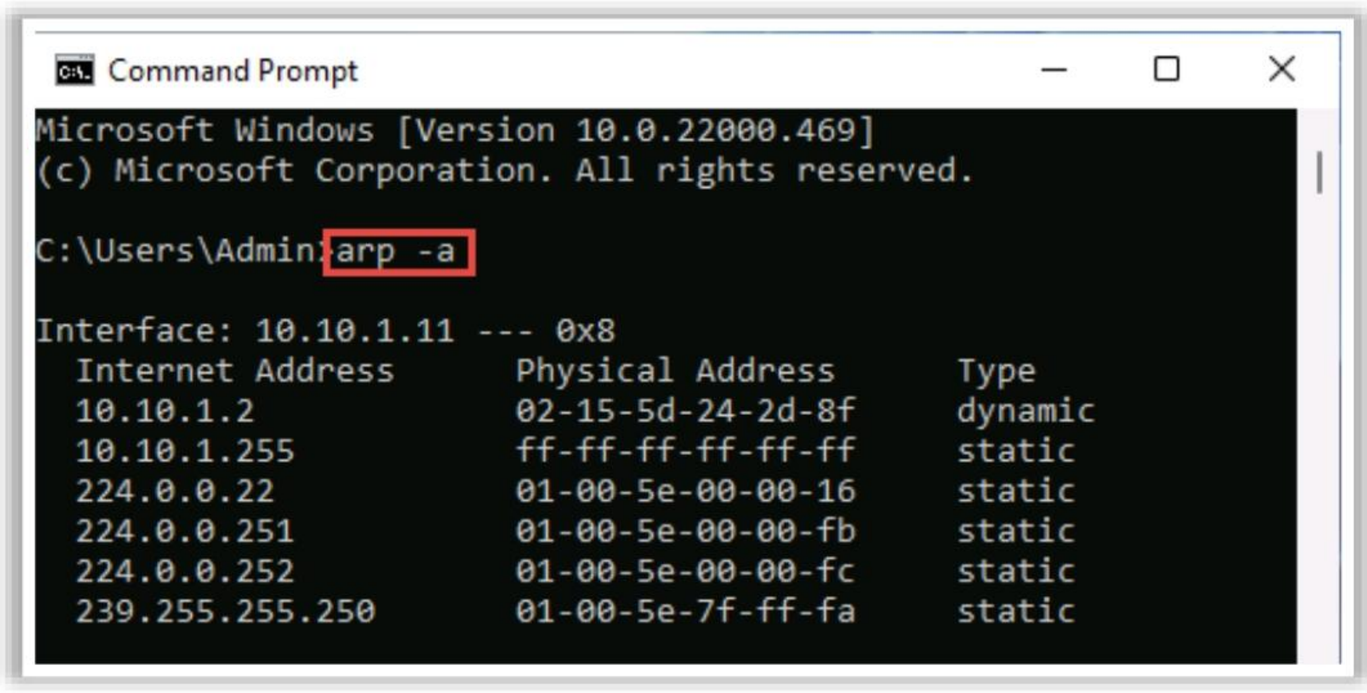


Figure 8.33: ARP cache

ARP Spoofing Attack

ARP resolves IP addresses to the MAC (hardware) address of the interface to send data. ARP packets can be forged to send data to the attacker’s machine. ARP spoofing involves constructing a large number of forged ARP request and reply packets to overload a switch. When a machine sends an ARP request, it assumes that the ARP reply will come from the right machine. ARP provides no means of verifying the authenticity of the responding device. Even systems that have not made an ARP request can accept the ARP replies 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 switch is set in forwarding mode, and the attacker intercepts all the data that flows from the victim’s machine without the victim being aware of the attack. Attackers flood a target computer’s ARP cache with forged entries, which is also known as poisoning. ARP spoofing is an intermediary for performing attacks such as DoS, MITM, and session hijacking.

How does ARP Spoofing Work?

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

ARP spoofing is a method of attacking an Ethernet LAN. It succeeds by changing the IP address of the attacker’s computer to that of the target computer. A forged ARP request and reply

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

packet can 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. The attacker can also launch a DoS attack by associating a non-existent MAC address to the IP address of the gateway; alternatively, the attacker may sniff the traffic passively and then forward it to the target destination.

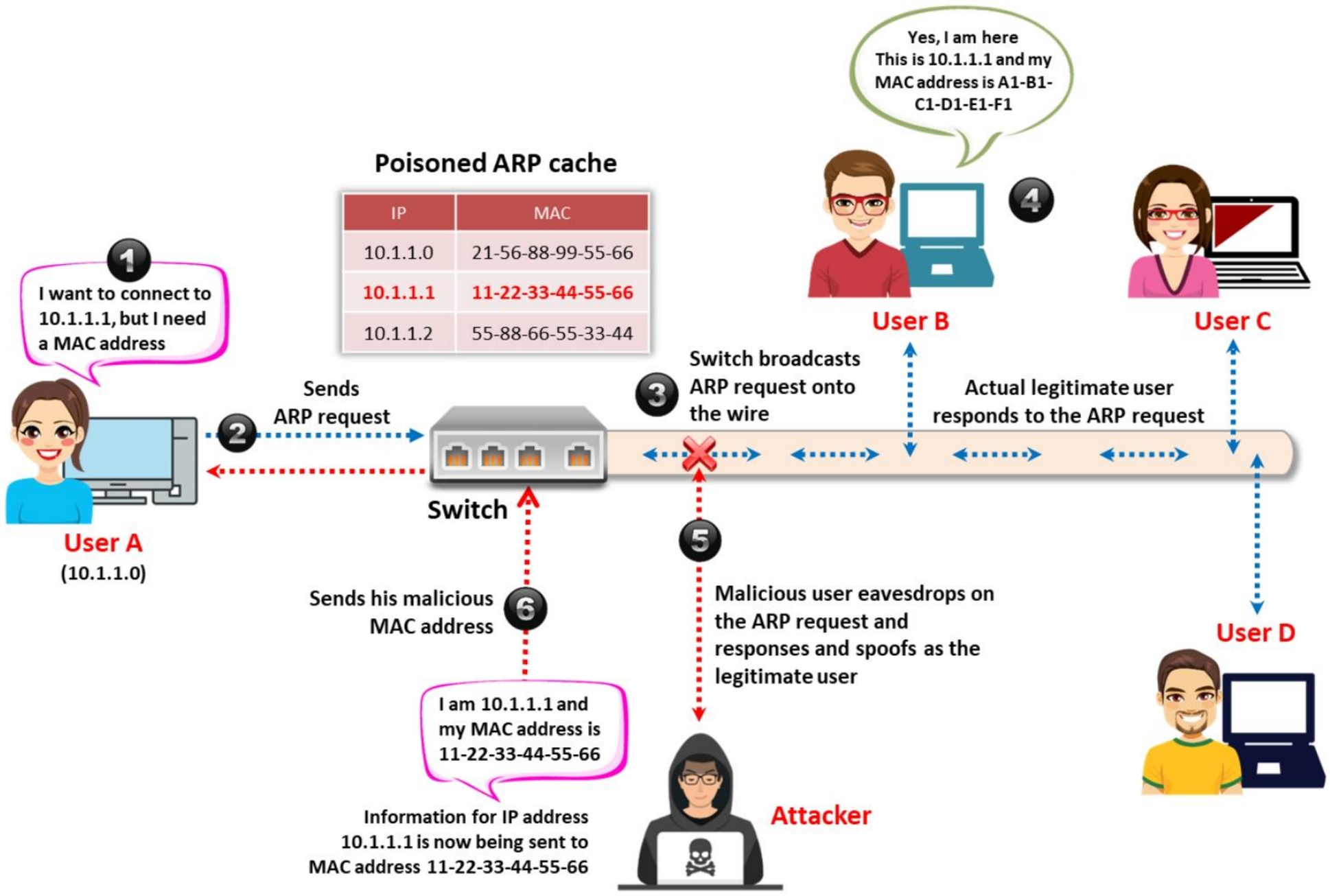
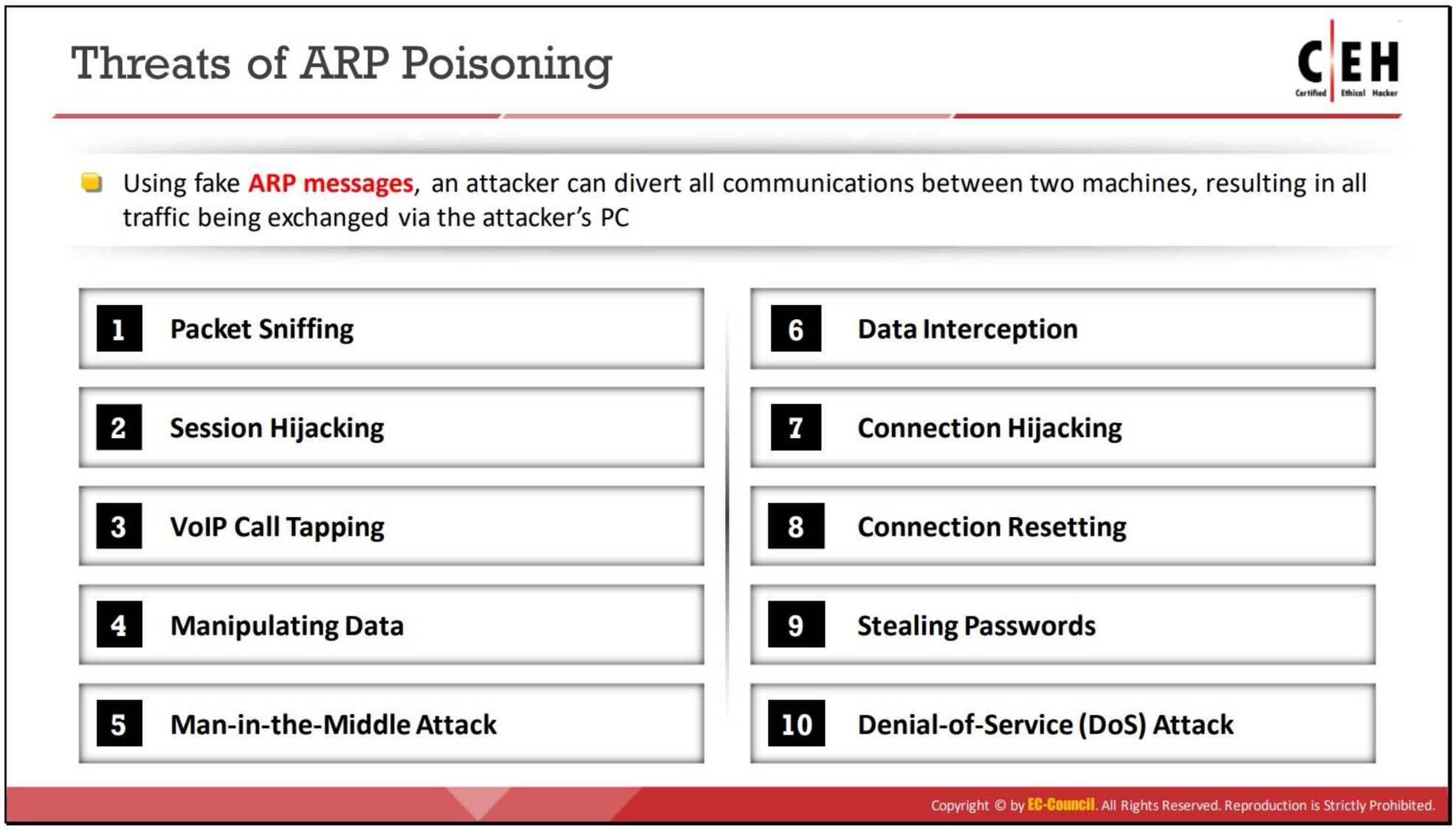


Figure 8.34: Working of an ARP spoofing attack

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



Threats of ARP Poisoning

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

The threats of ARP poisoning include:

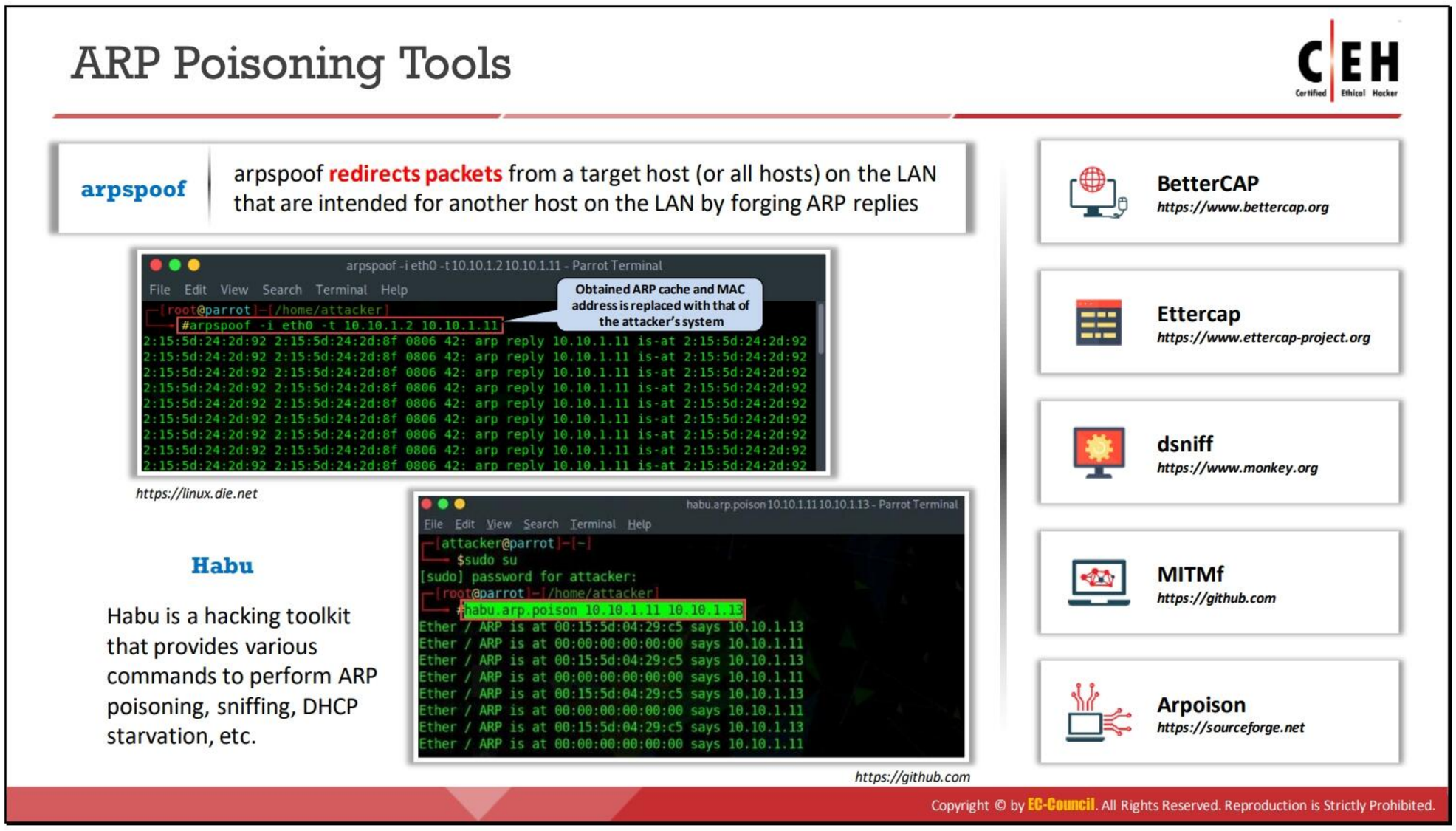
- **Packet Sniffing**: Sniffs traffic over a network or a part of the network.
- **Session Hijacking**: Steals valid session information and uses it to gain unauthorized access to an application.
- **VoIP Call Tapping**: Uses port mirroring, which allows the VoIP call tapping unit to monitor all network traffic, and picks only the VoIP traffic to record by MAC address.
- **Manipulating Data**: ARP spoofing allows attackers to capture and modify data, or stops the flow of traffic.
- **Man-in-the-Middle Attack**: An attacker performs a MITM attack where they reside between the victim and server.
- **Data Interception**: Intercepts IP addresses, MAC addresses, and VLANs connected to the switch in a network.
- **Connection Hijacking**: In a network, the hardware addresses are supposed to be unique and fixed, but a host may move when its hostname changes and use another 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 a hardware/software error. In such cases, if a host fails to initiate a connection, that host

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

should inform the Address Resolution module to delete its information. The reception of data from that host will reset a connection timeout in the ARP entry used to transmit data to that host. This entry in the ARP module is deleted if the host does not send any information for a certain period of time.

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

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



ARP Poisoning Tools

- **arpspoof**

  Source: *https://linux.die.net*

  arpspoof redirects packets from a target host (or all hosts) on the LAN that are intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.

  Syntax:

  ```
  arpspoof –i [Interface] –t [Target Host]
  ```

  As shown in the screenshot, attackers use the arpspoof tool to obtain the ARP cache; then, the MAC address is replaced with that of an attacker's system. Therefore, any traffic flowing from the victim to the gateway will be redirected to the attacker's system.

  Further, an attacker can issue the same command in reverse as he/she is in the middle and can send ARP replies in both directions.

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

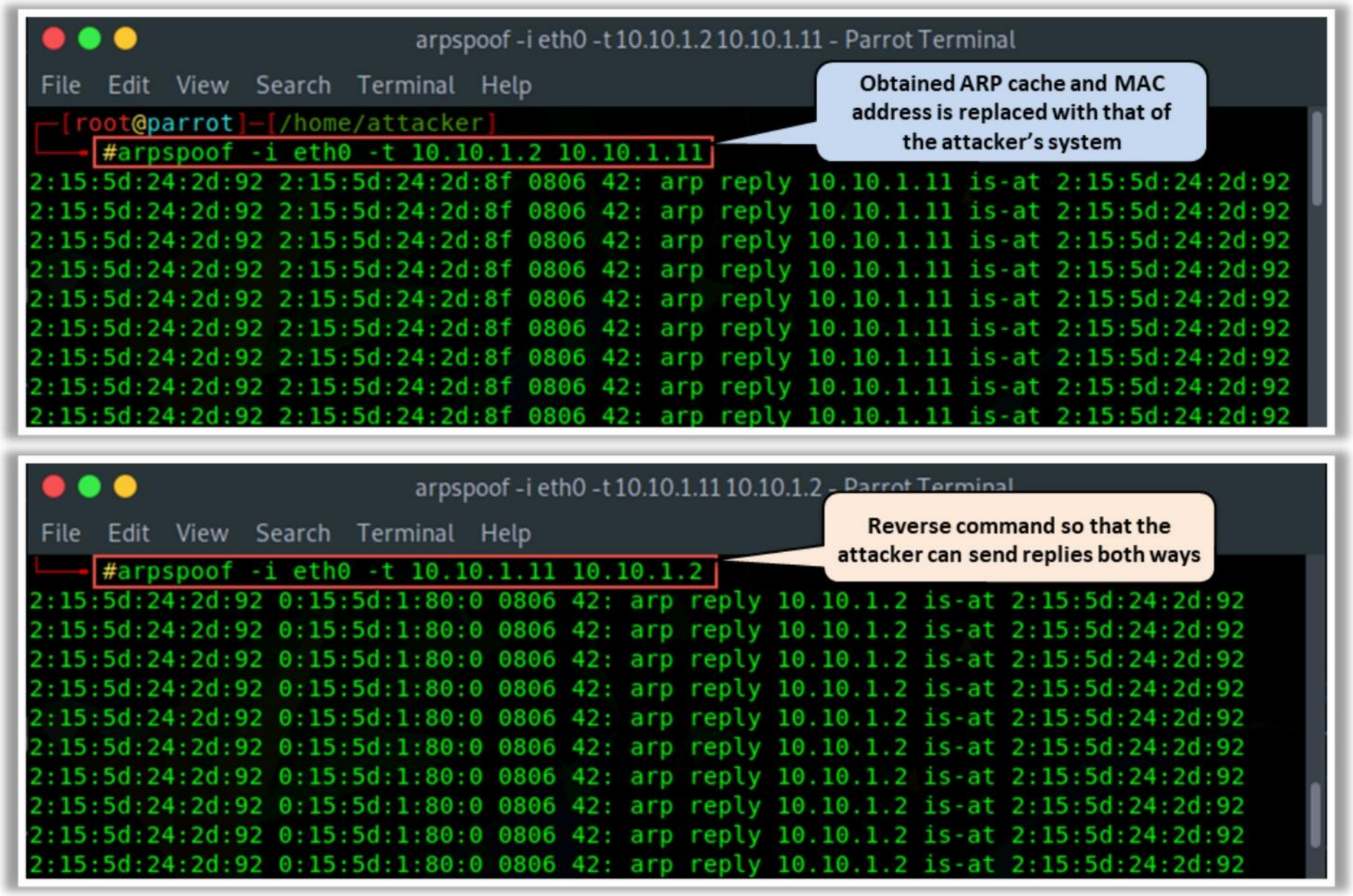


Figure 8.35: Screenshots of arpspoof

- **Habu**

  Source: *https://github.com*

  Habu is a hacking toolkit that provides various commands to perform the following attacks:

  - ARP poisoning and sniffing
  - DHCP discovery and starvation
  - Subdomain identification
  - Certificate cloning
  - TCP analysis (ISN, flags)
  - Username check on social networks
  - Web technology identification

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

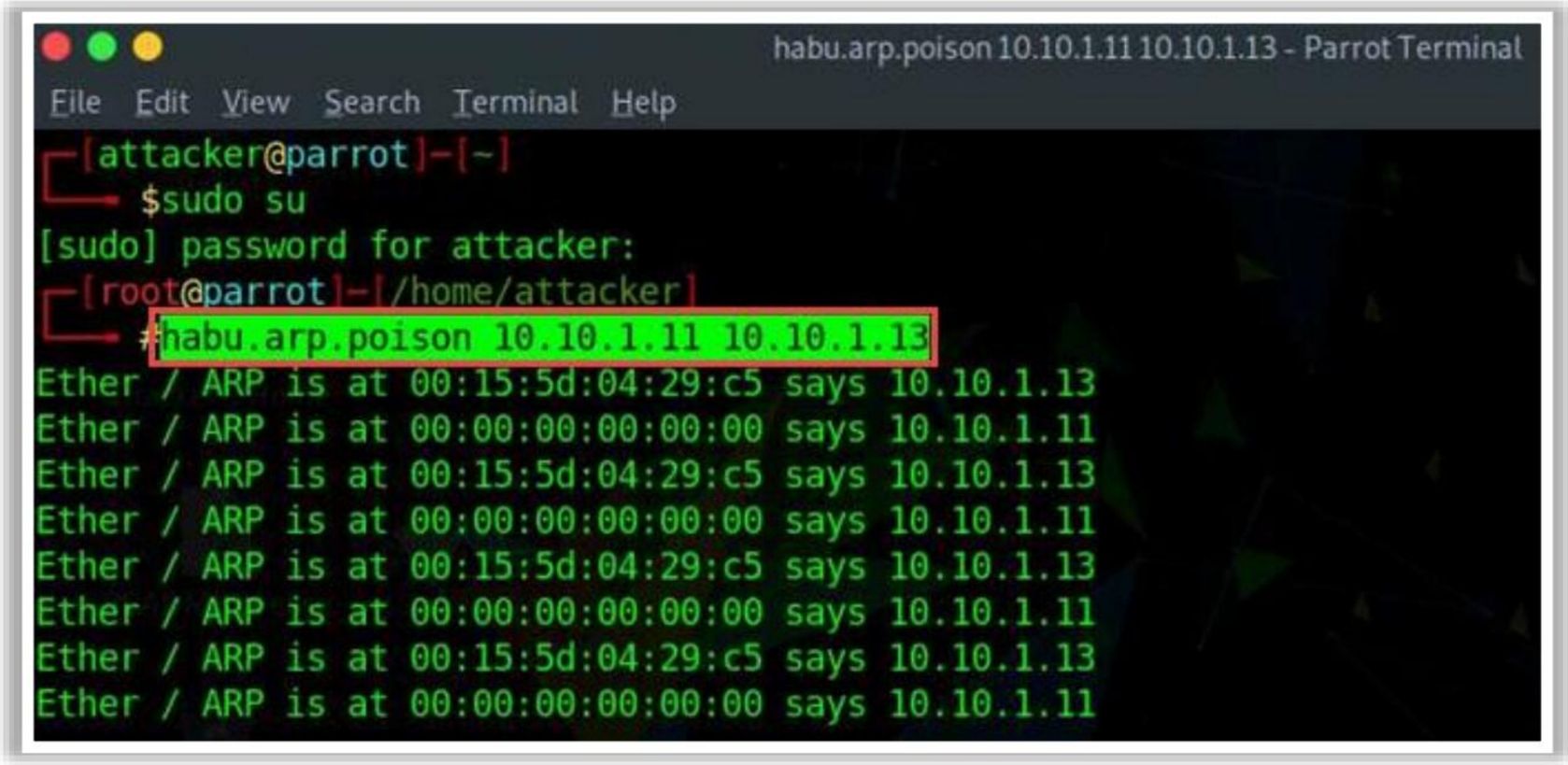
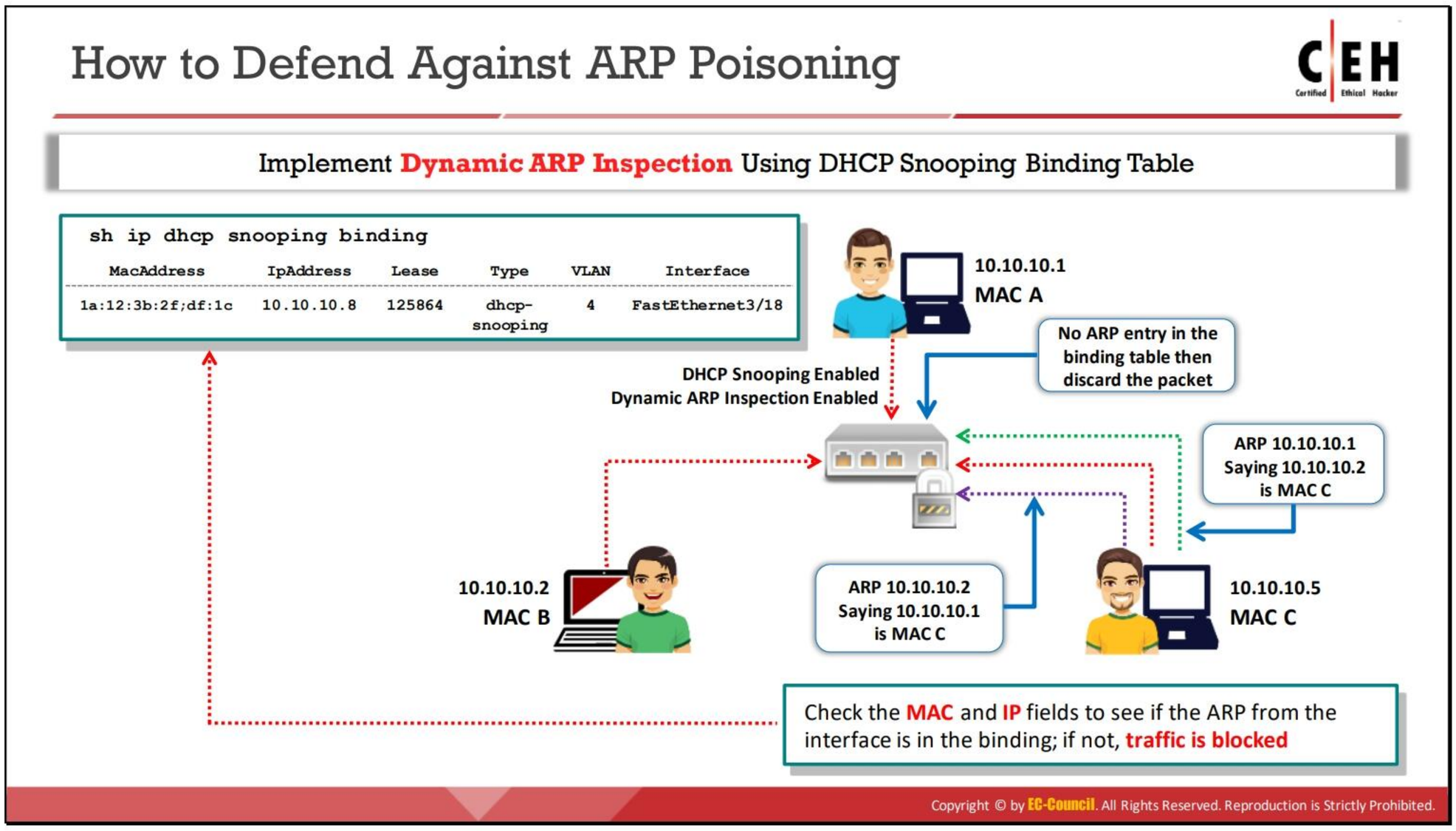


Figure 8.36: Screenshot of Habu

Some examples of ARP poisoning tools are listed below:

- BetterCAP (*https://www.bettercap.org*)
- Ettercap (*https://www.ettercap-project.org*)
- dsniff (*https://www.monkey.org*)
- MITMf (*https://github.com*)
- Arpoison (*https://sourceforge.net*)

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



How to Defend Against ARP Poisoning

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

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

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

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

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

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

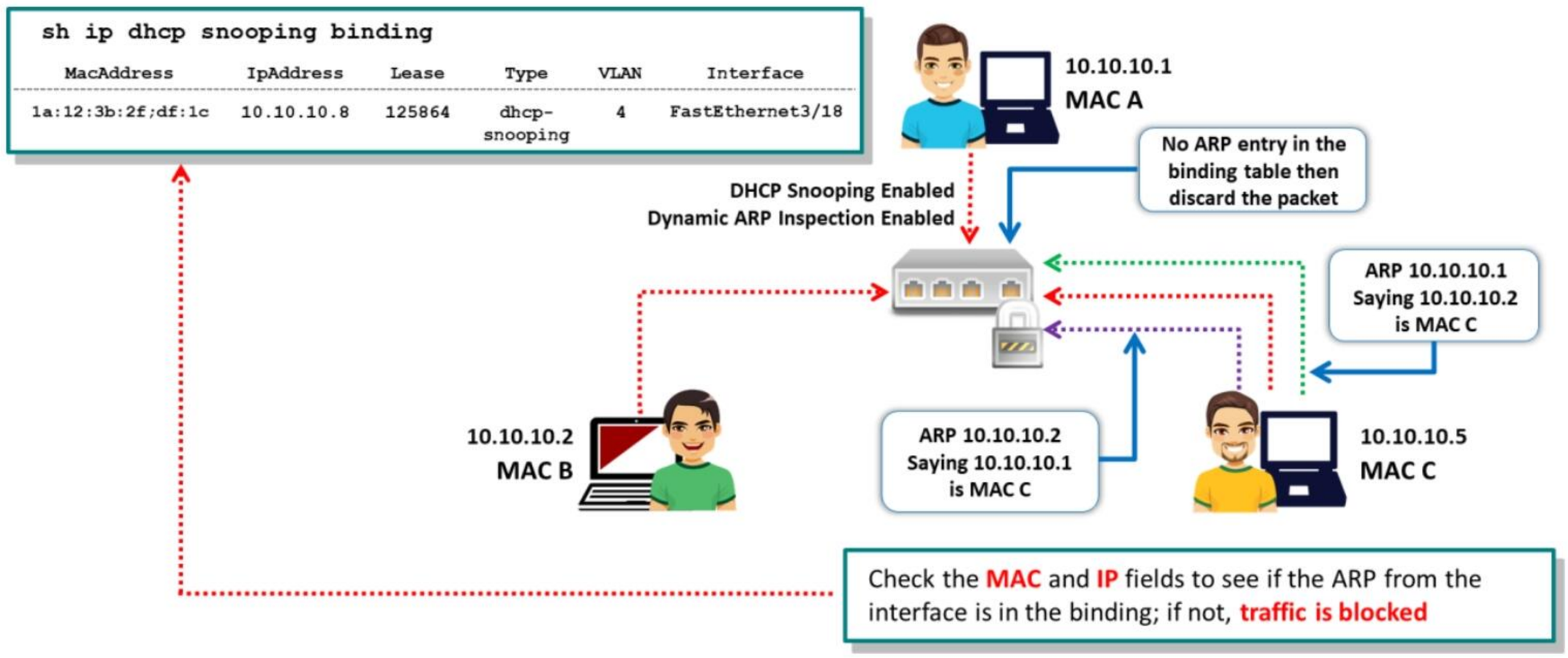
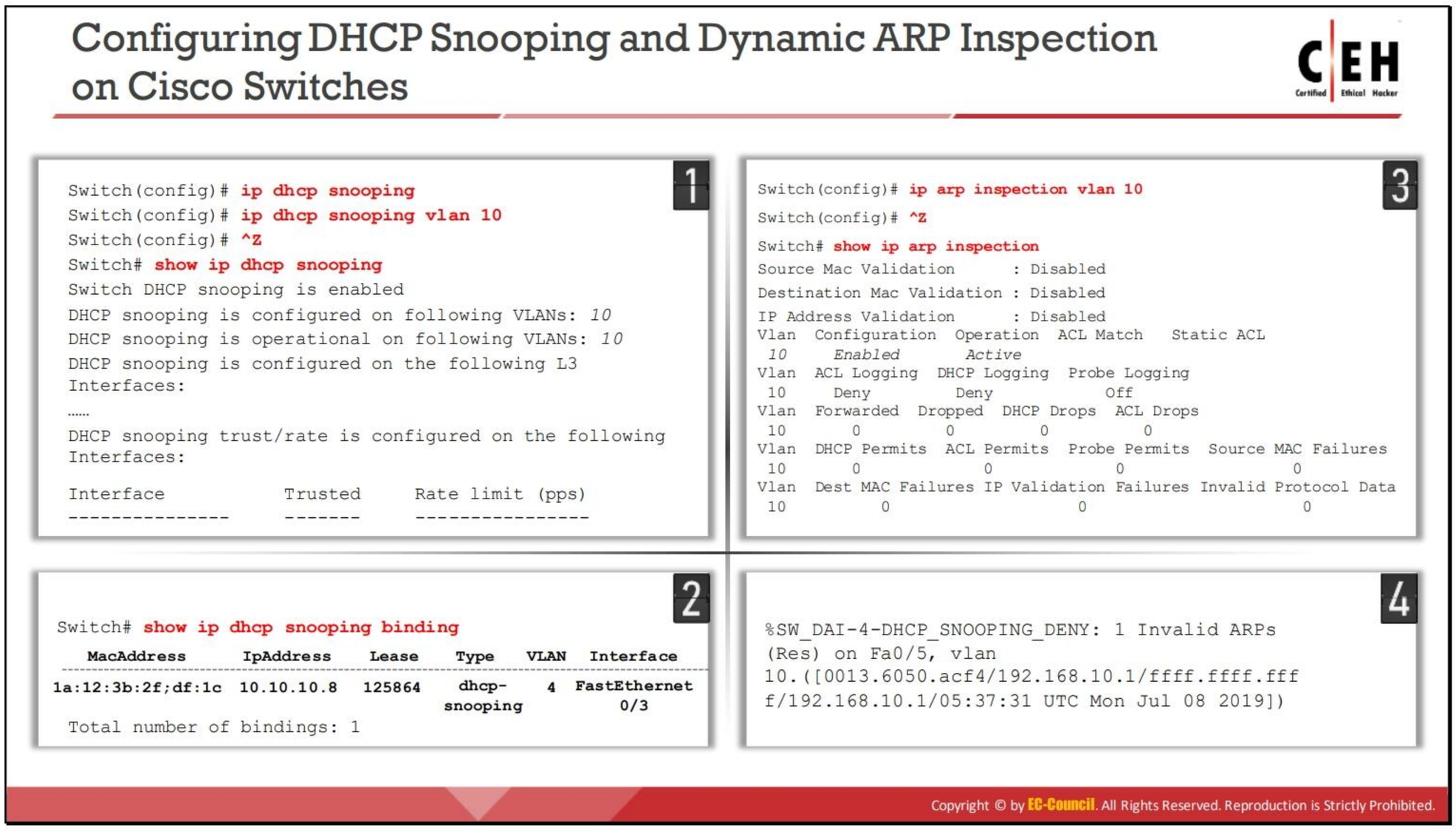


Figure 8.37: Defending against ARP poisoning

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



Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

As discussed, DHCP snooping must be enabled before enabling 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 2 segment and track IP addresses to switch port mapping.

