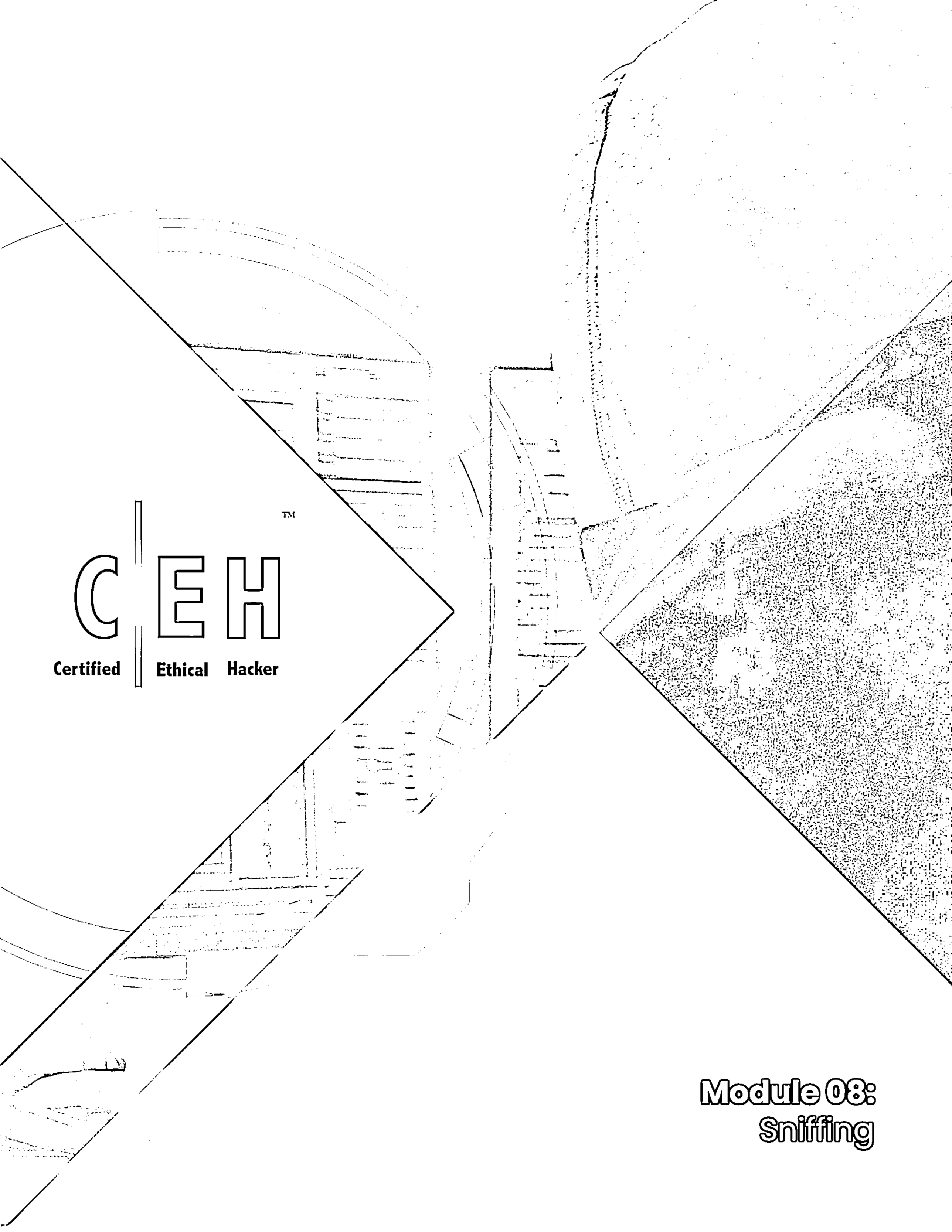


CEH™

Certified Ethical Hacker

Module 08: Sniffing

Module Objectives

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

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

Module Objectives

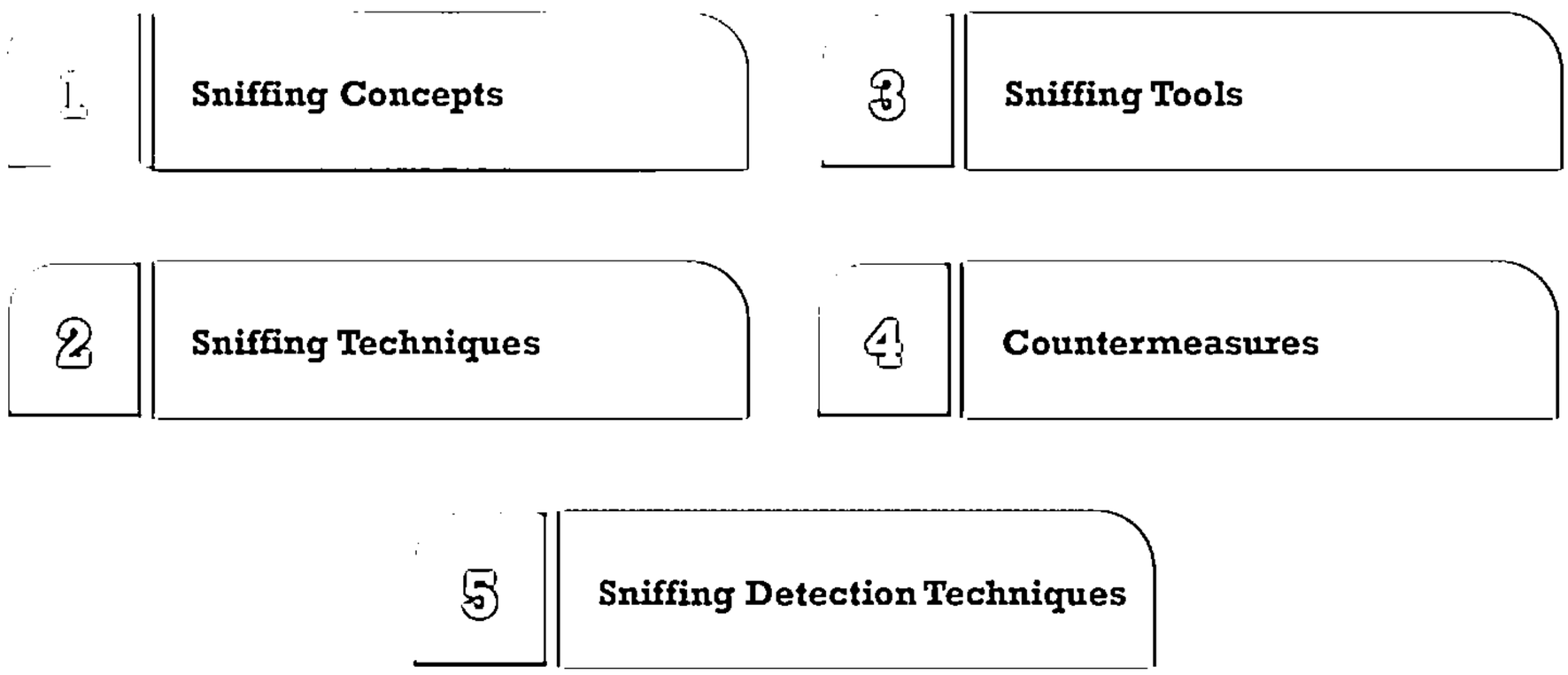
This module starts with an overview of sniffing concepts and provides an insight into MAC, DHCP, ARP, MAC spoofing, and DNS poisoning attacks. Later, the module discusses various sniffing tools, countermeasures, and detection techniques.

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.

Module Flow



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.

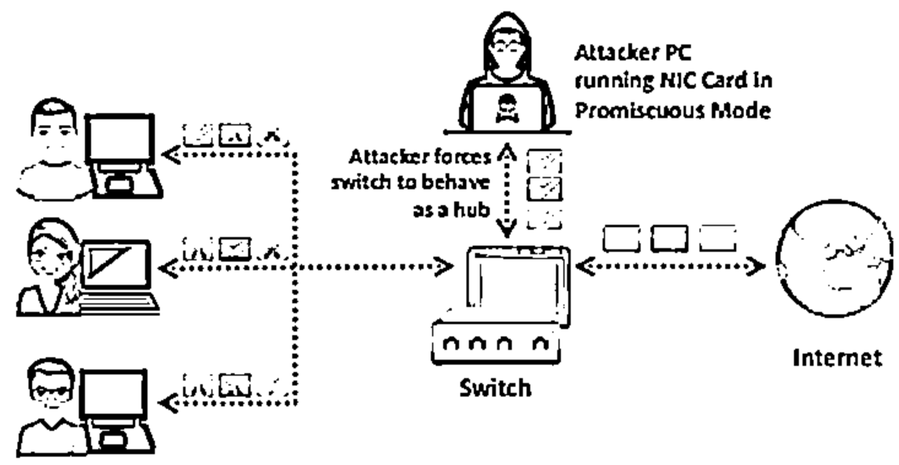
Network Sniffing

Packet Sniffing

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

How a Sniffer Works

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



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:

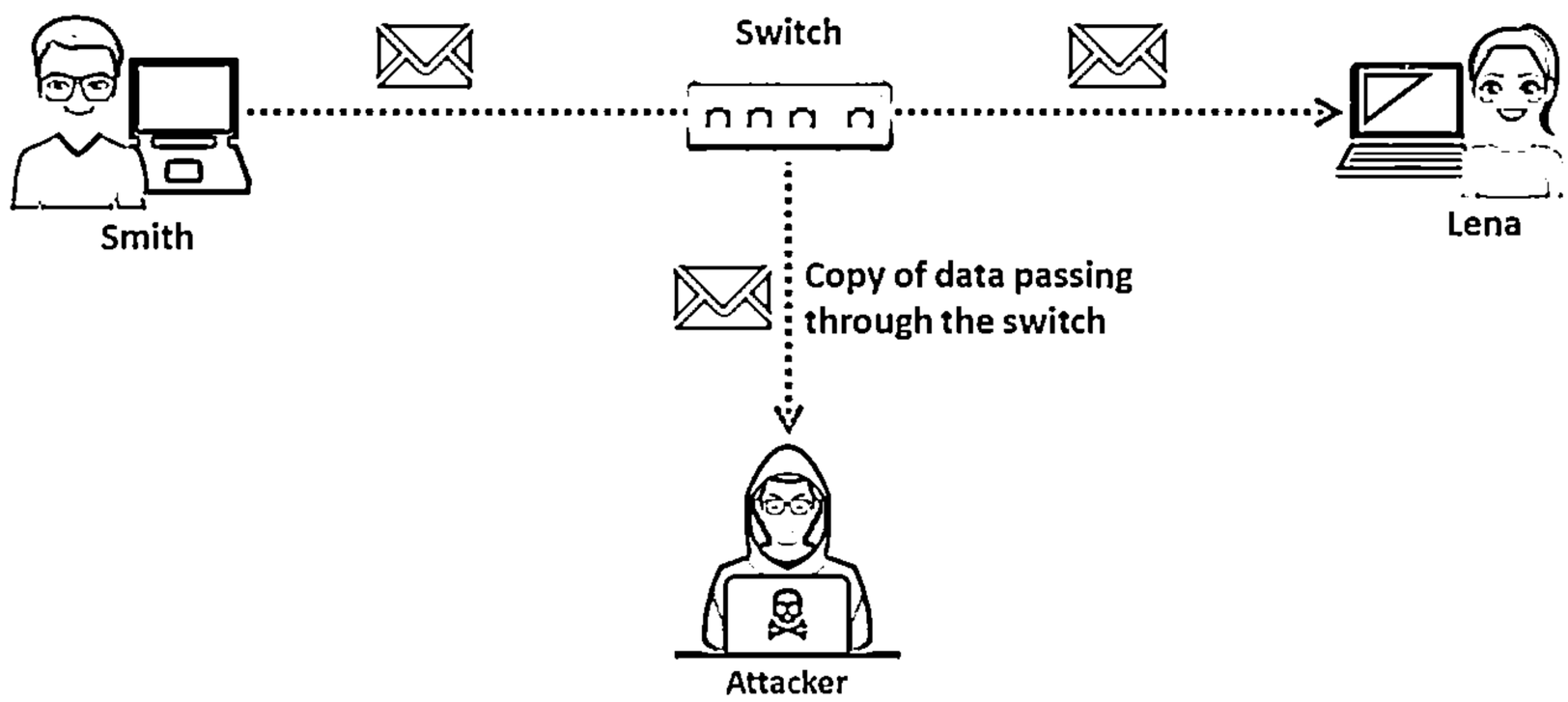


Figure 8.1: Packet sniffing scenario

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

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

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 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

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

the card starts accepting all the packets. Thus, the attacker can view all the packets that are being transmitted in the network.

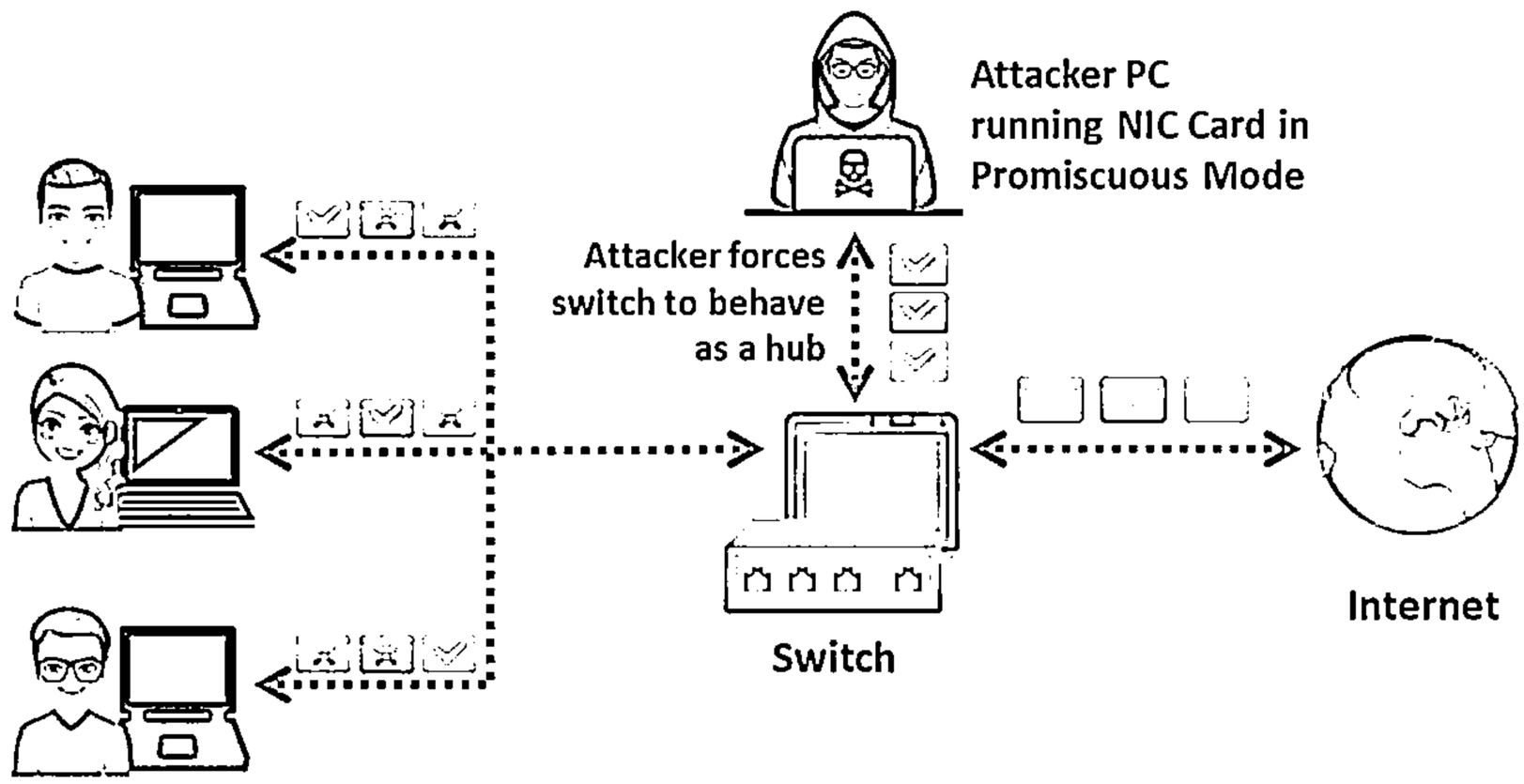


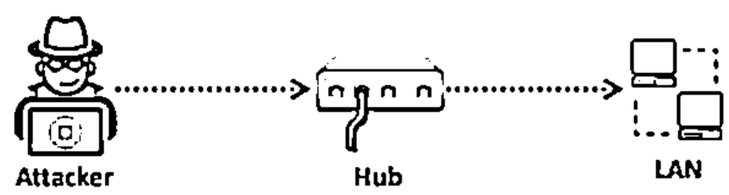
Figure 8.2: Working of a sniffer

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

Types of Sniffing

Passive Sniffing

- Passive sniffing refers to sniffing through a hub, wherein the traffic is sent to all ports
- It involves monitoring packets sent by others without sending any additional data packets in the network traffic
- In a network that uses hubs to connect systems, all hosts on the network can see the all traffic, and therefore, the attacker can easily capture traffic going through the hub
- Hub usage is an outdated approach. Most modern networks now use switches



Note: Passive sniffing provides significant stealth advantages over active sniffing

Active Sniffing

- Active sniffing is used to sniff a switch-based network
- Active sniffing involves injecting Address Resolution Packets (ARP) into the network to flood the switch's Content Addressable Memory (CAM) table, which keeps track of host-port connections

Active Sniffing Techniques

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

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.

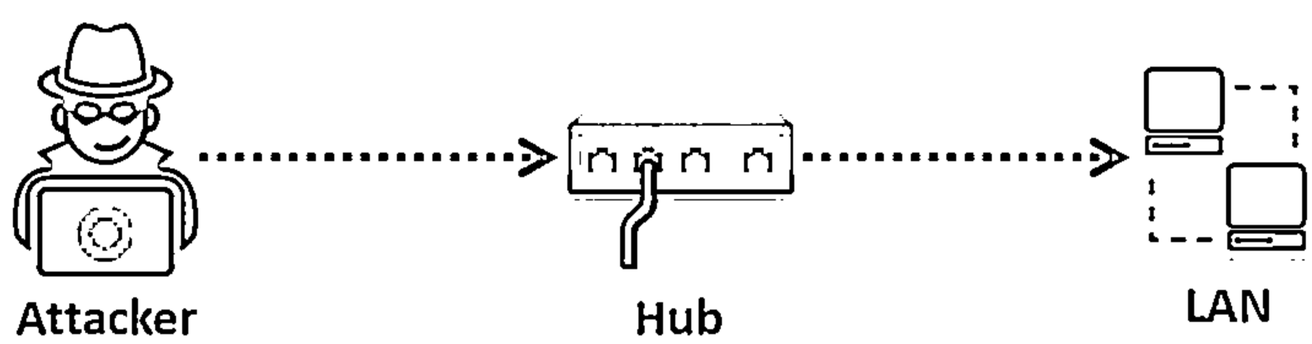


Figure 8.3: Passive sniffing

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.

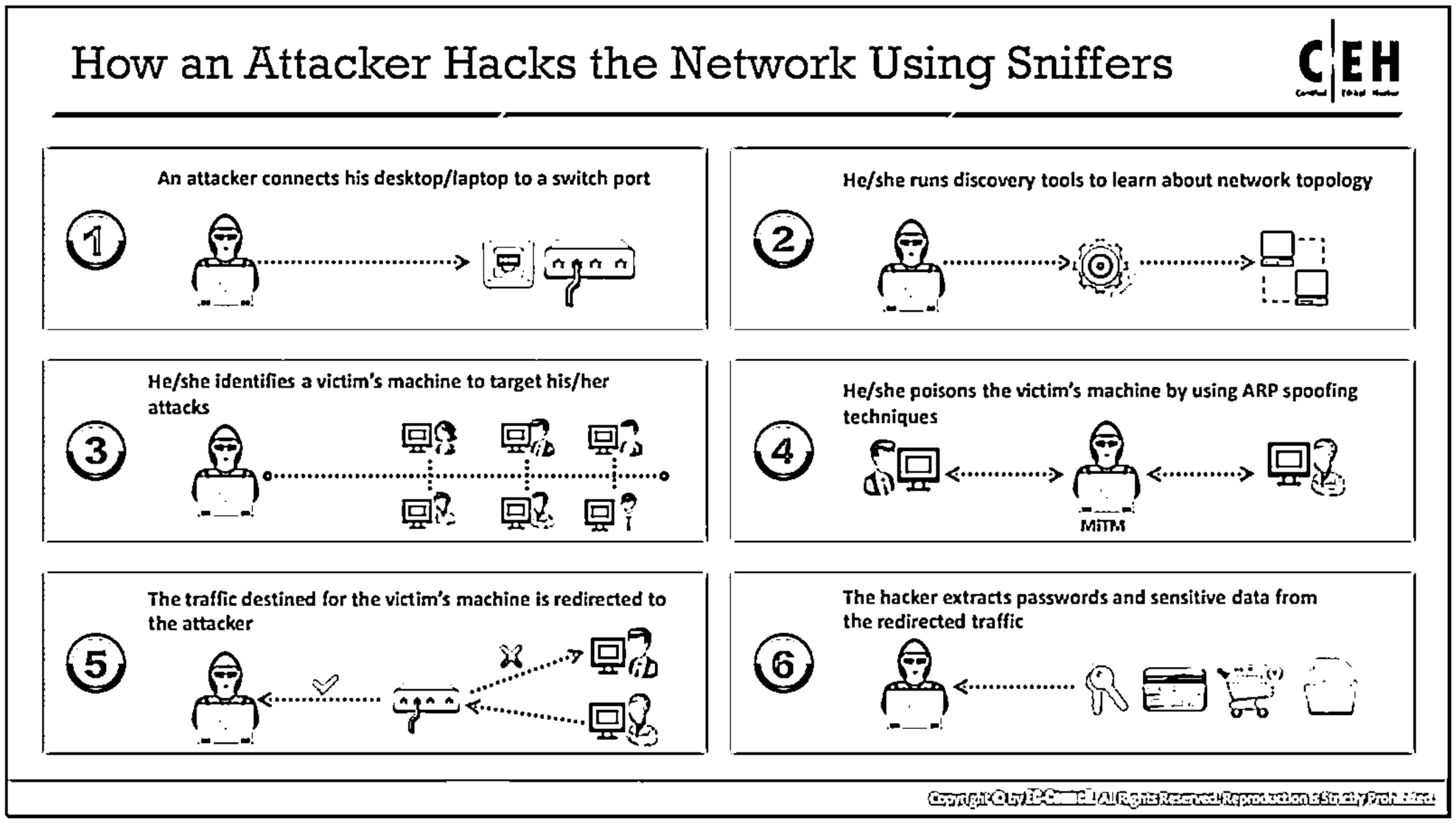
Switches examine data packets for source and destination addresses and then transmit them to the appropriate destinations. Therefore, it is cumbersome to sniff switches. However, attackers can actively inject ARP traffic into a LAN to sniff around a switched network and capture the traffic. Switches 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.

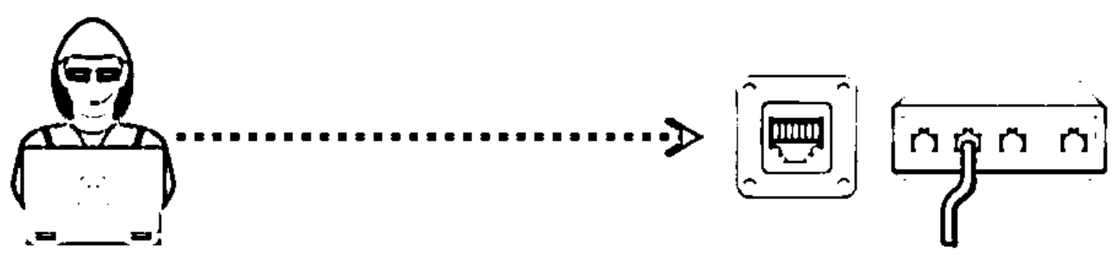


Figure 8.4: Discovering a switch to access the network

- **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.

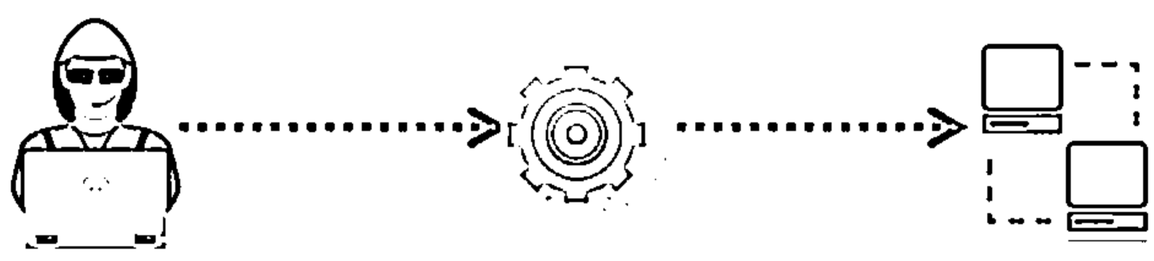


Figure 8.5: Using network discovery tools to learn topology

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.

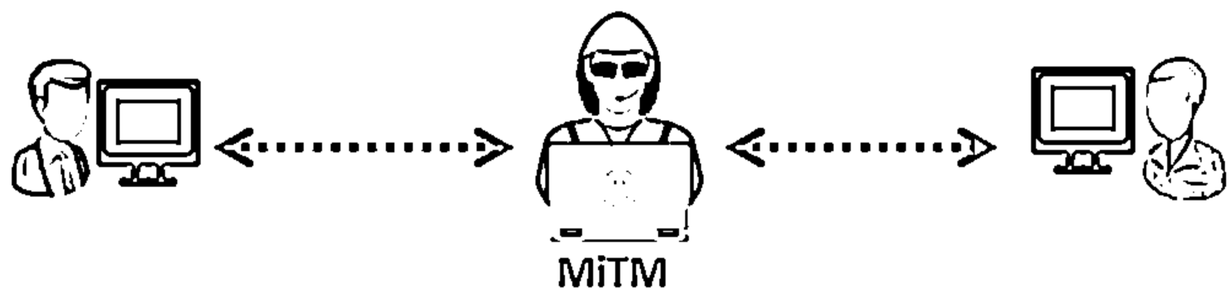


Figure 8.7: Attacker sending fake ARP messages

- **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.

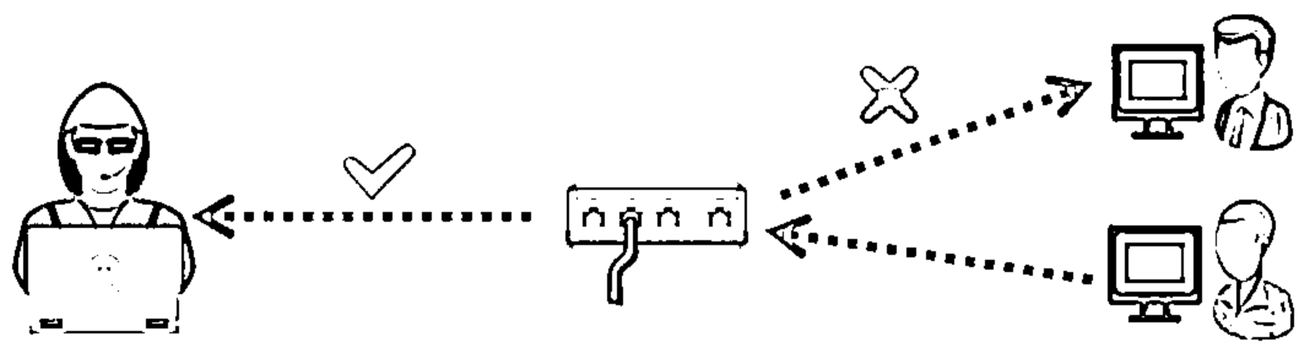


Figure 8.8: Redirecting the traffic to the attacker

- **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.

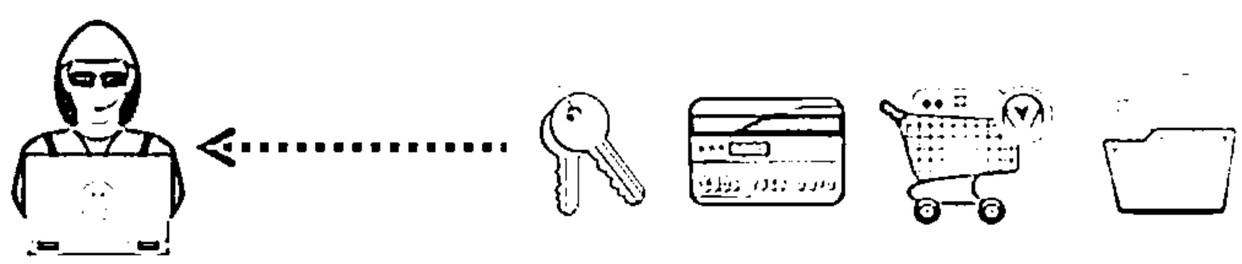


Figure 8.9: Attacker extracting sensitive information

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

Protocols Vulnerable to Sniffing

Telnet and Rlogin	Keystrokes including usernames and passwords are sent in clear text	IMAP	Passwords and data are sent in clear text
HTTP	Data is sent in clear text	SMTP and NNTP	Passwords and data are sent in clear text
POP	Passwords and data are sent in clear text	FTP	Passwords and data are sent in clear text

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

Protocols Vulnerable to Sniffing

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

- **Telnet and Rlogin**

  Telnet is a protocol used for communicating with a remote host (via port 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) 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.

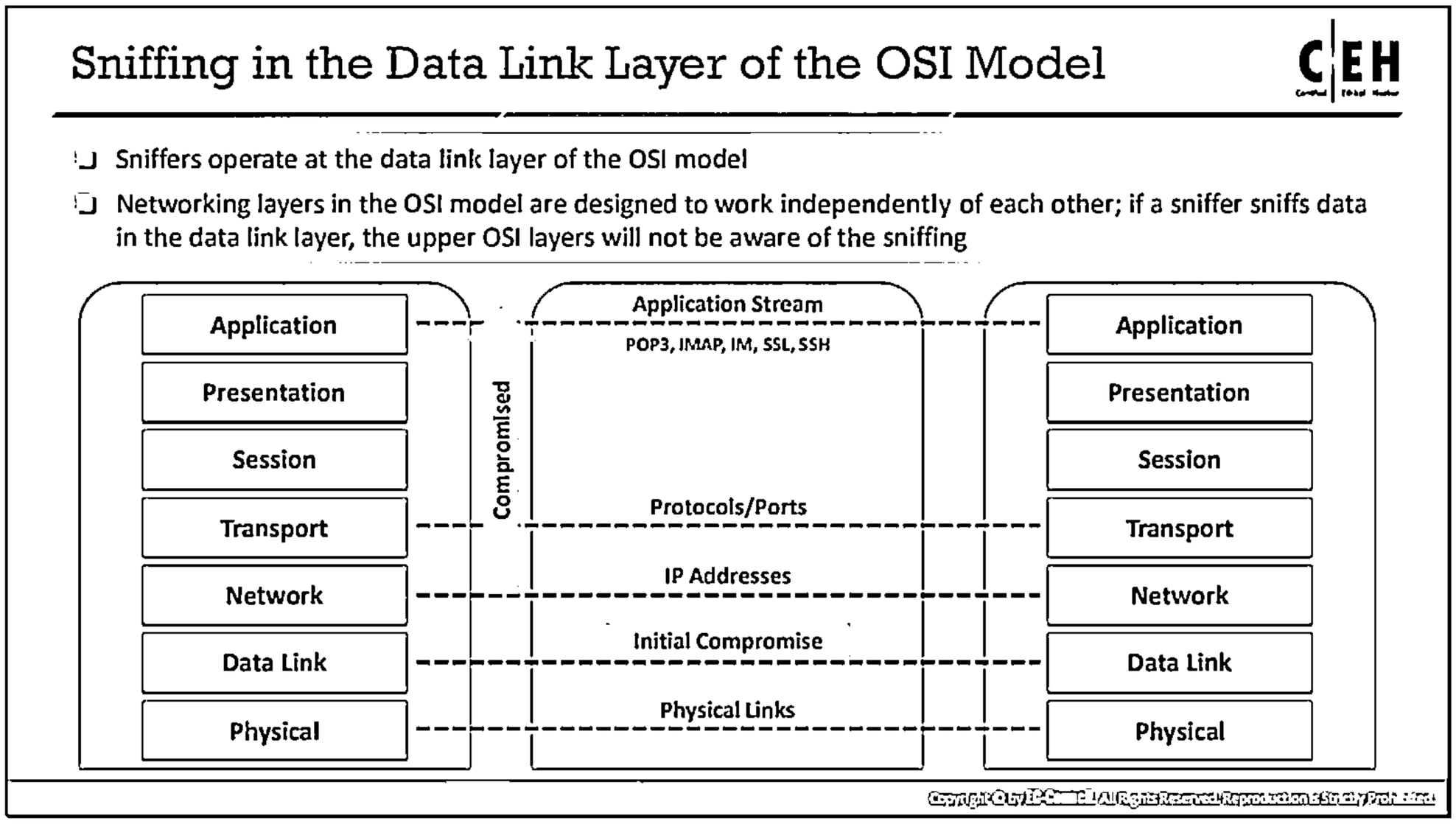
- **FTP**

  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.

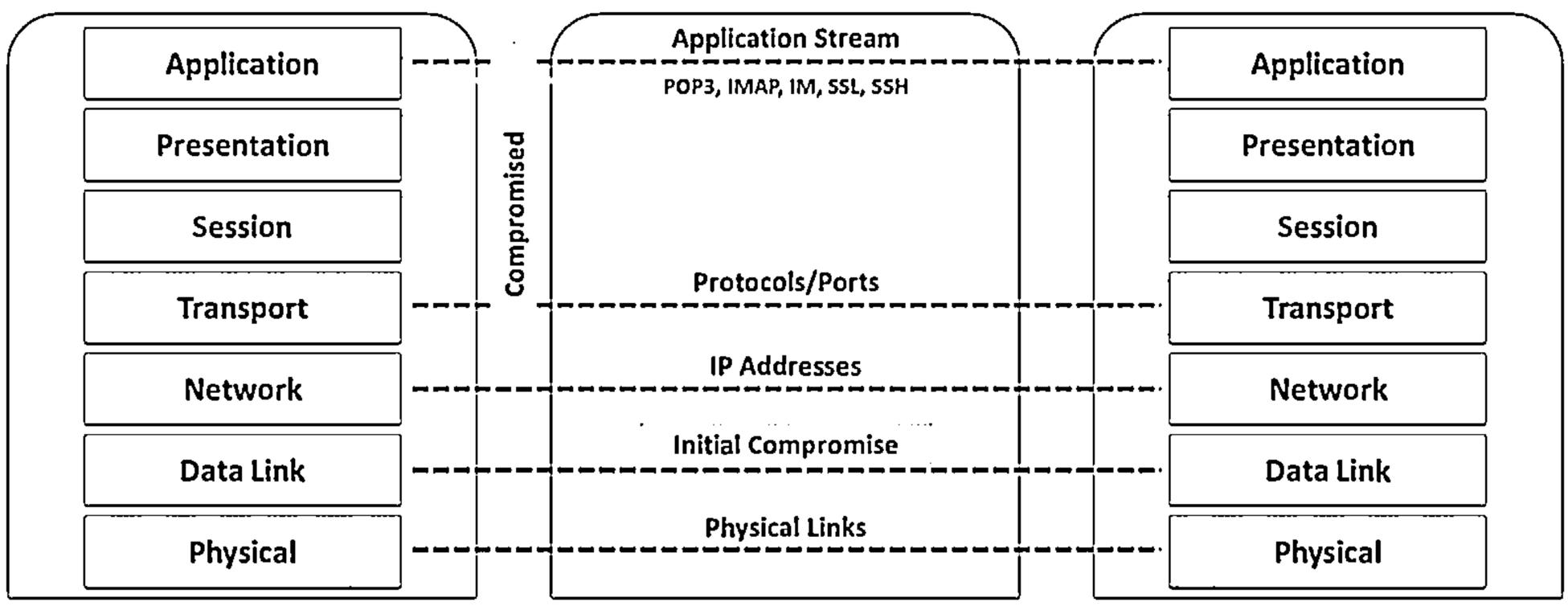


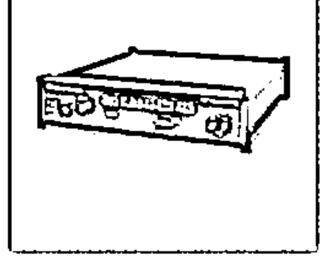
Figure 8.10: Sniffing in the data link layer of the OSI model

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

Hardware Protocol Analyzers

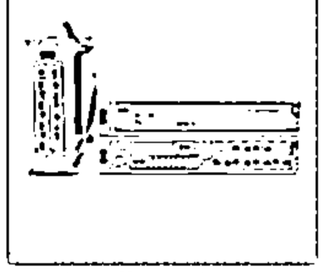
1. A hardware protocol analyzer is a piece of equipment that captures signals without altering the traffic in a cable segment
2. It can be used to monitor network usage and identify malicious network traffic generated by hacking software installed in the network
3. It captures a data packet, decodes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

Voyager M4x Protocol Analyzer



https://teledynelecroy.com

N2X N5540A Agilent Protocol Analyzer



https://www.volutronics.com

Hardware Protocol Analyzers

- Keysight E2960B (*https://www.keysight.com*)
- STINGA Protocol Analyzer (*https://utelsystems.com*)
- NETSCOUT's OneTouch AT Network Assistant (*https://enterprise.netscout.com*)
- NETSCOUT's OptiView XG Network Analysis Tablet (*https://enterprise.netscout.com*)
- Agilent (Keysight) Technologies 87S3ES (*https://www.microleose.com*)

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

Hardware Protocol Analyzers

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

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:

- **Voyager M4x Protocol Analyzer**

  Source: *https://teledynelecroy.com*

  The Voyager M4x analyzer platform provides accurate and reliable capture of USB4 and Thunderbolt 3 protocols for fast debugging, analysis, and problem-solving. Voyager M4x features the highest-fidelity probe design and provides unmatched reliability when testing devices at the full USB4 Gen3x2 (40 Gb/s aggregate) speed.

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

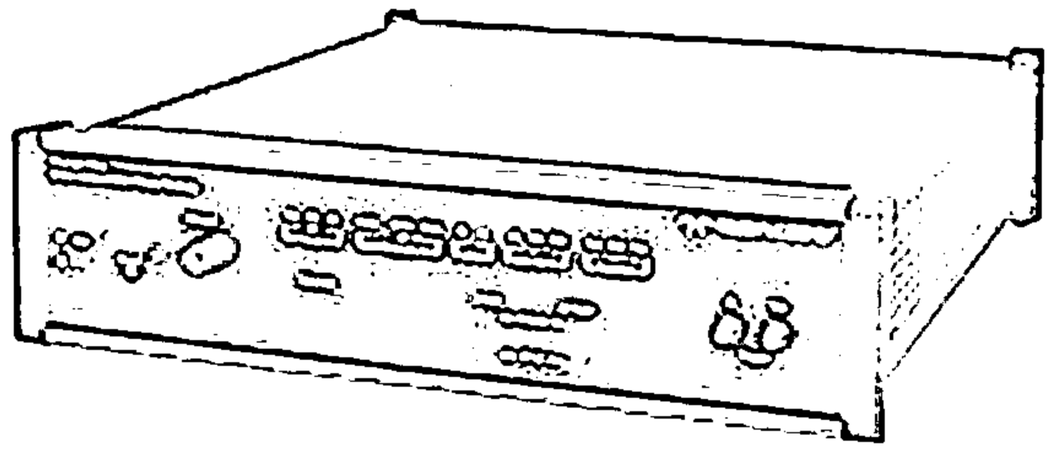


Figure 8.11: Voyager M4x Protocol Analyzer

- **N2X N5540A Agilent Protocol Analyzer**

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

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

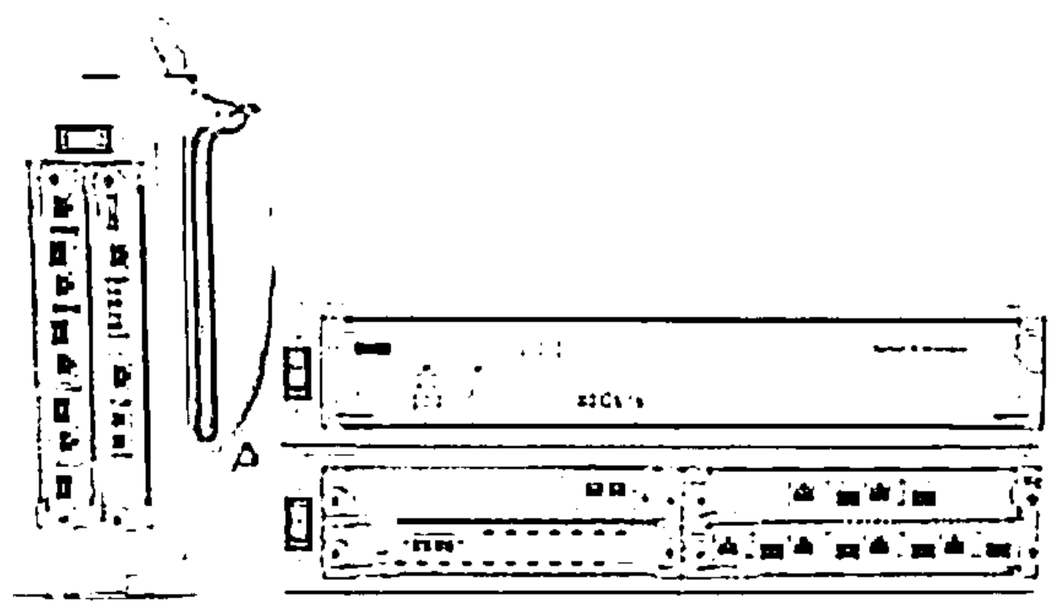
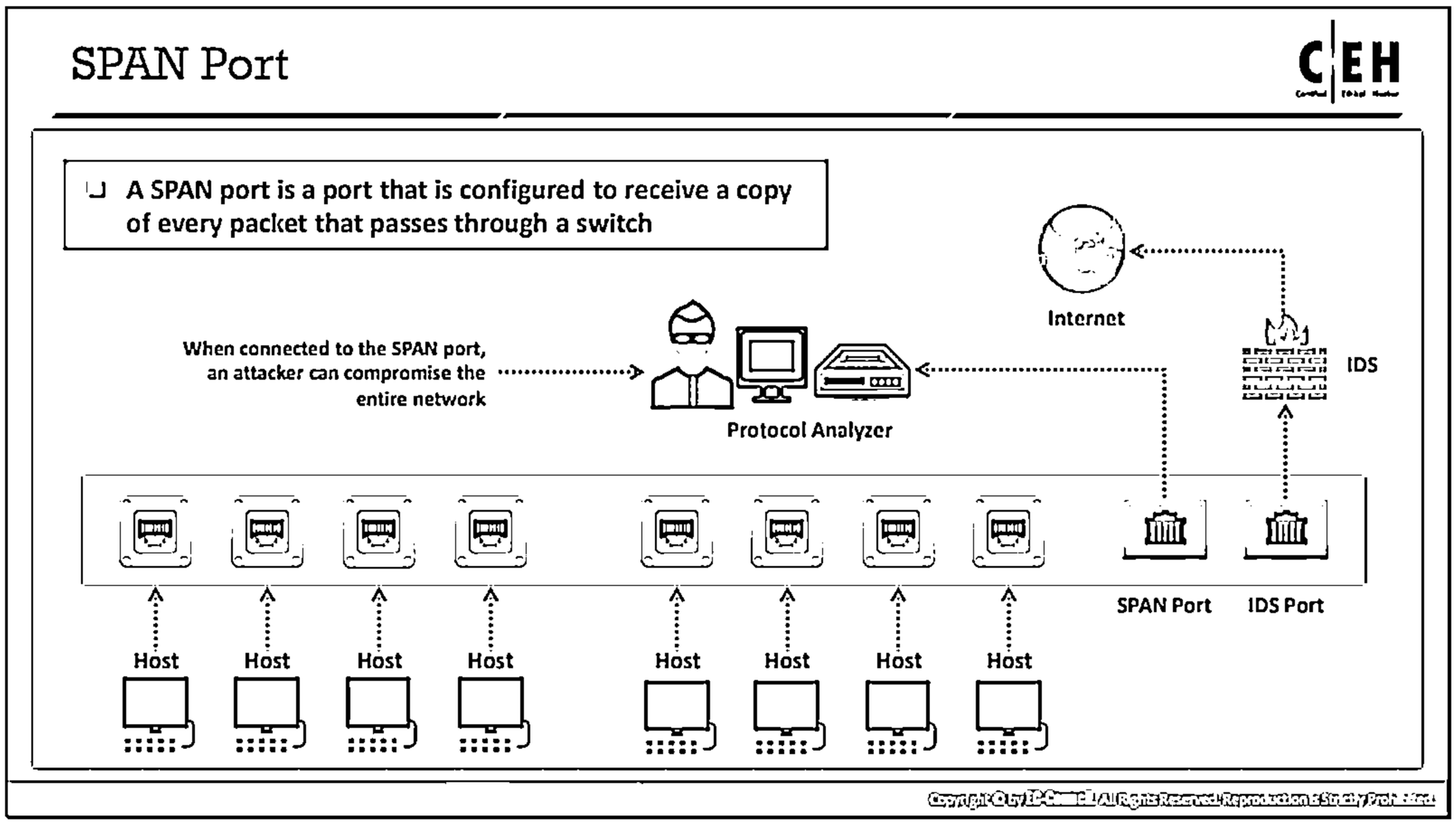


Figure 8.12: N2X N5540A Agilent Protocol Analyzer

Some examples of hardware protocol analyzers are listed below:

- Keysight E2960B (*https://www.keysight.com*)
- STINGA Protocol Analyzer (*https://utelsystems.com*)
- NETSCOUT OneTouch AT Network Assistant (*https://enterprise.netscout.com*)
- NETSCOUT OptiView XG Network Analysis Tablet (*https://enterprise.netscout.com*)
- Agilent (Keysight) Technologies 8753ES (*https://www.microlease.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).

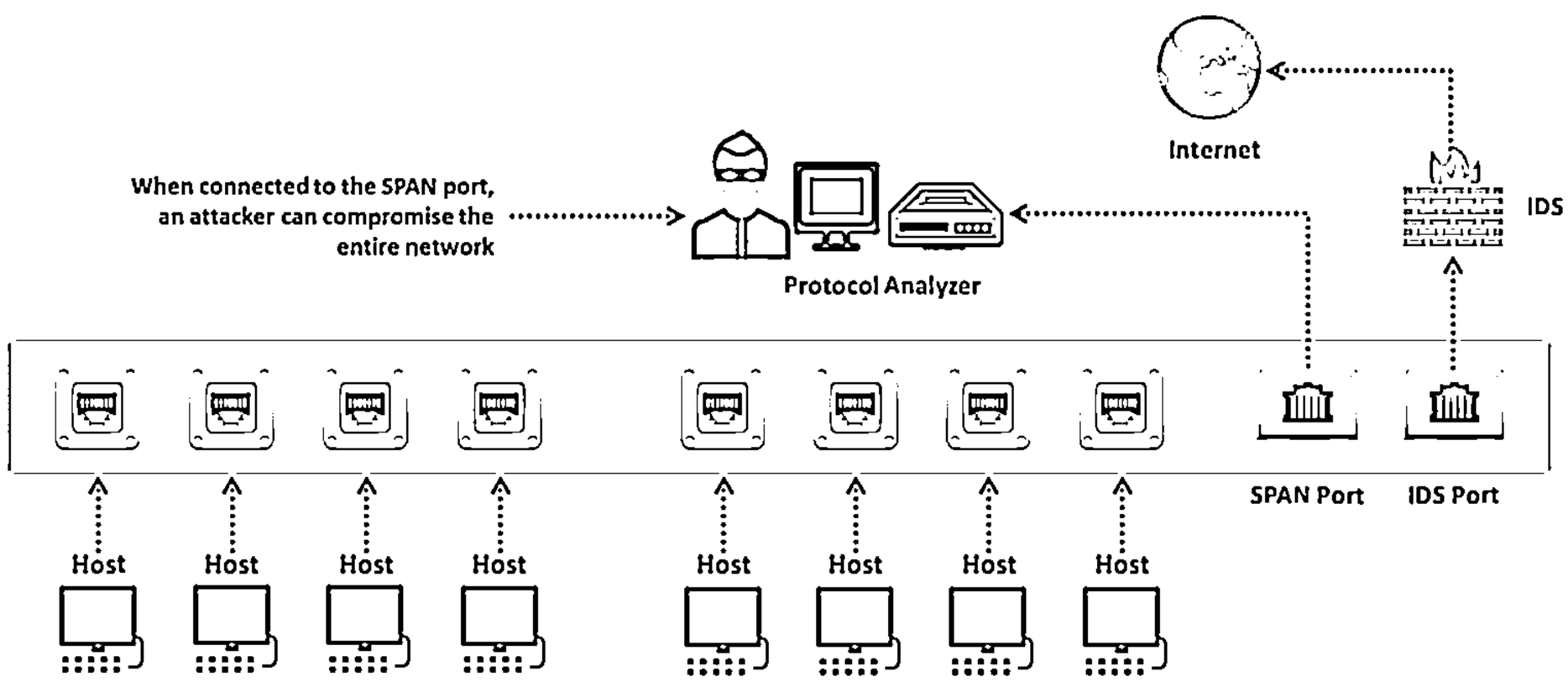


Figure 8.13: Working of SPAN

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

Wiretapping

1. Wiretapping is the process of the monitoring of telephone and Internet conversations by a third party
2. Attackers connect a listening device (hardware, software, or a combination of both) to the circuit carrying information between two phones or hosts on the Internet
3. It allows an attacker to monitor, intercept, access, and record information contained in a data flow in a communication system

Types of Wiretapping

Active Wiretapping

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

Passive Wiretapping

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

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

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

Wiretapping

Wiretapping, or telephone tapping, 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**

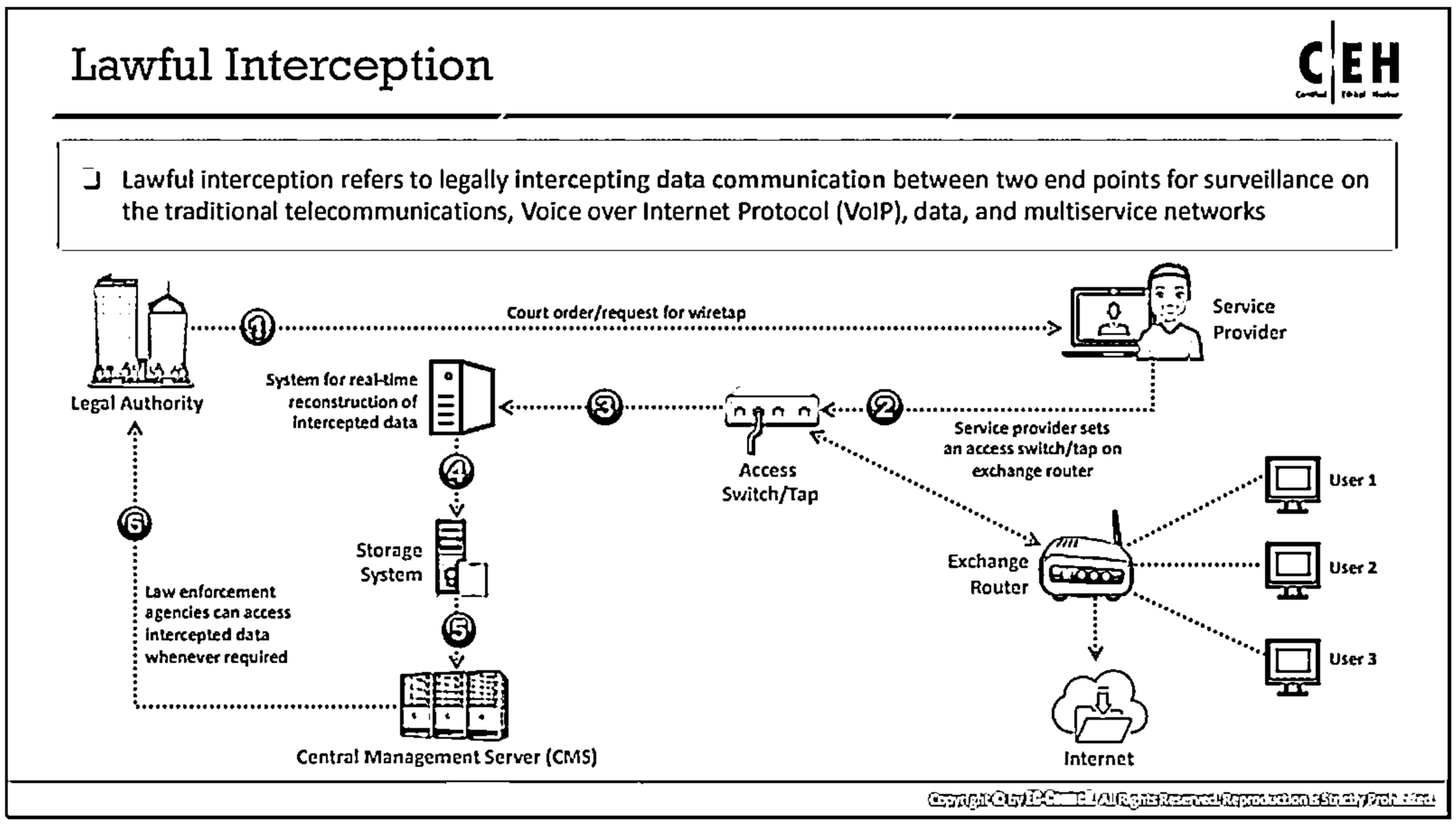
  In hacking terminology, active wiretapping is an MITM attack. This allows an attacker to monitor and record the traffic or data flow in a communication system. The attacker can also alter or inject data into communication or traffic.

- **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.

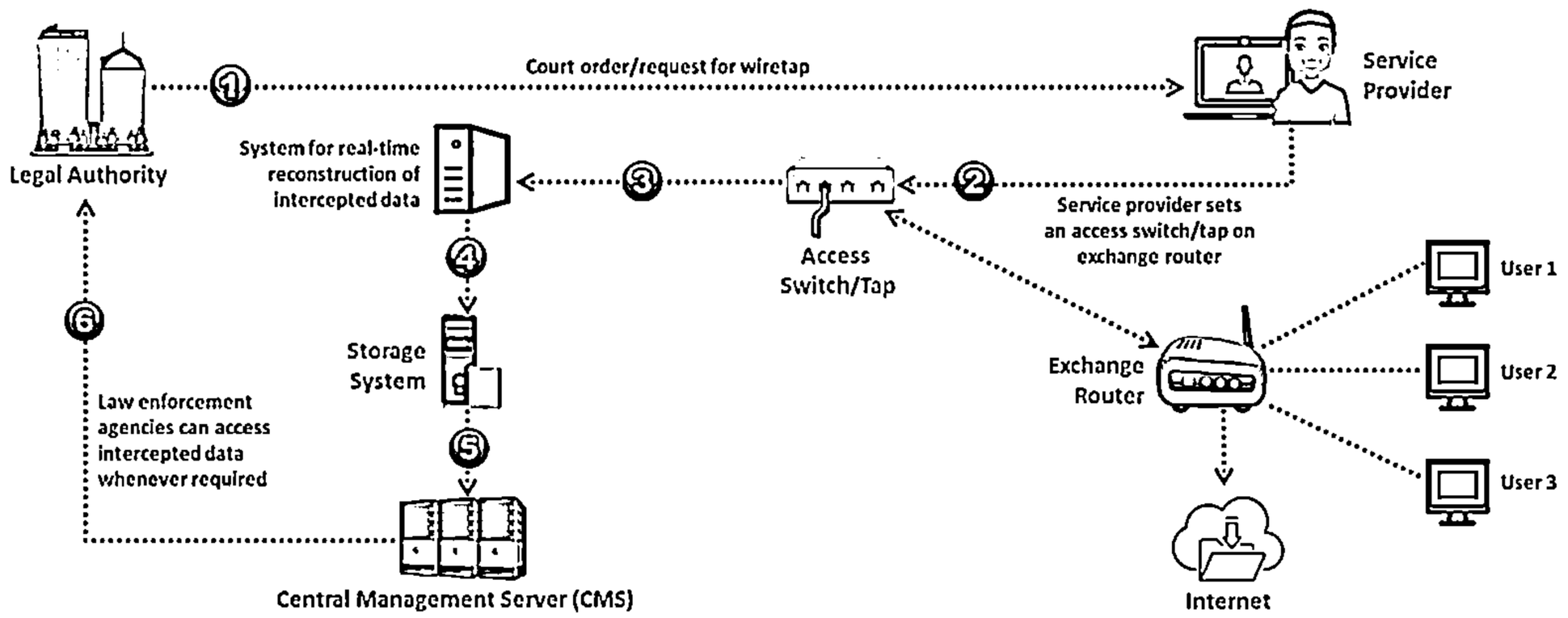
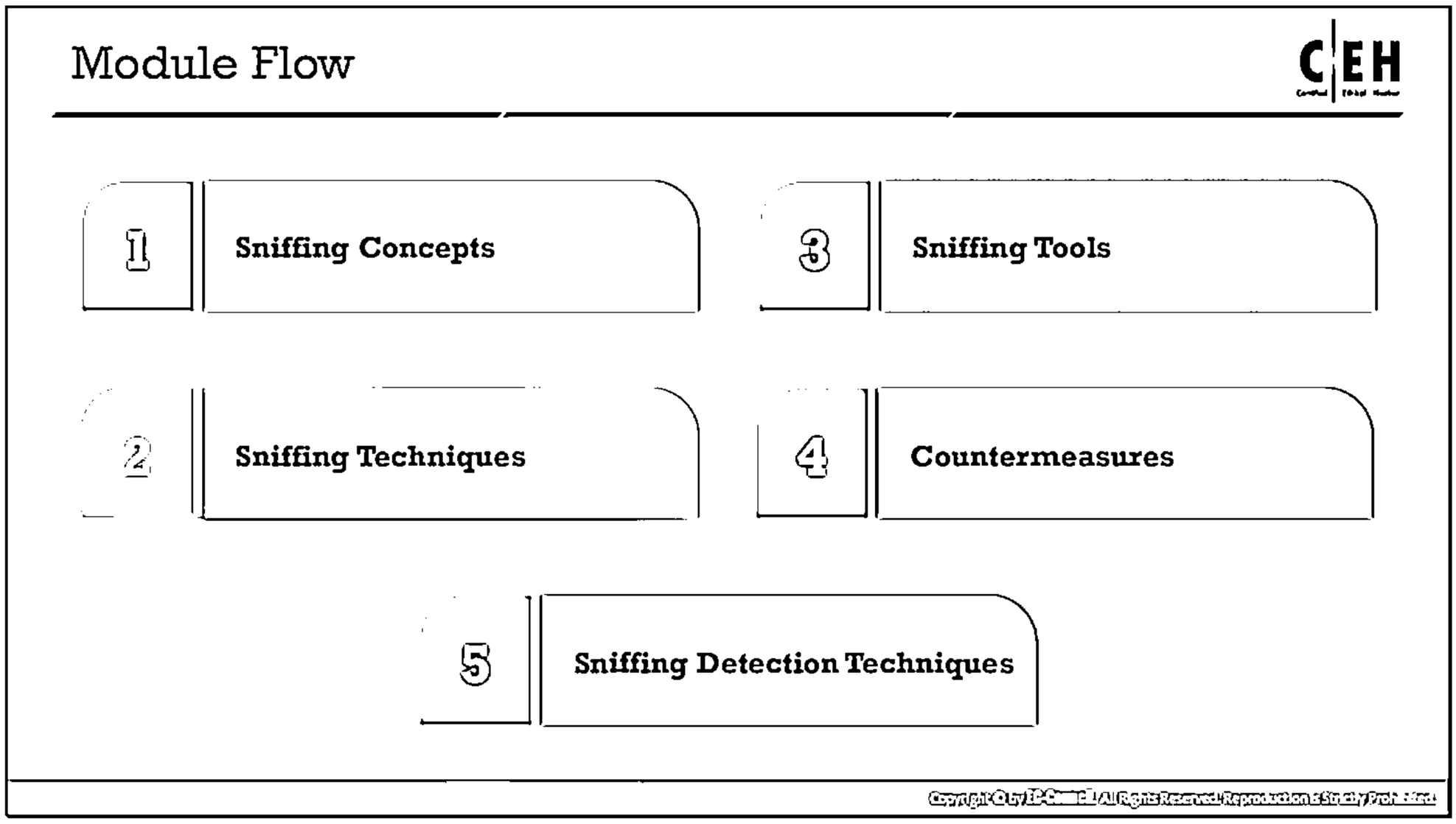


Figure 8.14: Telco/ISP lawful solution

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

Module Flow



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.

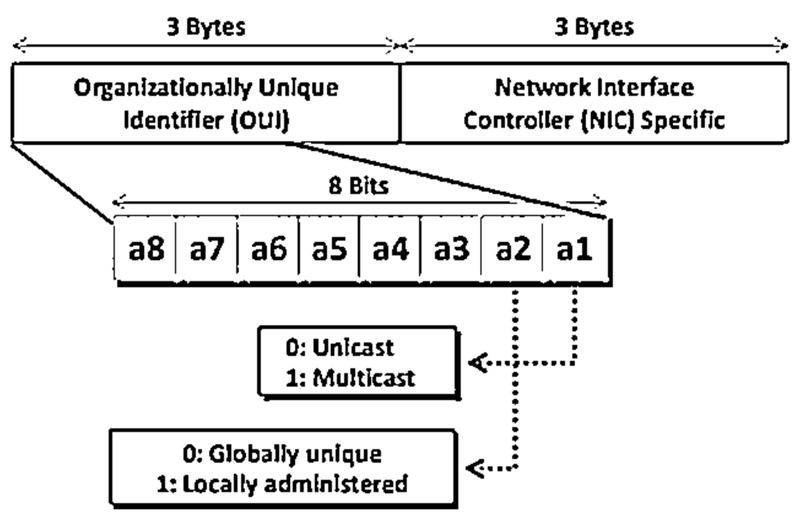
This section discusses MAC attacks or MAC flooding. Attackers use the MAC flooding technique to force a switch to act as a hub, so that they can easily sniff the traffic.

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

MAC Address/CAM Table

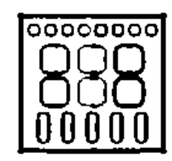
- Each switch has a fixed-size dynamic Content Addressable Memory (CAM) table
- The CAM table stores information such as MAC addresses available on physical ports with their associated virtual LAN (VLAN) parameters

MAC Address



CAM Table

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



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

MAC Address

A MAC address uniquely identifies each node of a network. Each device in the network has a MAC address associated with a physical port on the network switch, which makes it possible to designate a specific single point of the network. 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.

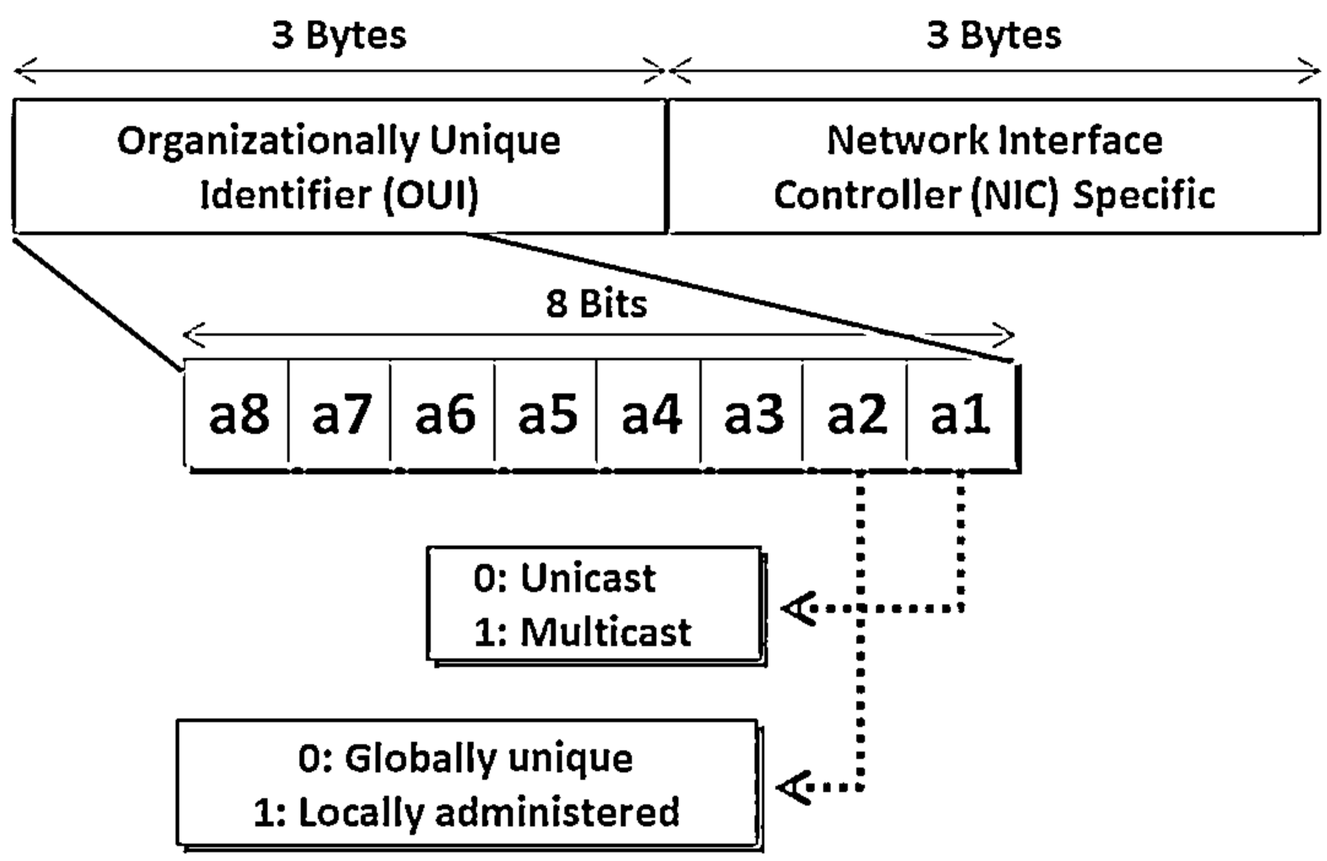


Figure 8.15: MAC address

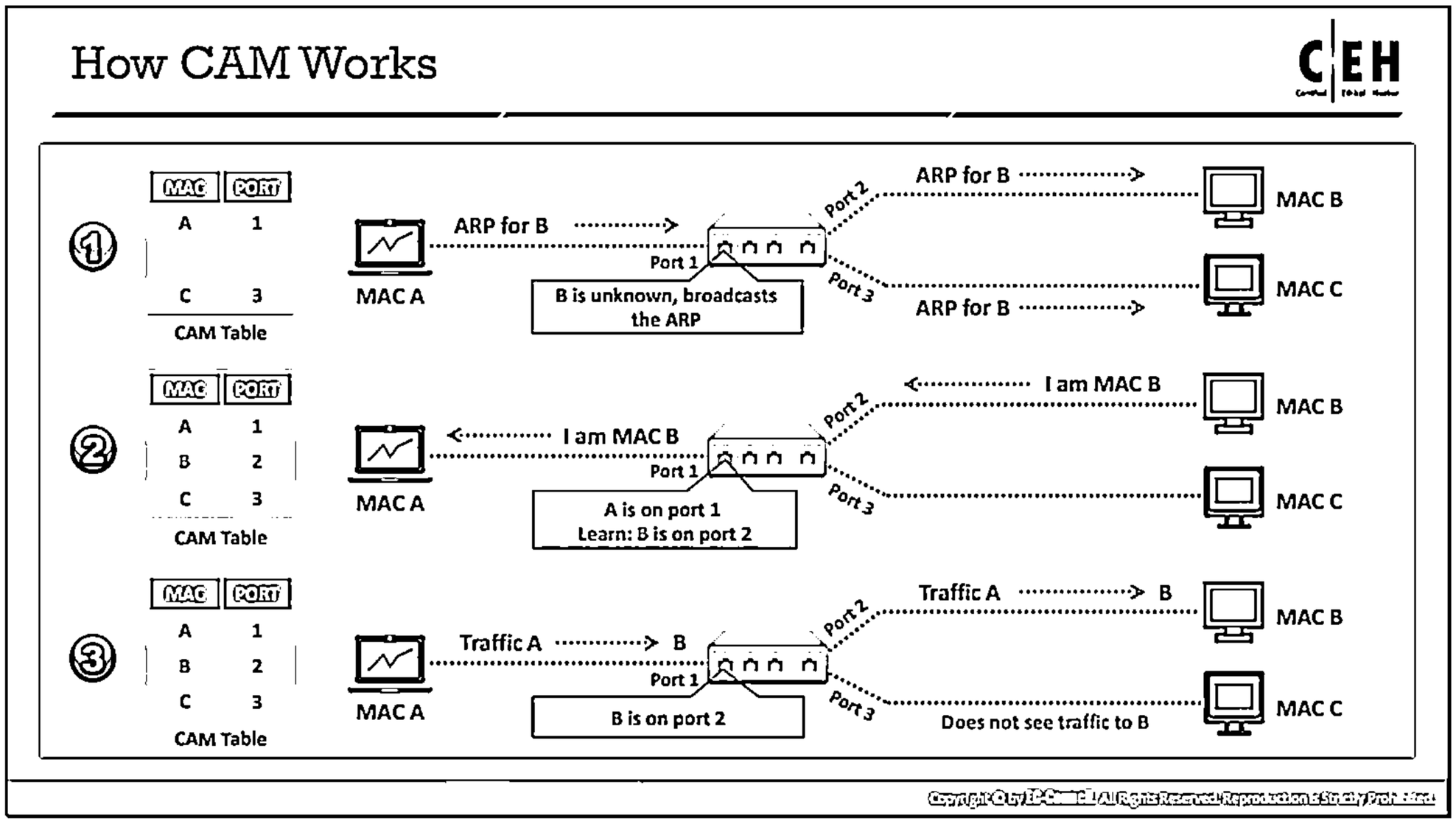
CAM Table

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	00d3.ad34.123g	Dynamic	Yes	0	Gi5/2
5	as23.df45.45t6	Dynamic	Yes	0	Gi2/5
5	er23.23er.t5e3	Dynamic	Yes	0	Gi1/6

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.

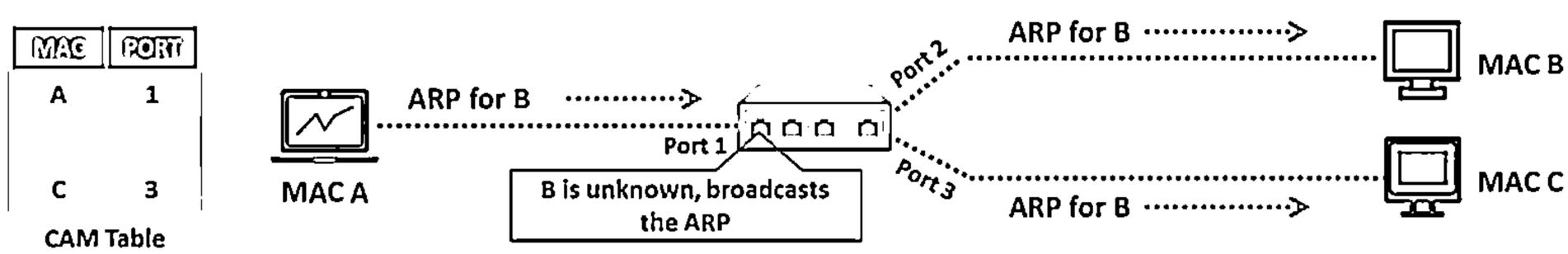


Figure 8.16: Working of CAM table step-1

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.

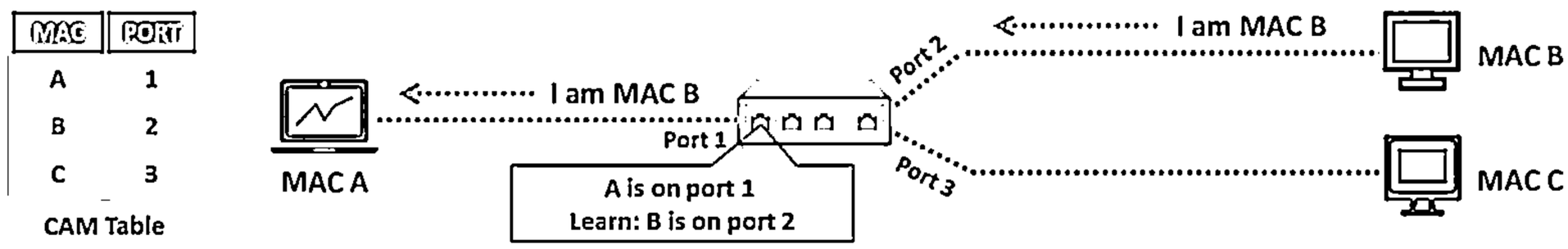


Figure 8.17: Working of CAM table step-2

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.

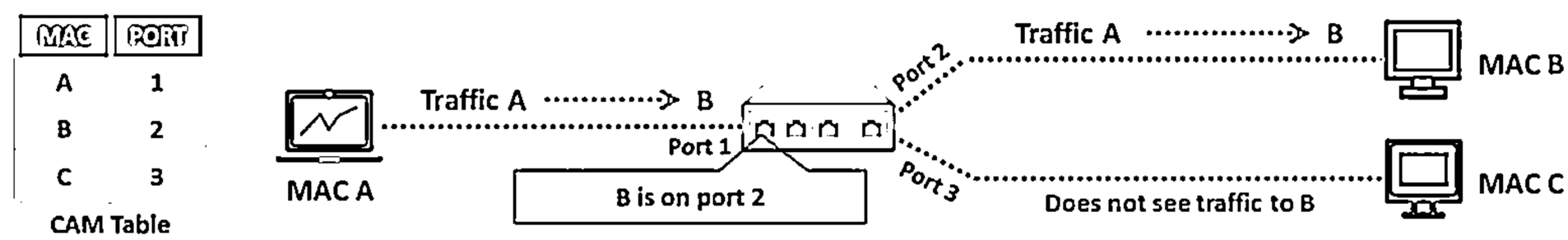
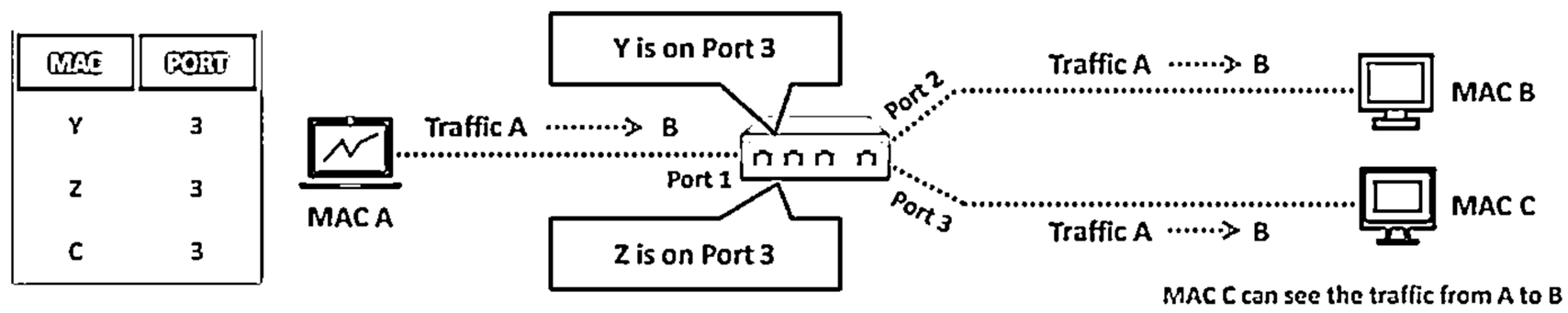


Figure 8.18: Working of CAM table step-3

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.

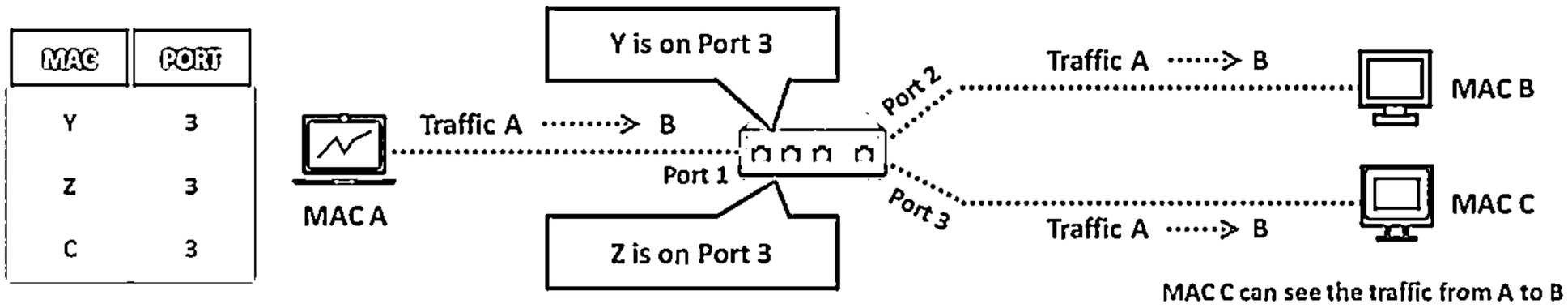
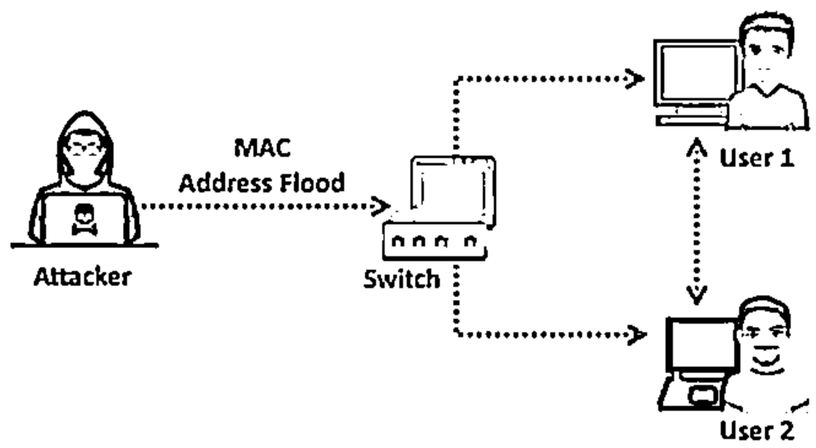


Figure 8.19: Flooding a CAM table

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

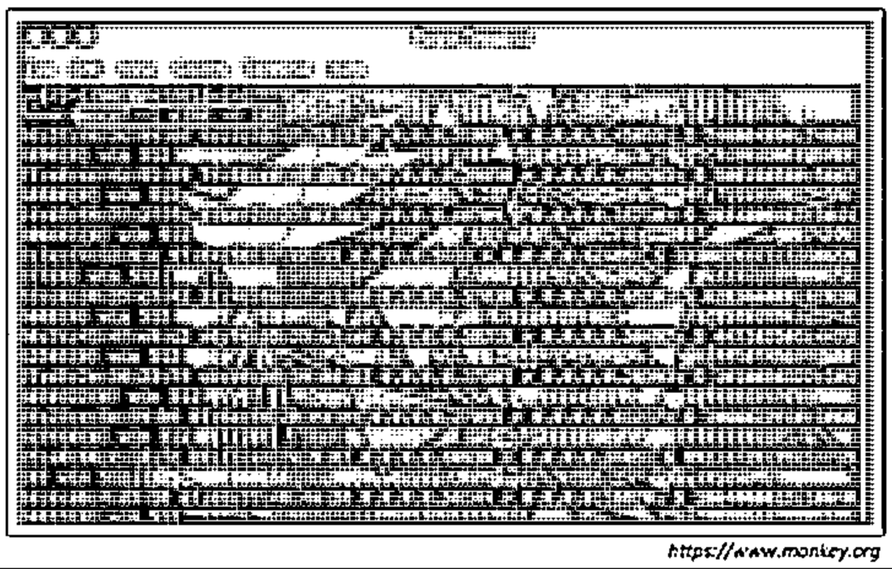
MAC Flooding

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



Mac Flooding Switches with macof

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



https://www.monkey.org

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

MAC Flooding

MAC flooding is a technique used to compromise the security of network switches that connect network segments or 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.