To configure DHCP snooping on a Cisco switch, ensure DHCP snooping is enabled both globally and per access VLAN. To enable DHCP snooping, execute the following commands:

Configuring DHCP snooping in global configuration mode

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

Configuring DHCP snooping for a VLAN

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

To view the DHCP snooping status

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 10
DHCP snooping is operational on following VLANs: 10
DHCP snooping is configured on the following L3 Interfaces:
.....
DHCP snooping trust/rate is configured on the following Interfaces:

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


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

If the switch is functioning only at layer 2, apply the **`ip dhcp snooping trust`** command to the layer 2 interfaces 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 view the DHCP snooping table, you have to execute the following command:

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

This displays the DHCP snooping table, which contains the MAC addresses, respective IP addresses, and total number of bindings. The following is an example of a 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 DAI for the VLAN. To enable DAI for multiple VLANs, specify a range of VLAN numbers.

Command to configure ARP inspection for a VLAN

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

Command to configure ARP inspection for a range of VLANs

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

Or

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

To view the ARP inspection status

```
Switch(config)# show ip arp inspection
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan  Configuration  Operation  ACL Match   Static ACL
 10     Enabled        Active
Vlan  ACL Logging  DHCP Logging  Probe Logging
 10     Deny                    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

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

additional validation checks. To do so, execute the command **`ip arp inspection validate`** followed by the address type.

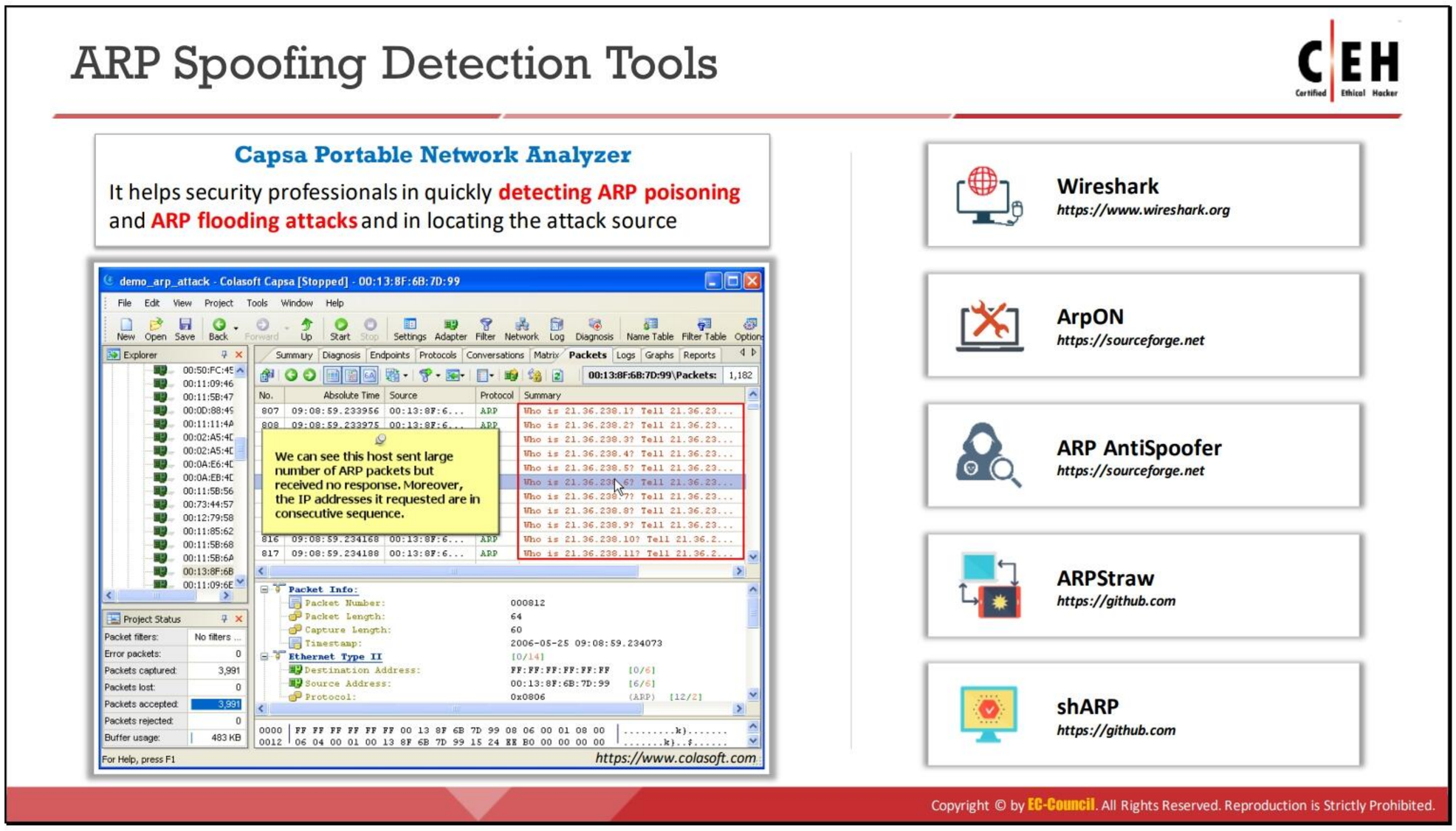
Assume that an attacker with the source IP address 192.168.10.1 connects to VLAN 10 on interface FastEthernet0/5 and sends ARP replies, pretending to be the default router for the subnet in an attempt to initiate an MITM attack. The switch with DAI enabled inspects these reply packets by comparing them 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 Tue
APR 12 2022])
```

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

```
Switch(config)# show ip arp inspection
Source Mac Validation: Disabled
Destination Mac Validation: Disabled
IP Address Validation: Disabled
Vlan  Configuration Operation     ACL Match Static ACL
----  ------------- ---------     --------- ----------
10    Enabled         Active
Vlan  ACL Logging   DHCP Logging  Probe Logging
----  -----------   ------------  -------------
10      Deny            Deny           Off


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


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



ARP Spoofing Detection Tools

- **Capsa Portable Network Analyzer**

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

  Capsa, a portable network performance analysis and diagnostics tool, provides packet capture and analysis capabilities with an easy-to-use interface, allowing users to protect and monitor networks in a critical business environment. It helps security professionals in quickly detecting ARP poisoning and ARP flooding attacks and in locating the attack source.

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

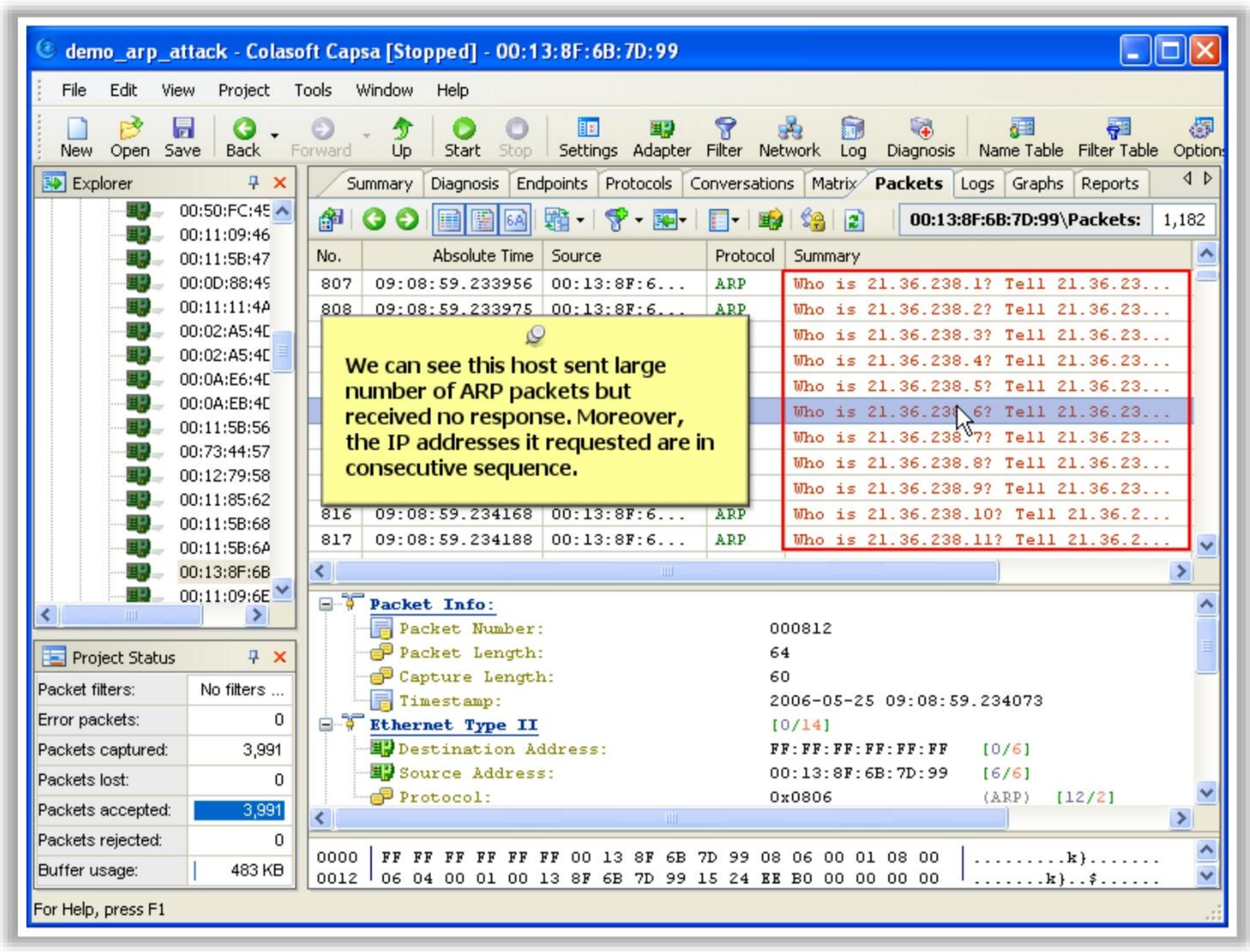
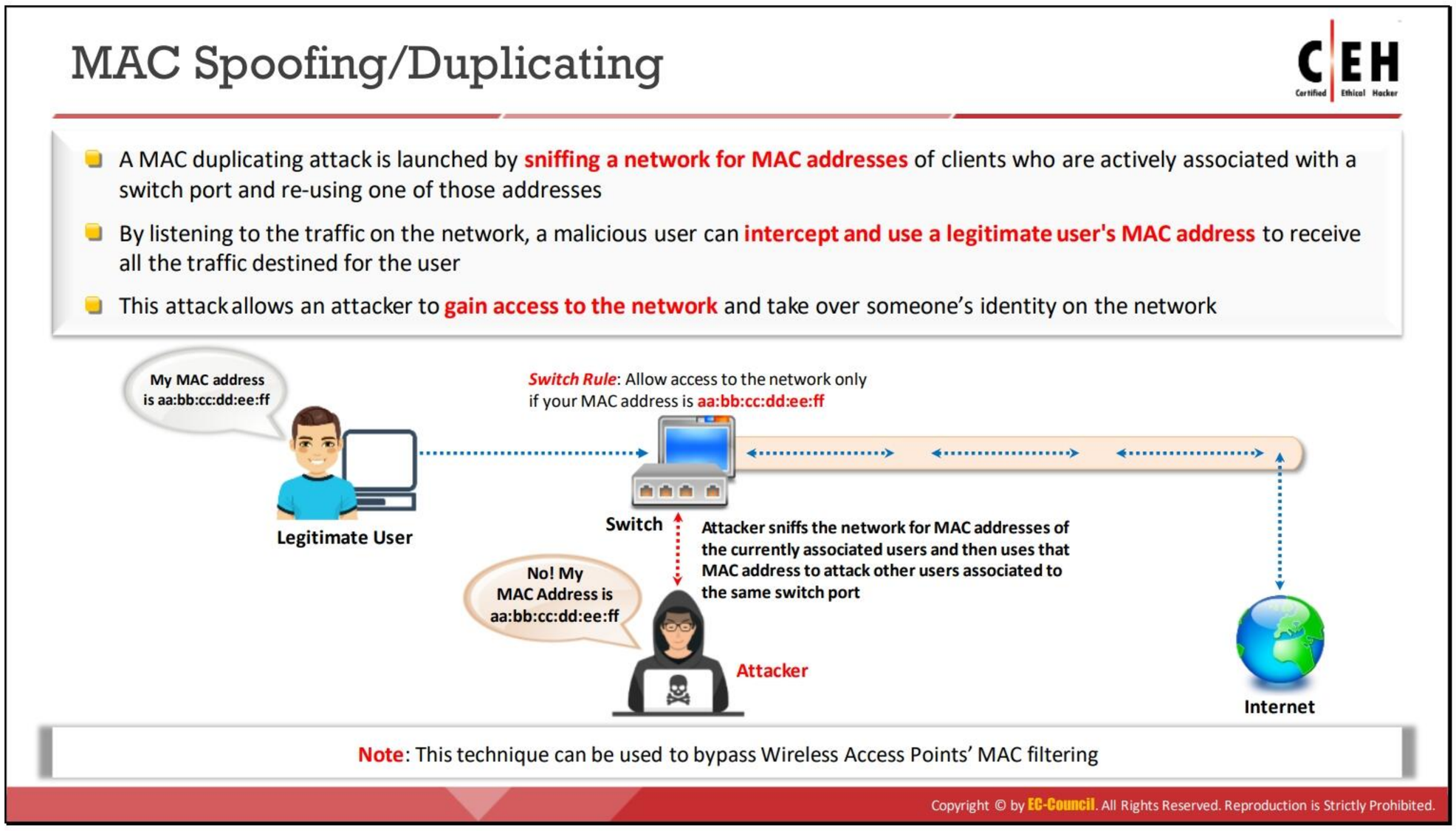


Figure 8.38: Screenshot of Capsa Portable Network Analyzer

Some examples of ARP spoofing detection tools are listed below:

- Wireshark (*https://www.wireshark.org*)
- ArpON (*https://sourceforge.net*)
- ARP AntiSpoofer (*https://sourceforge.net*)
- ARPStraw (*https://github.com*)
- shARP (*https://github.com*)

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



Sniffing Technique: Spoofing Attacks

Besides ARP spoofing, an attacker can also use MAC spoofing, IRDP spoofing, VLAN hopping, and STP attacks to sniff the traffic of a target network. This section describes spoofing techniques that help attackers to steal sensitive information. This section also explains how to defend against MAC spoofing, VLAN hopping, and STP attacks.

MAC Spoofing/Duplicating

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

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

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

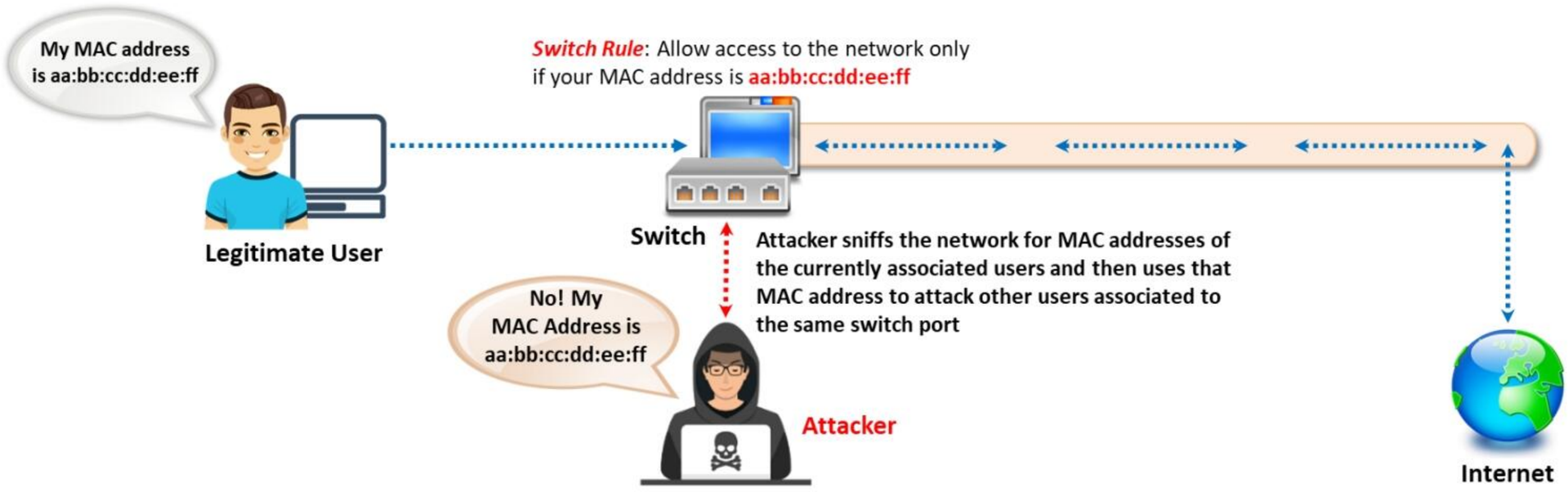


Figure 8.39: MAC spoofing/duplicating attack

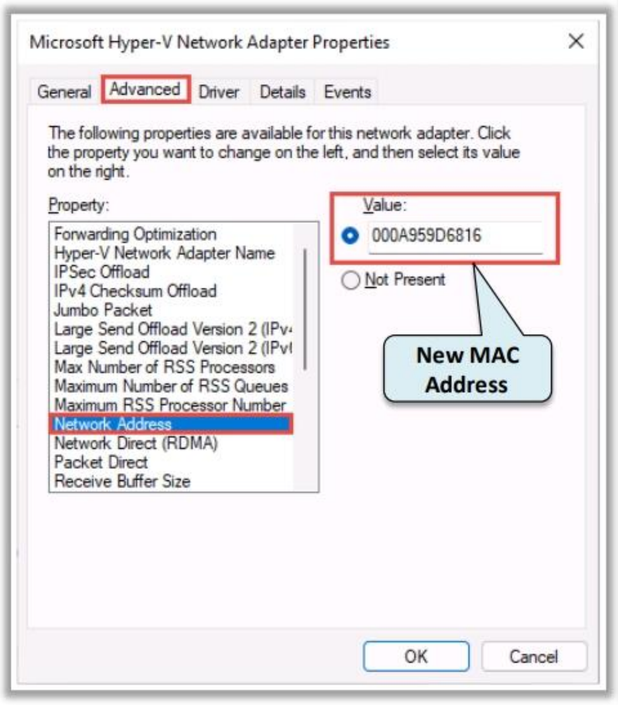
Note: This technique can be used to bypass wireless access points' MAC filtering.

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

MAC Spoofing Technique: Windows

In Windows 11 OS

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



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

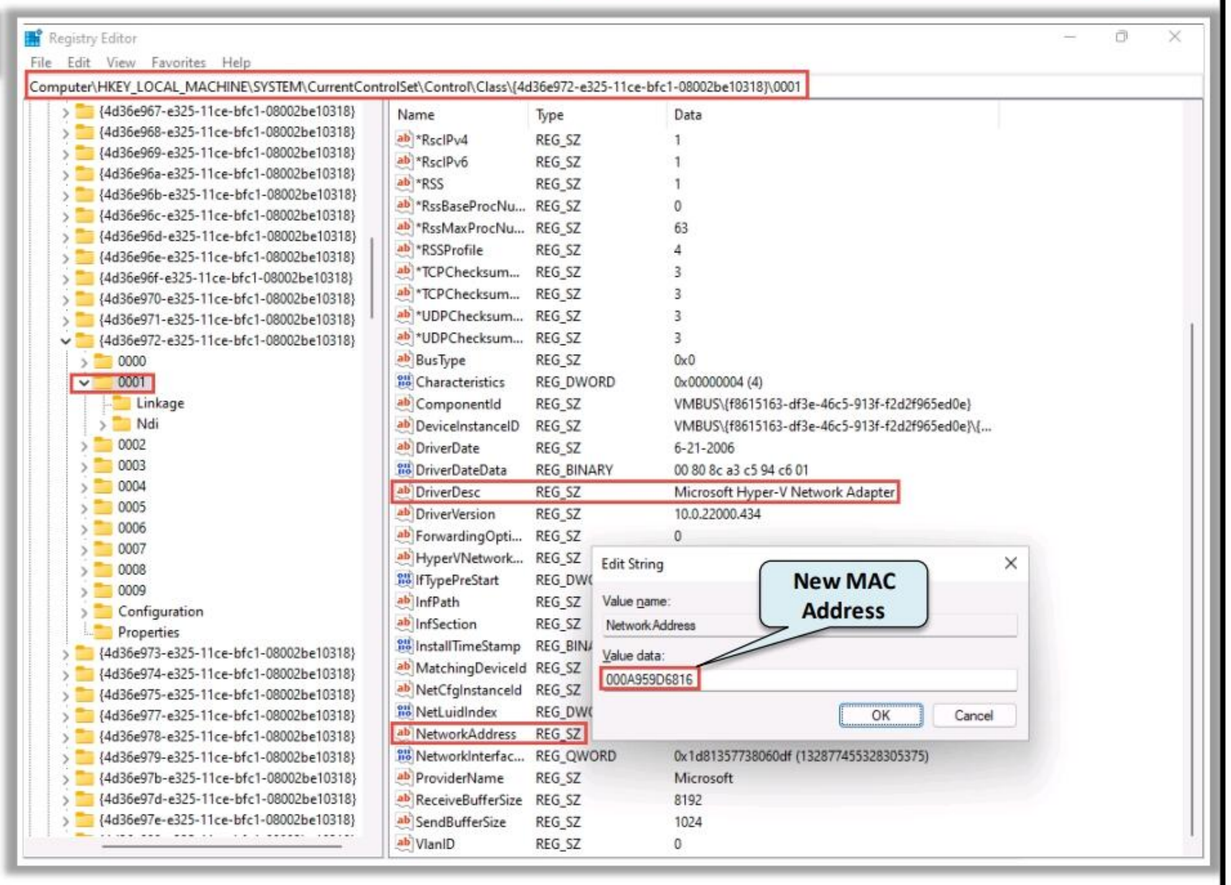
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Spoofing Technique: Windows (Cont'd)

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

- Press **Win + R** to open Run, type **regedit** to start the 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 displayed (starting with 0000, 0001, 0002, etc.)
- Search for the proper "**DriverDesc**" key to find the desired interface
- Right-click on the appropriate sub key and add, new string value "**NetworkAddress**" (data type "REG_SZ") to contain the new MAC address
- Right click on the "**NetworkAddress**" string value on the right side and select **Modify...**
- In the "**Edit String**" dialogue box, "**Value data**" field enter the new MAC address and click "**OK**"
- **Disable** and then **re-enable** the network interface that was changed or reboot the system



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

MAC Spoofing Technique: Windows

There are two methods for MAC spoofing in Windows 11 OS:

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

1. Click on **Start**, search for **Control Panel** and open it, then navigate to **Network and Internet** → **Networking and Sharing Center**.

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

2. Click on **Ethernet** and then click on **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-hand side, under "**Value,**" type in the new MAC address you would like to assign and click **OK**.

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

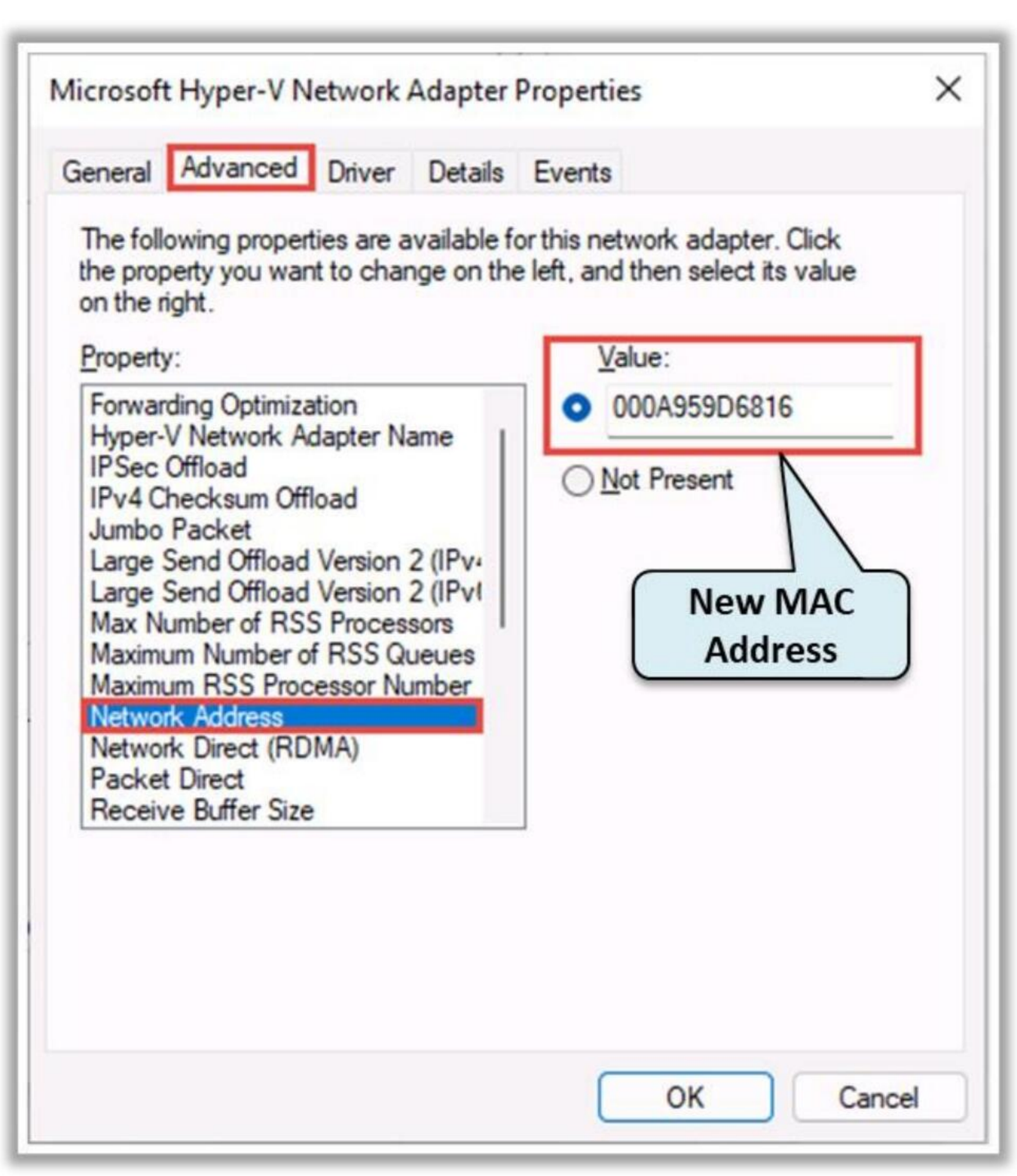


Figure 8.40: Ethernet Properties dialog box

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

Method 2: Steps to change the MAC address in the registry:

1. Press **Win + R** to open Run, and type **regedit** to start the registry editor.
2. Go to "**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}** and double-click on it to expand the tree.
3. Four-digit sub keys representing network adapters will be found (starting with 0000, 0001, 0002, etc.).
4. Search for the proper "**DriverDesc**" key to find the desired interface.
5. Right-click on the appropriate sub key and add the new string value "**NetworkAddress**" (data type "REG_SZ") to contain the new MAC address.
6. Right-click on the "**NetworkAddress**" string value on the right side and select **Modify…**
7. Now, in the "**Edit String**" dialog box, enter the new MAC address in the "**Value data**" field and click "**OK.**"
8. **Disable** and then **re-enable** the network interface that was changed, or reboot the system.

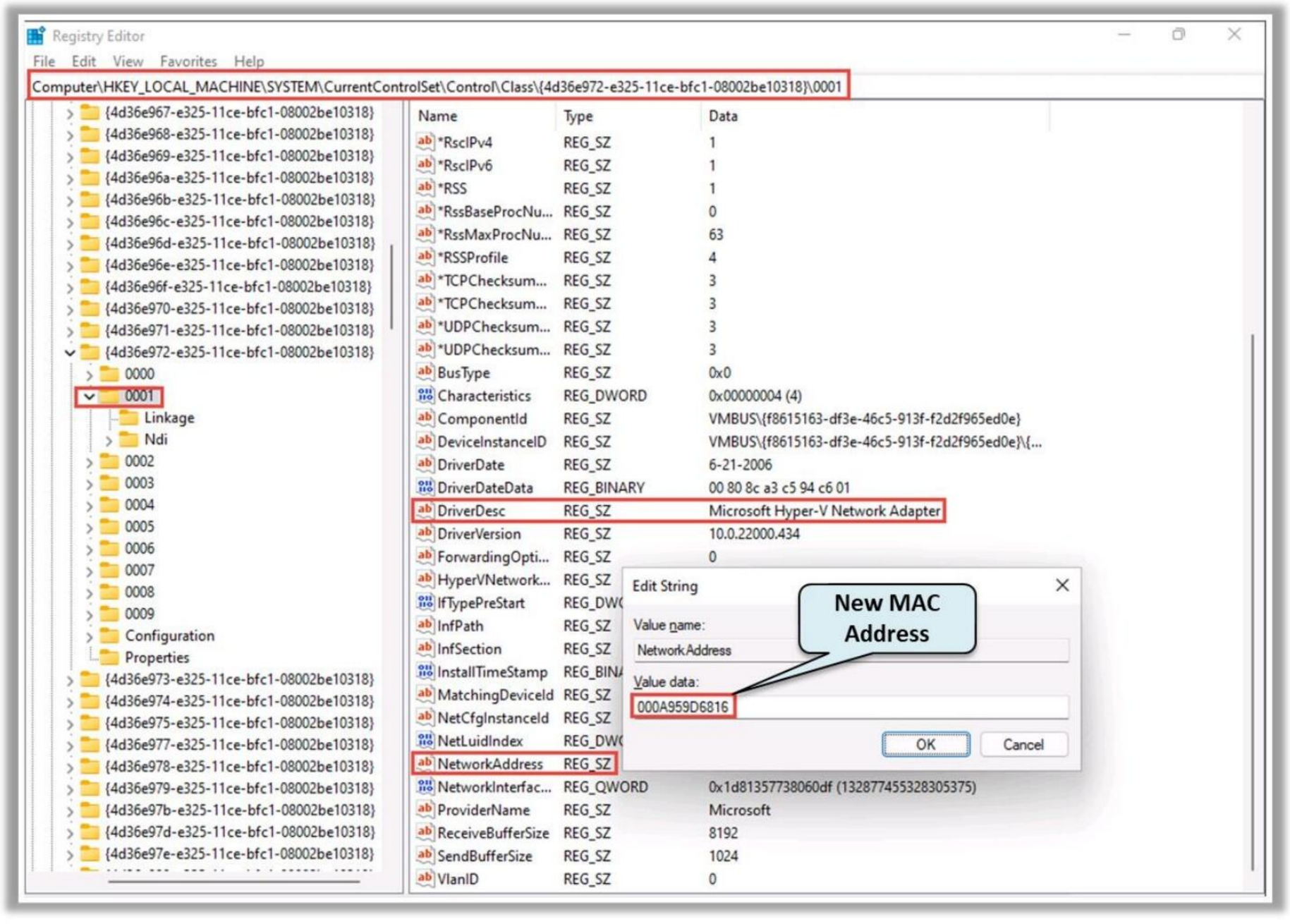
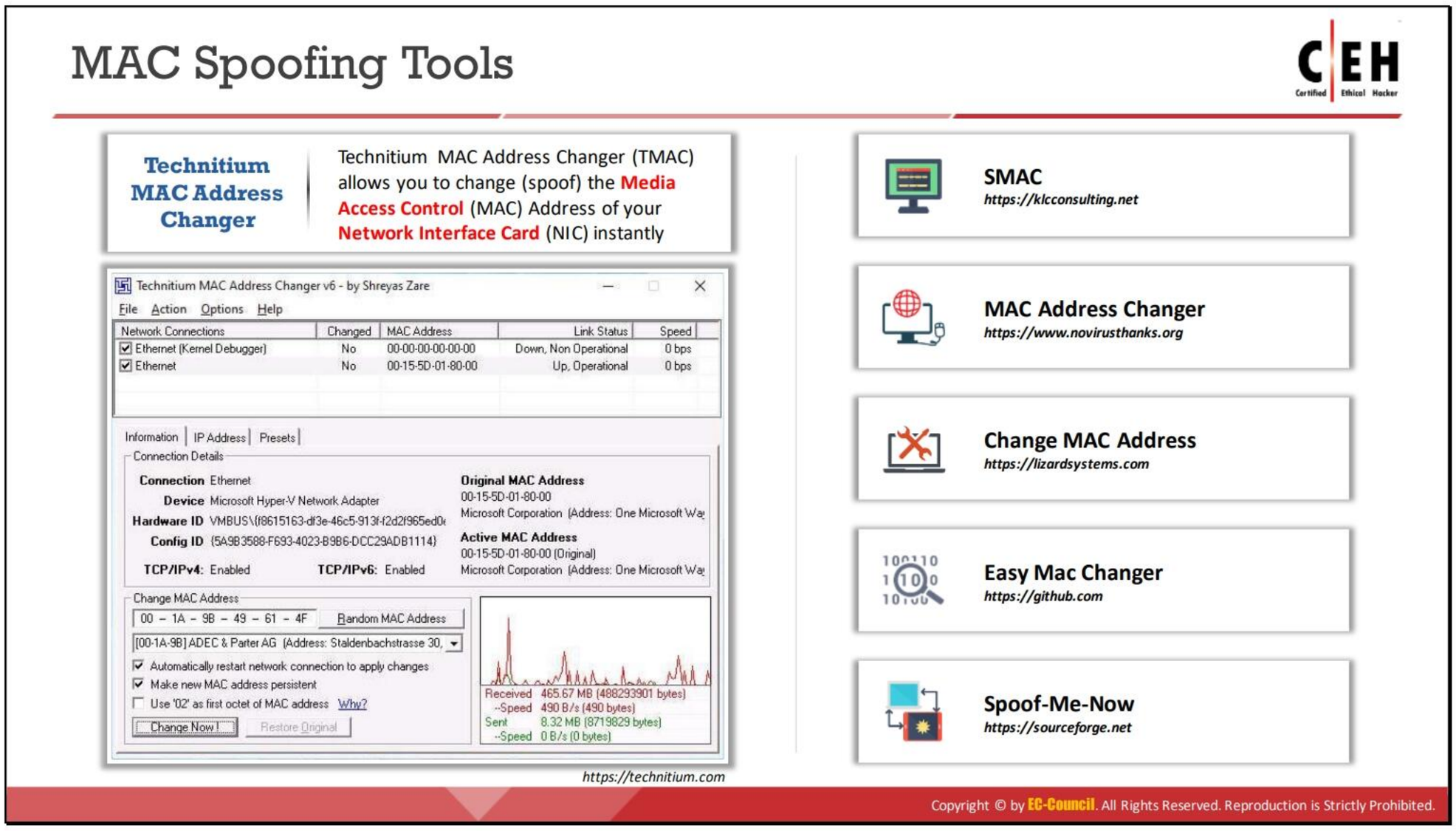


Figure 8.41: Registry Editor

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



MAC Spoofing Tools

- **Technitium MAC Address Changer**

  Source: *https://technitium.com*

  Technitium MAC Address Changer (TMAC) allows you to change (spoof) the MAC address of your NIC instantly. Every NIC has a MAC address hardcoded in its circuit by the manufacturer. This hard-coded MAC address is used by Windows drivers to access the Ethernet network (LAN). This tool can set a new MAC address to your NIC, bypassing the original hard-coded MAC address.

  As shown in the screenshot, attackers can use TMAC to spoof or change their MAC address to perform an attack on the target system.

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

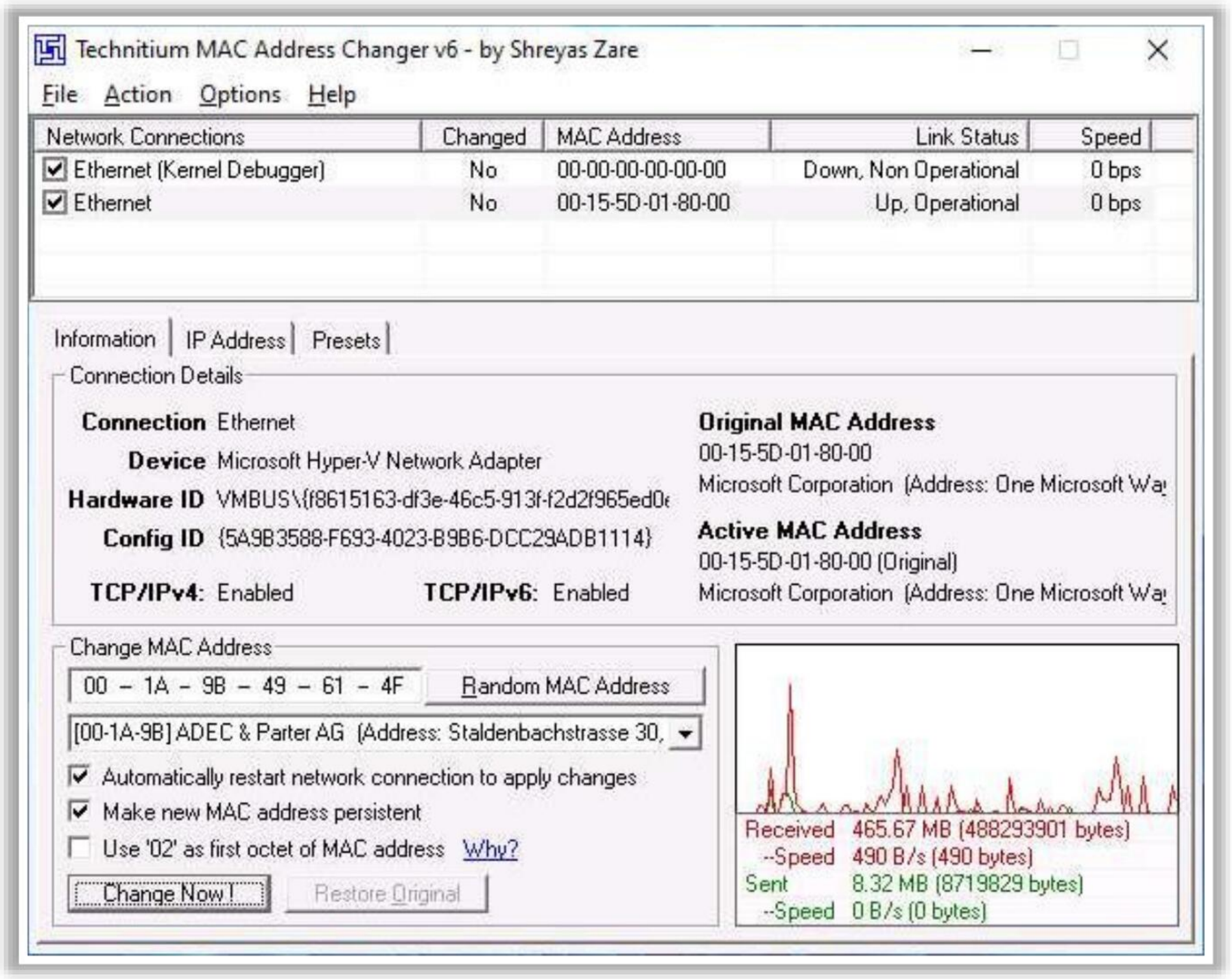
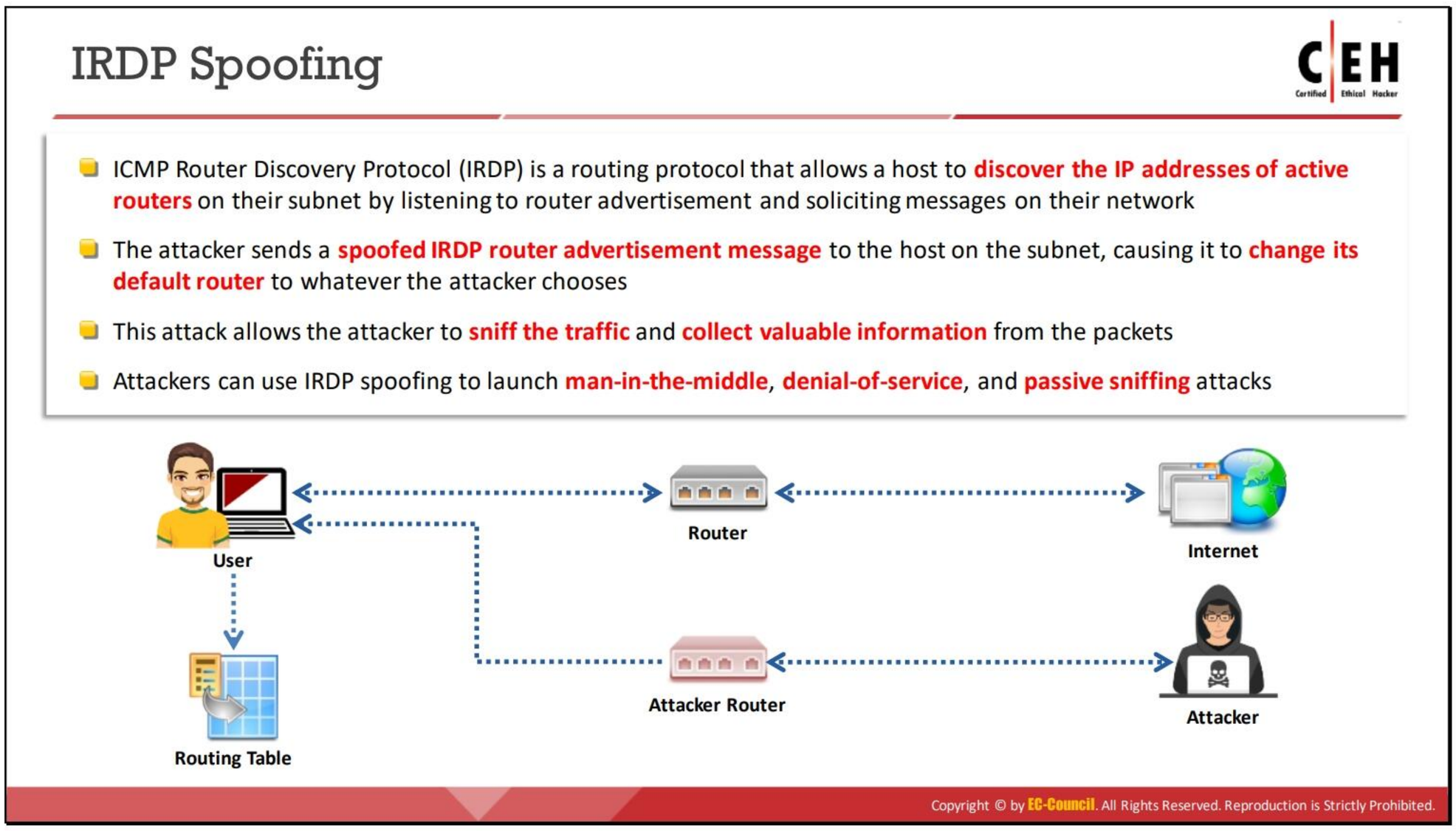


Figure 8.42: Screenshot of Technitium MAC Address Changer (TMAC)

Some examples of MAC spoofing tools are listed below:

- SMAC (*https://klcconsulting.net*)
- MAC Address Changer (*https://www.novirusthanks.org*)
- Change MAC Address (*https://lizardsystems.com*)
- Easy Mac Changer (*https://github.com*)
- Spoof-Me-Now (*https://sourceforge.net*)

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



IRDP Spoofing

ICMP Router Discovery Protocol (IRDP) is a routing protocol that allows a host to discover the IP addresses of active routers on its subnet by listening to router advertisement and solicitation messages on its network. The attacker can add default route entries on a system remotely by spoofing router advertisement messages. As IRDP does not require any authentication, the target host will prefer the default route defined by the attacker over the default route provided by the DHCP server. The attacker accomplishes this by setting the preference level and 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 so, then it adds the default route entry; otherwise, it ignores the advertisement.

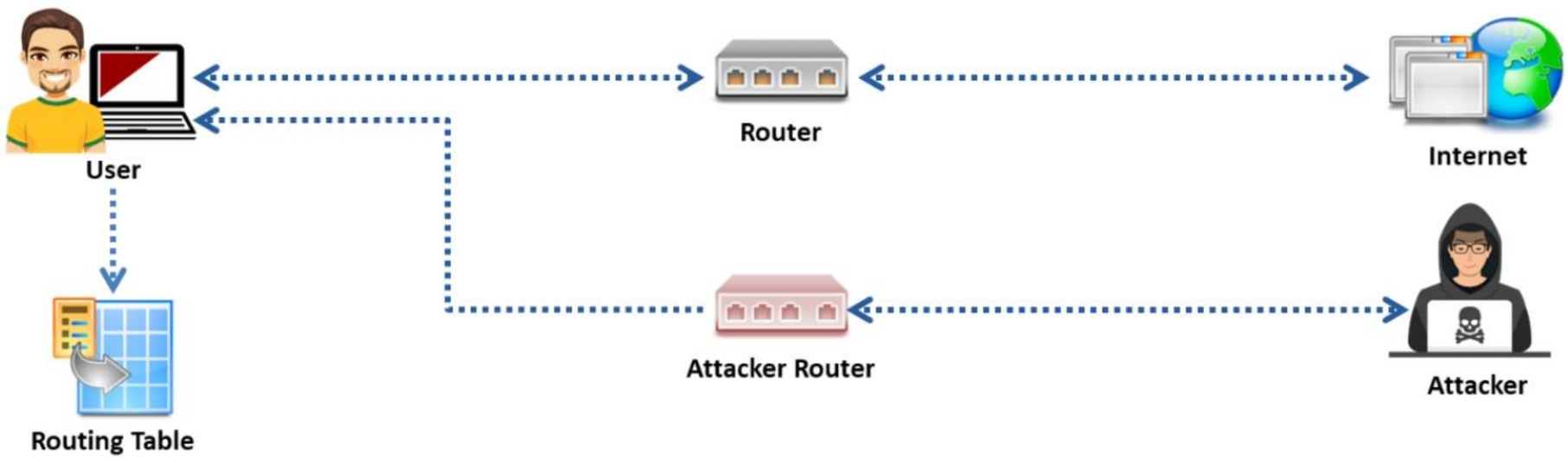


Figure 8.43: IRDP spoofing

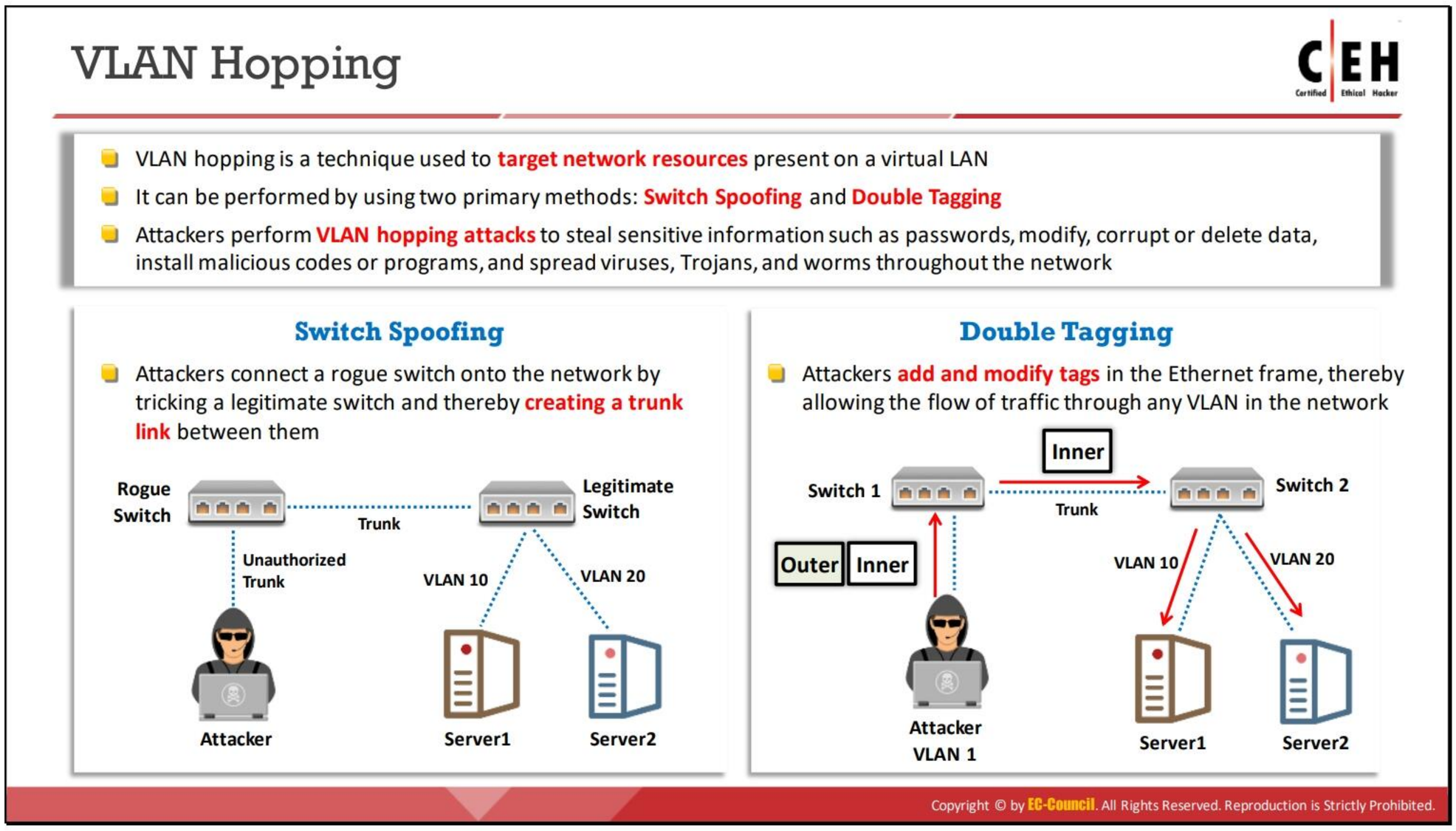
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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 the destination. The attacker plays an MITM role and tries to modify the traffic.
- **DoS:** IRDP spoofing allows remote attackers to add wrong route entries into the victim's 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.



VLAN Hopping

Virtual local area network (VLAN) hopping is a technique used to target network resources present on a VLAN. The main purpose behind a VLAN hopping attack is to gain access to the traffic flowing in other VLANs present in the same network, which is otherwise inaccessible. Networks usually have poor VLAN implementation or have misconfigurations that allow attackers to perform this type of attack. Attackers perform VLAN hopping attacks to steal sensitive information such as passwords; modify, corrupt, or delete data; install malicious codes or programs; or spread viruses, Trojans, and worms throughout the network.

VLAN hopping attacks can be performed via two primary methods, as given below:

- **Switch Spoofing**

  Using switch spoofing, the attacker connects a rogue switch into the network by tricking a legitimate switch and thereby creating a trunk link between them. After establishing a trunk link, the traffic from multiple VLANs can be sent to and through the rogue switch, therefore allowing an attacker to sniff and view the packet content. This attack is successful only when the legitimate switch is configured to negotiate a trunk connection, or when the interface is configured with “dynamic auto,” “dynamic desirable,” or “trunk” mode.

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

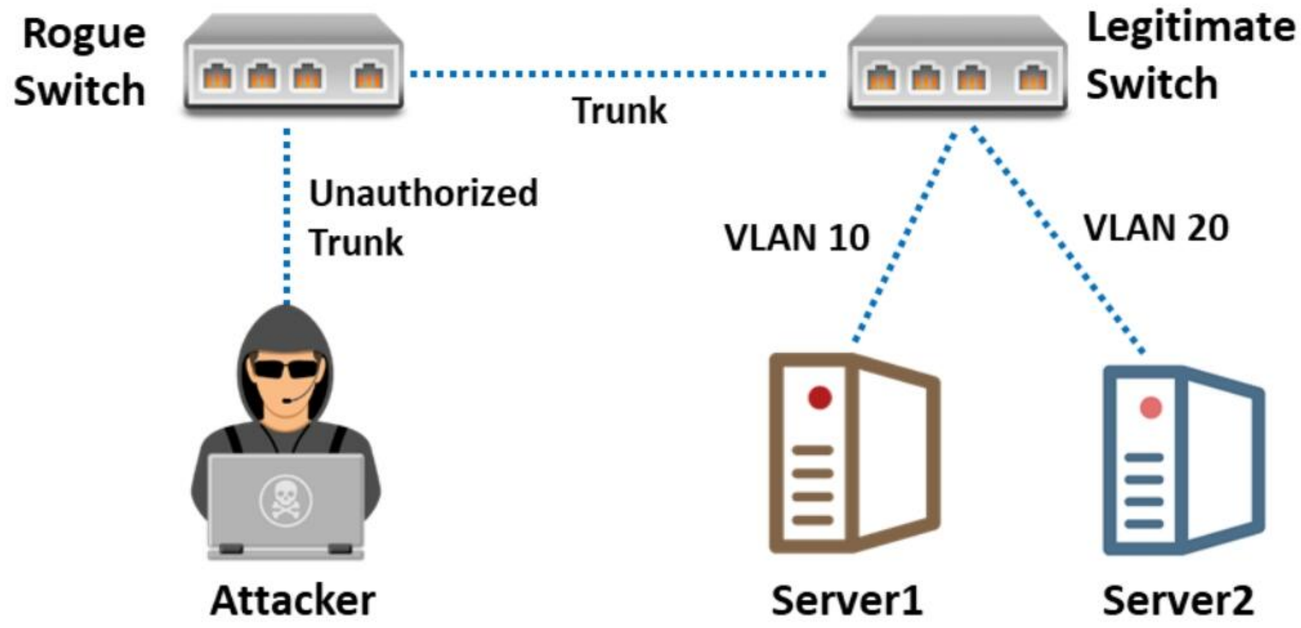


Figure 8.44: Illustration of switch spoofing

- **Double Tagging**

Using double tagging, the attacker adds and modifies tags in the Ethernet frame, thereby allowing the flow of traffic through any VLAN in the network. The Ethernet frame that is sent by the attacker contains two 802.1Q tags, inner and outer; the inner tag is the VLAN tag of a target switch that the attacker wants to reach, and the outer tag is the native VLAN of the attacker. When the switch receives the Ethernet frame, it strips off the outer tag, as it is the same as the tag for the native VLAN, and forwards the frame with an inner tag on all its trunk interfaces. This allows an attacker to bypass the network mechanism by jumping from his native VLAN to the victim's VLAN(s), and also allows him/her to send the traffic to other VLANs. This attack is possible only if the switch ports are configured to use native VLANs.

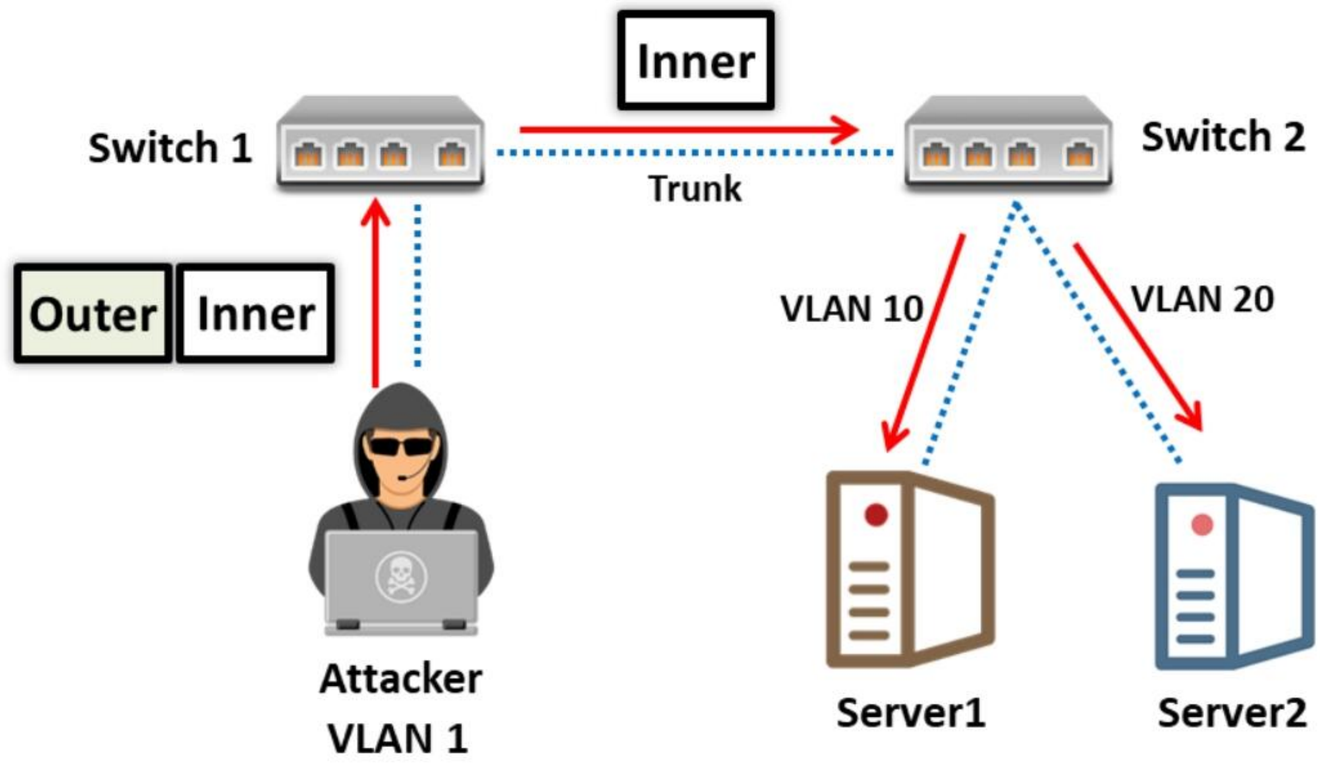
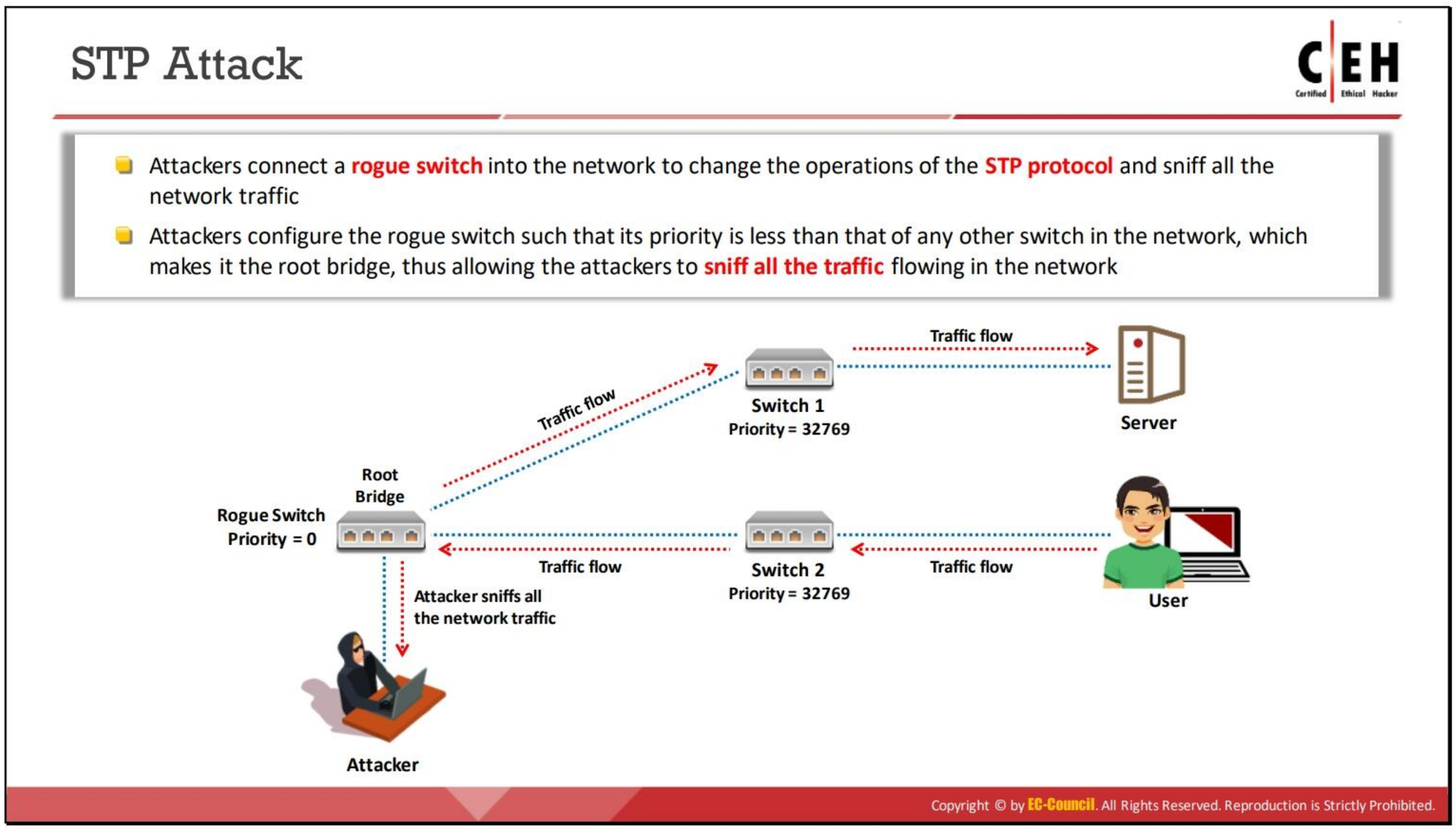


Figure 8.45: Illustration of double tagging

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



STP Attack

In a Spanning Tree Protocol (STP) attack, attackers connect a rogue switch into the network to change the operation of the STP protocol and sniff all the network traffic. STP is used in LAN-switched networks with the primary function of removing potential loops within the network. STP ensures that the traffic inside the network follows an optimized path to enhance network performance. In this process, a switch inside the network is appointed as the root bridge. After the selection of the root bridge, other switches in the network connect to it by selecting a root port (the closest port to the root bridge).

The root bridge is selected with the help of Bridge Protocol Data Units (BPDUs). BPDUs each have an identification number known as a BID or ID. These BIDs consist of the Bridge Priority and the MAC address. By default, the value of the Bridge Priority is 32769.

If an attacker has access to two switches, he/she introduces a rogue switch in the network with a priority lower than any other switch in the network. This makes the rogue switch the root bridge, thus allowing the attacker to sniff all the traffic flowing in the network.

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

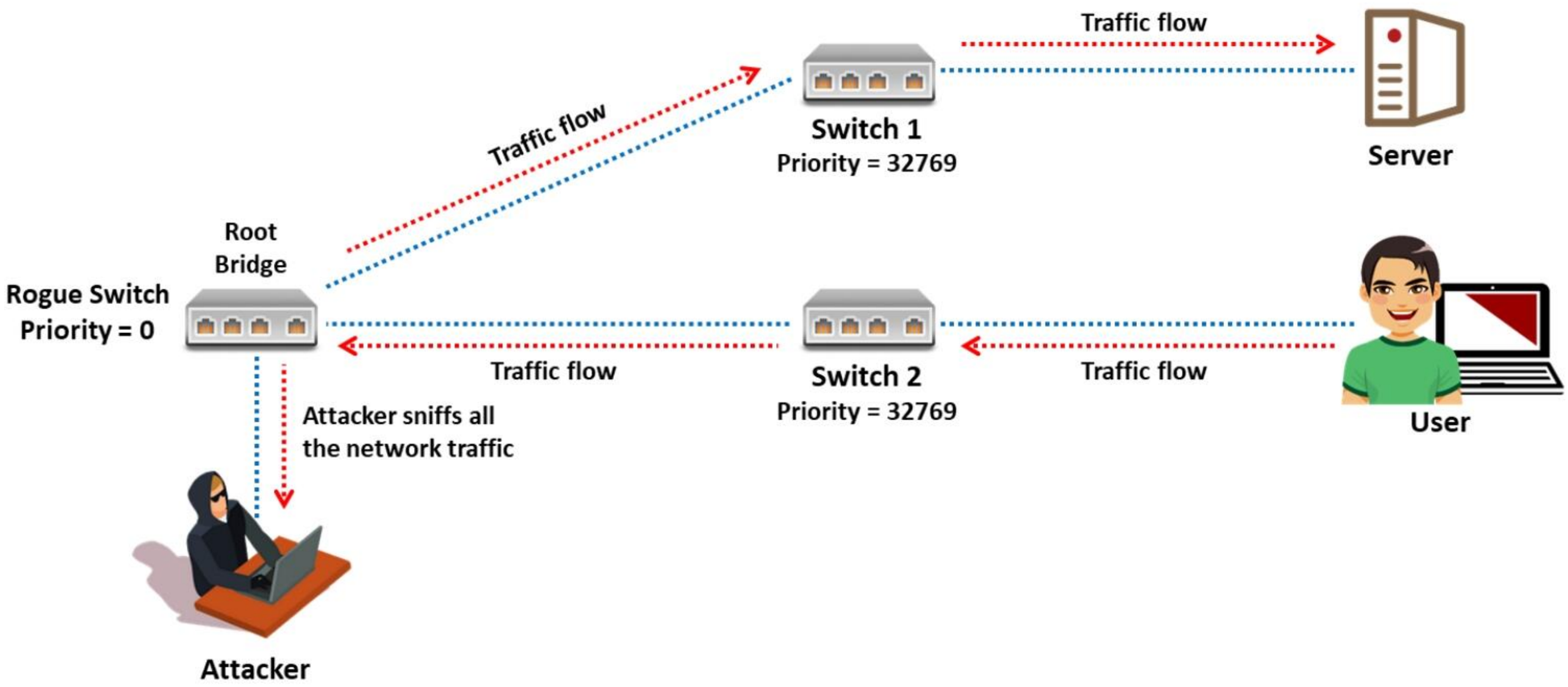
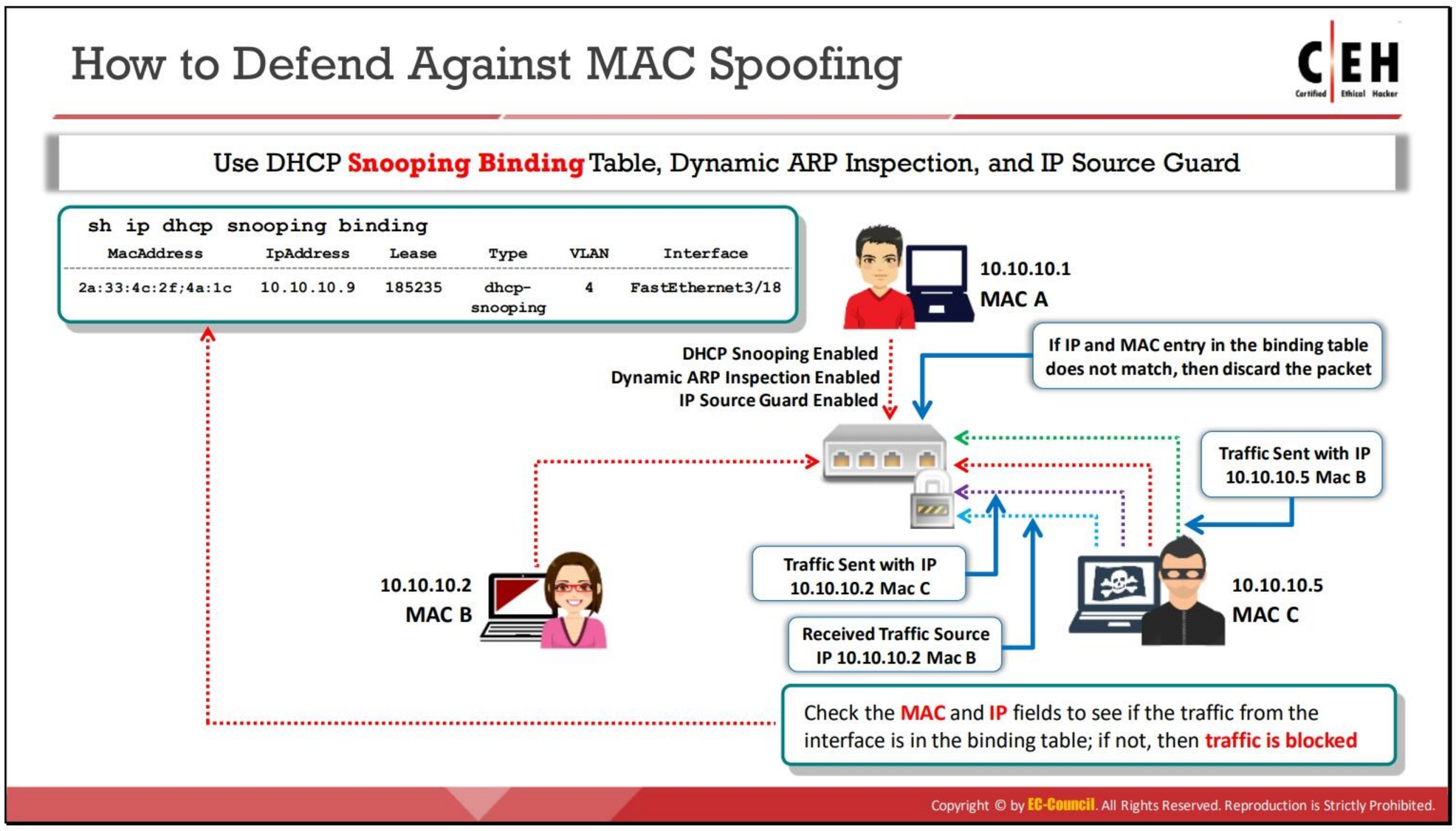


Figure 8.46: Illustration of an STP attack

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



How to Defend Against MAC Spoofing

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

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

To detect MAC spoofing, it is necessary to know all the MAC addresses in the network. The best way to defend against MAC address spoofing is to place the server behind the router. This is because routers depend only on IP addresses, whereas switches depend on MAC addresses for communication in a network. Making changes to the port security interface configuration is another way to prevent MAC spoofing attacks. Once you enable the port-security command, it allows you to specify the MAC address of the system connected to the specific port. It also allows for specific action to be taken if a port security violation occurs.

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

- **DHCP Snooping Binding Table**: The DHCP snooping process filters untrusted DHCP messages and helps to build and bind a DHCP binding table. This table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information to correspond with untrusted interfaces of a switch. It acts as a firewall between

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

untrusted hosts and DHCP servers. It also helps in differentiating between trusted and untrusted interfaces.

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

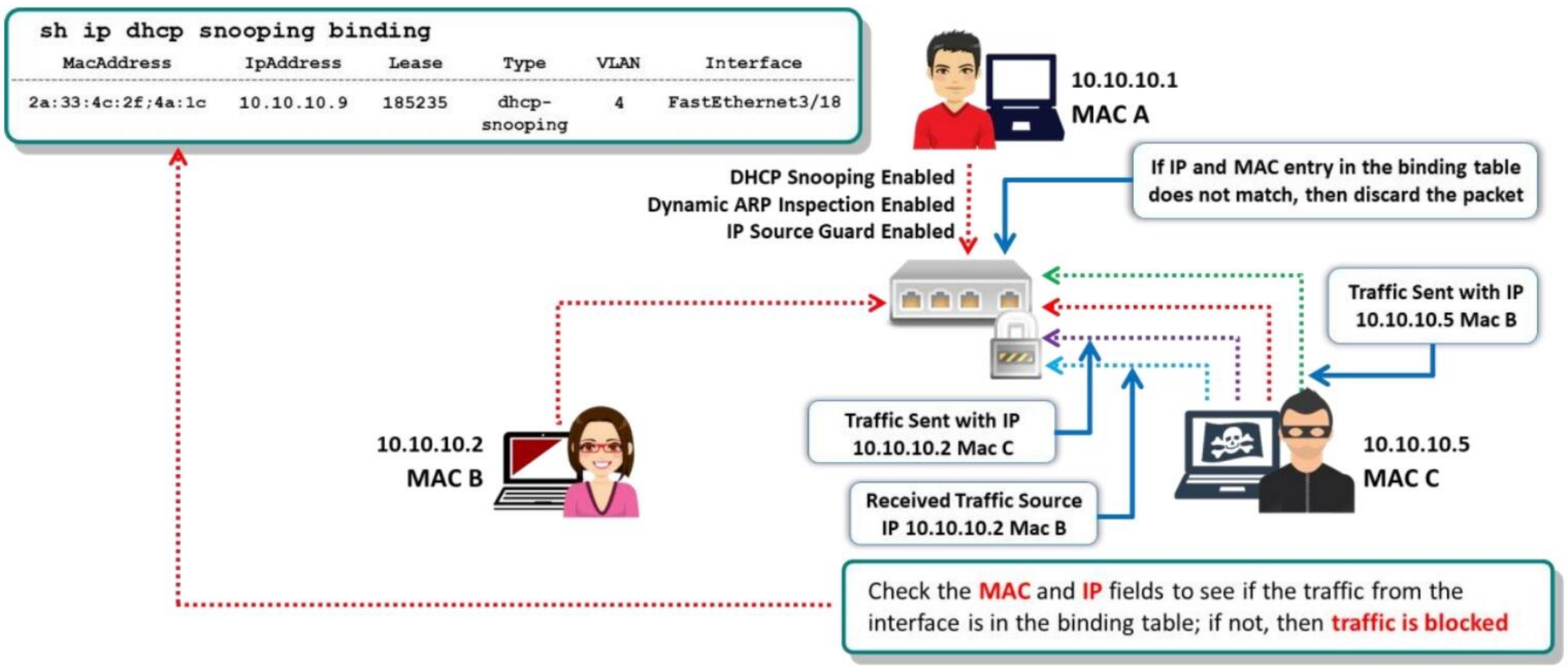
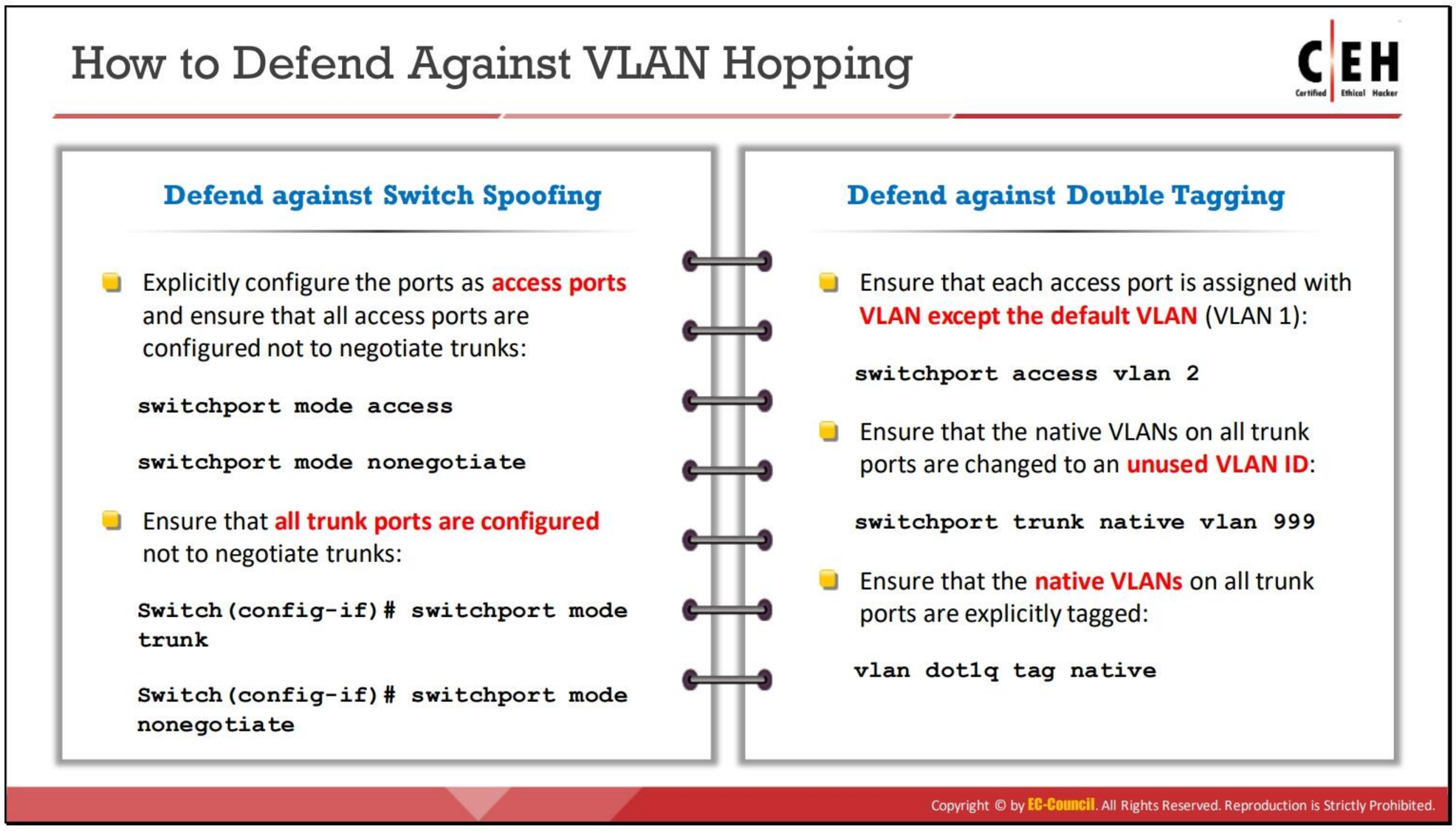


Figure 8.47: Defending against MAC spoofing

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



How to Defend Against VLAN Hopping

Defend Against Switch Spoofing

Perform the following steps to configure a switch to prevent switch spoofing attacks:

- Explicitly configure the ports as access ports, and ensure that all access ports are configured not to negotiate trunks:

  ```
  switchport mode access
  switchport mode nonegotiate
  ```

- Ensure that all trunk ports are configured not to negotiate trunks:

  ```
  switchport mode trunk
  switchport mode nonegotiate
  ```

Defend Against Double Tagging

Perform the following steps to configure a switch to prevent double tagging attacks:

- Ensure that each access port is assigned with VLAN except the default VLAN (VLAN 1):

  ```
  switchport access vlan 2
  ```

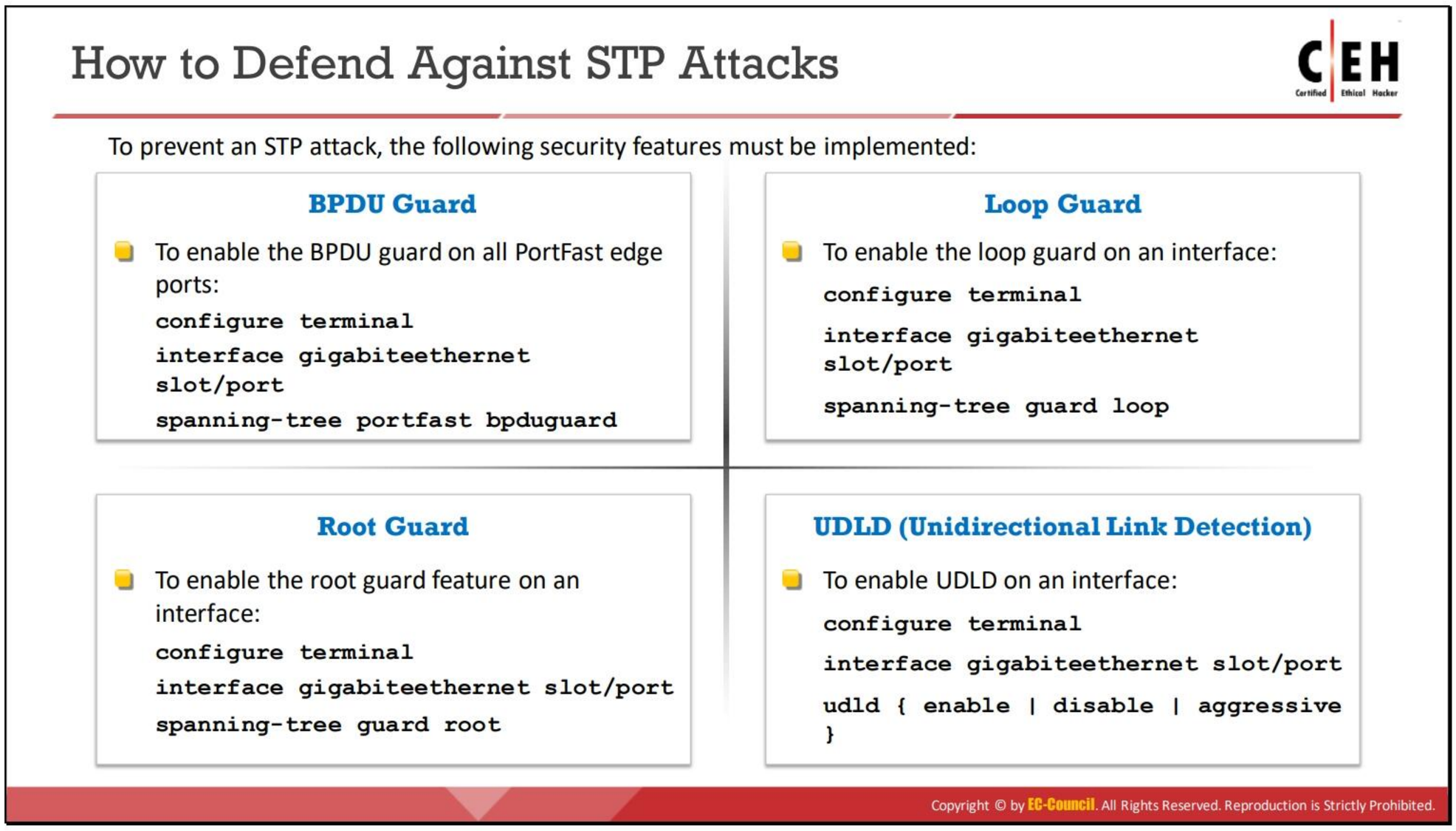
- Ensure that the native VLANs on all trunk ports are changed to an unused VLAN ID:

  ```
  switchport trunk native vlan 999
  ```

- Ensure that the native VLANs on all trunk ports are explicitly tagged:

  ```
  vlan dot1q tag native
  ```


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



How to Defend Against STP Attacks

Implement the following countermeasures to defend against STP attacks on switches:

- **BPDU Guard**: BPDU guard must be enabled on the ports that should never receive a BPDU from their connected devices. This is used to avoid the transmission of BPDUs on PortFast-enabled ports. This feature helps in preventing potential bridging loops in the network. If BPDU guard is enabled on a switch interface and an unauthorized switch connects to it, the port will be set to errdisable mode when a BPDU is received. The errdisable mode shuts down the port and disables it from sending or receiving any traffic.

  Use the following commands to enable BPDU guard on a switch interface:

  ```
  configure terminal
  interface gigabiteethernet slot/port
  spanning-tree portfast bpduguard
  ```

- **Root Guard**: Root guard protects the root bridge and ensures that it remains as the root in the STP topology. It forces the interfaces to become the designated ports (forwarding ports) to prevent the nearby switches from becoming root switches. Therefore, if a port enabled with the root guard feature receives a superior BPDU, it converts that port into a loop inconsistent state (not errdisabled), thus protecting an STP topology change. This port remains inactive only for that specific switch/switches attempting to change the STP topology. This port remains in down state until the issue is resolved.

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

Use the following commands to enable the root guard feature on a switch interface:

```
configure terminal
interface gigabiteethernet slot/port
spanning-tree guard root
```

- **Loop Guard**: Loop guard improves the stability of the network by preventing it against the bridging loops. It is generally used to protect against a malfunctioned switch.

  Use the following commands to enable the loop guard feature on a switch interface:

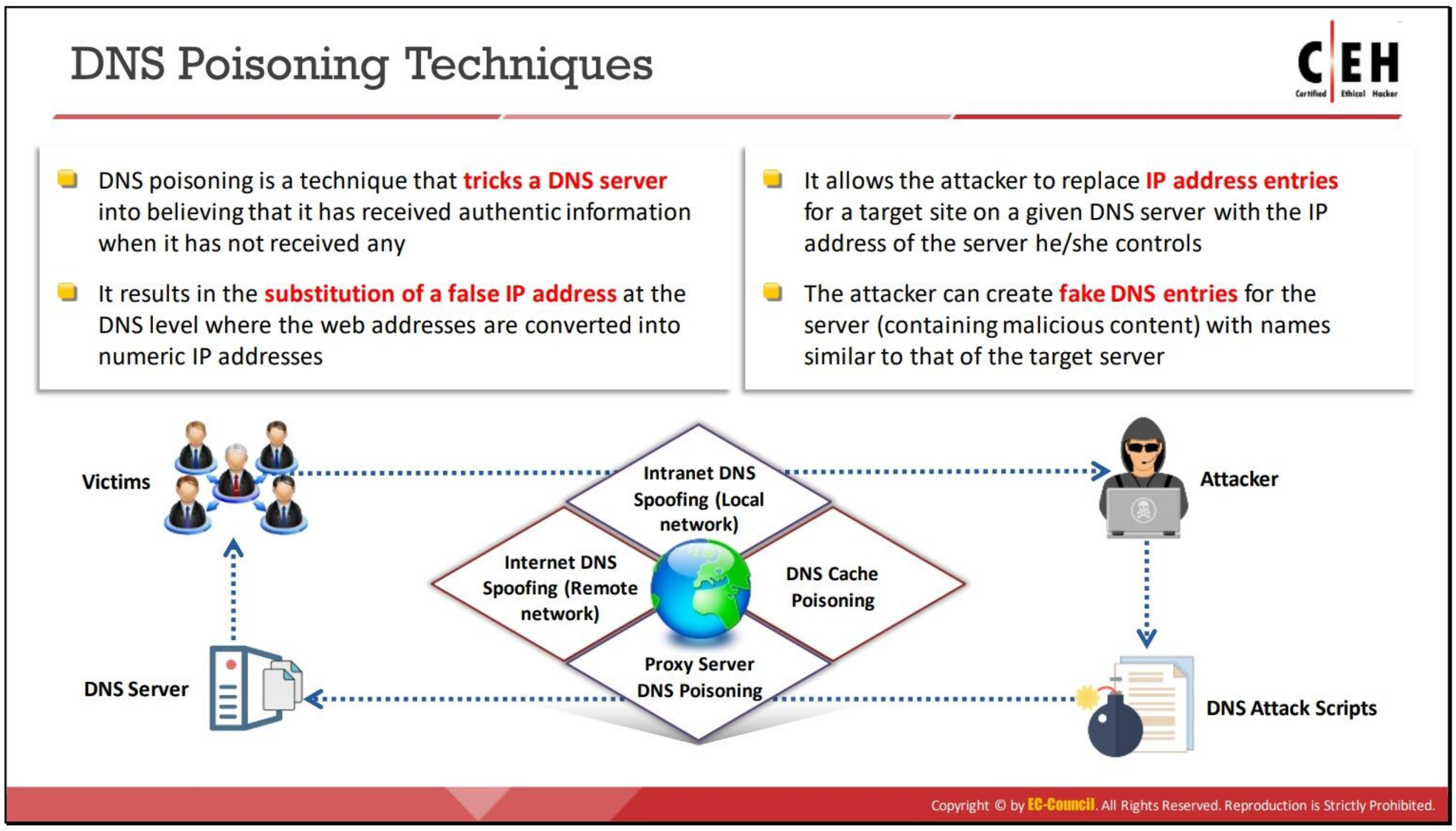
```
configure terminal
interface gigabiteethernet slot/port
spanning-tree guard loop
```

- **UDLD (Unidirectional Link Detection)**: UDLD enables devices to detect the existence of unidirectional links and further disable the affected interfaces in the network. These unidirectional links in the network can cause STP topology loops.

  Use the following command to enable UDLD on a switch interface:

```
configure terminal
interface gigabiteethernet slot/port
udld { enable | disable | aggressive }
```


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



Sniffing Technique: DNS Poisoning

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

DNS Poisoning Techniques

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 known as DNS spoofing, the attacker tricks a DNS server into believing that it has received authentic information when, in reality, it has not received any. The attacker tries to redirect the victim to a malicious server instead of the legitimate server. The attacker does this by manipulating the DNS table entries in the DNS. This results in substitution of a false IP address at the DNS level, where web addresses are converted into numeric IP addresses.

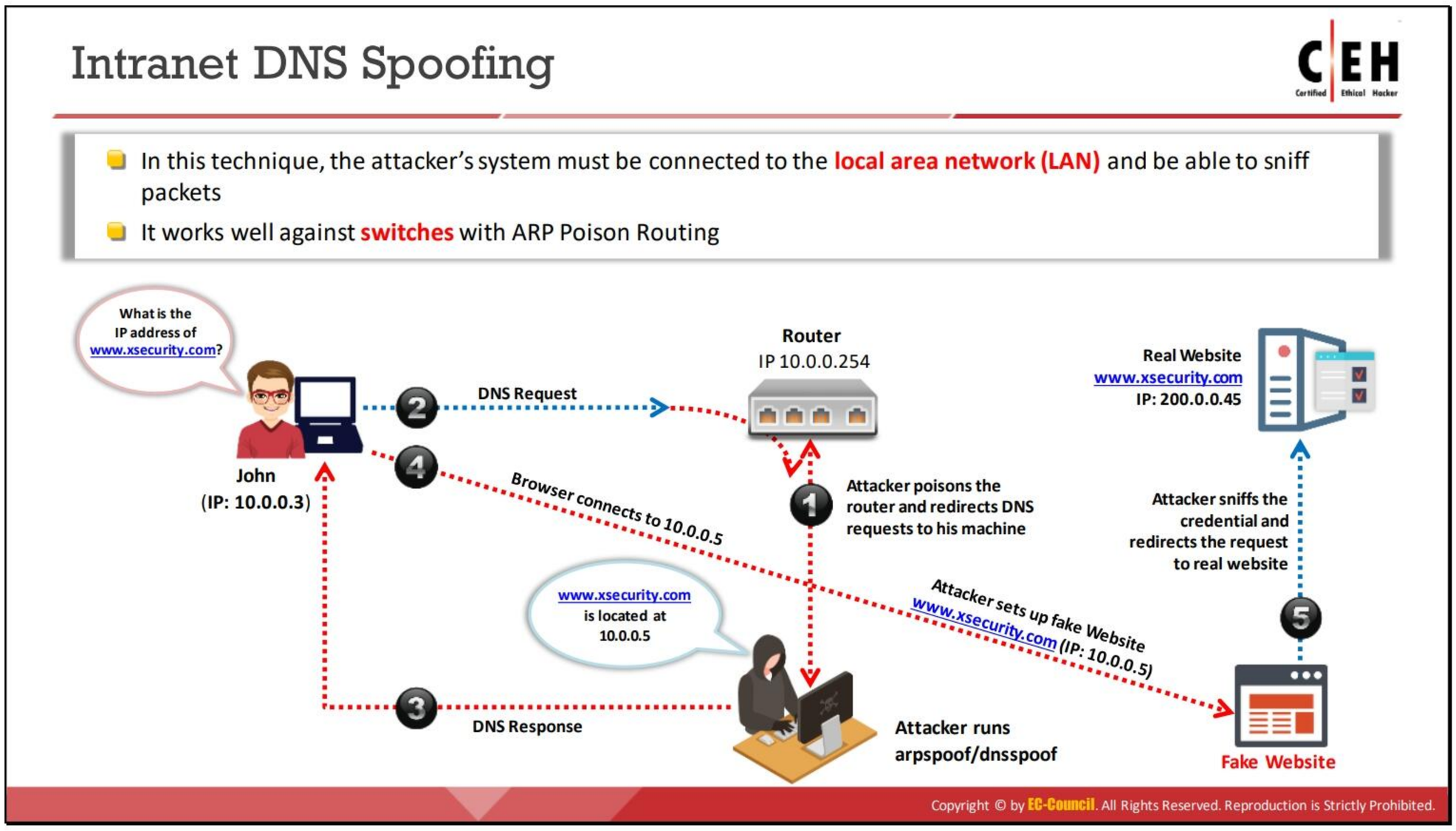
When the victim tries to access a website, the attacker manipulates the entries in the DNS table so that the victim's system redirects the URL to the attacker's server. The attacker replaces IP address entries for a target site on a given DNS server with the IP address of the server (malicious server)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

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

DNS poisoning is possible using the following techniques:

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

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



Intranet DNS Spoofing

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 describes how an attacker performs an intranet DNS spoofing.

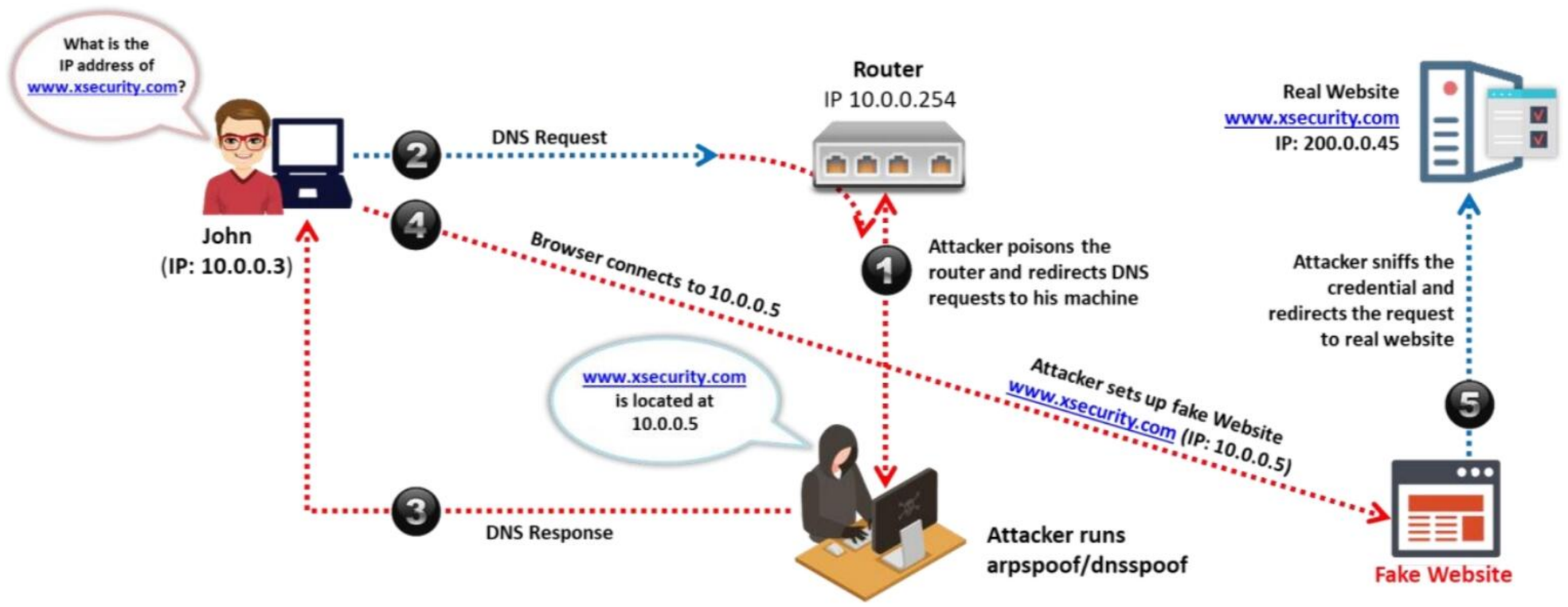


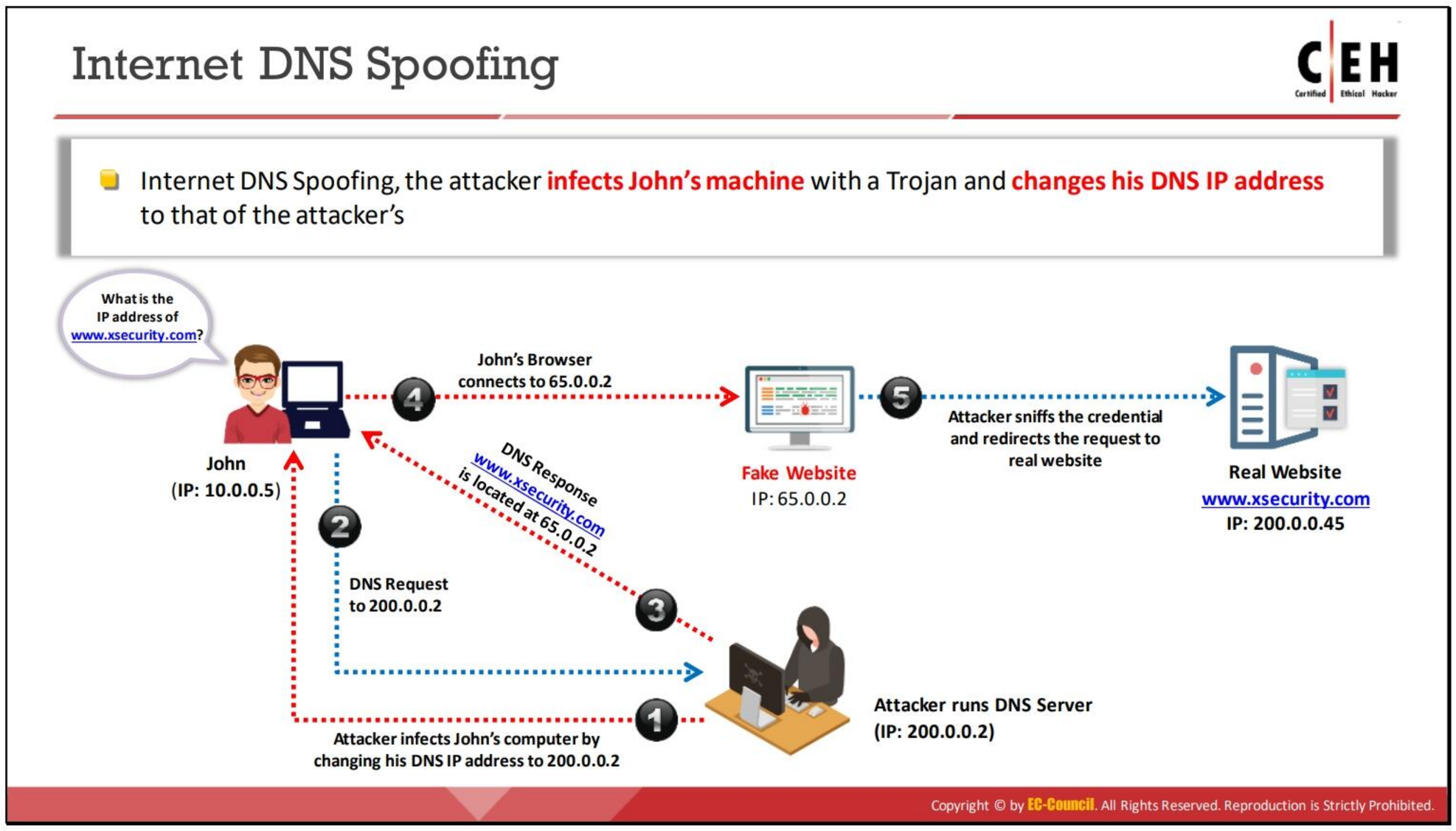
Figure 8.48: Intranet DNS spoofing

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 (John) sends a DNS request to the router, the poisoned router sends the DNS request packet to the attacker's machine. Upon

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

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, submitted to the fake website. The attacker retrieves the required information and then redirects the client to the real website.

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



Internet DNS Spoofing

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

Attackers perform Internet DNS spoofing with the help of Trojans when the victim's system connects to the Internet. This 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 a fake IP address that resolves to the attacker's system. Thus, the victim's traffic redirects to the attacker's system. At this point, the attacker can easily sniff the victim's confidential information.

The figure illustrates an attacker performing Internet DNS spoofing. The attacker infects John's machine with a Trojan and changes his DNS IP address to that of the attacker.

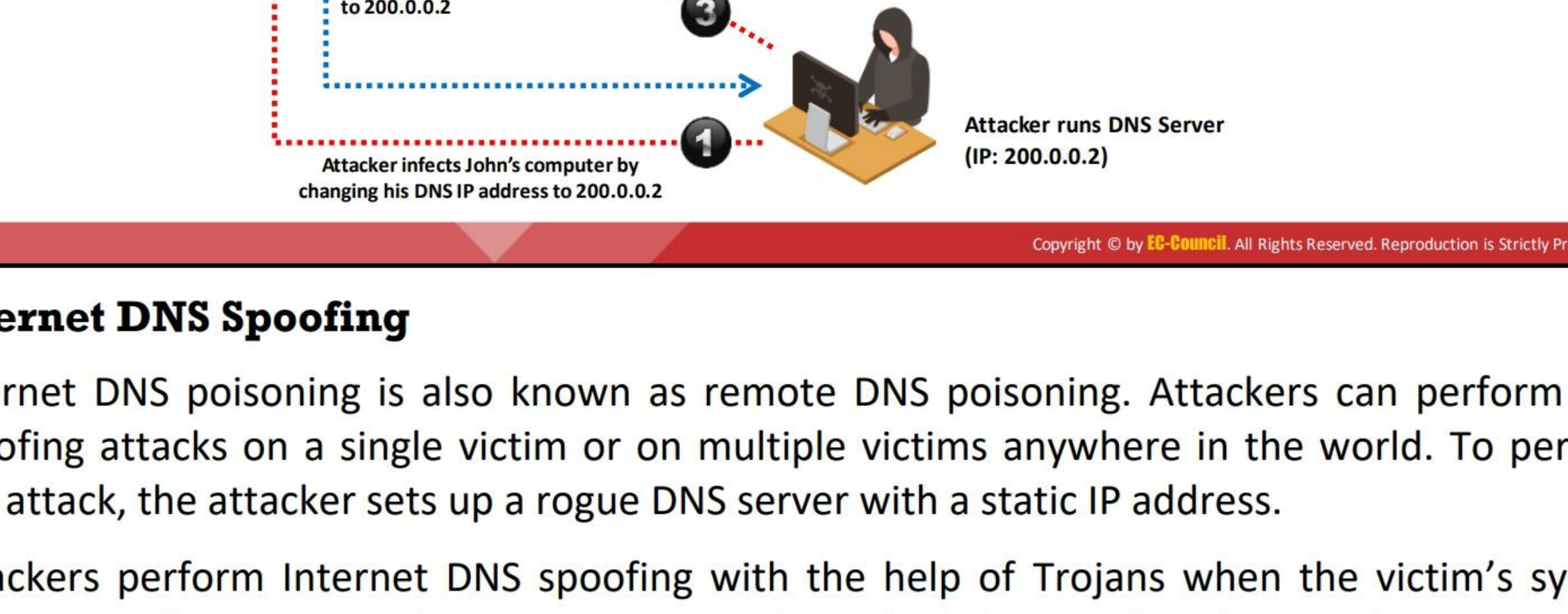
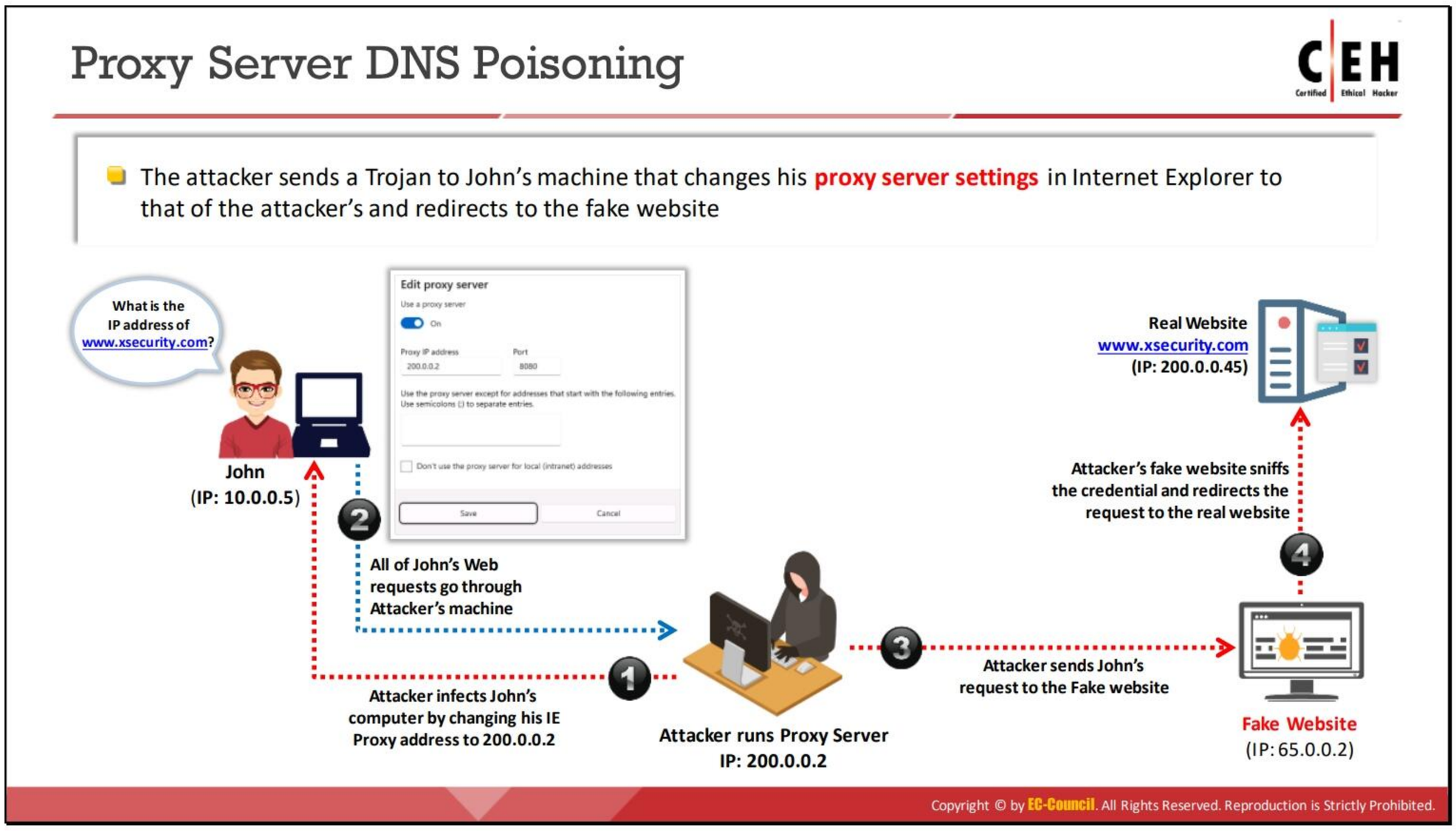


Figure 8.49: Internet DNS Spoofing

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



Proxy Server DNS Poisoning

In the proxy server DNS poisoning technique, the attacker 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.

As shown in the figure, an attacker sends a Trojan to John's machine that changes his proxy server settings in Internet Explorer to those of the attacker, and redirects the request to a fake website.

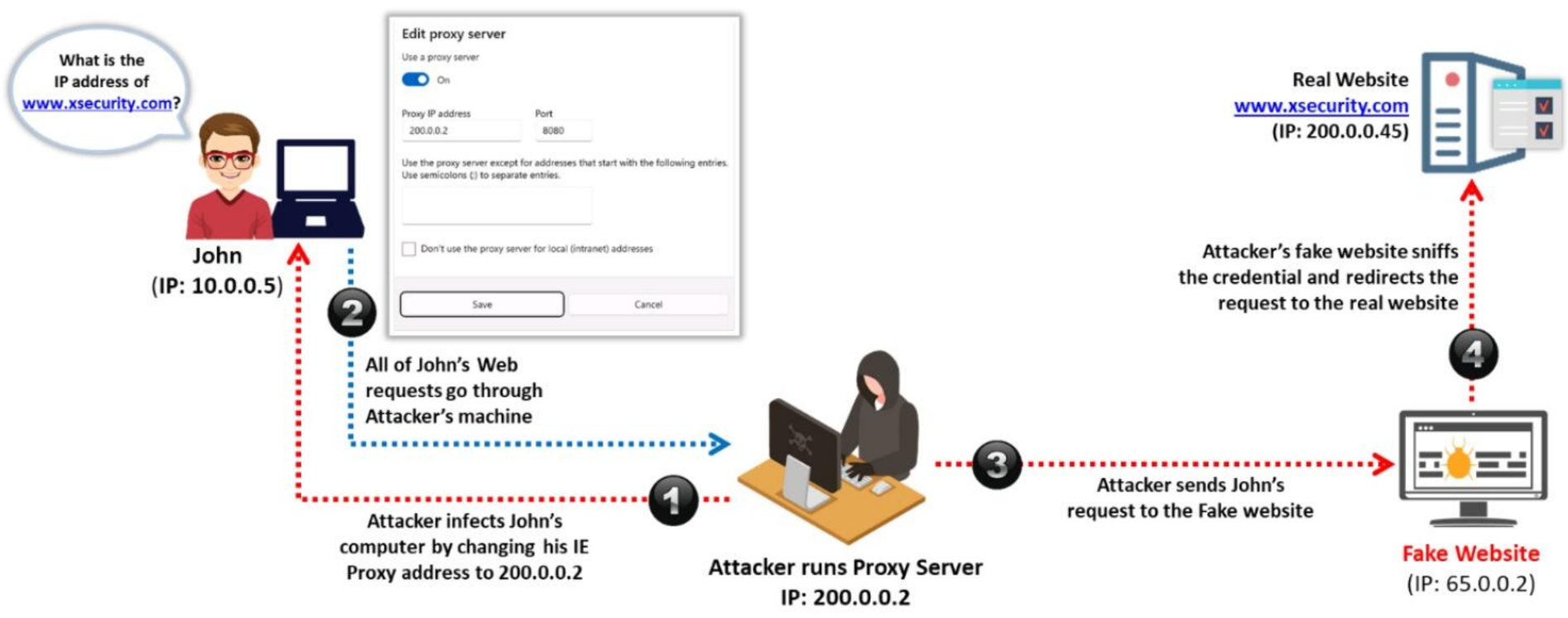
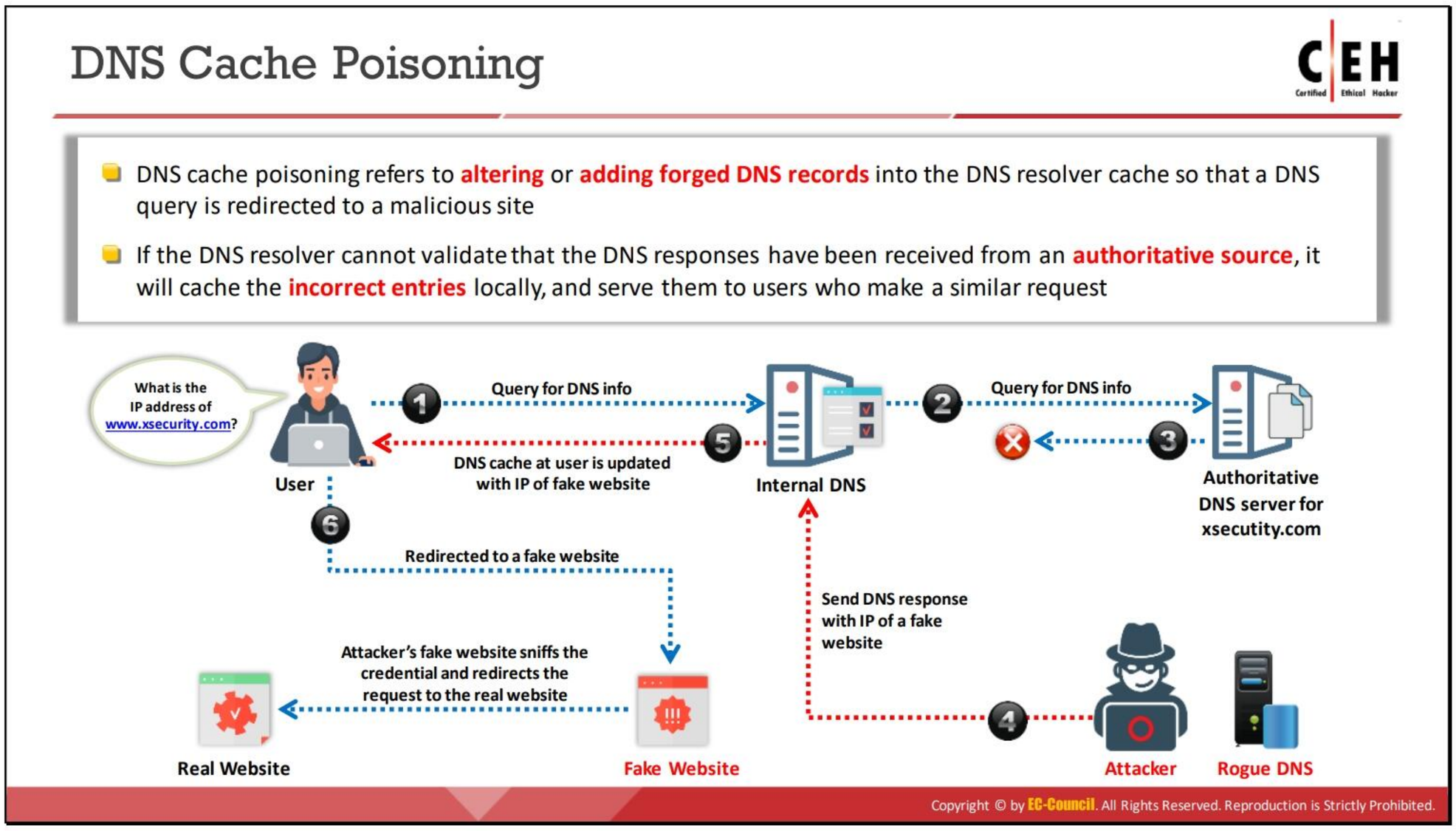


Figure 8.50: Proxy server DNS poisoning

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



DNS Cache Poisoning

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

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

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

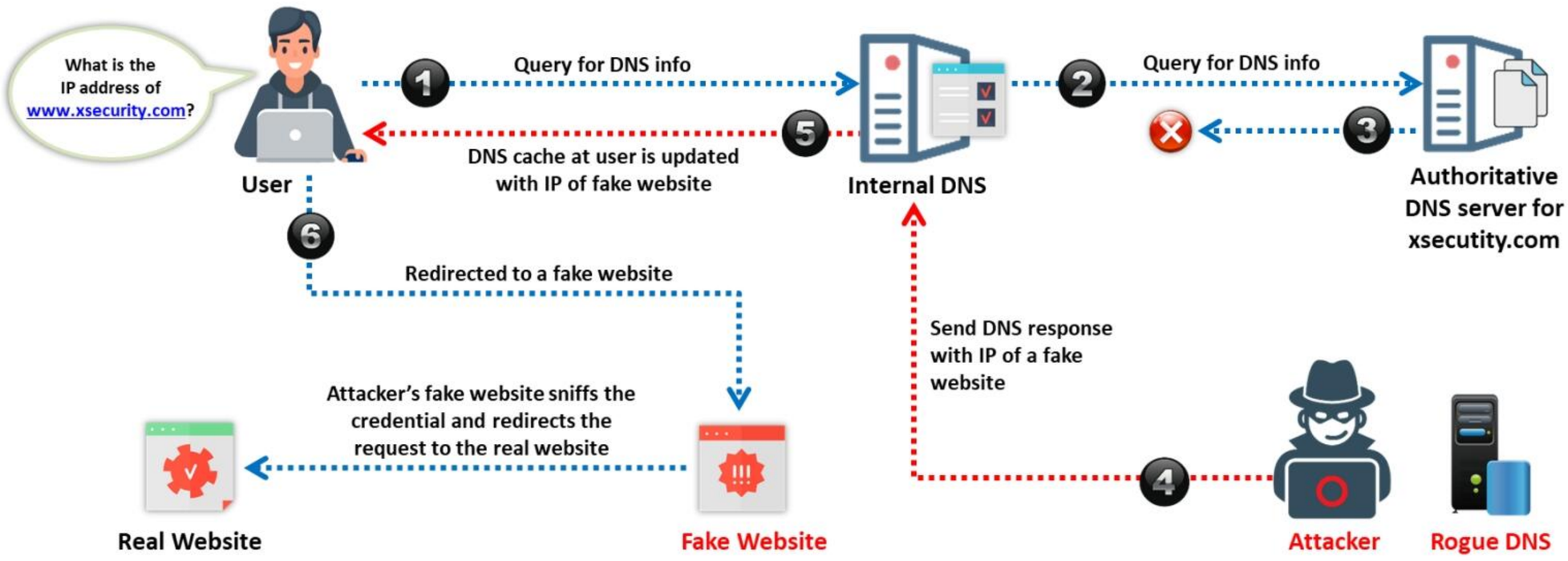
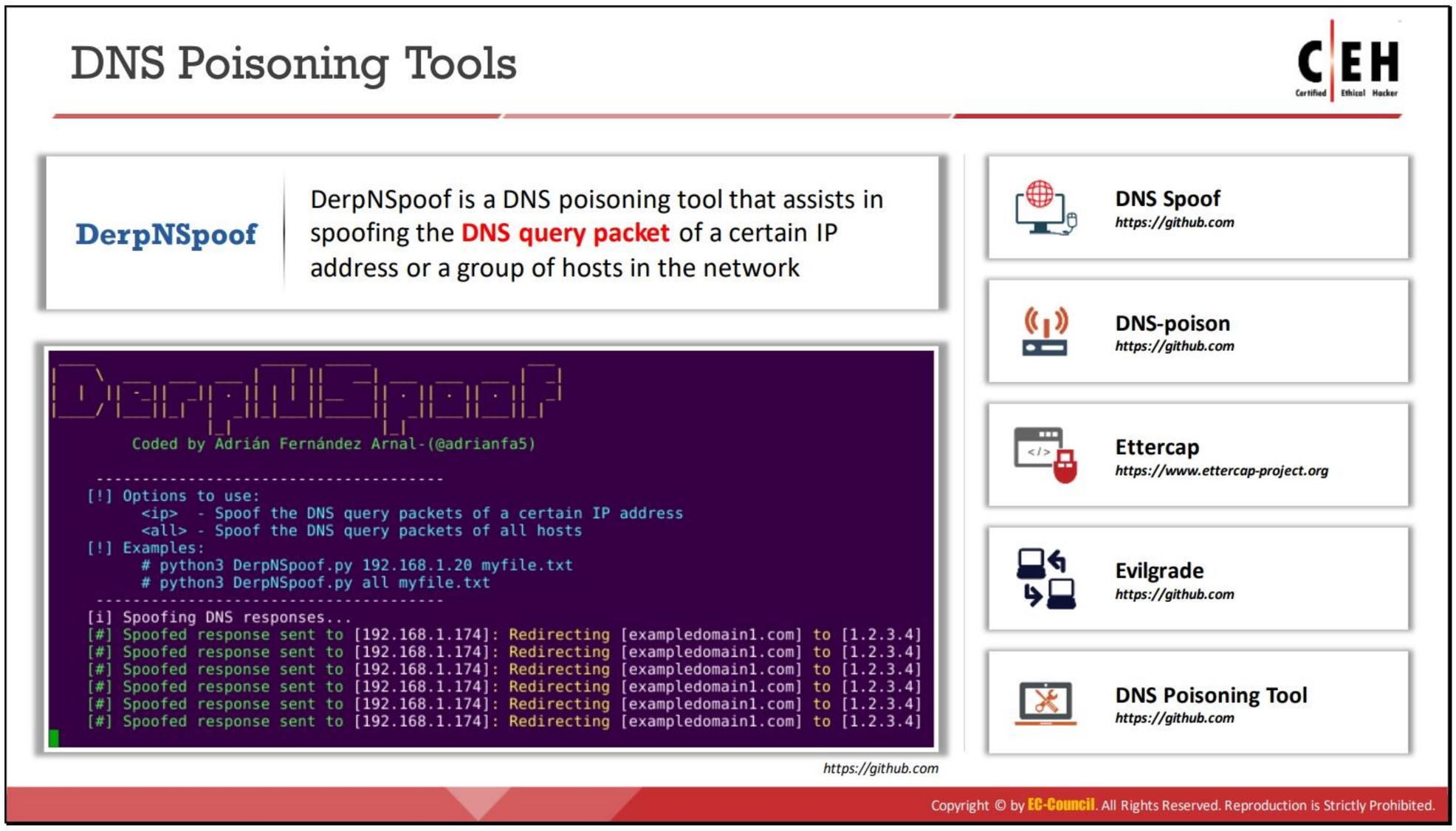


Figure 8.51: DNS cache poisoning

SAD DNS Attack

SAD DNS is a new variant of DNS cache poisoning, in which an attacker injects harmful DNS records into a DNS cache to divert all traffic toward their own servers. With this technique, attackers attempt to mislead client browsers to fake websites infected with malicious files, instead of the legitimate website. Attackers exploit side channels; flaws such as dnsmasq, unbound, and BIN in the latest OSes; and obsolete DNS software used to resolve DNS queries to perform SAD DNS attacks.

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



DNS Poisoning Tools

DNS poisoning tools allow attackers to redirect a domain name to a different IP address listed in a fake DNS entry file. The DNS request made to the target site goes through a server containing malicious content with the same name.

- **DerpNSpoof**

  Source: *https://github.com*

  DerpNSpoof is a DNS poisoning tool that assists in spoofing the DNS query packet of a certain IP address or a group of hosts in the network.

  Using this tool, attackers can create a list of fake DNS records and load it while running the tool to redirect the victim to some other website.

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

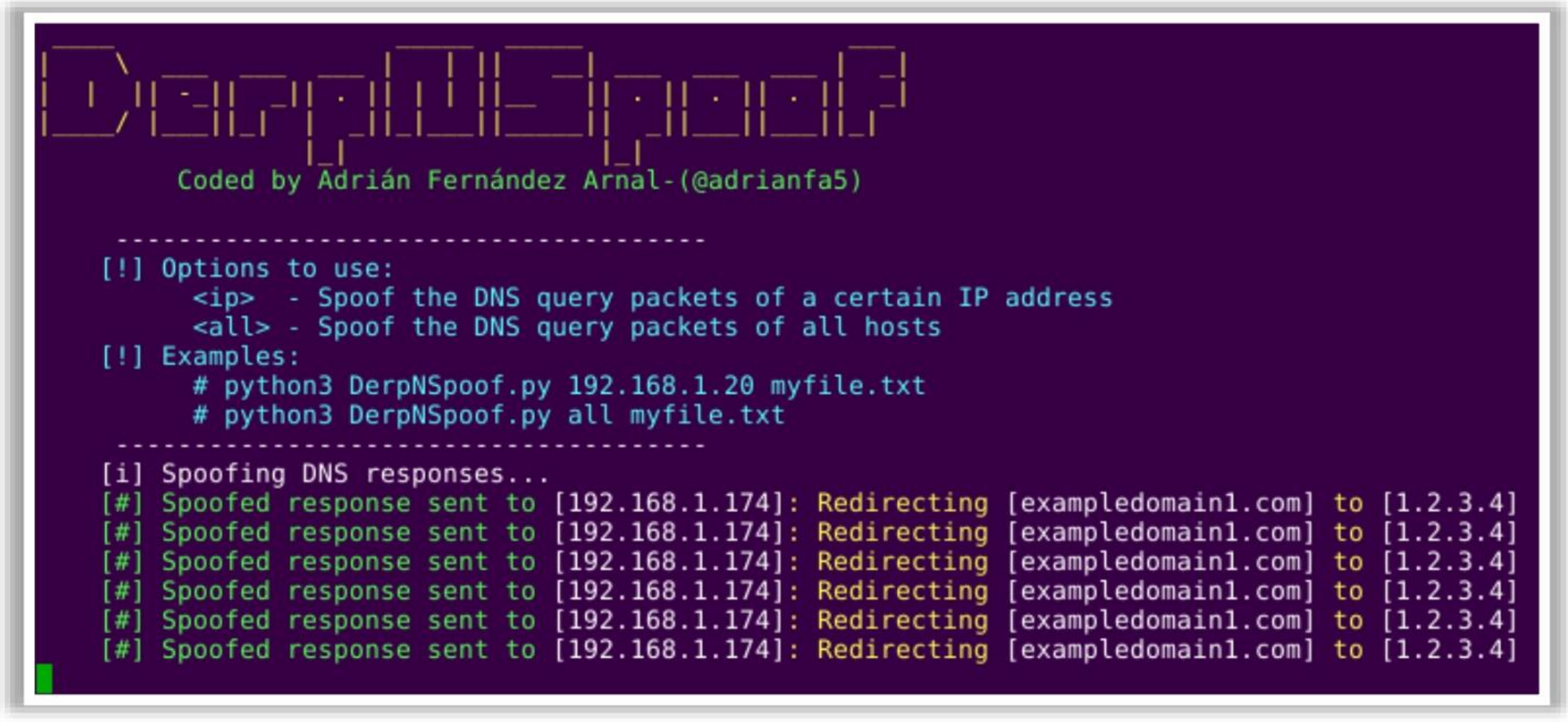
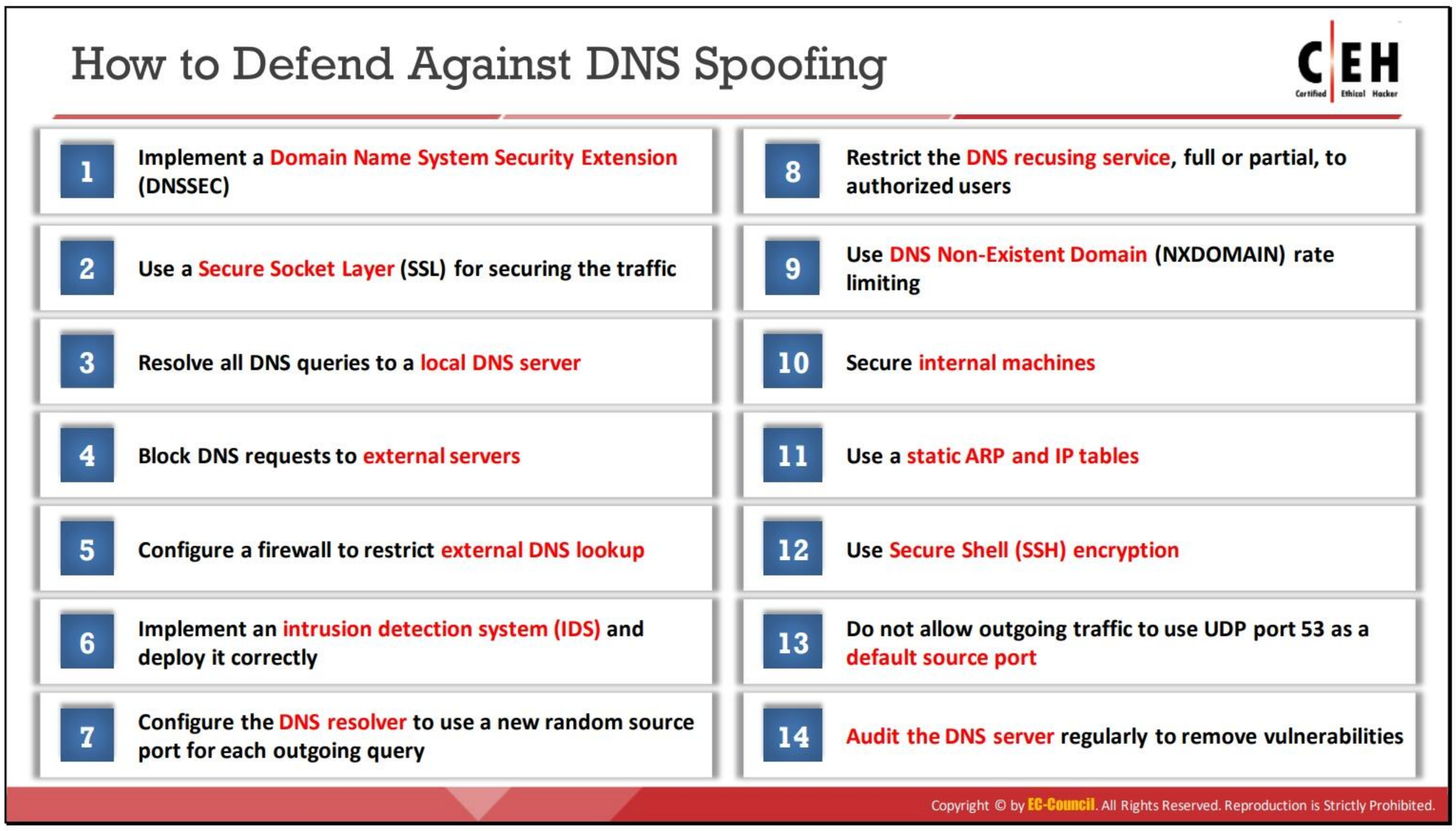


Figure 8.52: Screenshot of DerpNSpoof tool

Some examples of additional DNS poisoning tools are listed below:

- DNS Spoof (*https://github.com*)
- DNS-poison (*https://github.com*)
- Ettercap (*https://www.ettercap-project.org*)
- Evilgrade (*https://github.com*)
- DNS Poisoning Tool (*https://github.com*)

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



How to Defend Against DNS Spoofing

Major DNS implementations have reported attacks using DNS spoofing, and this vulnerability still affects a large number of organizations. This is because of a lack of information when performing DNS queries, which allows attackers to spoof DNS responses. We have already discussed how an attacker performs different types of DNS spoofing attacks. We now discuss how to defend a network from these types of attacks.

Countermeasures that help prevent DNS spoofing attacks are as follows:

- Implement Domain Name System Security Extensions (DNSSEC).
- Use a Secure Socket Layer (SSL) for securing the traffic.
- Resolve all DNS queries to a local DNS server.
- Block DNS requests to external servers.
- Configure a firewall to restrict external DNS lookup.
- Implement an intrusion detection system (IDS) and deploy it correctly.
- Configure the DNS resolver to use a new random source port for each outgoing query.
- Restrict the DNS recusing service, full or partial, to authorized users.
- Use DNS nonexistent domain (NXDOMAIN) rate limiting.
- Secure internal machines.
- Use static ARP and IP tables.
- Use Secure Shell (SSH) encryption.
- Do not allow outgoing traffic to use UDP port 53 as a default source port.

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

- Audit the DNS server regularly to remove vulnerabilities.
- Use sniffing detection tools.