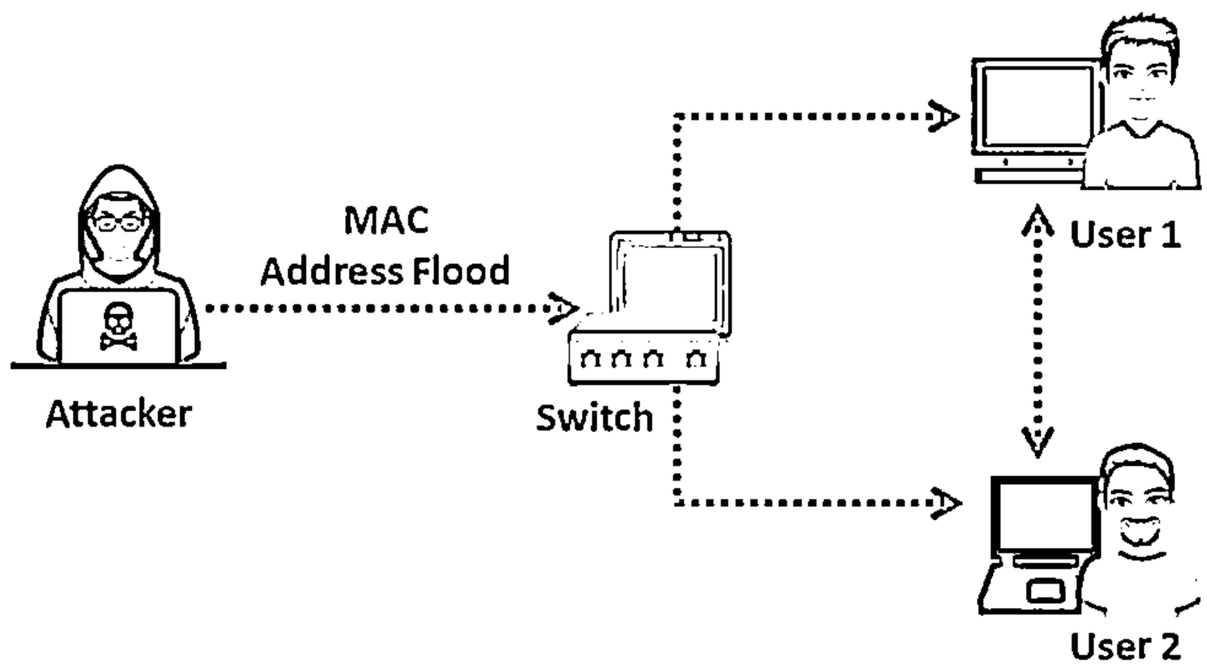


Figure 8.20: MAC flooding

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.

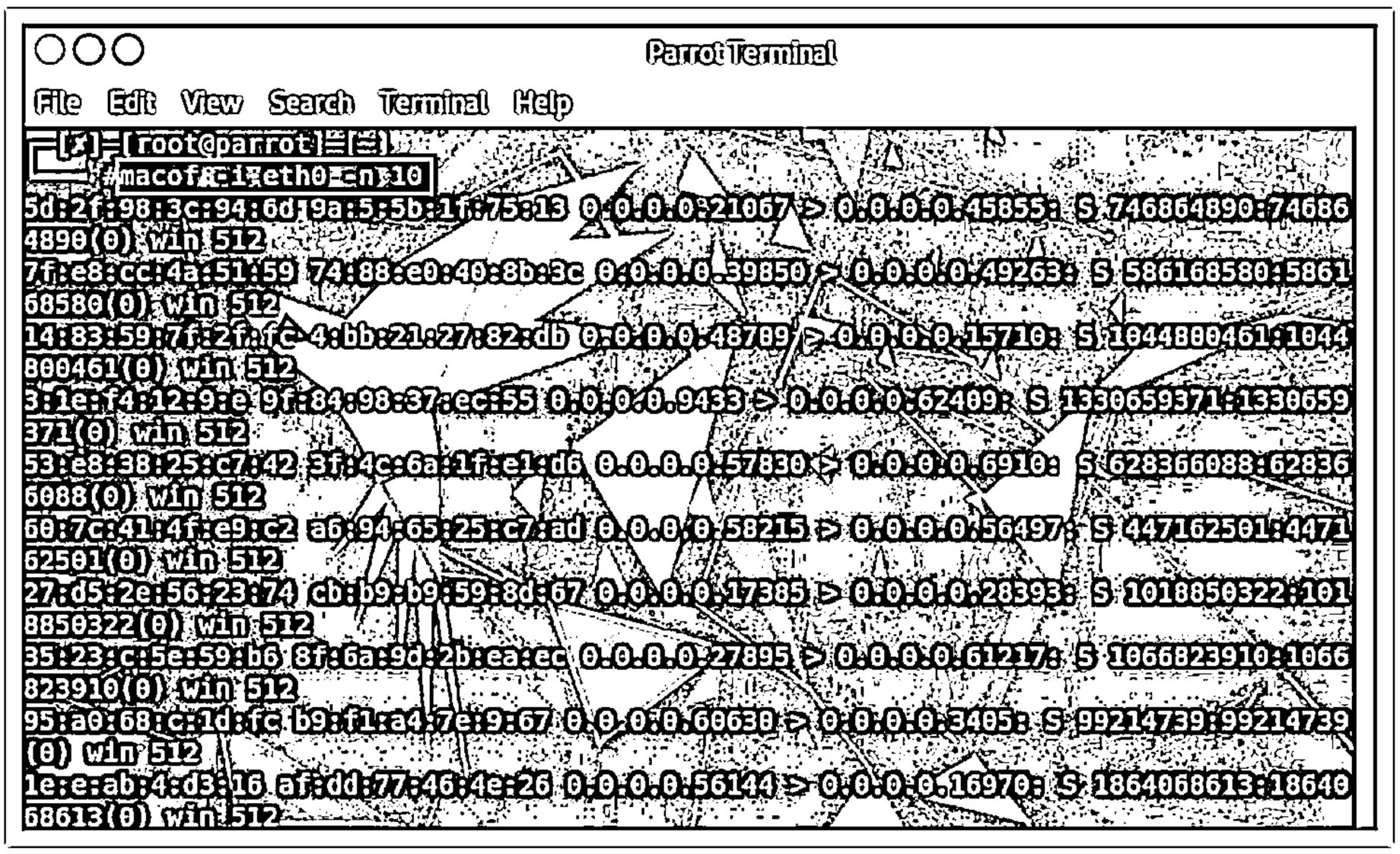
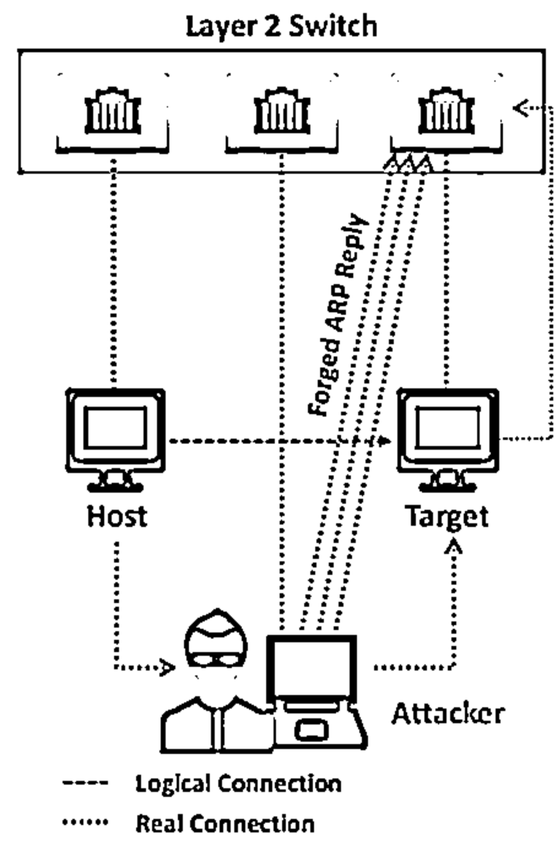


Figure 8.21: MAC flooding using macof

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 the target host's packets occurs; thus the switch must change its MAC address, binding constantly between two different ports
- In such a case, if the attacker is fast enough, he/she will able to direct the packets intended for the target host toward his/her switch port
- The attacker now manages to steal the target host's switch port and sends ARP requests to the stolen 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 toward the targeted host



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 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.

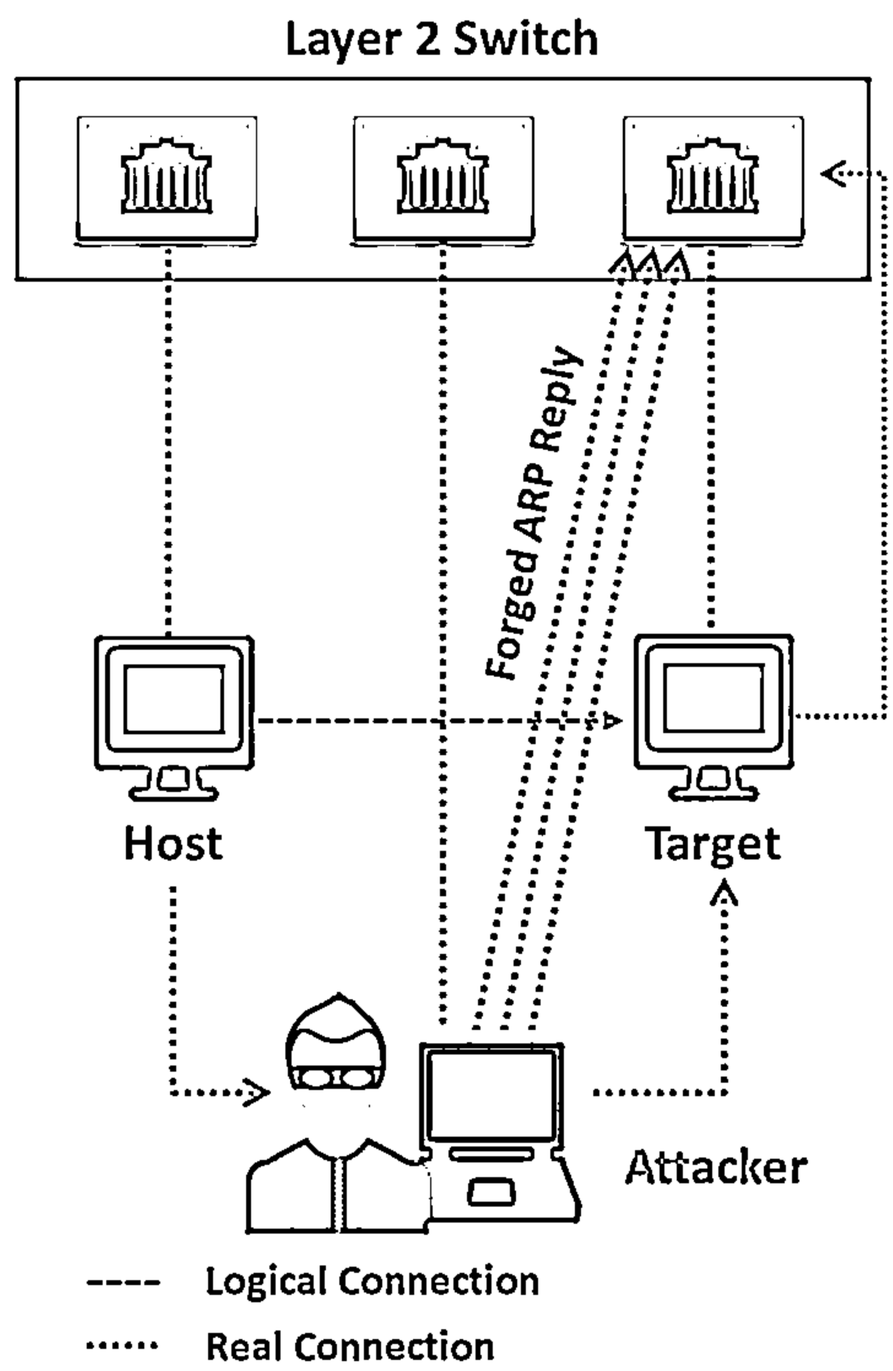


Figure 8.22: Switch port stealing

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.

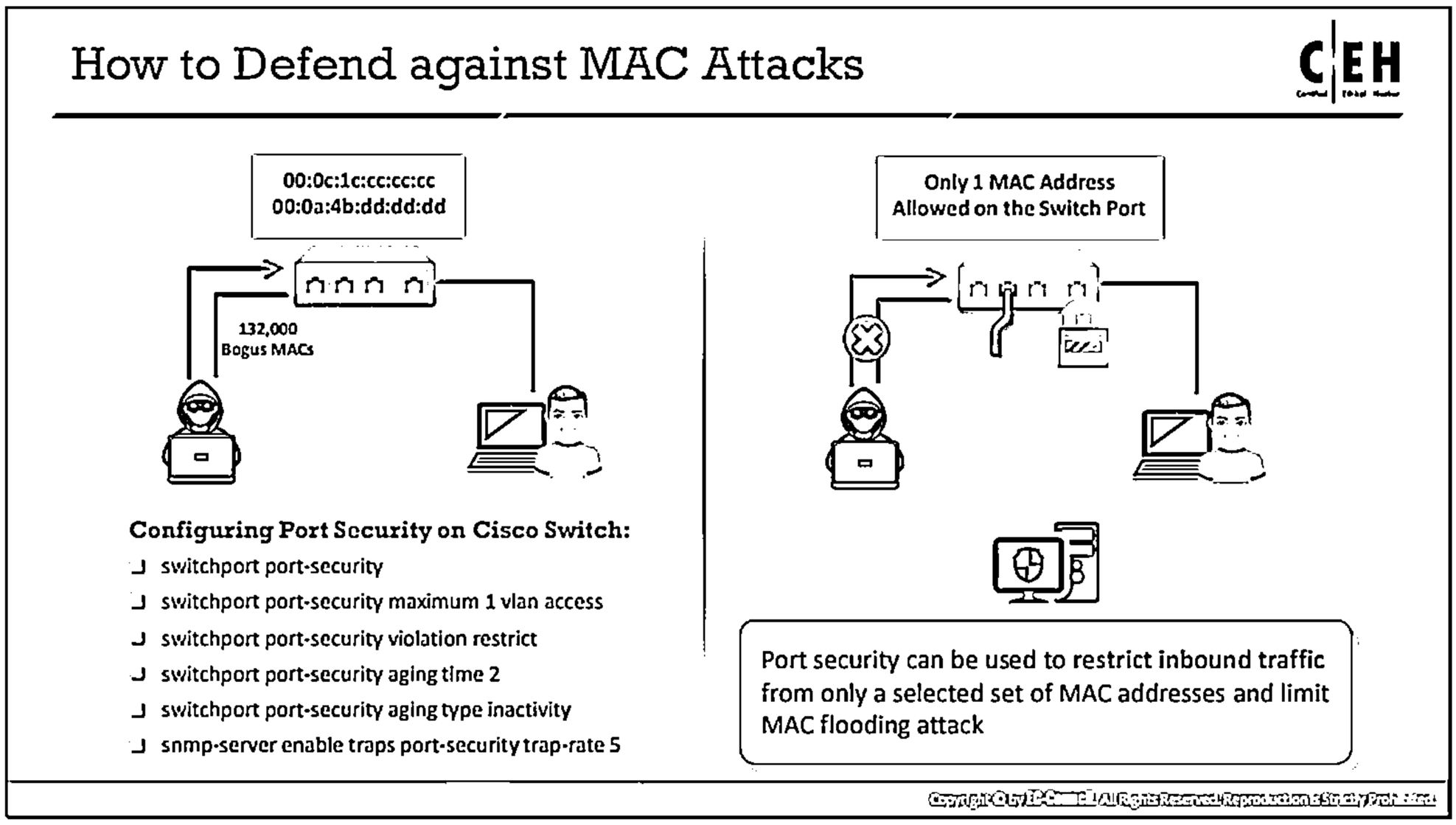
VLAN	MAC Address	Type	Learn	Age	Ports
255	Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	0	Port A
5	Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port B
5	Host C	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port C

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.

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.

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

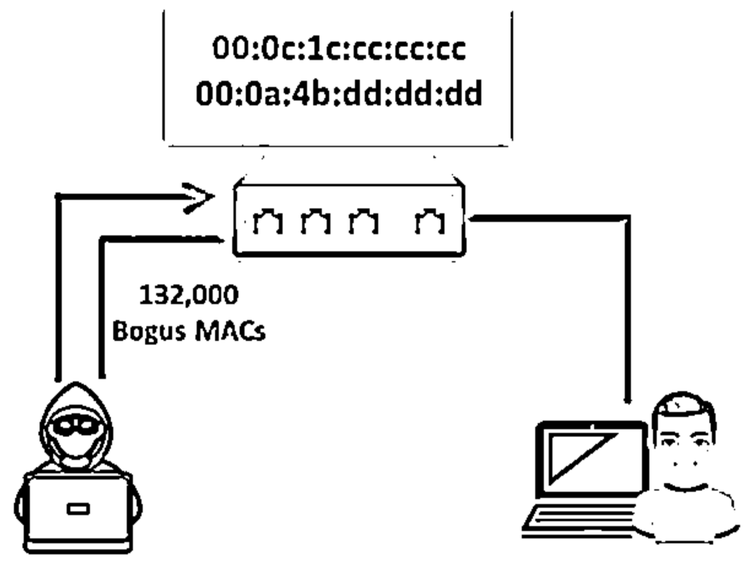


Figure 8.23: Flooding CAM tables

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.

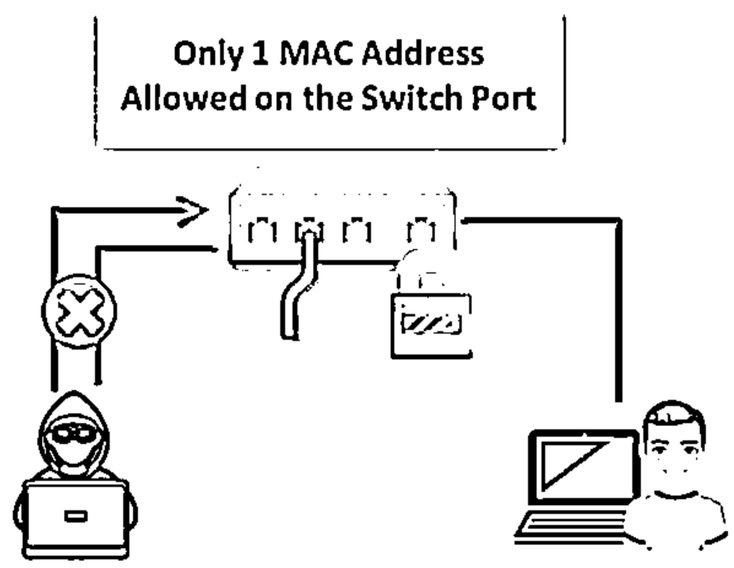


Figure 8.24: Blocking MAC flooding

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.

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.

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

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`**

    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.

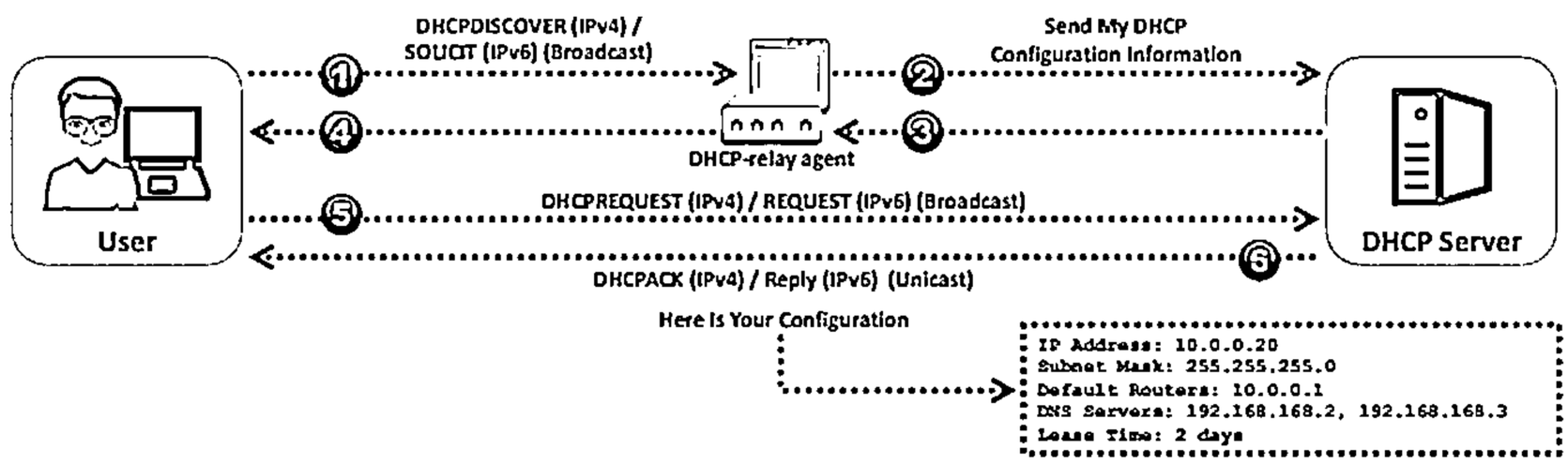
- **`snmp-server enable traps port-security trap-rate 5`**

  Controls the rate at which SNMP traps are generated.

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

How DHCP Works

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



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.
3. A DHCP server unicasts DHCPOFFER/ADVERTISE, which contains the client's and server's MAC addresses.

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

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.

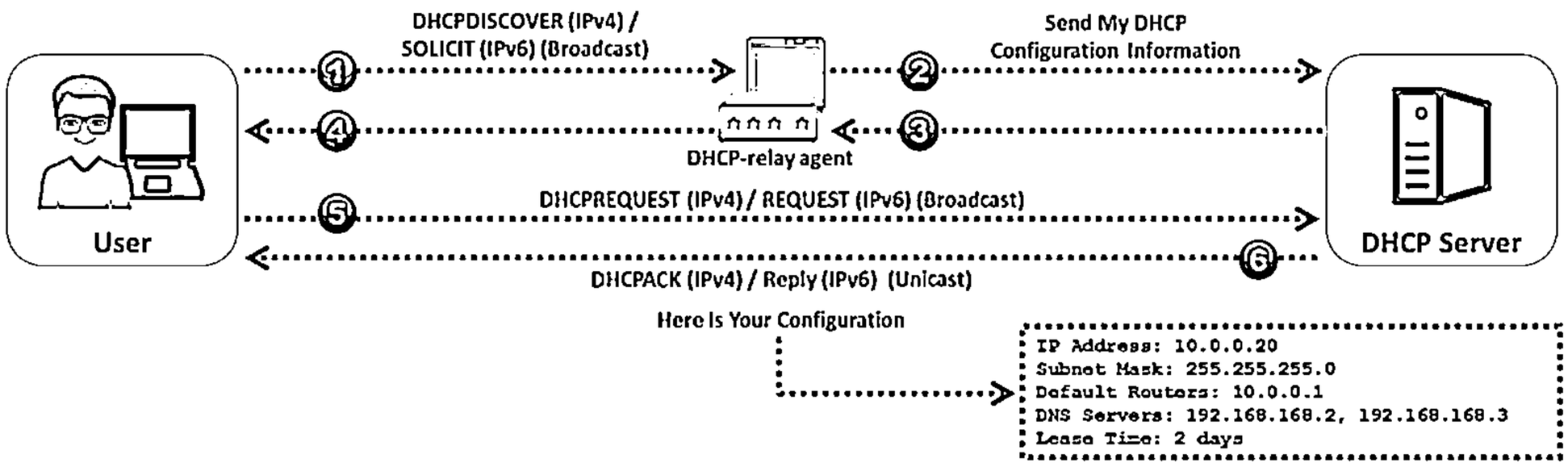


Figure 8.25: Working of DHCP

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

DHCP Request/Reply Messages

DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client broadcast to locate 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
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

IPv4 DHCP Packet Format

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

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

DHCP Request/Reply Messages

A device that already has an IP address can use the simple request/reply exchange to 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
DHCPRelease	Release	Client to server relinquishing the network address and canceling the remaining lease

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

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.

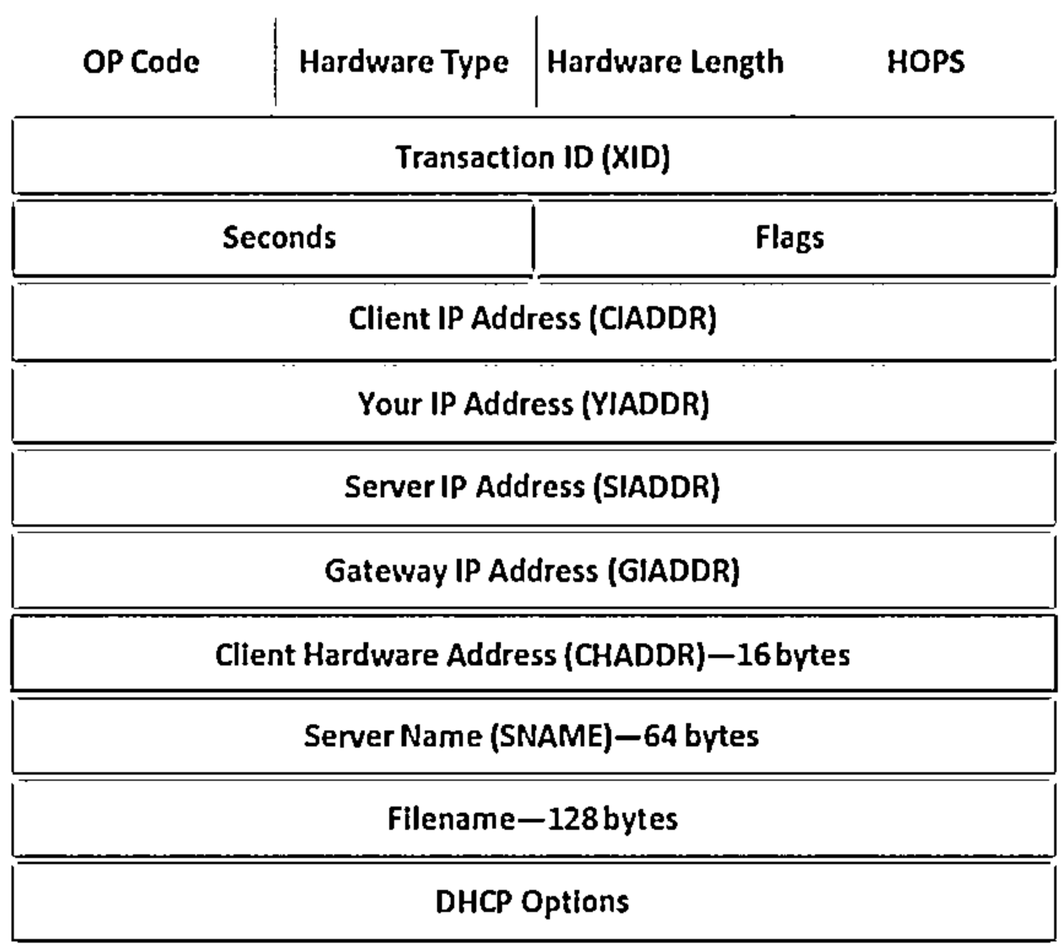


Figure 8.26: IPv4 DHCP packet format

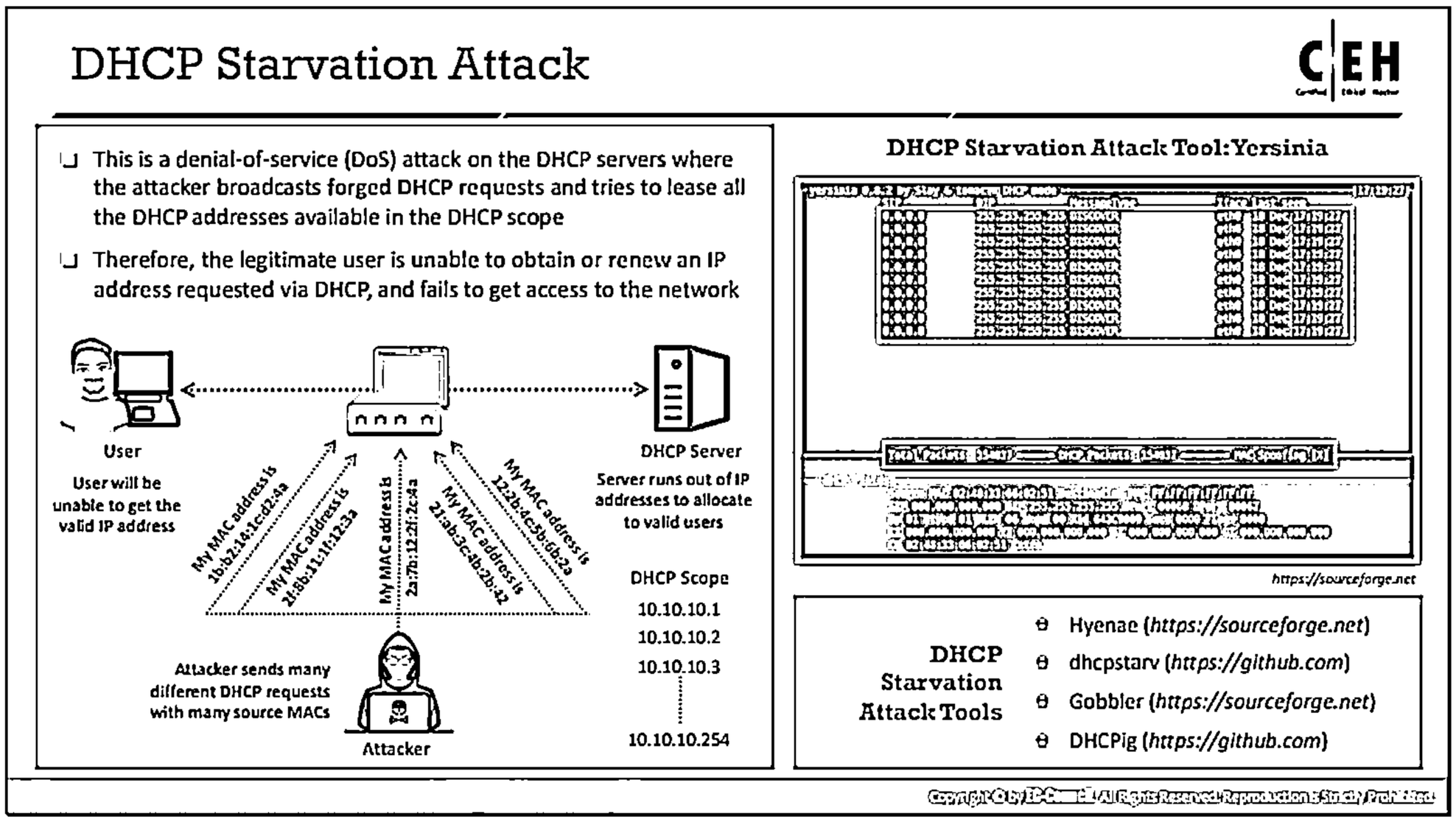
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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
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

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



DHCP Starvation Attack

In a DHCP starvation attack, an attacker floods the DHCP server by sending 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.

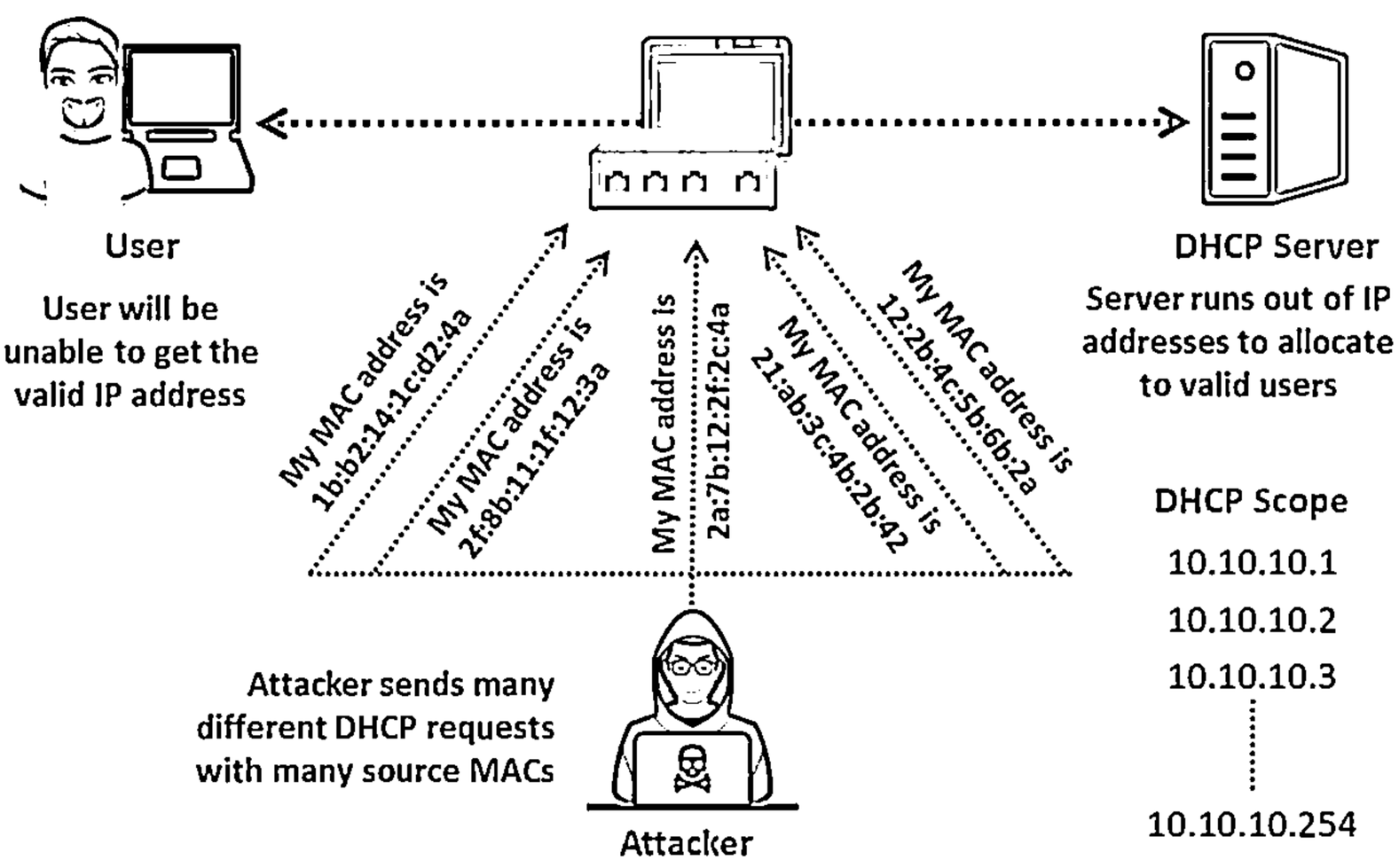


Figure 8.27: DHCP starvation attack

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

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.

- **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.

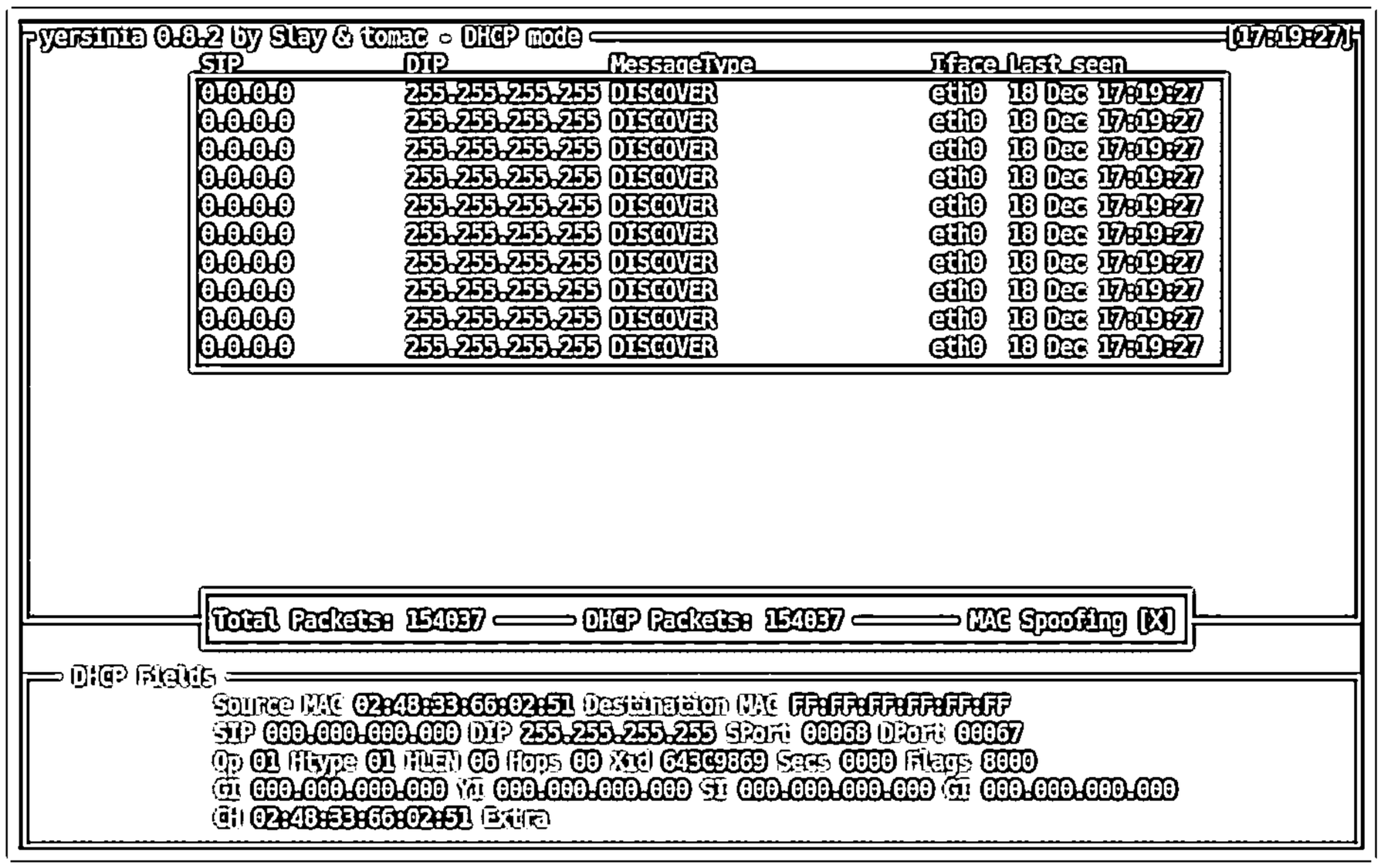
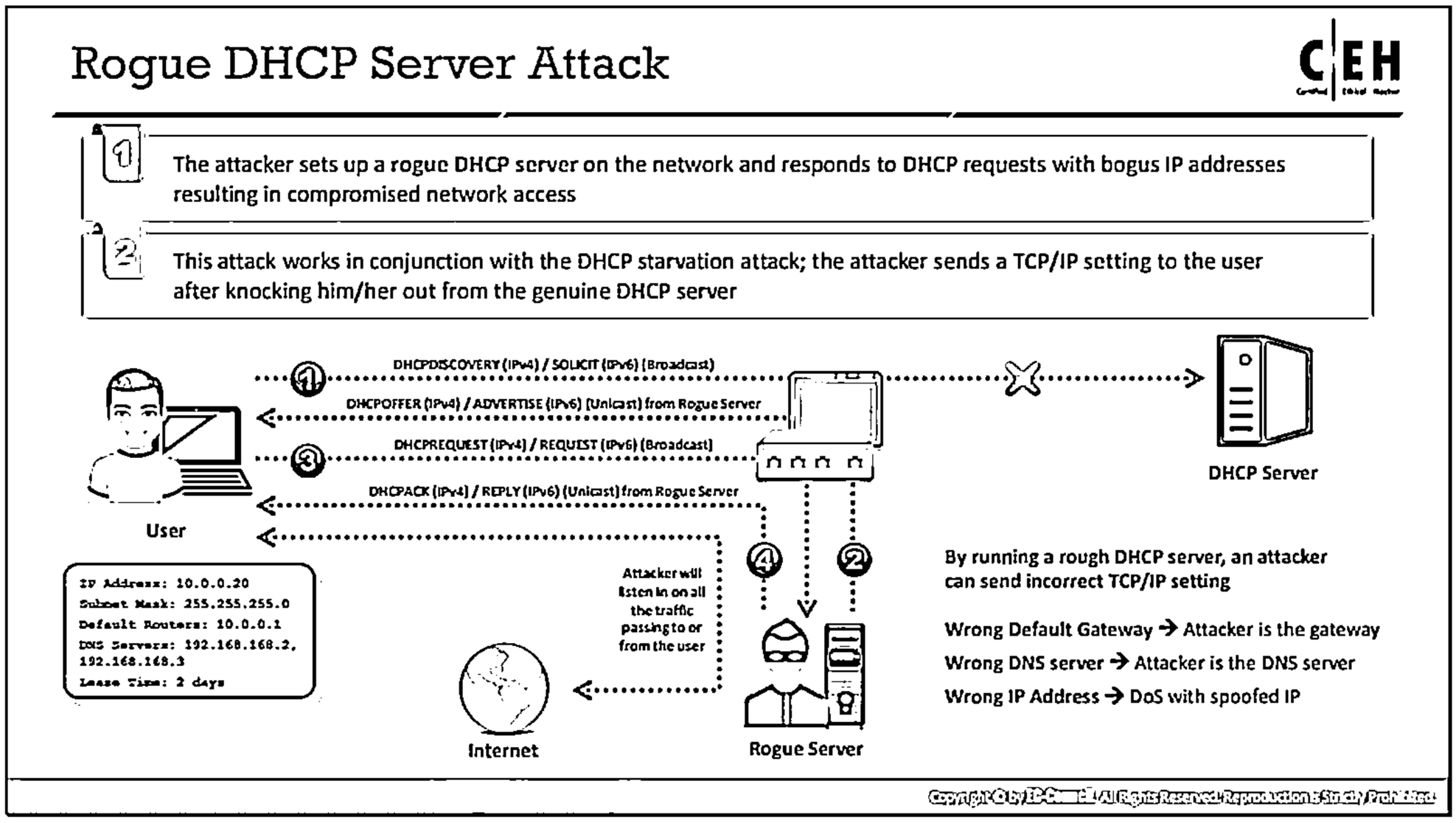


Figure 8.28: Screenshot of Yersinia

Some examples of DHCP starvation attack tools are listed below:

- 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.

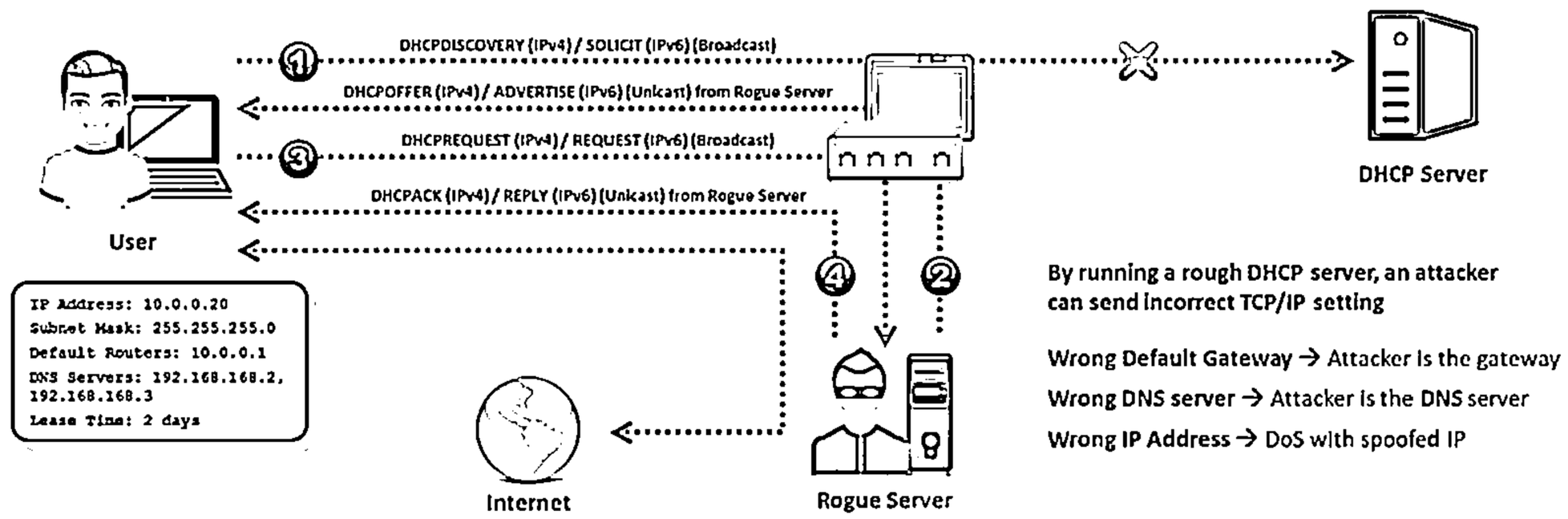
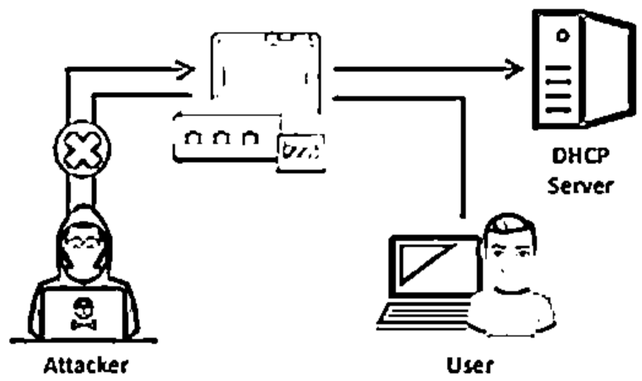


Figure 8.29: Rogue DHCP server attack

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

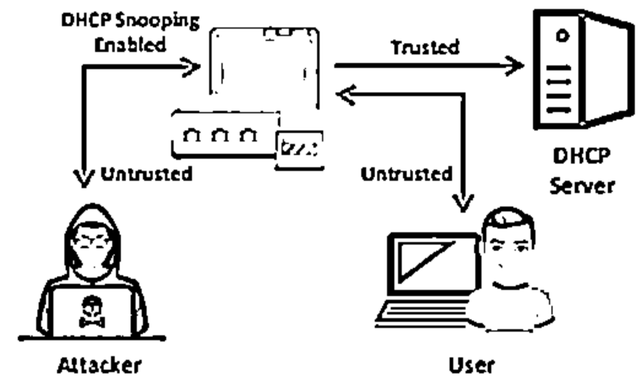
- Enable port security to defend against DHCP starvation attacks
  - Configuring the MAC limit on the switch's edge ports drops the packets from further MACs once the limit is reached



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

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.

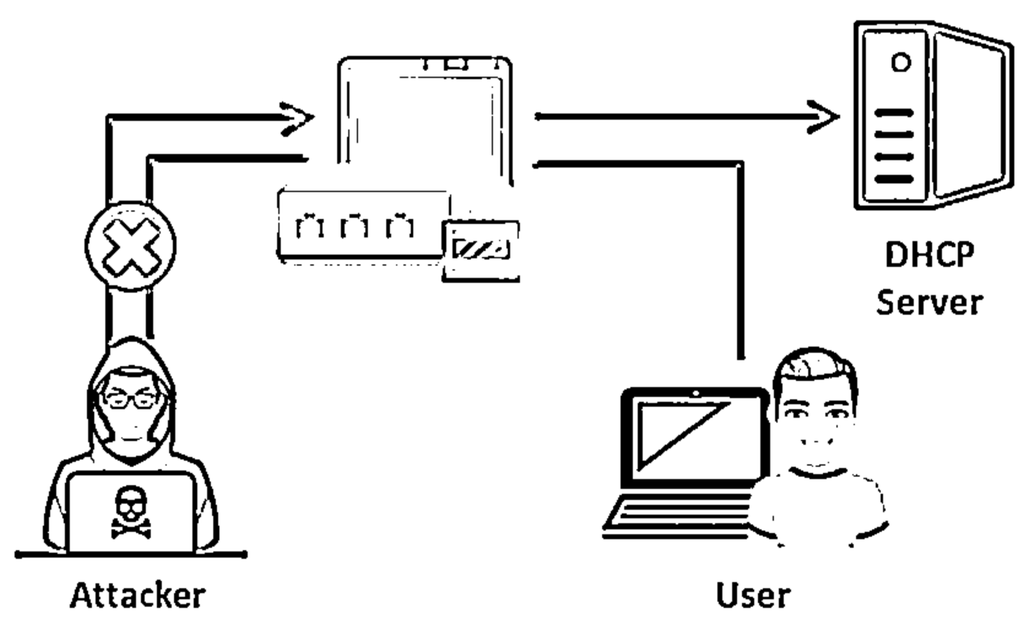


Figure 8.30: Defending against a DHCP starvation attack

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.

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

- **`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.

  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.

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

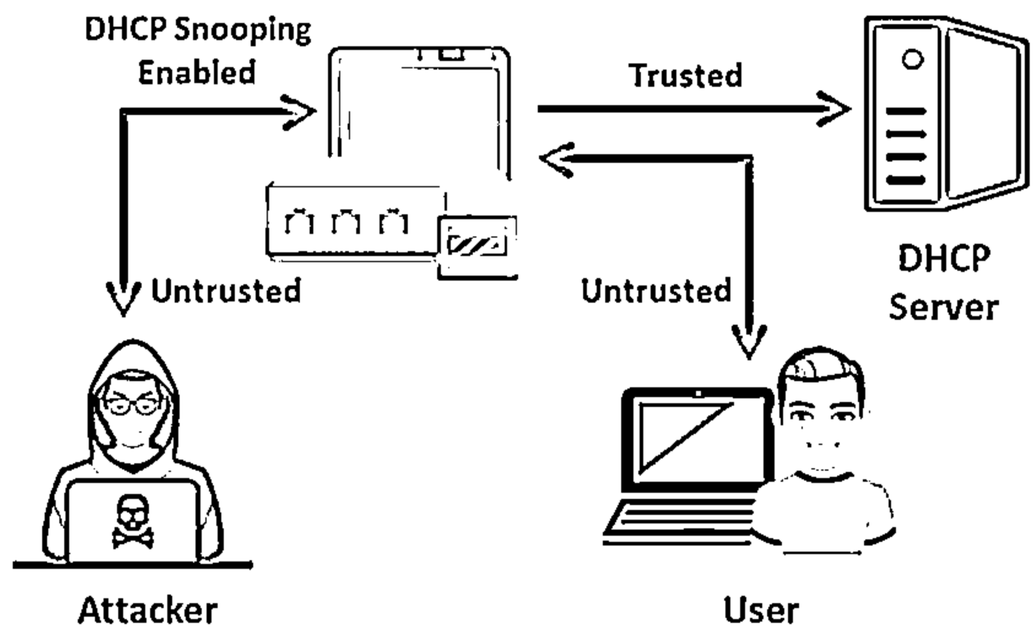


Figure 8.31: Defending against a rogue server attack

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.

5. `end`

   Exits configuration mode.

6. `show ip dhcp snooping`

   Verifies the configuration.

Additional DCHP snooping command:

- `no ip dhcp snooping information option`

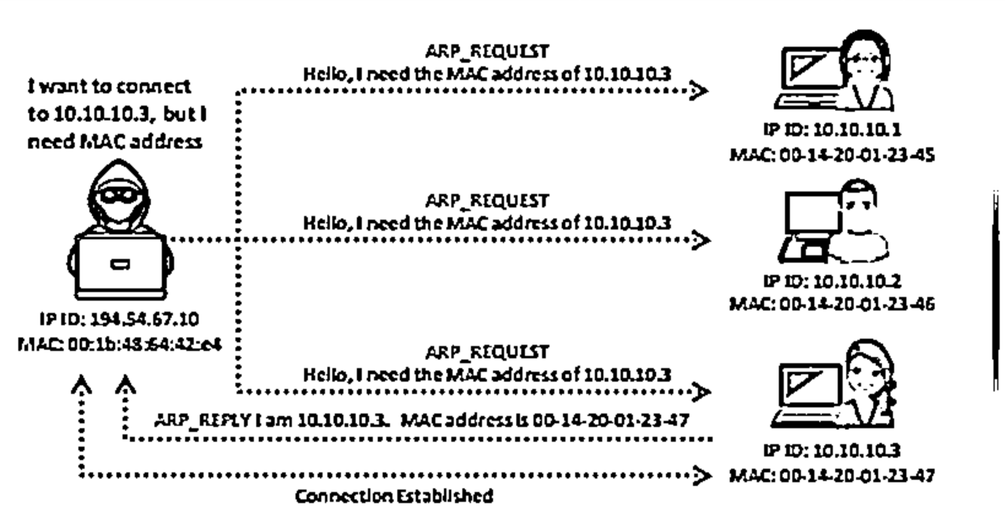
  To disable the insertion and the removal of the option-82 field, use the `no ip dhcp snooping information option` in global configuration command. To configure an aggregation, switch to drop incoming DHCP snooping packets with option-82 information from an edge switch, and use the "no IP dhcp snooping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

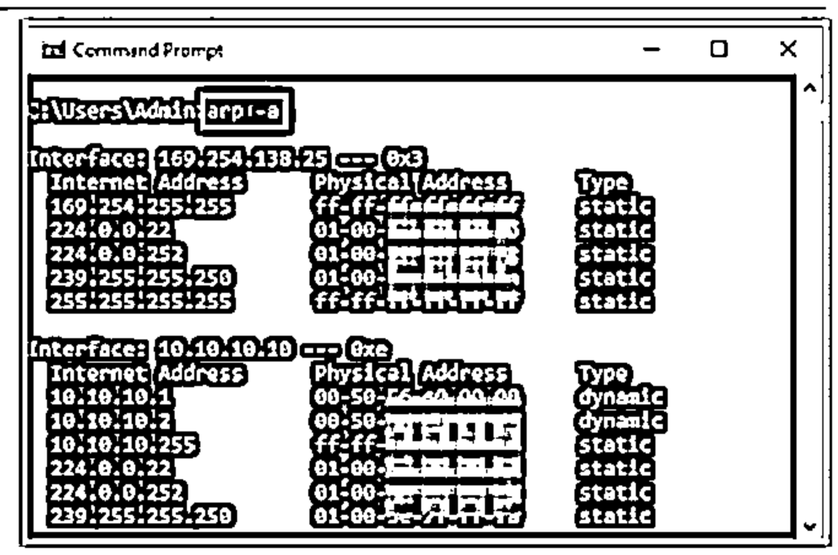
Note: All ports in the VLAN are untrusted by default.

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

What Is Address Resolution Protocol (ARP)?

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





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)?

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

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

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

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.

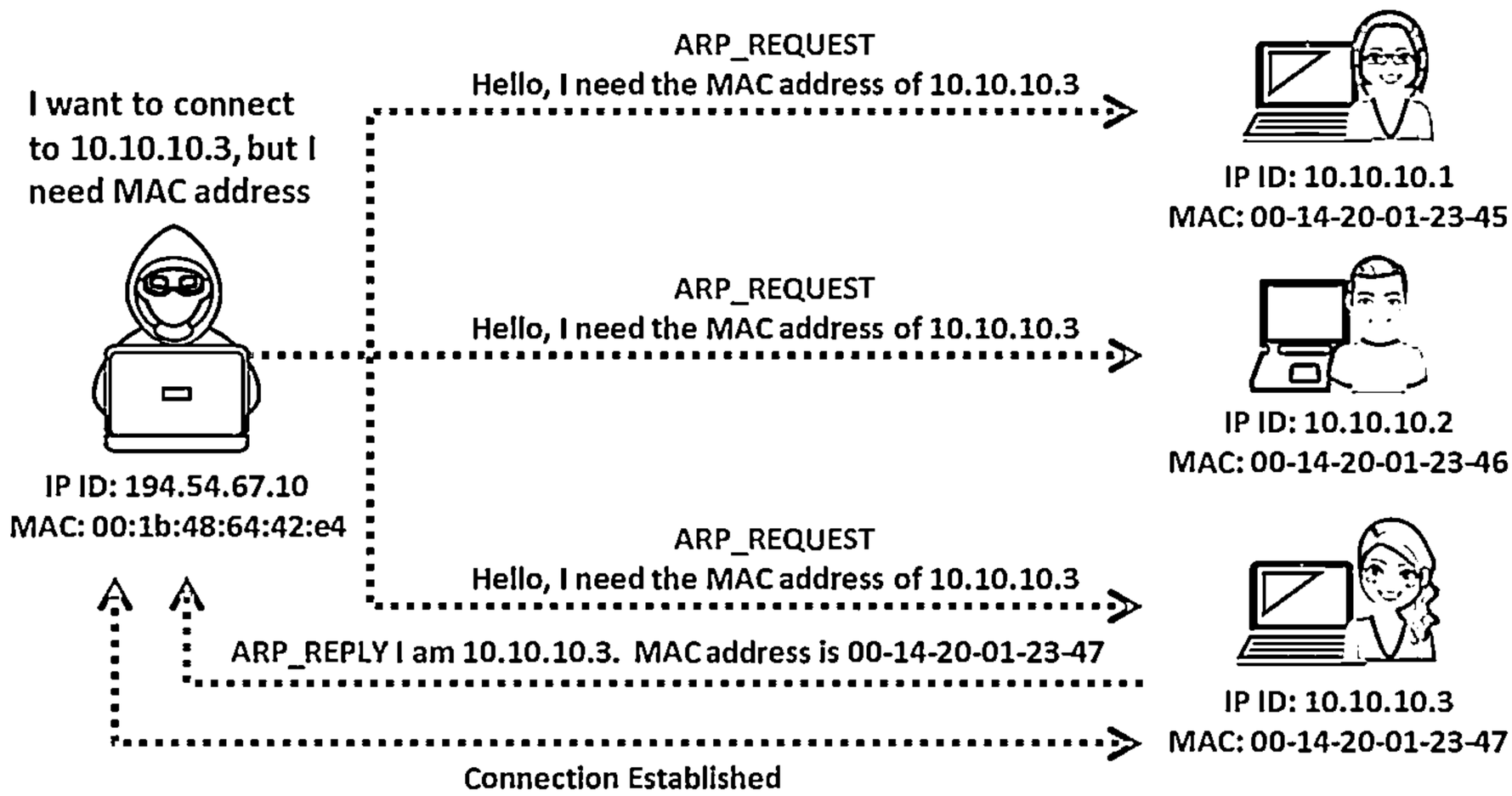


Figure 8.32: Working of ARP protocol

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.

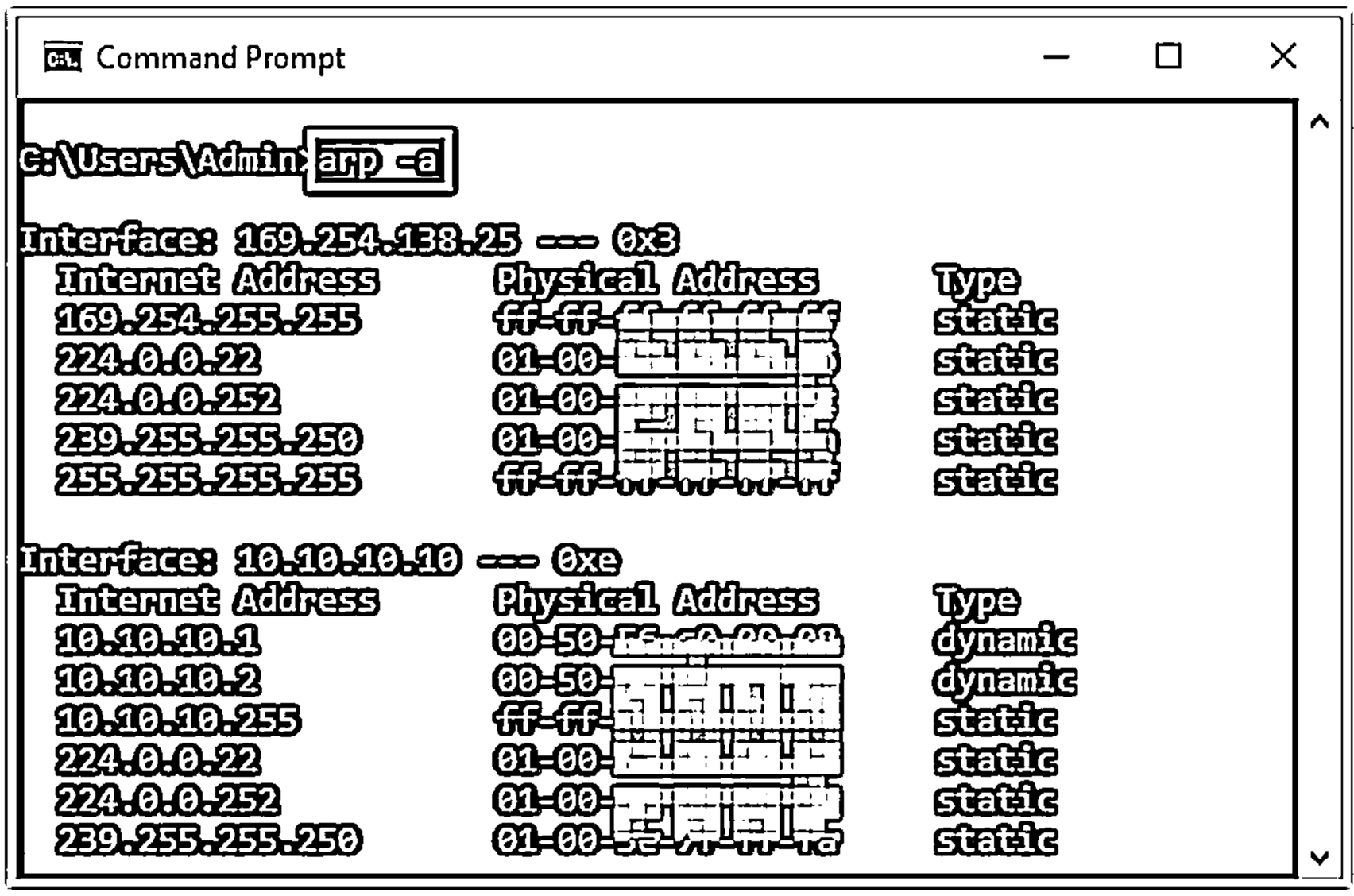
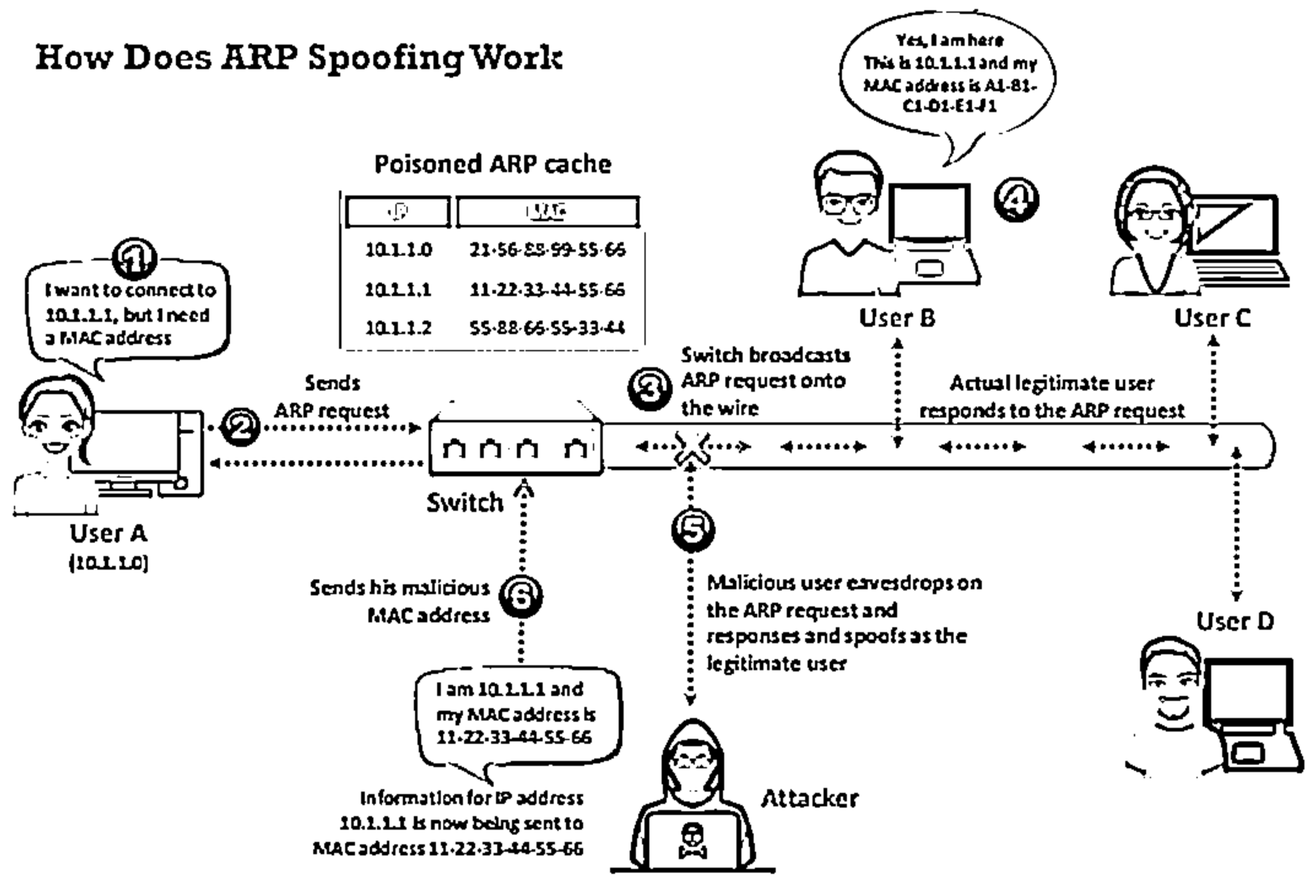


Figure 8.33: ARP cache

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

ARP Spoofing Attack

- ARP packets can be forged to send data to the attacker's machine
- ARP spoofing involves constructing many forged ARP request and reply packets to overload the switch
- The switch is set in "forwarding mode" after the ARP table is flooded with spoofed ARP replies, and attackers can then sniff all the network packets
- Attackers flood a target computer's ARP cache with forged entries, which is also known as poisoning



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.

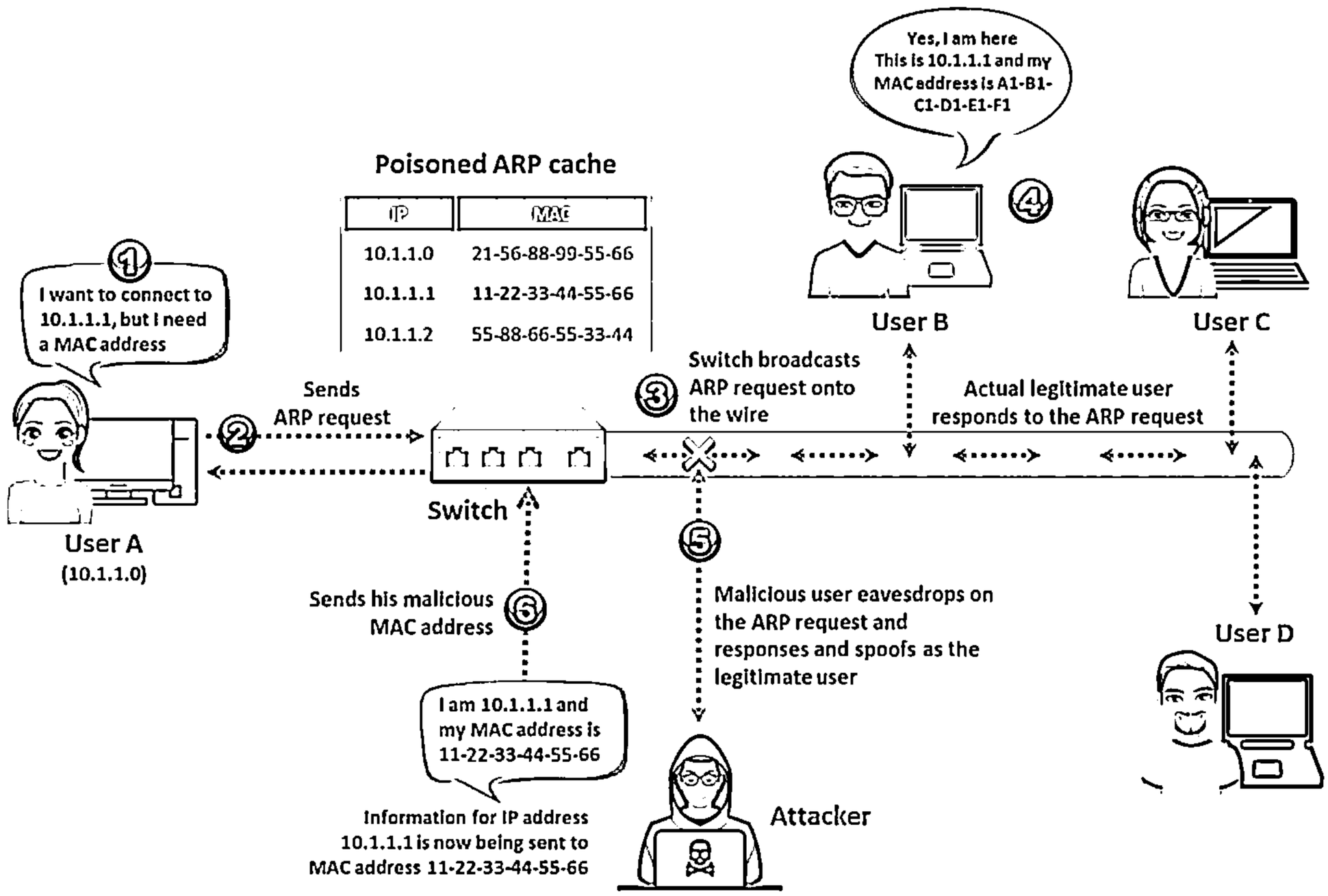


Figure 8.34: Working of an ARP spoofing attack

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

Threats of ARP Poisoning

- Using fake ARP messages, an attacker can divert all communications between two machines, resulting in all traffic being exchanged via the attacker's PC

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

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

Threats of ARP Poisoning

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

The threats of ARP poisoning include:

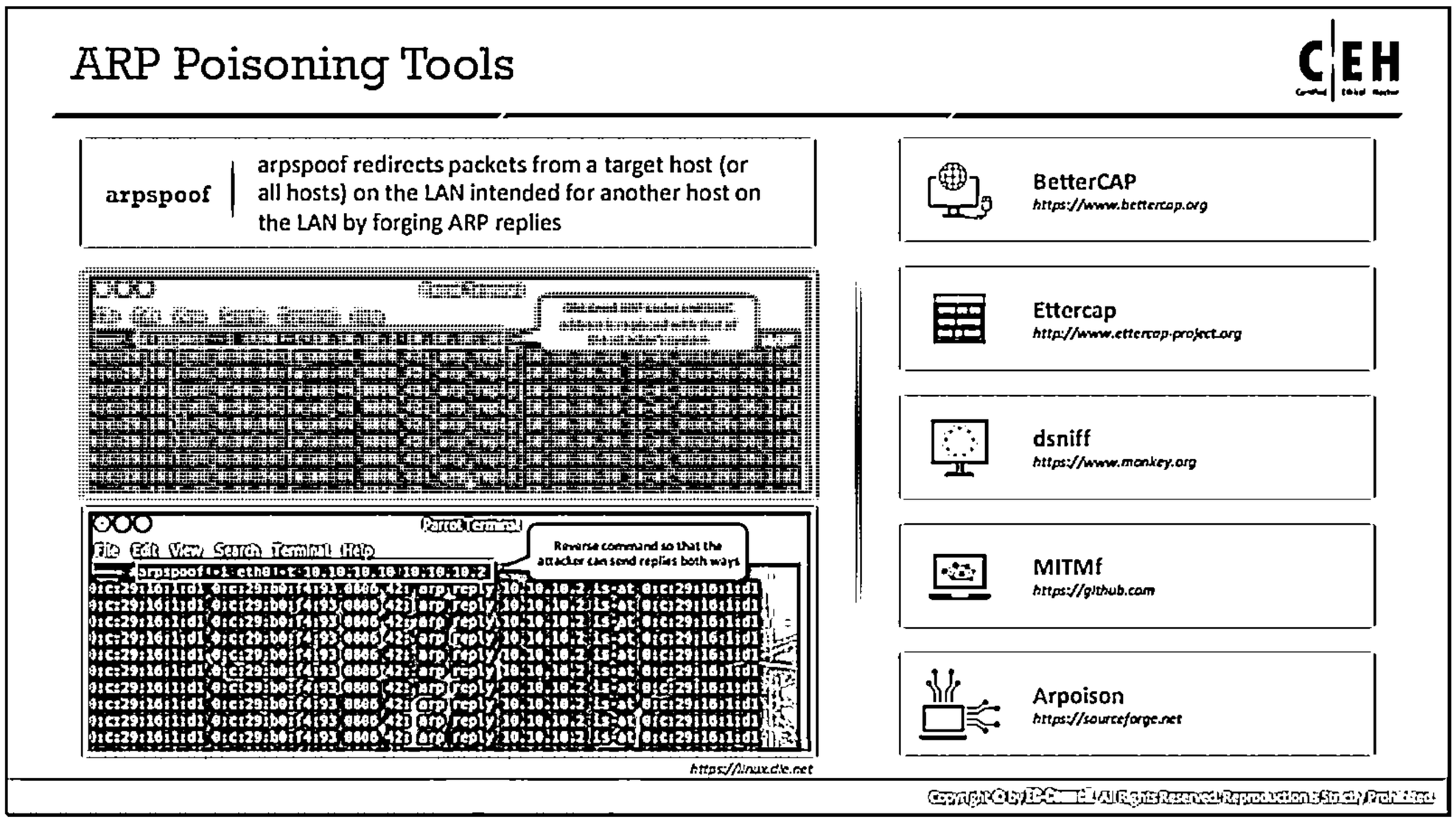
- **Packet Sniffing**: Sniffs traffic over a network or a part of the network.
- **Session Hijacking**: Steals valid session information and uses it to gain unauthorized access to an application.
- **VoIP Call Tapping**: Uses port mirroring, which allows the VoIP call tapping unit to monitor all network traffic, and picks only the VoIP traffic to record by MAC address.
- **Manipulating Data**: ARP spoofing allows attackers to capture and modify data, or stops the flow of traffic.
- **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 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.

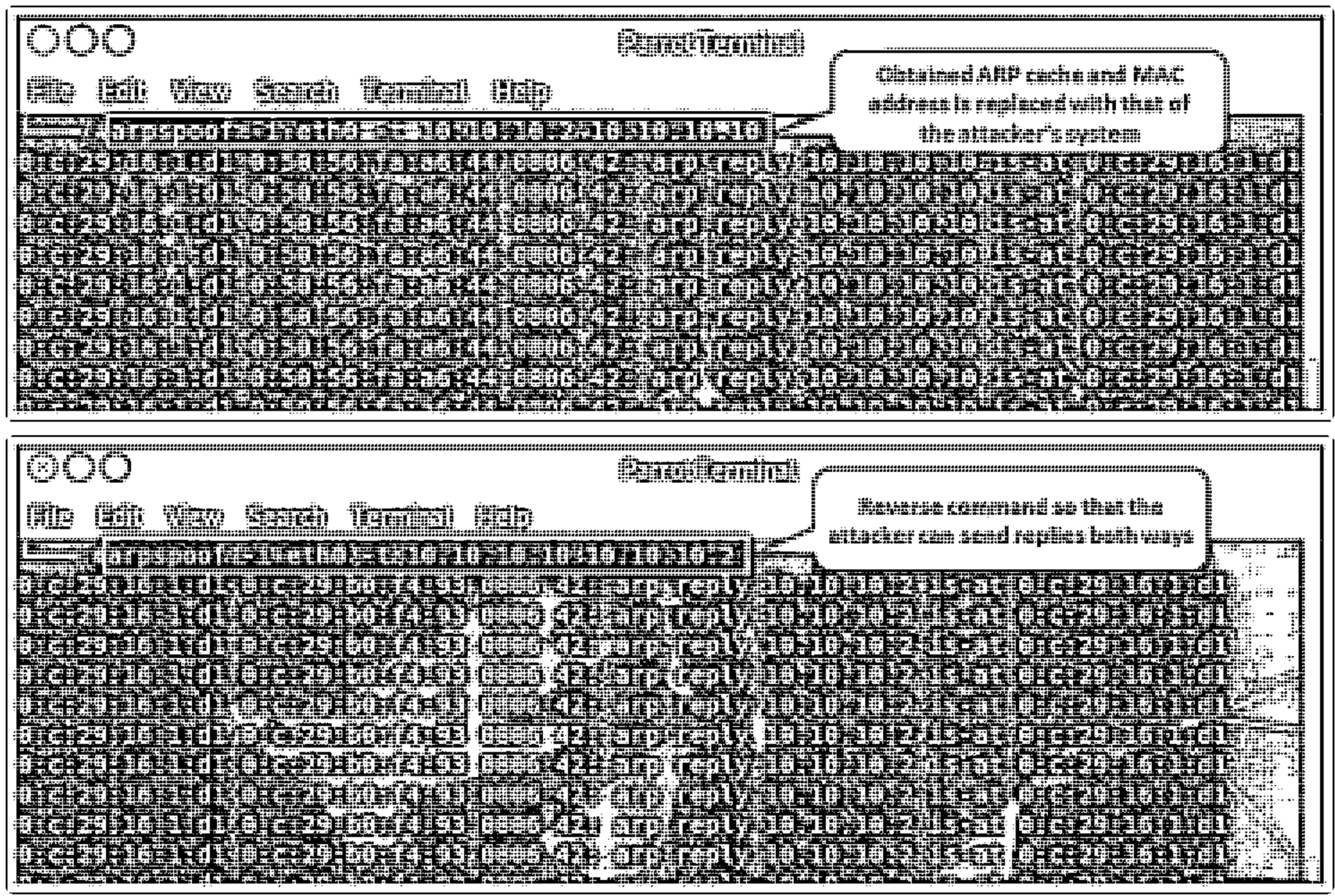
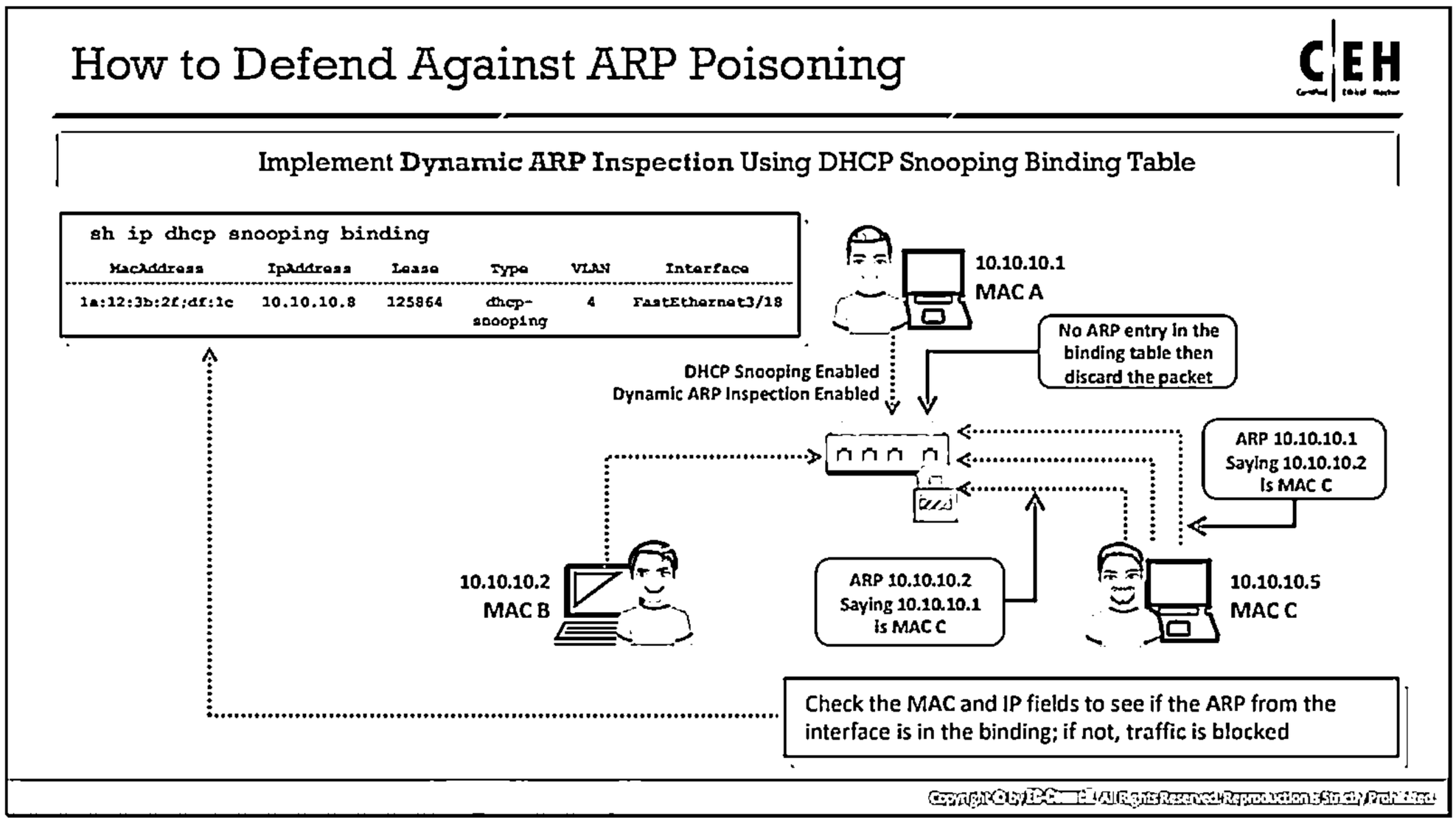


Figure 8.35: Screenshots of arpspoof

Some examples of ARP poisoning tools are listed below:

- BetterCAP (*https://www.bettercap.org*)
- Ettercap (*http://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.

The implementation of cryptographic protocols such as HTTP Secure (HTTPS), Secure Shell (SSH), Transport Layer Security (TLS), and various other networking cryptographic protocols

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

prevents ARP spoofing attacks by encrypting data before transmission and authenticating it after it is received.

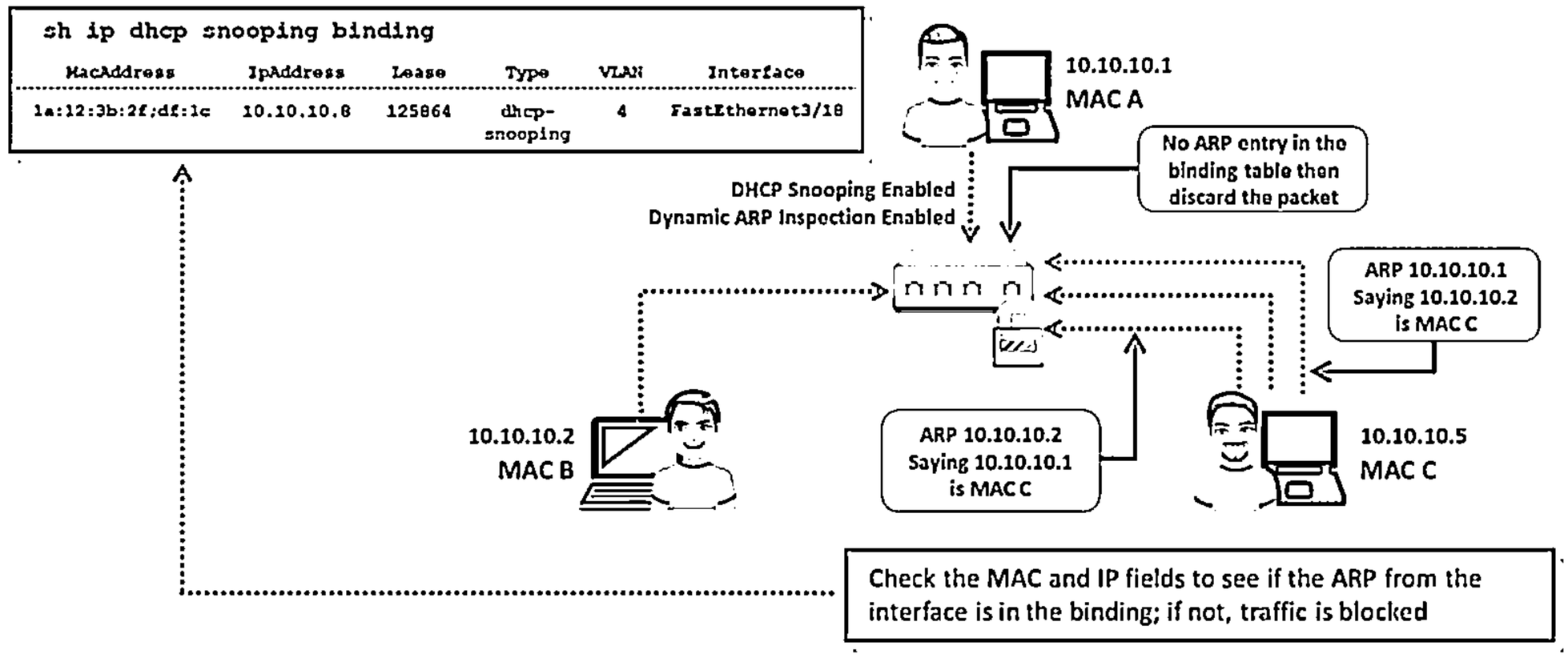


Figure 8.36: Defending against ARP poisoning

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

1

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

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

2

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

3

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

4

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs
(Res) on Fa0/5, vlan
10.([0013.6050.acf4/192.168.10.1/ffff.ffff.fff
f/192.168.10.1/05:37:31 UTC Mon Jul 08 2019])
```

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.

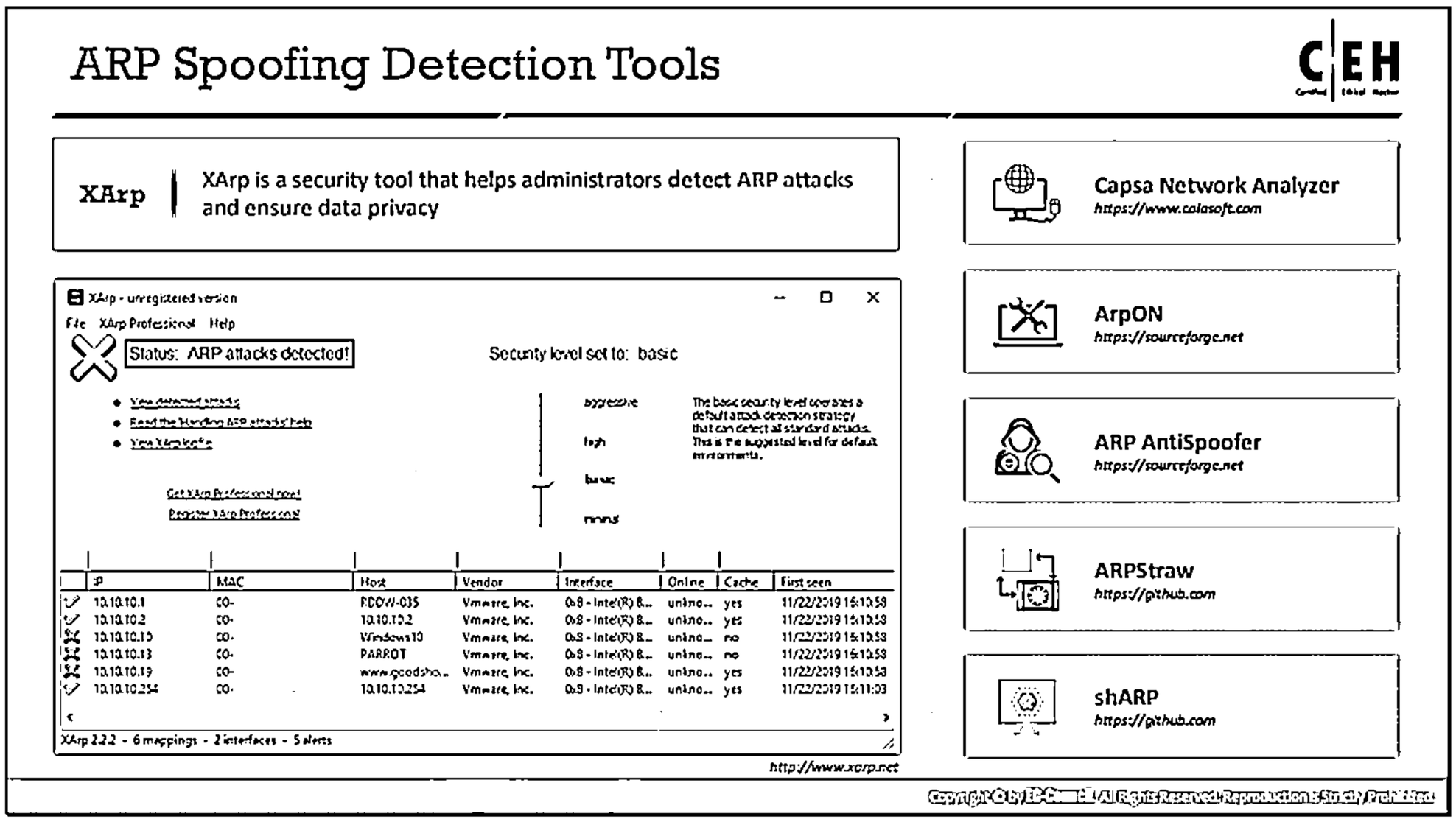
Assume that an attacker with the source IP address 192.168.10.1 connects to VLAN 10 on interface FastEthernet0/5 and sends ARP replies, pretending to be the default router for the subnet in an attempt to initiate an MITM attack. The switch with DAI enabled inspects these reply packets by comparing them 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 Mon
JUL 08 2019])
```

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

- **XArp**

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

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

  As shown in the screenshot, security professionals use XArp to detect ARP spoofing attacks performed on the systems.

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

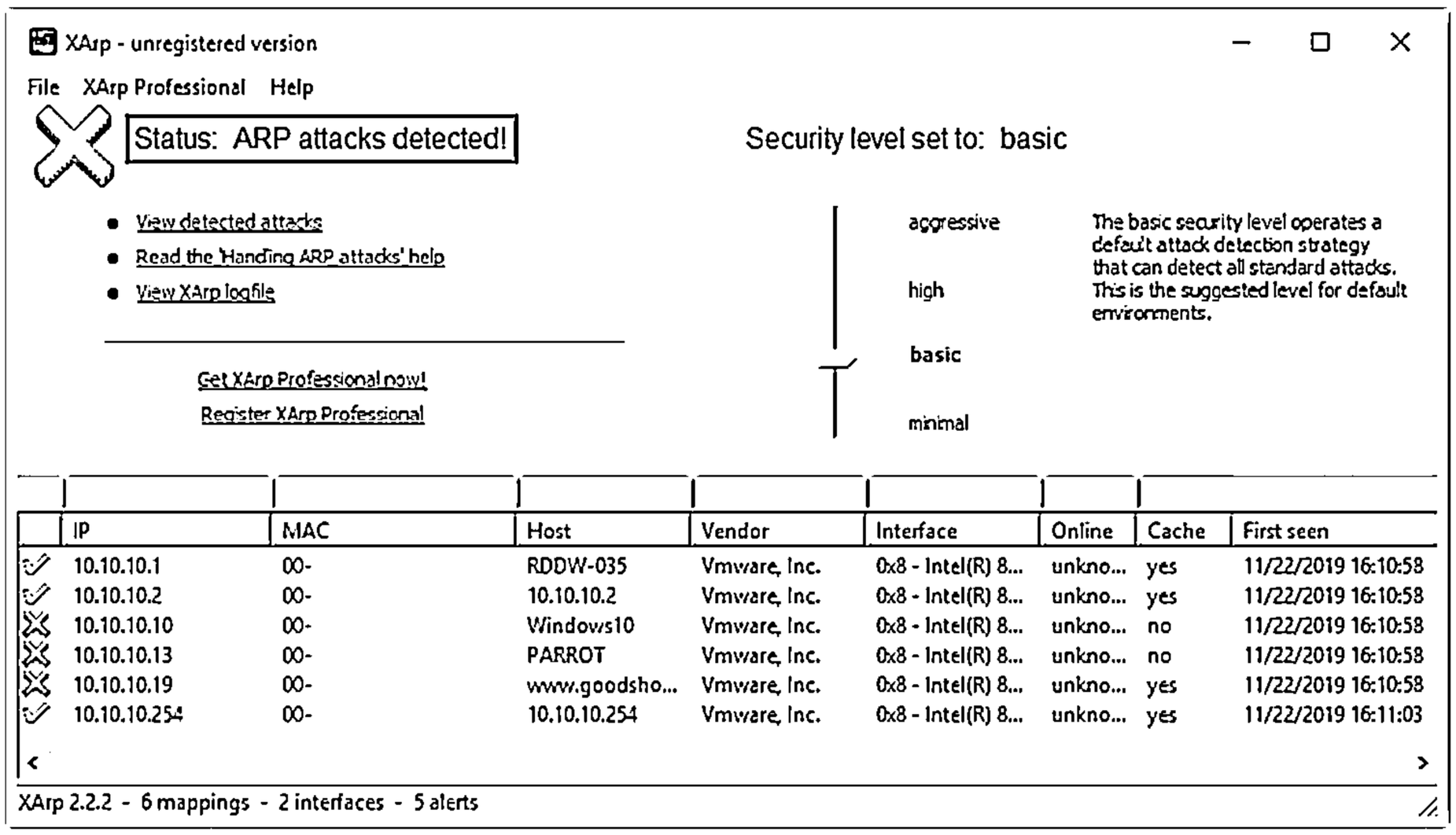


Figure 8.37: Screenshot of XArp

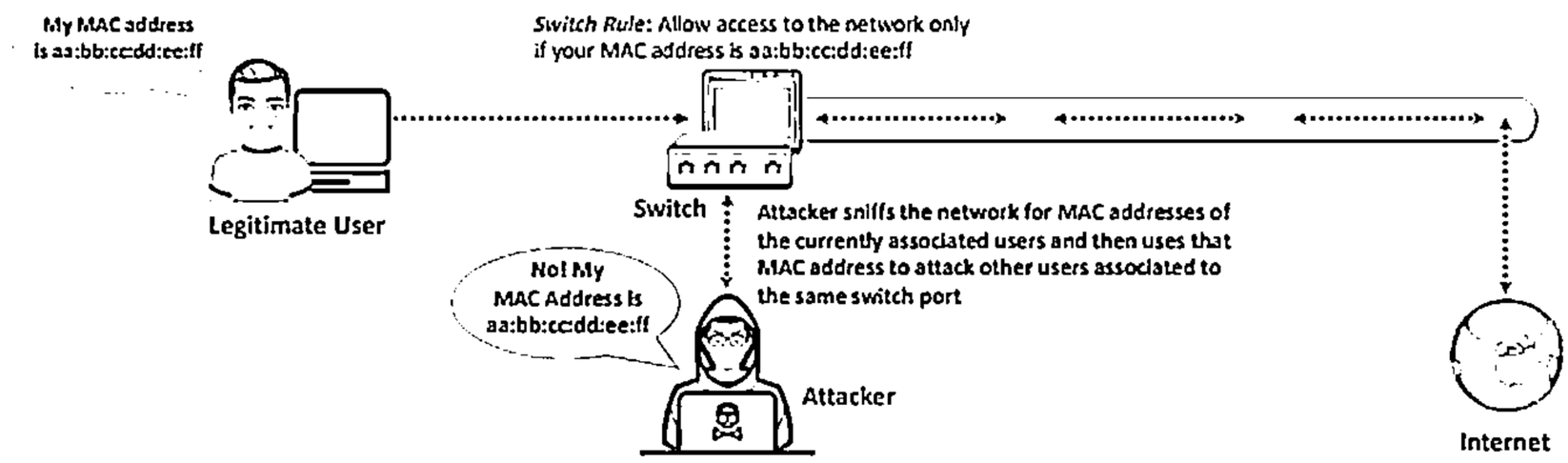
Some examples of ARP spoofing detection tools are listed below:

- Capsa Network Analyzer (*https://www.colasoft.com*)
- 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.

MAC Spoofing/Duplicating

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



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

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

Sniffing Technique: Spoofing Attacks

Besides ARP spoofing, an attacker can also use MAC spoofing, 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.

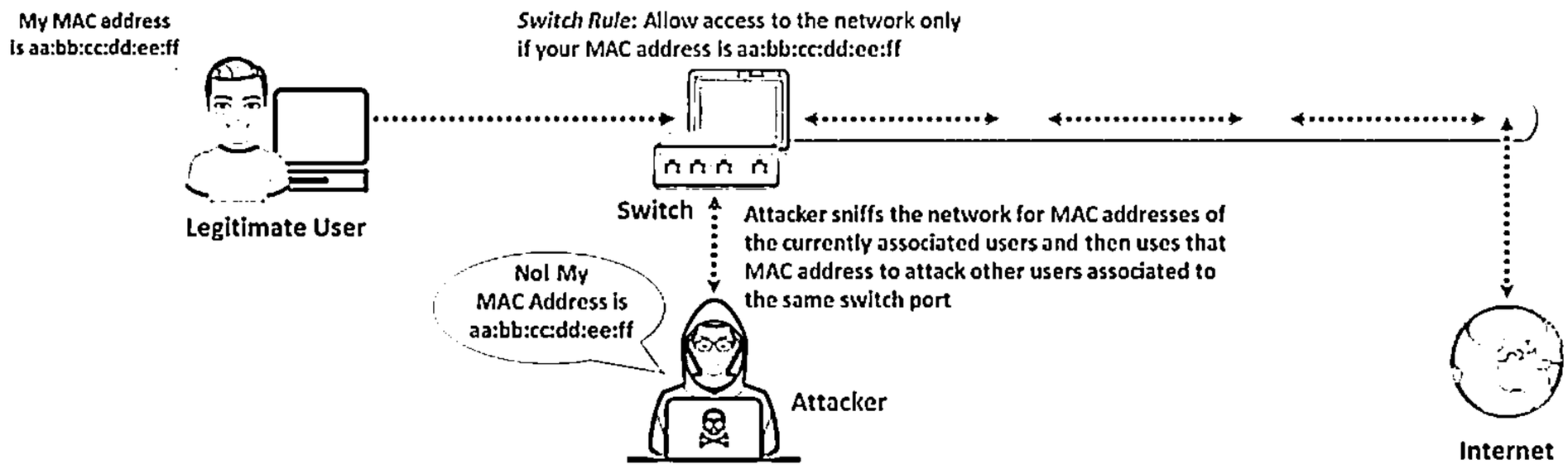


Figure 8.38: MAC spoofing/duplicating attack

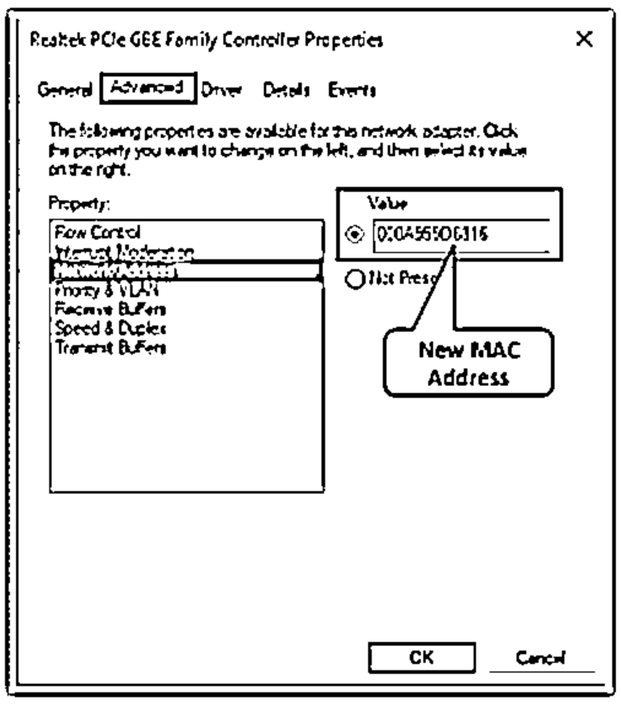
Note: This technique can be used to bypass wireless access points' MAC filtering.

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

MAC Spoofing Technique: Windows

In Windows 10 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)

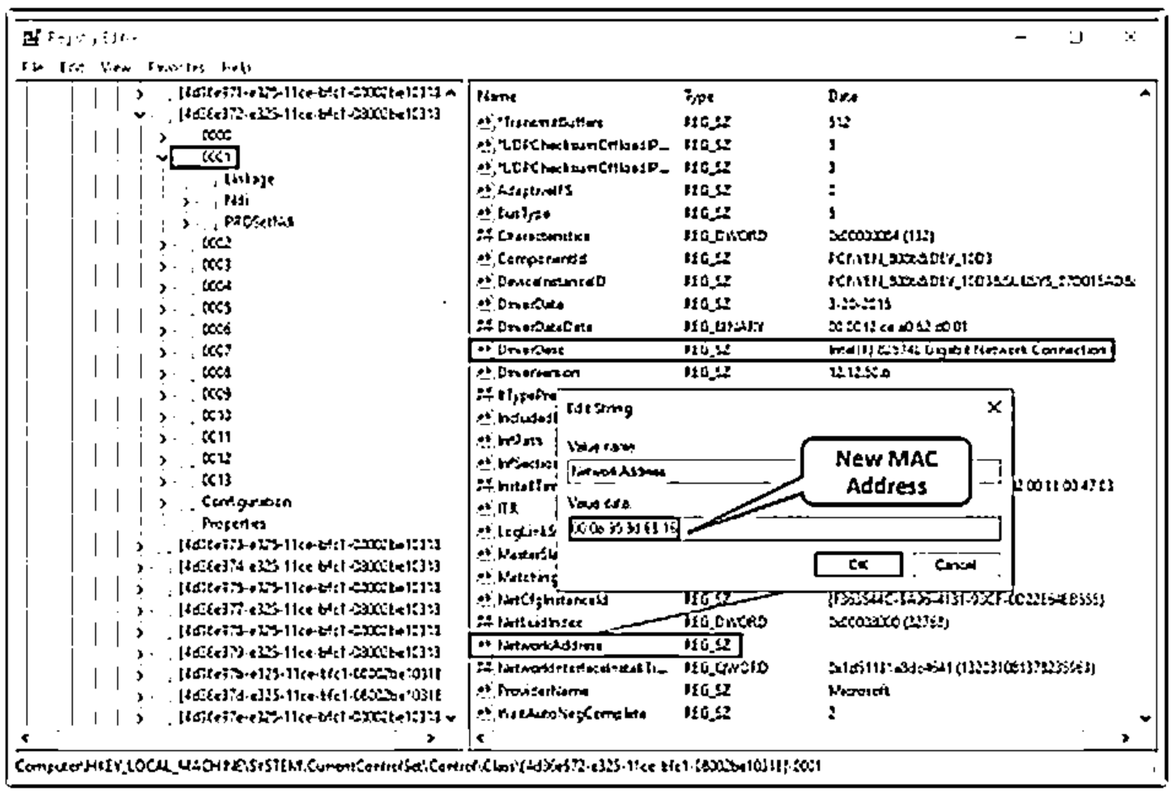
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Spoofing Technique: Windows (Cont'd)

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

- Press Win + R to open Run, type regedt32 to start the registry editor

  Note: Do not type Regedit to start the registry editor
- Go to "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318} and double click 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 10 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.**
2. Click on **Ethernet** and then click on **Properties** in the **Ethernet Status** window.

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

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).

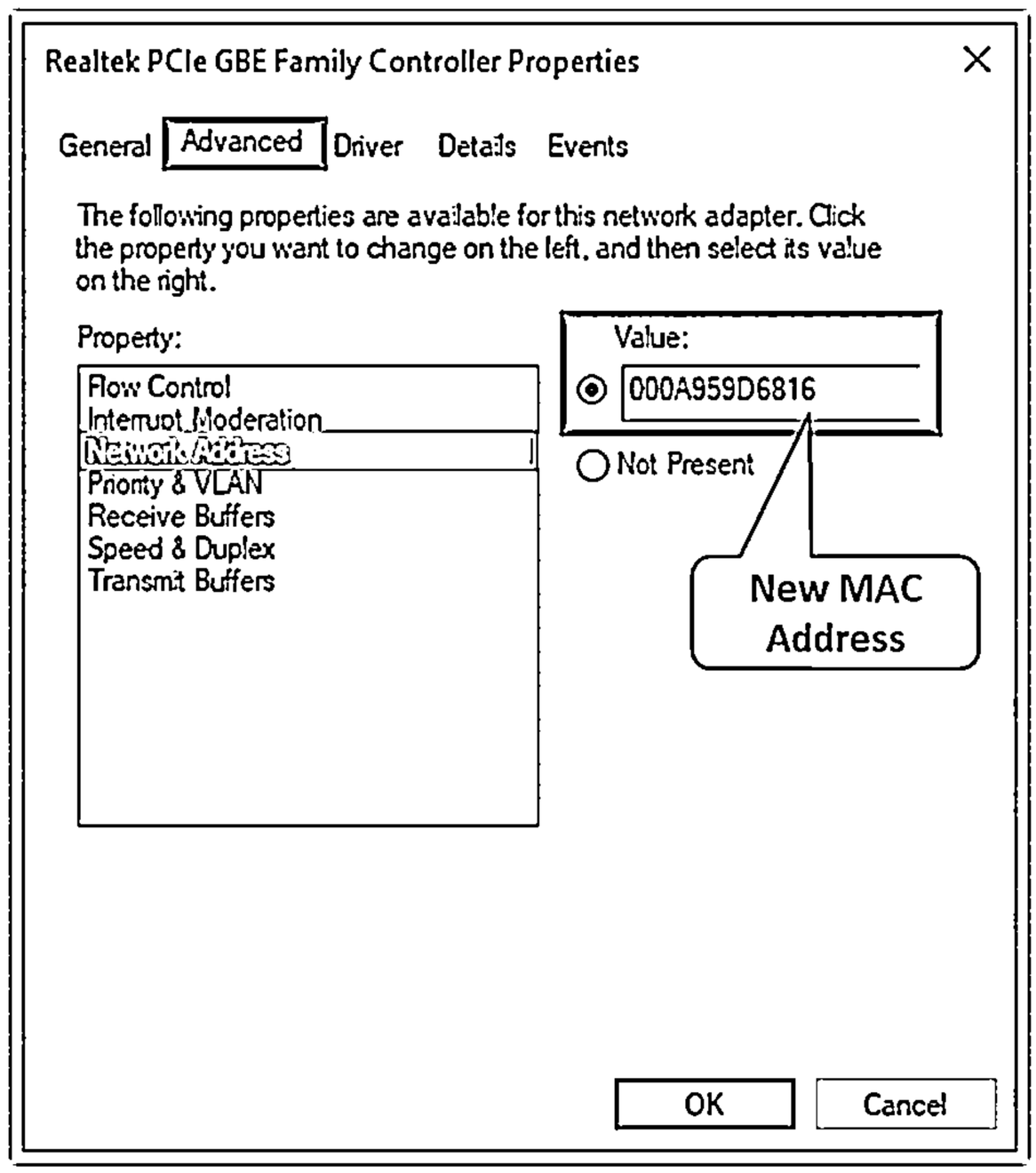


Figure 8.39: Ethernet Properties dialog box

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

1. Press **Win + R** to open Run, and type **regedit32** to start the registry editor.
2. **Note:** Do not type **Regedit** to start the registry editor. Go to **"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}** and double-click on it to expand the tree.
3. Four-digit sub keys representing network adapters will be found (starting with 0000, 0001, 0002, etc.).

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

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.

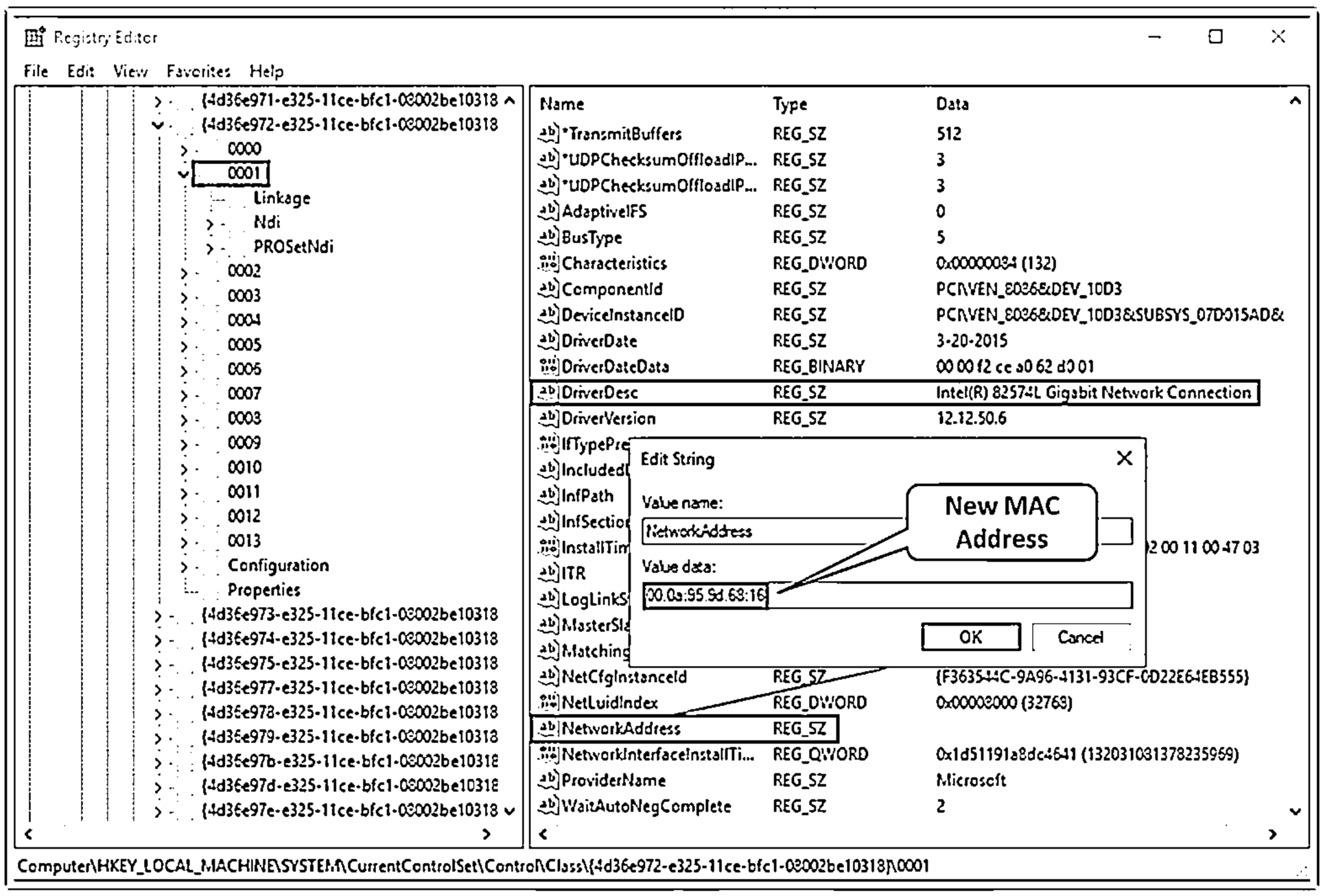
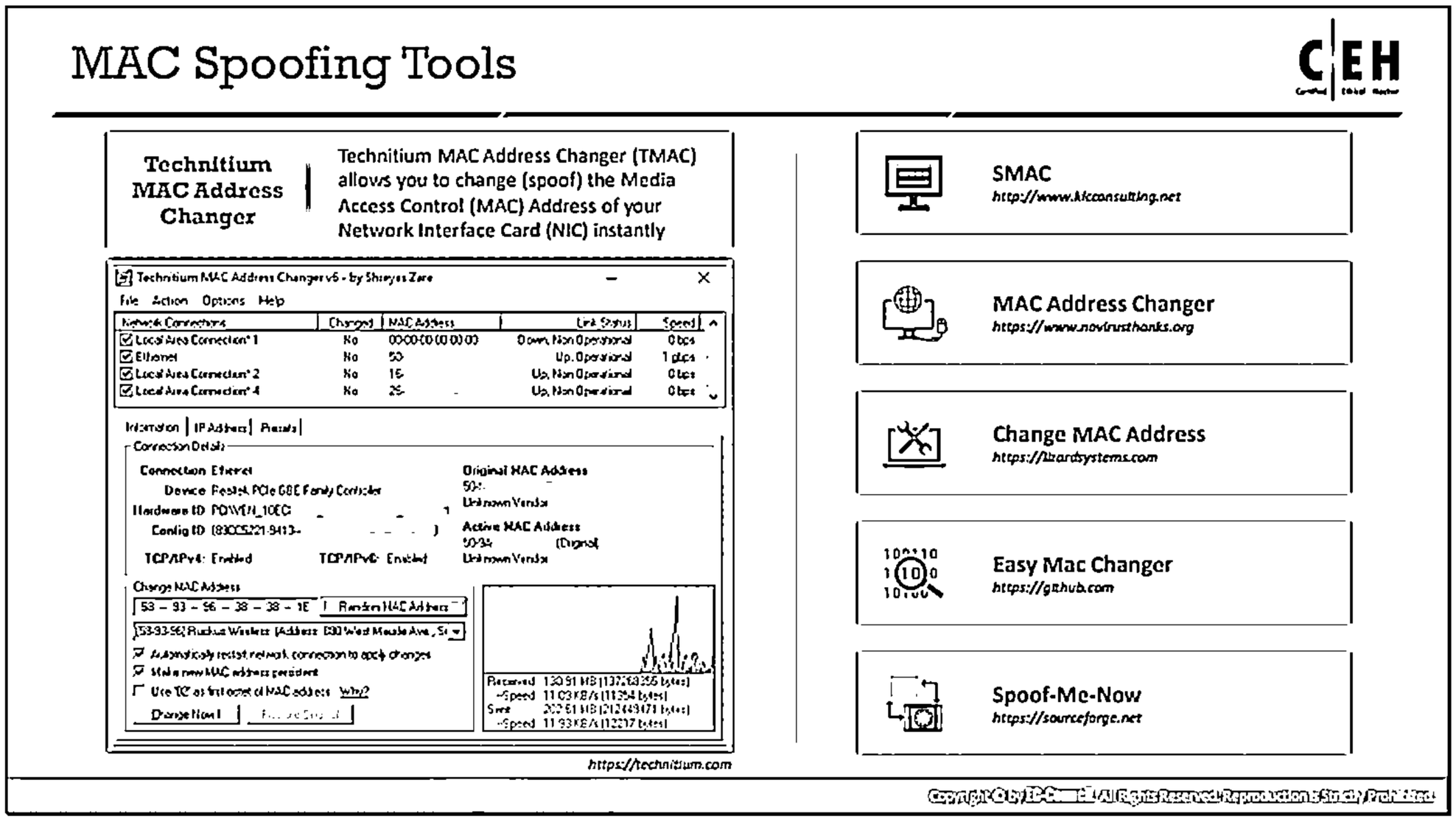


Figure 8.40: Registry Editor

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.

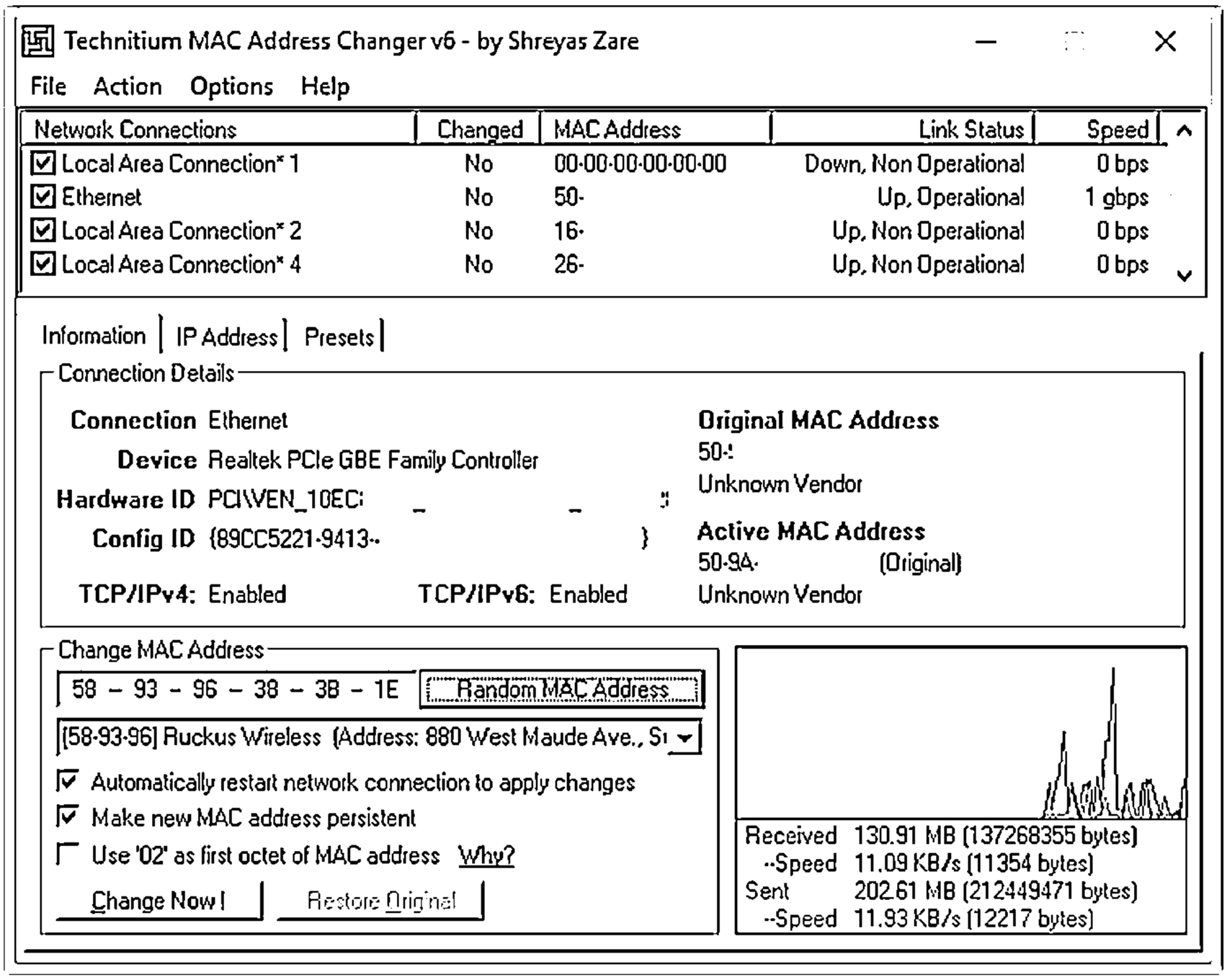


Figure 8.41: Screenshot of Technitium MAC Address Changer (TMAC)

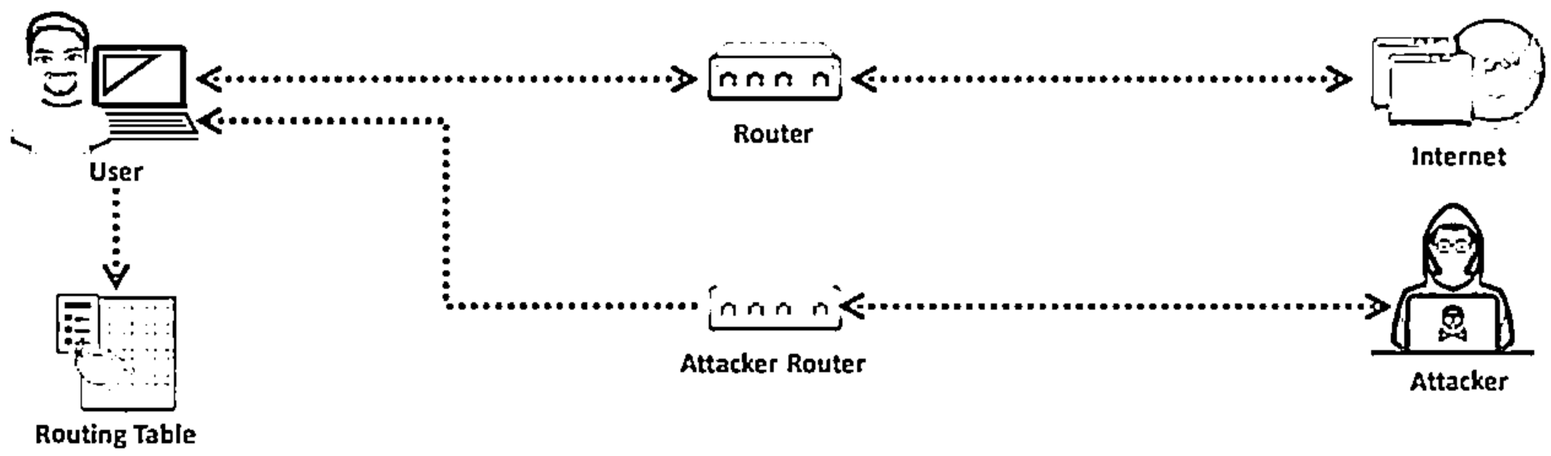
Some examples of MAC spoofing tools are listed below:

- SMAC (*http://www.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 their subnet by listening to router advertisement and soliciting messages on their network
- The attacker sends a spoofed IRDP router advertisement message to the host on the subnet, causing it to change its default router to whatever the attacker chooses
- This attack allows the attacker to sniff the traffic and collect valuable information from the packets
- Attackers can use IRDP spoofing to launch man-in-the-middle, denial-of-service, and passive sniffing attacks



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

IRDP Spoofing

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.

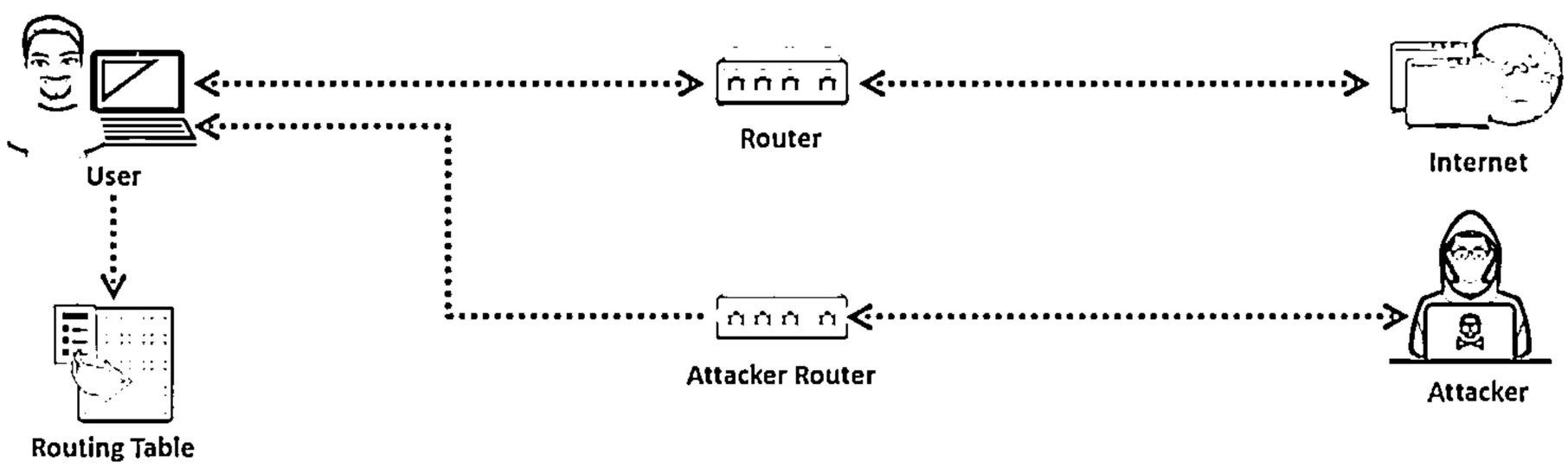


Figure 8.42: IRDP spoofing

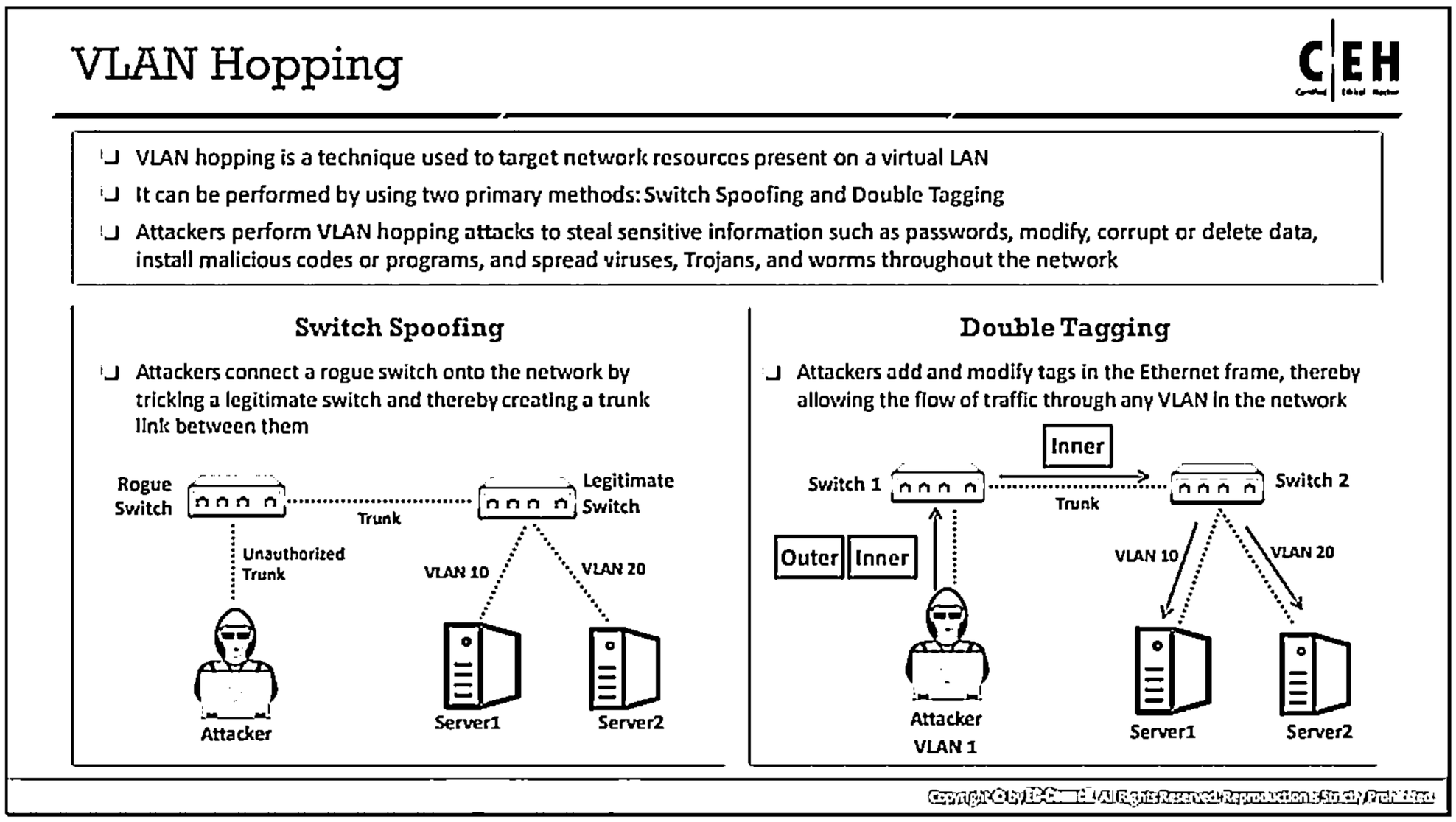
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

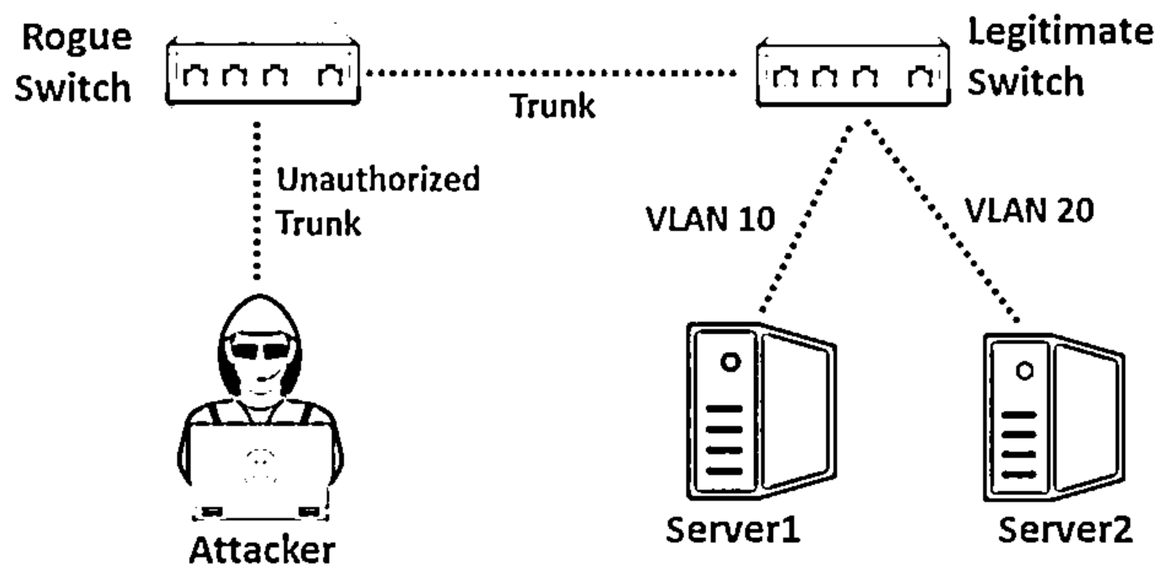


Figure 8.43: Illustration of switch spoofing

- **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.

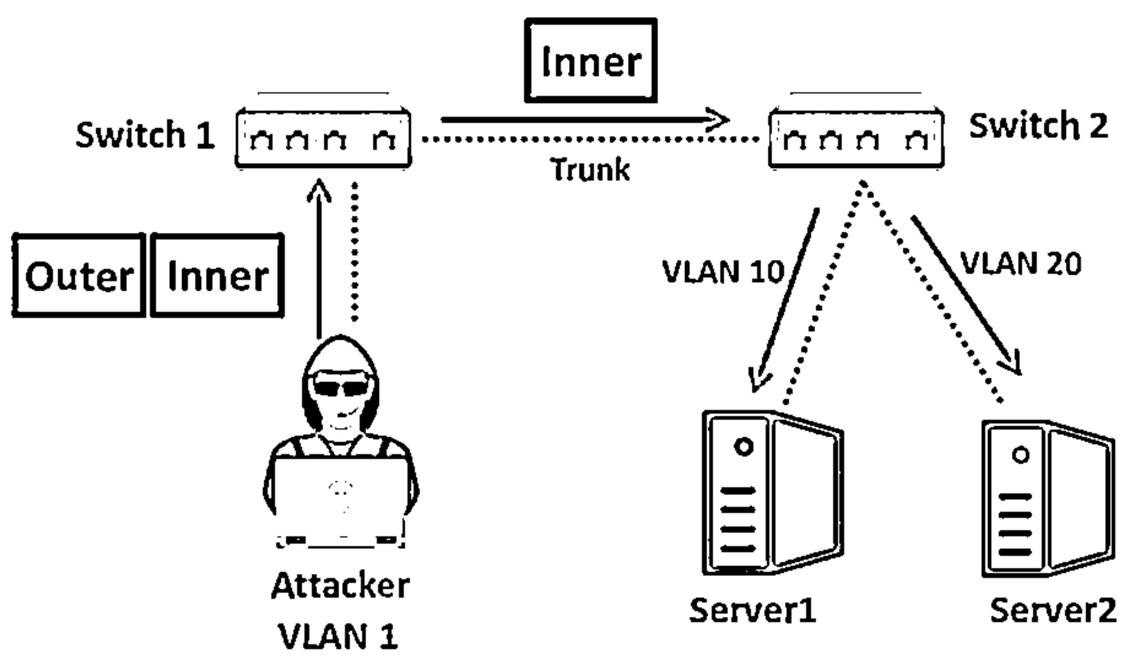
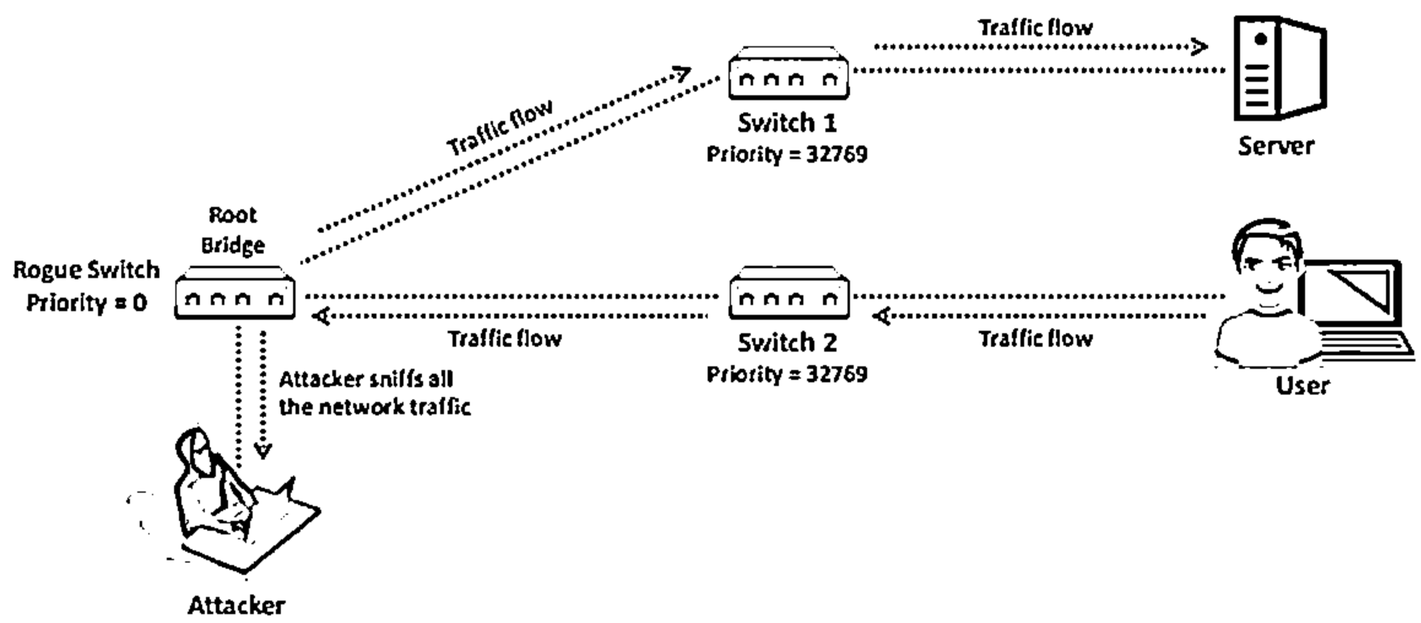


Figure 8.44: Illustration of double tagging

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

STP Attack

- Attackers connect a rogue switch into the network to change the operations of the STP protocol and sniff all the network traffic
- Attackers configure the rogue switch such that its priority is less than that of any other switch in the network, which makes it the root bridge, thus allowing the attackers to sniff all the traffic flowing in the network



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.

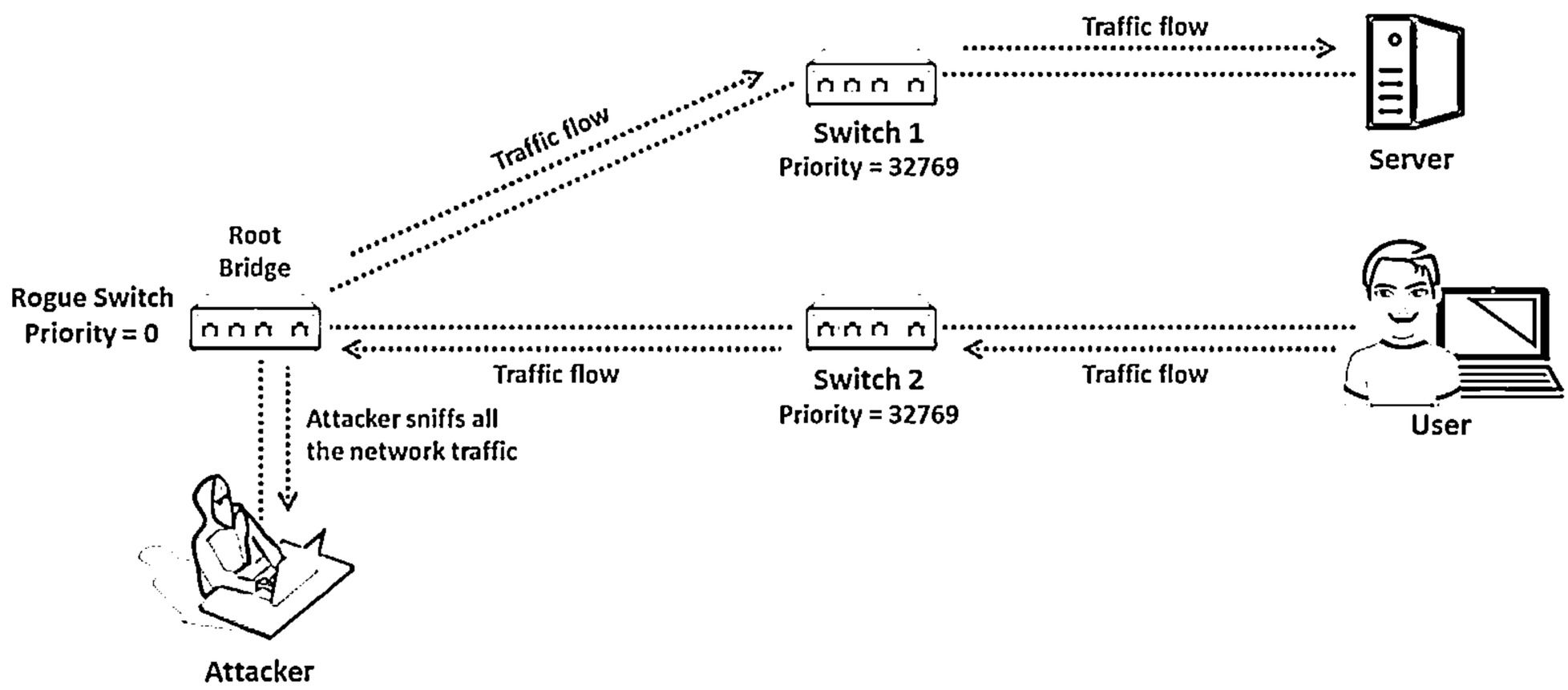
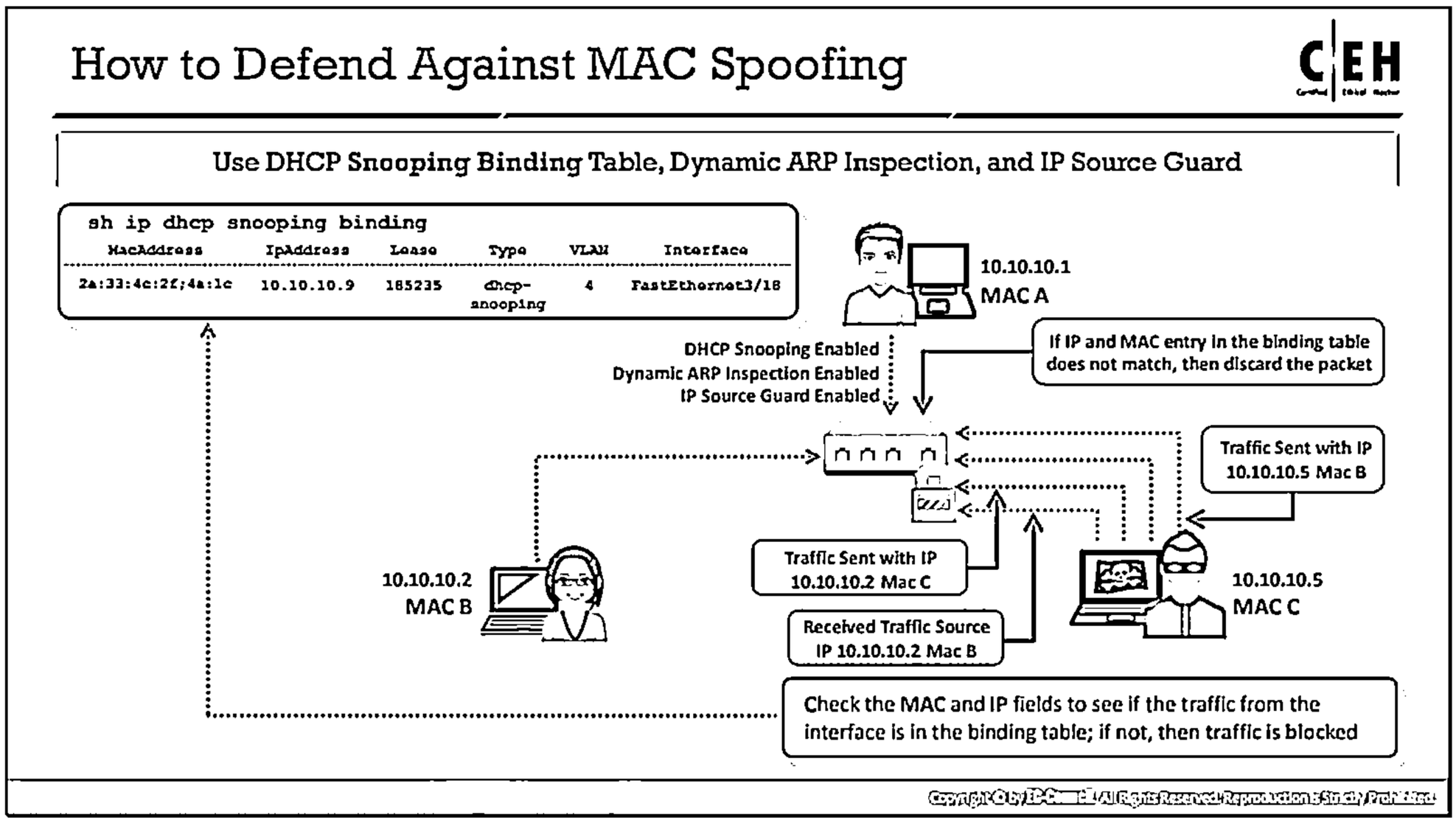


Figure 8.45: Illustration of an STP attack

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.

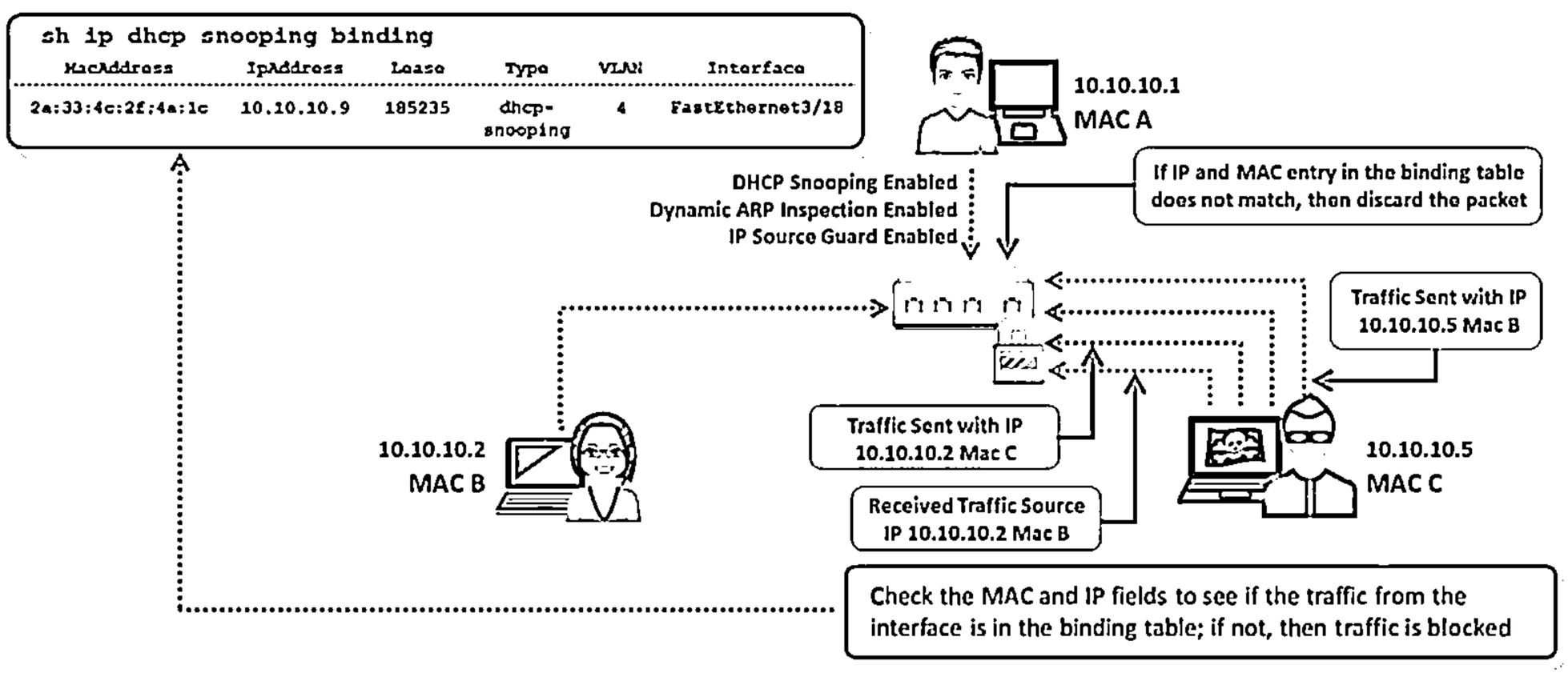


Figure 8.46: Defending against MAC spoofing

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

- 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:

```
Switch(config-if)# switchport mode
trunk

Switch(config-if)# switchport mode
nonegotiate
```

Defend against Double Tagging

- 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
```

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

To prevent an STP attack, the following security features must be implemented:

BPDU Guard

- To enable the BPDU guard on all PortFast edge ports:

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

Loop Guard

- To enable the loop guard on an interface:

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

Root Guard

- To enable the root guard feature on an interface:

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

UDLD (Unidirectional Link Detection)

- To enable UDLD on an interface:

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

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.

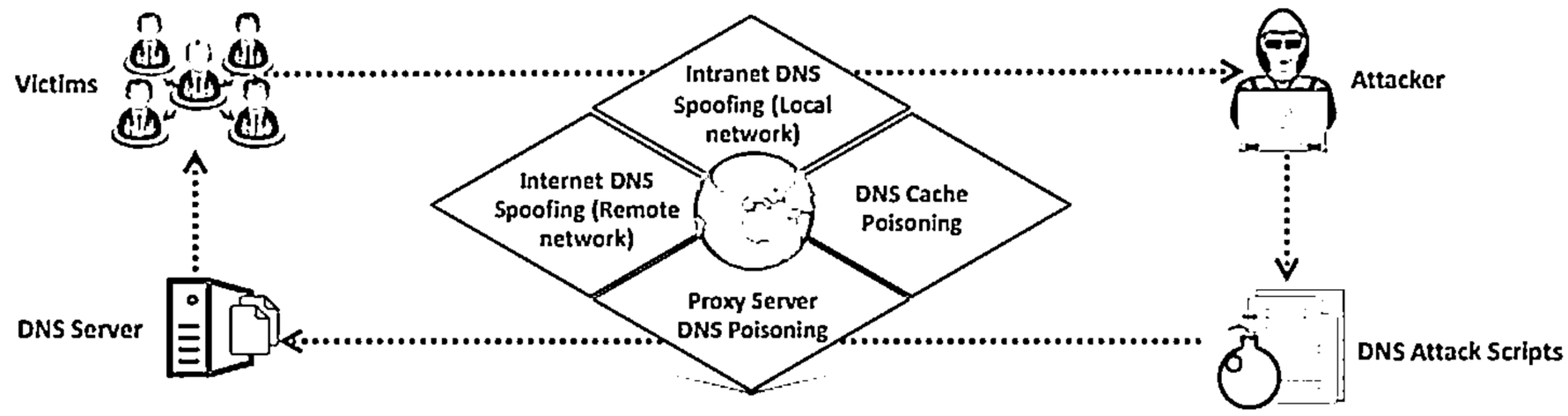
  Use the following command to enable UDLD on a switch interface:

```
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.

DNS Poisoning Techniques

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



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.

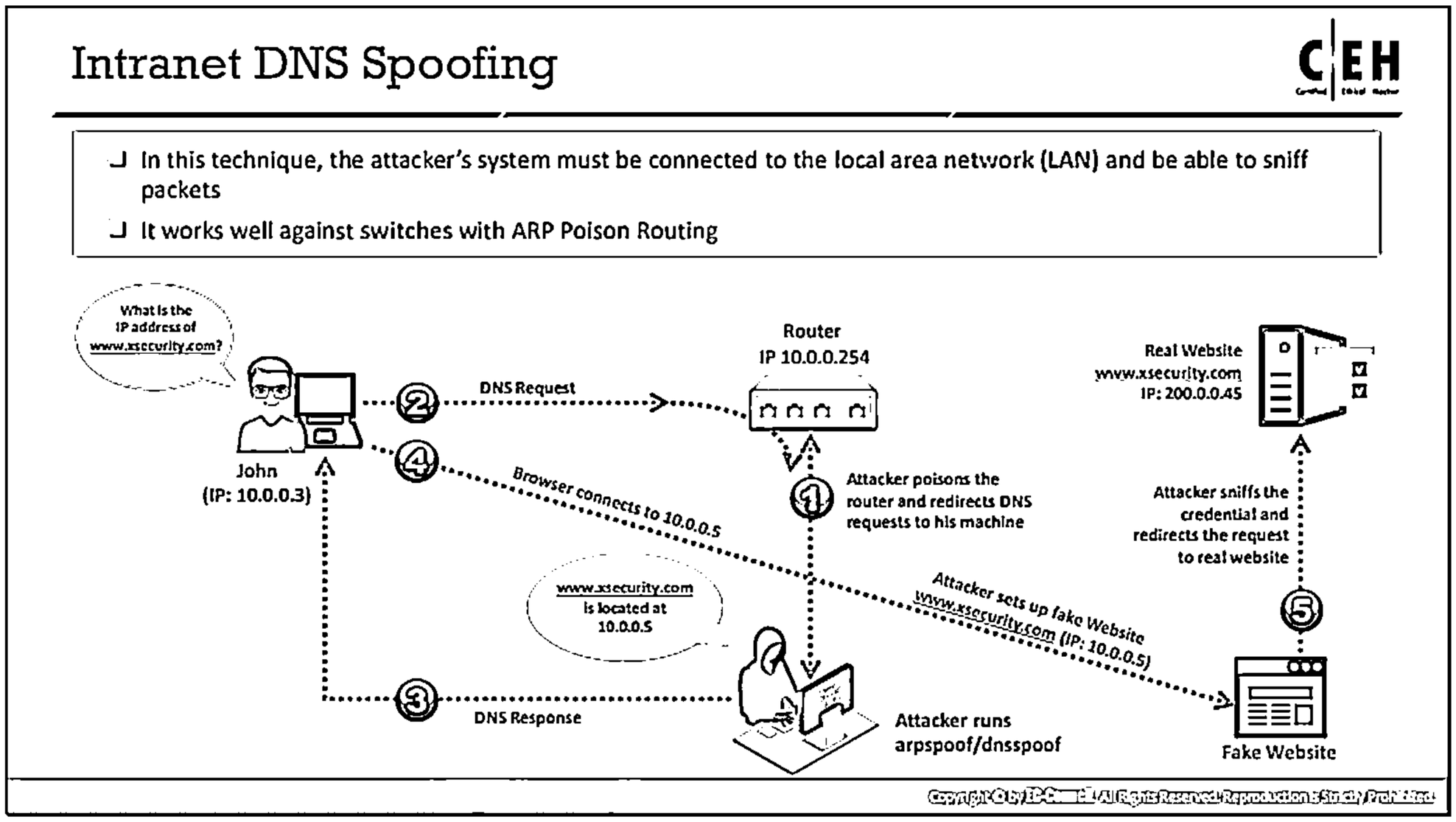
When the victim tries to access a website, the attacker manipulates the entries in the DNS table so that the victim's system redirects the URL to the attacker's server. The attacker replaces IP address entries for a target site on a given DNS server with the IP address of the server (malicious server) 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.

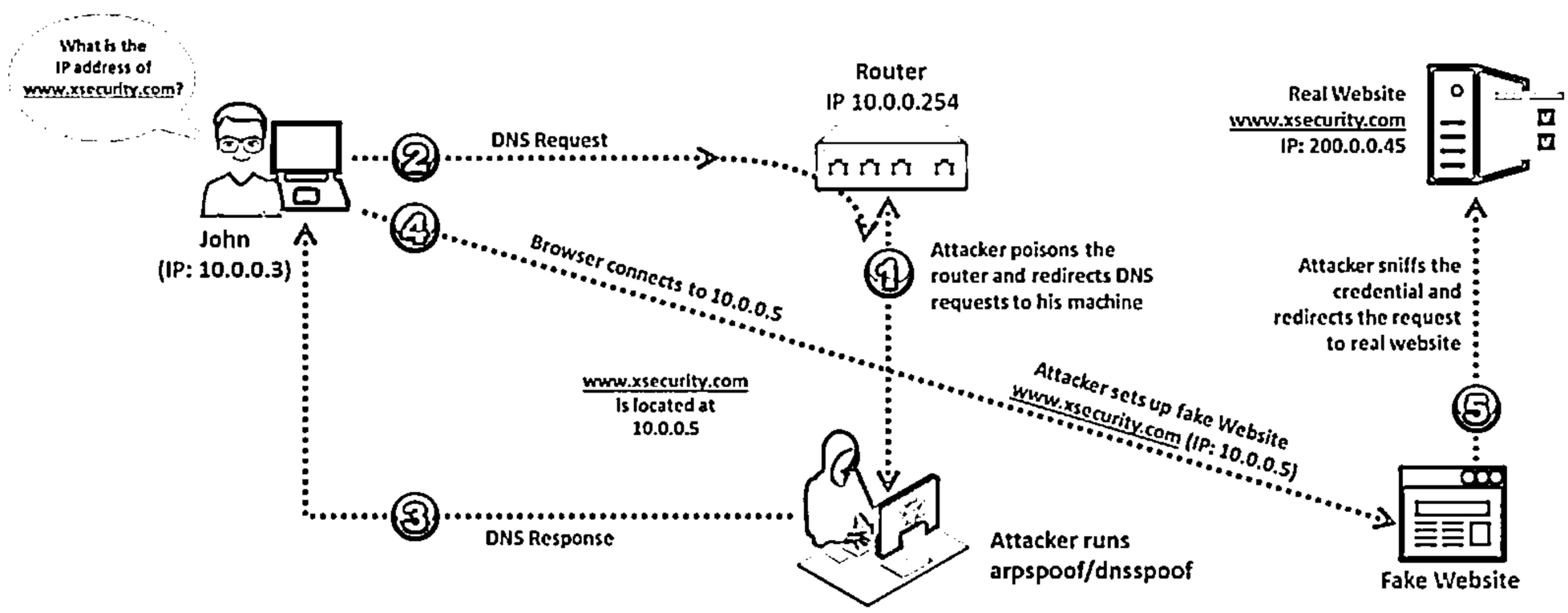


Figure 8.47: Intranet DNS spoofing

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

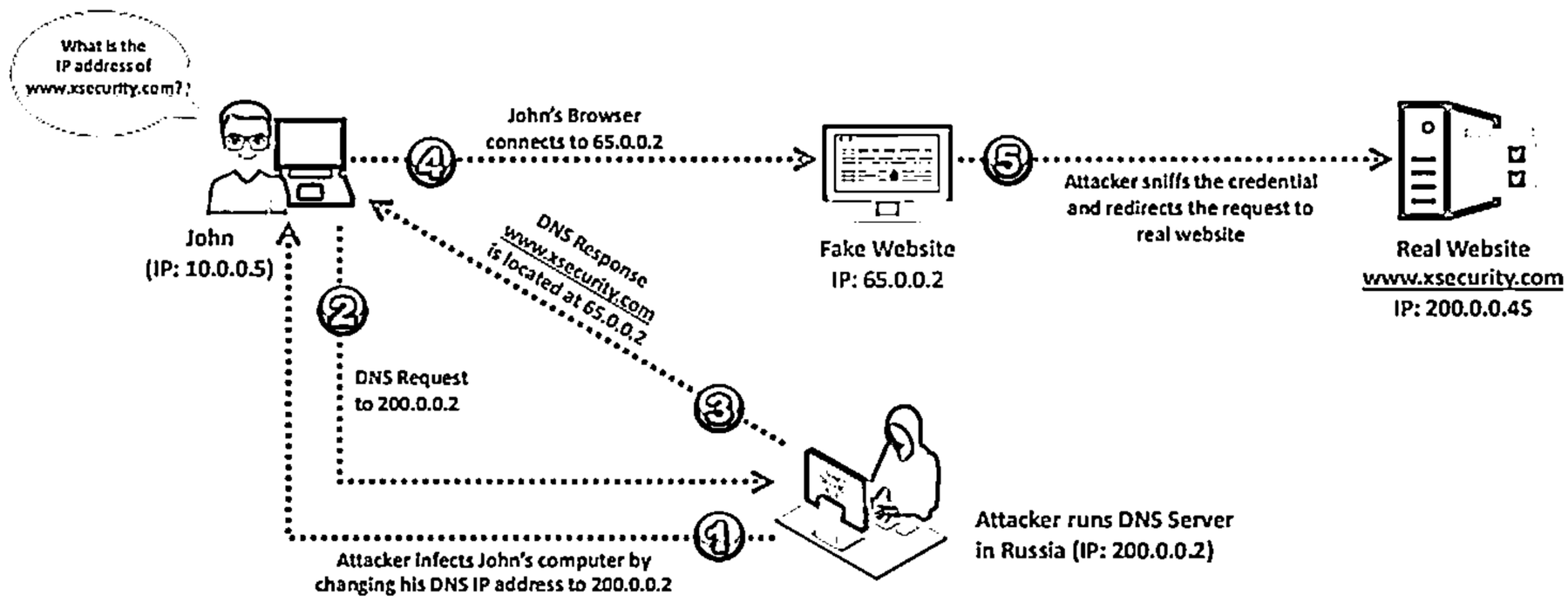
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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 Spoofing, the attacker infects John's machine with a Trojan and changes his DNS IP address to that of the attacker's



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.

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

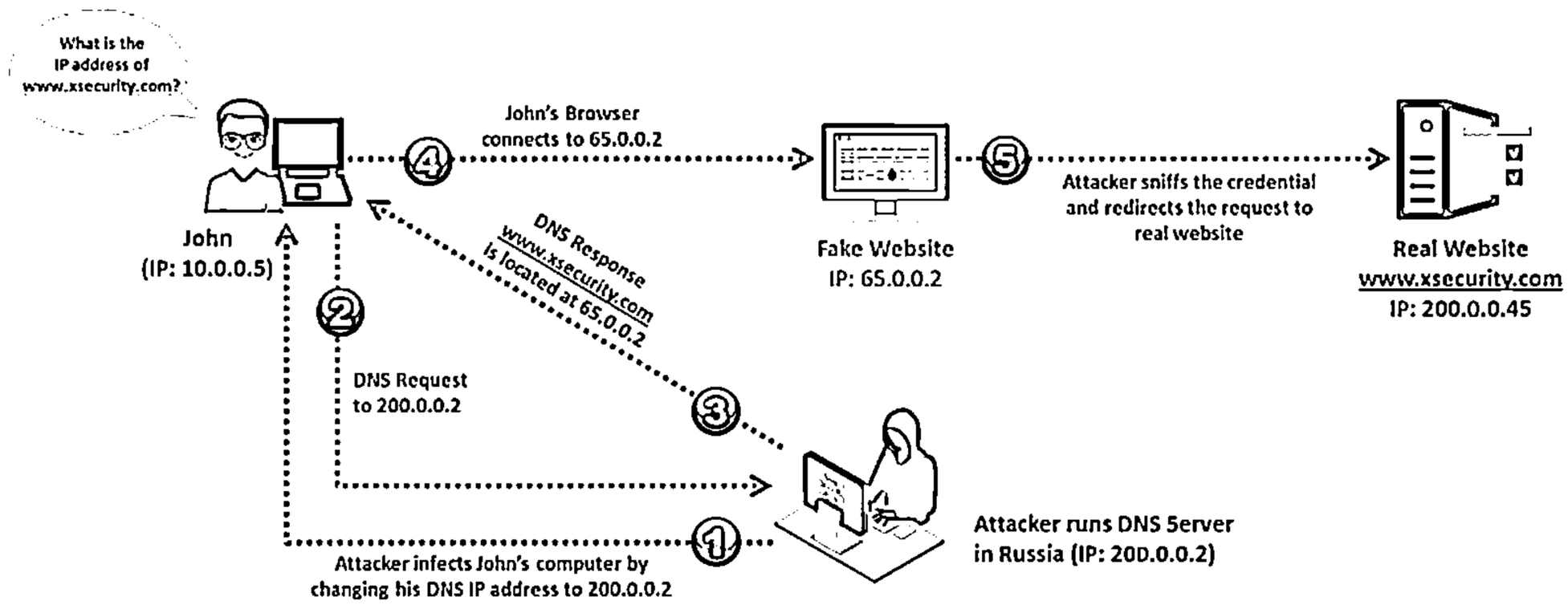
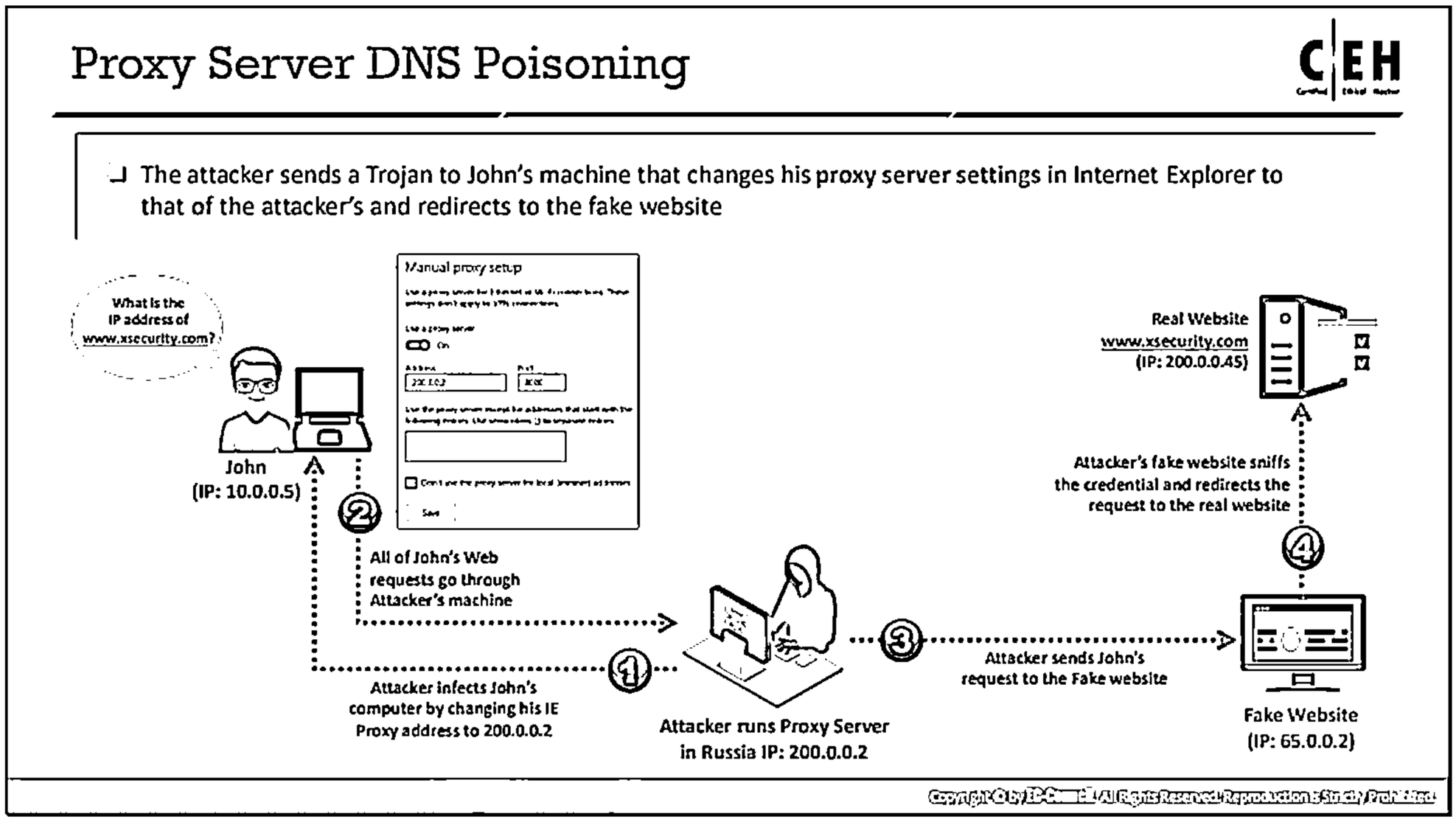


Figure 8.48: Internet DNS Spoofing

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.