- Do not open suspicious files.
- Always use trusted proxy sites.
- If a company handles its own resolver, it should be kept private and well protected.
- Randomize source and destination IP addresses.
- Randomize query IDs.
- Randomize the case in name requests.
- Use Public Key Infrastructure (PKI) to protect the server.
- Maintain a single or specific range of IP addresses to log into systems.
- Implement packet filtering for both inbound and outbound traffic.
- Restrict DNS zone transfers to a limited set of IP addresses.
- Employ DNS Cookie RFC 7873 or deactivate departing ICMP packets to prevent SAD DNS attacks.
- Use 0x20 encoding and DNS cookies as additional security to DNS messages.
- Reduce the timeout period for outstanding queries to prevent SAD DNS attacks.
- Update the DNS servers to the latest patches to prevent breaches.
- Use Remote Name Daemon Control (RNDC) keys if responses are to be made on port 53.
- Ensure that the “Hosts” file resolution is disabled on both the clients and servers.
- Configure STUB zones for frequently accessed domains.
- Implement robust password policies for users managing DNS records.

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

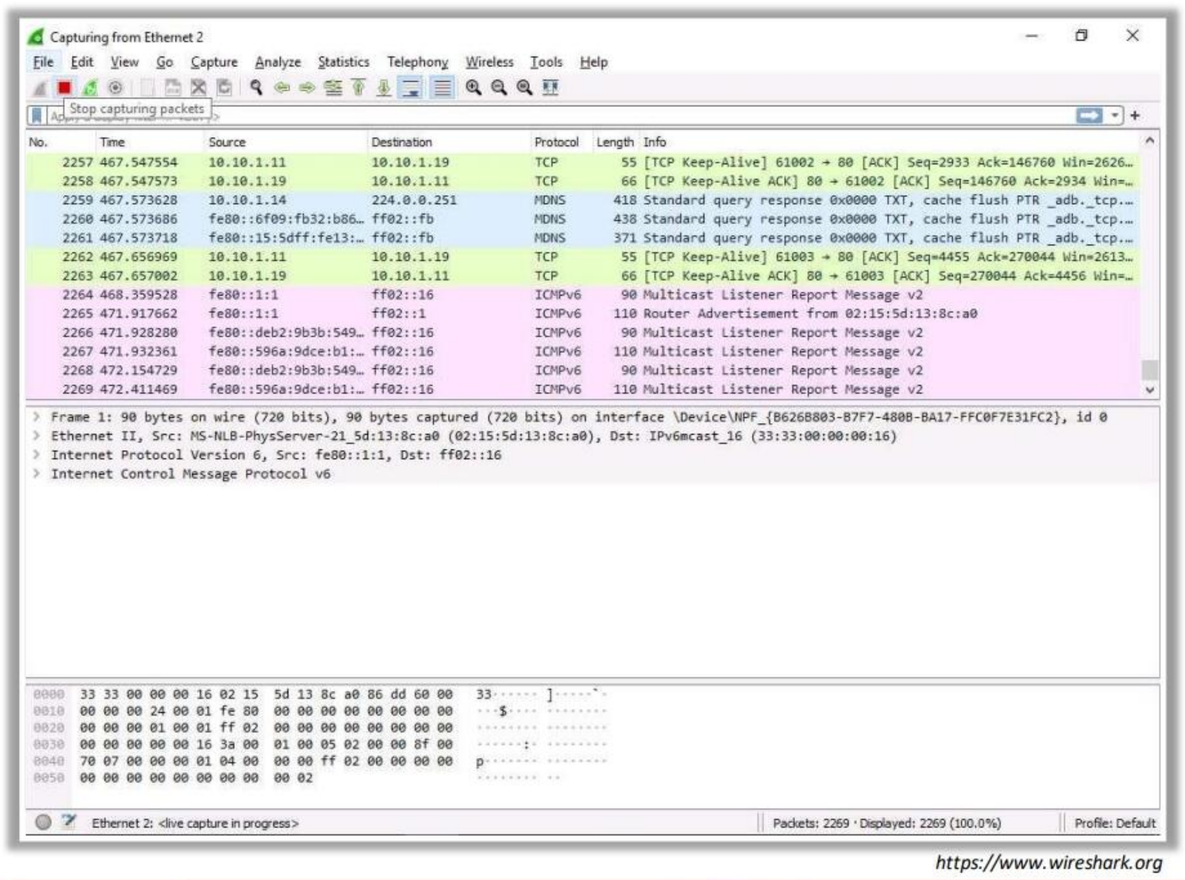
Sniffing Tools

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

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

Sniffing Tool: Wireshark

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



https://www.wireshark.org

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

Wireshark

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

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

As shown in the screenshot, attackers use Wireshark to sniff and analyze the packet flow in the target network and extract critical information about the target.

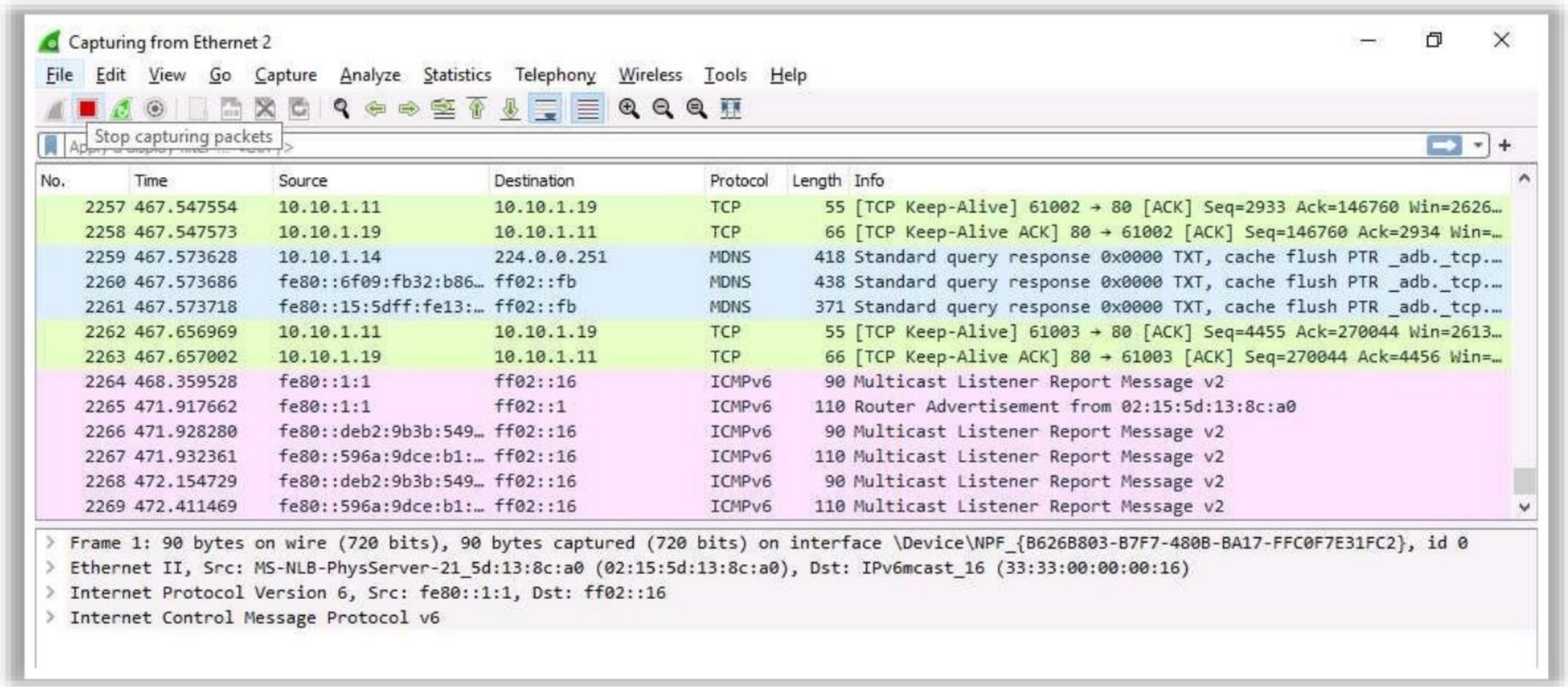
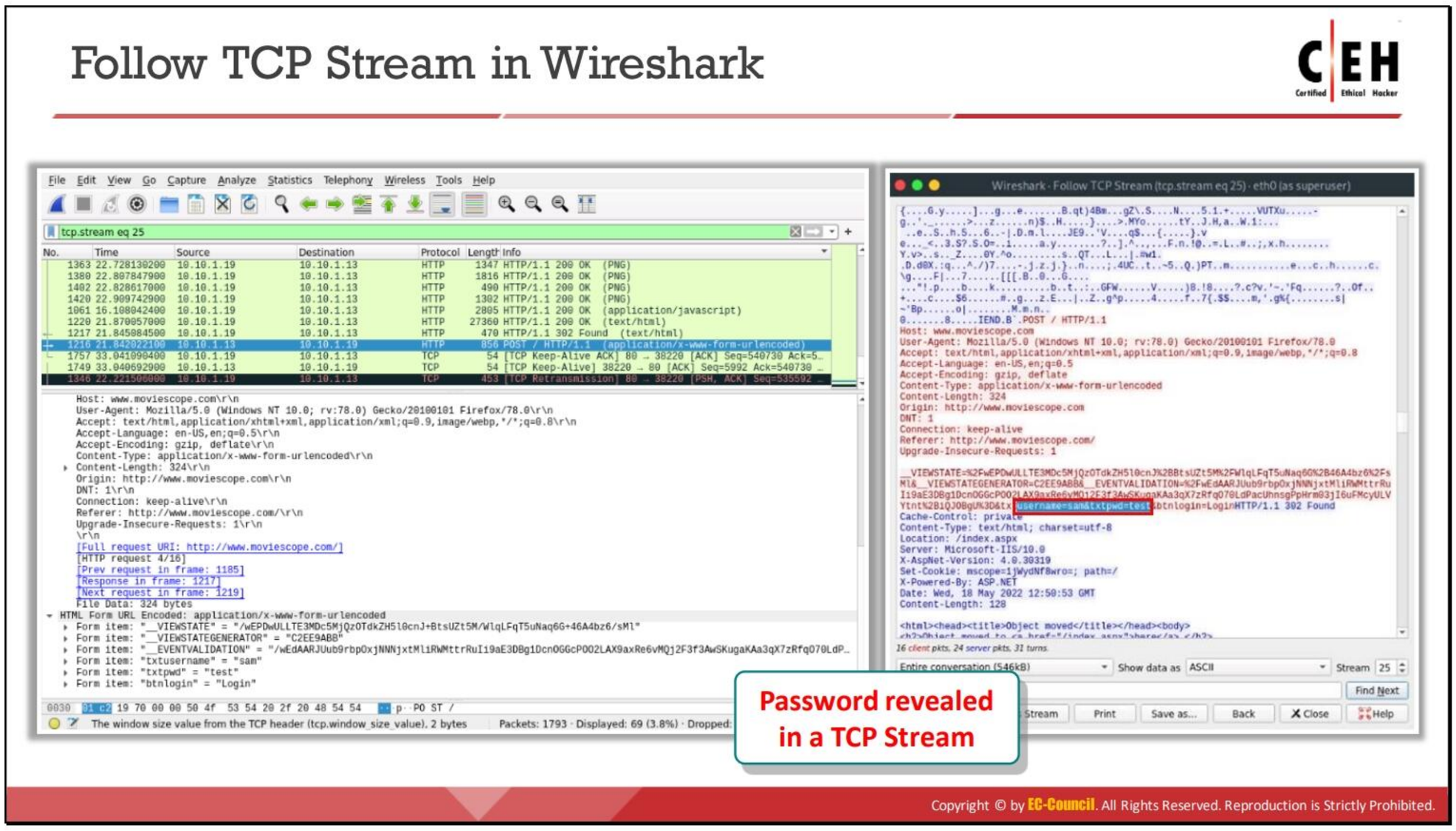


Figure 8.53: Capturing packets using Wireshark

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



Follow TCP Stream in Wireshark

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

Wireshark displays data from the TCP port with a feature known as "**Follow TCP stream**." The tool sees TCP data in the same way as that of the application layer. Use this tool to find passwords in a telnet session or to interpret 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 **Analyze** menu. Wireshark displays all the data from the TCP stream by setting an appropriate display filter. The tool displays the streaming content in the same sequence as it appeared on the network. It displays the captured data in ASCII, EBCDIC, hex dump, C array, or raw formats.

As shown in the screenshot, attackers can capture network traffic and gain the credentials of a target machine. They attempt to capture its remote interface and monitor the traffic generated from a user's browsing activities to extract confidential user information.

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

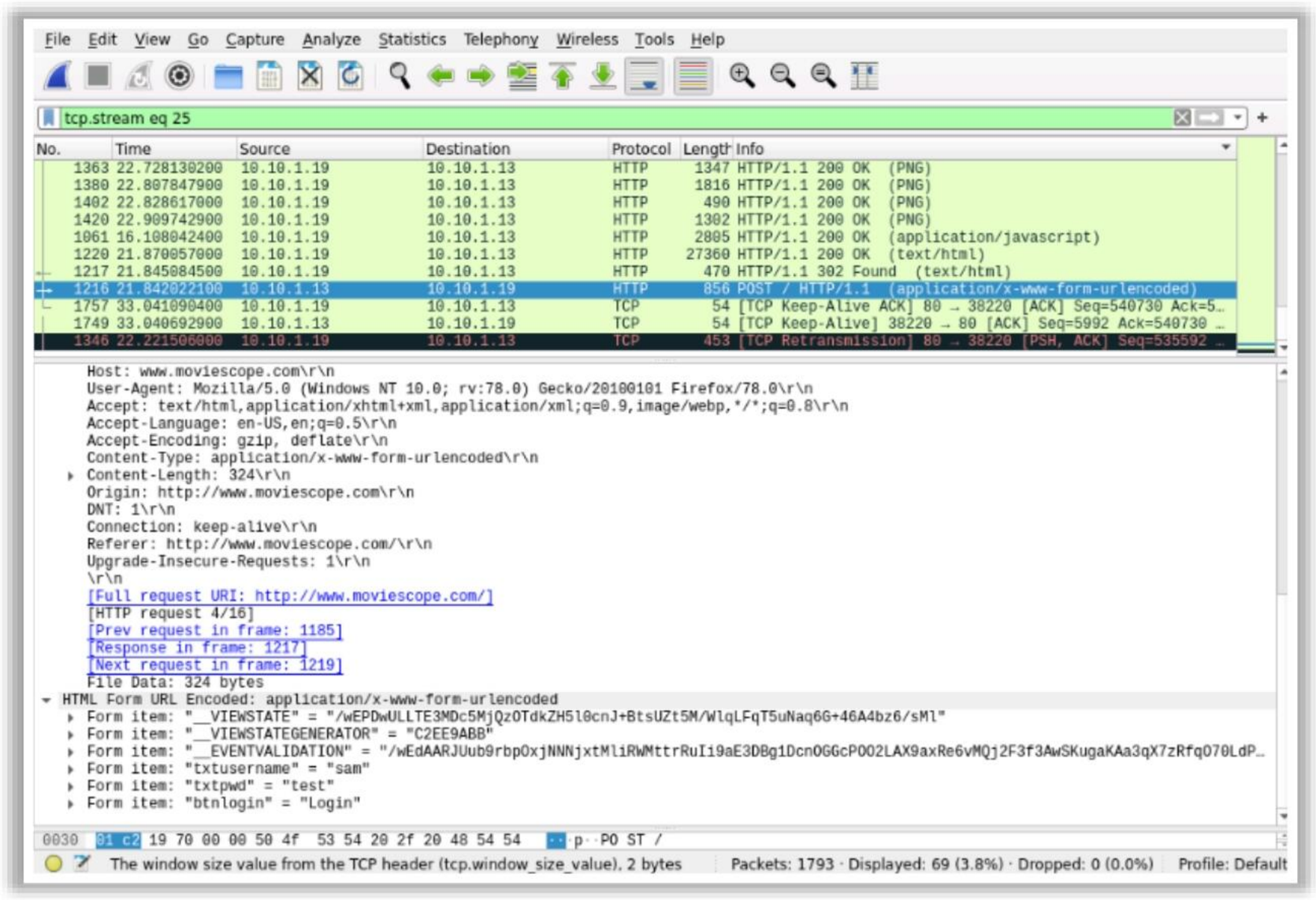


Figure 8.54: Wireshark capturing TCP Stream

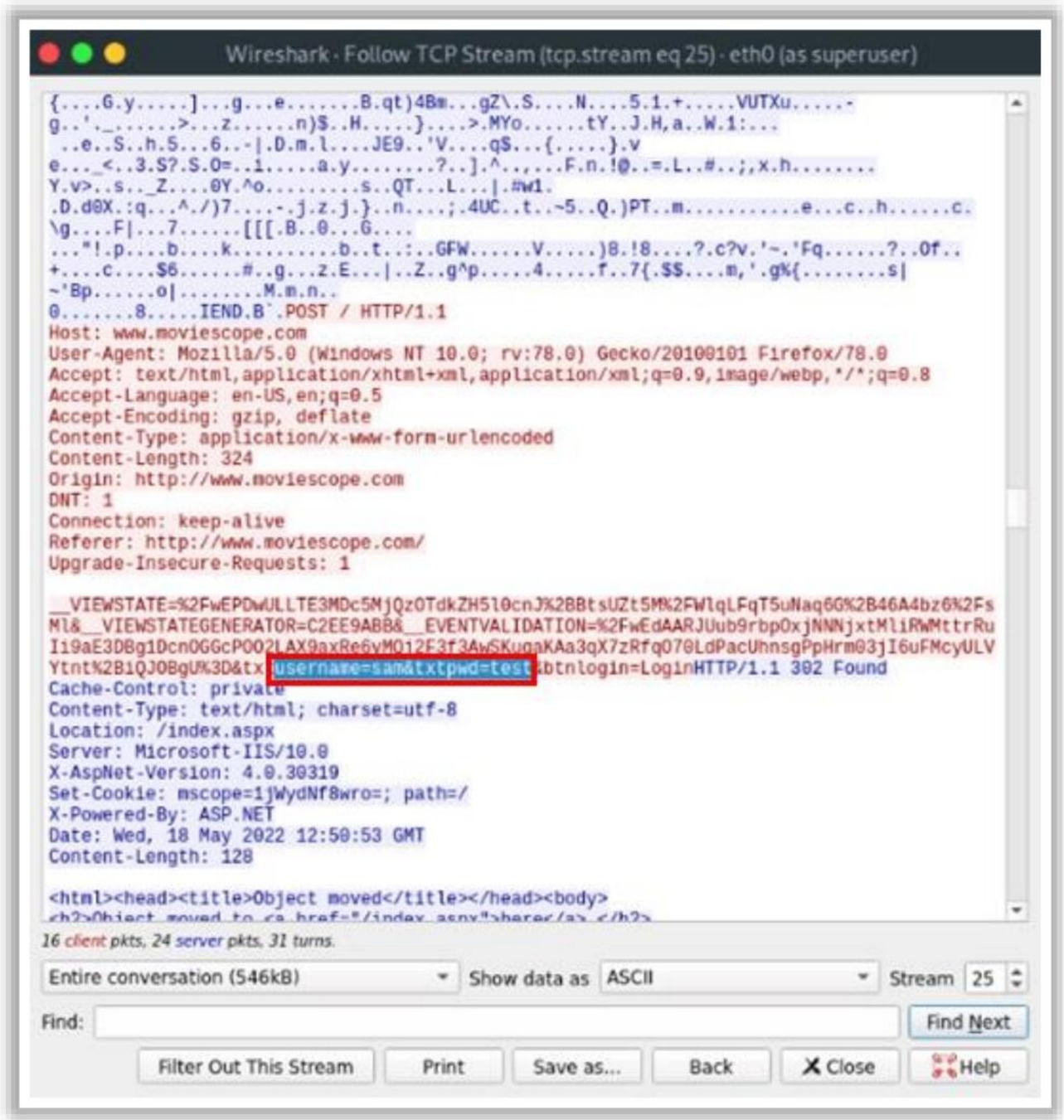
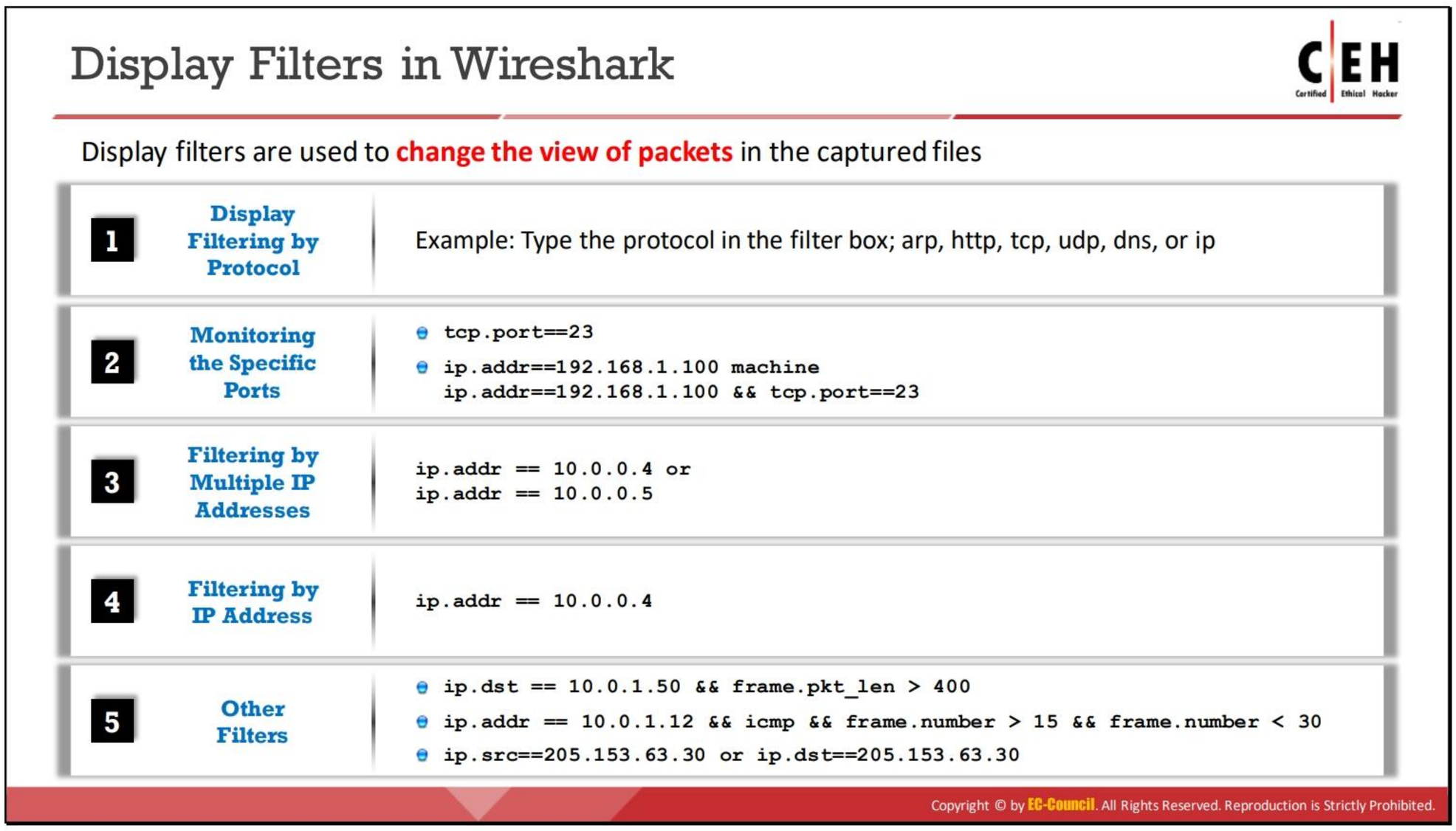


Figure 8.55: Password revealed in a TCP Stream

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



Display Filters in Wireshark

Source: *https://wiki.wireshark.org*

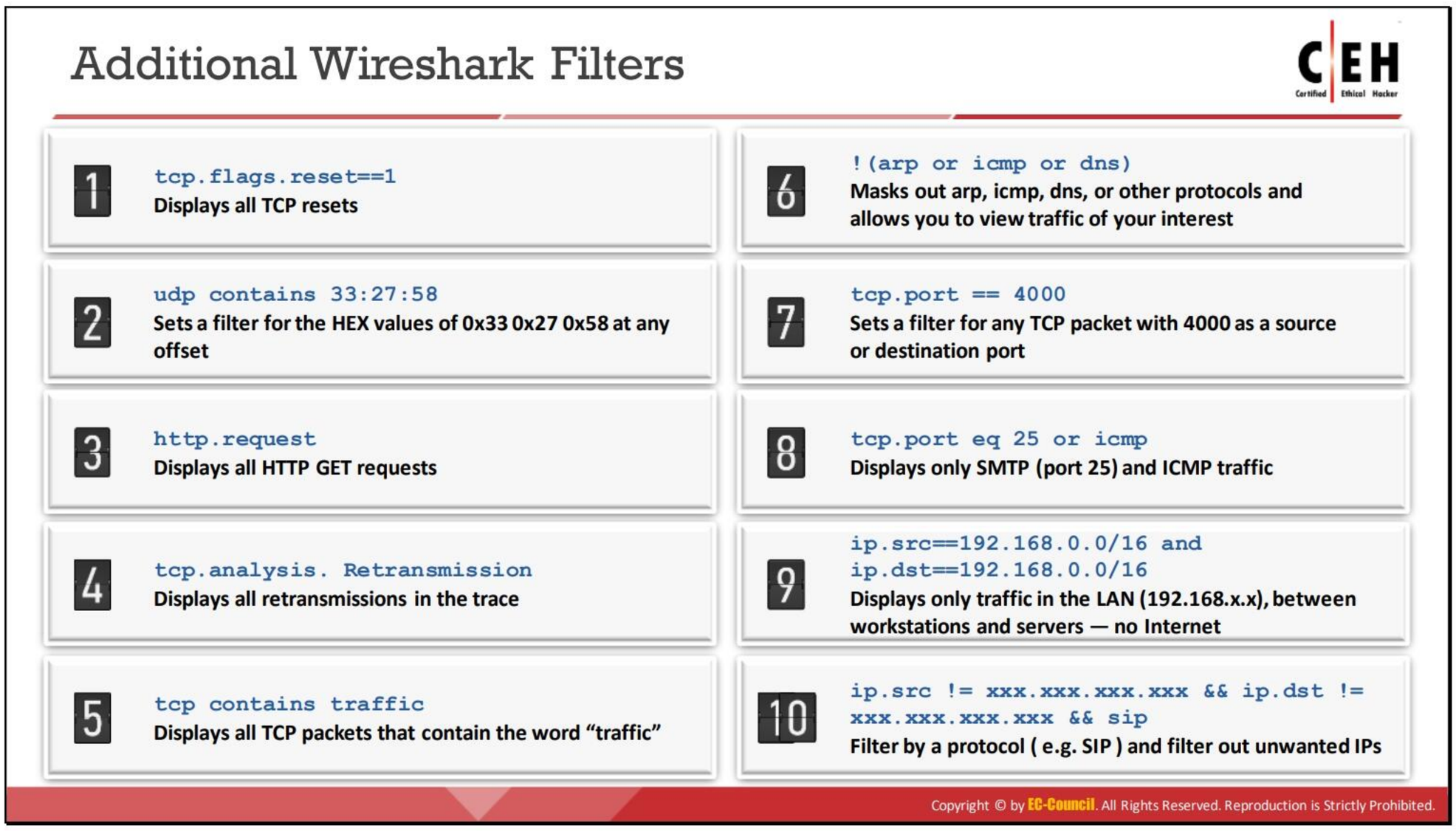
Wireshark features display filters that filter traffic on the target network by protocol type, IP address, port, etc. Display filters are used to change the view of packets in the captured files. To set up a filter, type the protocol name, such as arp, http, tcp, udp, dns, and ip, in the filter box of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

Some of the display filters in Wireshark are listed below:

- **Display Filtering by Protocol**

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

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



Additional Wireshark Filters

Source: *https://wiki.wireshark.org*

Some examples of additional Wireshark filters are listed below:

- **`tcp.flags.reset==1`**

  Displays all TCP resets

- **`udp contains 33:27:58`**

  Sets a filter for the hex values of 0×33 0×27 0×58 at any offset

- **`http.request`**

  Displays all HTTP GET requests

- **`tcp.analysis.retransmission`**

  Displays all retransmissions in the trace

- **`tcp contains traffic`**

  Displays all TCP packets that contain the word "traffic"

- **`!(arp or icmp or dns)`**

  Masks out arp, icmp, dns, or other protocols and allows you to view the traffic of your interest

- **`tcp.port == 4000`**

  Sets a filter for any TCP packet with 4000 as a source or destination port

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

- **`tcp.port eq 25 or icmp`**

  Displays only SMTP (port 25) and ICMP traffic

- **`ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16`**

  Displays only traffic in the LAN (192.168.x.x), between workstations and servers—no Internet

- **`ip.src != xxx.xxx.xxx.xxx && ip.dst != xxx.xxx.xxx.xxx && sip`**

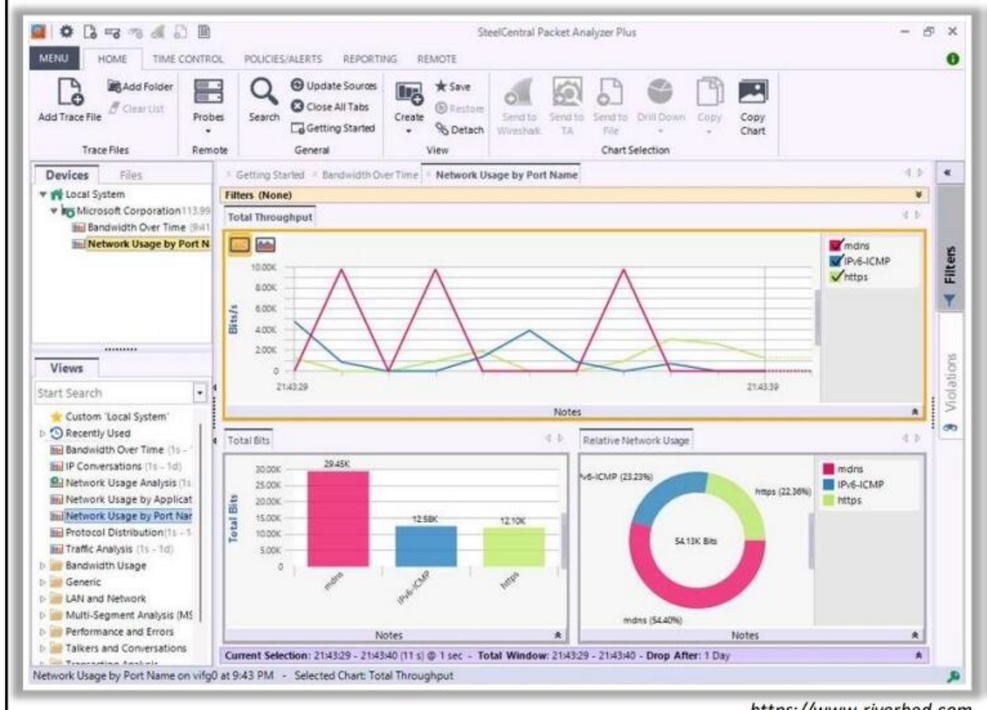
  Filters by a protocol (e.g., SIP) and filters out unwanted Ips

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

Sniffing Tools

Riverbed Packet Analyzer Plus

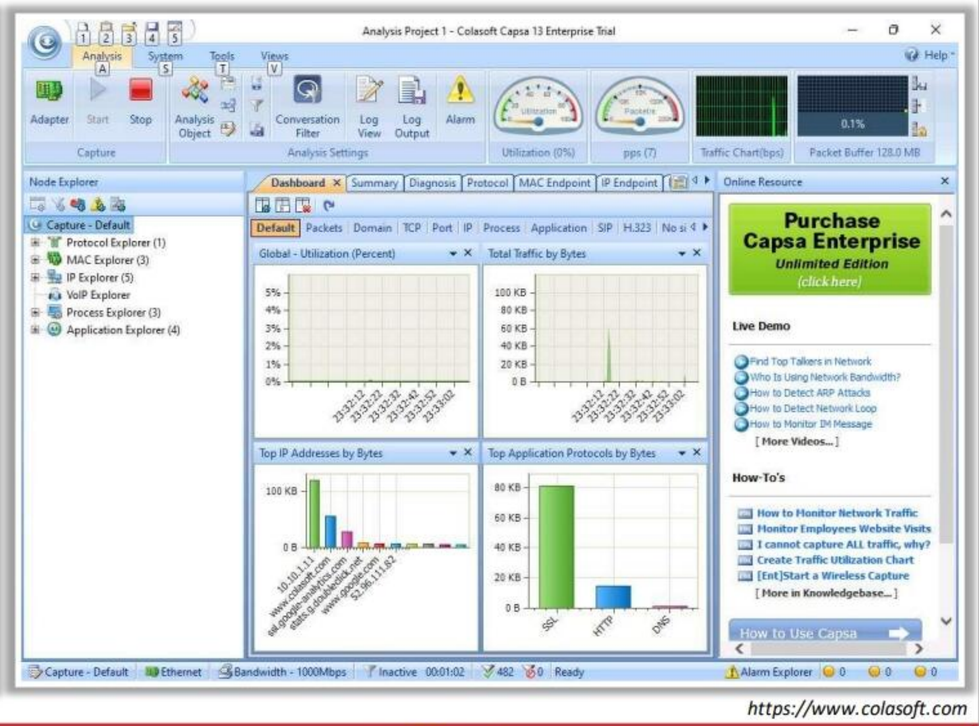
Riverbed Packet Analyzer Plus performs the **real-time network packet analysis** and reporting of large trace files



https://www.riverbed.com

Capsa Portable Network Analyzer

Capsa, a portable network performance analysis and diagnostics tool, provides **packet capture** and **analysis** capabilities with an easy-to-use interface



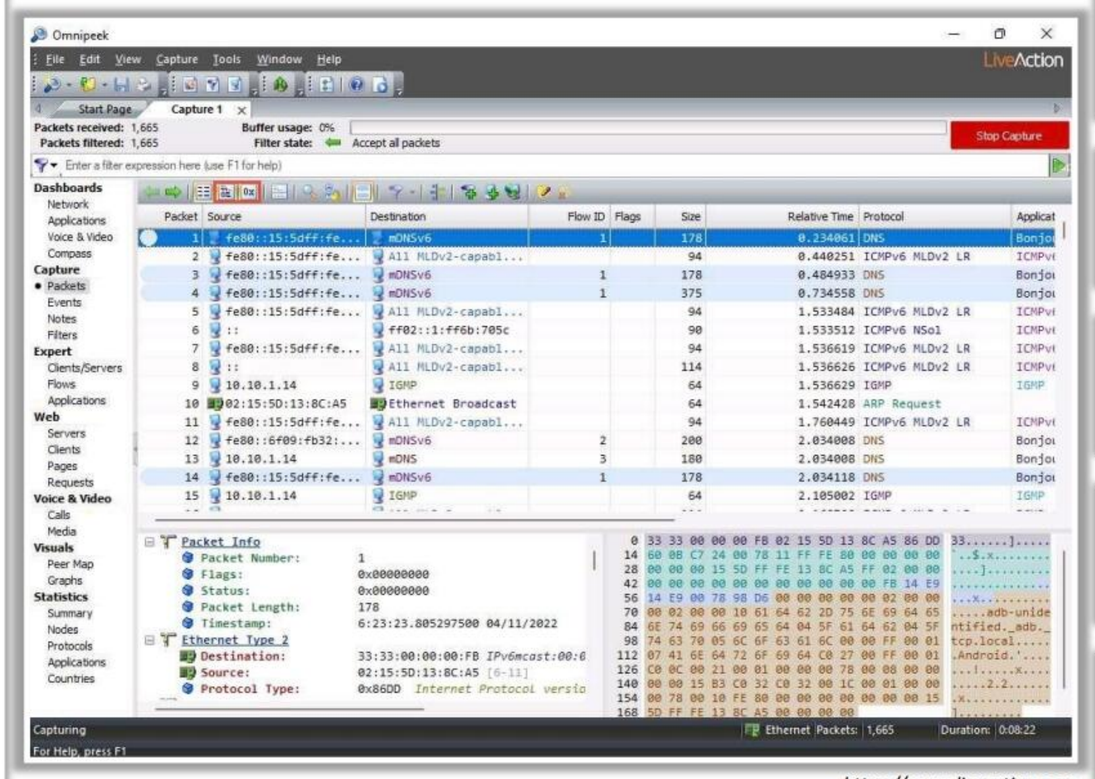
https://www.colasoft.com

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

Sniffing Tools (Cont'd)

OmniPeek

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



https://www.liveaction.com

RITA (Real Intelligence Threat Analytics)
https://www.activecountermeasures.com

Observer Analyzer
https://www.viavisolutions.com

PRTG Network Monitor
https://www.paessler.com

SolarWinds Deep Packet Inspection and Analysis
https://www.solarwinds.com

Xplico
https://www.xplico.org

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

Sniffing Tools

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

- **Riverbed Packet Analyzer Plus**

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

  Riverbed Packet Analyzer Plus performs the real-time network packet analysis and reporting of large trace files using an intuitive GUI and a broad selection of pre-defined analysis views. Use Packet Analyzer Plus with Riverbed AppResponse or any locally presented trace files to quickly identify and troubleshoot complex network and application performance issues down to the bit level through full integration with Wireshark.

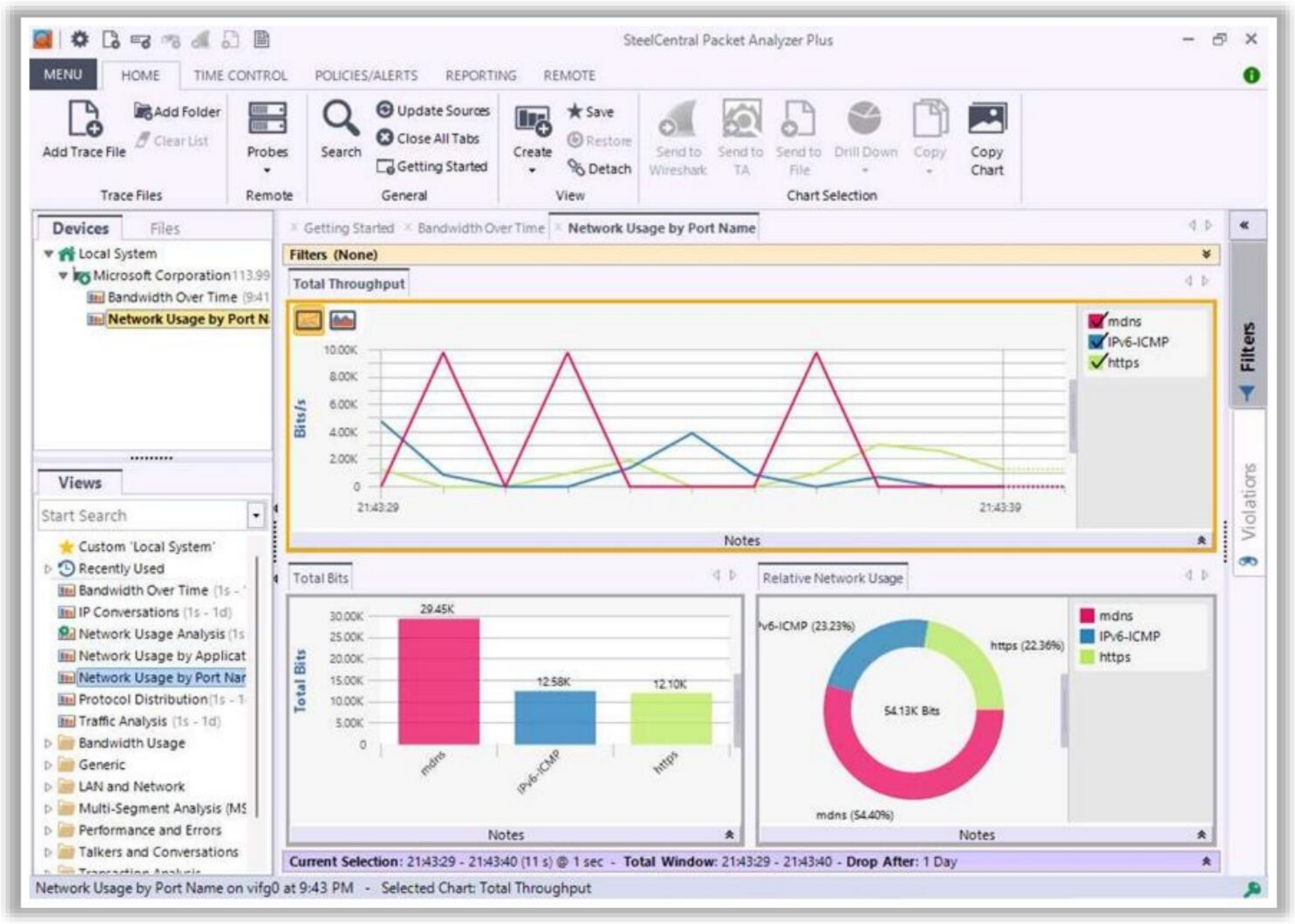