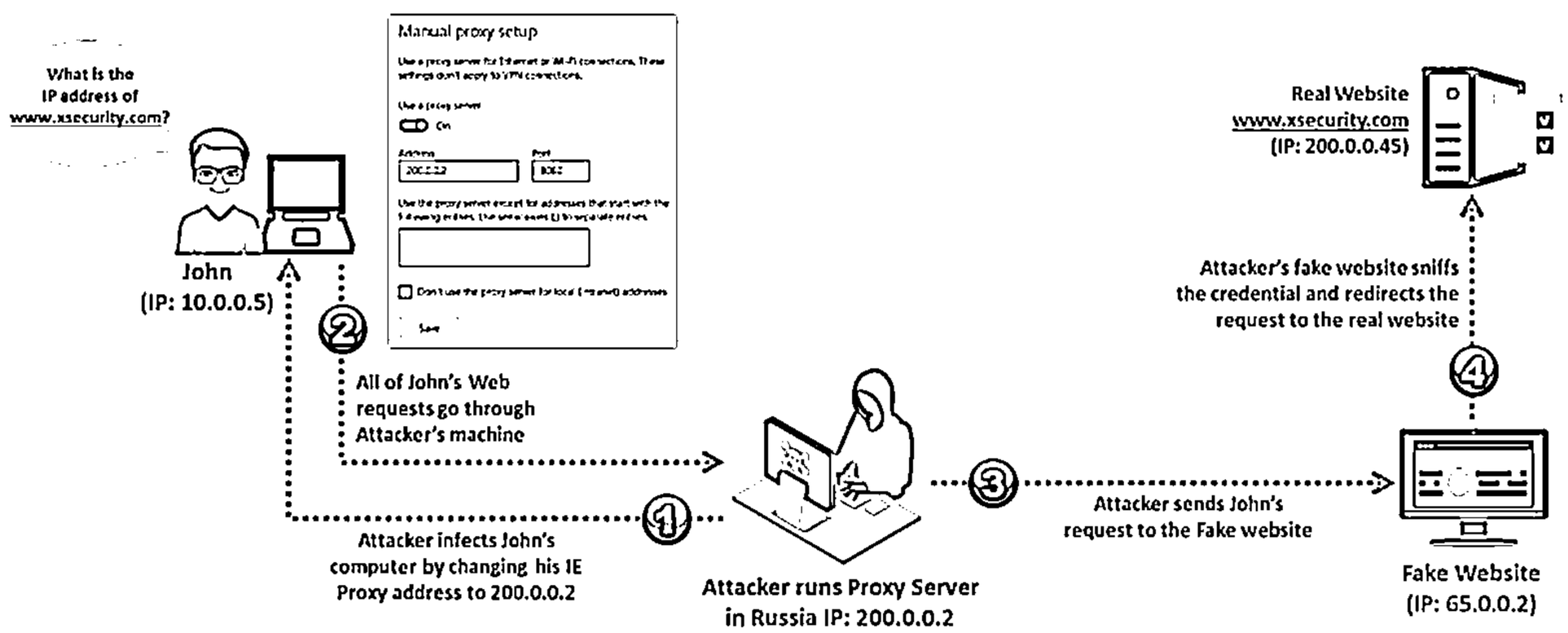
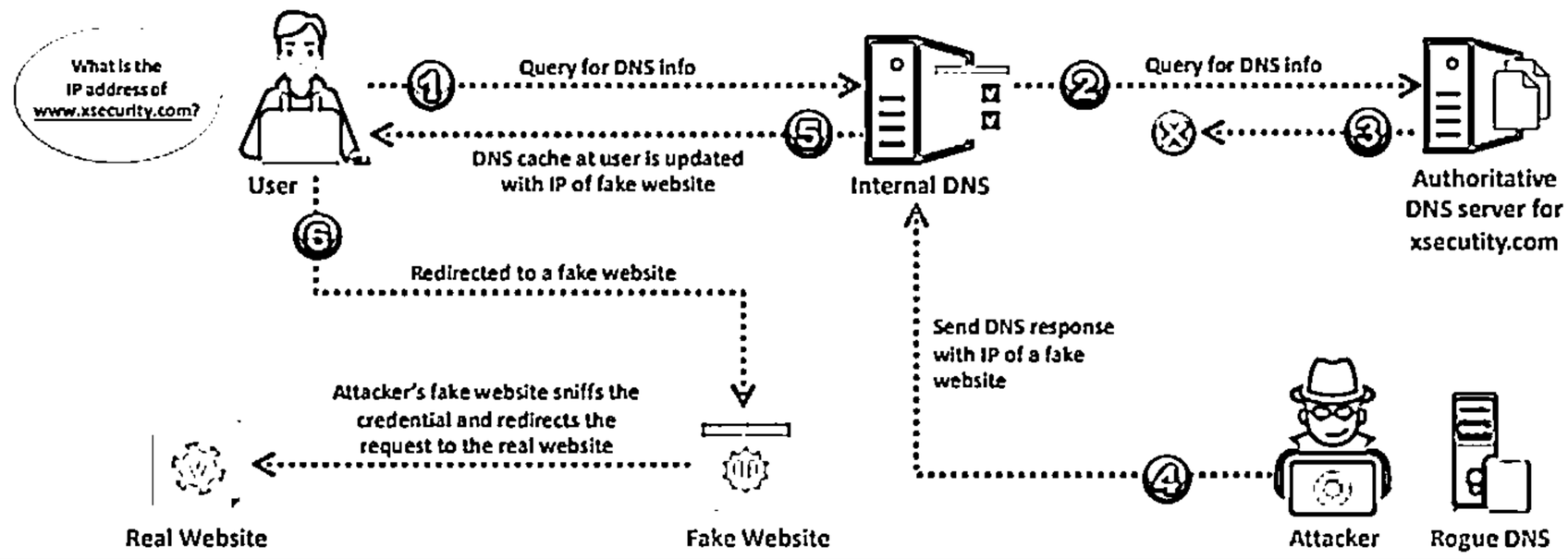


Figure 8.49: Proxy server DNS poisoning

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 into the DNS resolver cache so that a DNS query is redirected to a malicious site
- If the DNS resolver cannot validate that the DNS responses have been received from an authoritative source, it will cache the incorrect entries locally, and serve them to users who make a similar request



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.

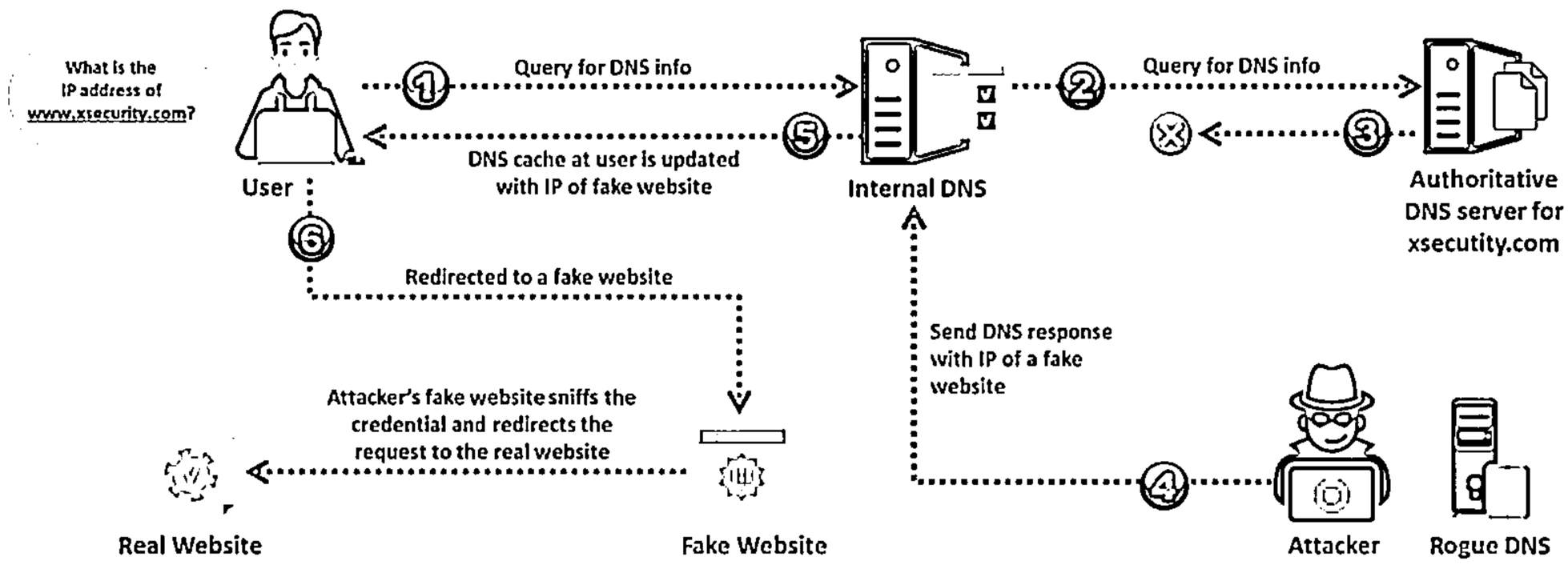


Figure 8.50: DNS cache poisoning

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

DNS Poisoning Tools

DerpNSpoof | 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

DerpNSpoof
Coded by Adrián Fernández Arnal-(@adrianfa5)
[i] Options to use:
<ip> - Spoof the DNS query packets of a certain IP address
<all> - Spoof the DNS query packets of all hosts
[i] Examples:
python3 DerpNSpoof.py 192.168.1.20 myfile.txt
python3 DerpNSpoof.py all myfile.txt
[i] Spoofing DNS responses...
[#] Spoofed response sent to [192.168.1.174]: Redirecting [redacted] to [1.2.3.4]
[#] Spoofed response sent to [192.168.1.174]: Redirecting [redacted] to [1.2.3.4]
[#] Spoofed response sent to [192.168.1.174]: Redirecting [redacted] to [1.2.3.4]
[#] Spoofed response sent to [192.168.1.174]: Redirecting [redacted] to [1.2.3.4]
[#] Spoofed response sent to [192.168.1.174]: Redirecting [redacted] to [1.2.3.4]
[#] Spoofed response sent to [192.168.1.174]: Redirecting [redacted] to [1.2.3.4]
https://github.com

DNS Spoof
https://github.com

DNS-poison
https://github.com

Ettercap
http://www.ettercap-project.org

Evilgrade
https://github.com

TORNADO
https://github.com

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.

```
DerpNSpoof
Coded by Adrián Fernández Arnal-(@adrianfa5)

[!] Options to use:
      <ip>  - Spoof the DNS query packets of a certain IP address
      <all> - Spoof the DNS query packets of all hosts
[!] Examples:
      # python3 DerpNSpoof.py 192.168.1.20 myfile.txt
      # python3 DerpNSpoof.py all myfile.txt

[i] Spoofing DNS responses...
[#] Spoofed response sent to [1.1.1.1] Redirecting [www.pickomini.com] to [1.2.3.4]
[#] Spoofed response sent to [1.1.1.1] Redirecting [www.pickomini.com] to [1.2.3.4]
[#] Spoofed response sent to [1.1.1.1] Redirecting [www.pickomini.com] to [1.2.3.4]
[#] Spoofed response sent to [1.1.1.1] Redirecting [www.pickomini.com] to [1.2.3.4]
[#] Spoofed response sent to [1.1.1.1] Redirecting [www.pickomini.com] to [1.2.3.4]
[#] Spoofed response sent to [1.1.1.1] Redirecting [www.pickomini.com] to [1.2.3.4]
```

Figure 8.51: 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 (*http://www.ettercap-project.org*)
- Evilgrade (*https://github.com*)
- TORNADO (*https://github.com*)

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

How to Defend Against DNS Spoofing

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

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

How to Defend Against DNS Spoofing

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

Countermeasures that help prevent DNS spoofing attacks:

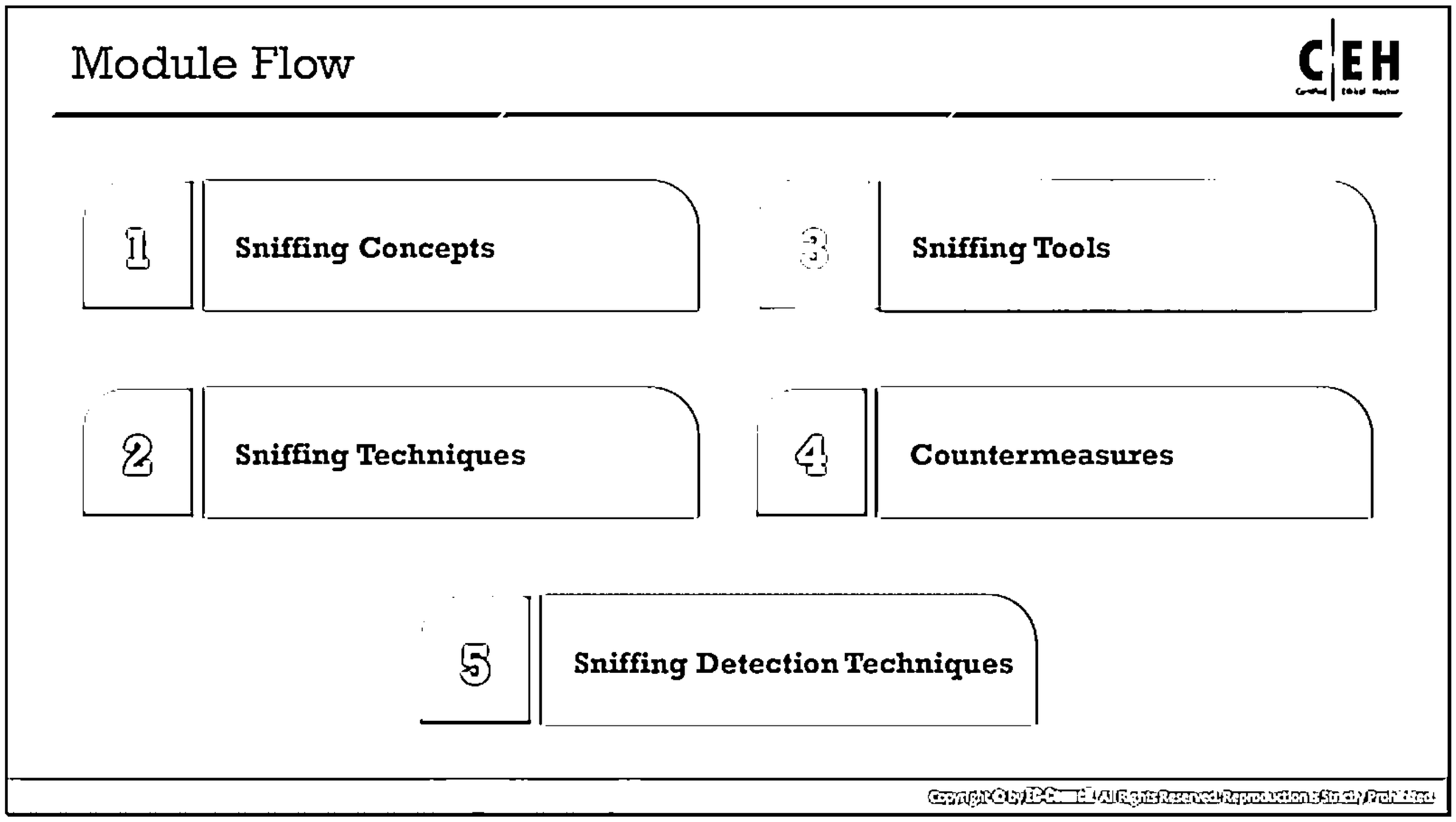
- Implement Domain Name System Security Extension (DNSSEC)
- Use Secure Socket Layer (SSL) for securing the traffic
- Resolve all DNS queries to a local DNS server
- Block DNS requests being sent to external servers
- Configure a firewall to restrict external DNS lookup
- Implement an intrusion detection 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, either full or partial, to authorized users
- Use DNS non-existent domain (NXDOMAIN) rate limiting
- Secure your internal machines
- Use static ARP and IP tables
- Use SSH encryption

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

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

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

Module Flow



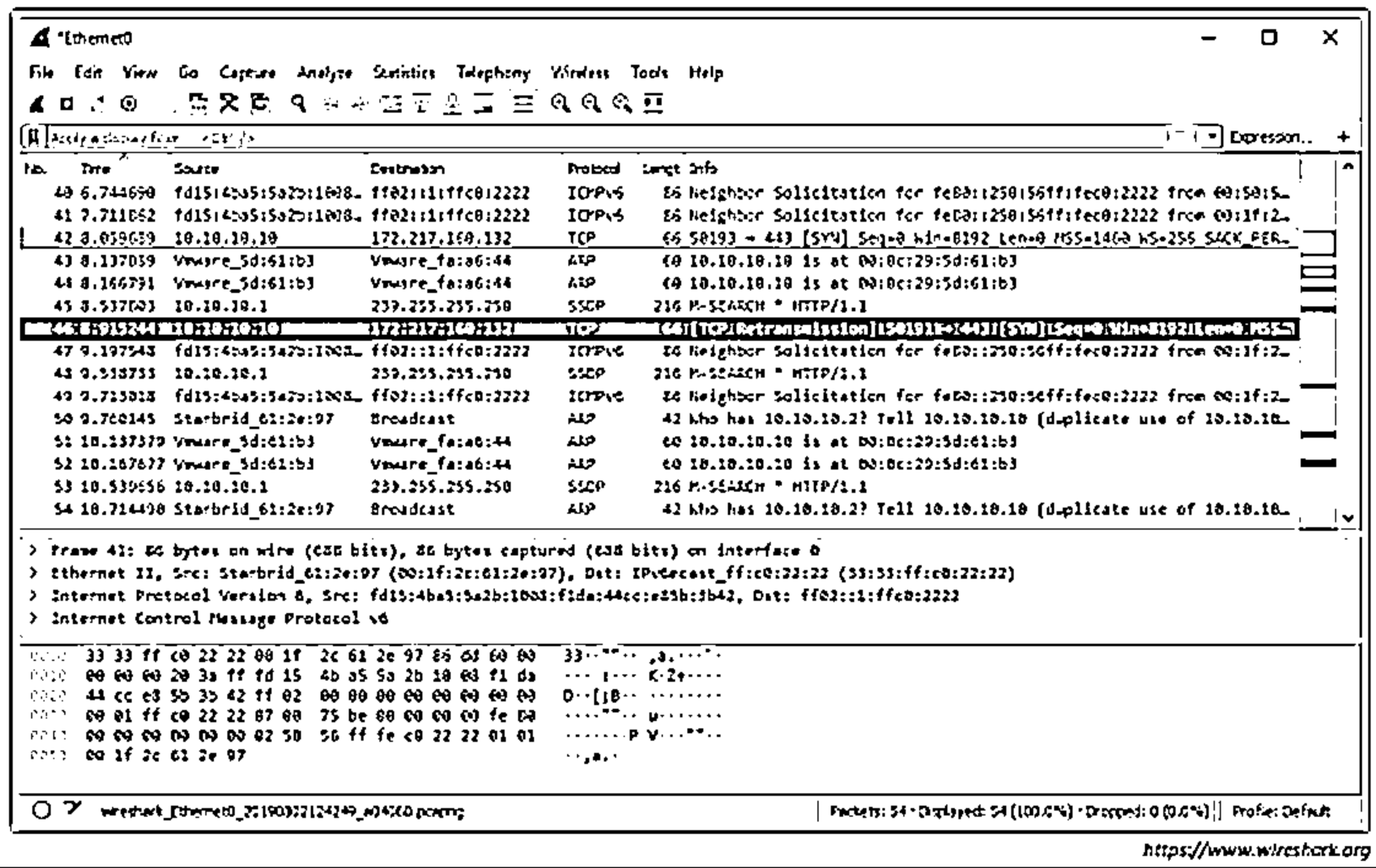
Sniffing Tools

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



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.

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

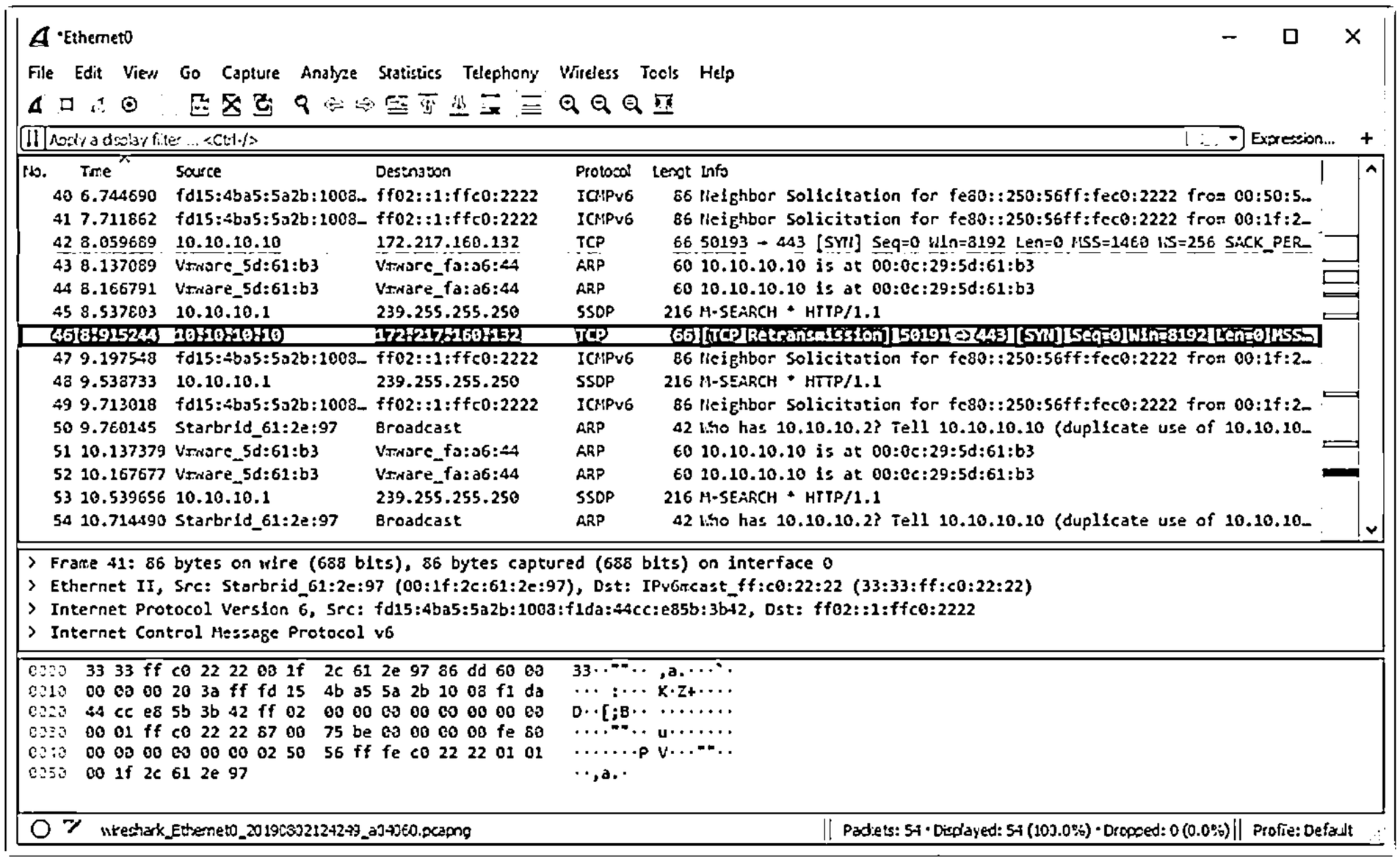
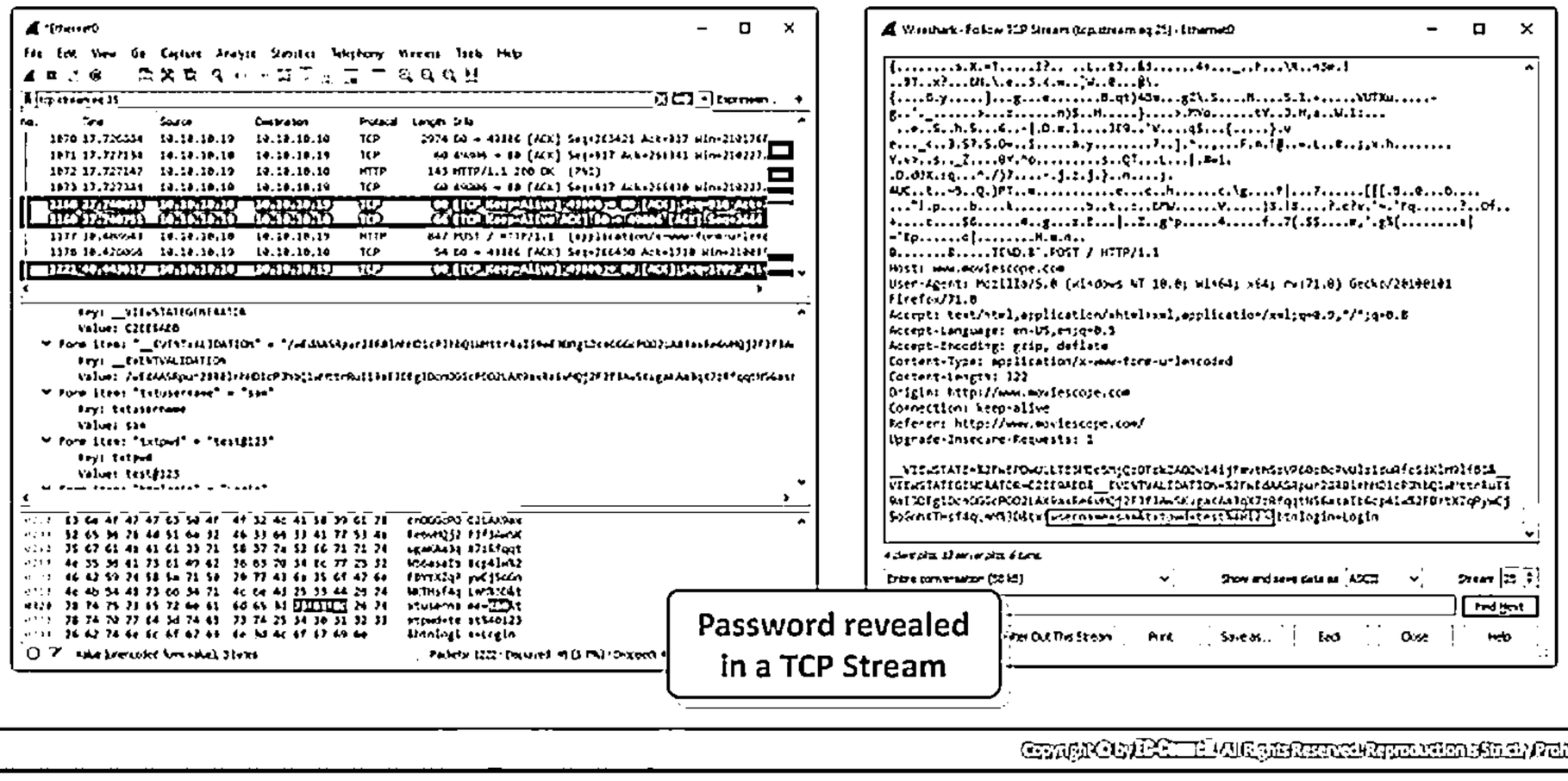


Figure 8.52: Capturing packets using Wireshark

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

Follow TCP Stream in Wireshark



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 **Tools** 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.

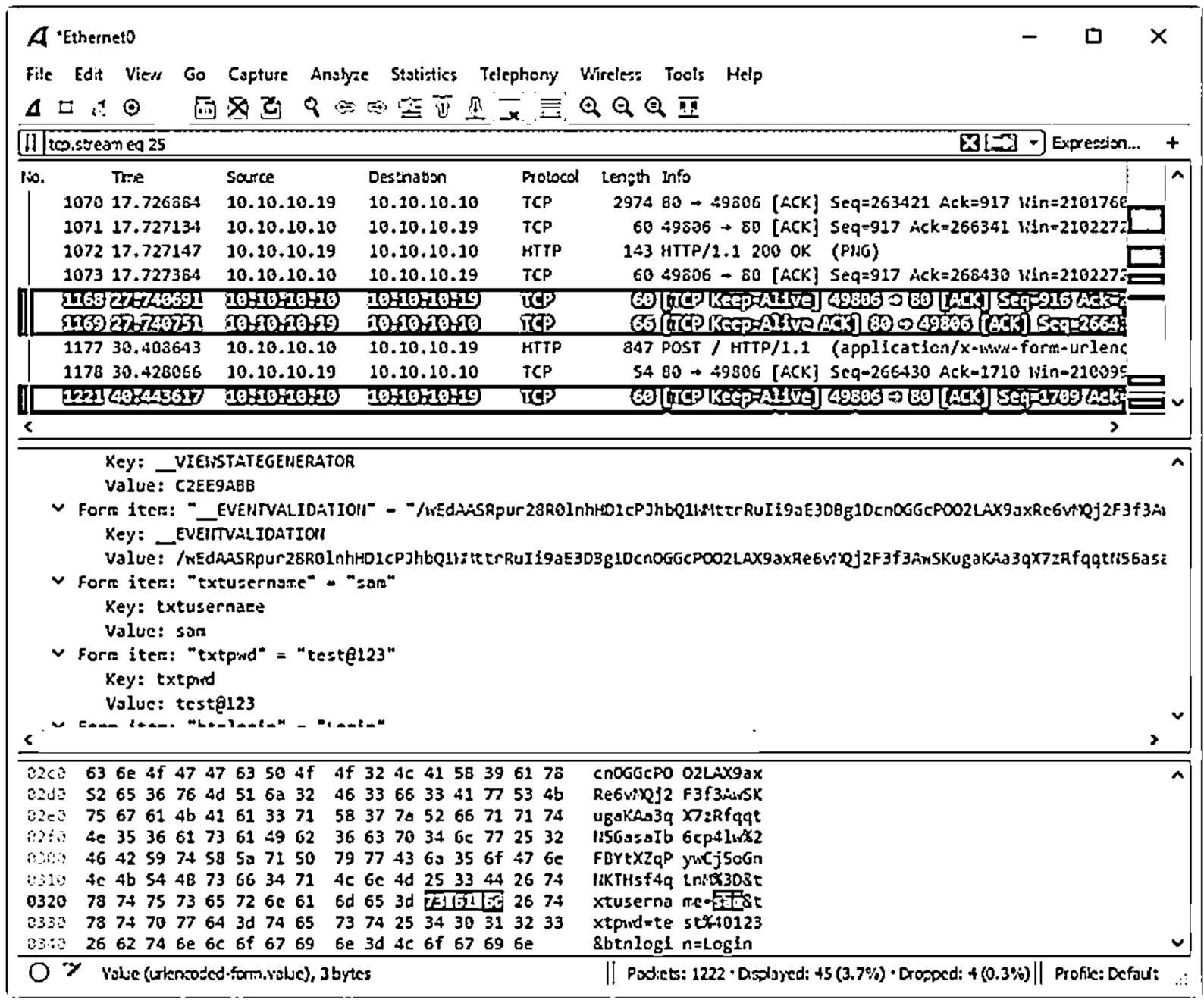


Figure 8.53: Wireshark capturing TCP Stream

Figure 8.54: Wireshark feature Follow TCP Stream

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

Display Filters in Wireshark

Display filters are used to change the view of packets in the captured files

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

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

Display Filters in Wireshark

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

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

1. `tcp.flags.reset==1`
   Displays all TCP resets
2. `udp contains 33:27:58`
   Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset
3. `http.request`
   Displays all HTTP GET requests
4. `tcp.analysis. Retransmission`
   Displays all retransmissions in the trace
5. `tcp contains traffic`
   Displays all TCP packets that contain the word "traffic"
6. `!(arp or icmp or dns)`
   Masks out arp, icmp, dns, or other protocols and allows you to view traffic of your interest
7. `tcp.port == 4000`
   Sets a filter for any TCP packet with 4000 as a source or destination port
8. `tcp.port eq 25 or icmp`
   Displays only SMTP (port 25) and ICMP traffic
9. `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
10. `ip.src != xxx.xxx.xxx.xxx && ip.dst != xxx.xxx.xxx.xxx && sip`
    Filter by a protocol (e.g. SIP) and filter out unwanted IPs

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`

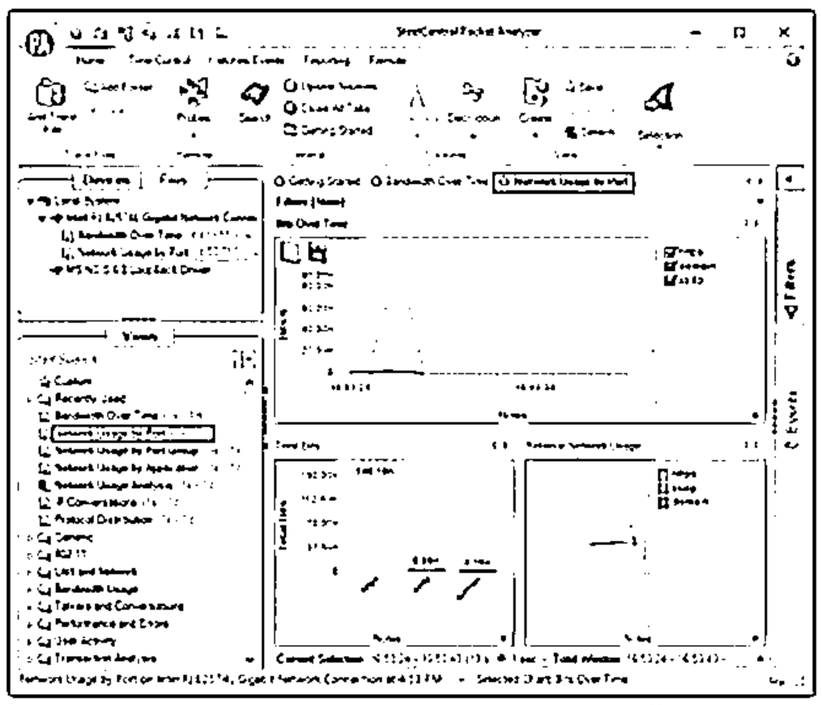
  Filters by a protocol (e.g., SIP) and filters out unwanted IPs

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

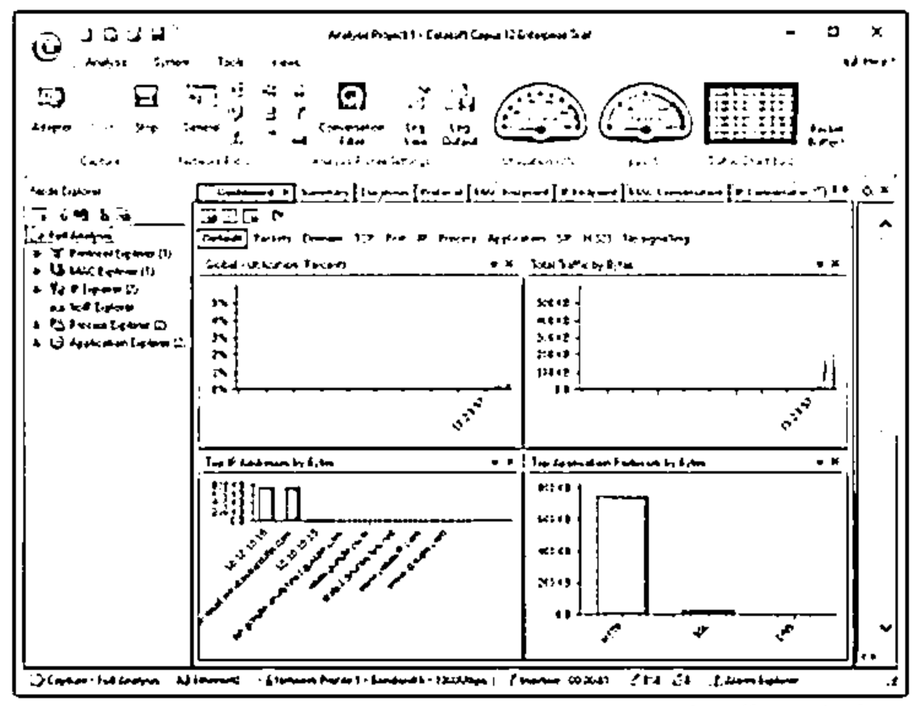
Sniffing Tools

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

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



https://www.riverbed.com



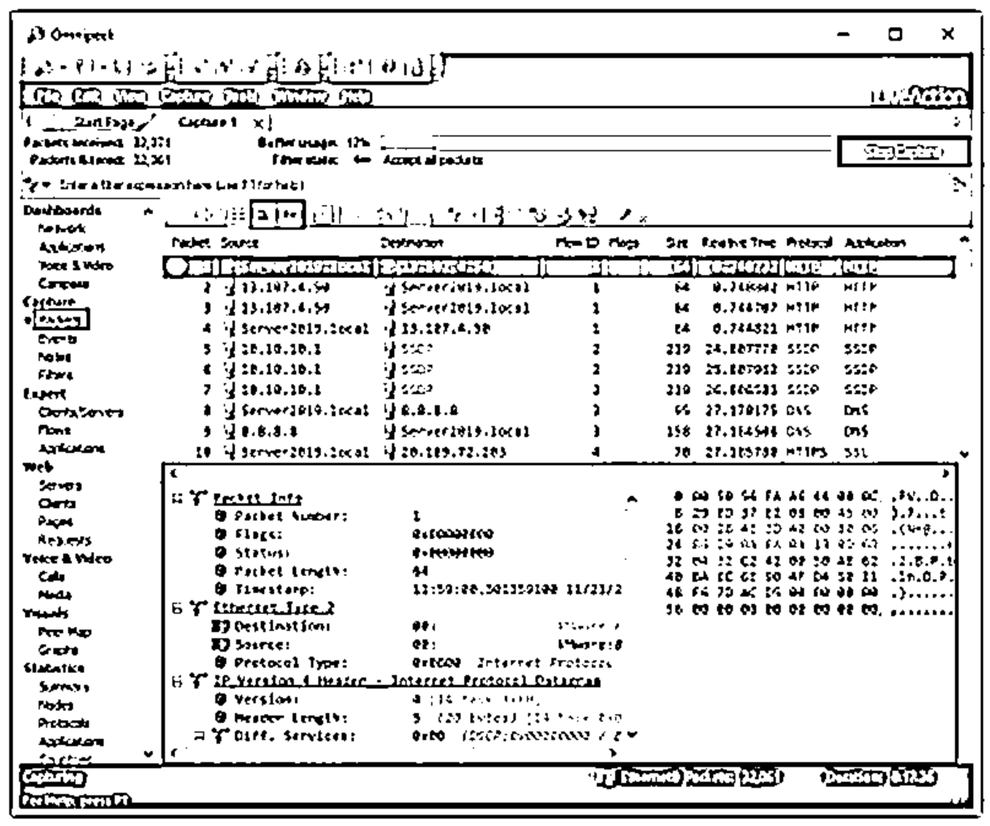
https://www.colasoft.com

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

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

Colasoft Packet Builder
https://www.colasoft.com

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

Sniffing Tools

- **SteelCentral Packet Analyzer**

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

  SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. This tool comes integrated with Riverbed AirPcap adapters to analyze and troubleshoot 802.11 wireless networks.

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

As it captures terabytes of packet data traversing the network, this tool reads that traffic and displays it in a graphical user interface (GUI). It can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (physical, virtual, or embedded on SteelHeads) without a large file transfer, to identify anomalous network issues or diagnose and troubleshoot complex network and application performance issues down to the bit level.

Attackers can use SteelCentral Packet Analyzer to capture and monitor long-duration network traffic as well as to analyze different types of data on the network.

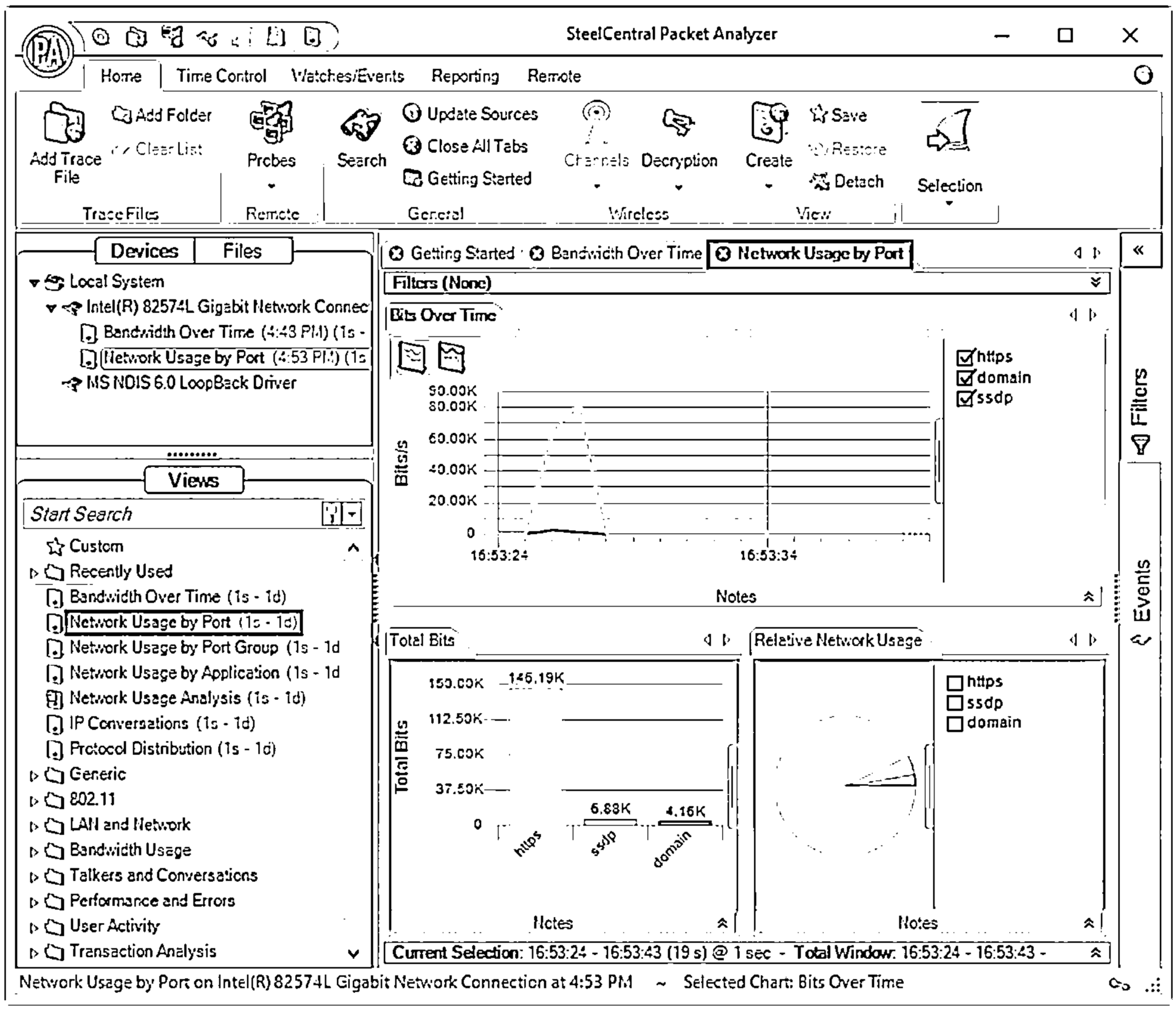


Figure 8.55: Screenshot of SteelCentral Packet Analyzer

- **Capsa Network Analyzer**

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

  Capsa Network Analyzer is a network-monitoring tool that captures all the data transmitted over the network and provides a wide range of analysis statistics in an intuitive and graphic way. The tool helps to analyze and troubleshoot the problem that

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

has occurred (if any) in the network. It is also able to perform reliable network forensics, advanced protocol analyzing, in-depth packet decoding, and automatic expert diagnosis. It helps you to detect network vulnerabilities.

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

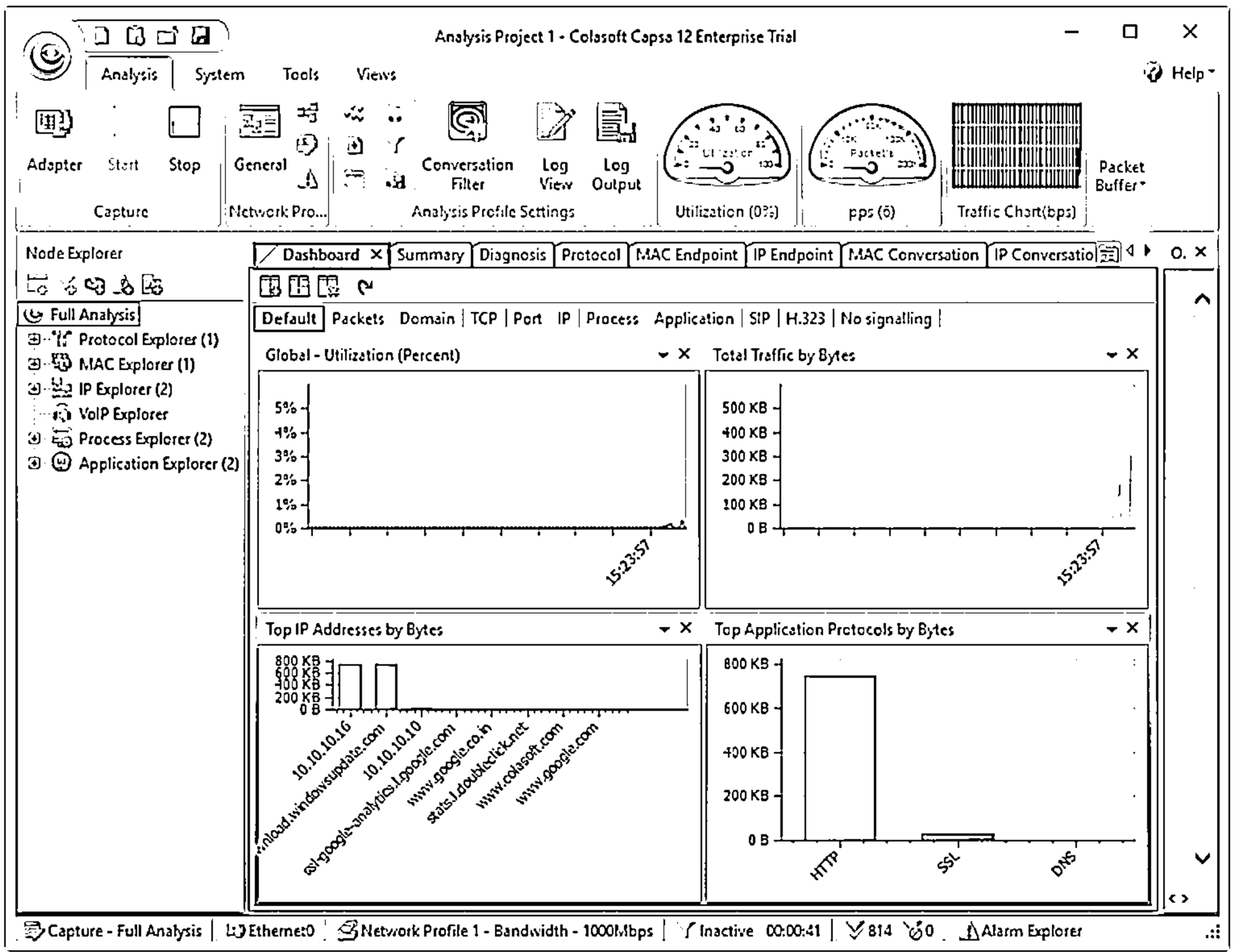


Figure 8.56: Screenshot of Capsa Network Analyzer

- **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.

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

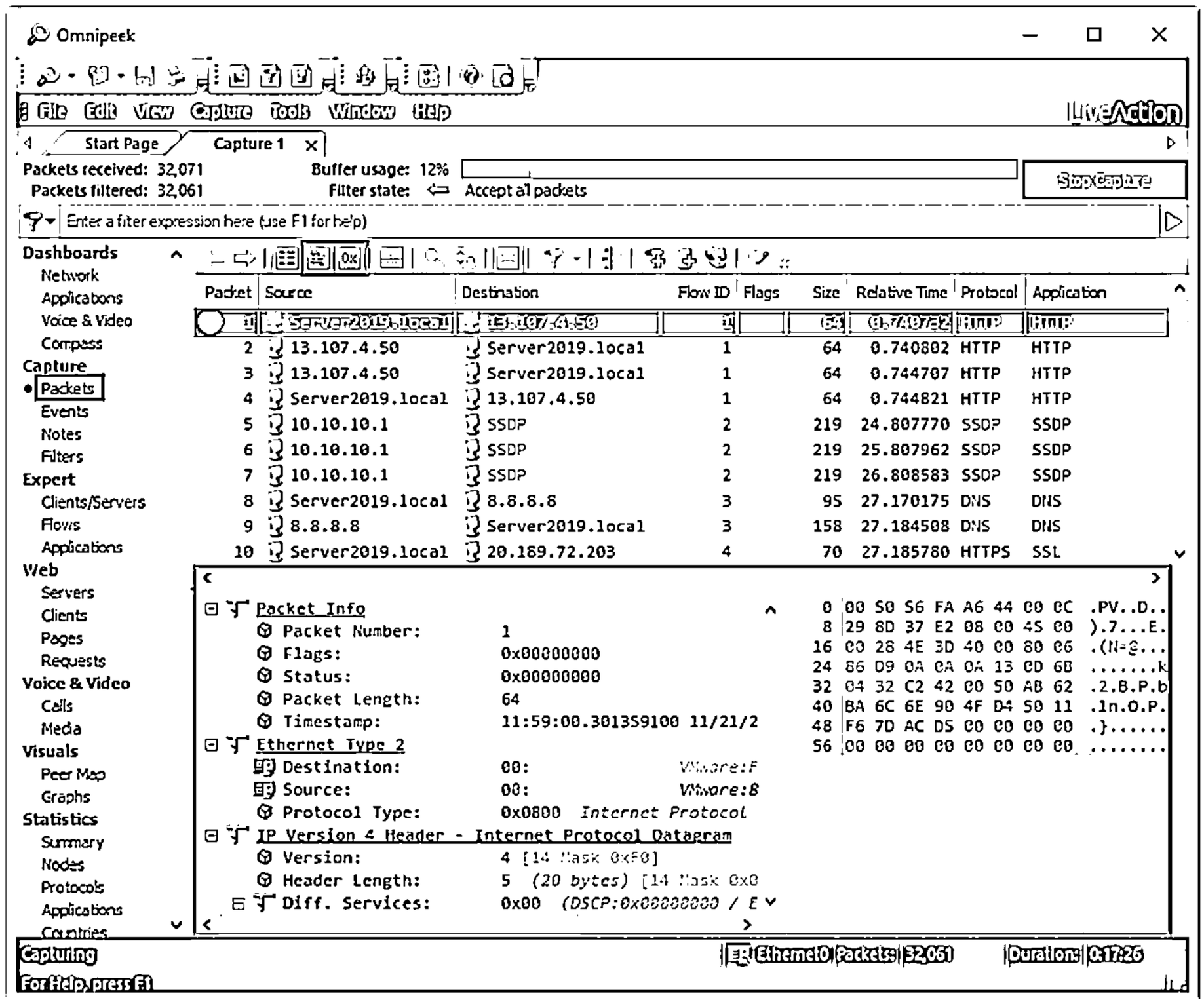
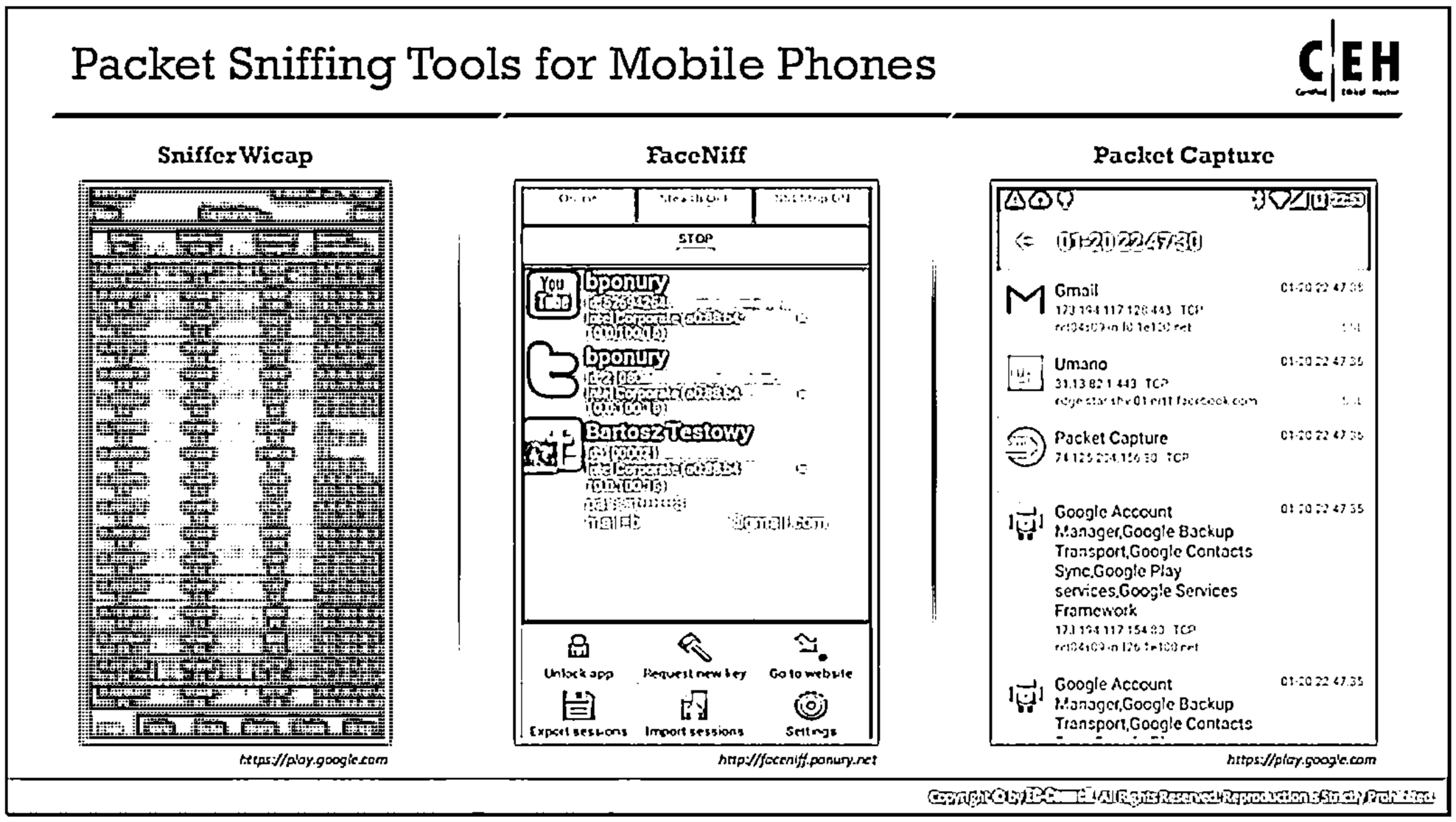


Figure 8.57: Screenshot of OmniPeek

Some examples of additional sniffing tools are listed below:

- 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*)
- Colasoft Packet Builder (*https://www.colasoft.com*)

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.

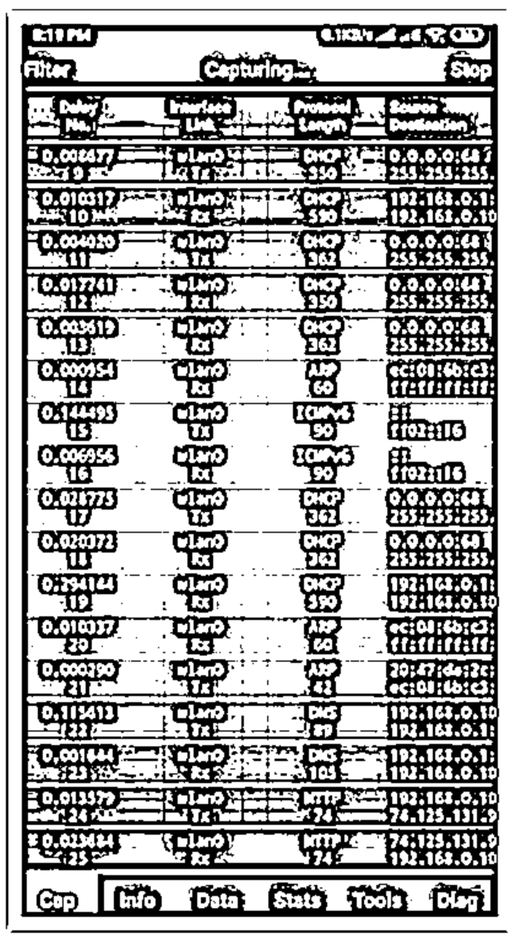


Figure 8.58: Screenshot of Sniffer Wicap

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

- **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.

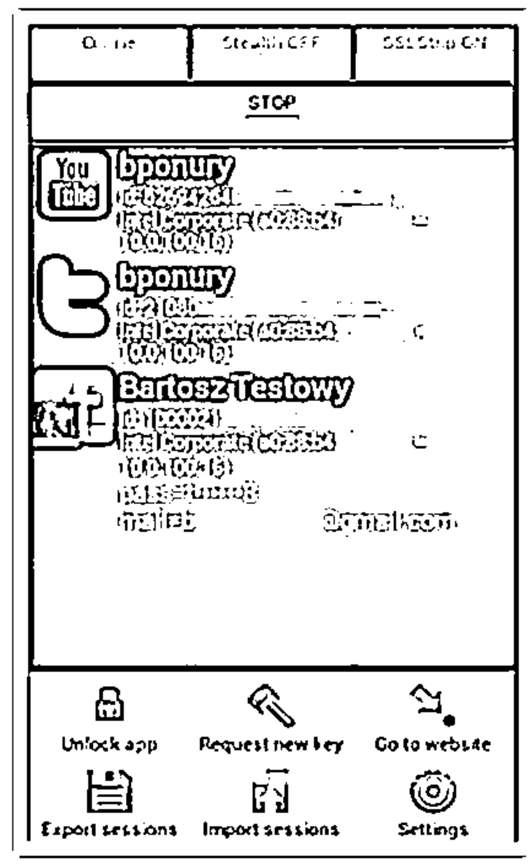


Figure 8.59: Screenshot of FaceNiff

- **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.

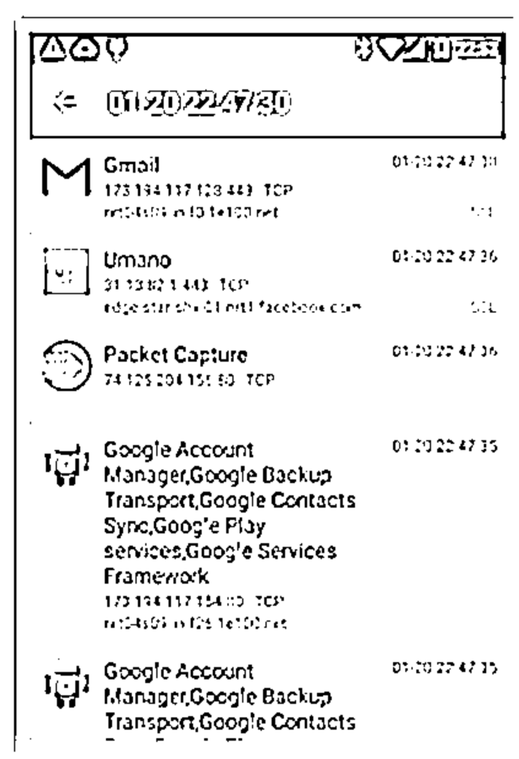
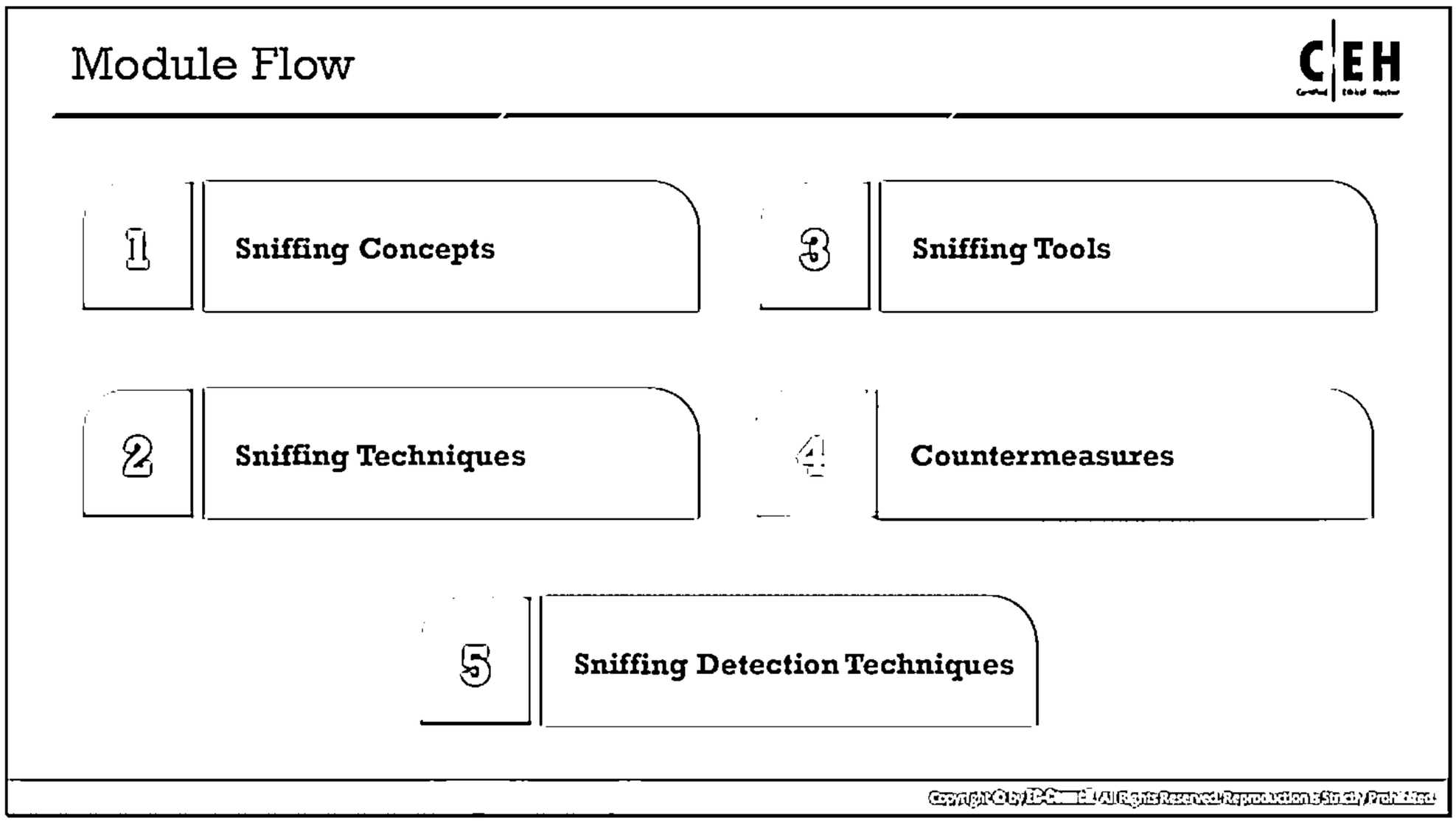


Figure 8.60: Screenshot of Packet Capture

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

Module Flow



Countermeasures

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

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

How to Defend Against Sniffing

- 01 Restrict 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 WPA and WPA2
- 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 the concept of Access Control List (ACL) to allow access to only a fixed range of trusted IP addresses in a network

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

How to Defend Against Sniffing

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

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

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

- 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
- Use encrypted sessions such as SSH instead of telnet, Secure Copy (SCP) instead of FTP, and SSL for email connection 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 secure transfer of files
- Use PGP and S/MIME, VPN, IPSec, SSL/TLS, SSH, and one-time passwords (OTP)
- Use POP2 or POP3 instead of POP to download emails from email servers
- Use SNMPv3 instead of SNMPv1 and SNMPv2 to manage networked devices
- Always encrypt the wireless traffic with a strong encryption protocol such as WPA or WPA2
- 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 promiscuous mode
- Use the concept of Access Control List (ACL) to allow access only to a fixed range of trusted IP addresses in a network
- Change default passwords to complex passwords
- Avoid broadcasting SSIDs (Session Set Identifiers)
- Implement a MAC filtering mechanism on your router
- Implement network scanning and monitoring tools to detect malicious intrusions, rogue devices, and sniffers connected to the network

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

Module Flow

1. Sniffing Concepts
2. Sniffing Techniques
3. Sniffing Tools
4. Countermeasures
5. Sniffing Detection Techniques

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

Sniffing Detection Techniques

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

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

How to Detect Sniffing

Check the Devices Running in Promiscuous Mode

- You need to check which machines are running in the promiscuous mode
- Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety

Run IDS

- Run IDS and see if the MAC address of any of the machines has changed (Example: router's MAC address)
- IDS can alert the administrator about suspicious activities

Run Network Tools

- Run network tools such as Capsa Portable Network Analyzer to monitor the network for detecting strange packets
- Enables you to collect, consolidate, centralize, and analyze traffic data across different network resources and technologies

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

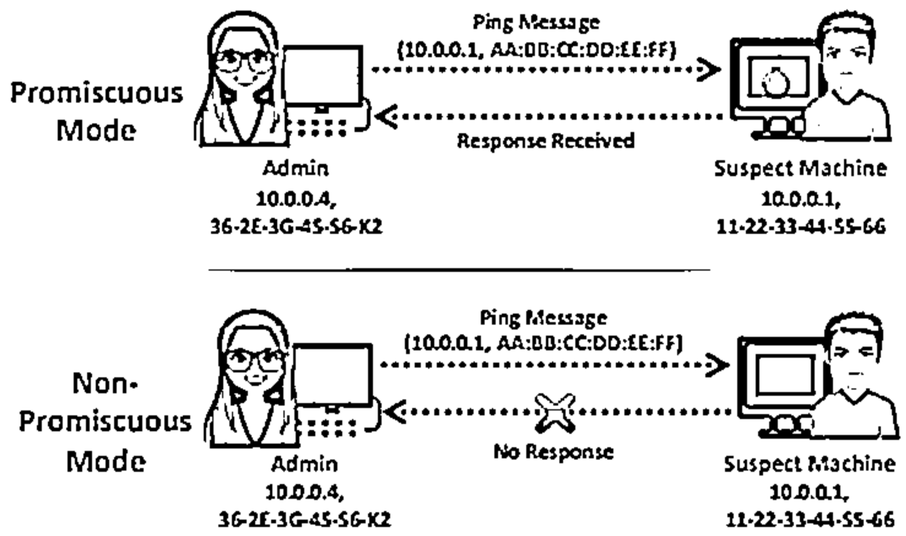
How to Detect Sniffing

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

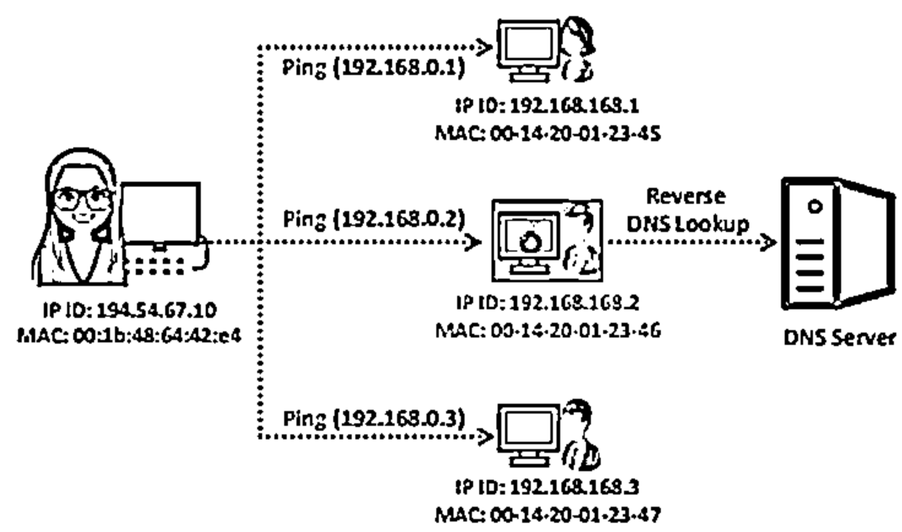
Ping Method



- 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

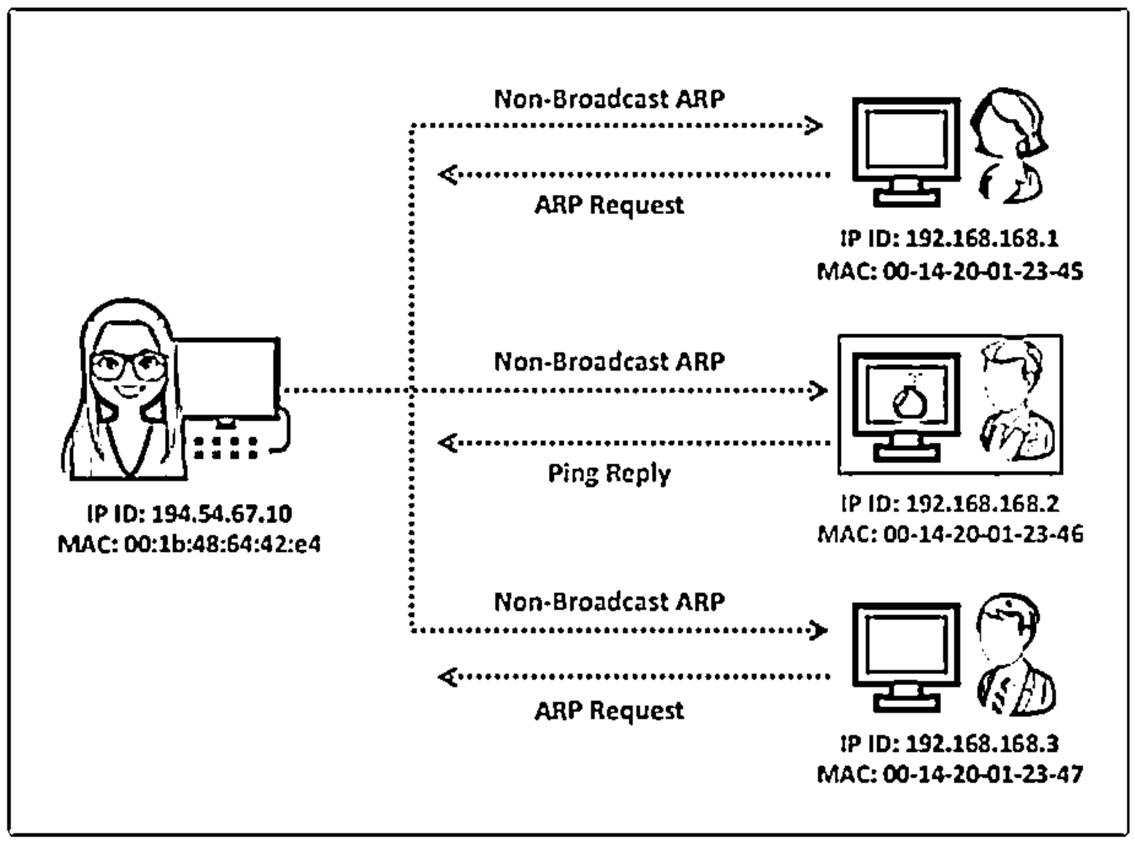


- A machine generating reverse DNS lookup traffic is very likely to be running a sniffer

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.

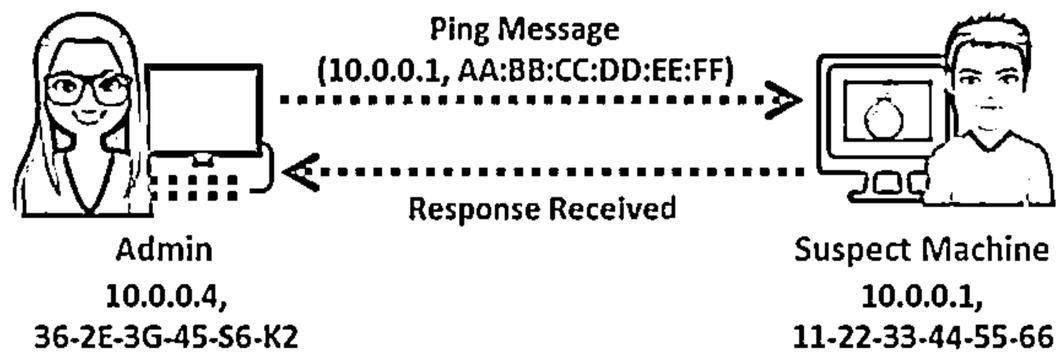


Figure 8.61: Promiscuous mode

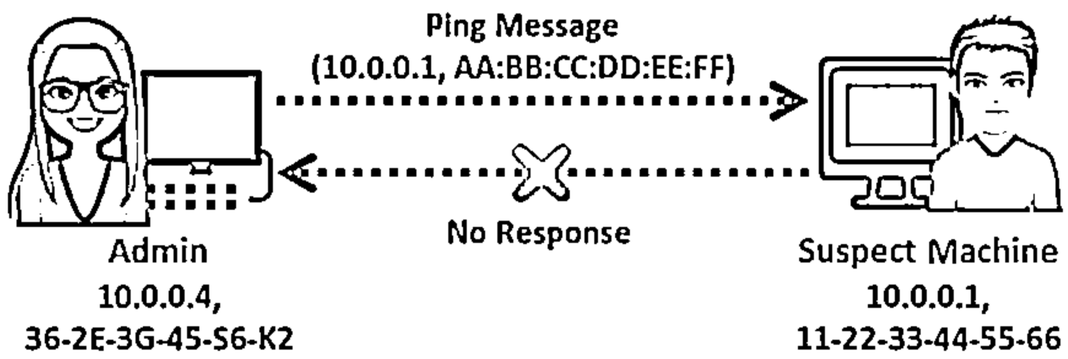


Figure 8.62: Non-promiscuous mode

- **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.

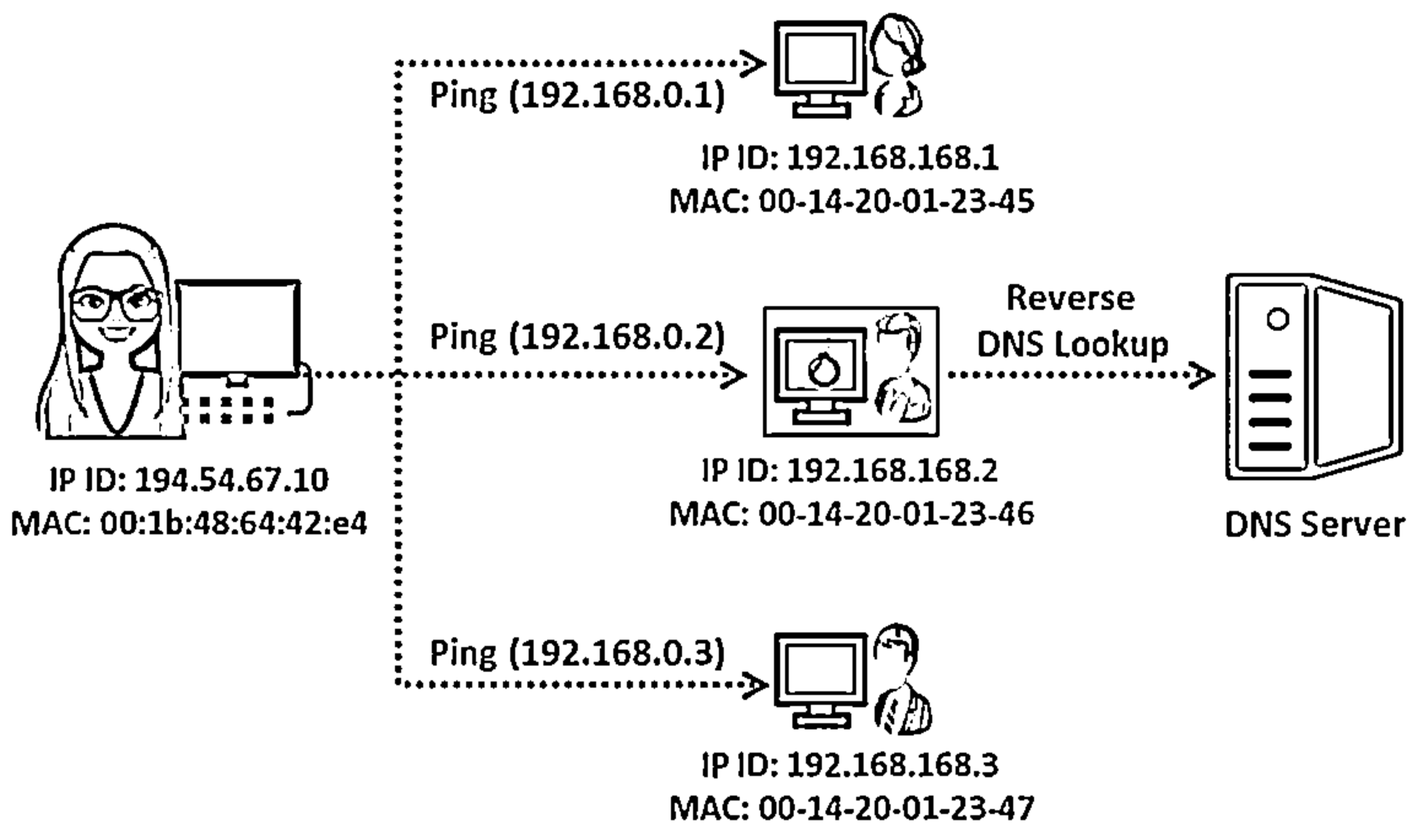


Figure 8.63: Sniffing detection using the DNS method

- **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.

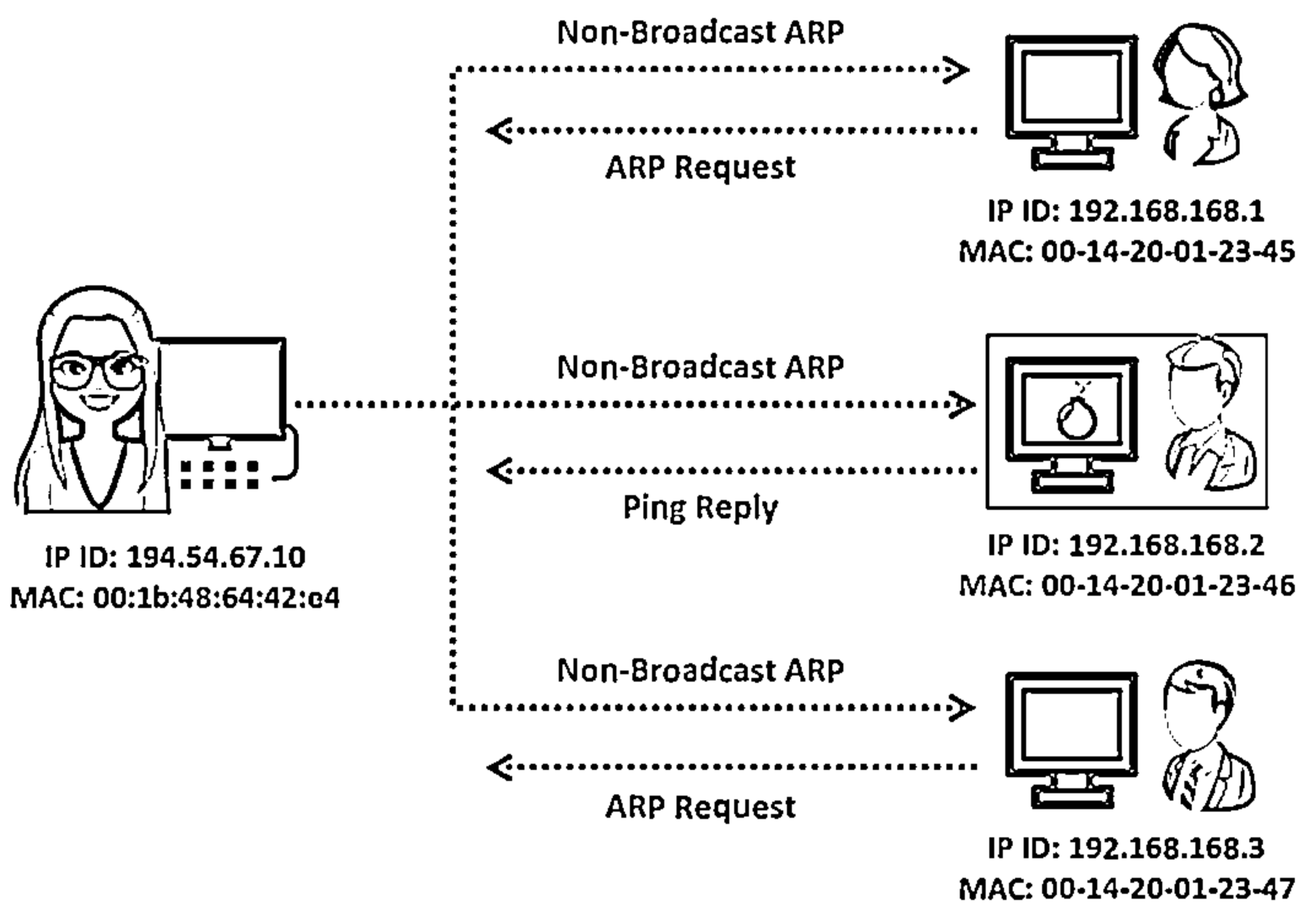


Figure 8.64: Detecting sniffing via the ARP method

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

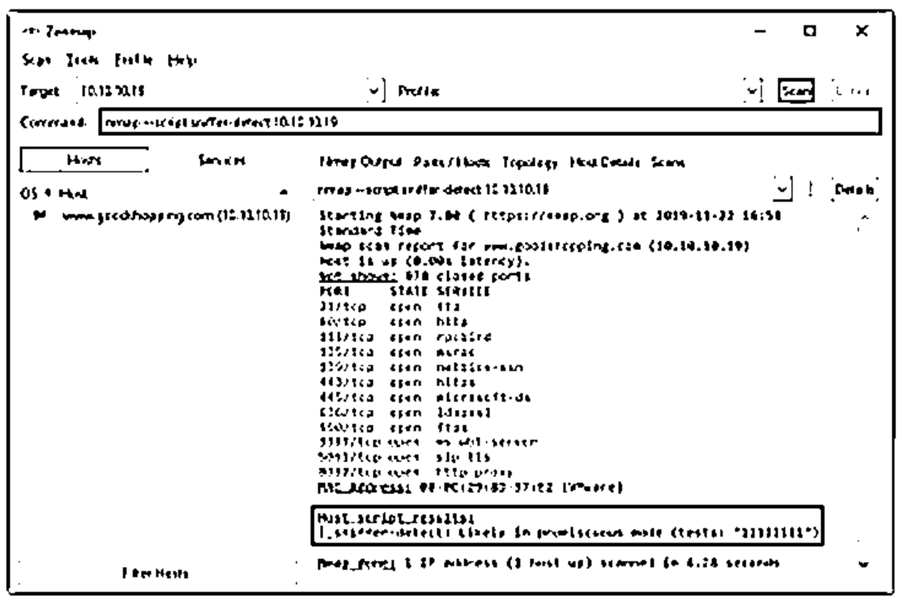
Promiscuous Detection Tools

Nmap

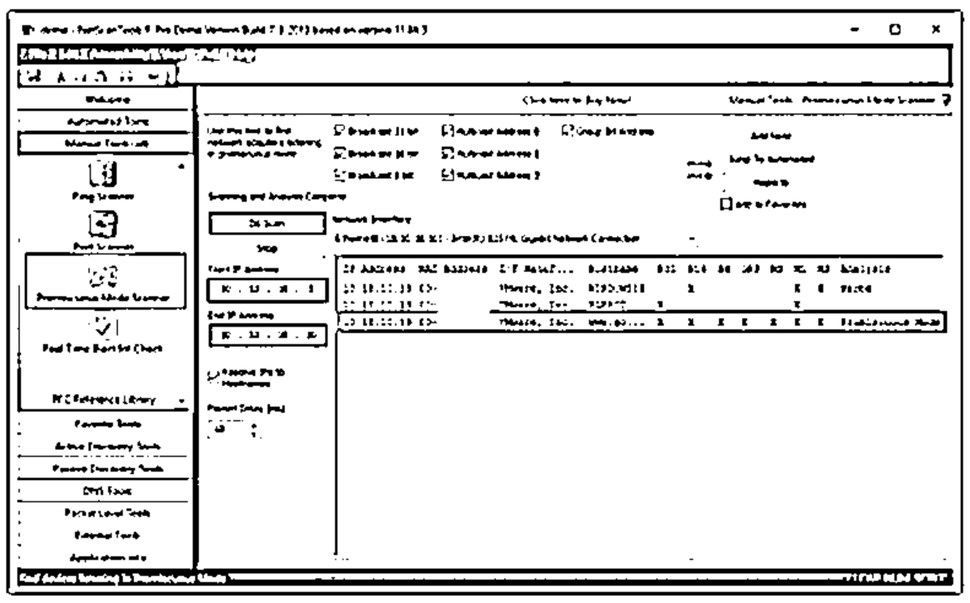
- Nmap's NSE script allows you to check if a system on a local Ethernet has its network card in the promiscuous mode
- Command to detect NIC in promiscuous mode:
  `nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]`

NetScan Tools Pro

- NetScanTools Pro includes a Promiscuous Mode Scanner tool to scan your subnet for network interfaces listening for all ethernet packets in the promiscuous mode



https://nmap.org



https://www.netscantools.com

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.

Zenmap

Scan Tools Profile Help

Target: 10.10.10.19 Profile: Scan Cancel

Command: nmap --script sniffer-detect 10.10.10.19

Hosts Services

OS Host

www.goodshopping.com (10.10.10.19)

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap --script sniffer-detect 10.10.10.19 Details

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 16:58
Standard Time
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00s latency).
Not shown: 978 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
111/tcp  open  rpcbind
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
636/tcp  open  ldapssl
990/tcp  open  ftps
3389/tcp open  ms-wbt-server
5061/tcp open  sip-tls
8080/tcp open  http-proxy
MAC Address: 00:0C:29:8D:37:E2 (VMware)