Figure 8.56: Screenshot of Riverbed Packet Analyzer Plus

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

- **Capsa Portable Network Analyzer**

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

  Capsa, a portable network performance analysis and diagnostics tool, provides packet capture and analysis with an easy-to-use interface, allowing users to protect and monitor networks in a critical business environment.

  An attacker can use this tool to sniff packets from the target network and detect network vulnerabilities.

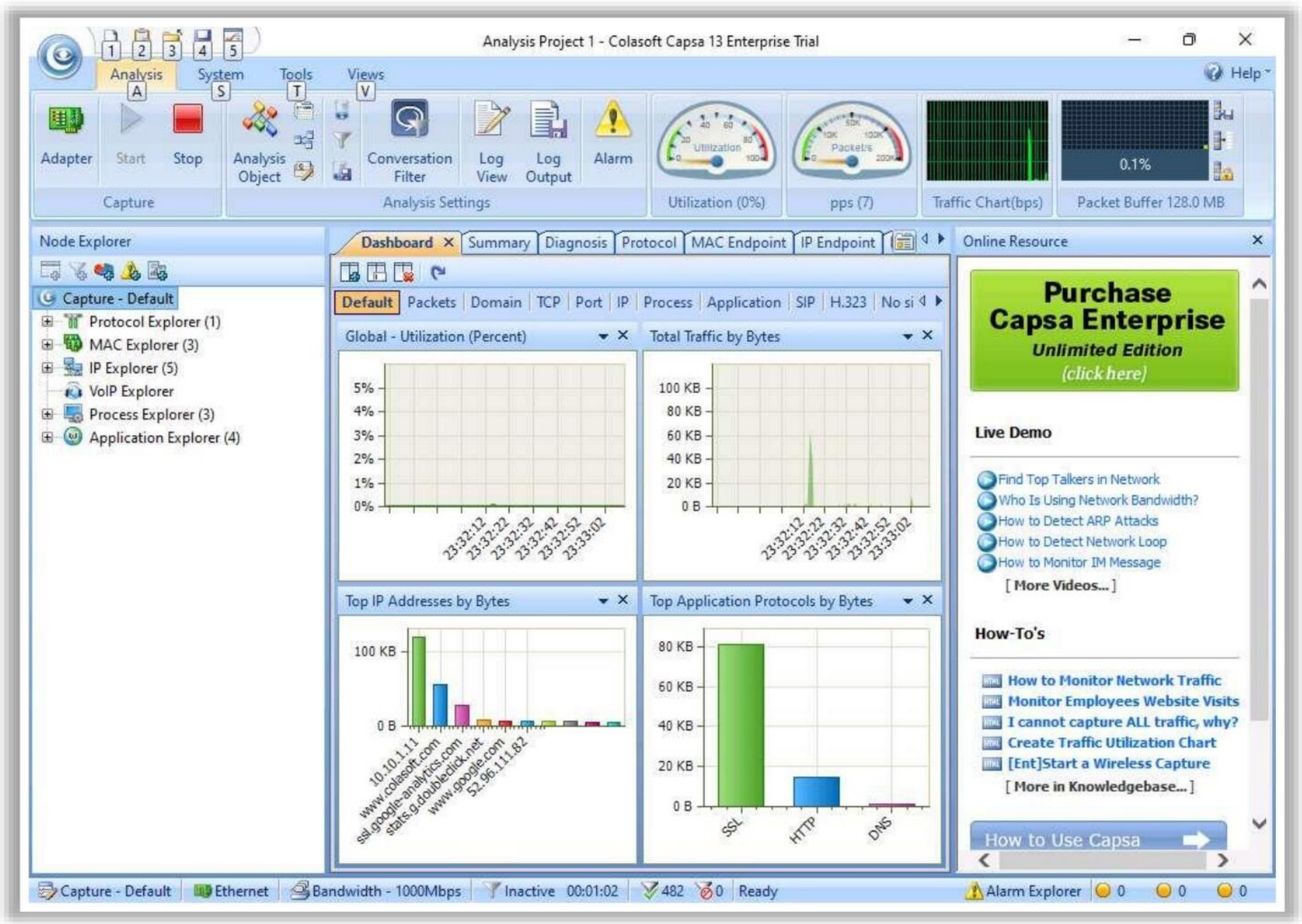


Figure 8.57: Screenshot of Capsa Portable Network Analyzer

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

- **OmniPeek**

  Source: *https://www.liveaction.com*

  OmniPeek Network Analyzer provides real-time visibility and expert analysis of each part of the target network. This tool will analyze, drill down, and fix performance bottlenecks across multiple network segments. Analytic plug-ins provide targeted visualization and search abilities within OmniPeek. The Google Maps plug-in enhances the analysis capabilities of OmniPeek. It displays a Google map in the OmniPeek capture window that shows the locations of all the public IP addresses of captured packets.

  Attackers can use OmniPeek to monitor and analyze network traffic of the target network in real time, identify the source location of that traffic, and attempt to obtain sensitive information, as well as find any network loopholes.

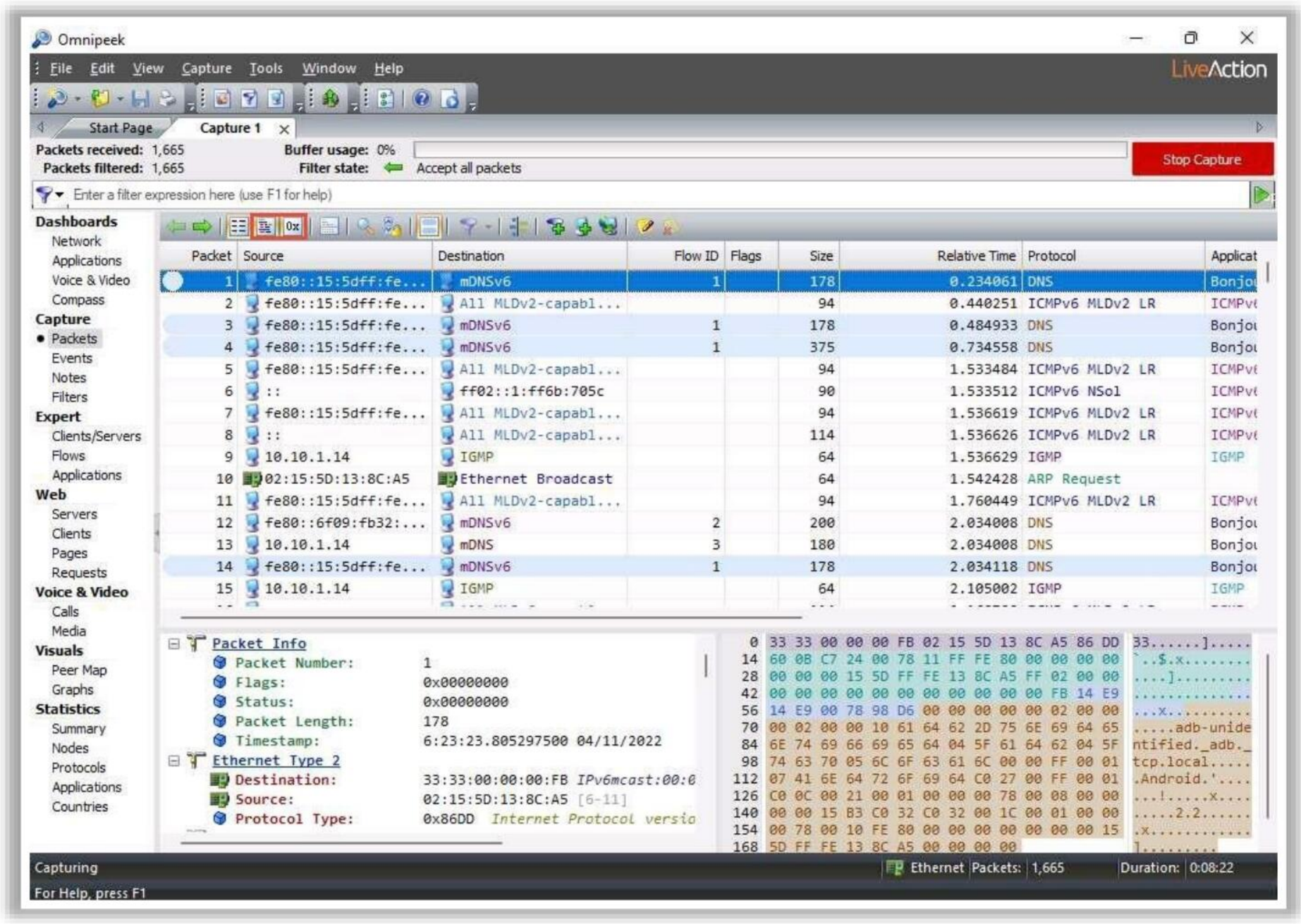


Figure 8.58: Screenshot of OmniPeek

Some examples of additional sniffing tools are listed below:

- RITA (Real Intelligence Threat Analytics) (*https://www.activecountermeasures.com*)
- Observer Analyzer (*https://www.viavisolutions.com*)
- PRTG Network Monitor (*https://www.paessler.com*)
- SolarWinds Deep Packet Inspection and Analysis (*https://www.solarwinds.com*)
- Xplico (*https://www.xplico.org*)

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

Packet Sniffing Tools for Mobile Phones

- **Sniffer Wicap**

  Source: *https://play.google.com*

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

  Attackers can use this tool to capture packets for various types of connections, such as Wi-Fi, 3G, and LTE.

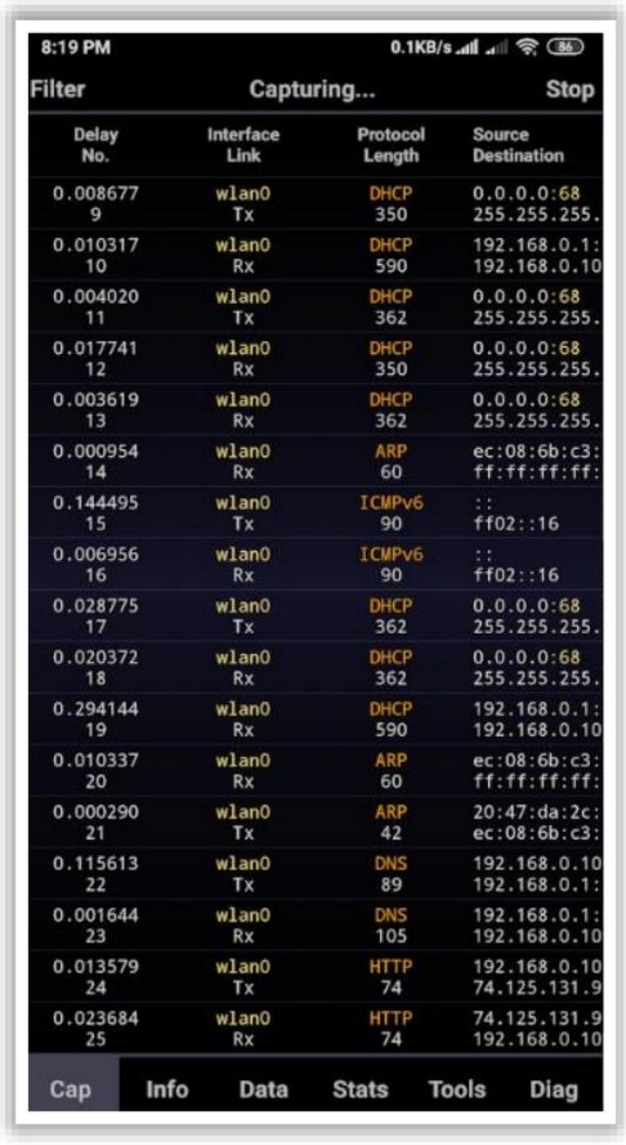


Figure 8.59: Screenshot of Sniffer Wicap

- **FaceNiff**

  Source: *http://faceniff.ponury.net*

  FaceNiff is an Android app that can sniff and intercept web session profiles over a Wi-Fi connection to a 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**
All Rights Reserved. Reproduction is Strictly Prohibited.

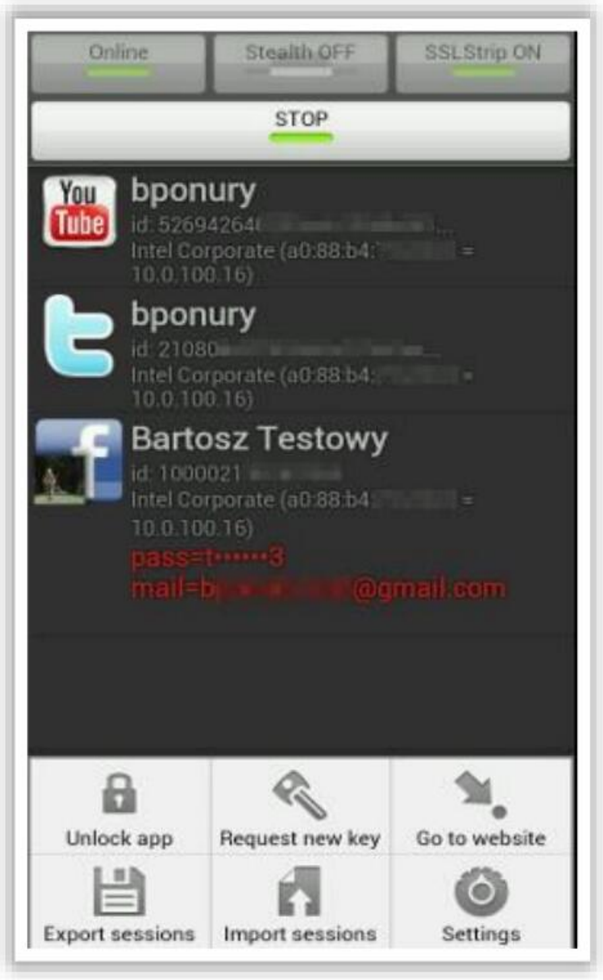


Figure 8.60: Screenshot of FaceNiff

- **Packet Capture**

  Source: *https://play.google.com*

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

  Attackers can use this tool to capture network packets and record them, perform SSL decryption using MITM techniques, and further show packets in either hex or text.

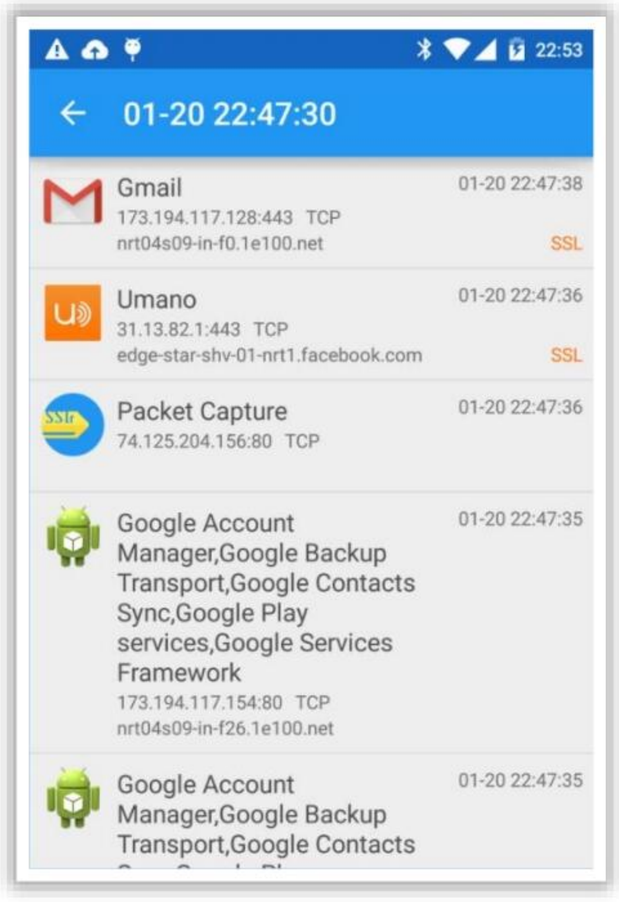
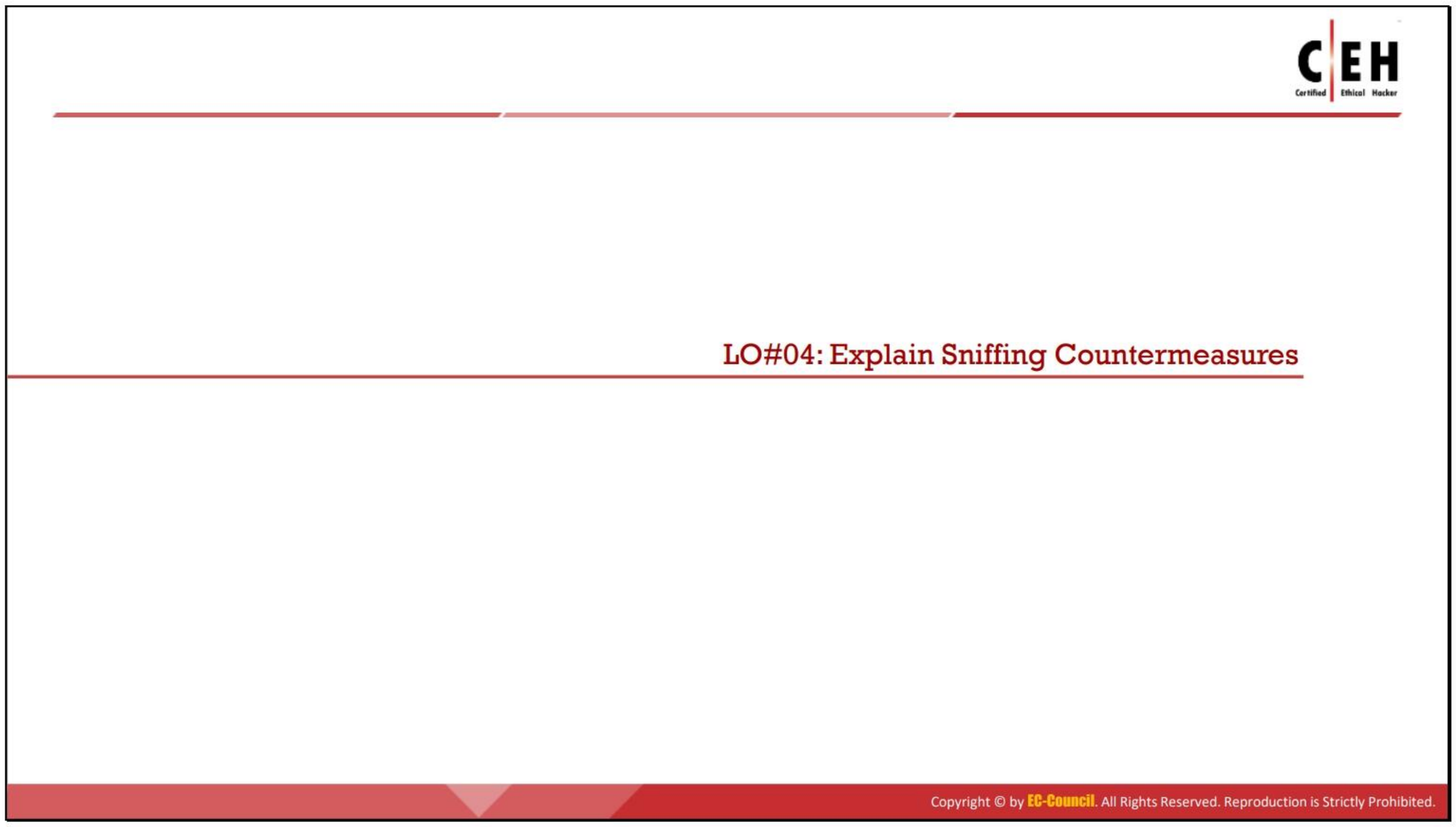


Figure 8.61: Screenshot of Packet Capture

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



Sniffing Countermeasures

The previous section described how an attacker performs sniffing with different techniques and tools. It is very difficult to detect passive sniffers, especially when they are running on a shared Ethernet connection. This section describes countermeasures and possible defensive techniques used to defend a target network against sniffing attacks. This section also discusses some sniffing detection techniques.

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

How to Defend Against Sniffing

01	**Restrict physical access** to the network media to ensure that a packet sniffer cannot be installed
02	Use **end-to-end encryption** to protect confidential information
03	Permanently add the **MAC address of the gateway** to the ARP cache
04	Use **static IP addresses** and **ARP tables** to prevent attackers from adding spoofed ARP entries for machines in the network
05	Turn off **network identification broadcasts**, and if possible, restrict the network to authorized users to protect the 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, and SSL for email connections, 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)

08	Use **HTTPS** instead of HTTP to protect usernames and passwords
09	Use a **switch instead of a hub** as a switch delivers data to the intended recipient only
10	Use **Secure File Transfer Protocol (SFTP)**, instead of FTP for the secure transfer of files
11	Use **PGP** and **S/MIME**, **VPN**, **IPsec**, **SSL/TLS**, **Secure Shell (SSH)**, and One-time passwords (OTPs)
12	Always encrypt wireless traffic with a **strong encryption protocol** such as WPA2 and WPA3
13	**Retrieve the MAC** directly from the NIC instead of the OS; this prevents MAC address spoofing
14	Use **tools** to determine if any NICs are running in the promiscuous mode
15	Use **access-control lists (ACLs)** to allow access only to a fixed range of trusted IP addresses in a network

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

How to Defend Against Sniffing

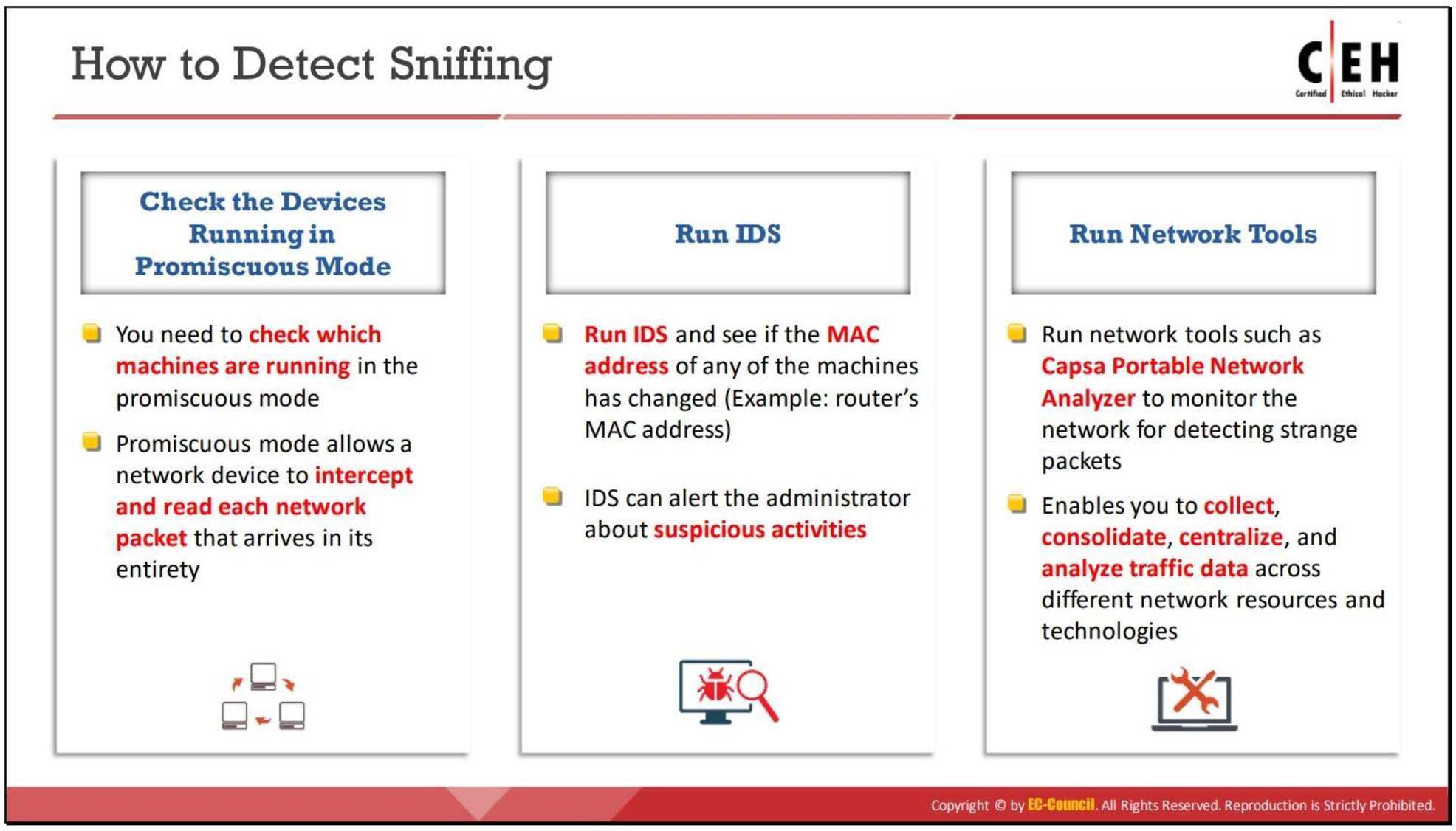
Listed below are some of the countermeasures to defend against sniffing:

- Restrict physical access to the network media to ensure that a packet sniffer cannot be installed.
- Use end-to-end encryption to protect confidential information.

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

- Permanently add the MAC address of the gateway to the ARP cache.
- Use static IP addresses and ARP tables to prevent attackers from adding the spoofed ARP entries for machines in the network.
- Turn off network identification broadcasts and, if possible, restrict the network to authorized users to protect the network from being discovered with sniffing tools.
- Use IPv6 instead of IPv4, as IPsec implementation is optional in IPv4 but mandatory in IPv6.
- Use encrypted sessions such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, and SSL for email connections to protect wireless network users against sniffing attacks.
- Use HTTPS instead of HTTP to protect usernames and passwords.
- Use a switch instead of the hub, as a switch delivers data only to the intended recipient.
- Use Secure File Transfer Protocol (SFTP) instead of FTP for the secure transfer of files.
- Use PGP and S/MIME, VPN, IPsec, SSL/TLS, SSH, and one-time passwords (OTPs).
- Use POP2 or POP3 instead of POP to download emails from email servers.
- Use SNMPv3 instead of SNMPv1 or SNMPv2 to manage networked devices.
- Always encrypt the wireless traffic with a strong encryption protocol such as WPA2 or WPA3.
- Retrieve MAC addresses directly from NICs instead of the OS; this prevents MAC address spoofing.