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

Nmap done: 1 IP address (1 host up) scanned in 4.28 seconds
```

Figure 8.65: 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.

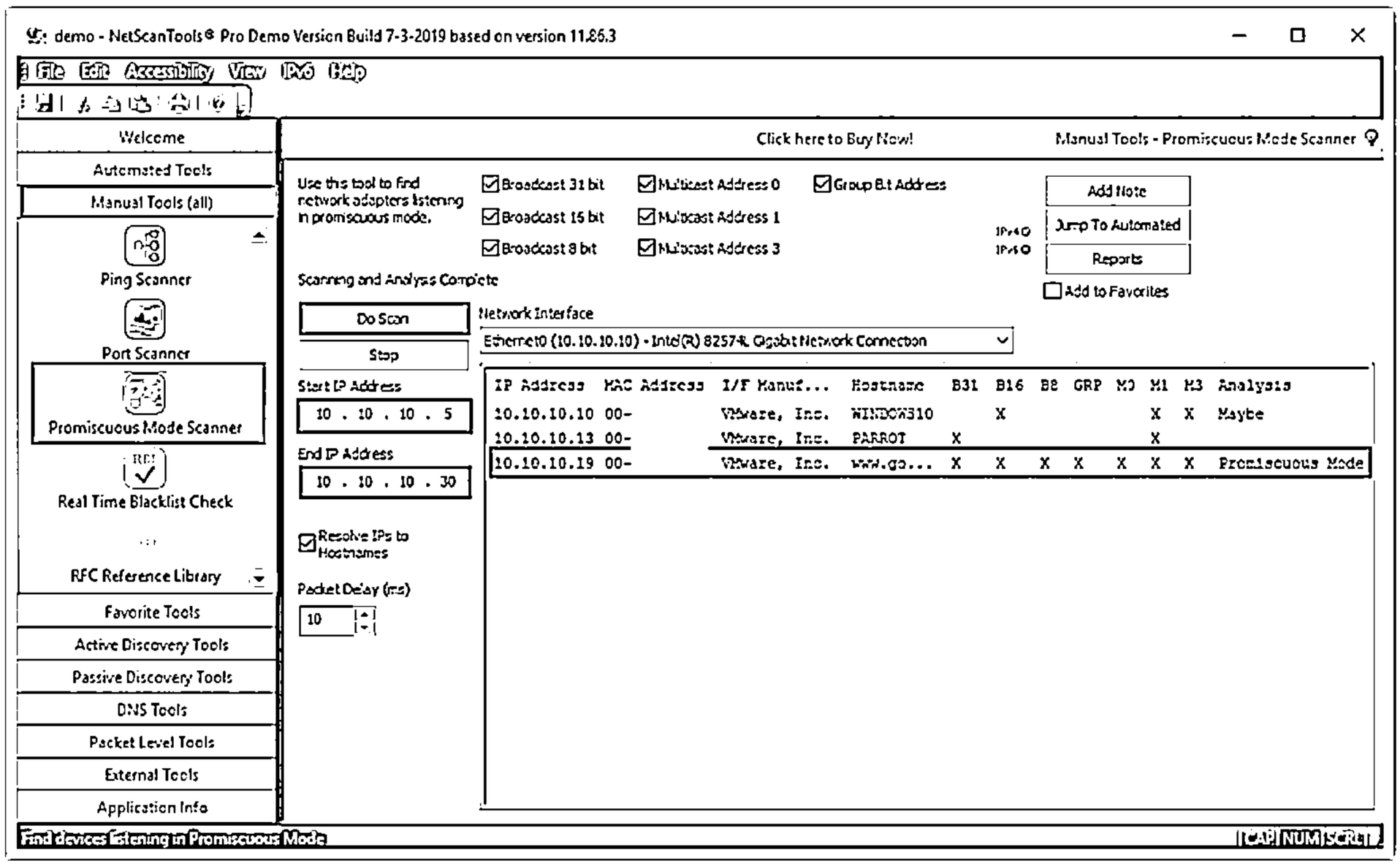


Figure 8.66: Screenshot of NetScanTools Pro – Promiscuous Mode Scanner

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

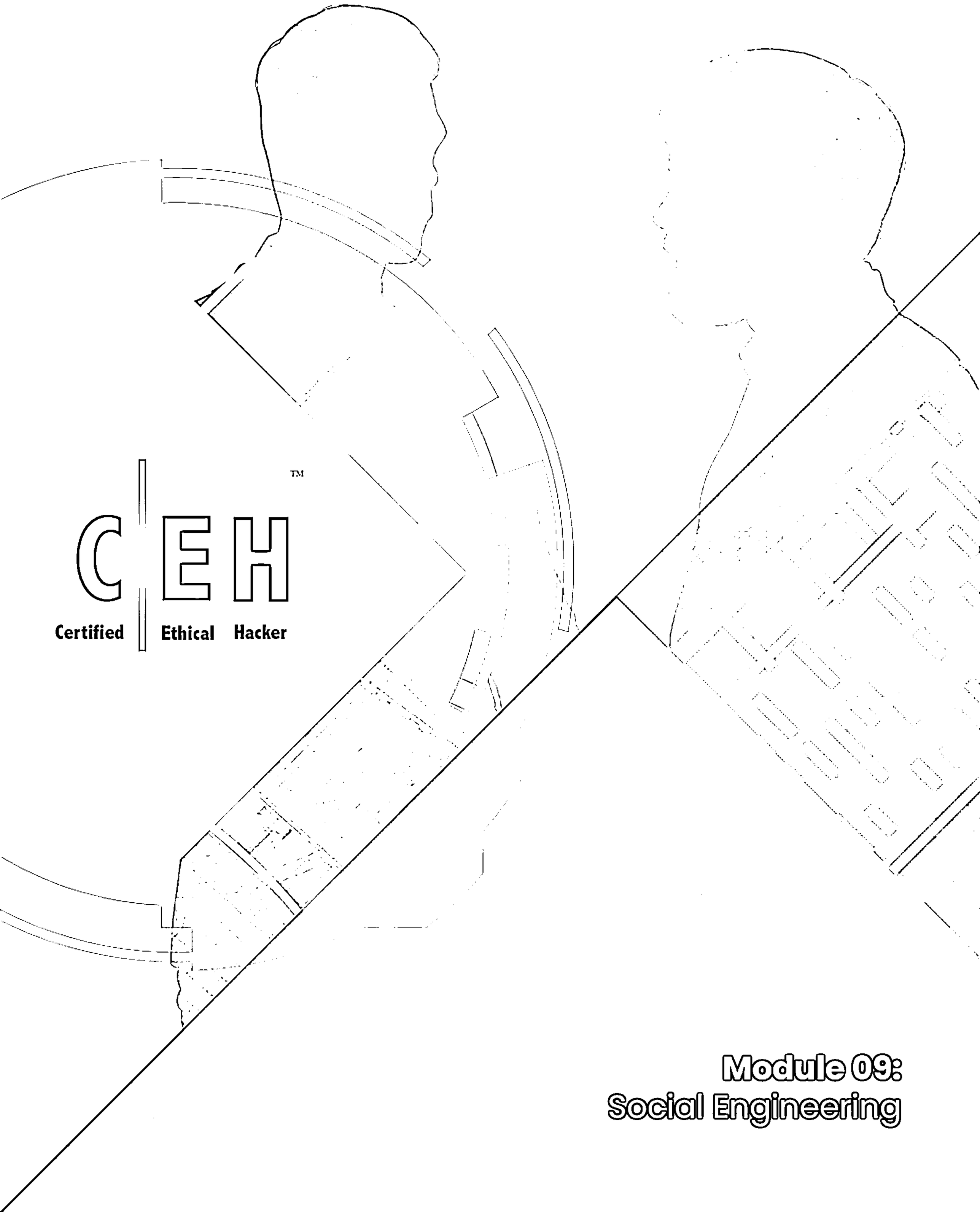
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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.



C|EH™

Certified Ethical Hacker

Module 09: Social Engineering

Module Objectives

- Understanding Social Engineering Concepts
- Understanding Various Social Engineering Techniques
- Understanding Insider Threats
- Understanding Impersonation on Social Networking Sites
- Understanding Identity Theft
- Understanding Different Social Engineering Countermeasures
- Understanding Different Insider Threats and Identity Theft Countermeasures

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

Module Objectives

This module provides an overview of social engineering. Although it focuses on fallacies and advocates effective countermeasures, the possible methods of extracting information from another human being rely on attackers' ingenuity. The features of these techniques make them art, but the psychological nature of some of these techniques makes them a science. The "**bottom line**" is that there is no ready defense against social engineering; only constant vigilance can circumvent some social engineering techniques used by attackers.

This module provides insight into human-based, computer-based, and mobile-based social engineering techniques. It also discusses various insider threats — impersonation on social networking sites, identity theft, as well as possible countermeasures.

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

- Describe social engineering concepts
- Perform social engineering using various techniques
- Describe insider threats
- Perform impersonation on social networking sites
- Describe identity theft
- Apply social engineering countermeasures
- Apply knowledge of insider threats and identity theft countermeasures

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

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures

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

Social Engineering Concepts

There is no single security mechanism that can protect from the social engineering techniques used by attackers. Only educating employees on how to recognize and respond to social engineering attacks can minimize attackers' chances of success. Before going ahead with this module, it is first necessary to discuss various social engineering concepts.

This section describes social engineering, frequent targets of social engineering, behaviors vulnerable to attack, factors making companies vulnerable to attack, why social engineering is effective, the principles of social engineering, and the phases of a social engineering attack.

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

What is Social Engineering?

- Social engineering is the art of convincing people to reveal confidential information
- Common targets of social engineering include help desk personnel, technical support executives, system administrators, etc.
- Social engineers depend on the fact that people are unaware of the valuable information to which they have access and are careless about protecting it

Impact of Attack on an Organization

- Economic losses
- Damage of goodwill
- Loss of privacy
- Dangers of terrorism
- Lawsuits and arbitration
- Temporary or permanent closure

Behaviors Vulnerable to Attacks

- Authority
- Intimidation
- Consensus
- Scarcity
- Urgency
- Familiarity
- Trust
- Greed

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

What is Social Engineering? (Cont'd)

Factors that Make Companies Vulnerable to Attacks

- Insufficient security training
- Unregulated access to information
- Several organizational units
- Lack of security policies

Why is Social Engineering Effective?

- Security policies are as strong as their weakest link, and human behavior is the most susceptible factor
- It is difficult to detect social engineering attempts
- There is no method that can be applied to ensure complete security from social engineering attacks
- There is no specific software or hardware to defend against a social engineering attack

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

What is Social Engineering?

Before performing a social engineering attack, the attacker gathers information about the target organization from various sources such as:

- The organization's official websites, where employees' IDs, names, and email addresses are shared

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

- Advertisements of the target organization cast through media reveal information such as products and offers.
- Blogs, forums, and other online spaces where employees share basic personal and organizational information.

After gathering information, an attacker executes social engineering attacks using various approaches such as impersonation, piggybacking, tailgating, reverse social engineering, and other methods.

Social engineering is the art of manipulating people to divulge sensitive information to use it to perform some malicious action. Despite security policies, attackers can compromise an organization's sensitive information by using social engineering, which targets the weakness of people. Most often, employees are not even aware of a security lapse on their part and inadvertently reveal the organization's critical information. For instance, unwittingly answering strangers' questions or replying to spam email.

To succeed, attackers take a special interest in developing social engineering skills and can be so proficient that the victims might not even notice the fraud. Attackers always look for new ways to access information. They also ensure that they know the organization's perimeter and the people on its **perimeter**, such as security guards, receptionists, and help-desk workers, to exploit human oversight. People have conditioned themselves to not be overly suspicious, and they associate specific behaviors and appearances with known entities. For instance, a man in a uniform carrying a pile of packages for delivery will be perceived as a delivery person. With the help of social engineering tricks, attackers succeed in obtaining confidential information, authorization, and access details from people by deceiving and manipulating human vulnerability.

Common Targets of Social Engineering

A social engineer uses the vulnerability of human nature as their most effective tool. Usually, people believe and trust others and derive fulfillment from helping the needy. Discussed below are the most common targets of social engineering in an organization:

- **Receptionists and Help-Desk Personnel**: Social engineers generally target service-desk or help-desk personnel by tricking them into divulging confidential information about the organization. To extract information, such as a phone number or password, the attacker first wins the trust of the individual with the information. On winning their trust, the attacker manipulates them to get valuable information. Receptionists and help-desk staff may readily share information if they feel they are doing so to help a customer.
- **Technical Support Executives**: Another target of social engineers is technical support executives. The social engineers may take the approach of contacting technical support executives to obtain sensitive information by pretending to be senior management, customers, vendors, or other figures.
- **System Administrators**: A system administrator in an organization is responsible for maintaining the systems. Thus, they may have critical information such as the type and

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

version of OS and admin passwords, that could be helpful for an attacker in planning an attack.

- **Users and Clients**: Attackers could approach users and clients of the target organization, pretending to be a tech support person to extract sensitive information.
- **Vendors of the Target Organization**: Attackers may also target the vendors of the organization to gain critical information that could help in executing attacks.
- **Senior Executives:** Attackers could also approach senior executives from various departments such as Finance, HR, and CxOs to obtain critical information about the organization

Impact of Social Engineering Attack on an Organization

Social engineering does not seem like a serious threat, but it can lead to substantial losses for organizations. The impact of social engineering attack on organizations include:

- **Economic Losses**: Competitors may use social engineering techniques to steal sensitive information such as the development plans and marketing strategies of the target company, which can result in an economic loss.
- **Damage to Goodwill**: For an organization, goodwill is important for attracting customers. Social engineering attacks may damage that goodwill by leaking sensitive organizational data.
- **Loss of Privacy**: Privacy is a major concern, especially for big organizations. If an organization is unable to maintain the privacy of its stakeholders or customers, then people can lose trust in the company and may discontinue their business association with the organization. Consequently, the organization could face losses.
- **Dangers of Terrorism**: Terrorism and anti-social elements pose a threat to an organization's assets — people and property. Terrorists may use social engineering techniques to make blueprints of their targets to infiltrate their targets.
- **Lawsuits and Arbitration**: Lawsuits and arbitration result in negative publicity for an organization and affects the business's performance.
- **Temporary or Permanent Closure**: Social engineering attacks can result in a loss of goodwill. Lawsuits and arbitration may force the temporary or permanent closure of an organization and its business activities.

Behaviors Vulnerable to Attacks

- **Authority**

  Authority implies the right to exercise power in an organization. Attackers take advantage of this by presenting themselves as a person of authority, such as a technician or an executive, in a target organization to steal important data.

  For example, an attacker can call a user on the phone and can claim to be working as a network administrator in the target organization. The attacker then informs the victim about a security incident in the network and asks them to provide their account

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

credentials to protect their data against theft. After obtaining the victim's credentials, the attacker steals sensitive information from the victim's account.

- **Intimidation**

  Intimidation refers to an attempt to intimidate a victim into taking several actions by using bullying tactics. It is usually performed by impersonating some other person and manipulating users into disclosing sensitive information.

  For example, an attacker might call the executive's receptionist with this request:

  "Mr. Tibiyani is about to give a big presentation to the customers, but he is unable to open his files; it seems they are corrupt. He told me to call you and ask you to send the files to me immediately so that he can start his talk."

- **Consensus or Social Proof**

  Consensus or social proof refers to the fact that people are usually willing to like things or do things that other people like or do.

  Attackers take advantage of this by doing things like creating websites and posting fake testimonials from users about the benefits of certain products such as anti-malware (rogueware). Therefore, if users search the Internet to download the rogueware, they encounter these websites and believe the forged testimonials. Further, if users download the malicious product, attackers may install a trojan along with it.

- **Scarcity**

  Scarcity implies the state of being scarce. In the context of social engineering, scarcity often implies creating a feeling of urgency in a decision-making process. Due to this urgency, attackers can control the information provided to victims and manipulate the decision-making process.

  For example, when Apple releases a new iPhone product that sells out and goes out of stock, attackers can take advantage of this situation by sending a phishing email to the target users, encouraging them to click on a link provided in the email to buy the product. If the users click on this link, they get redirected to some malicious website controlled by the attacker. As a result, the user might end up revealing their account details or downloading some malicious programs such as trojans.

- **Urgency**

  Urgency implies encouraging people to take immediate action. Attackers can take advantage of this by tricking victims into performing unintended tasks.

  For example, ransomware often uses the urgency principle, which makes the victim take urgent action under a time-limit. The victims see the countdown timer running on their infected systems and know that failure to make the required decision within the given time can result in the loss of important data.

  Similarly, attackers can send phishing emails indicating that a certain product is available at a low price and that to buy it, the user should click on the "Buy Now" link. The user is

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

tricked, and they click on the link to take immediate action. As a result, they are redirected to a malicious website and end up revealing their account details or downloading a virus file.

- **Familiarity or Liking**

  Familiarity or liking implies that people are more likely to be persuaded to do something when they are asked by someone whom they like. This indicates that people are more likely to buy products if they are advertised by an admired celebrity.

  For example, people are more likely to allow someone to look over their shoulder if they like that person or they are familiar with them. If people do not like the person, they immediately recognize the shoulder surfing attack and prevent it. Similarly, people often allow someone to tailgate them if they like that person or are familiar with them. In some cases, social engineers use a charming smile and sweet-talk to deceive the other person into liking them.

- **Trust**

  Attackers often attempt to build a trusting relationship with victims.

  For example, an attacker can call a victim and introduce themself as a security expert. Then, they may claim that they were working with XYZ company, and they noticed some unusual errors sent from the victim's system. The attacker builds trust by using the company name and their experience in the security field. After establishing trust, the attacker guides the victim to follow a series of steps to "view and disable the system errors." They later send an email containing a malicious file and persuade the victim to click on and download it. Through this process, the attacker successfully installs malware on the victim's system, infecting it and allowing the attacker to steal important information.

- **Greed**

  Some people are possessive by nature and seek to acquire vast amounts of wealth through illegal activities. Social engineers lure their targets to divulge information by promising something for nothing (appealing to their greed).

  For example, an attacker may pretend to be a competitor and lure the employees of the target into revealing critical information by offering a considerable reward.

Factors that Make Companies Vulnerable to Attacks

Many factors make companies vulnerable to social engineering attacks; some of them are as follows:

- **Insufficient Security Training**

  Employees can be ignorant about the social engineering tricks used by attackers to lure them into divulging sensitive data about the organization. Therefore, the minimum responsibility of any organization is to educate their employees about social engineering techniques and the threats associated with them to prevent social engineering attacks.

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

- **Unregulated Access to Information**

  For any company, one of its main assets is its database. Providing unlimited access or allowing everyone access to such sensitive data might cause trouble. Therefore, companies must ensure proper training for and surveillance of key personnel accessing sensitive data.

- **Several Organizational Units**

  Some organizations have their units at different geographic locations, making it difficult to manage the system. Further, this sort of setup makes it easier for an attacker to access the organization's sensitive information.

- **Lack of Security Policies**

  Security policy is the foundation of security infrastructure. It is a high-level document describing the security controls implemented in a company. An organization should take extreme measures related to every possible security threat or vulnerability. Implementation of certain security measures such as password change policy, information sharing policy, access privileges, unique user identification, and centralized security, prove to be beneficial.

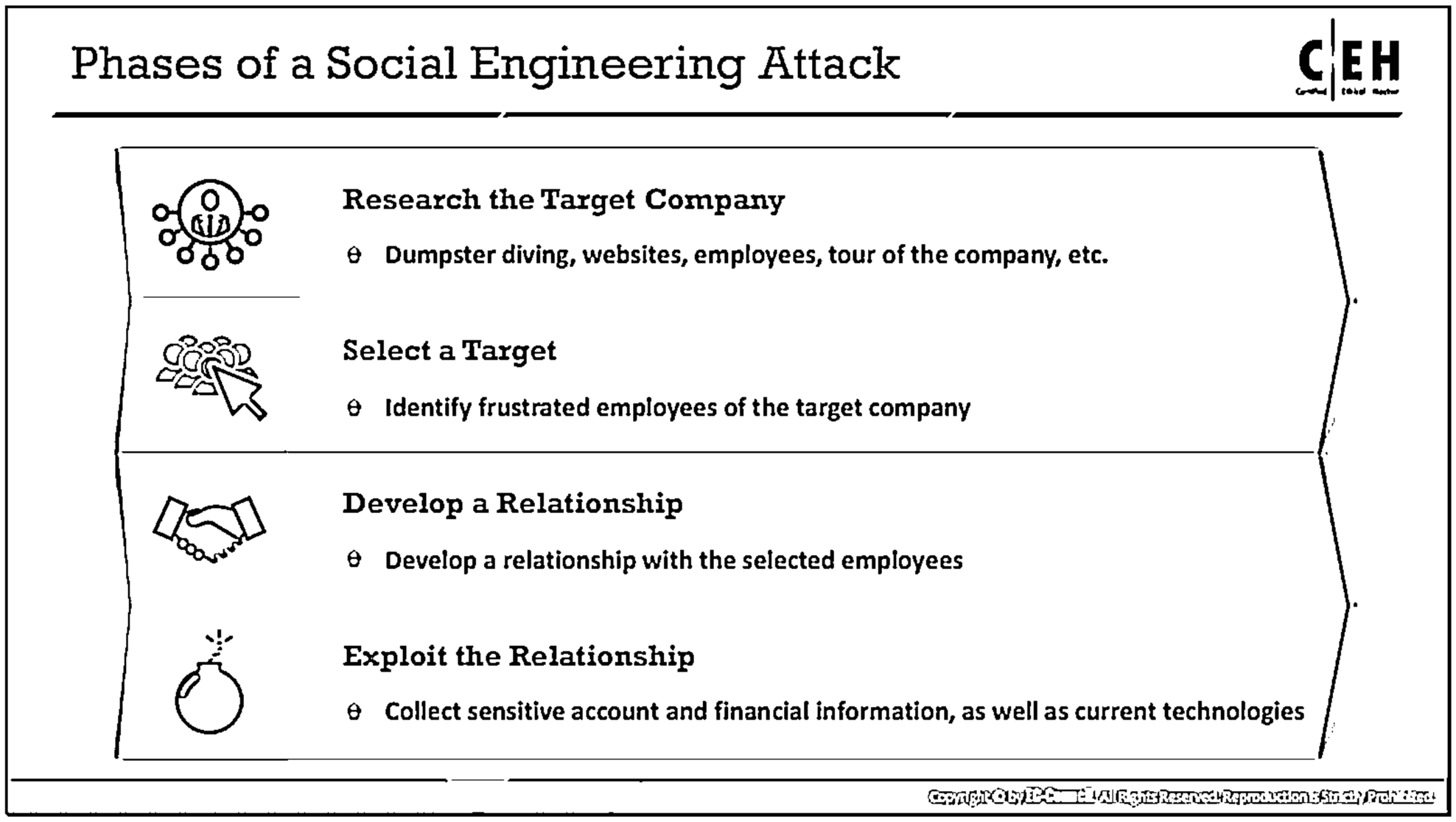
Why is Social Engineering Effective?

Like other techniques, social engineering does not deal with network security issues; instead, it deals with the psychological manipulation of a human being to extract desired information.

The following are reasons why social engineering continues to be effective:

- Despite various security policies, preventing social engineering is a challenge because human beings are most susceptible to variation.
- It is challenging to detect social engineering attempts. Social engineering is the art and science of manipulating people into divulging information.
- No method guarantees complete security from social engineering attacks.
- No specific hardware or software is available to safeguard against social engineering attacks.
- This approach is relatively cheap (or free) and easy to implement.

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



Phases of a Social Engineering Attack

Attackers take the following steps to execute a successful social engineering attack:

- **Research the Target Company**

  Before attacking the target organization's network, an attacker gathers enough information to infiltrate the system. Social engineering is one technique that helps in extracting information. Initially, the attacker researches basic information about the target organization, such as the nature of the business, its location, number of employees, and other facts. While researching, the attacker indulges in activities such as dumpster diving, browsing the company's website, and finding employee details.

- **Select a Target**

  After finishing their research, the attacker selects a target for extracting sensitive information about the organization. Usually, attackers try to reach out to disgruntled employees because they are easier to manipulate.

- **Develop a Relationship**

  Once the target is set, the attacker builds a relationship with that employee to accomplish their task.

- **Exploit the Relationship**

  The attacker exploits the relationship and extracts sensitive information about the organization's accounts, finance information, technologies in use, and upcoming plans.

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

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures

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

Social Engineering Techniques

Attackers implement various social engineering techniques to gather sensitive information from people or organizations that might help them to commit fraud or participate in other criminal activities.

This section deals with various human-based, computer-based, and mobile-based social engineering techniques, coded with examples for a better understanding.

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

Types of Social Engineering

Human-based Social Engineering

- Sensitive information is gathered by interaction
- Techniques:
  - Impersonation
  - Vishing
  - Eavesdropping
  - Shoulder Surfing
  - Dumpster Diving
  - Reverse Social Engineering
  - Piggybacking
  - Tailgating
  - Diversion Theft
  - Honey Trap
  - Baiting and Quid Pro Quo
  - Elicitation

Computer-based Social Engineering

- Sensitive information is gathered with the help of computers
- Techniques:
  - Phishing
  - Pop-up Window Attacks
  - Spam Mail
  - Instant Chat Messenger
  - Scareware

Mobile-based Social Engineering

- Sensitive information is gathered with the help of mobile apps
- Techniques:
  - Publishing Malicious Apps
  - Using Fake Security Apps
  - Repackaging Legitimate Apps
  - SMiShing (SMS Phishing)

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

Types of Social Engineering

In a social engineering attack, the attacker uses their social skills to trick the victim into disclosing personal information such as credit card numbers, bank account numbers, and phone numbers, or confidential information about their organization or computer system. Attackers use this data to either launch an attack or to commit fraud. Social engineering attacks are categorized into three categories: human-based, computer-based, and mobile-based.

- **Human-based Social Engineering**

  Human-based social engineering involves human interaction. Acting as though they were a legitimate person, the attacker interacts with the employee of the target organization to collect sensitive information, such as business plans and networks, that might help them in launching their attack. For example, impersonating an IT support technician, the attacker can easily access the server room.

  An attacker can perform human-based social engineering by using the following techniques:

  - Impersonation
  - Vishing
  - Eavesdropping
  - Shoulder Surfing
  - Dumpster Diving
  - Reverse Social Engineering
  - Piggybacking
  - Tailgating
  - Diversion Theft
  - Honey Trap
  - Baiting
  - Quid Pro Quo
  - Elicitation

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

- **Computer-based Social Engineering**

  Computer-based social engineering relies on computers and Internet systems to carry out the targeted action.

  The following techniques can be used for computer-based social engineering:

  - Phishing
  - Spam mail
  - Instant chat messenger
  - Pop-up window attacks
  - Scareware

- **Mobile-based Social Engineering**

  Attackers use mobile applications to carry out mobile-based social engineering. Attackers trick the users by imitating popular applications and creating malicious mobile applications with attractive features and submitting them to the major app stores with the same name. Users unknowingly download the malicious app, allowing the malware to infect their device.

  Listed below are some techniques attackers use to perform mobile-based social engineering:

  - Publishing malicious apps
  - Repackaging legitimate apps
  - Using fake security applications
  - SMiShing (SMS Phishing)

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

Human-based Social Engineering

Impersonation

- The attacker pretends to be someone legitimate or an authorized person
- Attackers may impersonate a legitimate or authorized person either personally or using a communication medium such as phone, email, etc.
- Impersonation helps attackers to trick a target into revealing sensitive information
- The most common human-based social engineering technique

Impersonation Examples

Posing as a legitimate end user

- The attacker gives this identity and asks for the sensitive information

"Hi! This is John from the Finance Department. I have forgotten my password. Can I get it?"

Posing as an important user

- The attacker poses as a VIP of a target company, valuable customer, etc.

"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system's password. Can you help me out?"

Posing as a technical support agent

- The attacker poses as technical support staff and requests IDs and passwords

"Sir, this is Matthew, Technical Support, X company. Last night we had a system crash here, and we are checking for the lost data. Can you give me your ID and password?"

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

Human-based Social Engineering (Cont'd)

Impersonation (Vishing)

- Vishing (voice or VoIP phishing) is an impersonation technique (electronic fraud) in which the attacker tricks individuals to reveal personal and financial information using voice technology such as the telephone system, VoIP, etc.

Vishing Examples

Abusing the Over-Helpfulness of Help Desks

- The attacker calls a company's help desk, pretends to be someone in a position of authority or relevance and tries to extract sensitive information from the help desk

"A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.

The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker a clear entrance into the corporate network."

Third-party Authorization

- The attacker obtains the name of the authorized employee of the targeted organization who has access to the information he/she wants
- The attacker then places a call to the target organization where information is stored and claims that this employee has requested that such information be provided

"Hi, I am John, I spoke with Mr. X last week before he went on vacation and he said that you would be able to provide me with this information in his absence. Can you help me out?"

Tech Support

- The attacker pretends to be technical support staff of the targeted organization's software vendors or contractors
- He/she may request user IDs and passwords for troubleshooting a problem in the organization

Attacker: *"Hi, this is Mike with tech support. We have had some people from your office report/complain about slowdowns in logging in lately. Is this true?"*

Employee: *"Yes, it has been slow lately."*

Attacker: *"Well, we have moved you to a new server to improve your service. Could you give me your password so that I can check your service? Things should be better for you now."*

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

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

Human-based Social Engineering (Cont'd)

Eavesdropping

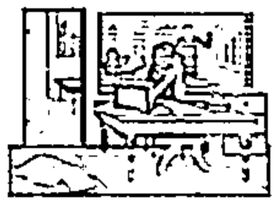
- Unauthorized listening of conversations, or reading of messages
- Interception of audio, video, or written communication
- Can be done using communication channels such as telephone lines, email, instant messaging, etc.

Shoulder Surfing

- Direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.
- Can also be done from a farther distance with the aid of vision enhancing devices such as binoculars

Dumpster Diving

- Looking for treasure in someone else's trash
- Involves collecting phone bills, contact information, financial information, operations-related information, etc. from the target company's trash bins or printer bins, or user desks (e.g., sticky notes), etc.



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

Human-based Social Engineering (Cont'd)

Reverse Social Engineering	The attacker presents him/herself as an authority and the target seeks his or her advice before or after offering the information that the attacker needs
Piggybacking	An authorized person intentionally or unintentionally allows an unauthorized person to pass through a secure door e.g., "I forgot my ID badge at home. Please help me"
Tailgating	The attacker, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door that requires key access
Diversion Theft	The attacker tricks a person responsible for making a genuine delivery into delivering the consignment to a location other than the intended location

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

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

Human-based Social Engineering (Cont'd)

Honey Trap	Attackers target a person inside the company online, pretending to be an attractive person. They then begin a fake online relationship to obtain confidential information about the target company
Baiting	Attackers offer end users something alluring in exchange for important information such as login details and other sensitive data A physical device such as USB flash drive containing malicious files is left in a location where people can easily find it
Quid Pro Quo	Attackers call numerous random numbers within a company, claiming to be from technical support They offer their service to end users in exchange for confidential data or login credentials
Elicitation	Attackers extract information from the victim by engaging him/her in normal and disarming conversations Based on the victim's interests, attackers must work to target their elicitation approach to extract the relevant information

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

Human-based Social Engineering

Impersonation

Impersonation is a common human-based social engineering technique where an attacker pretends to be a legitimate or authorized person. Attackers perform impersonation attacks personally or use a phone or another communication medium to mislead their target and trick them into revealing information. The attacker might impersonate a courier or delivery person, janitor, businessman, client, technician, or they may pretend to be a visitor. Using this technique, the attacker gathers sensitive information by scanning terminals for passwords, searching for important documents on employees' desks, rummaging through bins, and through other tactics. The attacker may even try to overhear confidential conversations and "**shoulder surf**" to obtain sensitive information.

Types of impersonation used in social engineering:

- Posing as a legitimate end-user
- Posing as an important user
- Posing as a technical support agent
- Posing as an internal employee, client, or vendor
- Posing as a repairman
- Abusing the over-helpfulness of the help desk
- Posing as someone with third-party authorization
- Posing as a tech support agent through vishing
- Posing as a trusted authority

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

Some impersonation tricks that an attacker performs to gather sensitive information about the target organization exploit the human nature of trust, fear, and moral obligation.

- **Posing as a Legitimate End User**

  An attacker might impersonate an employee and then resort to deviant methods to gain access to privileged data. They may provide a false identity to obtain sensitive information.

  Another example is when a "**friend**" of an employee asks them to retrieve information that a bedridden employee supposedly needs. There is a well-recognized rule in social interaction that a favor begets a favor, even if the original "**favor**" is offered without a request from the recipient. This is known as reciprocation. Corporate environments deal with reciprocation daily. Social engineers try to take advantage of this social trait via impersonation.

  Example:

  "Hi! This is John from the finance department. I have forgotten my password. Can I get it?"

- **Posing as an Important User**

  Another behavioral factor that aids a social engineer is people's habit of not questioning authority. People often go out of their way for those whom they perceive to have authority. An attacker posing as an important individual — such as a vice president or director — can often manipulate an unprepared employee. Attackers who take impersonation to a higher level by assuming the identity of an important employee add an element of intimidation. The reciprocation factor also plays a role in this scenario where lower-level employees might go out of their way to help a higher-authority. For example, it is less likely that a help-desk employee will turn down a request from a vice president who is hard-pressed for time and needs some vital information for a meeting. In case an employee refuses to divulge information, social engineers may use authority to intimidate employees and may even threaten to report the employee's misconduct to their supervisors. This technique assumes greater significance when the attacker considers it a challenge to get away with impersonating an authority figure.

  Example:

  "Hi! This is Kevin, the CFO's Secretary. I'm working on an urgent project, and I forgot my system password. Can you help me out?"

- **Posing as a Technical Support Agent**

  Another technique involves an attacker masquerading as a technical support agent, particularly when the victim is not proficient in technical areas. The attacker may pretend to be a hardware vendor, a technician, or a computer supplier. One demonstration at a hacker meeting had the speaker calling Starbucks and asking its employees whether their broadband connection was properly working. The perplexed employee replied that it was the modem that was giving them trouble. The hacker,

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

without giving any credentials, went on to make him read out the credit card number of the last transaction. In a corporate scenario, the attacker may ask employees to reveal their login information, including their password, to fix a nonexistent problem.

Example:

"Sir, this is Mathew, technical support at X Company. Last night we had a system crash here, and we are checking for lost data. Can you give me your ID and password?"

- **Posing as an Internal Employee, Client, or Vendor**

  The attacker usually dresses up in business clothes or another suitable uniform. They enter an organization's building while pretending to be a contractor, client, service personnel, or another authorized person. Then they roam around unnoticed and look for passwords stuck on terminals, extract critical data from wastepaper bins, papers lying on desks, and perform other information gathering. The attacker may also implement other social engineering techniques such as shoulder surfing (observing users typing login credentials or other sensitive information) and eavesdropping (purposely overhearing confidential conversations between employees) to gather sensitive information that might help launch an attack on the organization.

- **Repairman**

  Computer technicians, electricians, and telephone repairpersons are generally unsuspected people. Attackers might impersonate a technician or repair person and enter the organization. They perform normal activities associated with their assumed duty while looking for hidden passwords, critical information on desks, information in trash bins, and other useful information; they sometimes even plant snooping devices in hidden locations.

Impersonation (Vishing)

Vishing (voice or VoIP phishing) is an impersonation technique in which the attacker uses Voice over IP (VoIP) technology to trick individuals into revealing their critical financial and personal information and uses the information for financial gain. The attacker uses caller ID spoofing to forge identification. In many cases, Vishing includes pre-recorded messages and instructions resembling a legitimate financial institution. Through Vishing, the attacker tricks the victim into providing bank account or credit card details for identity verification over the phone.

The attacker may send a fake SMS or email message to the victim, asking the victim to call the financial institution for credit card or bank account verification. In some cases, the victim receives a voice call from the attacker. When the victim calls the number listed in the message or receives the attacker's call, they hear recorded instructions that insist they provide personal and financial information like name, date of birth, social security number, bank account numbers, credit card numbers, or credentials like usernames, passwords. Once the victim provides the information, the recorded message confirms verification of the victim's account.

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

Discussed below are some tricks attackers use when Vishing to gather sensitive information.

- **Abusing the Over-Helpfulness of Help Desk**

  Help desks are frequently targeted for social engineering attacks for a reason. The staff members are trained to be helpful, and they often give away sensitive information such as passwords and network information without verifying the authenticity of the caller.

  The attacker should know employees' names and have details about the person he is trying to impersonate to be effective. The attacker may call a company's help desk pretending to be a senior official to try to extract sensitive information out of the help desk.

  Example:

  A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.

  The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker entrance into the corporate network.

- **Third-party Authorization**

  Another popular technique used by an attacker is to represent themself as an agent authorized by some senior authority in an organization to obtain information on their behalf.

  For instance, when an attacker knows the name of the employee in the target organization authorized to access the required information, they keep a vigil on them so that they can access the required data in the absence of the concerned employee. In this case, the attacker can approach the help desk or other personnel in the company claiming that the employee (authority figure) has requested the information.

  Even though there might be suspicion attached to the authenticity of the request, people tend to overlook this in favor of being helpful in the workplace. People tend to believe that others are being honest when they reference an important person and provide the required information.

  This technique is effective, particularly when the authority figure is on vacation or traveling, making instant verification impossible.

  Example:

  "Hi, I am John, I spoke with Mr. XYZ last week before he went on vacation and he said that you would be able to provide me with the information in his absence. Could you help me out?"

- **Tech Support**

  Like the impersonation of a tech support agent above, an attacker can use vishing to pretend to be a technical support staff member of the target organization's software vendor or contractor to obtain sensitive information. The attacker may pretend to troubleshoot a network problem and ask for the user ID and password of a computer to

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

detect the problem. Believing them to be a troubleshooter, the user would provide the required information.

Example:

Attacker: "Hi, this is Mike from tech support. Some folks in your office have reported a slowdown in logging. Is this true?"

Employee: "Yes, it has seemed slow lately."

Attacker: "Well, we have moved you to a new server, and your service should be much better now. If you want to give me your password, I can check your service. Things will be better from now on."

- **Trusted Authority Figure**

The most effective method of social engineering is posing as a trusted authority figure. An attacker might pretend to be a fire marshal, superintendent, auditor, director, or other important figure over the phone or in-person to obtain sensitive information from the target.

Example:

1. "Hi, I am John Brown. I'm with the external auditor, Arthur Sanderson. We've been requested by the corporate to do a surprise inspection of your disaster recovery procedures. Your department has 10 minutes to show me how you would recover from a website crash."
2. "Hi, I'm Sharon, a sales rep out of the New York office. I know this is short notice, but I have a group of prospective clients out in the car, and I've been trying to get them to outsource their security training needs to us for months.

   They're located just a few miles away, and I think that if I can give them a quick tour of our facilities, it would be enough to push them over the edge and get them to sign up.

   Oh yeah, they are particularly interested in what security precautions we've adopted. It seems someone hacked into their website a while back, which is one of the reasons they're considering our company."
3. "Hi, I'm with Aircon Express Services. We received a call that the computer room is getting too warm, so I need to check your HVAC system." Using professional-sounding terms like HVAC (Heating, Ventilation, and Air Conditioning) may add just enough credibility to an intruder's masquerade to allow them to access the targeted secured resource.

Eavesdropping

Eavesdropping refers to an unauthorized person listening to a conversation or reading others' messages. It includes the interception of any form of communication, including audio, video, or written, using channels such as telephone lines, email, and instant messaging. An attacker can obtain sensitive information such as passwords, business plans, phone numbers, and addresses.

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

Shoulder Surfing

Shoulder surfing is the technique of looking over someone's shoulder as they key information into a device. Attackers use shoulder surfing to find out passwords, personal identification numbers, account numbers, and other information. They sometimes even use binoculars and other optical devices or install small cameras to record the actions performed on the victim's system to obtain login details and other sensitive information.

Dumpster Diving

Dumpster diving is the process of retrieving sensitive personal or organizational information by searching through trash bins. Attackers can extract confidential data such as user IDs, passwords, policy numbers, network diagrams, account numbers, bank statements, salary data, source code, sales forecasts, access codes, phone lists, credit card numbers, calendars, and organizational charts on paper or disk. Attackers can then use this information to perform various malicious activities. Sometimes attackers even use pretexts to support their dumpster diving initiatives, such as impersonating a repair person, technician, cleaner, or other legitimate worker.

Information that attackers can obtain by searching through trash bins includes:

- **Phone lists**: Disclose employees' names and contact numbers.
- **Organizational charts**: Disclose details about the structure of the company, physical infrastructure, server rooms, restricted areas, and other organizational data.
- **Email printouts, notes, faxes, and memos**: Reveal personal details of an employee, passwords, contacts, inside working operations, certain useful instructions, and other data.
- **Policy manuals**: Reveal information regarding employment, system use, and operations.
- **Event notes, calendars, or computer use logs**: Reveal information regarding the user's log on and off timings, which helps the attacker to decide on the best time to plan their attack.

Reverse Social Engineering

Generally, reverse social engineering is difficult to carry out. This is primarily because its execution needs a lot of preparation and skills. In reverse social engineering, a perpetrator assumes the role of a knowledgeable professional so that the organization's employees ask them for information. The attacker usually manipulates questions to draw out the required information.

First, the social engineer will cause an incident, creating a problem, and then present themself as the problem solver through general conversation, encouraging employees to ask questions. For example, an employee may ask how this problem has affected files, servers, or equipment. This provides pertinent information to the social engineer. Many different skills and experiences are required to carry out this tactic successfully. Provided below are some of the techniques involved in reverse social engineering:

- **Sabotage**: Once the attacker gains access, they will corrupt the workstation or make it appear corrupted. Under such circumstances, users seek help as they face problems.

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

- **Marketing**: To ensure that the user calls the attacker, the attacker must advertise. The attacker can do this either by leaving their business card in the target's office or by placing their contact number on the error message itself.
- **Support**: Even if the attacker has already acquired the desired information, they may continue to assist the users so that they remain ignorant of the hacker's identity.

  A good example of a reverse social engineering virus is the "**My Party**" worm. This virus does not rely on sensational subject lines but rather makes use of inoffensive and realistic names for its attachments. By using realistic words, the attacker gains the user's trust, confirms the user's ignorance, and completes the task of information gathering.

Piggybacking

Piggybacking usually implies entry into a building or security area with the consent of the authorized person. For example, an attacker might request an authorized person to unlock a security door, saying that they have forgotten their ID badge. In the interest of common courtesy, the authorized person will allow the attacker to pass through the door.

Tailgating

Tailgating implies accessing a building or secured area without the consent of the authorized person. It is the act of following an authorized person through a secure entrance, as a polite user would open and hold the door for those following them. An attacker, wearing a fake badge, might attempt to enter the secured area by closely following an authorized person through a door that requires key access. They then try to enter the restricted area while pretending to be an authorized person.

Diversion Theft

Diversion theft is a technique where attackers target delivery professionals or transport companies. This technique is also known as "Round the Corner Game" or "Cornet Game." The main objective of this technique is to trick a person responsible for making a genuine delivery into delivering the consignment to the wrong location, thus interrupting the transaction. For example, if the victim is a van driver delivering a package, then that person would be persuaded to drive to a location other than the actual delivery location. Subjecting the van driver to a series of social engineering tricks thus allows the theft to be successful.

Diversion theft can also be practiced by social engineers on the Internet; victims can be persuaded to send sensitive or confidential files to some unassociated person who is not intended to receive them.

Honey Trap

The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.

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

Baiting

Baiting is a technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data. This technique relies on the curiosity and greed of the end-users. Attackers perform this technique by leaving a physical device such as a USB flash drive containing malicious files in locations where people can easily find them, such as parking lots, elevators, and bathrooms. This physical device is labeled with a legitimate company's logo, thereby tricking end-users into trusting it and opening it on their systems. Once the victim connects and opens the device, a malicious file downloads. It infects the system and allows the attacker to take control.

For example, an attacker leaves some bait in the form of a USB drive in the elevator with the label "Employee Salary Information 2019" and a legitimate company's logo. Out of curiosity and greed, the victim picks up the device and opens it up on their system, which downloads the bait. Once the bait is downloaded, a piece of malicious software installs on the victim's system, giving the attacker access.

Quid Pro Quo

Quid pro quo is a Latin phrase that meaning "something for something." In this technique, attackers keep calling random numbers within a company, claiming to be calling from technical support. This is a baiting technique where attackers offer their service to end-users in exchange of confidential data or login credentials.

For example, an attacker gathers random phone numbers of the employees of a target organization. They then start calling each number, pretending to be from the IT department. The attacker eventually finds someone with a genuine technical issue and offers their service to resolve it. The attacker can then ask the victim to follow a series of steps and to type in the specific commands to install and launch malicious files that contain malware designed to collect sensitive information.

Elicitation

Elicitation is the technique of extracting specific information from the victim by involving them in normal and disarming conversations. In this technique, attackers must possess good social skills to take advantage of professional or social opportunities to communicate with persons who have access to sensitive information. In social engineering, the purpose of elicitation is to extract relevant information to gain access to the target assets.

For example, if an attacker's objective is to obtain the victim's username and password and the conversation with them only yields things that they like, then the attacker must work more on the elicitation process to extract the relevant information.

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

Computer-based Social Engineering

Pop-Up Windows	Windows that suddenly pop up while surfing the Internet and ask for user information to login or sign-in
Hoax Letters	Emails that issue warnings to the user about new viruses, Trojans, or worms that may harm the user's system
Chain Letters	Emails that offer free gifts such as money and software on condition that the user forwards the mail to a specified number of people
Instant Chat Messenger	Gathering personal information by chatting with a selected user online to get information such as birth dates and maiden names
Spam Email	Irrelevant, unwanted, and unsolicited emails that attempt to collect financial information, social security numbers, and network information
Scareware	Malware that tricks computer users into visiting malware infested websites, or downloading/buying potentially malicious software

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

Computer-based Social Engineering

Attackers perform computer-based social engineering using various malicious programs such as viruses, trojans, and spyware, and software applications such as email and instant messaging. Discussed below are types of computer-based social engineering attacks:

- **Pop-Up Windows**

  Pop-ups trick or compel users into clicking a hyperlink that redirects them to fake web pages asking for personal information or downloading malicious programs such as keyloggers, trojans, or spyware.

  The common method of enticing a user to click a button in a pop-up window is by warning of a problem, such as displaying a realistic operating system or application error message, or by offering additional services. A window appears on the screen requesting the user to re-login or warning about an interruption in the host connection, and that the network connection needs re-authentication. When the user follows these instructions, a malicious program installs, extracts the target's sensitive information, and sends it to the attacker's email address or a remote site. This type of attack uses trojans and viruses.

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

Examples of pop-ups used for tricking users:

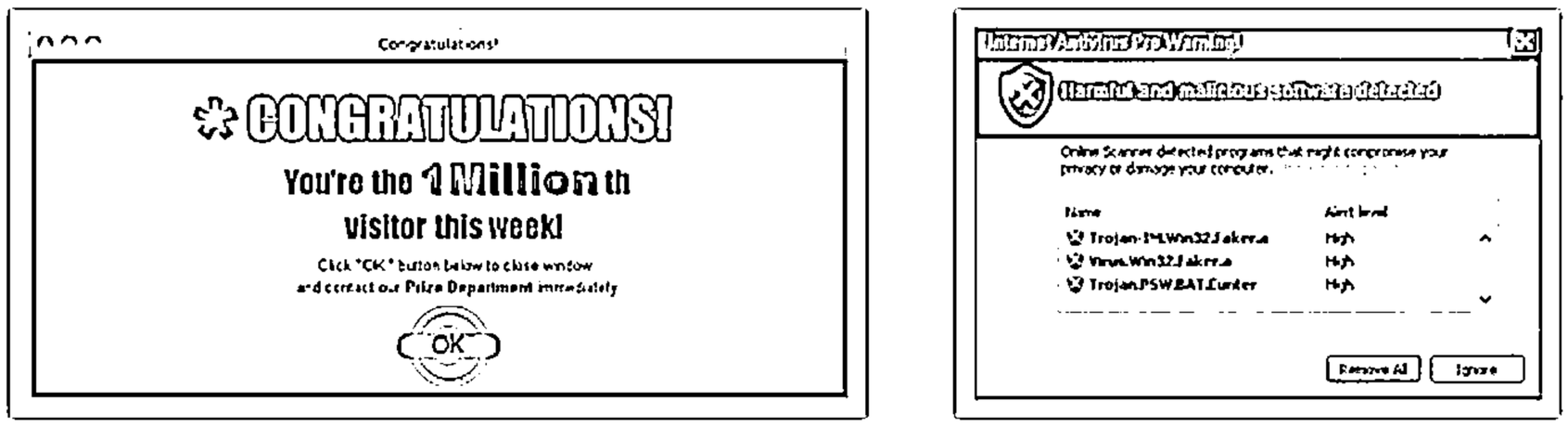


Figure 9.1: Screenshots showing sample pop-up windows

- **Hoax Letters**

  A hoax is a message warning its recipients of a non-existent computer virus threat. It relies on social engineering to spread its reach. Usually, hoaxes do not cause any physical damage or loss of information; but they cause a loss of productivity and use an organization's valuable network resources.

- **Chain Letters**

  A chain letter is a message offering free gifts, such as money and software, on the condition that the user forwards the email to a predetermined number of recipients. Common approaches used in chain letters are emotionally convincing stories, "**get-rich-quick**" pyramid schemes, spiritual beliefs, and superstitious threats of bad luck to the recipient if they "break the chain" and fail to pass on the message or simply refuse to read its content. Chain letters also rely on social engineering to spread.

- **Instant Chat Messenger**

  An attacker chats with selected online users via instant chat messengers and tries to gather their personal information such as date of birth or maiden name. They then use the acquired information to crack users' accounts.

- **Spam Email**

  Spam is irrelevant, unwanted, and unsolicited emails designed to collect financial information such as social security numbers, and network information. Attackers send spam messages to the target to collect sensitive information, such as bank details. Attackers may also send email attachments with hidden malicious programs such as viruses and trojans. Social engineers try to hide the file extension by giving the attachment a long filename.

- **Scareware**

  Scareware is a type of malware that tricks computer users into visiting malware-infested websites or downloading or buying potentially malicious software. Scareware is often seen in pop-ups that tell the target user that their machine has been infected with malware. These pop-ups convincingly appear as though they are coming from a legitimate source such as an antivirus company. Further, these pop-up ads always have a sense of urgency and tell the victim to quickly download the software if they want to get rid of the supposed virus.

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

Computer-based Social Engineering: Phishing

- Phishing is the practice of sending an illegitimate email claiming to be from a legitimate site in an attempt to acquire a user's personal or account information
- Phishing emails or pop-ups redirect users to fake webpages that mimic trustworthy sites, which ask them to submit their personal information

From:
To:
CC:
Subject: Tax Refund Notice I

Hi,
After the last annual calculations of your fiscal activity, we have determined that you are eligible to receive a tax refund of $800. Please submit the tax refund request and click here by having your tax refund sent to your bank account in due time.
Please Click "Get Started" to have your tax refund sent to your bank account, your tax refund will be sent to your bank account in due time take your time to go through the bank we have on our list
Get Started
Note: A refund can be delayed a variety of reasons, for example submitting invalid records or applying after deadline.
Best Regards
HM Revenue & Customs

Clicking the link directs you to a fraudulent web page that looks similar to a genuine HMRC page

HM Revenue & Customs

Address Information – Please enter your name and address as you have it listed for your credit card.
Cardholder Name:
Date of Birth: Day Month Year
Mother Maiden Name:
Address:
Town/City:
Postal Code:
Phone Number:
Credit Card Information – Please enter your Credit or Debit Card where refunds will be made.
Bank Name:
Debit / Credit Card Number:
Expiration Date: Month Year
Card Verification Number:
Sort Code: (If Shown On Card)
Submit Information

http://www.hmrc.gov.uk

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

Computer-based Social Engineering: Phishing (Cont'd)

Examples of Phishing Emails

From: An Attacker
Sent: Sunday, June 9, 2019 1:16:52 PM
To: User
Subject: Important changes to your account

Activity Alert
PERSONAL CHECKING/SAVINGS ACCOUNTS
Online Banking Unauthorized Sign-In.

Dear Valued Customer joeuser@mtech.edu,

As part of our security measures, our system regularly scheduled account maintenance and verification procedures, we have detected a slight error in your online banking information. Our system requires account verification for more security and protection to your account. To confirm this verification

Log Into Online Banking and update your information

Want to get more alerts? Sign in to your online banking account at Bank of America and within the Accounts Overview page select the "Alerts" tab.

You can sign in to Online or Mobile Banking to review this activity, or contact us for help.

Security Checkpoint
To confirm the authenticity of messages from us, always look for this Security Checkpoint

From: Job Student
Sent: Monday, May 13, 2019 8:57 AM
Subject: Tennessee Tech : Part Time Job

Tennessee Tech Job Placement & Student Services selected you as a Secret Shopper.

A job that will not affect your present employment or studies and no sign up fee. It's fun, rewarding and flexible. You can make up to $1000 weekly also, to view details of the job and apply please visit website

https://tinyurl.com/y3o3xzst

Job Placement & Student Services
Cookeville, TN 38505 USA

From: Compromised Account <compromised@students.tntech.edu>
Date: 6/1/19 6:31 PM (GMT-05:00)
To: <Students.tntech.edu>
Subject: The Security of Your Account

Paypal

The Security of Your Account

Dear joeuser@students.tntech.edu ,
We regret to inform you of this bad news

We have put your account in the list of limited accounts
because your account is safe and we need a little bit to a few information to protect your account

Click the button below and follow the steps simply

Yours Sincerely

Questions? Take a look at our FAQs or contact Customer Support

https://its.tntech.edu

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

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

Computer-based Social Engineering: Phishing (Cont'd)

Types of Phishing

Spear Phishing	❑ A targeted phishing attack aimed at specific individuals within an organization ❑ Attackers send spear phishing to send a message with specialized, social engineering content directed at a specific person, or a small group of people
Whaling	❑ An attacker targets high profile executives like CEOs, CFOs, politicians, and celebrities who have complete access to confidential and highly valuable information ❑ The attacker tricks the victim into revealing critical corporate and personal information through email or website spoofing
Pharming	❑ The attacker redirects web traffic to a fraudulent website by installing a malicious program on a personal computer or server ❑ Also known as "phishing without a lure", and performed by using DNS Cache Poisoning or Host File Modification
Spimming	❑ A variant of spam that exploits Instant Messaging platforms to flood spam across the networks ❑ Attacker uses bots to harvest Instant Message IDs and spread spam

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

Phishing

Phishing is a technique in which an attacker sends an email or provides a link falsely claiming to be from a legitimate site to acquire a user's personal or account information. The attacker registers a fake domain name, builds a lookalike website, and then mails the fake website's link to users. When a user clicks on the email link, it redirects them to the fake webpage, where they are lured into sharing sensitive details such as their address and credit card information. Some of the reasons behind the success of phishing scams include users' lack of knowledge, being visually deceived, and not paying attention to security indicators.

The screenshot below is an example of an illegitimate email that claims to be from a legitimate sender. The email link redirects users to a fake webpage and asks them to submit their personal or financial details.

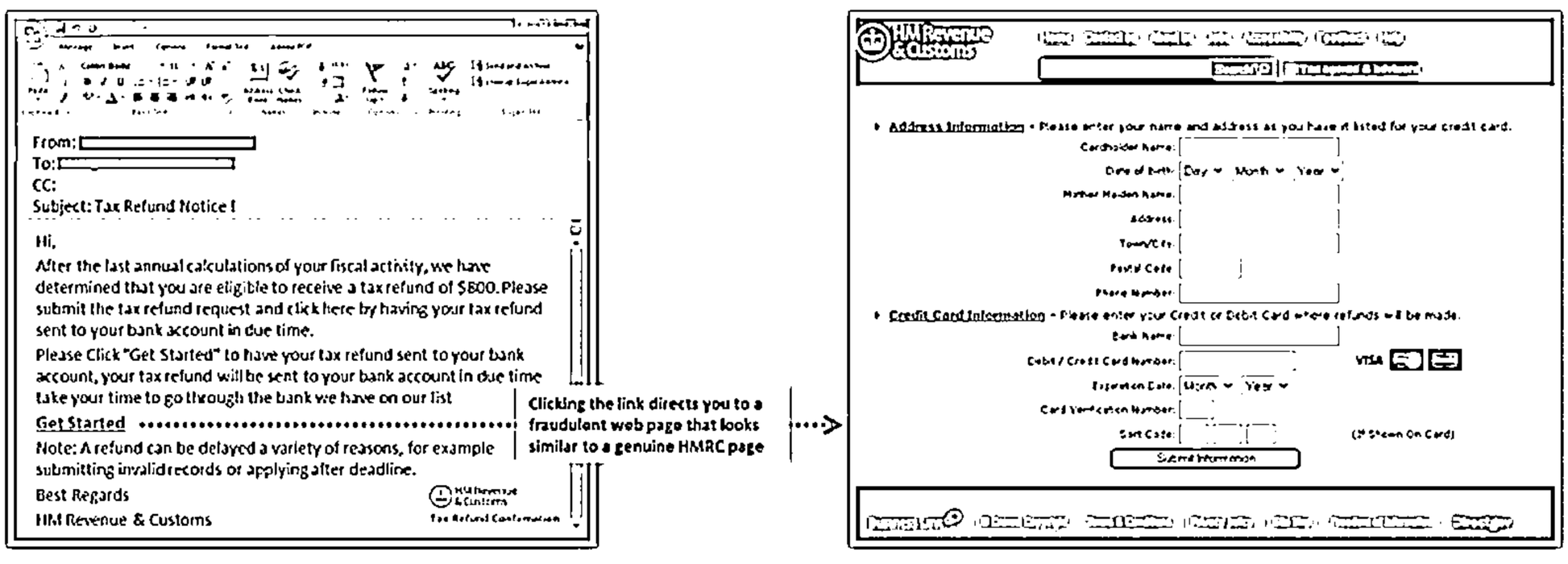


Figure 9.2: Screenshot showing the phishing technique

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

Examples of Phishing Emails

Source: *https://its.tntech.edu*

Today, most people use internet banking. Many people use Internet banking for all their financial needs, such as online share trading and e-commerce. Phishing involves fraudulently acquiring sensitive information (like passwords and credit card details) by masquerading as a trusted entity.

The target receives an email that appears to be from the bank and requests the user to click on the URL or the link provided. If the user is tricked and provides their username, password, and other information, then the site forwards the information to the attacker, who will use it for nefarious purposes.

From: An Attacker
Sent: Sunday, June 9, 2019 1:16:52 PM
To: User
Subject: Important changes to your account

Activity Alert
PERSONAL CHECKING/SAVINGS ACCOUNTS
Online Banking Unauthorized Sign-In.

Dear Valued Customer **joeuser@tntech.edu,**

As part of our security measures, our system regularly scheduled account maintenance and verification procedures, we have detected a slight error in your online banking information. Our system requires account verification for more security and protection to your account , To confirm this verification

Log into Online Banking and update your information.

Want to get more alerts? Sign in to your online banking account at Bank of America and within the Accounts Overview page select the "Alerts" tab.

You can sign in to Online or Mobile Banking to review this activity, or contact us for help.

Security Checkpoint

To confirm the authenticity of messages from us, always look for this Security Checkpoint.

Figure 9.3: Screenshot showing a phishing email

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

From: Compromised Account <compromised@students.tntech.edu>
Date: 6/1/19 6:31 PM (GMT-05:00)
To: <[illegible]t@students.tntech.edu>
Subject: The Security of Your Account

Paypal

The Security of Your Account

Dear joebstudent@students.tntech.edu ,
We regret to inform you of this bad news

We have put your account in the list of limited accounts
because your account is safe and we need a little bit to a few information to protect your account

Click the button below and follow the steps simply

Yours Sincerely

Confirm

Questions? Take a look at our FAQs or contact Customer Support.

Figure 9.4: Screenshot showing a phishing email

From: Joe B Student
Sent: Monday, May 13, 2019 8:57 AM
Subject: Tennessee Tech : Part Time Job

Tennessee Tech Job Placement & Student Services selected you as a Secret Shopper.

A job that will not affect your present employment or studies and no sign up fee. It's fun, rewarding and flexible. You can make up to $1000 weekly also, to view details of the job and apply please visit website

https://tinyurl.com/y3o3xzst

Job Placement & Student Services
Cookeville, TN 38505 USA

Figure 9.5: Screenshot showing a phishing email

Types of Phishing

- **Spear Phishing**

  Instead of sending out thousands of emails, some attackers opt for "**spear phishing**" and use specialized social engineering content directed at a specific employee or small group of employees in an organization to steal sensitive data such as financial information and trade secrets.

  Spear phishing messages seem to come from a trusted source with an official-looking website. The email also appears to be from an individual from the recipient's company, generally someone in a position of authority. In reality, the message is sent by an attacker attempting to obtain critical information about a specific recipient and their organization, such as login credentials, credit card details, bank account numbers,

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

passwords, confidential documents, financial information, and trade secrets. Spear phishing generates a higher response rate compared to a normal phishing attack, as it appears to be from a trusted company source.

- **Whaling**

  A whaling attack is a type of phishing that targets high profile executives like CEO, CFO, politicians, and celebrities who have complete access to confidential and highly valuable information. It is a social engineering trick in which the attacker tricks the victim into revealing critical corporate and personal information (like bank account details, employee details, customer information, and credit card details), generally, through email or website spoofing. Whaling is different from a normal phishing attack; the email or website used for the attack is carefully designed, usually targeting someone in the executive leadership.

- **Pharming**

  Pharming is a social engineering technique in which the attacker executes malicious programs on a victim's computer or server, and when the victim enters any URL or domain name, it automatically redirects the victim's traffic to an attacker-controlled website. This attack is also known as "Phishing without a Lure." The attacker steals confidential information like credentials, banking details, and other information related to web-based services.

  Pharming attack can be performed in two ways: DNS Cache Poisoning and Host File Modification

  DNS Cache Poisoning:

  - The attacker performs DNS Cache Poisoning on the targeted DNS server.
  - The attacker modifies the IP address of the target website "www.targetwebsite.com" to that of a fake website "www.hackerwebsite.com."
  - When the victim enters the target website's URL in the browser's address bar, a request is sent to the DNS server to obtain the IP address of the target website.
  - The DNS server returns a fake IP address that is already modified by the attacker.
  - Finally, the victim is redirected to the fake website.

  Host File Modification:

  - An attacker sends a malicious code as an email attachment.
  - When the user clicks on the attachment, the code executes and modifies local host files on the user's computer.
  - When the victim enters the target website's URL in the browsers address bar, the compromised host file automatically redirects the user's traffic to the fraudulent website controlled by the hacker.

  Pharming attacks can also be performed using malware like Trojan horses or worms.

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

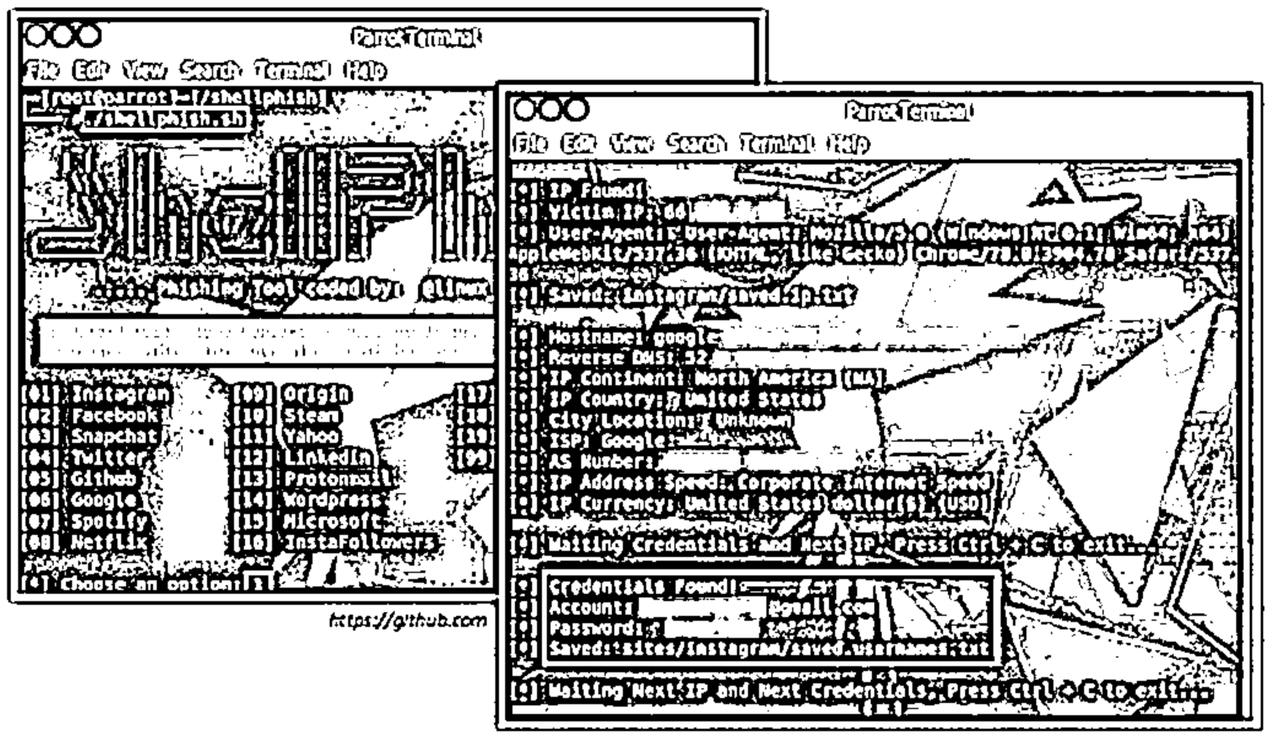
- **Spimming**

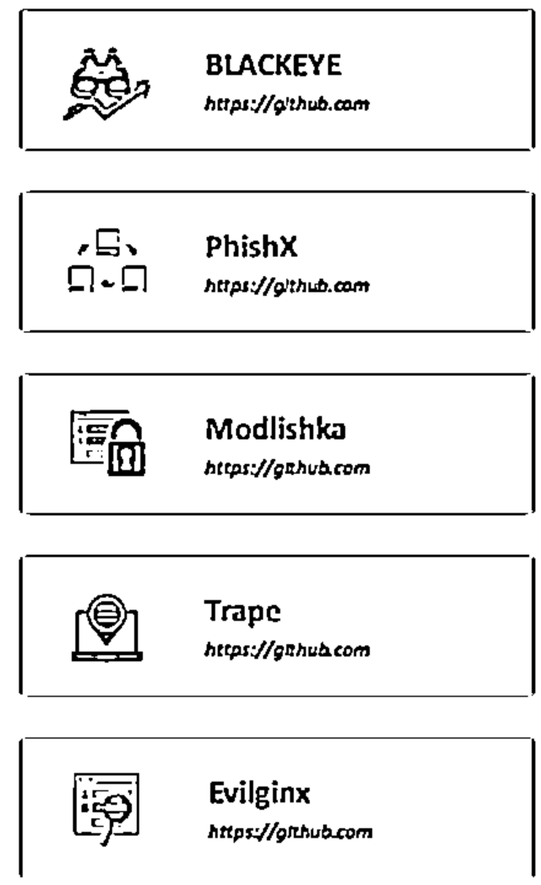
  SPIM (Spam over Instant Messaging) exploits Instant Messaging platforms and uses IM as a tool to spread spam. A person who generates spam over IM is called Spimmer. Spimmers generally make use of bots (an application that executes automated tasks over the network) to harvest Instant Message IDs and forward spam messages to them. SPIM messages, like email spam, generally include advertisements and malware as an attachment or embedded hyperlink. The user clicks the attachment and is redirected to a malicious website that collects financial and personal information like credentials, bank account, and credit card details.

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

Phishing Tools

ShellPhish	ShellPhish is a phishing tool used to phish user credentials from various social networking platforms such as Instagram, Facebook, Twitter, LinkedIn, etc.





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

Phishing Tools

Phishing tools can be used by attackers to generate fake login pages to capture usernames and passwords, send spoofed emails, and obtain the victim's IP address and session cookies. This information can further be used by the attacker, who will use it to impersonate a legitimate user and launch further attacks on the target organization.

- **ShellPhish**

  Source: *https://github.com*

  ShellPhish is a phishing tool used to phish user credentials from various social networking platforms such as Instagram, Facebook, Twitter, and LinkedIn. It also displays the victim system's public IP address, browser information, hostname, geolocation, and other information.

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

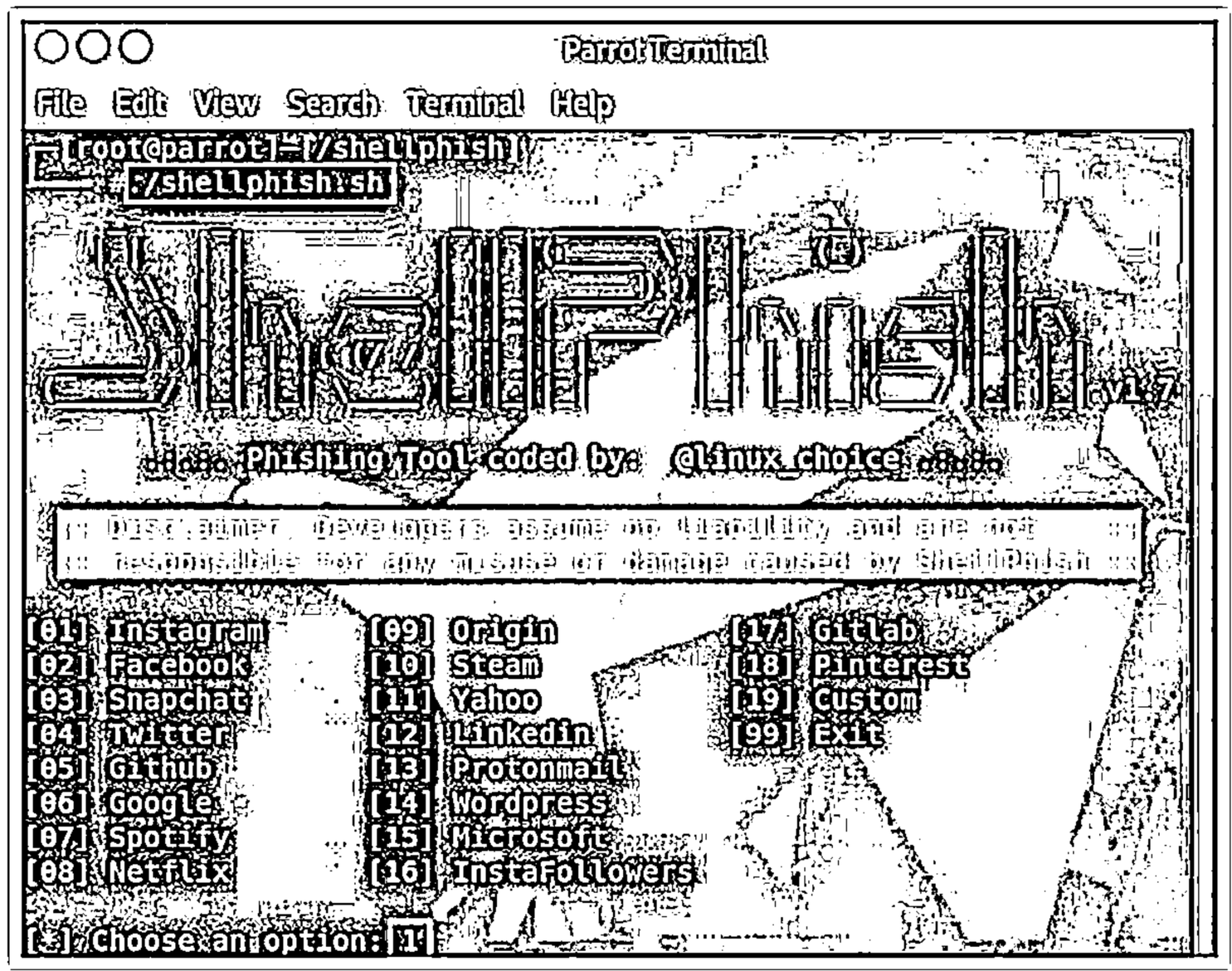


Figure 9.6: Screenshot of ShellPhish

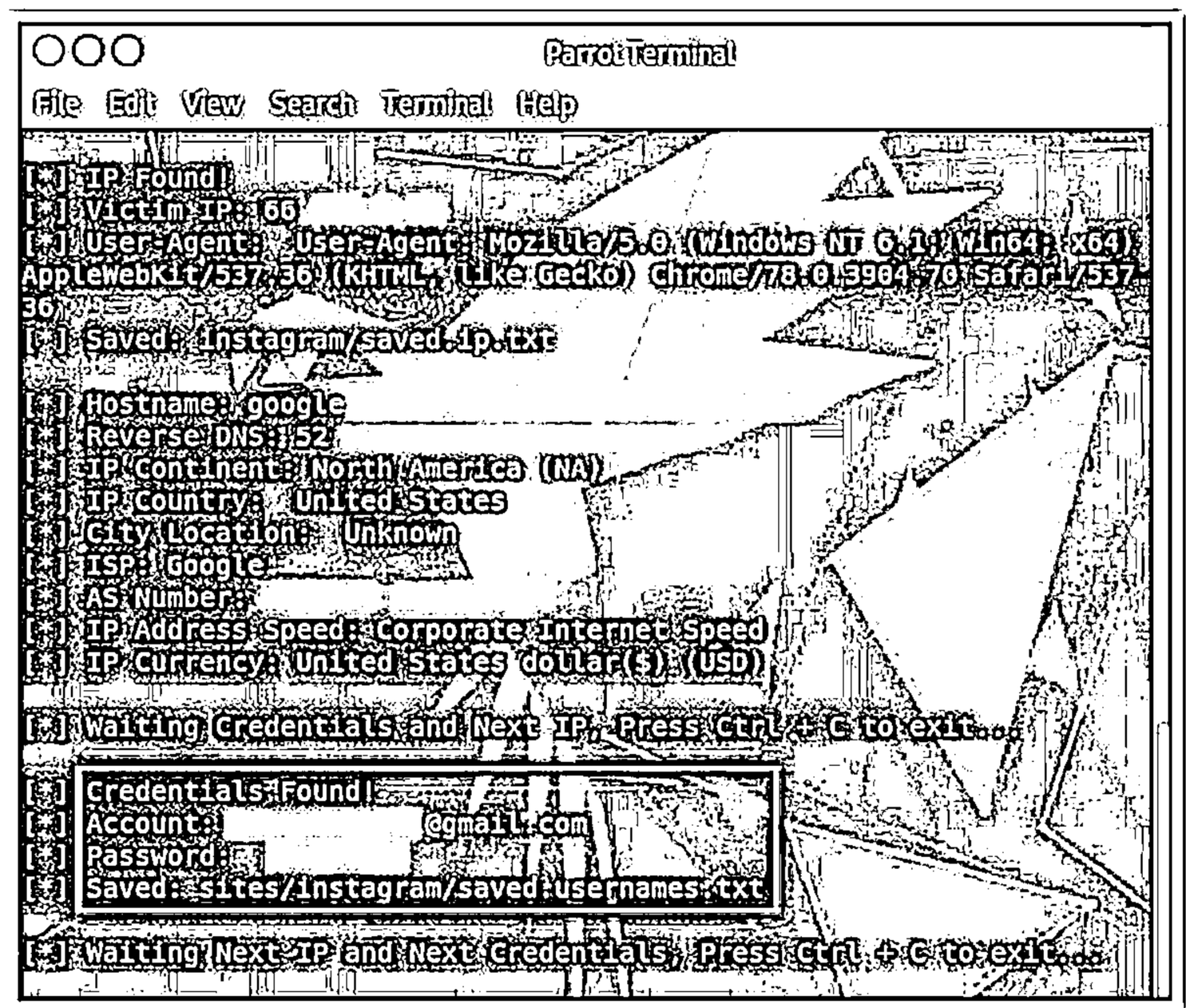


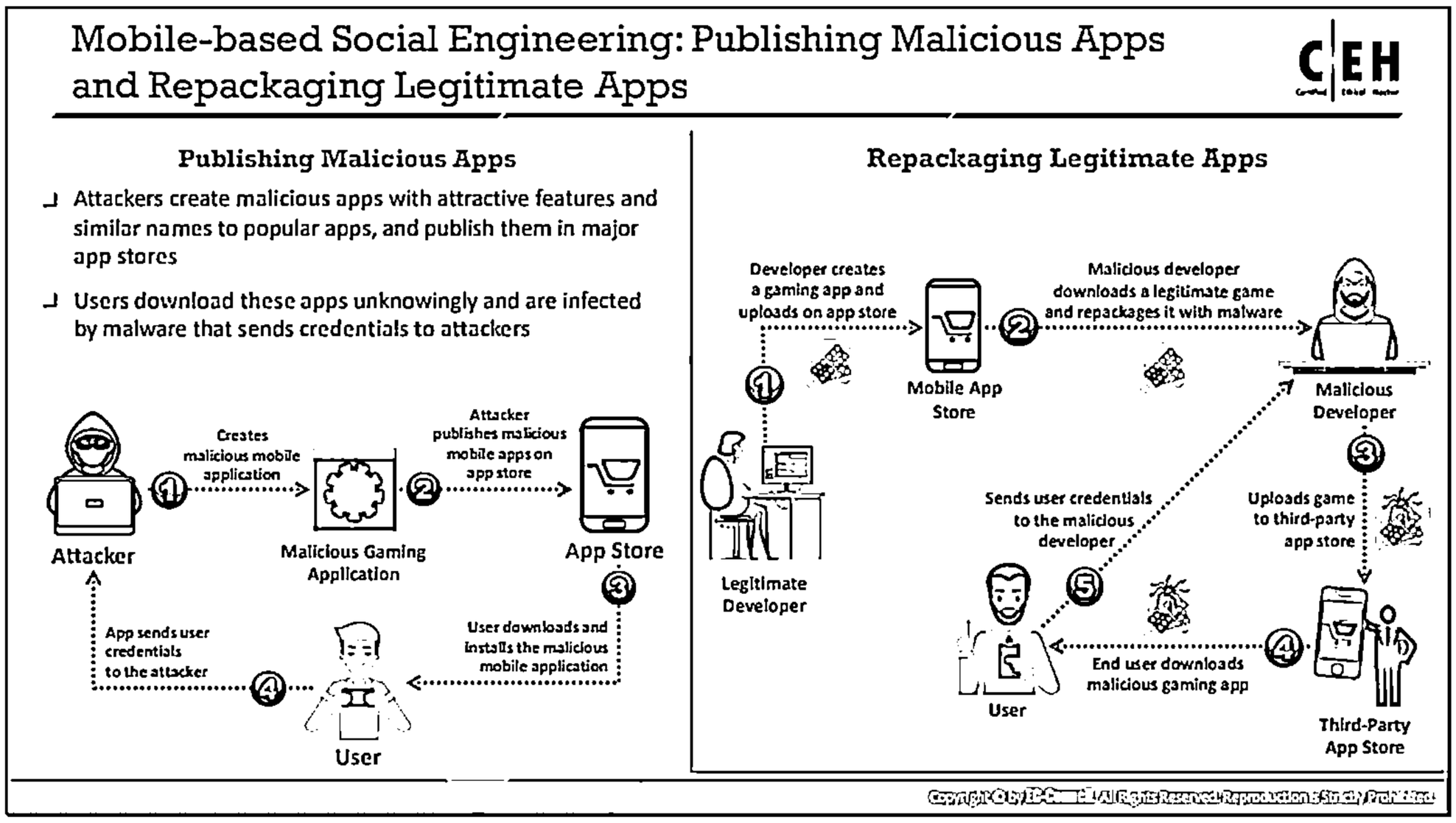
Figure 9.7: Screenshot showing the output of ShellPhish

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

Some additional phishing tools are listed below:

- BLACKEYE (*https://github.com*)
- PhishX (*https://github.com*)
- Modlishka (*https://github.com*)
- Trape (*https://github.com*)
- Evilginx (*https://github.com*)

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



Mobile-based Social Engineering

Publishing Malicious Apps

In mobile-based social engineering, the attacker performs a social engineering attack using malicious mobile apps. The attacker first creates the malicious application — such as a gaming app with attractive features — and publishes it on major application stores using the popular names. Unaware of the malicious application, a user will download it onto their mobile device, believing it to be genuine. Once the application is installed, the device is infected by malware that sends the user's credentials (usernames, passwords), contact details, and other information to the attacker.

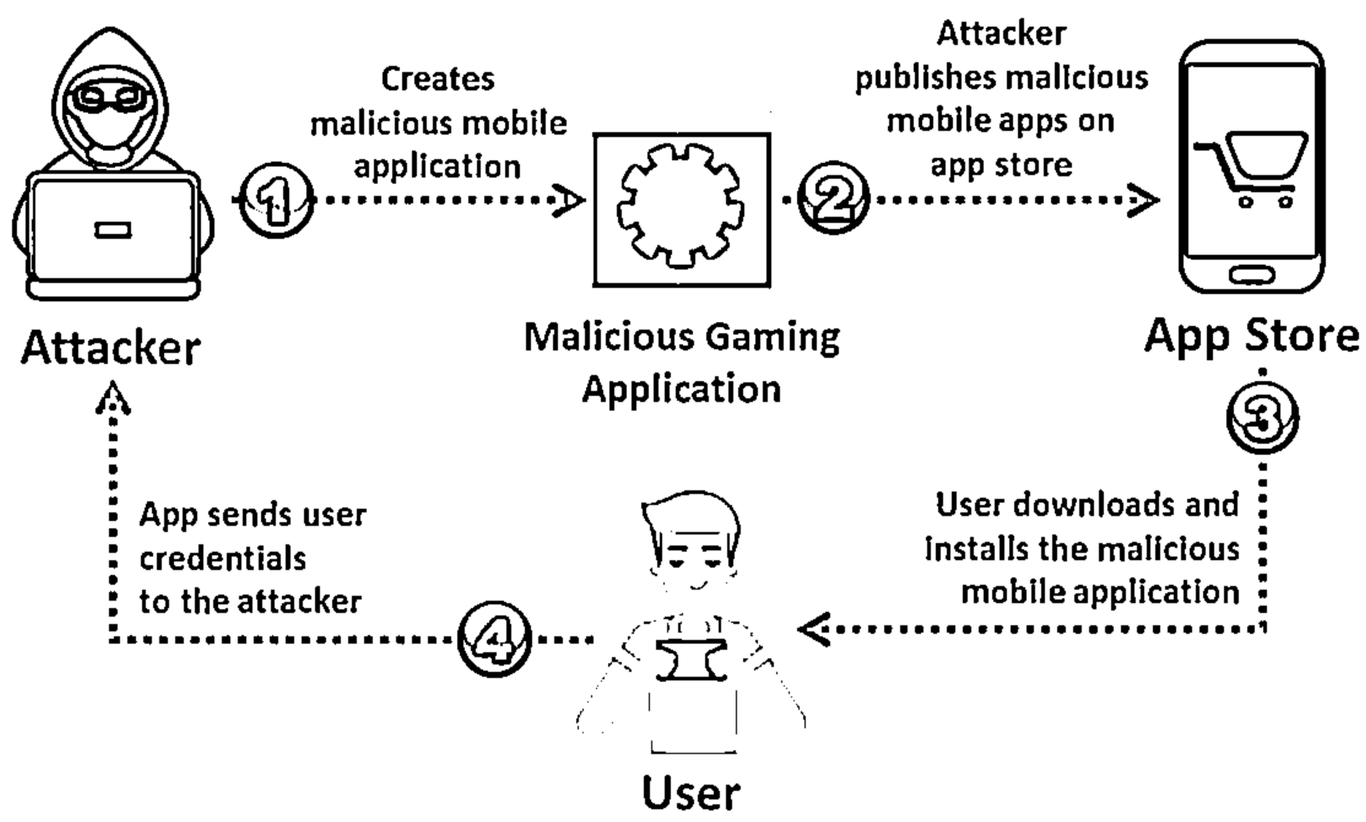


Figure 9.8: Publishing malicious apps

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

Repackaging Legitimate Apps

Sometimes malware can be hidden within legitimate apps. A legitimate developer creates legitimate gaming applications. Platform vendors create centralized marketplaces to allow mobile users to conveniently browse and install these games and apps. Usually, developers submit gaming applications to these marketplaces, making them available to thousands of mobile users. A malicious developer downloads a legitimate game, repackages it with malware, and uploads it to the third-party application store. Once a user downloads the malicious application, the malicious program installed on the user's mobile device collects the user's information and sends it to the attacker.

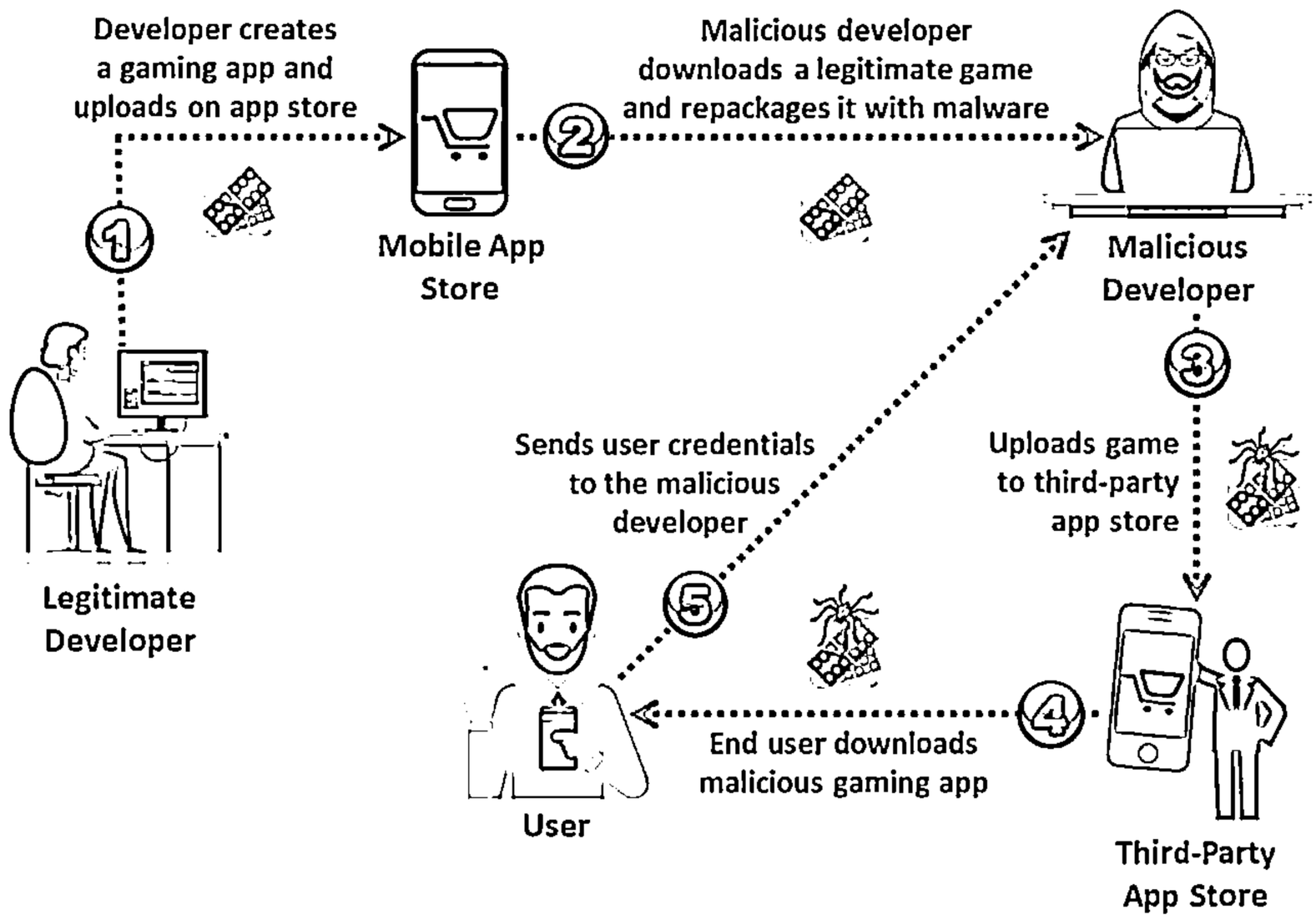
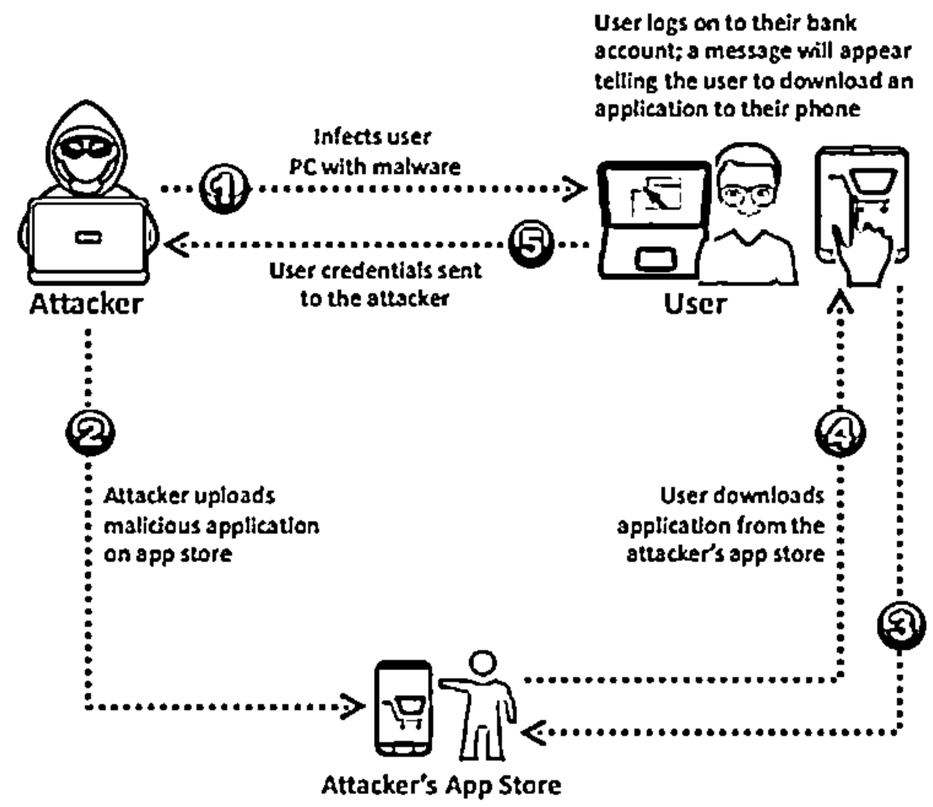


Figure 9.9: Repackaging legitimate apps

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

Mobile-based Social Engineering: Fake Security Applications

1. Attacker infects the victim's PC
2. Attacker uploads a malicious app to an app store
3. Victim logs into his or her bank account. Malware in the system displays a pop-up message telling the victim to download an app onto his or her phone to receive security messages
4. Victim downloads the malicious app on his or her phone
5. At this point, the attacker can access two-factor authentication information sent to the victim from the bank via SMS



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

Fake Security Applications

Attackers may send a fake security application to perform mobile-based social engineering. In this attack, the attacker first infects the victim's computer by sending something malicious. They then upload a malicious application to an app store. When the victim logs on to their bank account, malware in the system displays a pop-up message telling the victim that they need to download an application on their phone to receive a message from security. The victim downloads the application from the attacker's app store, believing they are downloading a genuine app. Once the user downloads the application, the attacker obtains confidential information such as bank account login credentials (username and password), whereupon a second authentication is sent by the bank to the victim via SMS. Using that information, the attacker accesses the victim's bank account.

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

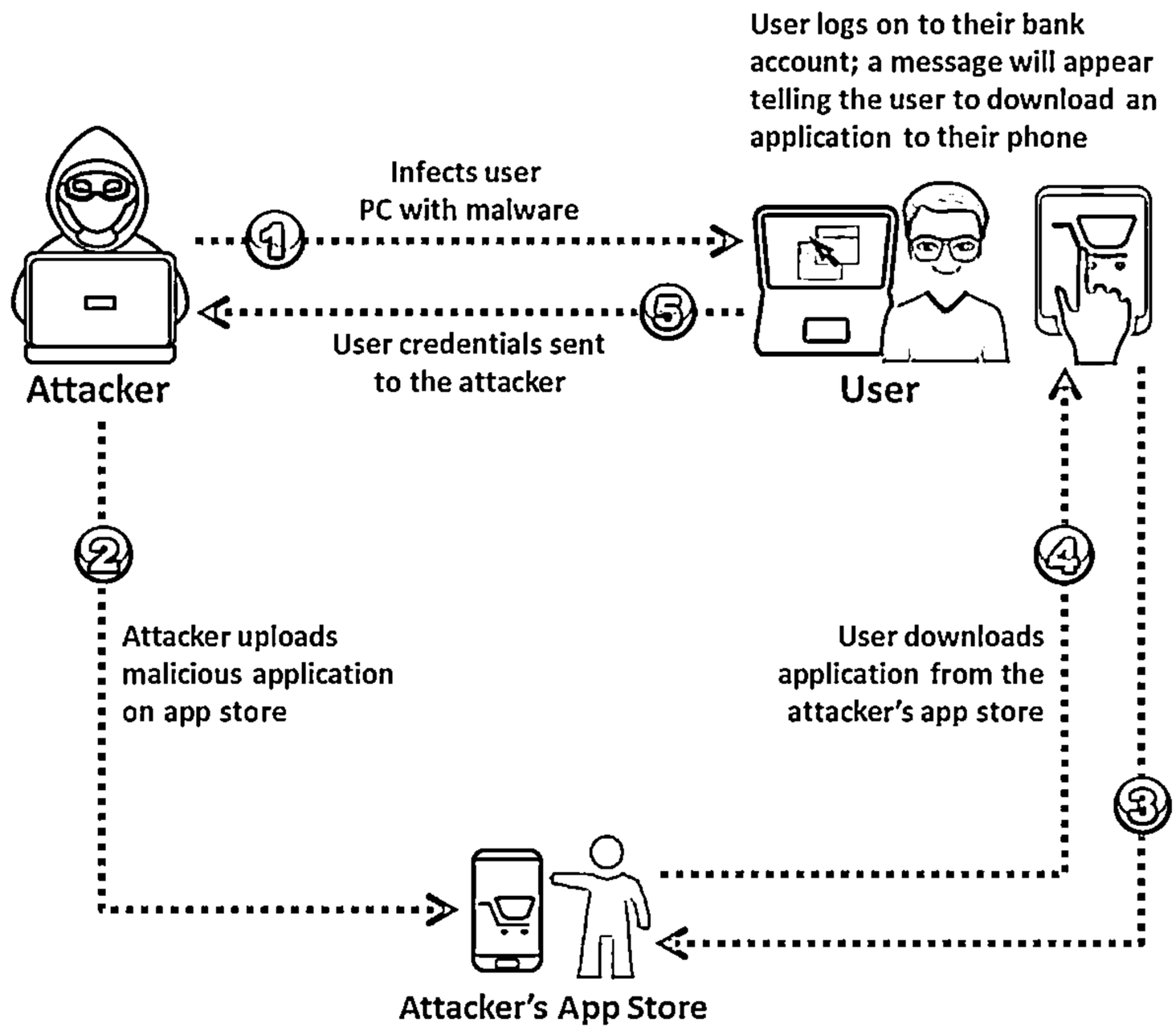


Figure 9.10: Fake security applications

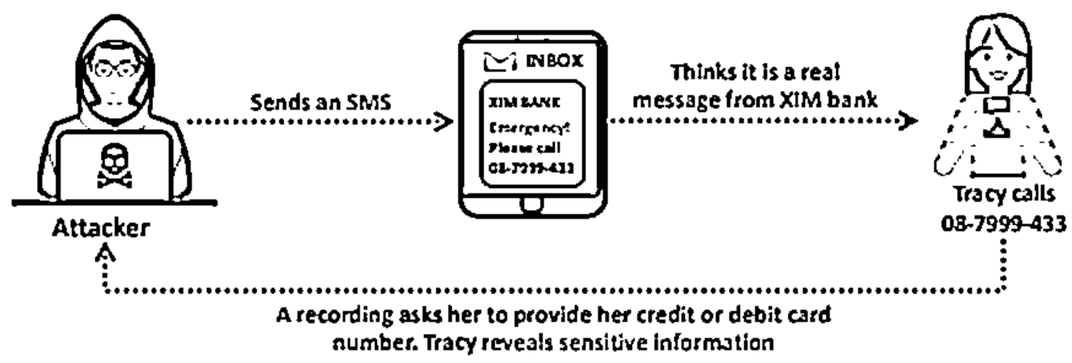
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile-based Social Engineering: SMiShing (SMS Phishing)

- SMiShing (SMS phishing) is the act of using SMS text messaging system of cellular phones or other mobile devices to lure users into instant action, such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number
- SMiShing messages are generally crafted to provoke an instant action from the victim, requiring them to divulge their personal information and account details

SMiShing Example

1. Tracy receives an SMS (text message), ostensibly from the security department at XIM Bank
2. It claims to be urgent and instructs Tracy to call the phone number in the SMS immediately
3. Worried, she calls, thinking it is an XIM Bank customer service number. She hears a recording asking her to provide her credit or debit card number
4. Tracy reveals the sensitive information due to the fraudulent texts



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

SMiShing (SMS Phishing)

Sending SMS is another technique used by attackers in performing mobile-based social engineering. In SMiShing (SMS Phishing), the SMS text messaging system is used to lure users into taking instant action such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number. SMiShing messages are crafted to provoke an instant action from the victim, requiring them to divulge their personal information and account details.

Consider Tracy, a software engineer working in a reputed company. She receives an SMS ostensibly from the security department of XIM Bank. It claims to be urgent, and the message says that Tracy should call the phone number listed in the SMS immediately. Worried, she calls to check on her account, believing it to be an authentic XIM Bank customer service phone number. A recorded message asks her to provide her credit or debit card number, as well as her password. Tracy believes it is a genuine message and shares sensitive information.

Sometimes a message claims that the user has won money or has been randomly selected as a lucky winner and that they merely need to pay a nominal fee and share their email address, contact number, or other information.

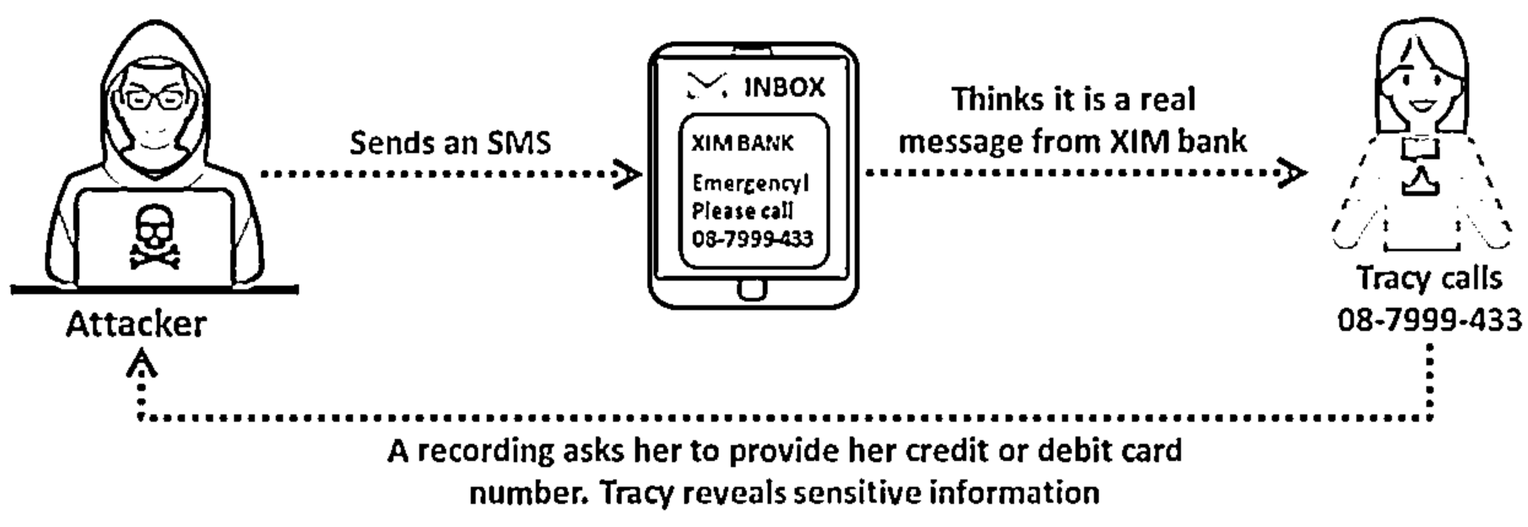


Figure 9.11: SMiShing (SMS Phishing)

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

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures

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

Insider Threats/Insider Attacks

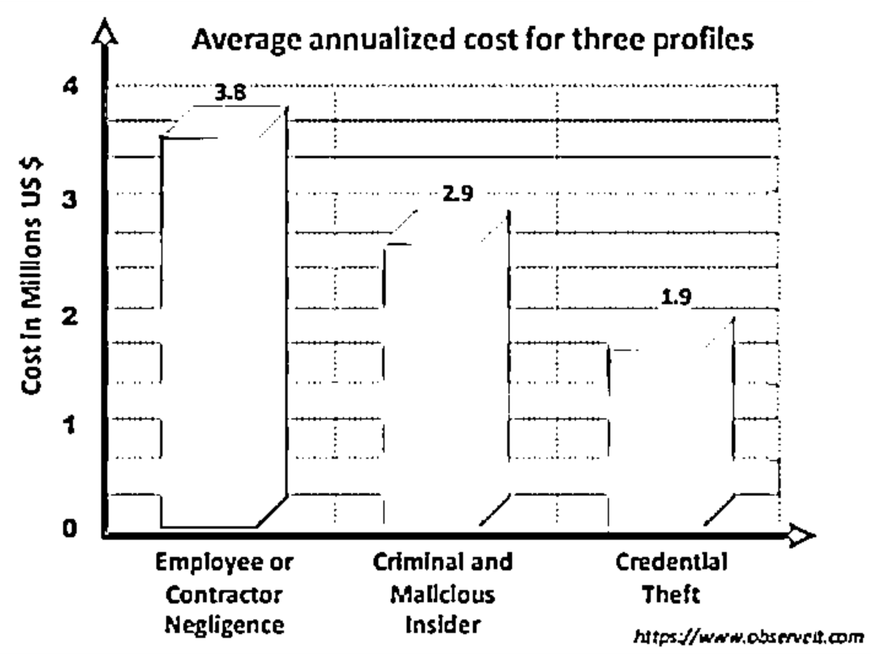
- An insider is any employee (trusted person or people) who have access to critical assets of an organization
- An insider attack involves using privileged access to intentionally violate rules or cause threat to the organization's information or information systems in any form
- Such attacks are generally performed by a privileged user, disgruntled employee, terminated employee, accident-prone employee, third party, undertrained staff, etc.

Reasons for Insider Attacks

- Financial gain
- Steal confidential data
- Revenge
- Become future competitor
- Perform competitor's bidding
- Public announcement

Insider Threat Statistics

According to a 2018 Cost of Insider Threats Study, an attack performed by employee or contractor negligence is costlier than criminal or malicious insider attacks and credential theft



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

Insider Threats

An insider is any employee (trusted person) who has access to the critical assets of an organization. An insider attack involves using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. Insider attacks may cause great loss to the company. Further, they are dangerous because they are easy to launch and difficult to detect.

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

Insider attacks are generally performed by:

- **Privileged Users**: Attacks may come from the most trusted employees of the company, such as managers and system administrators, who have access to the company's confidential data and a higher probability of misusing the data, either intentionally or unintentionally.
- **Disgruntled Employees**: Attacks may come from unhappy employees or contract workers. Disgruntled employees, who intend to take revenge on the company, first acquire information and then wait for the right time to compromise the organization's resources.
- **Terminated Employees**: Some employees take valuable information about the company with them when terminated. These employees access the company's data after termination using backdoors, malware, or their old credentials if they are not disabled.
- **Accident-Prone Employees**: If an employee accidentally loses their mobile device, sends an email to incorrect recipients, or leaves a system loaded with confidential data logged-in, it can lead to unintentional data disclosure.
- **Third Parties**: Third parties, like remote employees, partners, dealers, and vendors, have access to the company's information. However, the security of their systems is unpredictable and could be a source of information leaks.
- **Undertrained Staff**: A trusted employee becomes an unintentional insider due to a lack of cybersecurity training. They fail to adhere to cybersecurity policies, procedures, guidelines, and best practices.

Companies in which insider attacks are common include credit card companies, health-care companies, network service providers, as well as financial and exchange service providers.

Reasons for Insider Attacks

- **Financial Gain**

  An attacker performs an insider attack mainly for financial gain. The insider sells the company's sensitive information to its competitor, steals a colleague's financial details for personal use, or manipulates the company's financial records or that of its personnel.

- **Steal Confidential Data**

  A competitor may inflict damage upon the target organization, steal critical information, or even put them out of business just by finding a job opening, preparing someone to get through the interview, and having that person hired by the competitor.

- **Revenge**

  It only takes one disgruntled person to seek revenge, and the company is compromised. Attacks may come from unhappy employees or contract workers with negative opinions about the company.

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

- **Become Future Competitor**

  Current employees may plan to start their own competing business and, by using the company's confidential data, these employees may access the system to steal or alter the company's client list.

- **Perform Competitors Bidding**

  Due to corporate espionage, even the most honest and trustworthy employees can be coerced into revealing the company's critical information through bribery or blackmail.

- **Public Announcement**

  A disgruntled employee may want to make a political or social statement and so leaks or damages the company's confidential data.

Insider Threat Statistics

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

Although malicious intent is a serious factor for organizational security, according to a 2018 Cost of Insider Threats Study, an attack caused by employee or contractor negligence is costlier than theft and credential theft by a criminal or malicious insider:

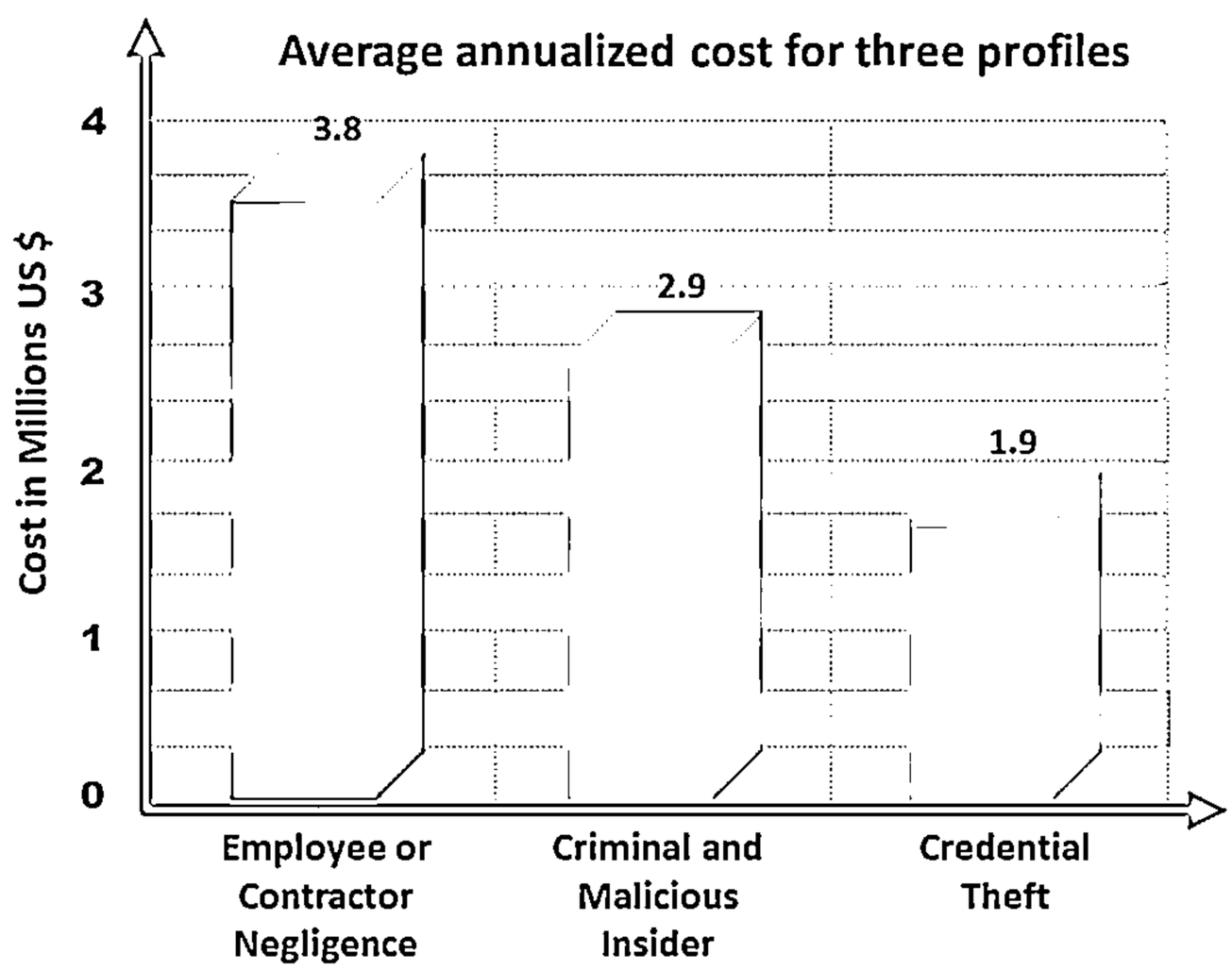


Figure 9.12: Graph Showing Insider Threat Statistics

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

Types of Insider Threats

Malicious Insider	A disgruntled or terminated employee who steals data or destroys the company's networks intentionally by introducing malware into the corporate network
Negligent Insider	Insiders who are uneducated on potential security threats or who simply bypass general security procedures to meet workplace efficiency
Professional Insider	Harmful insiders who use their technical knowledge to identify weaknesses and vulnerabilities in the company's network and sell confidential information to competitors or black market bidders
Compromised Insider	An insider with access to critical assets of an organization who is compromised by an outside threat actor

Why are Insider Attacks Effective?

- Easy to launch
- Prevention is difficult
- Succeed easily
- Employees can easily cover their tracks
- Differentiating harmful actions from the employee's regular work is very difficult
- Can go undetected for years and remediation is very expensive

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

Types of Insider Threats

There are four types of insider threats. They are:

- **Malicious Insider**

  Malicious insider threats come from disgruntled or terminated employees who steal data or destroy company networks intentionally by injecting malware into the corporate network.

- **Negligent Insider**

  Insiders, who are uneducated on potential security threats or simply bypass general security procedures to meet workplace efficiency, are more vulnerable to social engineering attacks. Many insider attacks result from employee's laxity towards security measures, policies, and practices.

- **Professional Insider**

  Professional insiders are the most harmful insiders. They use their technical knowledge to identify weaknesses and vulnerabilities in the company's network and sell the organization's confidential information to competitors or black-market bidders.

- **Compromised Insider**

  An outsider compromises an insider who has access to the critical assets or computing devices of an organization. This type of threat is more difficult to detect since the outsider masquerades as a genuine insider.

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

Why are Insider Attacks Effective?

Insider attacks are effective because:

- Insider attacks can go undetected for years, and remediation is expensive.
- Insider attacks are easy to launch.
- Preventing insider attacks is difficult; an inside attacker can easily succeed
- It is very difficult to differentiate harmful actions from the employee's regular work. It is hard to identify whether employees are performing malicious activities or not.
- Even after malicious activity is detected, the employee may refuse to accept responsibility and claim it was a mistake.
- It is easy for employees to cover their actions by editing or deleting logs to hide their malicious activities.

Example of Insider Attack: Disgruntled Employee

Most cases of insider abuse can be traced to individuals who are introverts, incapable of managing stress, experiencing conflict with management, frustrated with their job or office politics, craving respect or promotion, transferred, demoted, or issued an employment termination notice, among other reasons. Disgruntled employees may pass company secrets and intellectual property to competitors for monetary gain, thus harming the organization.

Disgruntled employees can use steganography programs to hide company secrets and later send the information to competitors as an innocuous-looking message such as a picture, image, or sound file using a work email account. No one suspects them because the attacker hides the stolen sensitive information in the picture or image file.

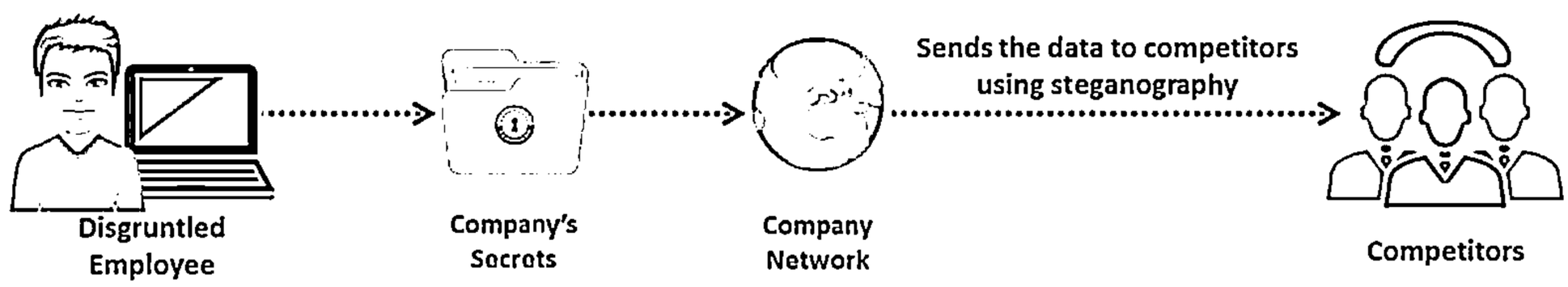


Figure 9.13: Example of Insider Attack — Disgruntled Employee

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

Behavioral Indications of an Insider Threat

1. Data exfiltration alerts
2. Missing or modified network logs
3. Changes in network usage patterns
4. Multiple failed login attempts
5. Behavioral and temperament changes
6. Unusual time and location of access
7. Missing or modified critical data
8. Unauthorized downloading or copying of sensitive data
9. Logging of different user accounts from different systems
10. Temporal changes in revenue or expenditure
11. Unauthorized access to physical assets
12. Increase or decrease in productivity of employee
13. Inconsistent working hours
14. Unusual business activities

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

Behavioral Indications of an Insider Threat

Indicators of insider threats are generally abnormal user activities that deviate from regular work activities. These represent unusual patterns of user behavior that require further analysis to identify malicious motives and intents. The most common indicator of insider threat is a lack of employee awareness about security measures.

The following are various behavioral indicators of insider threats:

- **Alerts of Data Exfiltration**

  Alerts of the unauthorized gathering and transmission of data on the network can represent an insider or malware attack. Insiders can also use paper, fax machines, hard drives, portable devices, and other computing equipment to gather and transfer sensitive data.

- **Missing or Modified Network Logs**

  Insiders try to access the log files to delete, modify, and edit unauthorized access events, file transfer logs, and other records from systems and network devices to avoid detection. Alerts of log modification, deletion, or access can indicate attacks.

- **Changes in Network Usage Patterns**

  Changes in the network patterns of the network-specific protocols, size of the packets, sources and destinations, frequency of user application sessions, and bandwidth usage can indicate malicious activity.

- **Multiple Failed Login Attempts**

  The insider can try to log in to unauthorized systems or applications by brute-force. So, multiple failed attempts may indicate an insider threat.

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

- **Behavioral and Temporal Changes**

  Deviation from established behavior and temporal changes in employee behavior such as spending capacity, frequent travel, anger management issues, constant quarrels with colleagues, and lethargy in performing work are some of the fraud indicators.

- **Unusual Time and Location of Access**

  Any mismatch in the timeline of an event can be suspicious and may indicate an insider threat. For example, if activities are logged on employee systems in their absence.

- **Missing or Modified Critical Data**

  Disgruntled employees can modify or delete sensitive data to damage the reputation of the organization.

- **Unauthorized Download or Copying of Sensitive Data**

  Insiders use legitimate and malicious tools to extract data from the organization's perimeter. Insiders can install malware, trojans, and backdoors to steal information.

- **Sending Sensitive Information to Personal Email Account**

  Insiders may send critical organizational information to their personal email accounts with malicious intent.

- **Logging of Different User Accounts from Different Systems**

  Unusual times of access combined with a change in the IP address of the system used to log into the account may represent malicious activities.

- **Temporal Changes in Revenue or Expenditure**

  Unexpected and unexplained changes in the financial status of an employee signify an income generated from external sources. The organization should audit their financial reports to identify whether the employee was involved in any malicious activities.

- **Unauthorized Access to Physical Assets**

  Activities such as employees using authorized assets without authentication, trying to escalate their privileges beyond their job requirements, or trying to gain physical access to the assets can represent a threat.

- **Increase or Decrease in Productivity of Employee**

  Employees who are unproductive, threatening, have legitimate or illegitimate job concerns, and disagree with intellectual property rights tend to be suspicious. A sudden increase or decrease in their productivity can signify suspicious behavior.

- **Inconsistent Working Hours, Unusual Business Activities, and Concealed or Frequent Foreign Trips**

  Employees with suspicious business activities like unusual login times, unusual office hours, unauthorized browsing and downloads, concealed trips abroad, and meetings with representatives from other countries or organizations may pose a threat to the organization.

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

- **Extreme Behavior Due to Mental Instability**

  Some employees possess unpredictable and extreme behavior, such as kleptomania, and a sudden change in behavior may be due to mental instability. This raises the probability that they will perform financial fraud, data theft, or physical theft.

- **Signs of vulnerability (Such as Drug or Alcohol Abuse, Financial Difficulties, Gambling, Illegal Activities)**

  Employees with bad habits such as drugs, gambling, and alcohol abuse, and relationship issues, may take a chance to breach the organization's data for money. Organizations must regularly monitor the activities of such employees.

- **Complaint on Sensitive Data Leak**

  Information or complaints regarding sensitive data leaks can represent an insider attack. Check for customer reviews and concerns to identify anomalies and analyze them to identify the insider.

- **Abnormal Access of Systems and User Accounts**

  The mismatch between the systems assigned and user accounts used to access the systems may indicate an insider threat.

- **Irresponsible Social Media Behavior**

  Insiders may attempt to create a negative impact on the organization by posting unnecessary information on social media websites.

- **Attempt to Access Restricted Zones**

  Employees with malicious intent may try to access restricted areas of the organization to collect sensitive information.

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

Module Flow

1 Social Engineering Concepts

2 Social Engineering Techniques

3 Insider Threats

4 Impersonation on Social Networking Sites

5 Identity Theft

6 Countermeasures

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

Impersonation on Social Networking Sites

Today social networking sites are widely used by many people that allow them to build online profiles, share information and media such as pictures, blog entries, and music clips. Thus, it is relatively easier for an attacker to impersonate someone. The victim is likely to trust the attacker and eventually reveal information that would help them gain access to the system.

This section describes how attackers perform social engineering through impersonation using various social networking sites such as Facebook, LinkedIn, and Twitter, and highlights the risks these sites pose to corporate networks.

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

Social Engineering through Impersonation on Social Networking Sites

Attacker

- Organization Details
- Professional Details
- Contacts and Connections
- Personal Details

- Malicious users gather confidential information from social networking sites and create accounts using another person's name
- Attackers use these fraudulent profiles to create large networks of friends and extract information using social engineering techniques
- Attackers attempt to join the target organization's employee groups where personal and company information is shared
- Attackers may can also use collected information to carry out other forms of social engineering attacks

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

Social Engineering through Impersonation on Social Networking Sites

As social networking sites such as Facebook, Twitter, and LinkedIn are widely used, attackers coopt them as a vehicle for impersonation. There are two ways an attacker can perform impersonation on social networking sites:

- By creating a fictitious profile of the victim on the social media site
- By stealing the victim's password or indirectly gaining access to the victim's social media account

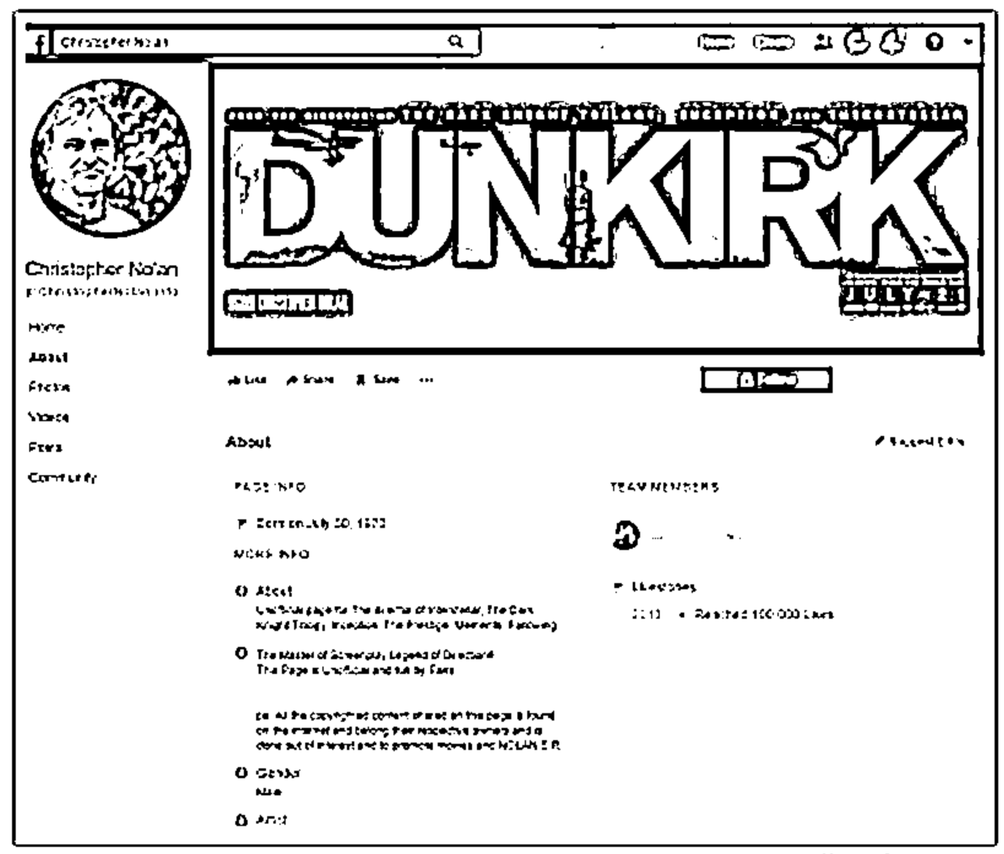
Social networking sites are a treasure trove for attackers because people share their personal and professional information on these sites, such as name, address, mobile number, date of birth, project details, job designation, company name, and location. The more information people share on a social networking site, the more likely it is that an attacker can impersonate them to launch attacks against them, their associates, or their organization. They may also try to join the target organization's employee groups to extract corporate data.

In general, the information attackers gather from social networking sites includes organization details, professional details, contacts and connections, and personal details, which they then use to execute other forms of social engineering attacks.

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

Impersonation on Facebook

- The attacker creates a fake user group on Facebook labeled as for "Employees of" the target company
- Using a false identity, the attacker then proceeds to "friend" or invite employees to the fake group
- Users join the group and provide their credentials such as date of birth, educational and employment backgrounds, spouses' names, etc.
- Using the details of any of these employees, the attacker can compromise a secured facility to gain access to the building
- Attackers scan details in profile pages. They use these for spear phishing, impersonation, and identity theft



https://www.facebook.com

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

Impersonation on Facebook

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

Facebook is a well-known social networking site that connects people. It is widely used between friends who share comments and upload photos, links, and videos. To impersonate users on Facebook, attackers use nicknames or aliases instead of their real names. They create fake accounts and try to add "**Friends**" to view others' profiles and obtain critical and valuable information.

The steps an attacker takes to lure a victim into revealing sensitive information:

- Create a fake user group on Facebook identified as "Employees of" the target company
- Using a false identity, proceed to "friend," or invite actual employees to the fake group, "Employees of Company XYZ"
- Users join the group and provide their credentials such as date of birth, educational and employment backgrounds, or spouses' names.
- Using the details of any one of the employees, an attacker can compromise a secured facility to gain access to the building

Attackers create a fake account and scan the details on the profile pages of various targets on social networking sites such as LinkedIn and Twitter to engage in spear phishing, impersonation, and identity theft.

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

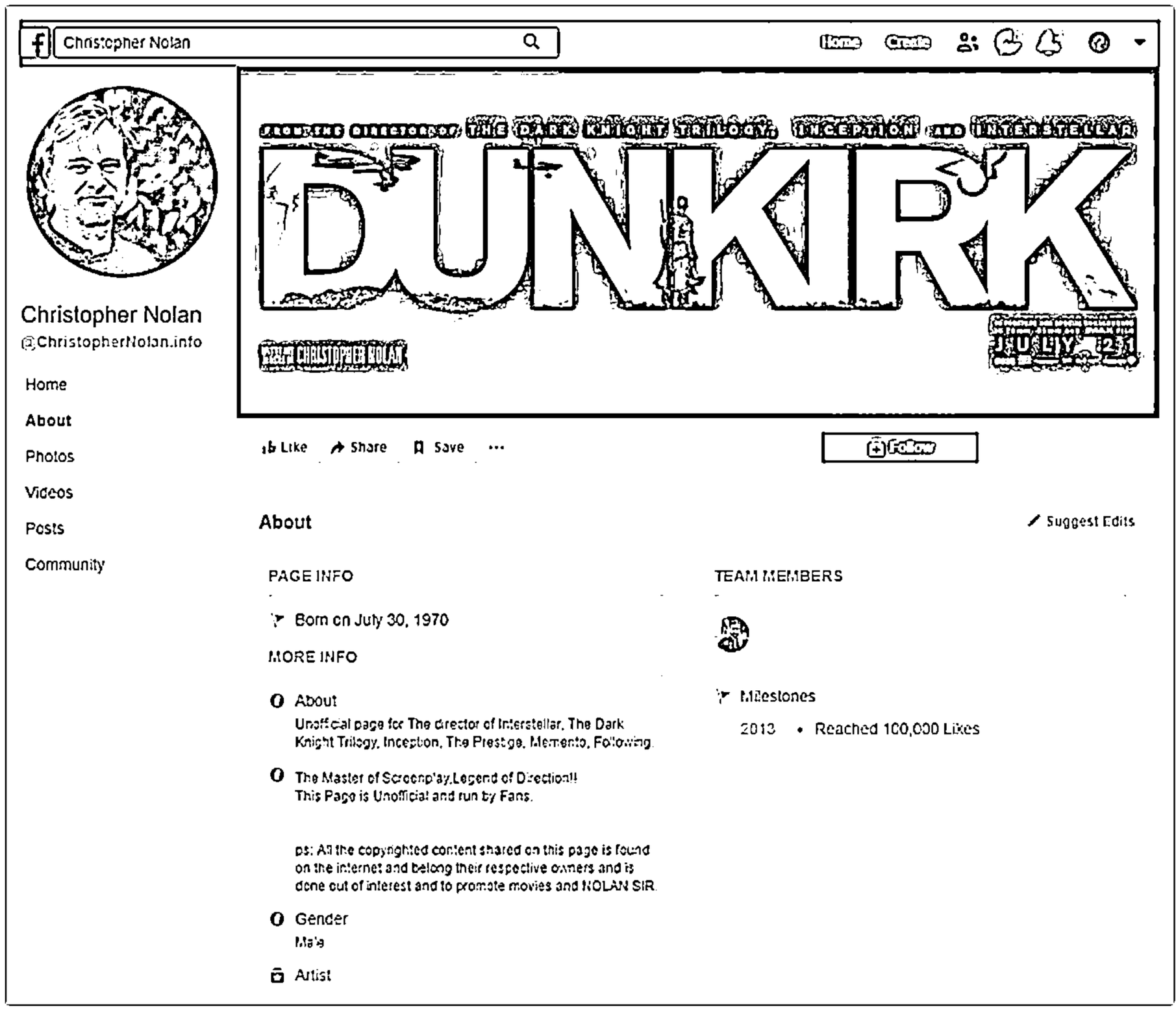


Figure 9.14: Screenshot showing Facebook profile

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

Social Networking Threats to Corporate Networks

1. Data Theft
2. Involuntary Data Leakage
3. Targeted Attacks
4. Network Vulnerability
5. Spam and Phishing
6. Modification of Content
7. Malware Propagation
8. Damage to Business Reputation
9. Infrastructure and Maintenance Costs
10. Loss of Productivity

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

Social Networking Threats to Corporate Networks

Before sharing data on a social networking site, or enhancing their channels, groups, or profiles, private and corporate users should be aware of the following social or technical security risks:

- **Data Theft**: Social networking sites are huge databases accessed by many people worldwide, increasing the risk of information exploitation.
- **Involuntary Data Leakage**: In the absence of a strong policy that sets clear lines between personal and corporate content, employees may unknowingly post sensitive data about their company on social networking sites, which might help an attacker to launch an attack on the target organization.
- **Targeted Attacks**: Attackers use the information posted on social networking sites to launch targeted attacks on specific users or companies.
- **Network Vulnerability**: All social networking sites are subject to flaws and bugs such as login issues and Java vulnerabilities, which attackers could exploit. This could, in turn, lead to the leakage of confidential information related to the target organization's network.
- **Spam and Phishing**: Employees using work e-mail IDs on social networking sites will probably receive spam and become targets of phishing attacks, which could compromise the organization's network.
- **Modification of Content**: In the absence of proper security measures and efforts to preserve identity, blogs, channels, groups, profiles, and other platforms can be spoofed or hacked.

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

- **Malware Propagation**: Social networking sites are ideal platforms for attackers to spread viruses, bots, worms, trojans, spyware, and other malware.
- **Business Reputation**: Attackers can falsify information about an organization or an employee on social networking sites, resulting in loss of reputation.
- **Infrastructure and Maintenance Costs**: Using social networking sites entails added infrastructure and maintenance resources for organizations to ensure that their defensive layers are effective safeguards.
- **Loss of Productivity**: Organizations must monitor employees' network activities to maintain security and ensure that such activities do not misuse the system and company resources.

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

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures

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

Identity Theft

- Identity theft is a crime in which an imposter steals your personally identifiable information such as name, credit card number, social security or driver's license numbers, etc. to commit fraud or other crimes
- Attackers can use identity theft to impersonate employees of a target organization and physically access facilities

Types of Identity Theft

- Child identity theft
- Criminal identity theft
- Financial identity theft
- Driver's license identity theft
- Insurance identity theft
- Medical identity theft
- Tax identity theft
- Identity cloning and Concealment
- Synthetic identity theft
- Social security identity theft

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

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

Identity Theft (Cont'd)

Common Techniques Attackers Use to Obtain Personal Information for Identity Theft

- Theft of wallets, computers, laptops, cell phones, etc.
- Internet searches
- Social engineering
- Dumpster diving and shoulder surfing
- Phishing
- Skimming
- Pretexting
- Pharming
- Hacking (compromising a user's system)
- Malware
- Wardriving
- Mail Theft and Rerouting

Indications of Identity Theft

- Unfamiliar charges to your credit card that you do not recognize
- No longer receiving credit card, bank, or utility statements
- Getting calls from the debit or credit fraud control department
- Charges for medical treatment or services you never received
- No longer receiving electricity, gas, water, etc. service bills

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

Identity Theft

Identity theft is a problem that many consumers face today. In the United States, some state legislators have imposed laws restricting employees from providing their SSNs (Social Security Numbers) during their recruitment. Identity theft frequently figures in news reports. Companies should be informed about identity theft so that they do not endanger their own anti-fraud initiatives.

This section discusses identity theft, including types of identity theft, common techniques attackers use to obtain personal information for identity theft, and various indications of identity theft.

The Identity Theft and Assumption Deterrence Act of 1998 defines identity theft as the illegal use of someone's identification. Identity theft occurs when someone steals others' personally identifiable information for fraudulent purposes. Attackers illegally obtain personally identifying information to commit fraud or other criminal acts.

Types of personally identifiable information stolen by identity thieves:

- Name
- Home and office address
- Social security number
- Phone number
- Date of birth
- Bank account number
- Credit card information
- Credit report
- Driving license number
- Passport number

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

The attacker steals people's identity for fraudulent purposes such as:

- To open new credit card accounts in the name of the user without paying the bills
- To open a new phone or wireless account in the user's name, or to run up charges on their existing account
- To use the victims' information to obtain utility services such as electricity, heating, or cable TV
- To open bank accounts with the intention of writing bogus checks using the victim's information
- To clone an ATM or debit card to make electronic withdrawals from the victim's accounts
- To obtain loans for which the victim is liable
- To obtain a driver's license, passport, or other official ID card that contains the victim's data with the attacker's photos
- Using the victim's name and Social Security number to receive their government benefits
- To impersonate an employee of a target organization to physically access its facility
- To take over the victim's insurance policies
- To sell the victim's personal information
- To order goods online using a drop-site
- To hijack email accounts
- To obtain health services
- To submit fraudulent tax returns
- To commit other crimes with the intention of providing the victim's name to the authorities during arrest, instead of their own

Types of Identity Theft

Identity theft is constantly increasing, and identity thieves are finding new ways or techniques to steal different types of target information. Some of the types of identity theft are as follows:

- **Child Identity Theft**

  This type of identity theft occurs when the identity of a minor is stolen. This is desirable because it may go undetected for a long time. After birth, parents apply for a Social Security Number for their child, which along with a different date of birth, is used by identity thieves to apply for credit accounts, loans or utility services, or to rent a place to live and apply for government benefits.

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

- **Criminal Identity Theft**

  This is one of the most common and most damaging types of identity theft. A criminal uses someone's identity to escape criminal charges. When they are caught or arrested, they provide the assumed identity. The best way to protect against criminal identity theft is to keep all personal information secure, which includes following safe Internet practices and being cautious of "shoulder surfers."

- **Financial Identity Theft**

  This type of identity theft occurs when a victim's bank account or credit card information is stolen and illegally used by a thief. They can max out a credit card and withdraw money from the account, or can use the stolen identity to open a new account, apply for new credit cards, and take out loans. The information that is required to hack into the victim's account and steal their information is obtained through viruses, phishing attacks, or data breaches.

- **Driver's License Identity Theft**

  This type of identity theft is the easiest as it requires a little sophistication. A person can lose their driver's license, or it can easily be stolen. Once it falls into the wrong hands, the perpetrator can sell the stolen driver's license or misuse it by committing traffic violations, of which the victim is unaware of and fails to pay fines for, ending up with their license suspended or revoked.

- **Insurance Identity Theft**

  Insurance identity theft is closely related to medical identity theft. It takes place when a perpetrator unlawfully takes the victim's medical information to access their insurance for medical treatment. Its effects include difficulties in settling medical bills, higher insurance premiums, and probable trouble in acquiring future medical coverage.

- **Medical Identity Theft**

  This is the most dangerous type of identity theft where the perpetrator uses the victim's name or information without the victim's consent or knowledge to obtain medical products and claim health insurance or healthcare services. Medical identity theft results in frequent erroneous entries in the victim's medical records, which could lead to false diagnoses and life-threatening decisions by the doctors.

- **Tax Identity Theft**

  This type of identity theft occurs when the perpetrator steals the victim's Social Security Number to file fraudulent tax returns and obtain fraudulent tax refunds. It creates difficulties for the victim in accessing their legitimate tax refunds and results in a loss of funds. Phishing emails are one of the main tricks used by the criminal to steal a target's information. Therefore, protection from such identity theft includes the adoption of safe Internet practices.

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

- **Identity Cloning and Concealment**

  This type of identity theft encompasses all forms of identity theft, where the perpetrators attempt to impersonate someone else simply in order to hide their identity. These perpetrators could be illegal immigrants, those hiding from creditors, or simply those who want to become "anonymous."

- **Synthetic Identity Theft**

  This is one of the most sophisticated types of identity theft, where the perpetrator obtains information from different victims to create a new identity. Firstly, he steals a Social Security Number and uses it with a combination of fake names, date of birth, address, and other details required for creating a new identity. The perpetrator uses this new identity to open new accounts, loans, credit cards, phones, other goods, and services.

- **Social Identity Theft**

  This is another common type of identity theft where the perpetrator steals victim's Social Security Number in order to derive various benefits such as selling it to an undocumented person, using it to defraud the government by getting a new bank account, loans, credit cards, or applying for and obtaining a new passport.

Common Techniques Attackers Use to Obtain Personal Information for Identity Theft

Discussed below are some of the methods by which attackers steal targets' identities, which in turn allow them to commit fraud and other criminal activities:

- **Theft of wallets, computers, laptops, cell phones, backup media, and other sources of personal information**

  Physical theft is common. Attackers steal hardware from places such as hotels and recreational places such as clubs, restaurants, parks, and beaches. Given adequate time, they can recover valuable data from these sources.

- **Internet Searches**

  Attackers can gather a considerable amount of sensitive information via legitimate Internet sites, using search engines such as Google, Bing, and Yahoo!.

- **Social Engineering**

  Social engineering is the art of manipulating people into performing certain actions or divulging personal information and accomplishing their task without using cracking methods.

- **Dumpster Diving and Shoulder Surfing**

  Attackers rummage through household garbage and the trash bins of organizations, ATM centers, hotels, and other places to obtain personal and financial information for fraudulent purposes.

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

Criminals may find user information by glancing at documents, observing personal identification numbers (PINs) typed into automatic teller machines (ATM), or by overhearing conversations.

- **Phishing**

  The "fraudster" may pretend to be from a financial institution or other reputable organization and send spam or pop-up messages to trick users into revealing their personal information.

- **Skimming**

  Skimming refers to stealing credit or debit card numbers by using special storage devices called skimmers or wedges when processing the card.

- **Pretexting**

  Fraudsters may impersonate executives from financial institutions, telephone companies, and other businesses. They rely on "smooth-talking" and win the trust of an individual to reveal sensitive information.

- **Pharming**

  Pharming, also known as domain spoofing, is an advanced form of phishing in which the attacker redirects the connection between the IP address and its target server. The attacker may use cache poisoning (modifying the Internet address to that of a rogue address) to do so. When the users type in the Internet address, it redirects them to a rogue website that resembles the original.

- **Hacking (compromising a user's system)**

  Attackers may compromise user systems and router information using listening devices such as sniffers and scanners. They gain access to an abundance of data, decrypt it (if necessary), and use it for identity theft.

- **Keyloggers and Password Stealers (Malware)**

  An attacker may infect the user's computer with trojans, viruses, or other malware and then record and collect the user's keystrokes to steal passwords, usernames, and other sensitive information of personal, financial, or business import.

  Attackers may also use emails to send fake forms, such as Internal Revenue Service (IRS) forms, to gather information from their victims.

- **Wardriving**

  Attackers search for unsecured Wi-Fi wireless networks in moving vehicles containing laptops, smartphones, or PDAs. Once they find unsecured networks, they access any sensitive information stored on the devices of the users on those networks.

- **Mail Theft and Rerouting**

  Often, mailboxes contain bank documents (credit cards or account statements), administrative forms, and other important correspondence. Criminals use this information to obtain credit card information or to reroute the mail to a new address.

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

Indications of Identity Theft

People do not realize that they are the victim of identity theft until they experience some unknown and unauthorized issues as a result of the theft. Therefore, it is of paramount importance that people watch out for the warning signs that their identities have been compromised. Listed below are some of the signs of identity theft:

- Unfamiliar charges to your credit card that you do not recognize.
- No longer receive credit card, bank, or utility statements
- Creditors call asking about an unknown account on your name.
- There are numerous traffic violations under your name that you did not commit.
- You receive charges for medical treatment or services you never received.
- There is more than one tax return filed under your name.
- Being denied access to your own account and unable to take out loans or use other services.
- Not receiving electricity, gas, water, or other services bills due to stolen mail.
- Sudden changes in your personal medical records showing a condition you do not suffer from.

Some additional indications of identity theft are as follow:

- Getting a notification that your information was compromised or misused by a data breach in a company where you are an employee or have an account.
- An inexplicable cash withdrawal from your bank account.
- Calls from debit or credit card fraud control departments giving warnings about suspicious activities on your accounts.
- A refusal of government benefits to you and your child because those benefits are already being received by some other account using your child's Social Security Number.
- Your medical insurance plan rejects your authentic medical claim because someone tampered with your medical records, causing you to reach your benefit limit.

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

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures

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

Countermeasures

Social engineers exploit human behavior (such as manners, enthusiasm toward work, laziness, or naivete) to gain access to the targeted company's information resources. Social engineering attacks are difficult to guard against, as the victim might not be aware that he or she has been deceived. They are very much like the other kinds of attacks used to extract a company's valuable data. To guard against social engineering attacks, a company needs to evaluate the risk of different kinds of attacks, estimate possible losses and spread awareness among its employees.

This section deals with countermeasures that an organization can implement to be more secure against social engineering attacks.

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

Social Engineering Countermeasures

- Good policies and procedures are ineffective if they are not taught and reinforced by employees
- After receiving training, employees should sign a statement acknowledging that they understand the policies
- The main objectives of social engineering defense strategies are to create user awareness, robust internal network controls, and secure policies, plans, and processes

Password Policies

- Periodic password changes
- Avoiding guessable passwords
- Account blocking after failed attempts
- Increasing length and complexity of passwords
- Improving secrecy of passwords

Physical Security Policies

- Identification of employees by issuing ID cards, uniforms, etc.
- Escorting visitors
- Restricting access to work areas
- Proper shredding of useless documents
- Employing security personnel

Defense Strategy

- Social engineering campaign
- Gap analysis
- Remediation strategies

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

Social Engineering Countermeasures (Cont'd)

1. Train individuals on security policies
2. Implement proper access privileges
3. Presence of proper incidence response time
4. Availability of resources only to authorized users
5. Scrutinize information
6. Background check and proper termination process
7. Anti-virus/anti-phishing defenses
8. Implement two-factor authentication
9. Adopt documented change management
10. Ensure software is regularly updated

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

Social Engineering Countermeasures

Attackers implement social engineering techniques to trick people into revealing organizations' confidential information. They use social engineering to perform fraud, identity theft, industrial espionage, and other disreputable behaviors. To guard against social engineering attacks, organizations must develop effective policies and procedures; however, merely developing them is not enough.

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

To be truly effective, an organization should:

- Disseminate policies among employees and provide proper education and training. Specialized training benefits employees in higher-risk positions against social engineering threats.
- Obtain employee signatures on a statement acknowledging that they understand the organization's policies.
- Define the consequences of policy violations.

The main objectives of social engineering defense strategies are to create user awareness, robust internal network controls, and security policies, plans, and processes.

Official security policies and procedures help employees or users make the right security decisions. They should include the following safeguards:

- **Password Policies**

  Password policies stating the following guidelines help to increase password security:

  - Change passwords regularly.
  - Avoid passwords that are easy to guess. It is possible to guess passwords from answers to social engineering questions such as, "Where were you born?" "What is your favorite movie?" or "What is your pet's name?"
  - Block user accounts if a user exceeds a certain number of failed attempts to guess a password.
  - Choose long (minimum of 6 – 8 characters) and complex (using various alphanumeric and special characters) passwords.
  - Do not disclose passwords to anyone.

  Password Security policies often include advice on proper password management, for example:

  - Avoid sharing a computer account.
  - Avoid using the same password for different accounts.
  - Avoid storing passwords on media or writing them down on a notepad or sticky note.
  - Avoid communicating passwords over the phone or through email or SMS.
  - Be sure to lock or shut down the computer before stepping away from it.

- **Physical Security Policies**

  Physical security policies address the following areas.

  - Issue identification cards (ID cards), and uniforms, along with other access control measures to the employees of the organization.

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

- Office security or personnel must escort visitors to designated visitor rooms or lounges.
- Restrict access to certain areas of an organization to prevent unauthorized users from compromising the security of sensitive data.
- Dispose of old documents that contain valuable information by using equipment such as paper shredders and burn bins. This prevents information gathering by attackers using techniques such as dumpster diving.
- Employ security personnel in an organization to protect people and property — supplement trained security personnel with alarm systems, surveillance cameras, and other equipment.

- **Defense Strategy**
  - **Social Engineering Campaign:** An organization should conduct numerous social engineering exercises using different techniques on a diverse group of people in order to examine how its employees might react to real social engineering attacks.
  - **Gap Analysis:** Using the information obtained from the social engineering campaign, a gap analysis evaluates the organization based on industry-leading practices, emerging threats, and mitigation strategies.
  - **Remediation Strategies:** Depending upon the result of the evaluation in the gap analysis, organizations develop a detailed remediation plan to mitigate the weaknesses or the loopholes found in the earlier step. The plan focuses mainly on educating and creating awareness among employees based on their roles and identifying and mitigating potential threats to the organization.

Some additional countermeasures against social engineering are as follows:

- **Train Individuals on Security Policies:** An efficient training program consists of basic social engineering concepts and techniques, all security policies, and methods to increase awareness of social engineering.
- **Implement Proper Access Privileges:** There should be administrator, user, and guest accounts with respective levels of authorization.
- **Presence of a Proper Incidence Response Time:** There should be proper guidelines for reacting to a social engineering attempt.
- **Availability of Resources Only to Authorized Users:** Make sure sensitive information is secured and that resources are only accessed by authorized users
- **Scrutinize Information:** Categorize the information as top secret, proprietary, for internal use only, and for public use, or use other categories.
- **Perform a Background Check and Proper Termination Process:** Insiders with a criminal background and terminated employees are easy targets for procuring information.
- **Anti-Virus and Anti-Phishing Defenses:** Use multiple layers of anti-virus defenses at end-user and mail gateway levels to minimize social engineering attacks.

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

- **Implement Two-Factor Authentication:** Instead of fixed passwords, use two-factor authentication for high-risk network services such as VPNs and modem pools. In the two-factor authentication (TFA) approach, the user must present two different forms of proof of identity. If an attacker is trying to break into a user account, then they need to break both forms of user identity, which is more difficult to do. Hence, TFA is a defense-in-depth security mechanism and part of the multifactor authentication family. The two pieces of evidence that a user provides could include a physical token such as a card, and is typically something the person can remember without much effort, such as a security code, PIN, or password.
- **Adopt Documented Change Management:** A documented change-management process is more secure than the ad-hoc process.
- **Ensure a Regular Update of Software:** Organizations should ensure that the system and software are regularly patched and updated as the attackers exploit unpatched and out-of-date software to obtain useful information to launch an attack.

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

Detecting Insider Threats

Insider Risk Controls	❑ Insider data risk presents another layer of complexity for security professionals, which requires designing security infrastructure that can efficiently monitor user permissions, access controls, and user actions
Deterrence Controls	❑ The security framework must contain safeguards, recommended actions by the employee and IT professionals, separation of duties, assigning privileges, etc. ❑ Security professionals can use tools such as DLP (Symantec Data Loss Prevention, SecureTrust Data Loss Prevention, etc.) and IAM (SailPoint IdentityIQ, RSA SecurID Suite, etc.) to deter insider threats
Detection Controls	❑ Security professionals must use a variety of security controls and tools to analyze and detect insider threats ❑ Tools such as IDS/IPS (Check Point IPS Software Blade, IBM Security Network Intrusion Prevention System, etc.), Log Management (SolarWinds Security Event Manager, Splunk, etc.), and SIEM (ArcSight ESM, LogRhythm NextGen SIEM Platform, etc.) may be used

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

Detecting Insider Threats

Most data attacks come from insiders, which only makes them more difficult to prevent or detect. Insiders are mostly aware of the security loopholes of the organization, and they exploit them to steal confidential information. It is essential to carefully handle insider threats as they are difficult to thwart and may incur huge financial losses and business interruptions. Some of the methods to detect insider threats are given below:

- **Insider Risk Controls**

  Insider data risk presents another layer of complexity for security professionals. It requires designing security infrastructure in such a way that user permissions, access controls, and user actions are monitored efficiently.

- **Deterrence Controls**

  The organization's security framework must contain safeguards, follow recommended actions of the employee and IT professionals, provide a separation of duties, and assign privileges. These security controls eliminate or minimize the security risks to the organization's critical assets.

  The deterrence controls that the security professionals must have in place to deter insider threats are DLP (Data Loss Prevention) tools, and Identity and Access Management (IAM) tools.

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

Some of the deterrence controls are:

- DLP Tools:
  - Symantec Data Loss Prevention (*https://www.symantec.com*)
  - SecureTrust Data Loss Prevention (*https://securetrust.com*)
  - Check Point Data Loss Prevention (*https://www.checkpoint.com*)
- IAM Tools:
  - SailPoint IdentityIQ (*https://www.sailpoint.com*)
  - RSA SecurID Suite (*https://www.rsa.com*)
  - Core Access Assurance Suite (*https://www.coresecurity.com*)

- **Detection Controls**

  Security professionals must use a variety of security controls and tools to analyze and detect insider threats in organizations.

  The detection controls that the security professionals must have in place to detect insider threats are IDS/IPS (Intrusion detection and prevention systems), log management systems, and Security Information and Event Management (SIEM) tools.

  Some of the detection controls are:

  - IDS/IPS Tools
    - Check Point IPS Software Blade (*https://www.checkpoint.com*)
    - IBM Security Network Intrusion Prevention System (*https://www.ibm.com*)
    - AlienVault Unified Security Management (*https://www.alienvault.com*)
  - Log Management Tools
    - SolarWinds Security Event Manager (*https://www.solarwinds.com*)
    - Splunk (*https://www.splunk.com*)
    - Loggly (*https://www.loggly.com*)
  - SIEM Tools
    - ArcSight ESM (*https://www.microfocus.com*)
    - LogRhythm NextGen SIEM Platform (*https://logrhythm.com*)
    - SolarWinds Log & Event Manager(*https://www.solarwinds.com*)

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

Insider Threats Countermeasures

1. Separation and rotation of duties
2. Least privileges
3. Controlled access
4. Logging and auditing
5. Employee monitoring
6. Legal policies
7. Archive critical data
8. Employee training on cyber security
9. Employee background verification
10. Periodic risk assessment
11. Privileged users monitoring
12. Credentials deactivation for terminated employees

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

Insider Threats Countermeasures

There are safety measures that help an organization to prevent or minimize insider threats:

- **Separation and rotation of duties**: Divide responsibilities among multiple employees to restrict the amount of power or influence held by any individual. This helps to avoid fraud, abuse, and conflict of interest and facilitates the detection of control failures (including bypassing security controls and information theft). Rotation of duties at random intervals helps an organization to deter fraud or the abuse of privileges.
- **Least privileges**: Provide users with only enough access privilege to allow them to perform their assigned tasks. This helps maintain information security.
- **Controlled access**: Access controls in various parts of an organization restrict unauthorized users from gaining access to critical assets and resources.
- **Logging and auditing**: Perform logging and auditing periodically to check for misuse of company resources.
- **Employee monitoring**: Use employee monitoring software that records all user sessions, and that can be reviewed by security professionals.
- **Legal policies**: Enforce legal policies to prevent employees from misusing the organization's resources and sensitive data theft.
- **Archive critical data**: Maintain a record of the organization's critical data in the form of archives to be used as backup resources, if needed.
- **Employee training on cybersecurity**: Train employees on how to protect their credentials and the company's confidential data from attack. They will be able to identify social engineering attempts and take proper mitigations and reporting steps.

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

- **Employee background verification**: Ensure thorough background checks of all employees before hiring them by using Google search and social networking sites and consulting previous employers.
- **Periodic risk assessment**: Perform a periodic risk assessment on critical assets to identify vulnerabilities and implement protection strategies against both insider and outsider threats.
- **Privileged users monitoring**: Implement additional monitoring mechanisms for system administrators and privileged users as these accounts can be used to can deploy malicious code or logic bomb on the system or network.
- **Credentials deactivation for terminated employees**: Disable all the employee's access profiles to the physical locations, networks, systems, applications, and data immediately after termination.
- **Periodic risk assessments**: Perform periodic risk assessments on all the organization's critical assets then develop and maintain a risk management strategy to secure those assets from both insiders and outsiders.
- **Layered defense**: Implement multiple layers of defense to prevent and protect critical assets from remote attacks originated from insiders. Develop appropriate remote access policies and procedures to thwart such attacks.
- **Physical security**: Build a professional security team that monitors the physical security of the organization.
- **Surveillance**: Install video cameras to monitor all critical assets. Install and enable screen-capturing software on all critical servers.

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

Identity Theft Countermeasures

1. Secure or shred all documents containing your private information
2. Ensure your name is not present in marketers' hit lists
3. Review your credit card statement regularly and store it securely, out of reach of others