- Use tools to determine if any NICs are running in the promiscuous mode.
- Use access-control lists (ACLs) to allow access only to a fixed range of trusted IP addresses in a network.
- Change default passwords to complex passwords.
- Avoid broadcasting session set identifiers (SSIDs).
- Implement a MAC filtering mechanism on the router.
- Implement network scanning and monitoring tools to detect malicious intrusions, rogue devices, and sniffers connected to the network.
- Avoid accessing unsecured networks and open Wi-Fi networks.
- Implement secure network segmentation.

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



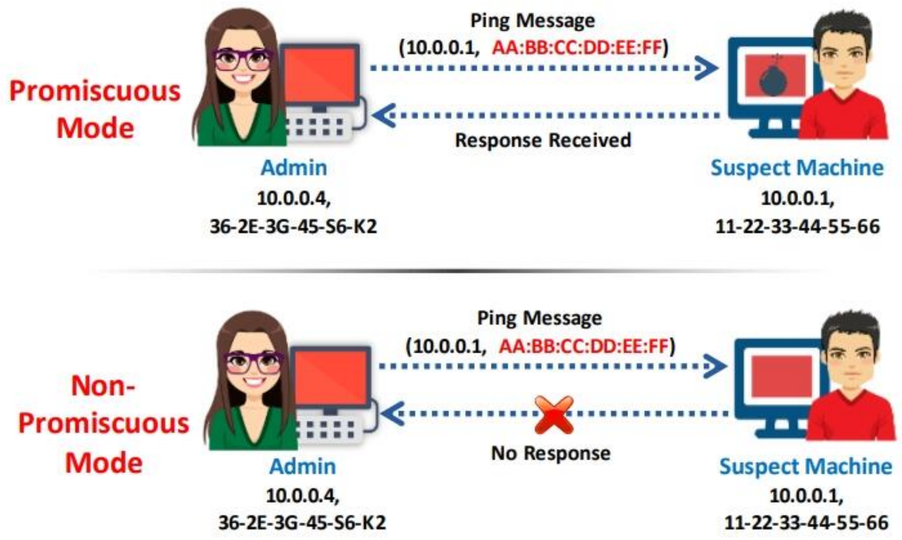
How to Detect Sniffing

It is not easy to detect a sniffer on a network as it only captures data and runs in promiscuous mode. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer leaves no trace as it does not transmit data. To find sniffers, check for systems that are running in promiscuous mode, which is an NIC mode that allows all packets (traffic) to pass without validating their destination address. Standalone sniffers are difficult to detect because they do not transmit data traffic. The reverse DNS lookup method helps to detect non-standalone sniffers. There are many tools, such as Nmap, that are available to use for the detection of promiscuous mode. Run IDS and note whether the MAC addresses of certain machines have changed (for example, the router's MAC address). An IDS can detect sniffing activities on a network. It notifies or alerts the administrator when a suspicious activity, such as sniffing or MAC spoofing, occurs. Network tools such as Capsa Portable Network Analyzer monitor the network for strange packets such as those with spoofed addresses. This tool can collect, consolidate, centralize, and analyze traffic data across different network resources and technologies.

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

Sniffer Detection Techniques: Ping Method and DNS Method

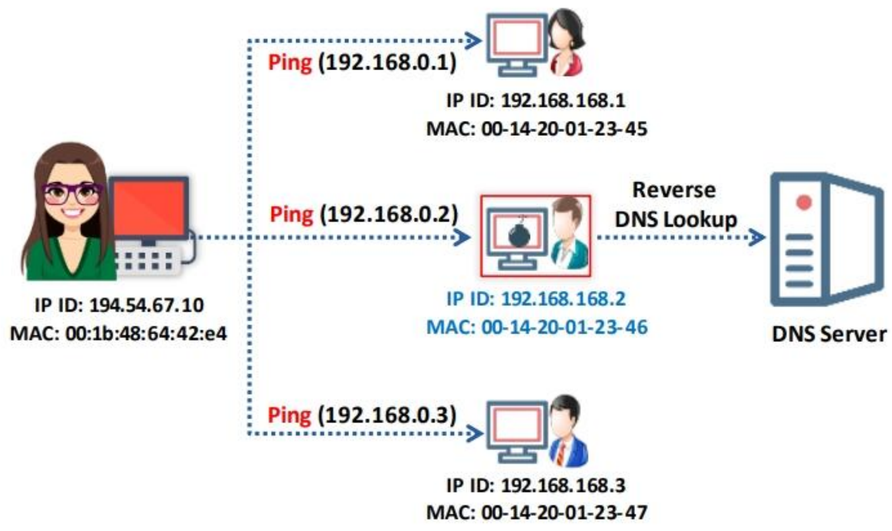
Ping Method



- Sends a ping request to the suspect machine with its IP address and an **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

DNS Method

- Most of the sniffers perform **reverse DNS lookups** to identify the machine from the IP address

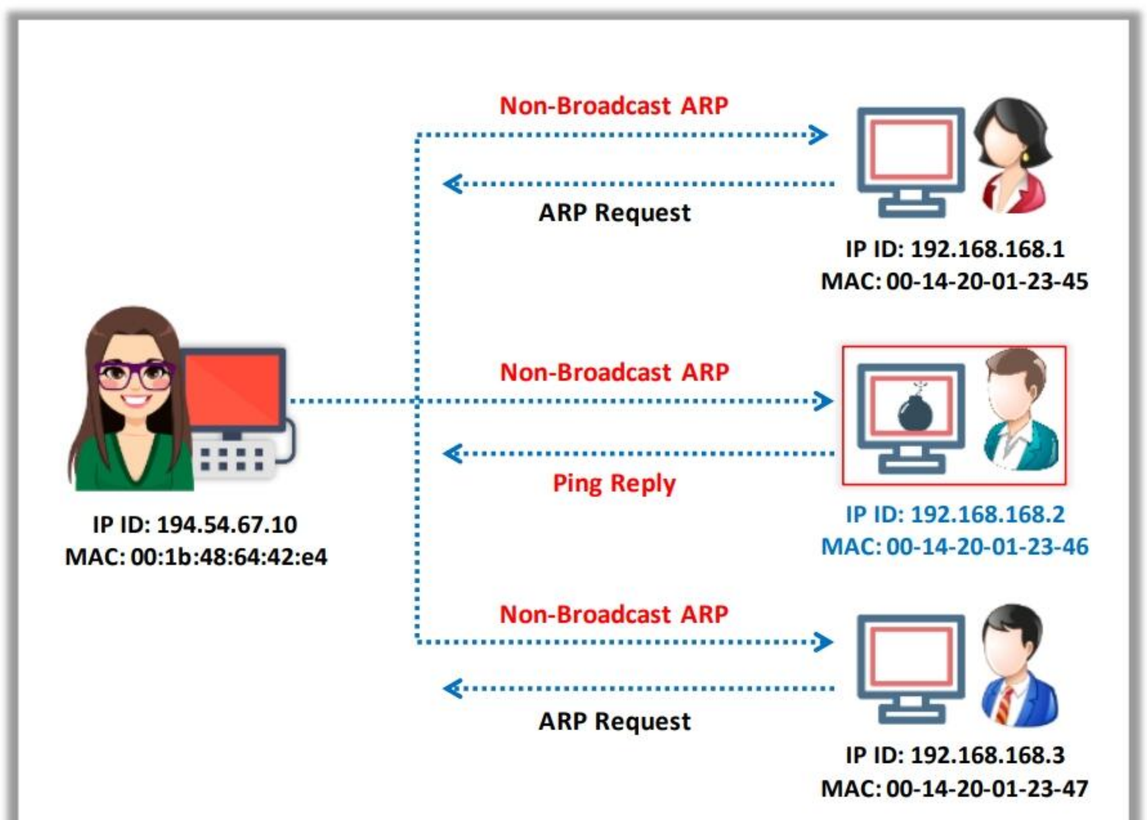


- A machine generating **reverse DNS lookup traffic** is very likely to be running a sniffer

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

Sniffer Detection Techniques: ARP Method

- Only the machine in the promiscuous mode (machine C) **caches the ARP information** (IP and MAC address mapping)
- A machine in the promiscuous mode **responds to the ping message** as it has the correct information about the host sending the **ping requests** in its cache; the rest of the machines will send an ARP probe to identify the source of the ping request



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

Sniffer Detection Techniques

- **Ping Method**

  To detect a sniffer on a network, identify the system on the network running in promiscuous mode. The ping method is useful in detecting a system that runs in promiscuous mode, which in turn helps to detect sniffers installed on the network.

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

Just send a ping request to the suspected machine with its IP address and incorrect MAC address. The Ethernet adapter will reject it because 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.

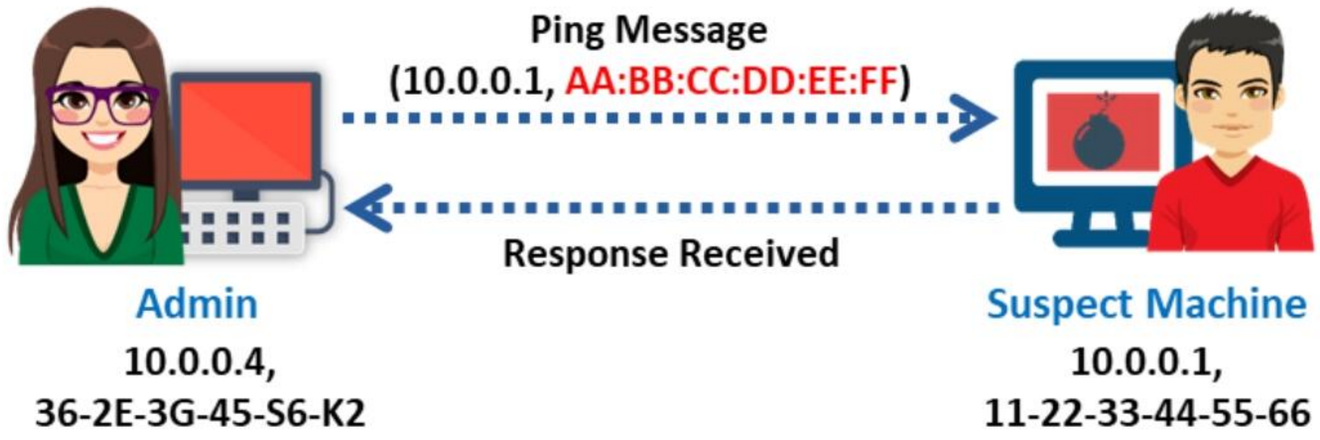


Figure 8.62: Promiscuous mode

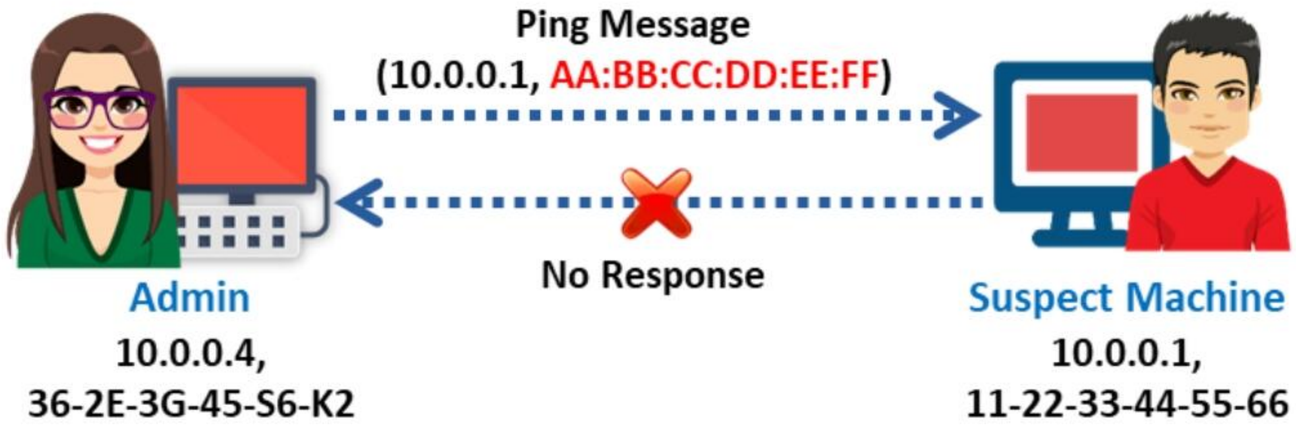


Figure 8.63: Non-promiscuous mode

- **DNS Method**

  The reverse DNS lookup is the opposite of the DNS lookup method. Sniffers using reverse DNS lookup increase network traffic. This increase in network traffic can be an indication of the presence of a sniffer on the network. 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. A machine generating reverse DNS lookup traffic will most likely be running a sniffer.

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

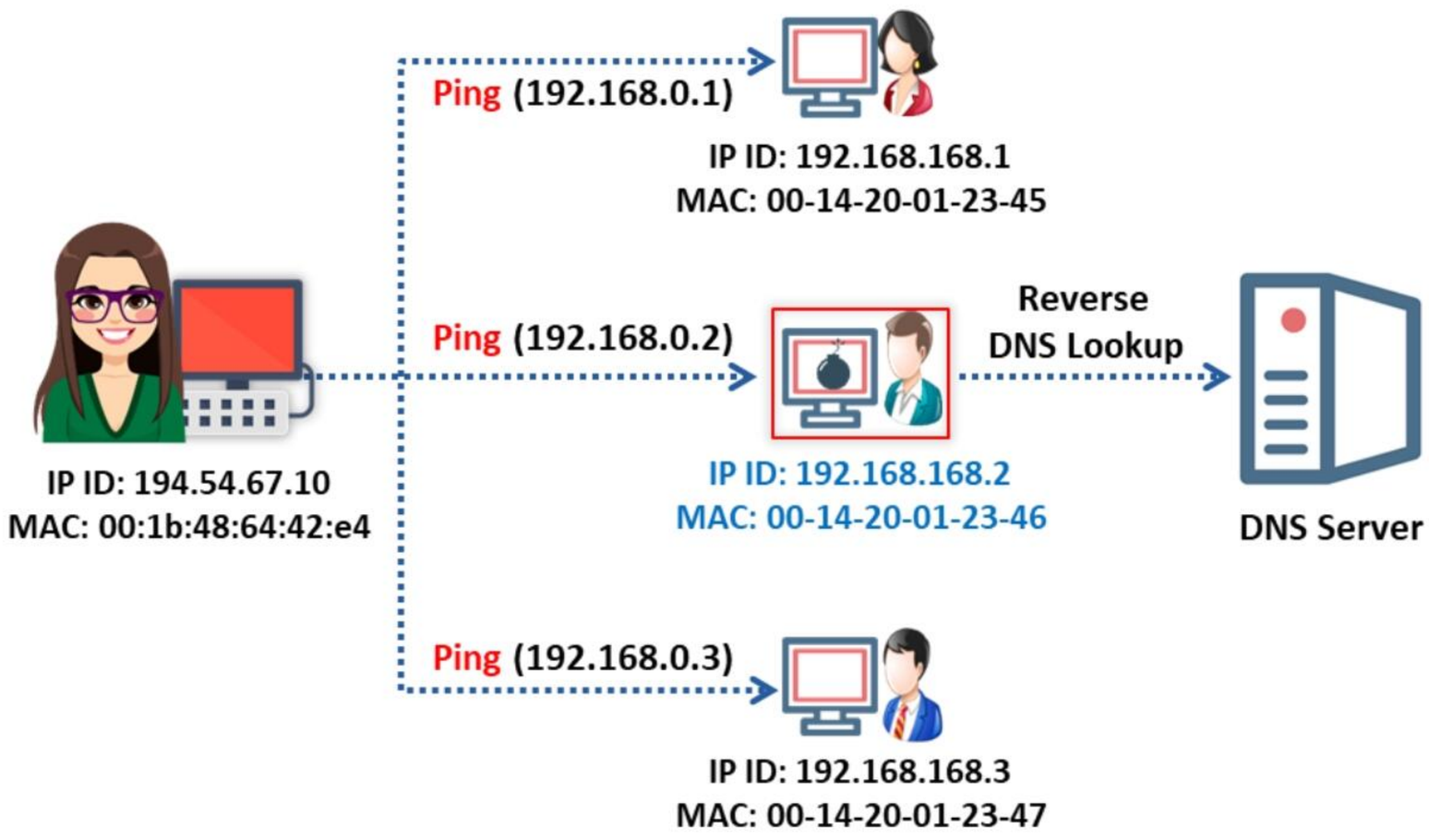


Figure 8.64: Sniffing detection using the DNS method

- **ARP Method**

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

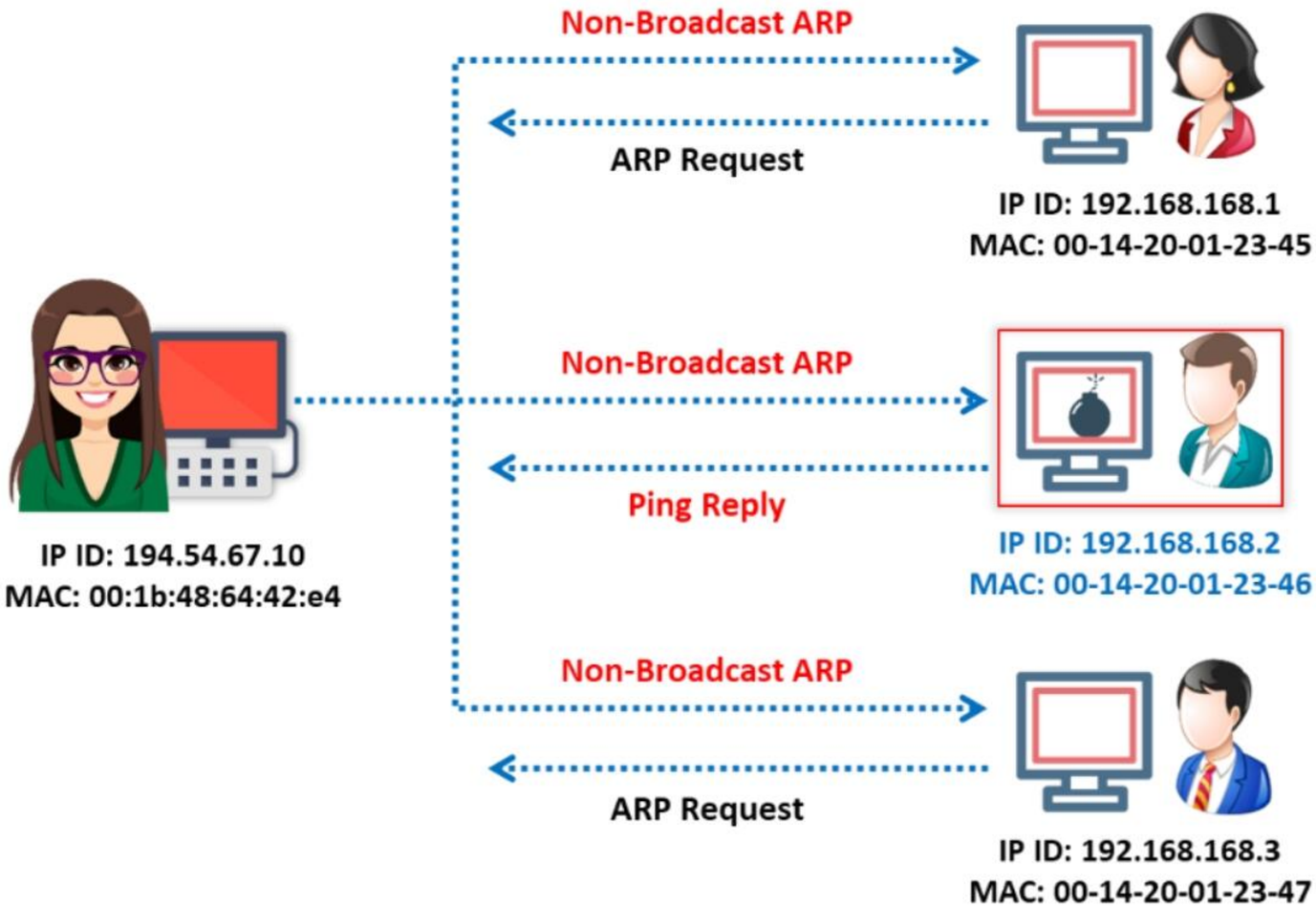
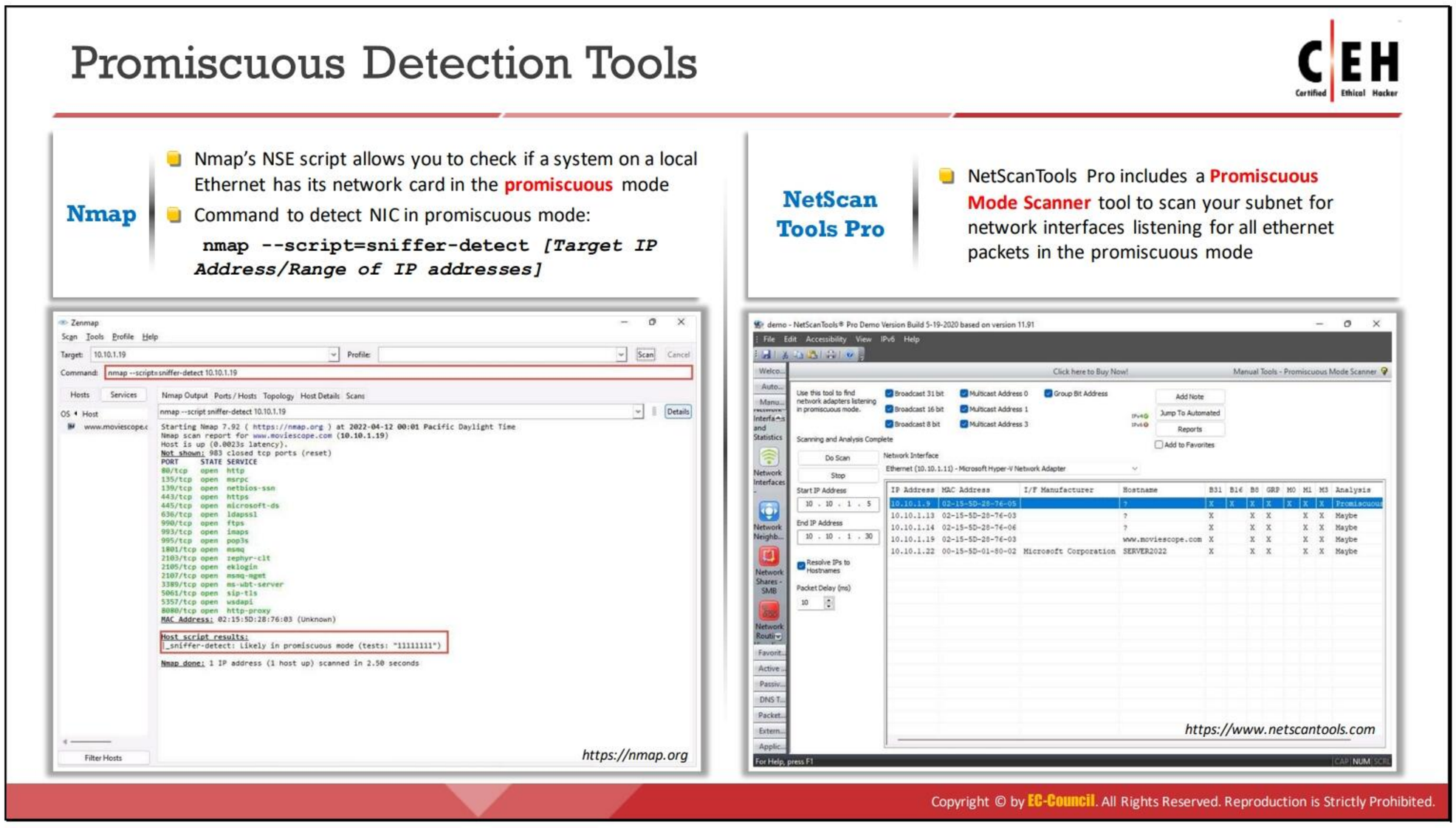


Figure 8.65: Detecting sniffing via the ARP method

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



Promiscuous Detection Tools

- **Nmap**

  Source: *https://nmap.org*

  Nmap's NSE script allows you to check whether a system 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]

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

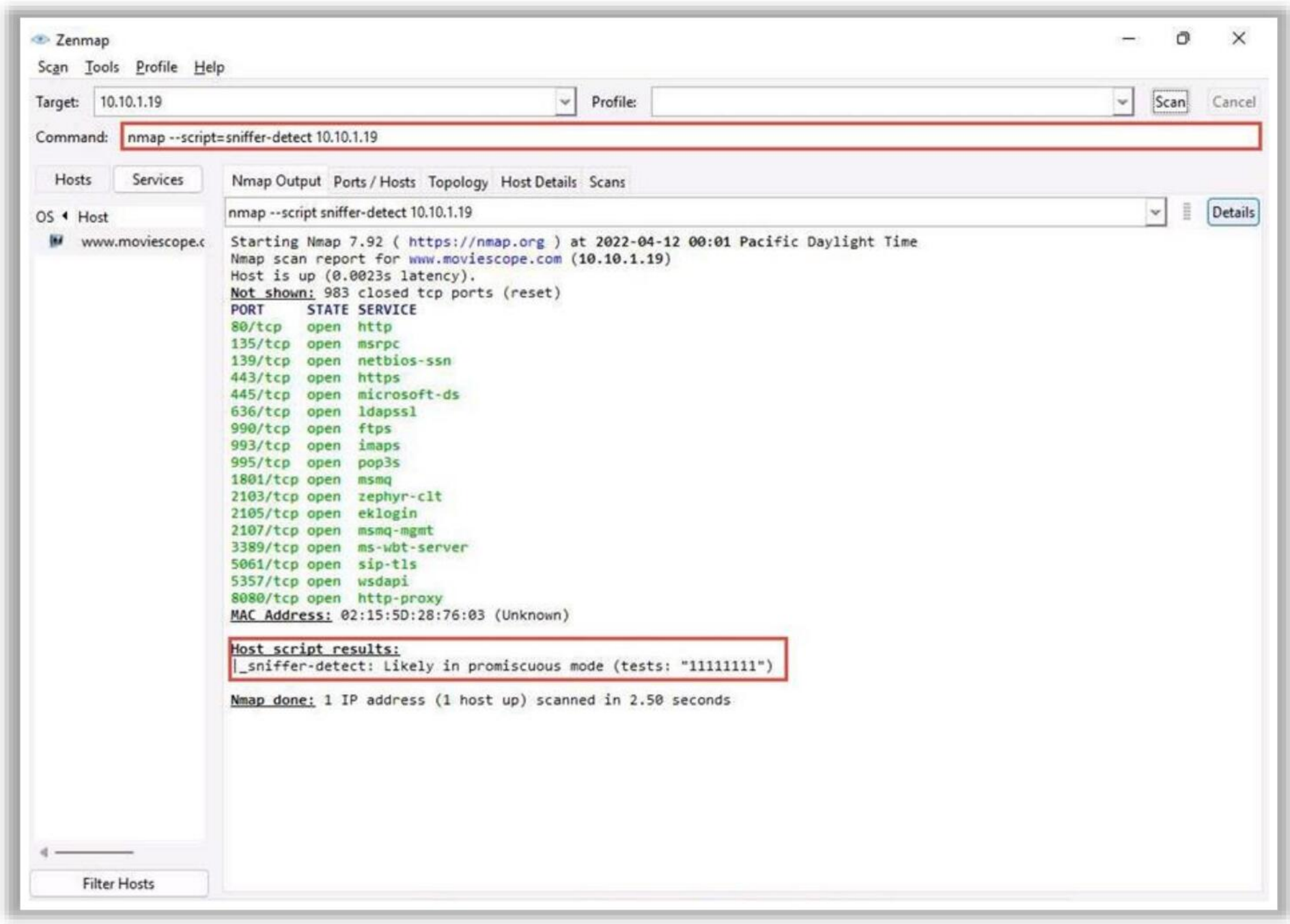


Figure 8.66: Screenshot showing Nmap output

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

- **NetScanTools Pro**

  Source: *https://www.netscantools.com*

  NetScanTools Pro includes the Promiscuous Mode Scanner tool to scan your subnet for network interfaces listening for all Ethernet packets in promiscuous mode. Security professionals use NetScanTools Pro to scan the subnet with modified ARP packets and identify devices responding to each type of ARP packet.

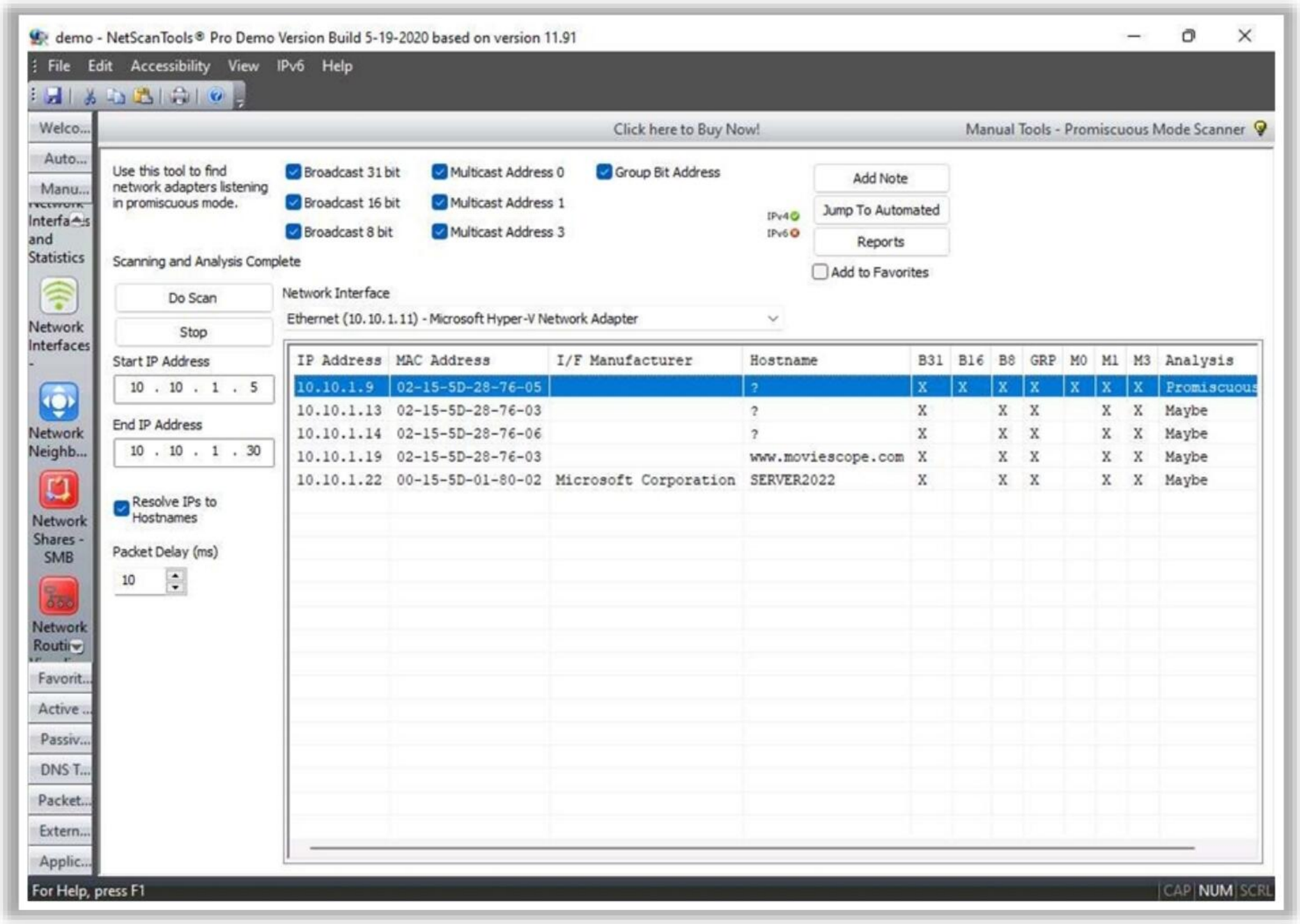


Figure 8.67: Screenshot of NetScanTools Pro – Promiscuous Mode Scanner

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

Module Summary

- In this module, we have discussed the following:
  - Sniffing concepts along with protocols vulnerable to sniffing and various hardware protocol analyzers
  - Various sniffing techniques such as MAC attacks, DHCP attacks, ARP poisoning, spoofing attacks, DNS poisoning, etc. along with their countermeasures
  - Various sniffing tools
  - Various countermeasures that are to be employed in order to prevent sniffing attacks
  - The module concluded with a detailed discussion on various sniffing detection techniques
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform social engineering to steal critical information related to the target organization

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

Module Summary

In this module, we have discussed sniffing concepts along with protocols vulnerable to sniffing and various hardware protocol analyzers. We have also discussed various sniffing techniques, such as MAC attacks, DHCP attacks, ARP poisoning, spoofing attacks, and DNS poisoning, along with their countermeasures. This module also illustrated various sniffing tools. In this module, we have also discussed various countermeasures to be employed to prevent sniffing attacks. This module ended with a detailed discussion on various sniffing detection techniques.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform social engineering to steal critical information related to the target organization.

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