4. Never give any personal information over the phone
5. Keep your mail secure by emptying the mailbox quickly
6. Be cautious and verify all requests for personal data
7. Protect your personal information from being publicized
8. Do not display or share any account/contact numbers unless mandatory
9. Monitor online banking activities regularly
10. Never list any personal identifiers on social media

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

Identity Theft Countermeasures

Identity theft occurs when someone uses personal information (such as a name, social security number, date of birth, mother's maiden name, or address) in a malicious way, such as for credit card or loan services, or even rentals and mortgages, without the person's knowledge or permission.

Listed below are countermeasures that, on implementation, will reduce the chances of identity theft:

- Secure or shred all documents containing private information
- Ensure your name is not present on the marketers' hit lists
- Review credit card reports regularly
- Never give any personal information over the phone
- To keep mail secure, empty the mailbox quickly
- Suspect and verify all requests for personal data
- Protect personal information from being publicized
- Do not display account or contact numbers unless mandatory
- Monitor online banking activities regularly
- Never list any personal identifiers on social media websites such as your father's name, pet's name, address, or city of birth.
- Enable two-factor authentication on all online accounts
- Never use public Wi-Fi for sharing or accessing sensitive information

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

- Install host security tools such as a firewall and anti-virus on your personal computer

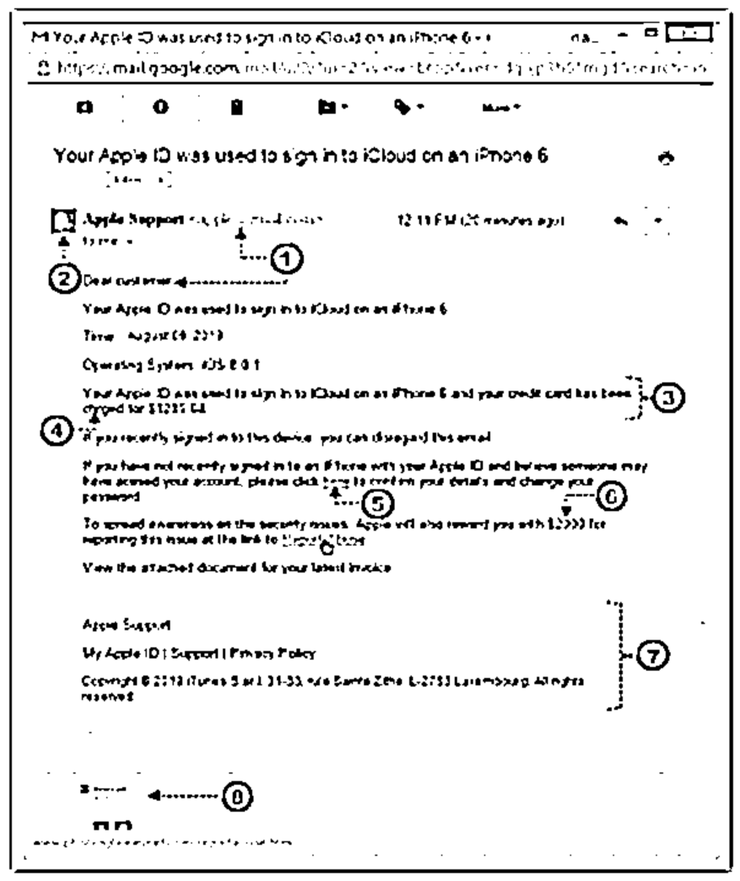
Some additional countermeasures against identity theft are as follows:

- To keep mail secure, empty your mailbox quickly and do not reply to unsolicited email requests asking for personal information.
- Shred credit card offers and "convenience checks" that are not useful.
- Do not store any financial information on the system and use strong passwords for all financial accounts.
- Check telephone and cell phone bills for calls you did not make.
- Keep your Social Security card, passport, license, and other valuable personal information hidden and secured.
- Read website privacy policies.
- Be cautious before clicking on a link provided in an email or instant message.

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

How to Detect Phishing Emails?

1. Appears to be from a bank, company, or social networking site, and has a generic greeting
2. Appears to be from a person listed in your email address book
3. Gives a sense of urgency or a veiled threat
4. May contain grammatical/spelling mistakes
5. Includes links to spoofed websites
6. May contain offers that seem to be too good to be true
7. Includes official-looking logos and other information taken from legitimate websites
8. May contain a malicious attachment



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

How to Detect Phishing Emails?

To detect phishing emails, first, hover your mouse pointer over the name in the "**From**" column. Doing so will show whether the original domain name is linked to the sender's name; if it is not, then it could be a phishing email. For example, an email from Gmail.com should probably display it's "**From**" domain as "**gmail.com**."

Check to see if the email provides a URL and prompts the user to click on it. If so, ensure that the link is legitimate by hovering the mouse pointer over it (to display the link's URL) and ensure it uses encryption (https://). To be on the safe side, always open a new window and visit the site by typing it in directly instead of clicking on the link provided in the email.

Do not provide any information to the suspicious website, as it will likely link directly to the attacker.

A few other indicators of phishing emails:

- It seems to be from a bank, company, or social networking site and has a generic greeting
- It seems to be from a person listed in your email address book
- It has an urgent tone or makes a veiled threat
- It may contain grammatical or spelling mistakes
- It includes links to spoofed websites
- It may contain offers that seem to be too good to be true
- It includes official-looking logos and other information taken from legitimate websites
- It may contain a malicious attachment

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

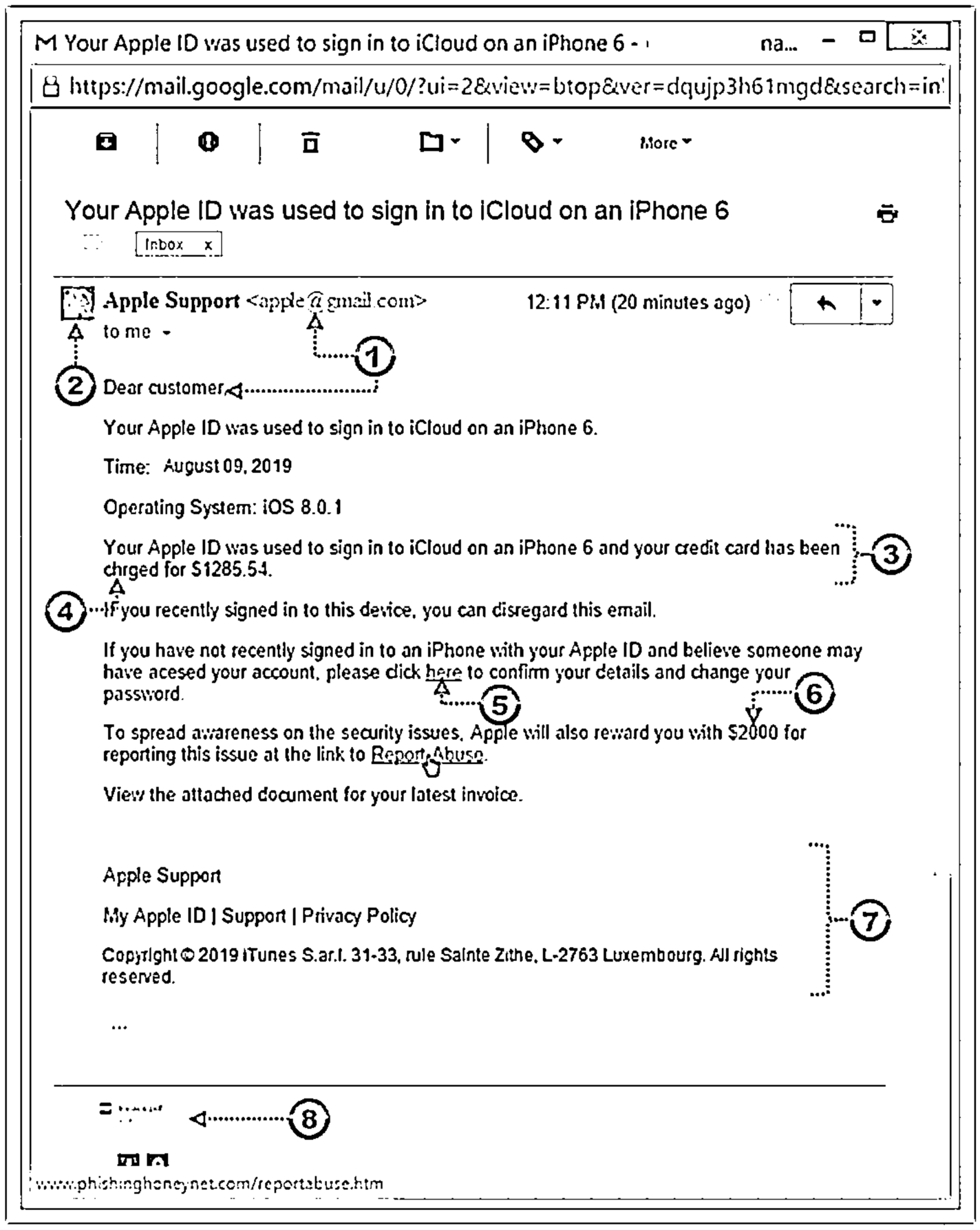


Figure 9.15: Screenshot Showing an Email with Indications of Phishing

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

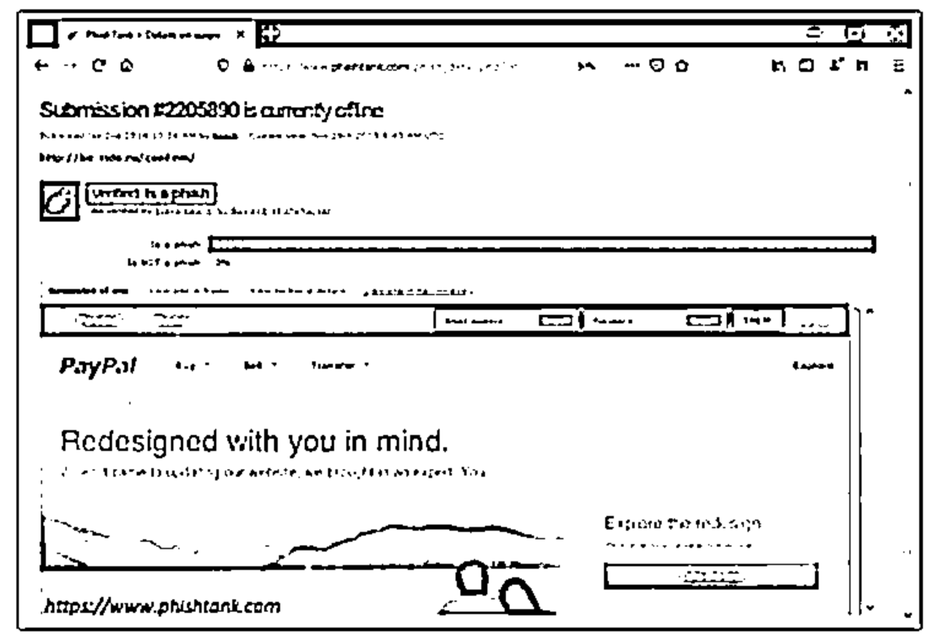
Anti-Phishing Toolbar

Netcraft

- The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks

Phish Tank

- PhishTank is a collaborative clearing house for data and information about phishing on the Internet
- It provides an open API for developers and researchers to integrate anti-phishing data into their apps



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

Anti-Phishing Toolbar

- **Netcraft**

  Source: *https://toolbar.netcraft.com*

  The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks. The Netcraft Toolbar provides updated information about sites that users visit regularly and blocks dangerous sites. The toolbar provides a wealth of information about popular websites. This information will help to make an informed choice about the integrity of those sites.

  As shown in the screenshot, Netcraft protects individuals and organizations from phishing attacks and fraudsters.

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

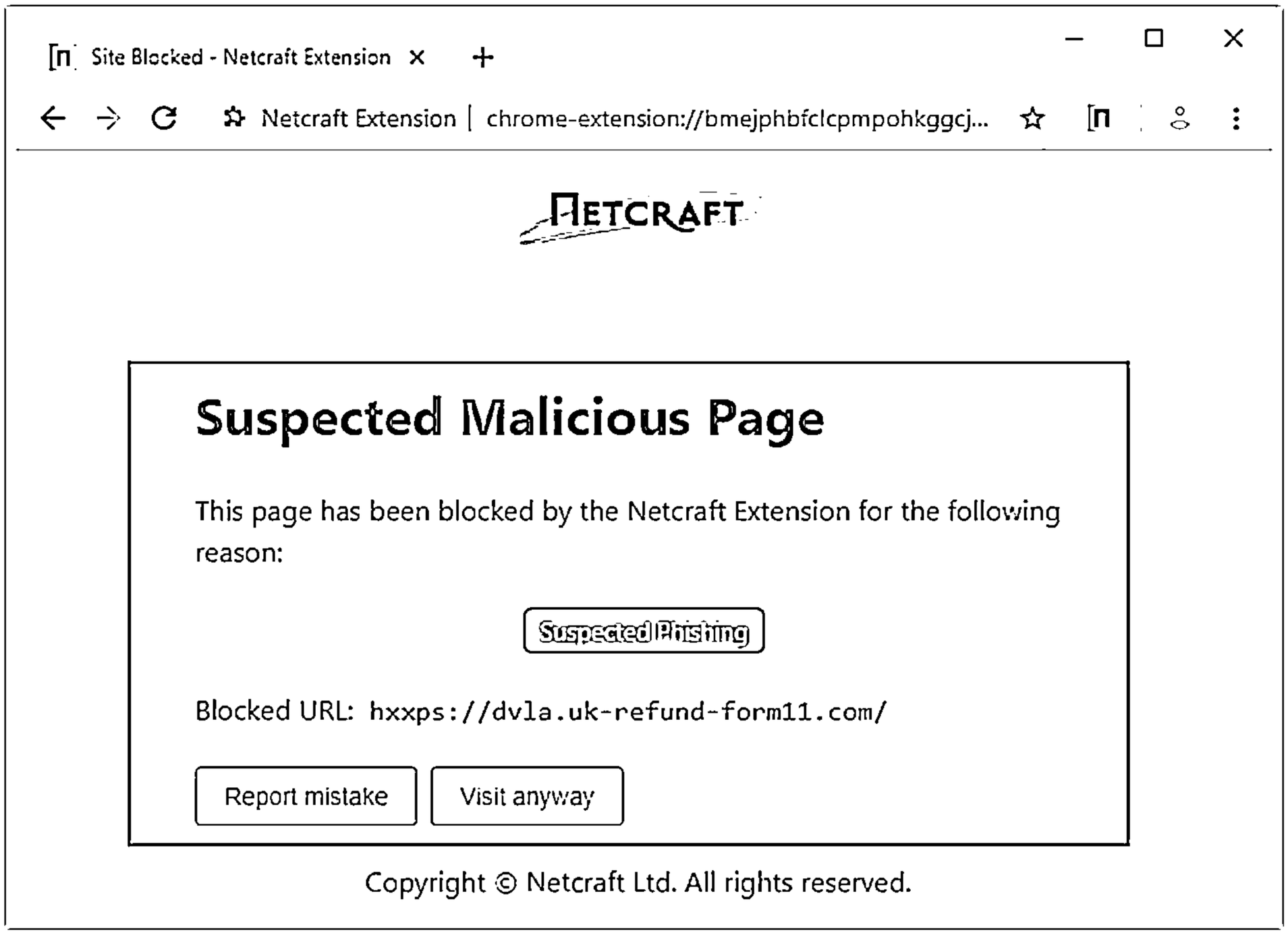


Figure 9.16: Screenshot of Netcraft

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

- **PhishTank**

  Source: *https://phishtank.com*

  PhishTank is a collaborative clearinghouse for data and information about phishing on the Internet. It provides an open API for developers and researchers to integrate anti-phishing data into their applications.

  As shown in the screenshot, security professionals can use PhishTank to check whether a malicious URL is a phishing site or not.

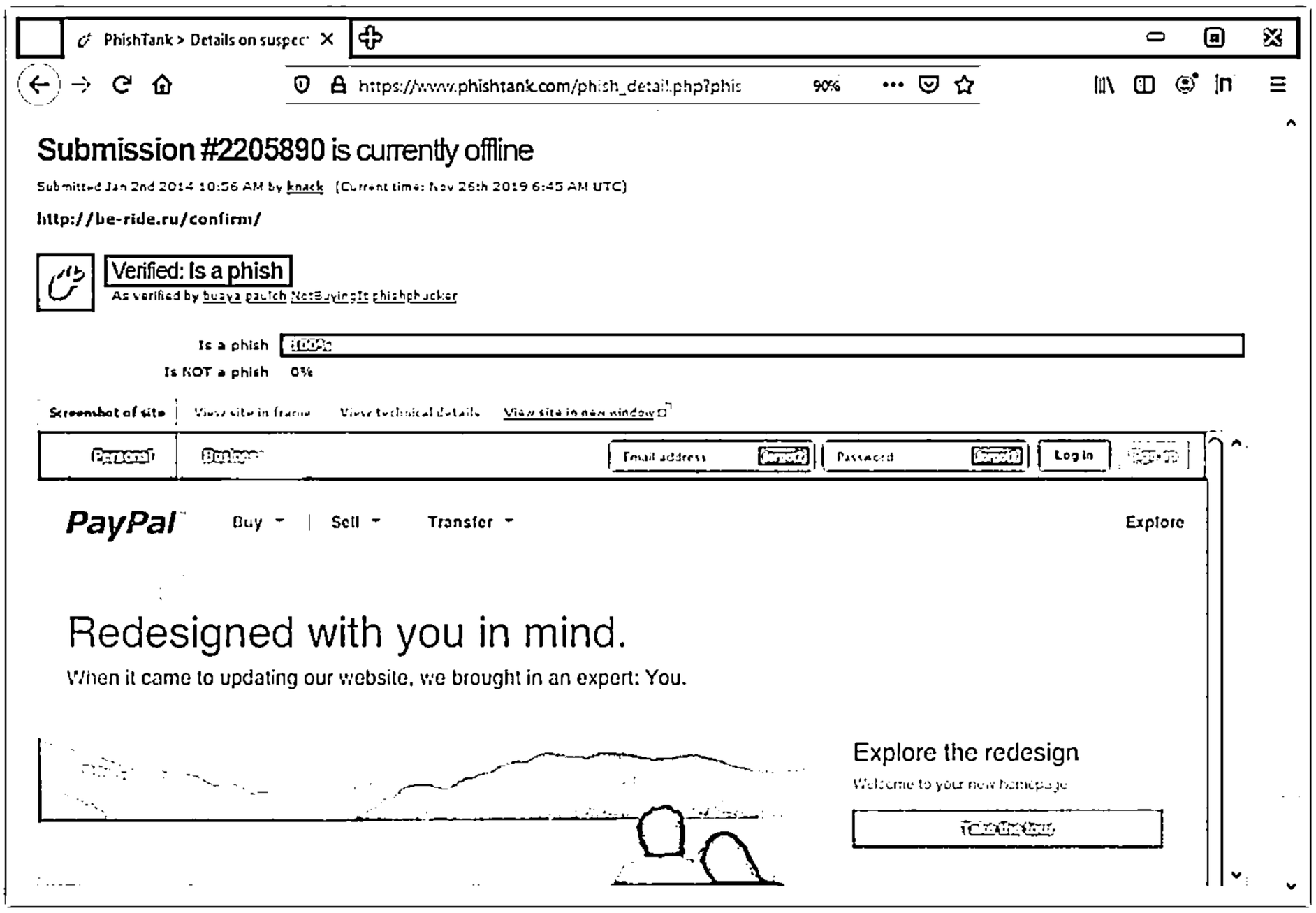


Figure 9.17: Screenshot of PhishTank

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

Common Social Engineering Targets and Defense Strategies

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees and help desk staff never to reveal passwords or other information over the phone. Enforce policies for the front office and help desk personnel
Technical support and system administrators	Impersonation, persuasion, intimidation, fake SMS, phone calls, and emails	Train technical support executives and system administrators never to reveal passwords or other information over the phone or email
Perimeter security	Impersonation, reverse social engineering, piggybacking, tailgating, etc.	Implement strict badge, token, or biometric authentication, employee training, and security guards
Office	Shoulder surfing, eavesdropping, ingratiation, etc.	Implement employee training, best practices, and checklists for using passwords. Escort all guests
Vendors of the target organization	Impersonation, persuasion, intimidation	Educate vendors about social engineering
Mail room	Theft, damage, or forging of mails	Lock and monitor mail room, train employees
Machine room/Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to extract confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment
Company's Executives	Fake SMS, phone calls, and emails to grab confidential data	Train executives never to reveal identity, passwords, or other confidential information over the phone or email
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas; shred important data; and erase magnetic media

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

Common Social Engineering Targets and Defense Strategies

Attackers implement various social engineering techniques to trick people into providing sensitive information about their organizations, thus helping attackers to launch malicious activities. These techniques are used on privileged individuals or those who deal with important information.

Below table shows common social engineering targets, various social engineering techniques that attackers use, and the defense strategies to counter these attacks.

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees and help desk staff never to reveal passwords or other information over the phone. Enforce policies for the front office and help desk personnel
Technical support and system administrators	Impersonation, persuasion, intimidation, fake SMS, phone calls, and emails	Train technical support executives and system administrators never to reveal passwords or other information over the phone or email
Perimeter security	Impersonation, reverse social engineering, piggybacking, tailgating, etc.	Implement strict badge, token, or biometric authentication, employee training, and security guards

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

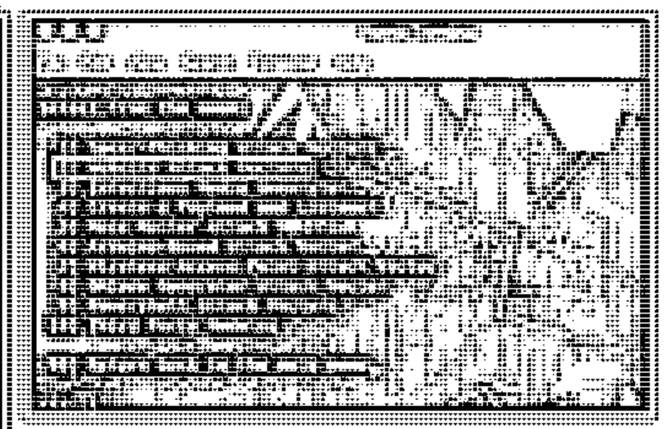
Office	Shoulder surfing, eavesdropping, and ingratiation	Implement employee training, best practices, and checklists for using passwords. Escort all guests
Vendors of the target organization	Impersonation, persuasion, and intimidation	Educate vendors about social engineering.
Mail room	Theft, damage, or forging of mails	Lock and monitor the mailroom, train employees
Machine room and Phone closet	Attempting to gain access, remove equipment, or attach a protocol analyzer to extract confidential data	Keep phone closets, server rooms, and other spaces locked at all times and keep an updated inventory of equipment
Company's Executives	Fake SMS, phone calls, and emails designed to grab confidential data	Train executives never to reveal identity, passwords, or other confidential information over the phone or email
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas; shred important data; and erase magnetic media

Table 9.1: Common social engineering targets and defense strategies

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

Social Engineering Tools: Social Engineering Toolkit (SET)

- The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing around social engineering



- SpeedPhish Framework (SPF) https://github.com
- Gophish https://getgophish.com
- King Phisher https://github.com
- LUCY https://www.lucysecurity.com
- MSI Simple Phish https://microsolved.com

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

Social Engineering Tools

- **Social Engineering Toolkit (SET)**

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

  The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. It is a generic exploit designed to perform advanced attacks against human elements to compromise a target and make them offer sensitive information. SET categorizes attacks such as email, web, and USB attacks according to the attack vector used to trick humans. The toolkit attacks human weakness, exploiting the trusting, fearful, greedy, and the helpful nature of humans.

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

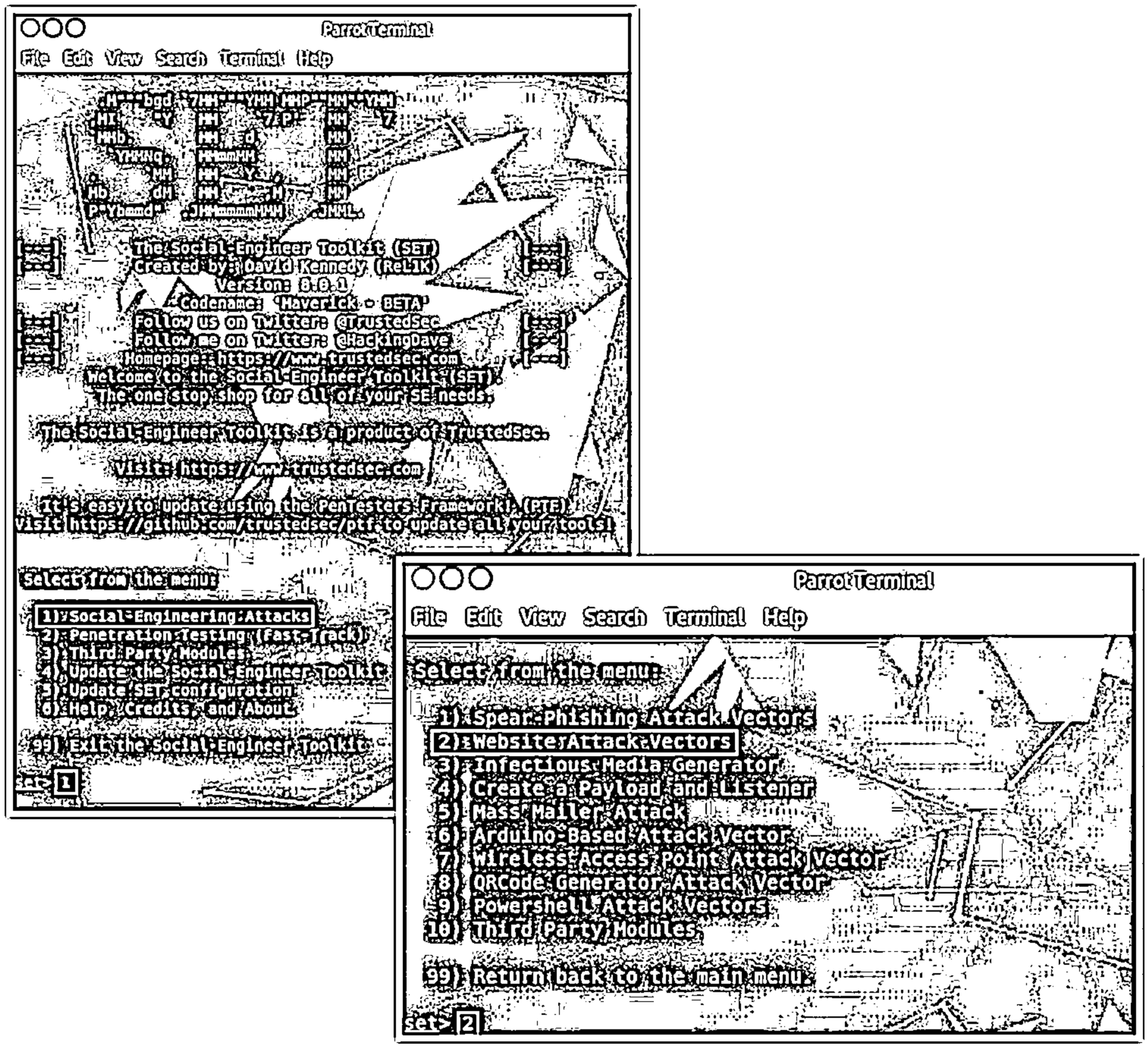


Figure 9.18: Screenshot of SET showing menu and attack options

Some social engineering tools are listed below:

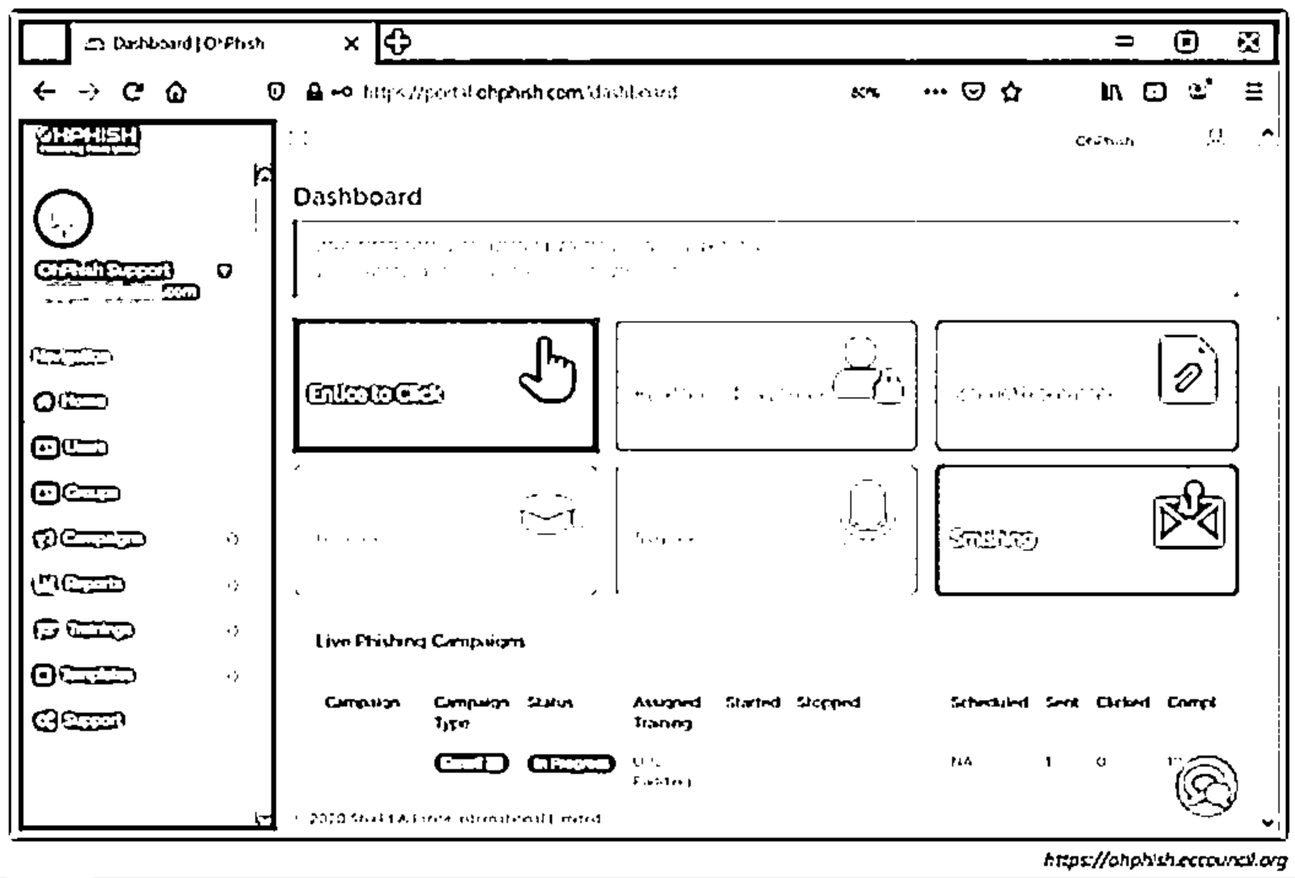
- SpeedPhish Framework (SPF) (*https://github.com*)
- Gophish (*https://getgophish.com*)
- King Phisher (*https://github.com*)
- LUCY (*https://www.lucysecurity.com*)
- MSI Simple Phish (*https://microsolved.com*)

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

Audit Organization's Security for Phishing Attacks using OhPhish

- OhPhish is a web-based portal to test employees' susceptibility to social engineering attacks
- OhPhish is a phishing simulation tool that provides the organization with a platform to launch phishing simulation campaigns on its employees

OHPHISH
Fortifying Front Lines



https://ohphish.eccouncil.org

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

Audit Organization's Security for Phishing Attacks using OhPhish

The primary objective of launching phishing campaigns against employees of the client organization is to assess the employees' susceptibility to phishing attacks and help the organization reduce risks that arise when the employees fall prey to phishing attacks sent by cyber-threat actors.

- **OhPhish**

  Source: *https://ohphish.eccouncil.org*

  OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides the organization with a platform to launch phishing simulation campaigns on its employees. The platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user, department, or designation.

  OhPhish can be used to audit an organization's security for phishing attacks using various phishing methods such as Entice to Click, Credential Harvesting, Send Attachment, Training, Vishing, and Smishing.

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

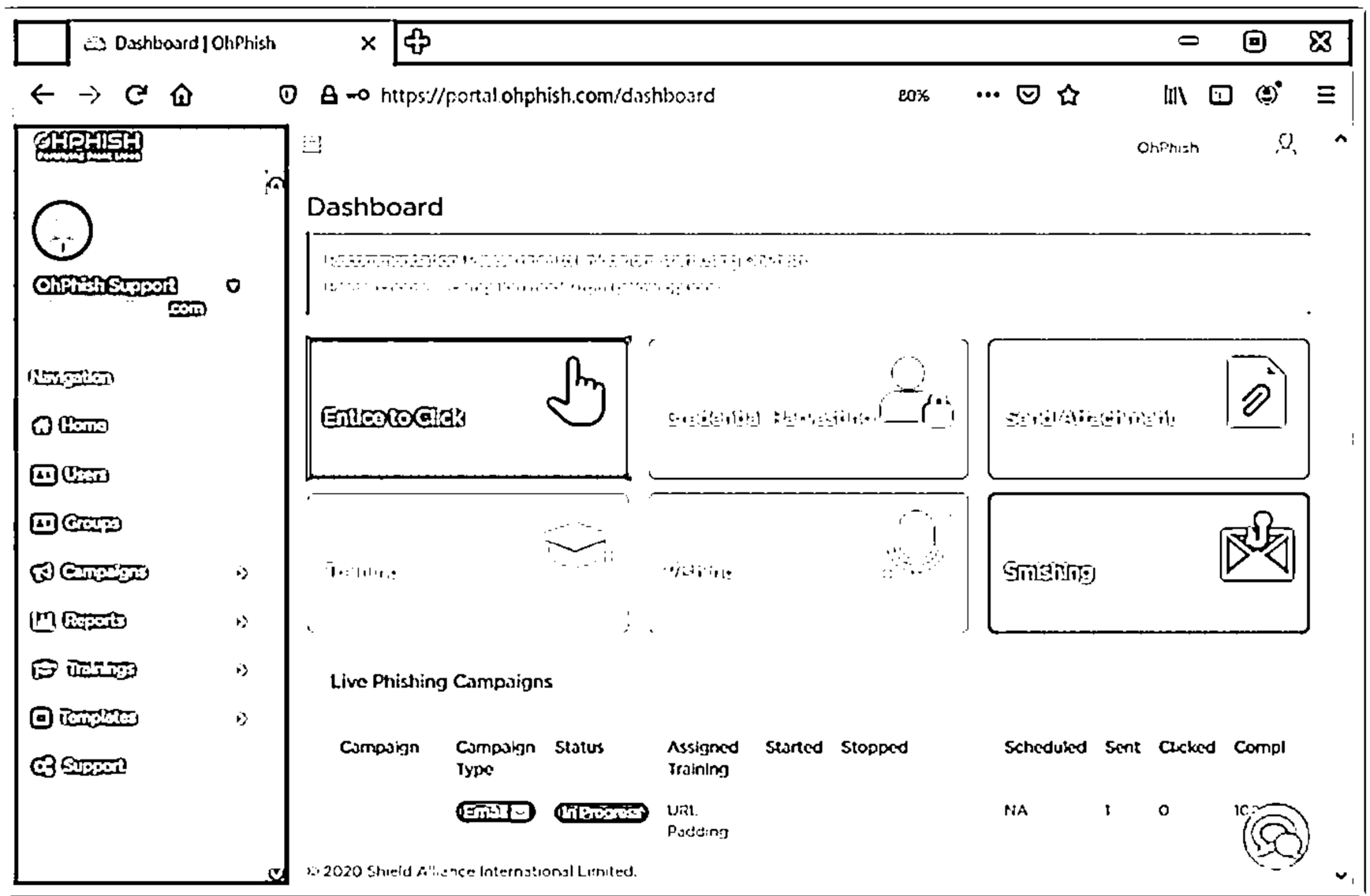


Figure 9.19: Screenshot of OhPhish

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:
  - Social engineering concepts along with various kinds of social engineering attacks
  - Human-, computer-, and mobile-based social engineering techniques
  - Insider threats and the various forms they can take
  - Impersonation on social networking sites
  - Identity theft and the various forms it can take
  - Details of various countermeasures that can defend an organization against social engineering attacks, insider threats, and identity theft
- In the next module, we will see how attackers, as well as ethical hackers and penetration testers, perform DoS/DDoS attacks

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

Module Summary

This module discussed social engineering concepts along with various phases of social engineering attack. It also discussed various human-based, computer-based, and mobile-based social engineering techniques. The module discussed insider threats, including the various types of insider threats. It gave an overview of impersonation on social networking sites. It also discussed identity theft and the types of identity theft. The module ended with a detailed discussion of various signs to watch for and countermeasures to employ in order to defend against social engineering attacks, insider threats, and identity theft.

The next module will show how attackers, as well as ethical hackers and pen testers, perform DoS/DDoS attacks.

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

Module 10: Denial-of-Service

Module Objectives

- Overview of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- Understanding Different DoS/DDoS Attack Techniques
- Understanding the Botnet Network
- Understanding Various DoS and DDoS Attack Tools
- Understanding Different Techniques to Detect DoS and DDoS Attacks
- Understanding Different DoS/DDoS Countermeasures

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

Module Objectives

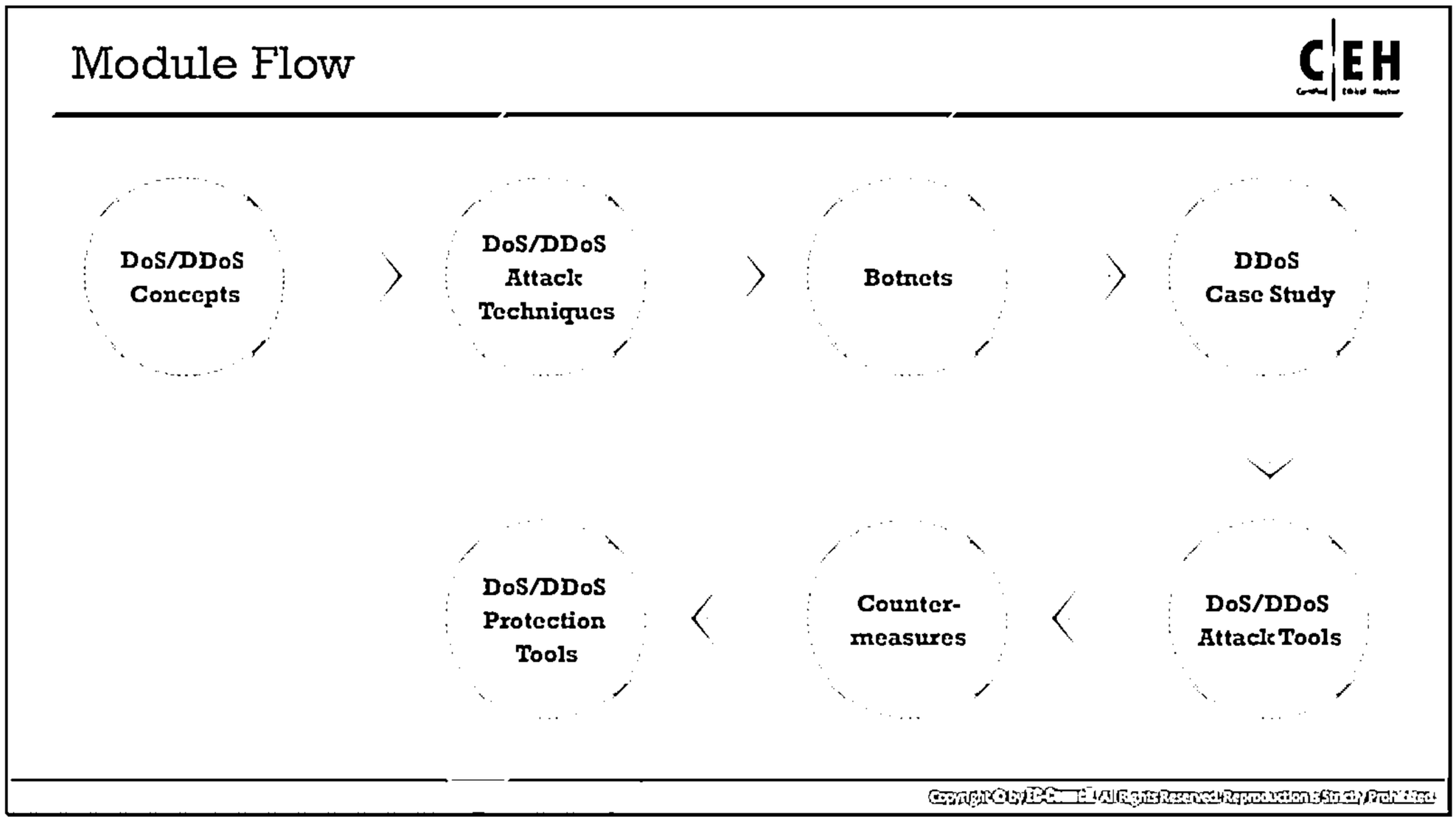
Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are a major threat to computer networks. These attacks attempt to make a machine or network resource unavailable to its authorized users. Usually, DoS/DDoS attacks exploit vulnerabilities in the implementation of the Transmission Control Protocol (TCP)/Internet Protocol (IP) model or bugs in a specific operating system (OS).

This module starts with an overview of DoS and DDoS attacks and then provides insight into different DoS/DDoS attack techniques. Later, it discusses the botnet network, DoS/DDoS attack tools, techniques to detect DoS/DDoS attacks, and DoS/DDoS countermeasures.

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

- Describe DoS/DDoS concepts
- Understand various DoS/DDoS attack techniques
- Describe botnets
- Illustrate DoS/DDoS case studies
- Explain different DoS/DDoS attack tools
- Apply best practices to mitigate DoS/DDoS attacks

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



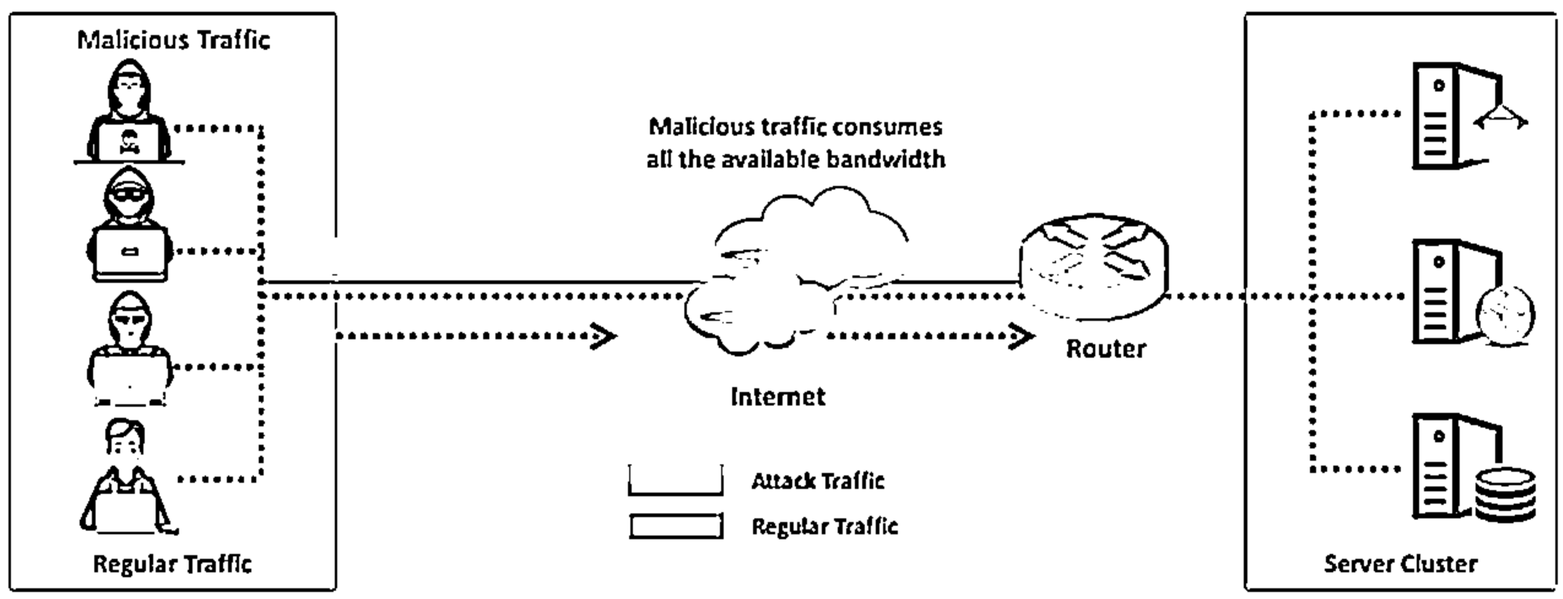
DoS/DDoS Concepts

For a good understanding of DoS/DDoS attacks, one must be familiar with related concepts in advance. This section defines DoS and DDoS attacks and discusses how DDoS attacks work.

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

What is a DoS Attack?

- Denial-of-Service (DoS) is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users
- In a DoS attack, attackers flood the victim system with non-legitimate service requests or traffic to overload its resources



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

What is a DoS Attack?

A DoS attack is an attack on a computer or network that reduces, restricts, or prevents access to system resources for legitimate users. In a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources and bring down the system, leading to the unavailability of the victim's website or at least significantly reducing the victim's system or network performance. The goal of a DoS attack is to keep legitimate users from using the system, rather than to gain unauthorized access to a system or to corrupt data.

The following are examples for types of DoS attacks:

- Flooding the victim's system with more traffic than it can handle
- Flooding a service (e.g., Internet Relay Chat (IRC)) with more events than it can handle
- Crashing a TCP/IP stack by sending corrupt packets
- Crashing a service by interacting with it in an unexpected manner
- Hanging a system by causing it to go into an infinite loop

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

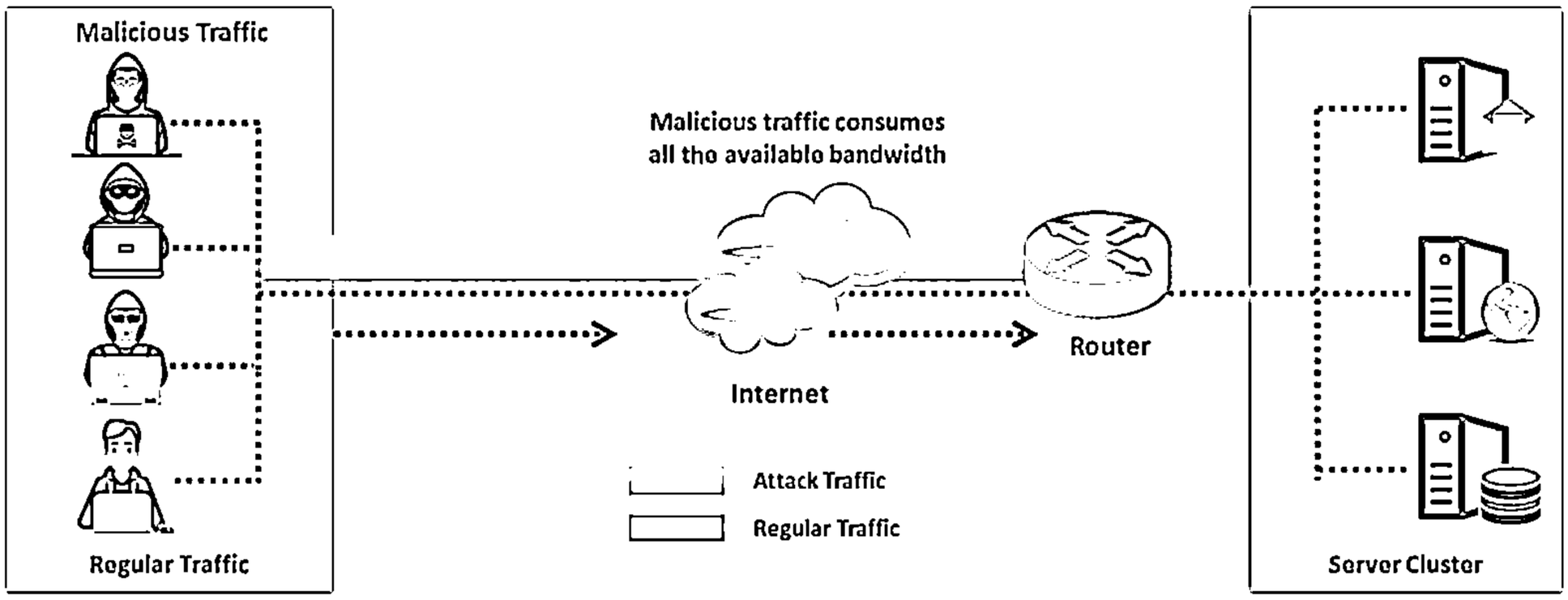


Figure 10.1: Schematic of a DoS attack

DoS attacks have various forms and target various services. The attacks may cause the following:

- Consumption of resources
- Consumption of bandwidth, disk space, CPU time, or data structures
- Actual physical destruction or alteration of network components
- Destruction of programming and files in a computer system

In general, DoS attacks target network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic by using existing network resources, thereby depriving legitimate users of these resources. Connectivity attacks overflow a system with a large number of connection requests, consuming all available OS resources to prevent the system from processing legitimate user requests.

Consider a food catering company that conducts much of its business over the phone. If an attacker wants to disrupt this business, they need to find a way to block the company's phone lines, which would make it impossible for the company to do business. A DoS attack works along the same lines—the attacker uses up all the ways to connect to the victim's system, making legitimate business impossible.

DoS attacks are a kind of security breach that does not generally result in the theft of information. However, these attacks can harm the target in terms of time and resources. Furthermore, security failure might cause the loss of a service such as email. In the worst-case scenario, a DoS attack can cause the accidental destruction of the files and programs of millions of people who were connected to the victim's system at the time of the attack.

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

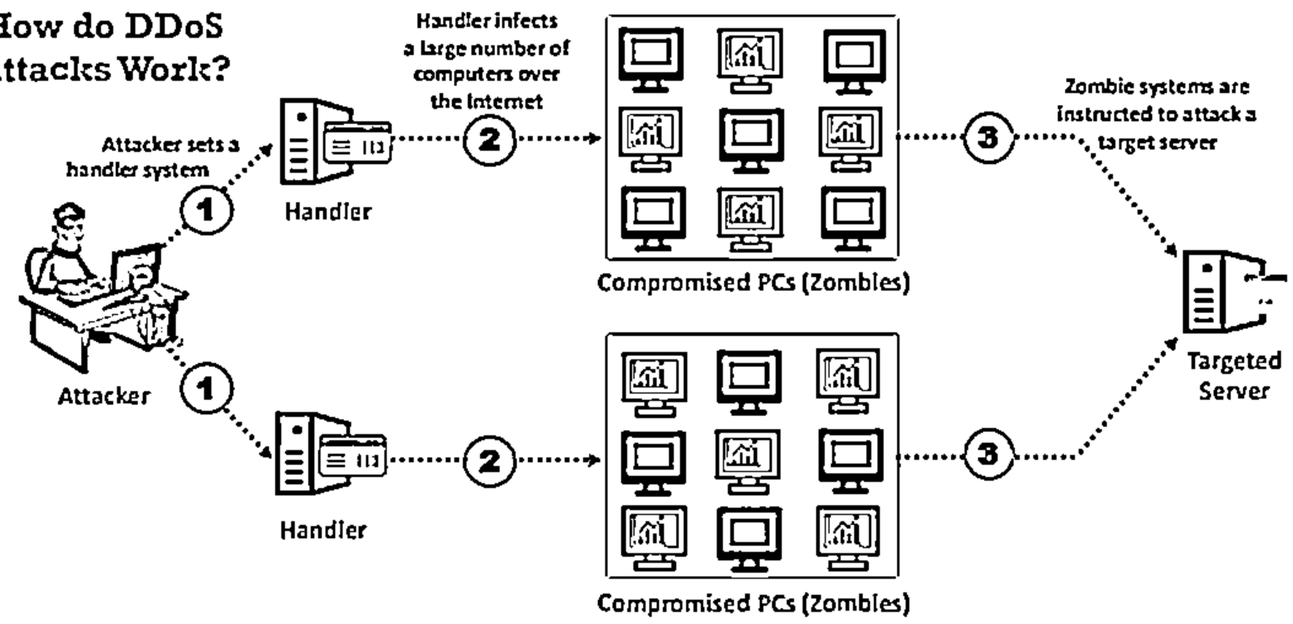
What is a DDoS Attack?

- Distributed denial-of-service (DDoS) is a coordinated attack that involves a multitude of compromised systems (Botnet) attacking a single target, thereby denying service to users of the targeted system

Impact of DDoS

- Loss of Goodwill
- Disabled Network
- Financial Loss
- Disabled Organization

How do DDoS Attacks Work?



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

What is a DDoS Attack?

Source: *http://searchsecurity.techtarget.com*

A DDoS attack is a large-scale, coordinated attack on the availability of services on a victim's system or network resources, and it is launched indirectly through many compromised computers (botnets) on the Internet.

As defined by the World Wide Web Security FAQ, "A distributed denial-of-service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the denial of service significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms." The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to legitimate users.

The services under attack belong to the "primary victim," whereas the compromised systems used to launch the attack are called "secondary victims." The use of secondary victims in performing a DDoS attack enables the attacker to mount a large and disruptive attack while making it difficult to track down the original attacker.

The primary objective of a DDoS attack is to first gain administrative access on as many systems as possible. In general, attackers use a customized attack script to identify potentially vulnerable systems. After gaining access to the target systems, the attacker uploads and runs DDoS software on these systems at the time chosen to launch the attack.

DDoS attacks have become popular because of the easy accessibility of exploit plans and the negligible amount of brainwork required to execute them. These attacks can be very dangerous because they can quickly consume the largest hosts on the Internet, rendering them useless.

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

The impacts of DDoS include the loss of goodwill, disabled networks, financial losses, and disabled organizations.

How do DDoS Attacks Work?

In a DDoS attack, many applications barrage a target browser or network with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the DDoS attack by sending a command to zombie agents, which are Internet-connected computers compromised by an attacker through malware programs to perform various malicious activities through a command and control (C&C) server. These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim, which causes the reflector systems to presume that these requests originate from the victim's machine instead of the zombie agents. Hence, the reflector systems send the requested information (response to the connection request) to the victim. Consequently, the victim's machine is flooded with unsolicited responses from several reflector computers simultaneously, which may either reduce the performance or cause the victim's machine to shut down completely.

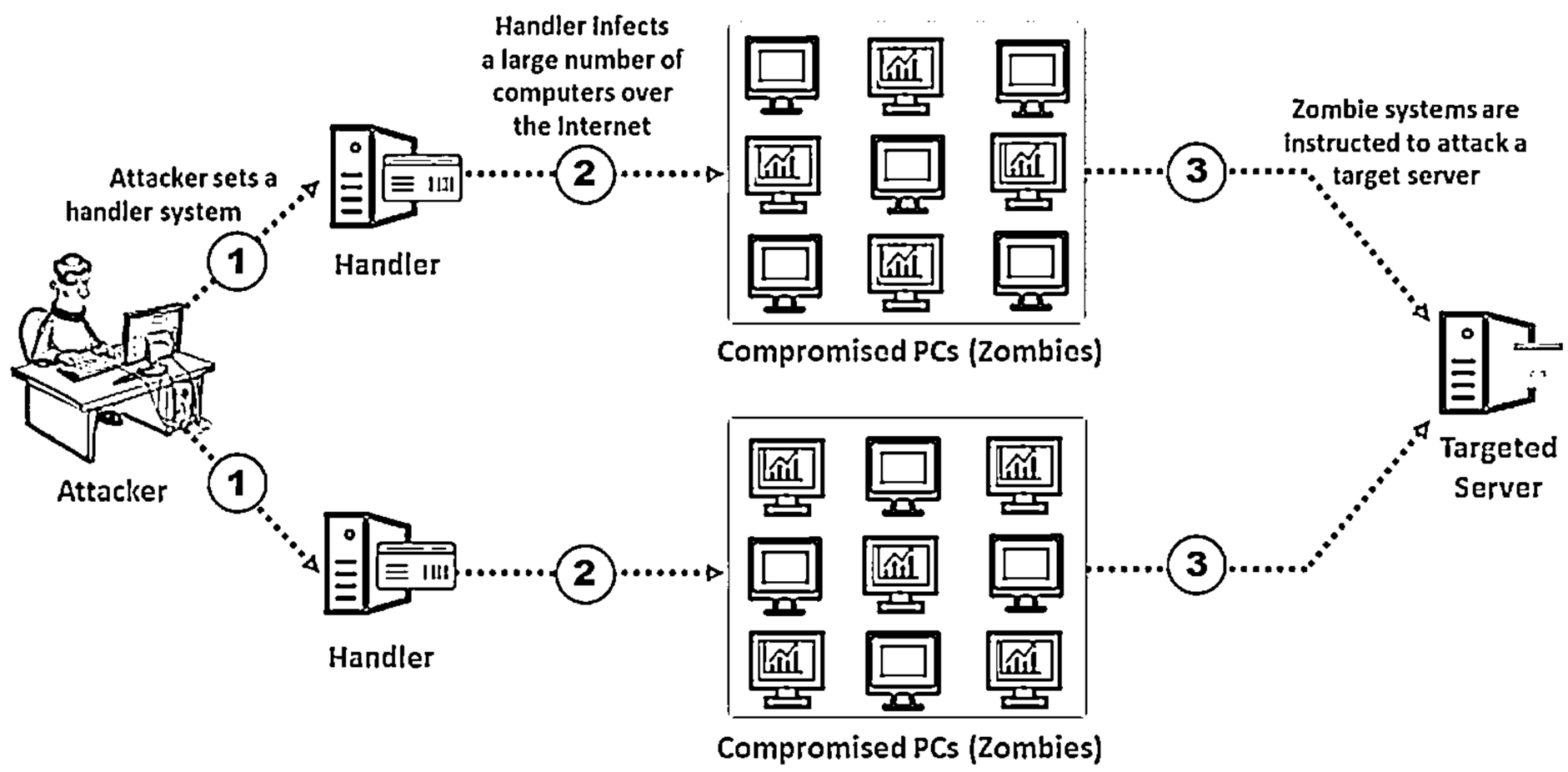
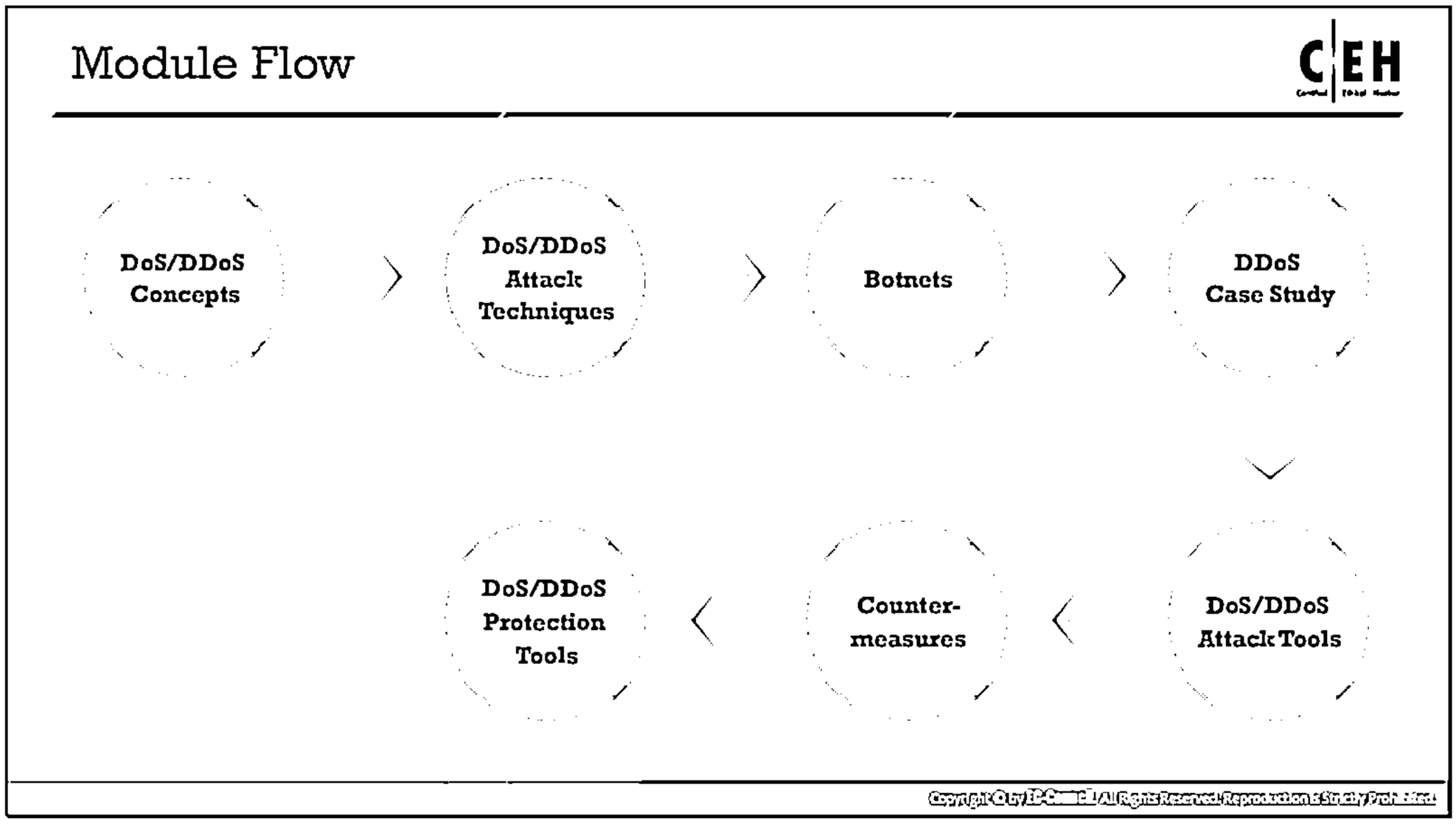


Figure 10.2: Schematic of a DDoS attack

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



DoS/DDoS Attack Techniques

Attackers implement various techniques to launch DoS/DDoS attacks on target computers or networks. This section discusses the basic categories of DoS/DDoS attack vectors and various attack techniques.

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

Basic Categories of DoS/DDoS Attack Vectors

Volumetric Attacks

- Consume the bandwidth of a target network or service
- The magnitude of attack is measured in bits-per-second (bps)
- Types of bandwidth depletion attacks:
  - Flood attacks
  - Amplification attacks

Attack Techniques

- UDP flood attack
- ICMP flood attack
- Ping of Death and Smurf attack
- Pulse wave and zero-day attack

Protocol Attacks

- Consume other types of resources like connection state tables present in network infrastructure components such as load-balancers, firewalls, and application servers
- The magnitude of attack is measured in packets-per-second (pps)

Attack Techniques

- SYN flood attack
- Fragmentation attack
- Spoofed session flood attack
- ACK flood attack

Application Layer Attacks

- Consume the resources or services of an application, thereby making the application unavailable to other legitimate users
- The magnitude of attack is measured in requests-per-second (rps)

Attack Techniques

- HTTP GET/POST attack
- Slowloris attack
- UDP application layer flood attack

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

Basic Categories of DoS/DDoS Attack Vectors

DDoS attacks mainly aim to diminish the network bandwidth by exhausting network, application, or service resources, thereby restricting legitimate users from accessing system or network resources. In general, DoS/DDoS attack vectors are categorized as follows:

- **Volumetric Attacks**

  These attacks exhaust the bandwidth either within the target network/service or between the target network/service and the rest of the Internet to cause traffic blockage, preventing access to legitimate users. The attack magnitude is measured in bits per second (bps).

  Volumetric DDoS attacks generally target protocols such as the Network Time Protocol (NTP), Domain Name System (DNS), and Simple Service Discovery Protocol (SSDP), which are stateless and do not have built-in congestion avoidance features. The generation of a large number of packets can cause the consumption of the entire bandwidth on the network. A single machine cannot make enough requests to overwhelm network equipment. Hence, in DDoS attacks, the attacker uses several computers to flood a victim. In this case, the attacker can control all the machines and instruct them to direct traffic to the target system. DDoS attacks flood a network, causing a significant statistical change in network traffic that overwhelms network equipment such as switches and routers. Attackers use the processing power of a large number of geographically distributed machines to generate huge traffic directed at the victim, which is why such an attack is called a DDoS attack.

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

There are two types of bandwidth depletion attacks:

- In a **flood attack**, zombies send large volumes of traffic to the victim's systems to exhaust the bandwidth of these systems.
- In an **amplification attack**, the attacker or zombies transfer messages to a broadcast IP address. This method amplifies malicious traffic that consumes the bandwidth of the victim's systems.

Attackers use botnets and perform DDoS attacks by flooding the network. The entire bandwidth is used up by attackers, and no bandwidth remains for legitimate use. The following are examples for volumetric attack techniques:

- User Datagram Protocol (UDP) flood attack
- Internet Control Message Protocol (ICMP) flood attack
- Ping of Death (PoD) attack
- Smurf attack
- Pulse wave attack
- Zero-day attack
- Malformed IP packet flood attack
- Spoofed IP packet flood attack

- **Protocol Attacks**

  Attackers can also prevent access to a target by consuming types of resources other than bandwidth, such as connection state tables. Protocol DDoS attacks exhaust resources available on the target or on a specific device between the target and the Internet. These attacks consume the connection state tables present in network infrastructure devices such as load balancers, firewalls, and application servers. Consequently, no new connections will be allowed, because the device will be waiting for existing connections to close or expire. In this case, the attack magnitude is measured in packets per second (pps) or connections per second (cps). These attacks can even take over the state of millions of connections maintained by high-capacity devices.

  The following are examples for protocol attack techniques:

  - Synchronize (SYN) flood attack
  - Fragmentation attack
  - Spoofed session flood attack
  - Acknowledgement (ACK) flood attack
  - SYN-ACK flood attack
  - ACK and PUSH ACK flood attack
  - TCP connection flood attack
  - TCP state exhaustion attack
  - RST attack

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

- **Application Layer Attacks**

  In these attacks, the attacker attempts to exploit vulnerabilities in the application layer protocol or in the application itself to prevent legitimate users from accessing the application. Attacks on unpatched, vulnerable systems do not require as much bandwidth as protocol or volumetric DDoS attacks for succeeding. In application DDoS attacks, the application layer or application resources are consumed by opening connections and leaving them open until no new connections can be made. These attacks destroy a specific aspect of an application or service and can be effective with one or a few attacking machines that produce a low traffic rate. Furthermore, these attacks are very difficult to detect and mitigate. The magnitude of attack is measured in requests per second (rps).

  Application-level flood attacks result in the loss of services of a particular network, such as emails and network resources, or the temporary shutdown of applications and services. Through this attack, attackers exploit weaknesses in programming source code to prevent the application from processing legitimate requests.

  Several kinds of DoS attacks rely on software-related exploits such as buffer overflows. A buffer overflow attack sends excessive data to an application that either shuts down the application or forces the data sent to the application to run on the host system. The attack crashes a vulnerable system remotely by sending excessive traffic to an application.

  Occasionally, attackers can also execute arbitrary code on the remote system via a buffer overflow. Sending too much data to an application overwrites the data that controls the program, enabling the hacker to run their code instead.

  Using application-level flood attacks, attackers attempt to do the following:

  - Flood web applications with legitimate user traffic
  - Disrupt service to a specific system or person by, for example, blocking a user's access through repeated invalid login attempts
  - Jam the application database connection by crafting malicious Structured Query Language (SQL) queries

  Application-level flood attacks can result in a substantial loss of money, service, and reputation for organizations. These attacks occur after the establishment of a connection. Because a connection is established and the traffic entering the target appears to be legitimate, it is difficult to detect these attacks. However, if the user identifies the attack, they can stop it and trace it back to its source more easily than other types of DDoS attacks.

  The following are examples for application layer attack techniques:

  - Hypertext Transfer Protocol (HTTP) flood attack
  - Slowloris attack
  - UDP application layer flood attack

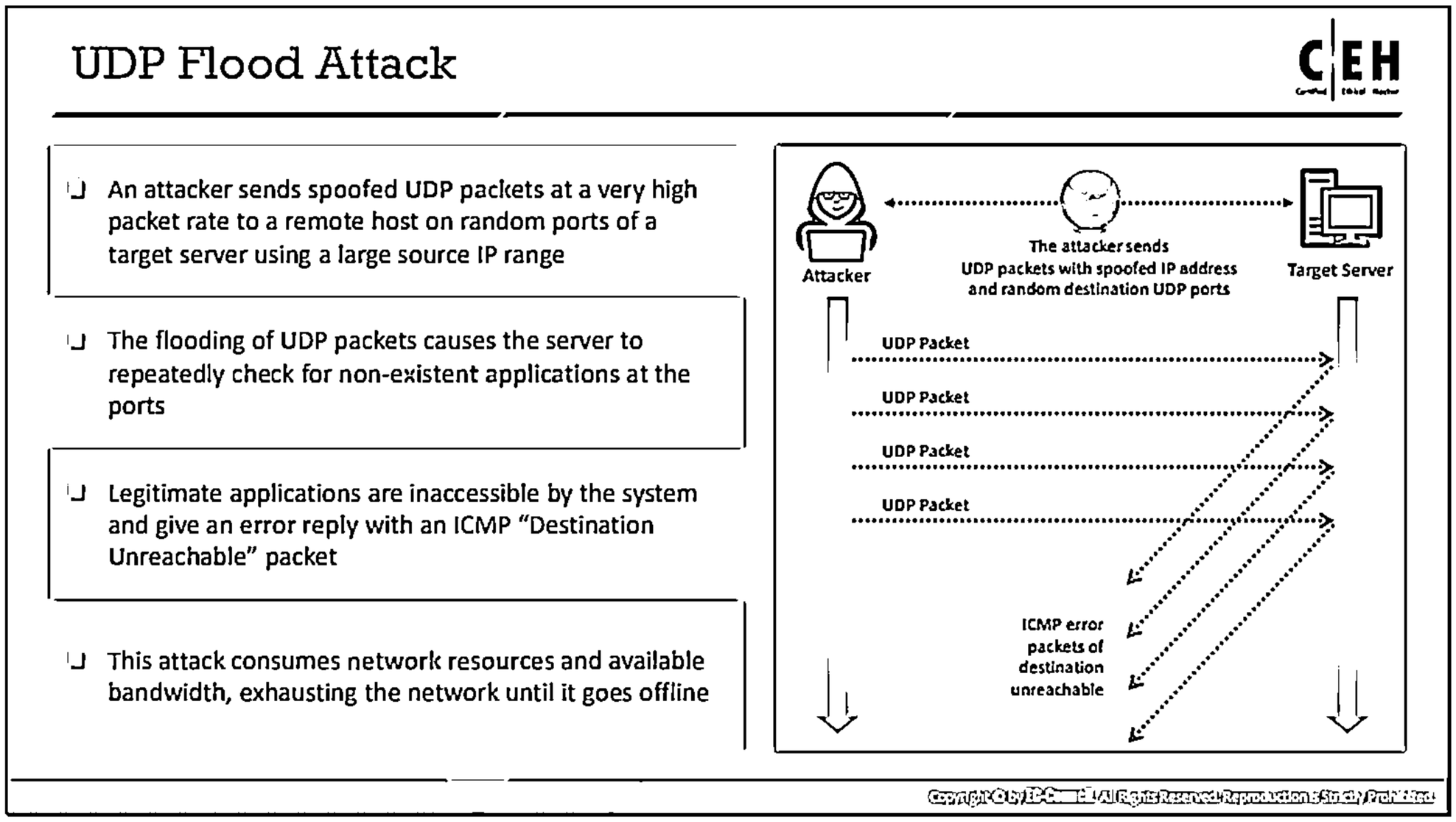
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

DoS/DDoS Attack Techniques

Next, the following DoS/DDoS attack techniques will be discussed:

- UDP flood attack
- ICMP flood attack
- PoD attack
- Smurf attack
- Pulse wave attack
- Zero-day attack
- SYN flood attack
- Fragmentation attack
- ACK flood attack
- TCP state exhaustion attack
- Spoofed session flood attack
- HTTPS GET/POST attack
- Slowloris attack
- UDP application layer flood attack
- Multi-vector attack
- Peer-to-peer attack
- Permanent DoS (PDoS) attack
- Distributed reflection DoS (DRDoS) attack

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



UDP Flood Attack

In a UDP flood attack, an attacker sends spoofed UDP packets at a very high packet rate to a remote host on random ports of a target server by using a large source IP range. The flooding of UDP packets causes the server to check repeatedly for nonexistent applications at the ports. Consequently, legitimate applications become inaccessible by the system, and any attempts to access them return an error reply with an ICMP "Destination Unreachable" packet. This attack consumes network resources and available bandwidth, exhausting the network until it goes offline.

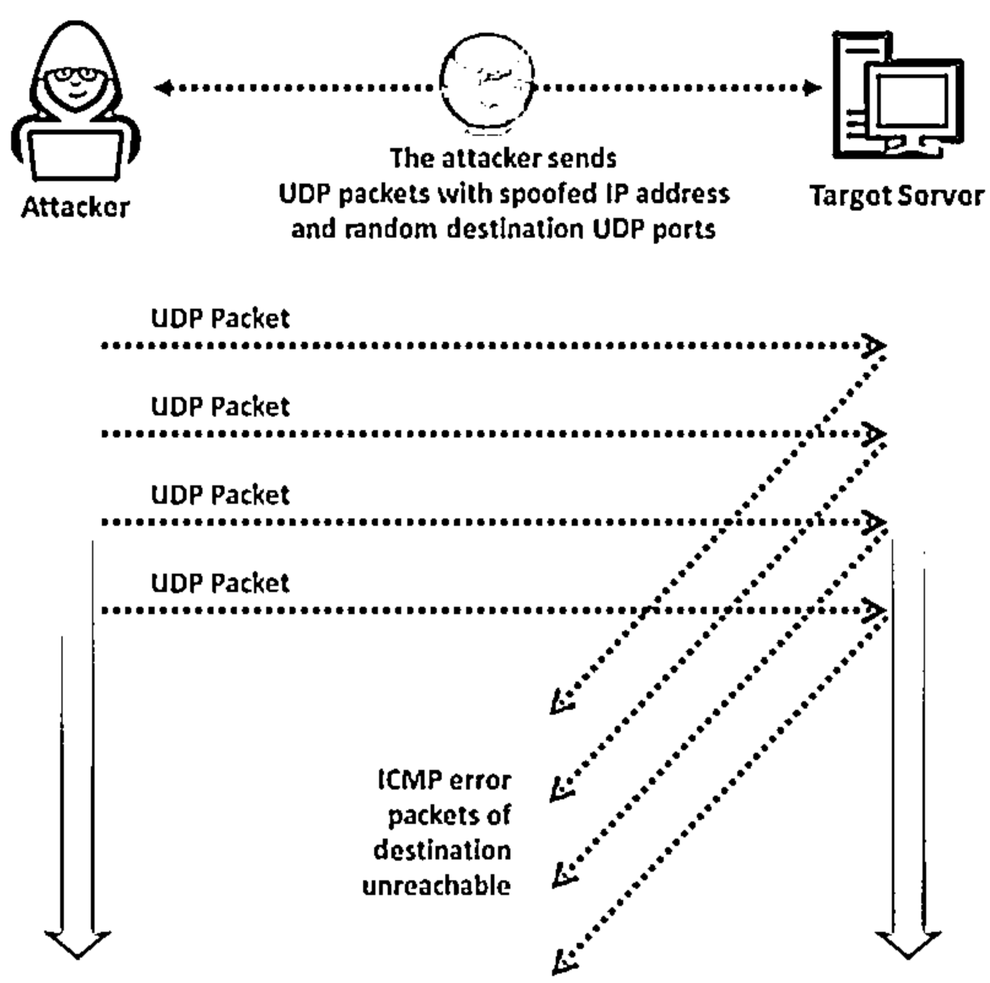
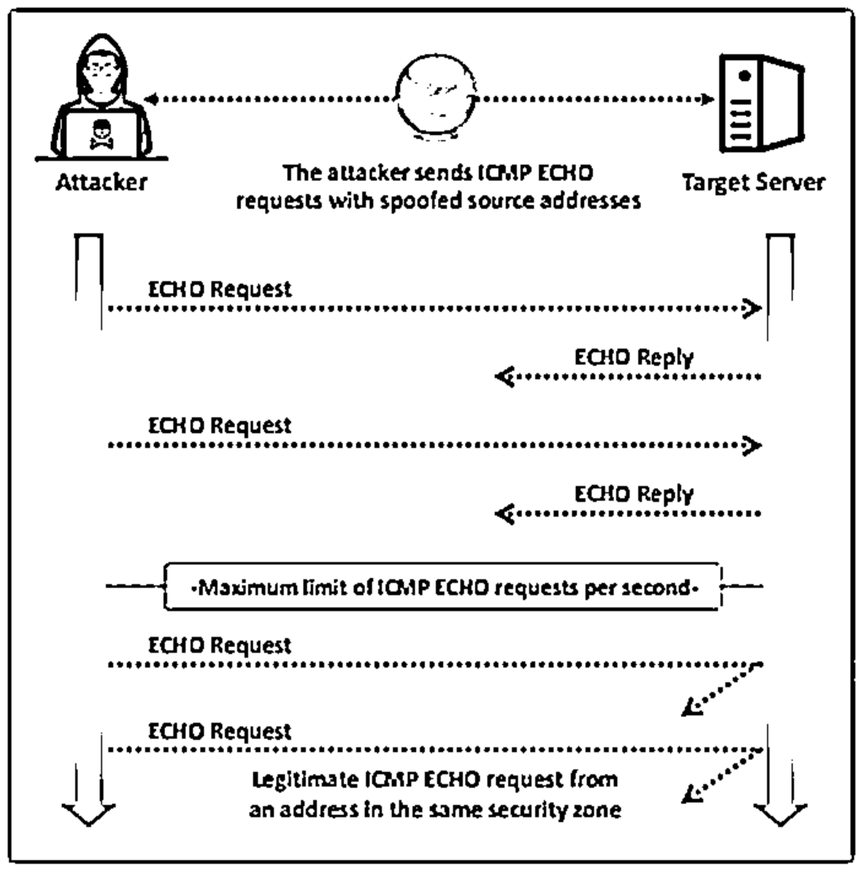


Figure 10.3: UDP flood attack

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

ICMP Flood Attack

- Network administrators use ICMP primarily for IP operations and troubleshooting, and error messaging is used for undeliverable packets
- ICMP flood attacks are a type of attack in which attackers send large volumes of ICMP echo request packets to a victim system directly or through reflection networks
- These packets signal the victim's system to reply, and the resulting combination of traffic saturates the bandwidth of the victim's network connection, causing it to be overwhelmed and subsequently stop responding to legitimate TCP/IP requests
- To protect against ICMP flood attacks, set a threshold limit that invokes an ICMP flood attack protection feature when exceeded



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

ICMP Flood Attack

Network administrators use ICMP primarily for IP operations, troubleshooting, and error messaging for undeliverable packets. In this attack, attackers send large volumes of ICMP echo request packets to a victim's system directly or through reflection networks. These packets signal the victim's system to reply, and the large traffic saturates the bandwidth of the victim's network connection, causing it to be overwhelmed and subsequently stop responding to legitimate TCP/IP requests.

To protect against ICMP flood attacks, it is necessary to set a threshold that invokes the ICMP flood attack protection feature when exceeded. When the ICMP threshold is exceeded (by default, the threshold value is 1000 packets/s), the router rejects further ICMP echo requests from all addresses in the same security zone for the remainder of the current second as well as the next second.

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

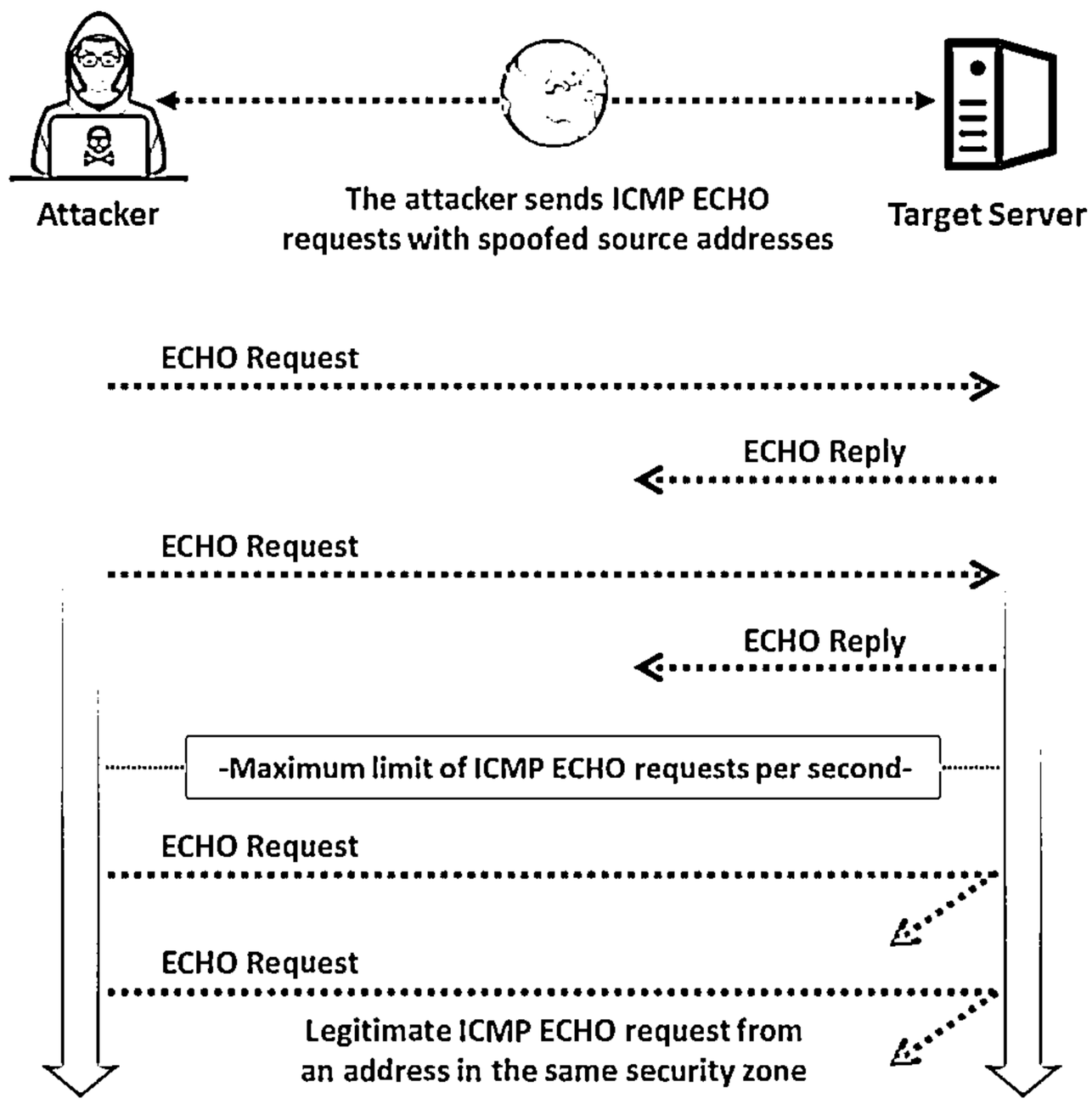


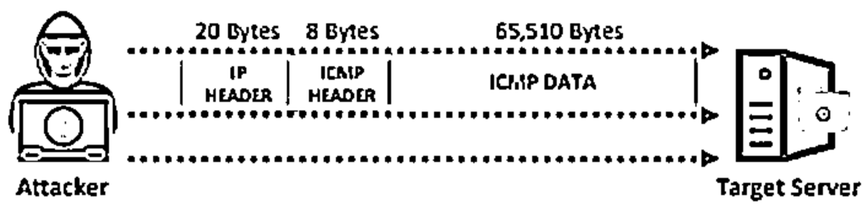
Figure 10.4: ICMP flood attack

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

Ping of Death and Smurf Attacks

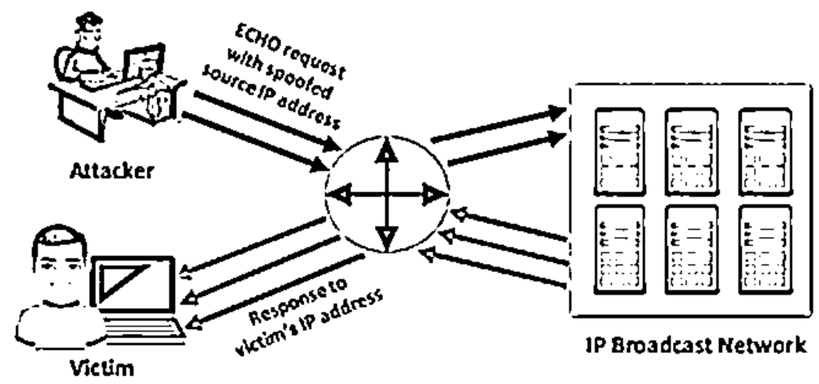
Ping of Death Attack

- In a Ping of Death (PoD) attack, an attacker tries to crash, destabilize, or freeze the targeted system or service by sending malformed or oversized packets using a simple ping command
- For instance, the attacker sends a packet which has a size of 65,538 bytes to the target web server. This packet size exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The reassembly process of the receiving system might cause the system to crash



Smurf Attack

- In a Smurf attack, the attacker spoofs the source IP address with the victim's IP address and sends a large number of ICMP ECHO request packets to an IP broadcast network
- This causes all the hosts on the broadcast network to respond to the received ICMP ECHO requests. These responses will be sent to the victim machine, ultimately causing the machine to crash



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

Ping of Death Attack

In a Ping of Death (PoD) attack, an attacker attempts to crash, destabilize, or freeze the target system or service by sending malformed or oversized packets using a simple ping command. Suppose an attacker sends a packet with a size of 65,538 bytes to the target web server. This size exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The reassembly process performed by the receiving system might cause the system to crash. In such attacks, the attacker's identity can be easily spoofed, and the attacker might not need detailed knowledge of the target machine, except its IP address.

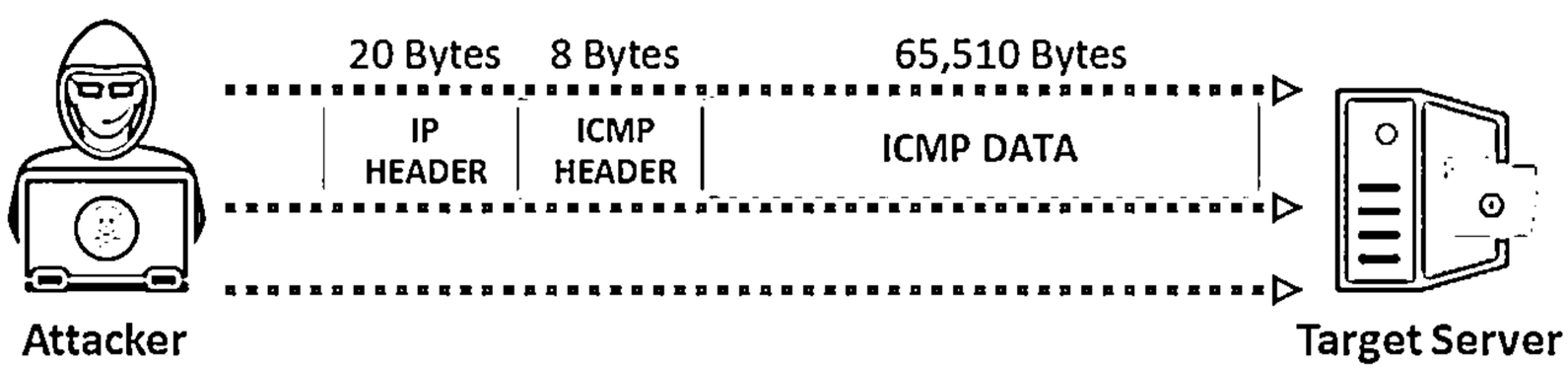


Figure 10.5: Ping-of-death attack

Smurf Attack

In a Smurf attack, the attacker spoofs the source IP address with the victim's IP address and sends a large number of ICMP ECHO request packets to an IP broadcast network. This causes all the hosts on the broadcast network to respond to the received ICMP ECHO requests. These responses are sent to the victim's machine because the IP address was spoofed by the attacker, causing significant traffic to the victim's machine and ultimately making it crash.

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

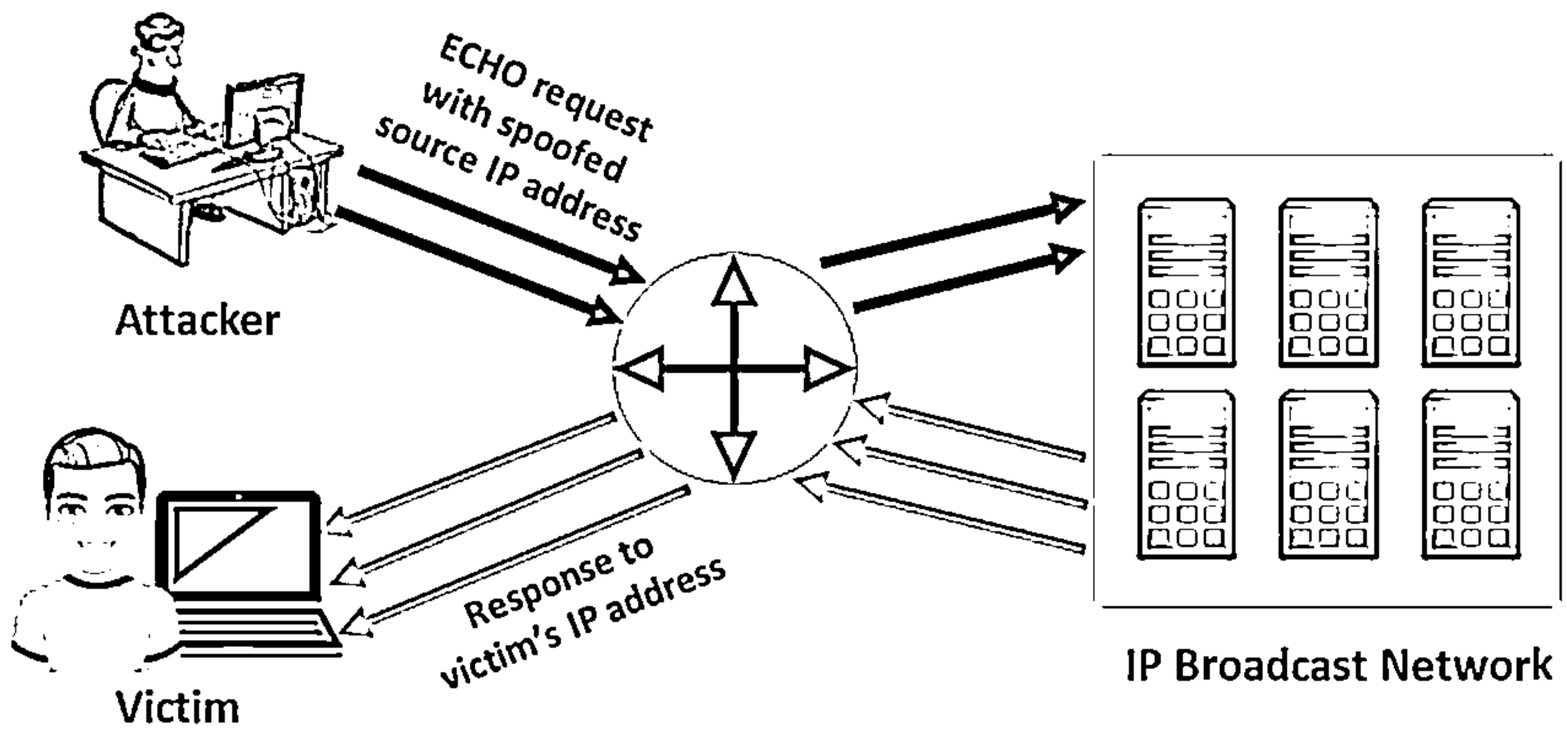


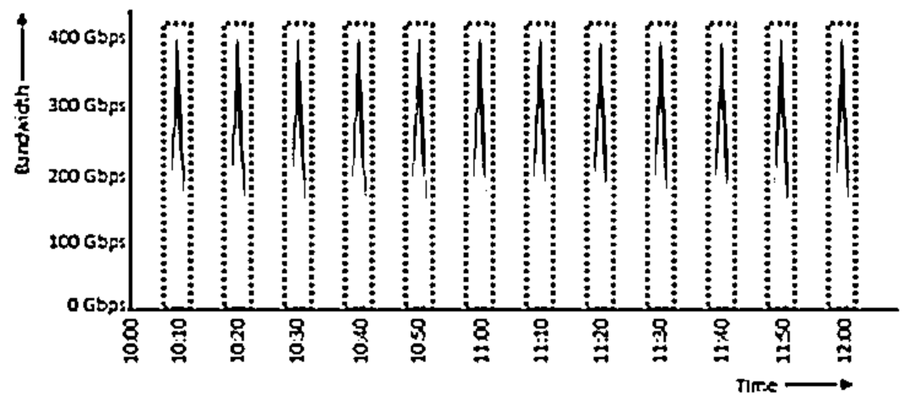
Figure 10.6: Smurf attack

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

Pulse Wave and Zero-Day DDoS Attacks

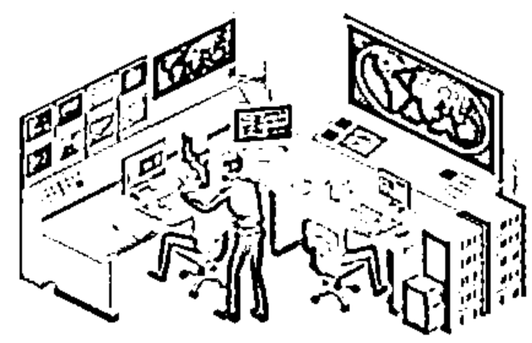
Pulse Wave DDoS Attack

- In a pulse wave DDoS attack, attackers send a highly repetitive, periodic train of packets as pulses to the target victim every 10 minutes, and each specific attack session can last for a few hours to days
- A single pulse (300 Gbps or more) is sufficient to crowd a network pipe



Zero-Day DDoS Attack

- A zero-day DDoS attack is delivered before the DDoS vulnerabilities of a system have been patched or effective defensive mechanisms are implemented
- Until the victim deploys a patch for the exploited DDoS vulnerability, an attacker can actively block all the victim's resources and steal the victim's data
- These attacks can cause severe damage to the victim's network infrastructure and assets



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

Pulse Wave DDoS Attack

Pulse wave DDoS attacks are the latest type of DDoS attacks employed by threat actors to disrupt the standard operations of targets. Generally, DDoS attack patterns are continuous incoming traffic flows. However, in pulse wave DDoS attacks, the attack pattern is periodic, and the attack is huge, consuming the entire bandwidth of target networks. Attackers send a highly repetitive train of packets as pulses to the target victim every 10 min, and the attack session lasts for approximately an hour or some days. A single pulse (300 Gbps or more) is more than enough to crowd a network pipe. Recovery from such attacks is very difficult and occasionally impossible.

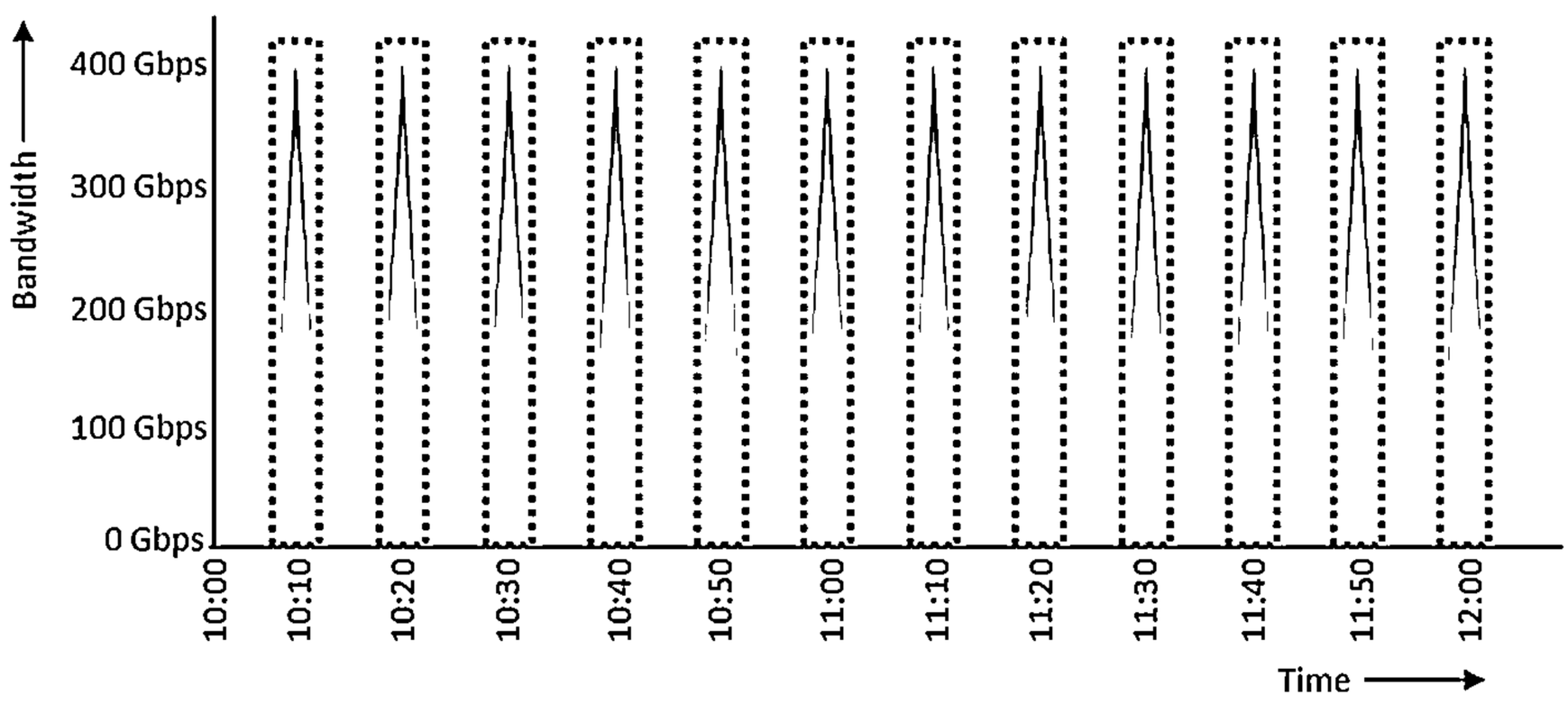


Figure 10.7: Pulse wave DDoS attack

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

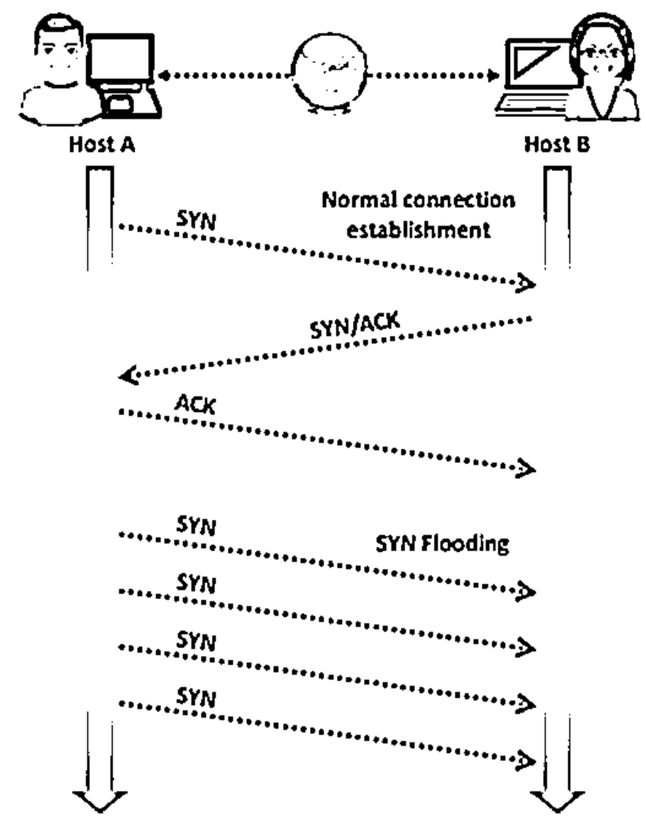
Zero-Day DDoS Attack

Zero-day DDoS attacks are attacks in which DDoS vulnerabilities do not have patches or effective defensive mechanisms. Until the victim identifies the threat actor's attack strategy and deploys a patch for the exploited DDoS vulnerability, the attacker actively blocks all the victim's resources and steals the victim's data. These attacks can cause severe damage to the victim's network infrastructure and assets. Currently, there is no versatile approach to protect networks from this type of attack.

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

SYN Flood Attack

- The attacker sends a large number of SYN requests with fake source IP addresses to the target server (victim)
- The target machine sends back a SYN/ACK in response to the request and waits for the ACK to complete the session setup
- The target machine does not get the response because the source address is fake
- SYN flooding takes advantage of a flaw in the implementation of the TCP three-way handshake in most hosts
- When Host B receives the SYN request from Host A, it must keep track of the partially opened connection in a "listen queue" for at least 75 seconds
- A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but never replying to the SYN/ACK
- The victim's listen queue is quickly filled up
- The ability to delay each incomplete connection for 75 seconds can be used cumulatively as a Denial-of-Service attack



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

SYN Flood Attack

In a SYN attack, the attacker sends a large number of SYN requests to the target server (victim) with fake source IP addresses. The attack creates incomplete TCP connections that use up network resources. Normally, when a client wants to begin a TCP connection to a server, the client and server exchange the following series of messages:

- A TCP SYN request packet is sent to a server.
- The server sends a SYN/ACK (acknowledgement) in response to the request.
- The client sends a response ACK to the server to complete the session setup.

This method is a "three-way handshake."

In a SYN attack, the attacker exploits the three-way handshake method. First, the attacker sends a fake TCP SYN request to the target server. After the server sends a SYN/ACK in response to the client's (attacker's) request, the client never sends an ACK response. This leaves the server waiting to complete the connection.

SYN flooding takes advantage of the flawed manner in which most hosts implement the TCP three-way handshake. This attack occurs when the attacker sends unlimited SYN packets (requests) to the host system. The process of transmitting such packets is faster than the system can handle. Normally, a connection is established with the TCP three-way handshake. The host keeps track of partially open connections while waiting for response ACK packets in a listening queue.

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

As shown in the figure, when Host B receives a SYN request from Host A, it must keep track of the partially opened connection in a "listen queue" for at least 75 s.

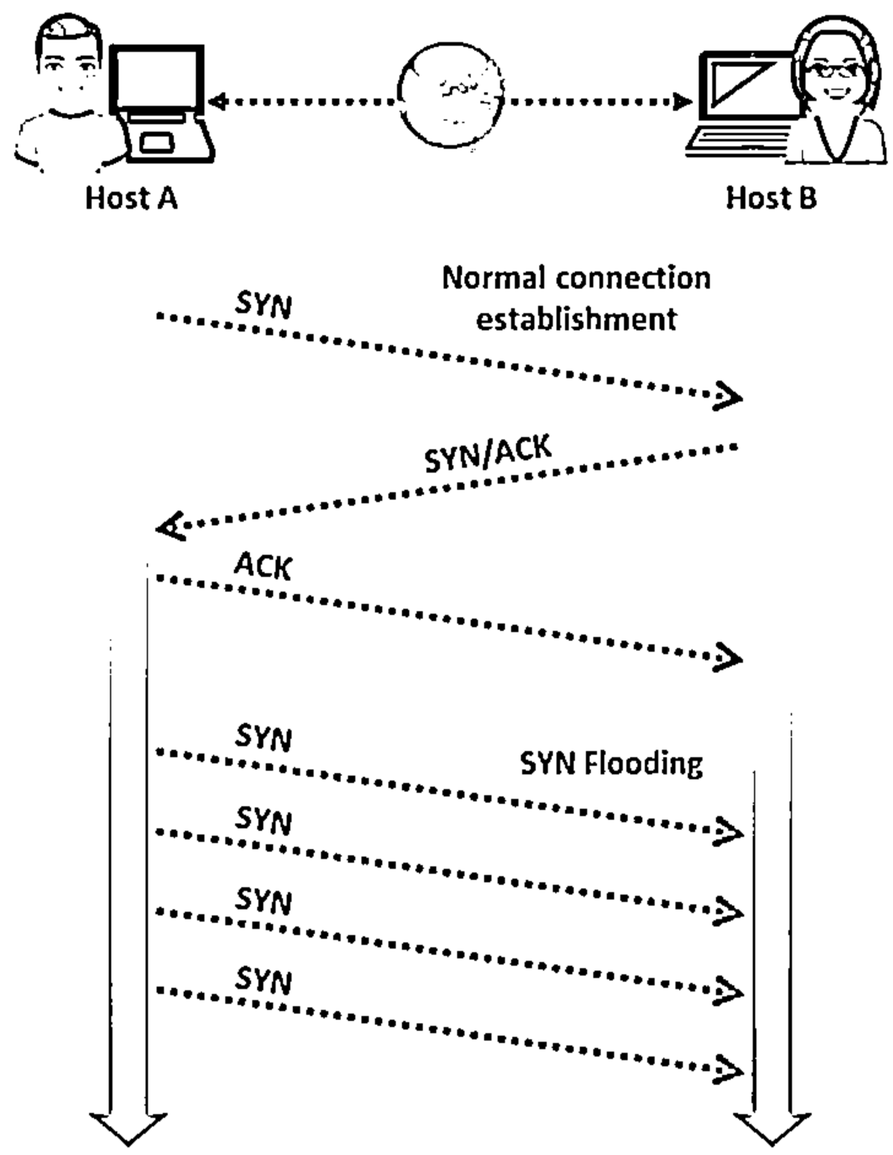


Figure 10.8: SYN flood attack

A malicious host can exploit another host, managing many partial connections by sending many SYN requests to the target host simultaneously. When the queue is full, the system cannot open new connections until it drops some entries from the connection queue through handshake timeouts. This ability to hold up each incomplete connection for 75 s can be cumulatively exploited in a DoS attack. The attack uses fake IP addresses, making it difficult to trace the source. An attacker can fill a table of connections even without spoofing the source IP address.

In addition to SYN flood attacks, attackers can also employ SYN-ACK and ACK/PUSH ACK flood attacks to disrupt target machines. All these attacks are similar in functionality with minor variations.

SYN-ACK Flood Attack

This type of attack is similar to the SYN flood attack, except that in this type of flood attack, the attacker exploits the second stage of a three-way handshake by sending a large number of SYN-ACK packets to the target machine to exhaust its resources.

ACK and PUSH ACK Flood Attack

During an active TCP session, ACK and PUSH ACK are the flags used to transfer information to and from the server and client machines till the session ends. In an ACK and PUSH ACK flood attack, attackers send a large amount of spoofed ACK and PUSH ACK packets to the target machine, making it non-functional.

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

Countermeasures for SYN Flood Attacks

Proper packet filtering is a viable solution to SYN flood attacks. An administrator can also tune the TCP/IP stack to reduce the impact of SYN attacks while allowing legitimate client traffic.

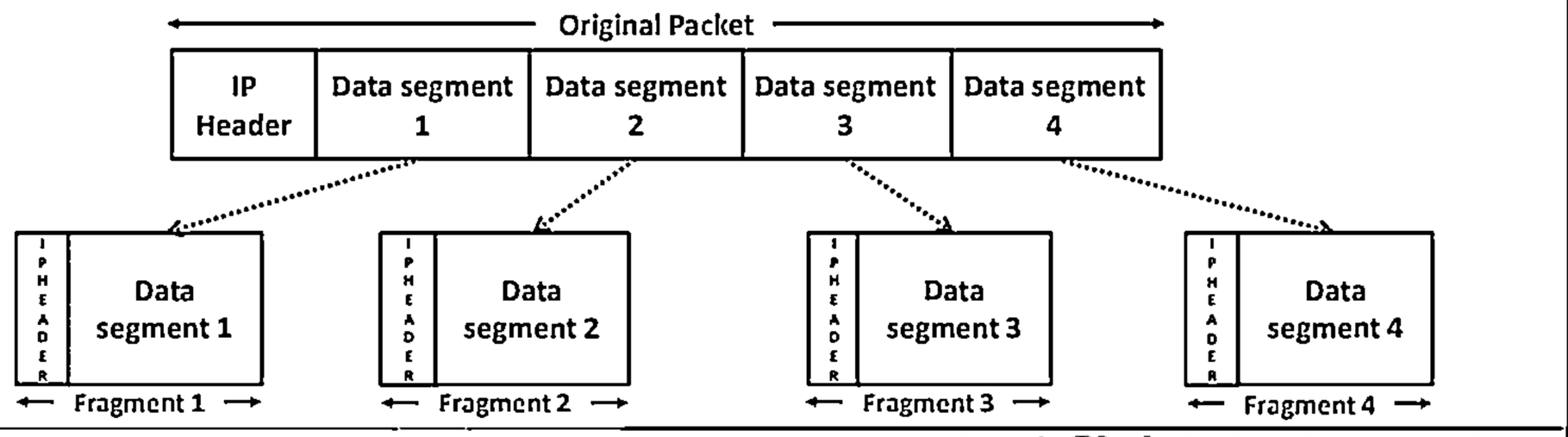
Some SYN attacks do not attempt to upset servers; instead, they attempt to consume the entire bandwidth of the Internet connection. Two tools to counter this attack are SYN cookies and SynAttackProtect.

To guard against an attacker attempting to consume the bandwidth of an Internet connection, an administrator can implement some additional safety measures; for example, they can decrease the time-out period in which a pending connection is maintained in the "SYN RECEIVED" state in the queue. Normally, if a client sends no response ACK, a server will retransmit the first ACK packet. This vulnerability can be removed by decreasing the time of the first packet's retransmission, decreasing the number of packet retransmissions, or turning off packet retransmissions entirely.

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

Fragmentation Attack

- These attacks stop a victim from being able to re-assemble fragmented packets by flooding the target system with TCP or UDP fragments, resulting in reduced performance. Attackers send a large number of fragmented (1500+ byte) packets to a target web server with a relatively small packet rate
- Because the protocol allows for fragmentation, these packets usually pass uninspected through network equipment such as routers, firewalls, and IDS/IPS
- Reassembling and inspecting these large fragmented packets consumes excessive resources. Moreover, the content in the packet fragments will be randomized by the attacker, which in turn makes the process consume more resources, causing the system to crash



Fragmentation Attack

These attacks destroy a victim's ability to reassemble fragmented packets by flooding it with TCP or UDP fragments, resulting in reduced performance. In fragmentation attacks, the attacker sends a large number of fragmented (1500+ byte) packets to a target web server with a relatively small packet rate. Since the protocol allows fragmentation, these packets are usually uninspected as they pass through network equipment such as routers, firewalls, and the intrusion detection system (IDS)/intrusion prevention system (IPS). The reassembly and inspection of these large fragmented packets consume excessive resources. Moreover, the content in the packet fragments is randomized by the attacker, which makes the reassembly and inspection consume more resources and, in turn, causes the system to crash.

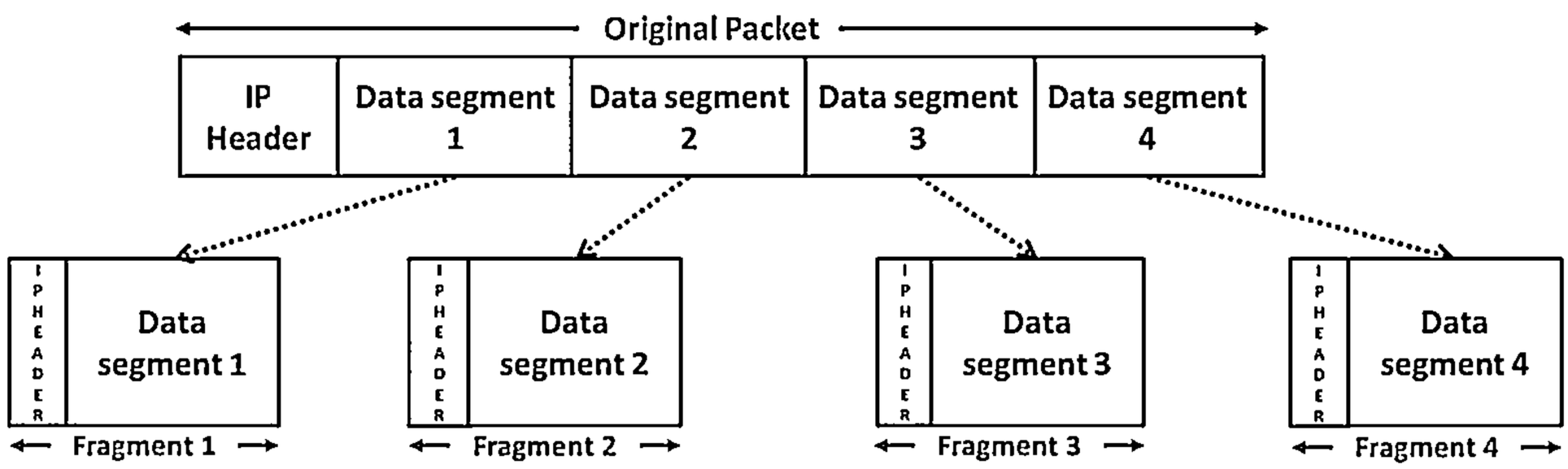
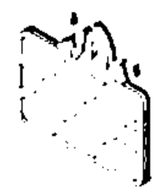


Figure 10.9: Fragmentation attack

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

Spoofed Session Flood Attack

- Attackers create fake or spoofed TCP sessions by carrying multiple SYN, ACK, and RST or FIN packets
- Attackers employ this attack to bypass firewalls and perform DDoS attacks against the target network, exhausting its network resources



Multiple SYN-ACK Spoofed Session Flood Attack

- Attackers create a fake session with multiple SYN and multiple ACK packets along with one or more RST or FIN packets

Multiple ACK Spoofed Session Flood Attack

- Attackers create a fake session by completely skipping the SYN packets and using only multiple ACK packets along with one or more RST or FIN packets

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

Spoofed Session Flood Attack

In this type of attack, attackers create fake or spoofed TCP sessions by carrying multiple SYN, ACK, and RST or FIN packets. Attackers employ this attack to bypass firewalls and perform DDoS attacks against target networks, exhausting their network resources.

The following are examples for spoofed session flood attacks:

- **Multiple SYN-ACK Spoofed Session Flood Attack**

  In this type of flood attack, attackers create a fake session with multiple SYN and multiple ACK packets, along with one or more RST or FIN packets.

- **Multiple ACK Spoofed Session Flood Attack**

  In this type of flood attack, attackers create a fake session by completely skipping SYN packets and using only multiple ACK packets along with one or more RST or FIN packets. Because SYN packets are not employed and firewalls mostly use SYN packet filters to detect abnormal traffic, the DDoS detection rate of the firewalls is very low for these types of attacks.

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

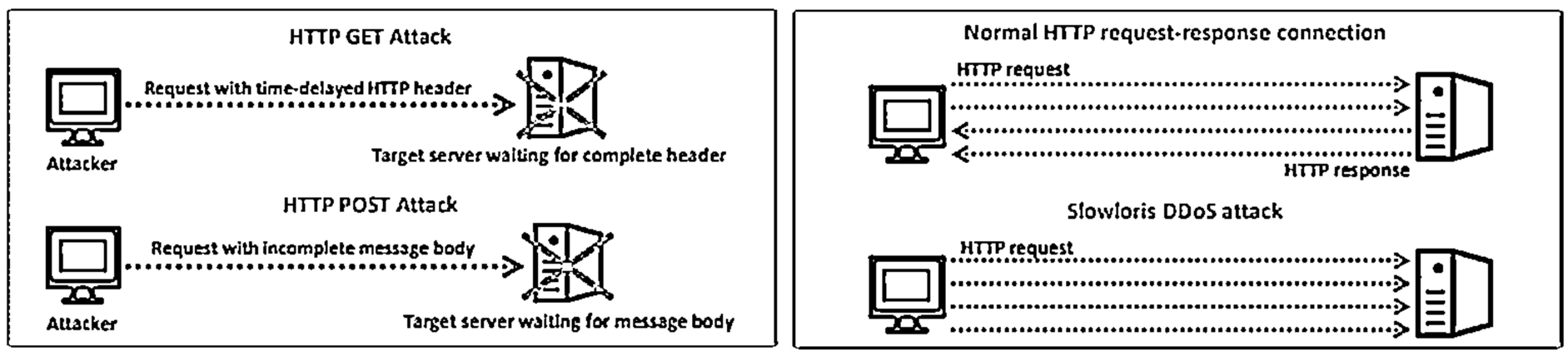
HTTP GET/POST and Slowloris Attacks

HTTP GET/POST Attack

- HTTP clients such as web browsers connect to a web server through the HTTP protocol to send HTTP requests. These requests can be either HTTP GET or HTTP POST
- In an HTTP GET attack, attackers use a time-delayed HTTP header to maintain HTTP connections and exhaust web server resources
- In an HTTP POST attack, attackers send HTTP requests with complete headers but with incomplete message bodies to the target web server or application, prompting the server to wait for the rest of the message body

Slowloris Attack

- In the Slowloris attack, the attacker sends partial HTTP requests to the target web server or application
- Upon receiving the partial HTTP requests, the target server opens multiple open connections and keeps waiting for the requests to complete
- These requests will not be complete, and as a result, the target server's maximum concurrent connection pool will be exhausted, and additional connection attempts will be denied



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

HTTP GET/POST Attack

HTTP attacks are layer-7 attacks. HTTP clients, such as web browsers, connect to a web server through HTTP to send HTTP requests, which can be either HTTP GET or HTTP POST. Attackers exploit these requests to perform DoS attacks.

In an HTTP GET attack, the attacker uses a time-delayed HTTP header to hold on to an HTTP connection and exhaust web-server resources. The attacker never sends the full request to the target server. Consequently, the server retains the HTTP connection and waits, making it inaccessible for legitimate users. In these types of attacks, all the network parameters appear healthy while the service remains unavailable.

In an HTTP POST attack, the attacker sends HTTP requests with complete headers but an incomplete message body to the target web server or application. Because the message body is incomplete, the server waits for the rest of the body, making the web server or web application unavailable to legitimate users.

An HTTP GET/POST attack is a sophisticated layer-7 attack that does not use malformed packets, spoofing, or reflection techniques. This type of attack requires less bandwidth than other attacks to bring down the targeted site or web server. This attack aims to compel the server to allocate as many resources as possible to serve the attack, thereby denying legitimate users access to the server's resources.

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

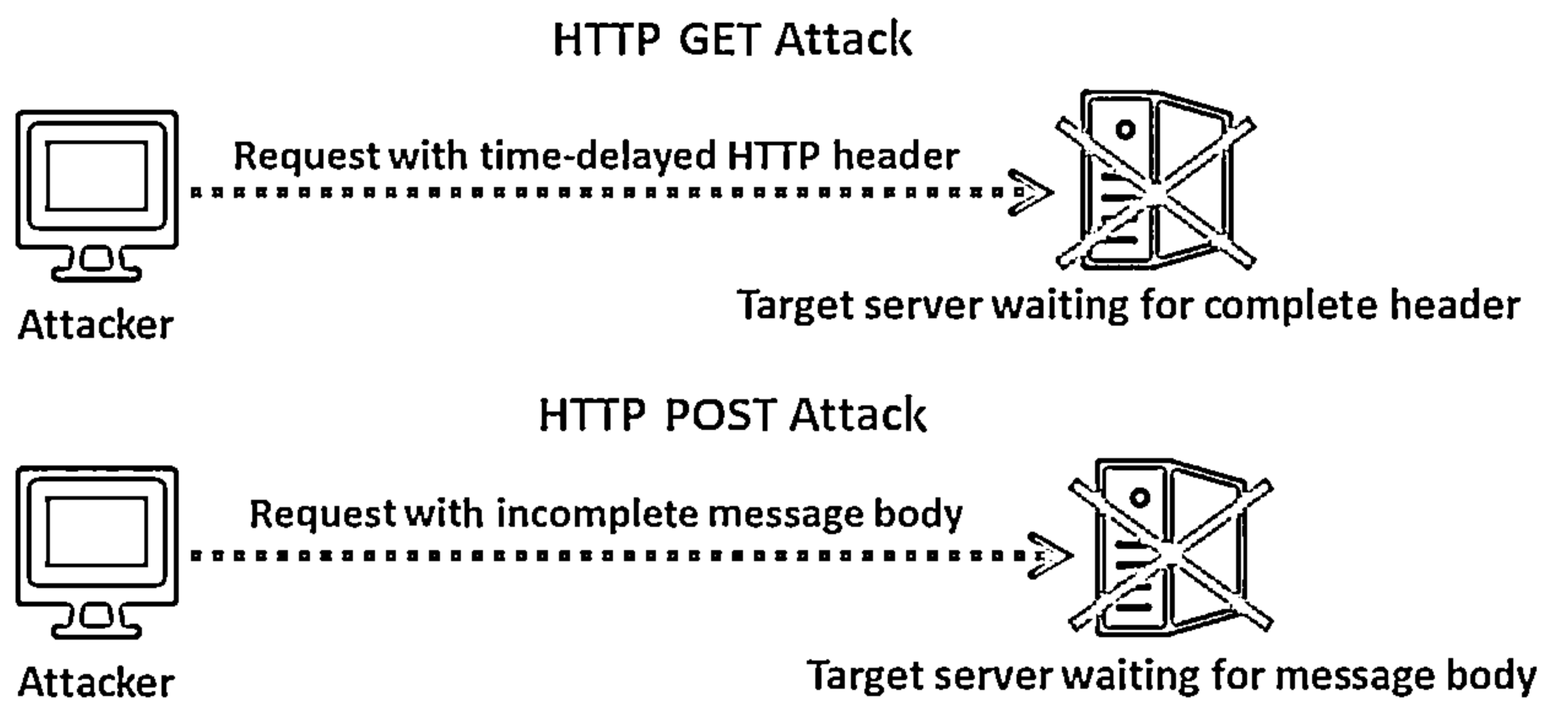


Figure 10.10: HTTP GET/POST attack

In addition to the aforementioned HTTP GET/POST attack, attackers can employ the following HTTP flood attacks to exhaust the target network's bandwidth:

- **Single-Session HTTP Flood Attack**

  In this type of flood attack, an attacker exploits the vulnerabilities in HTTP 1.1 to bombard a target with multiple requests in a single HTTP session.

- **Single-Request HTTP Flood Attack**

  In this type of flood attack, attackers make several HTTP requests from a single HTTP session by masking these requests within one HTTP packet. This technique allows attackers to be anonymous and invisible while performing DDoS attacks.

- **Recursive HTTP GET Flood Attack**

  Staying undetected is key for attackers. An attacker posing as a legitimate user and performing legitimate actions can trick any firewall into believing that the source is legitimate while it is not. Recursive GET collects a list of pages or images and appears to be going through these pages or images. However, it stealthily performs flooding attacks on the target. The recursive GET in combination with an HTTP flood attack can cause extreme damage to the target.

- **Random Recursive GET Flood Attack**

  This type of attack is a tweaked version of the recursive GET flood attack. It is designed for forums, blogs, and other websites that have pages in a sequence. Similar to the recursive GET flood attack, in this attack, the recursive GET pretends to be going through pages. Because the targets are forums, groups, and other blogs, the attacker uses random numbers from a valid page range to pose as a legitimate user and sends a new GET request each time. In both recursive GET and random recursive GET flood attacks, the target is bombarded with a large number of GET requests, exhausting its resources.

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

Slowloris Attack

Slowloris is a DDoS attack tool used to perform layer-7 DDoS attacks to take down web infrastructure. It is distinctly different from other tools in that it uses perfectly legitimate HTTP traffic to take down a target server. In Slowloris attacks, the attacker sends partial HTTP requests to the target web server or application. Upon receiving the partial requests, the target server opens multiple connections and waits for the requests to complete. However, these requests remain incomplete, causing the target server's maximum concurrent connection pool to be filled up and additional connection attempts to be denied.

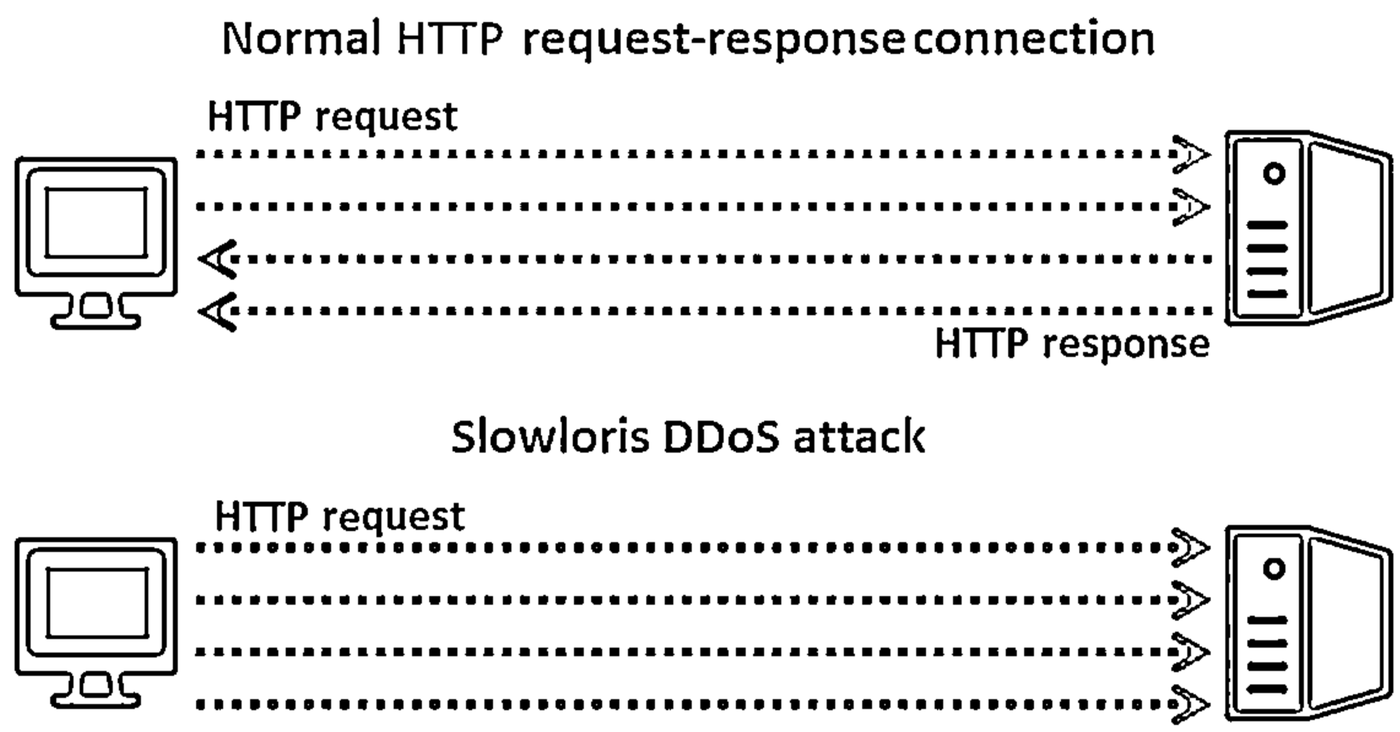


Figure 10.11: Slowloris attack

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

UDP Application Layer Flood Attack

- Some of the UDP-based application layer protocols that attackers can employ for flooding the target networks include:

1. CharGEN
2. SNMPv2
3. QOTD
4. RPC
5. SSDP
6. CLDAP
7. TFTP
8. NetBIOS
9. NTP
10. Quake Network Protocol
11. Steam Protocol
12. VoIP

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

UDP Application Layer Flood Attack

Though UDP flood attacks are known for their volumetric attack nature, some application layer protocols that rely on UDP can be employed by attackers to perform flood attacks on target networks.

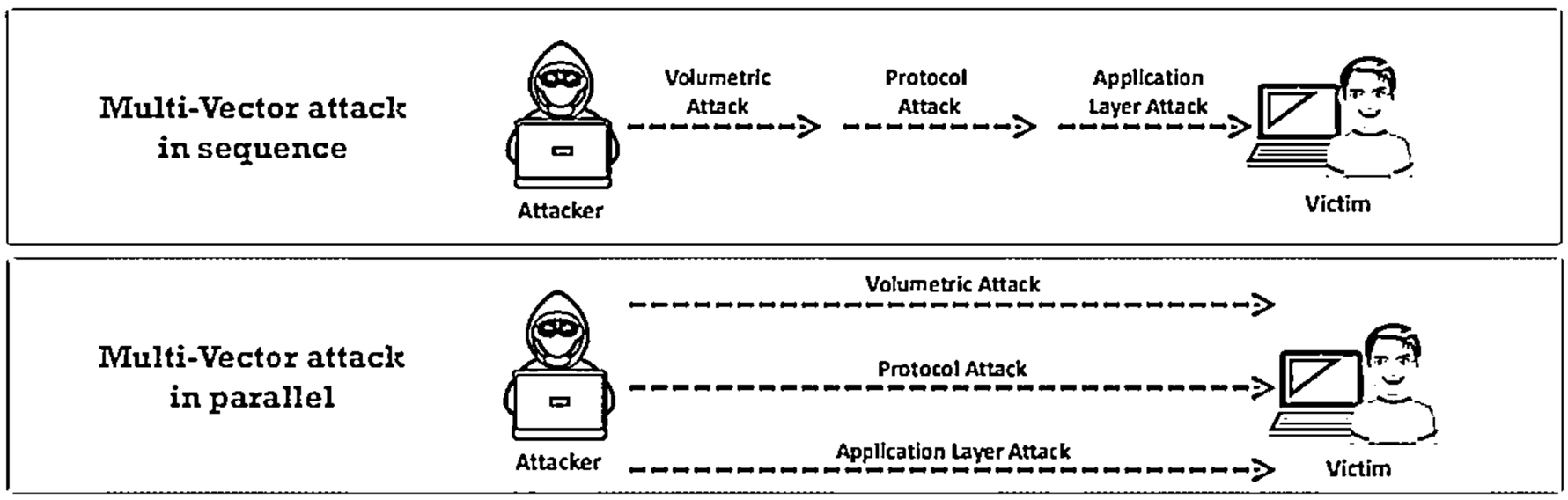
The following are examples for UDP-based application layer protocols that attackers can employ for flooding target networks:

- Character Generator Protocol (CHARGEN)
- Simple Network Management Protocol Version 2 (SNMPv2)
- Quote of the Day (QOTD)
- Remote procedure call (RPC)
- SSDP
- Connection-less Lightweight Directory Access Protocol (CLDAP)
- Trivial File Transfer Protocol (TFTP)
- Network Basic Input/Output System (NetBIOS)
- NTP
- Quake Network Protocol
- Steam Protocol
- Voice over Internet Protocol (VoIP)

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

Multi-Vector Attack

- In multi-vector DDoS attacks, the attackers use combinations of volumetric, protocol, and application-layer attacks to disable the target system or service
- Attackers rapidly and repeatedly change the form of their DDoS attack (e.g., SYN packets, Layer 7)
- These attacks are either launched one vector at a time or in parallel to confuse a company's IT department and exhaust their resources with their focus diverted to the wrong solution



Multi-Vector Attack

In multi-vector DDoS attacks, the attacker uses combinations of volumetric, protocol, and application layer attacks to take down the target system or service. The attacker quickly changes from one form of DDoS attack (e.g., SYN packets) to another (layer 7). These attacks are either launched through one vector at a time or through multiple vectors in parallel to confuse a company's IT department, making them spend all their resources and maliciously diverting their focus.

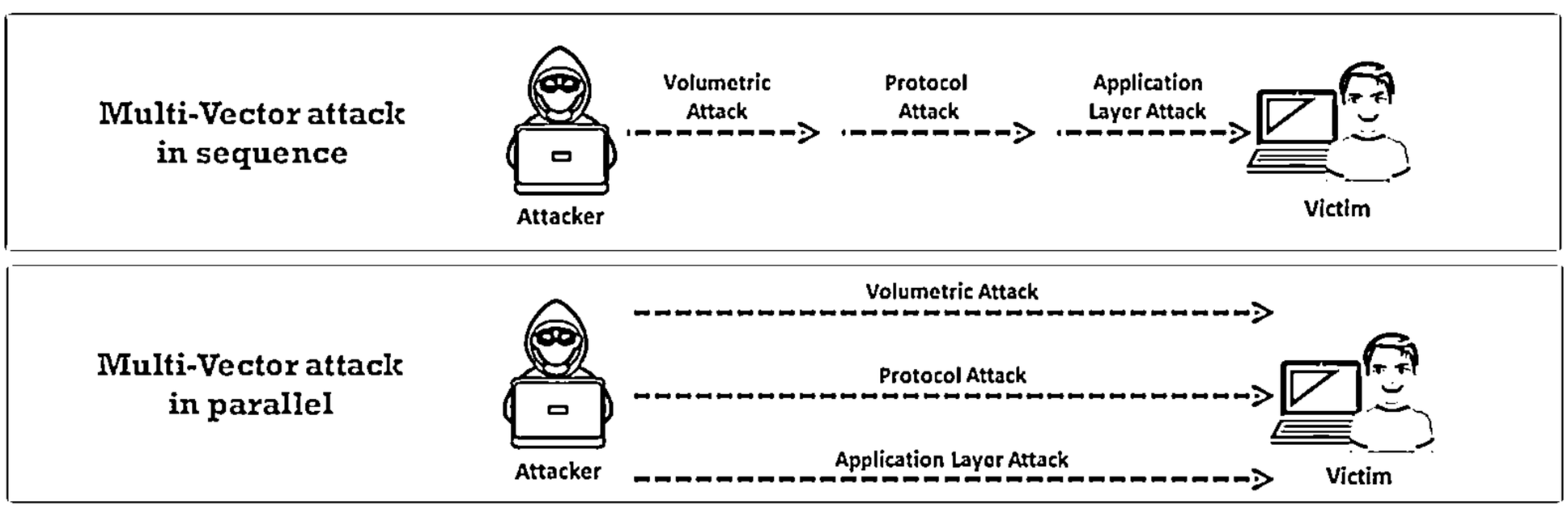
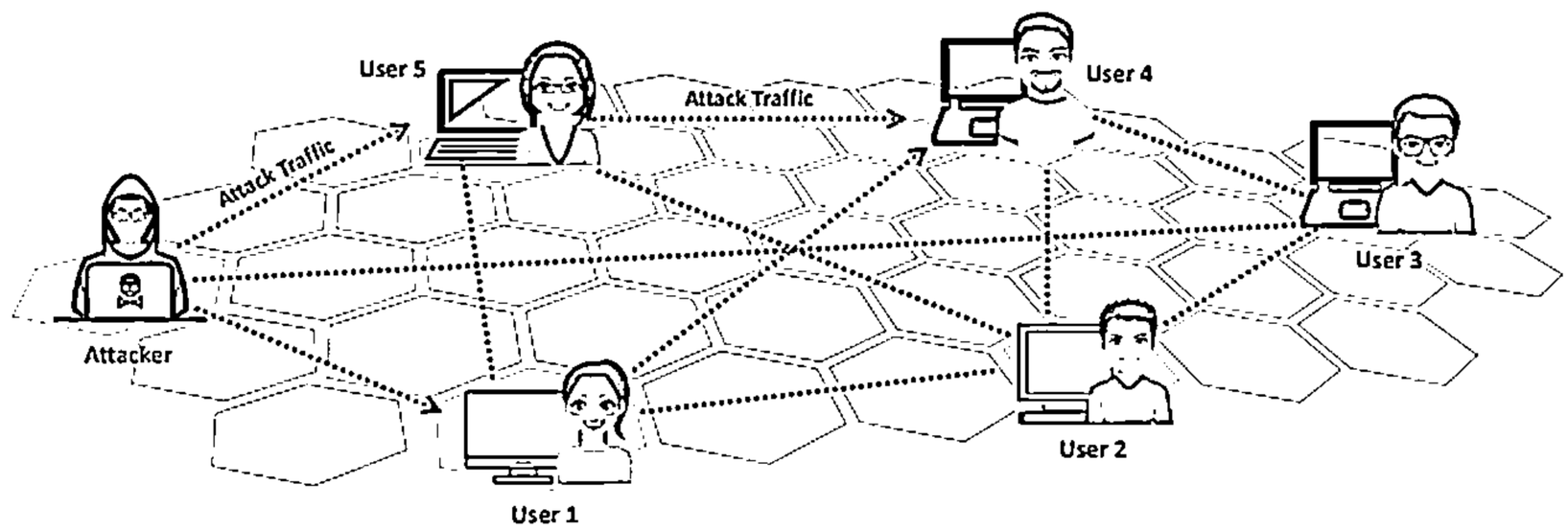


Figure 10.12: Multi-vector attack

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

Peer-to-Peer Attack

- Using peer-to-peer attacks, attackers instruct clients of peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's fake website
- Attackers exploit flaws found in the network using the DC++ (Direct Connect) protocol, which is used for sharing all types of files between instant messaging clients
- Using this method, attackers launch massive denial-of-service attacks and compromise websites



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

Peer-to-Peer Attack

A peer-to-peer attack is a form of DDoS attack in which the attacker exploits a number of bugs in peer-to-peer servers to initiate a DDoS attack. Attackers exploit flaws found in networks that use the Direct Connect (DC++) protocol, which allows the exchange of files between instant-messaging clients. This kind of attack does not use botnets. Unlike a botnet-based attack, a peer-to-peer attack eliminates the need for attackers to communicate with the clients they subvert. Here, the attacker instructs clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and instead connect to the victim's website. Consequently, several thousand computers may aggressively attempt to connect to a target website, causing a drop in the performance of the target website. It is easy to identify peer-to-peer attacks based on signatures. By using this method, attackers launch massive DoS attacks to compromise websites.

Peer-to-peer DDoS attacks can be minimized by specifying ports for peer-to-peer communication. For example, specifying port 80 to disallow peer-to-peer communication minimizes the possibility of attacks on websites.

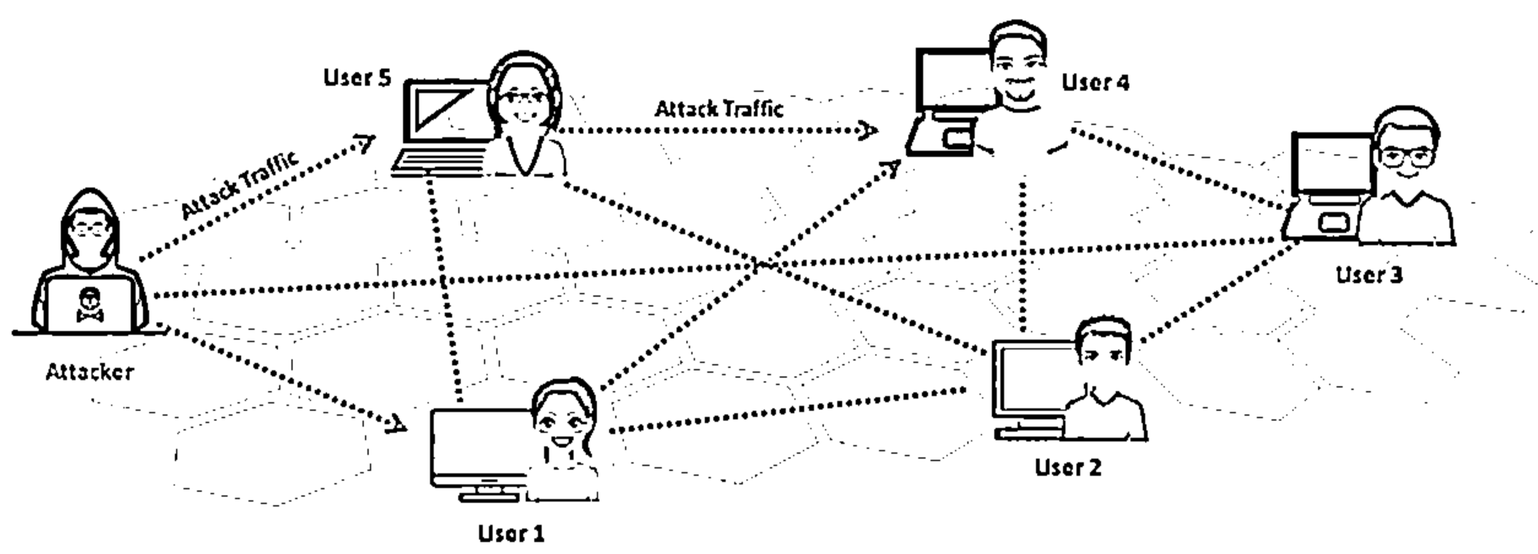


Figure 10.13: Peer-to-peer attack

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

Permanent Denial-of-Service Attack

Phlashing	❑ Permanent DoS, also known as phlashing, refers to attacks that cause irreversible damage to system hardware
Sabotage	❑ Unlike other DoS attacks, it sabotages the system hardware, requiring the victim to replace or reinstall the hardware
Bricking a system	❑ This attack is carried out using a method known as "bricking a system" ❑ Using this method, attackers send fraudulent hardware updates to the victims
Process	Attacker → Sends email, IRC chats, tweets, posts, videos with fraudulent content for hardware updates → Victim (Malicious code is executed) Attacker ← Attacker gets access to victim's computer ← Victim

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

Permanent Denial-of-Service Attack

Permanent DoS (PDoS) attacks, also known as phlashing, purely target hardware and cause irreversible damage to the hardware. Unlike other types of DoS attacks, it sabotages the system hardware, requiring the victim to replace or reinstall the hardware. The PDoS attack exploits security flaws in a device to allow remote administration on the management interfaces of the victim's hardware, such as printers, routers, and other networking devices.

This type of attack is quicker and more destructive than conventional DoS attacks. It works with a limited amount of resources, unlike a DDoS attack, in which attackers unleash a set of zombies onto a target. Attackers perform PDoS attacks by using a method known as the "bricking" of a system. In this method, the attacker sends emails, IRC chats, tweets, or videos with fraudulent content for hardware updates to the victim. The hardware updates are modified and corrupted with vulnerabilities or defective firmware. When the victim clicks on a link or pop-up window referring to the fraudulent hardware update, the victim installs it in their system. Consequently, the attacker attains complete control over the victim's system.

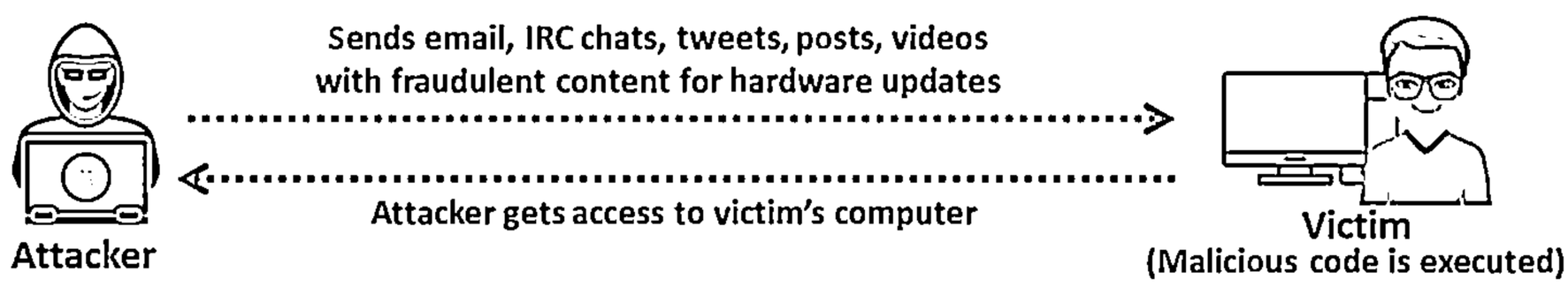


Figure 10.14: Permanent DoS attack

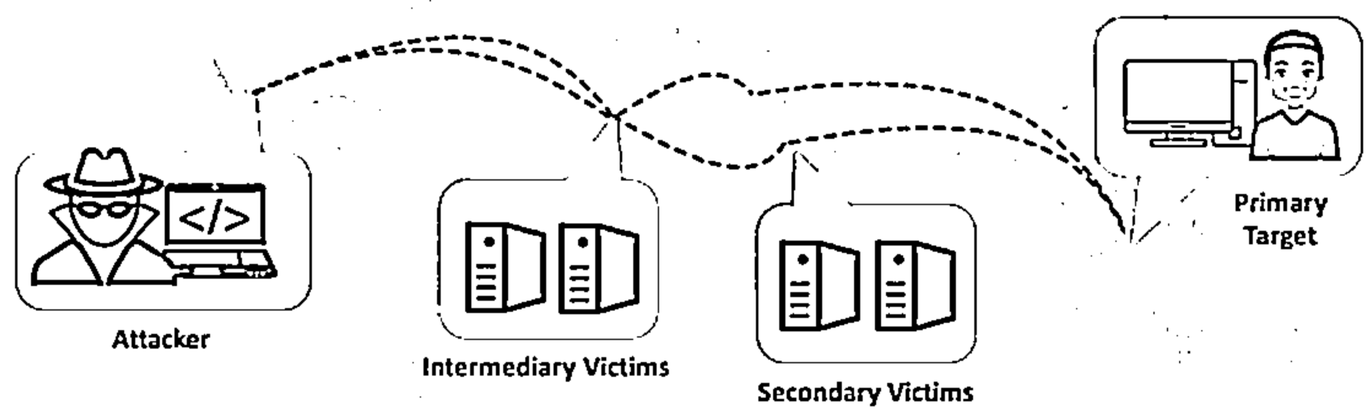
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Distributed Reflection Denial-of-Service (DRDoS) Attack

- A distributed reflected denial-of-service attack (DRDoS), also known as a spoofed attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application
- Attackers launch this attack by sending requests to the intermediary hosts, which then redirect the requests to the secondary machines, which in turn reflect the attack traffic to the target

Advantage

- The primary target seems to be directly attacked by the secondary victim rather than the actual attacker
- Multiple intermediary victim servers are used, which results in an increase in attack bandwidth



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

Distributed Reflection Denial-of-Service (DRDoS) Attack

A distributed reflection DoS (DRDoS) attack, also known as a "spoofed" attack, involves the use of multiple intermediary and secondary machines that contribute to a DDoS attack against a target machine or application. A DRDoS attack exploits the TCP three-way handshake vulnerability.

This attack involves an attacker machine, intermediary victims (zombies), secondary victims (reflectors), and a target machine. The attacker launches this attack by sending requests to the intermediary hosts, which in turn reflect the attack traffic to the target.

The process of a DRDoS attack is as follows. First, the attacker commands the intermediary victims (zombies) to send a stream of packets (TCP SYN) with the primary target's IP address as the source IP address to other non-compromised machines (secondary victims or reflectors) in order to exhort them to establish a connection with the primary target. Consequently, the reflectors send a huge volume of traffic (SYN/ACK) to the primary target to establish a new connection with it because they believe the host requested it. The primary target discards the SYN/ACK packets received from the reflectors because they did not send the SYN packet. Meanwhile, the reflectors wait for the ACK response from the primary target. Assuming that the packet was lost, the reflector machines resend SYN/ACK packets to the primary target to establish the connection, until a time-out occurs. In this manner, the target machine is flooded with a heavy volume of traffic from the reflector machines. The combined bandwidth of these reflector machines overwhelms the target machine.

A DRDoS attack is an intelligent attack because it is very difficult or even impossible to trace the attacker. Instead of the actual attacker, the secondary victims (reflectors) seem to attack the primary target directly. This attack is more effective than a typical DDoS attack because multiple intermediary and secondary victims generate huge attack bandwidth.

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

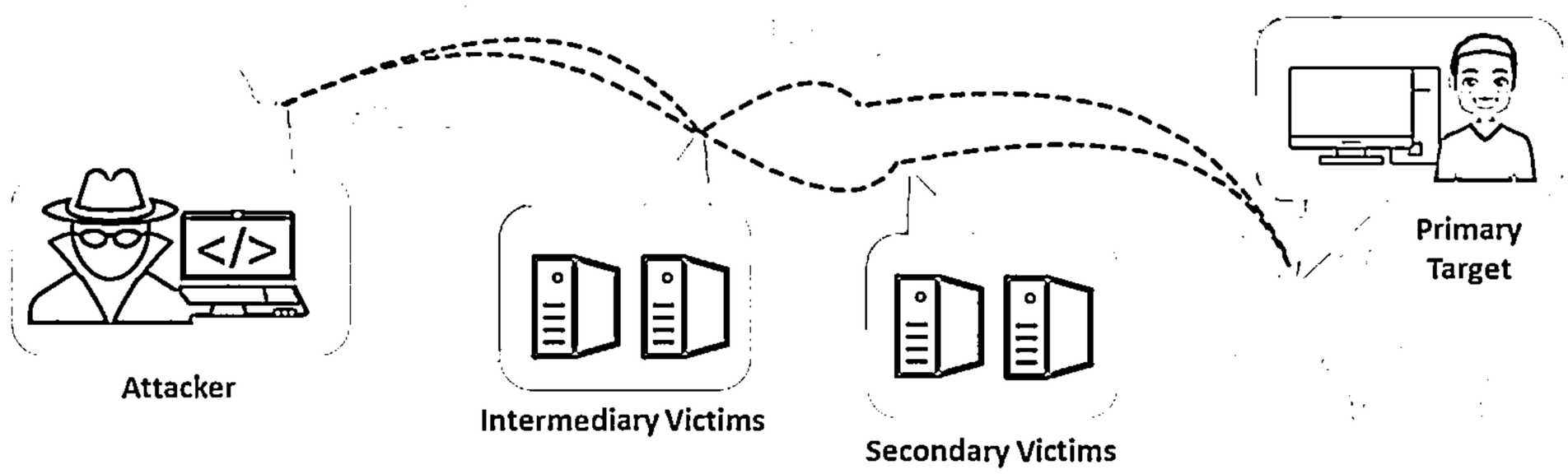
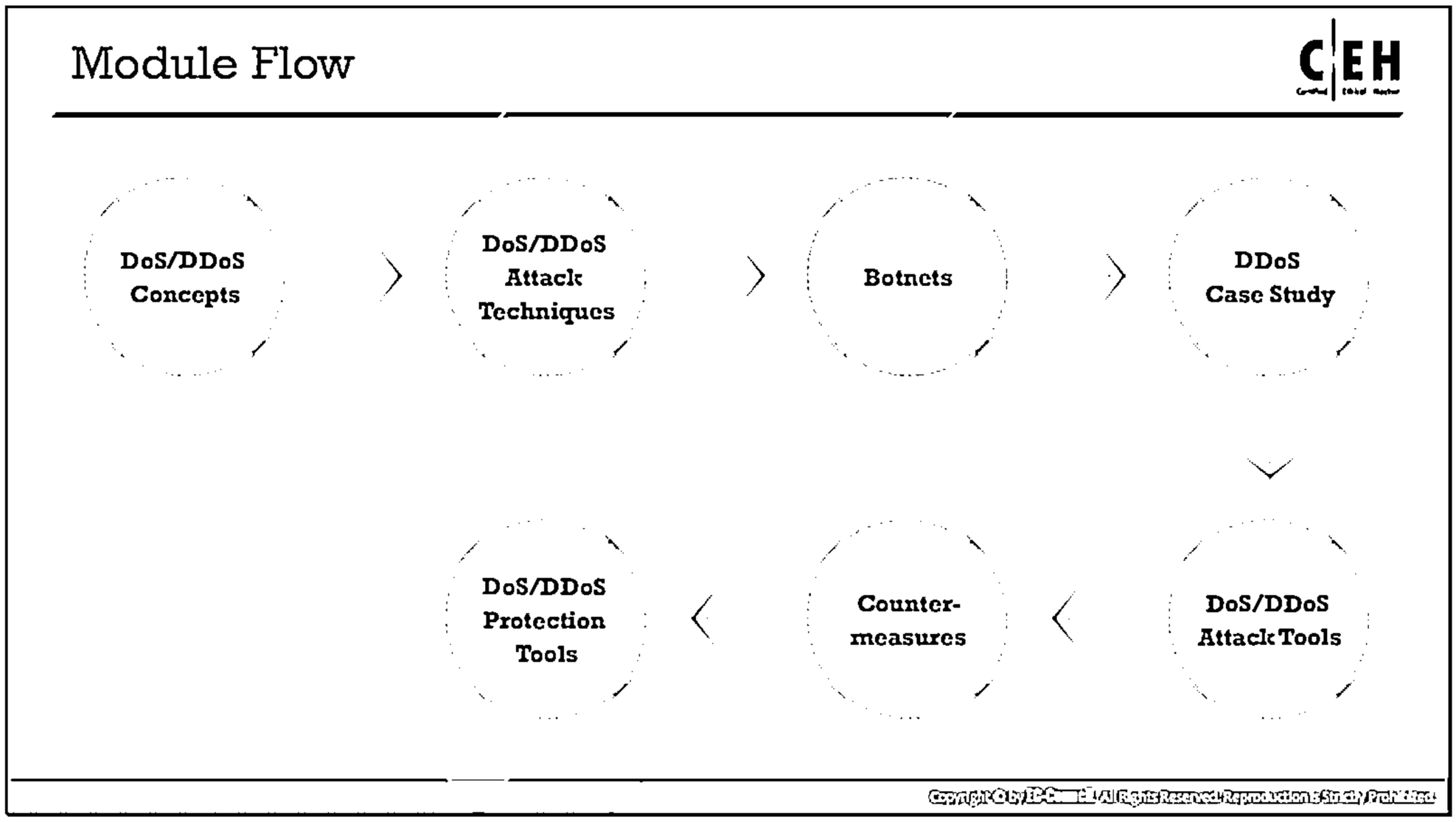


Figure 10.15: Distributed reflection DoS (DRDoS) attack

- **Countermeasures**
  - Turn off the Character Generator Protocol (CHARGEN) service to stop this attack method
  - Download the latest updates and patches for servers

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

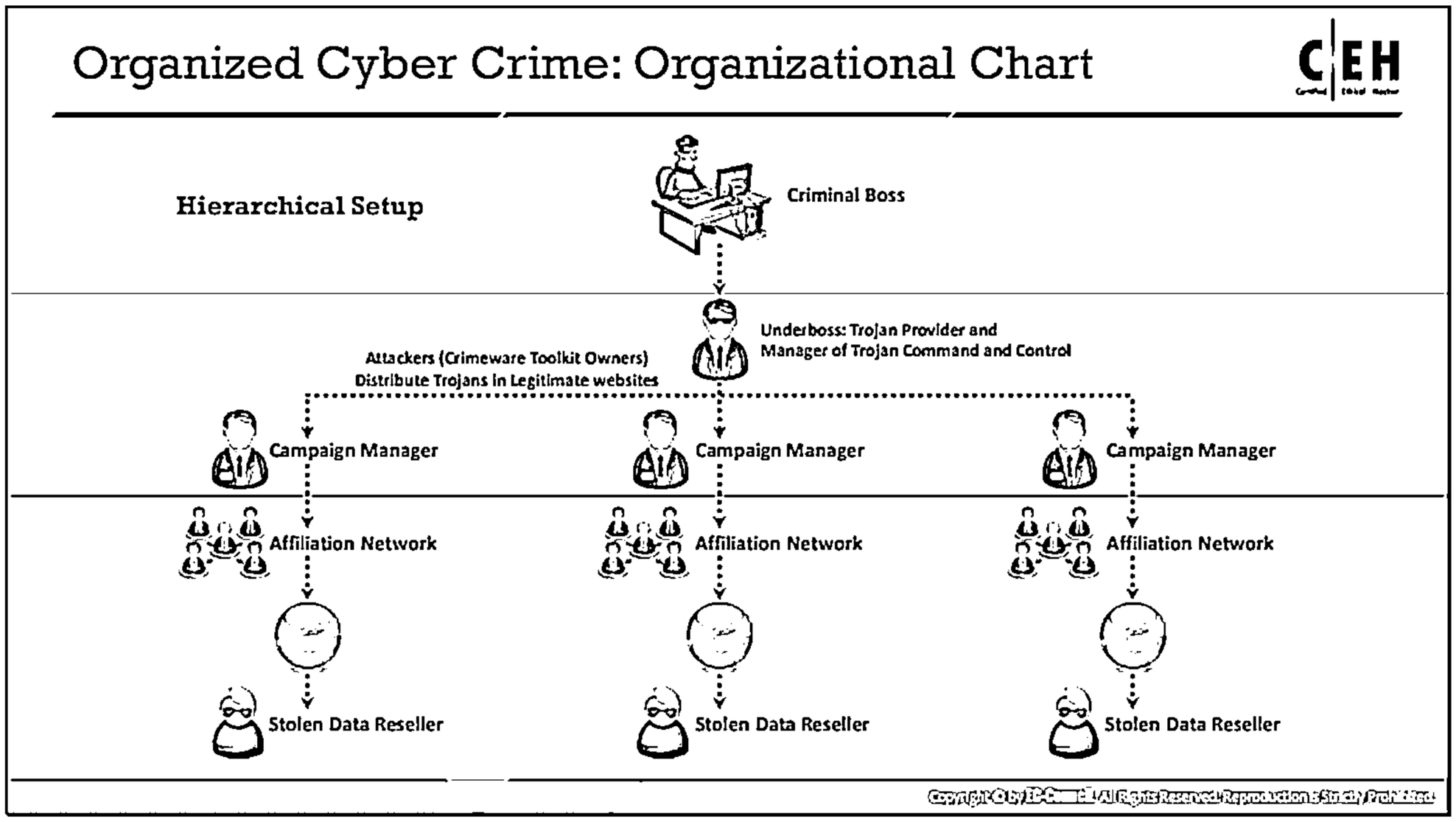


Botnets

The term "bot" is a contraction of "robot" and refers to software applications that run automated tasks over the Internet. Attackers use bots to infect a large number of computers that form a network, or "botnet," allowing them to launch DDoS attacks, generate spam, spread viruses, and commit other types of crime.

This section deals with organized cyber-crime syndicates, organizational charts, botnets, and botnet propagation techniques; botnet ecosystems; scanning methods for finding vulnerable machines; and the propagation of malicious code.

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



Organized Cyber Crime: Organizational Chart

Organized Crime Syndicates

While cyber criminals worked independently in the past, they now tend to operate in organized groups. They are increasingly associated with organized crime syndicates and take advantage of the sophisticated techniques of these syndicates to engage in illegal activity, usually for monetary benefit. There are organized groups of cyber criminals who work in a hierarchical set up with a predefined revenue-sharing model, which is a kind of major corporation that offers criminal services. Organized groups create and rent botnets and offer various services ranging from the development of malware and hacking of bank accounts to the deployment of massive DoS attacks against any target for a price.

For example, an organized crime syndicate might perform a DDoS attack against a bank to divert the attention of the bank's security team while they clean out bank accounts with stolen account credentials. The growing involvement of organized criminal syndicates in politically motivated cyber warfare and hacktivism is a matter of concern for national security agencies.

Cybercrime features a complicated range of players, and cyber criminals are paid according to the task they perform or the position they hold. The head of the cybercrime organization (i.e., the boss) acts as a business entrepreneur. The boss does not commit any crimes directly. Immediately below the boss in the organizational hierarchy is the "underboss," who sets up a C&C server and crimeware toolkit database to manage the implementation of attacks and provide Trojans. Below the underboss are various "campaign managers" with their own affiliation networks for implementing attacks and stealing data. Finally, resellers sell the stolen data.

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

Hierarchical Setup

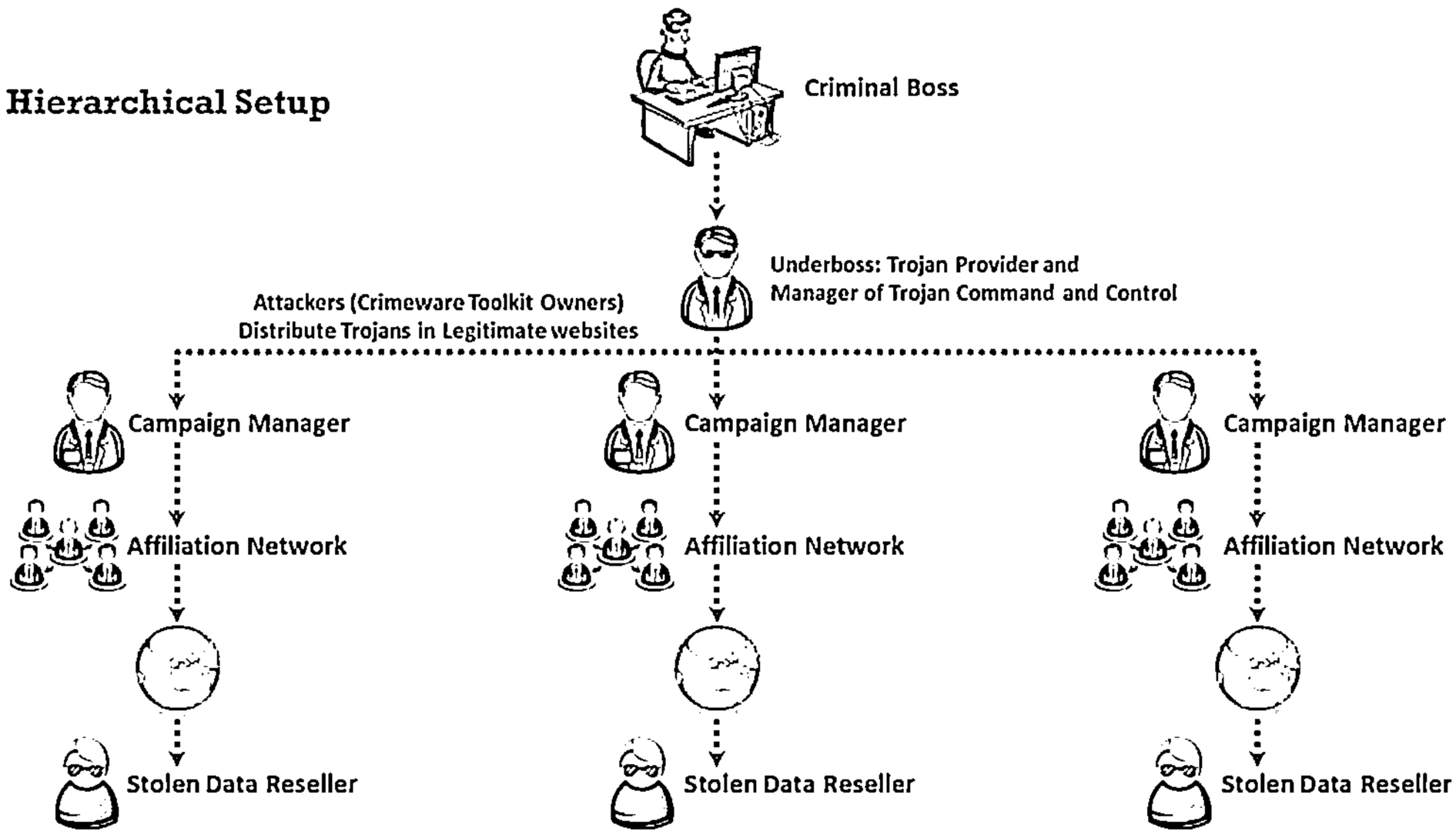
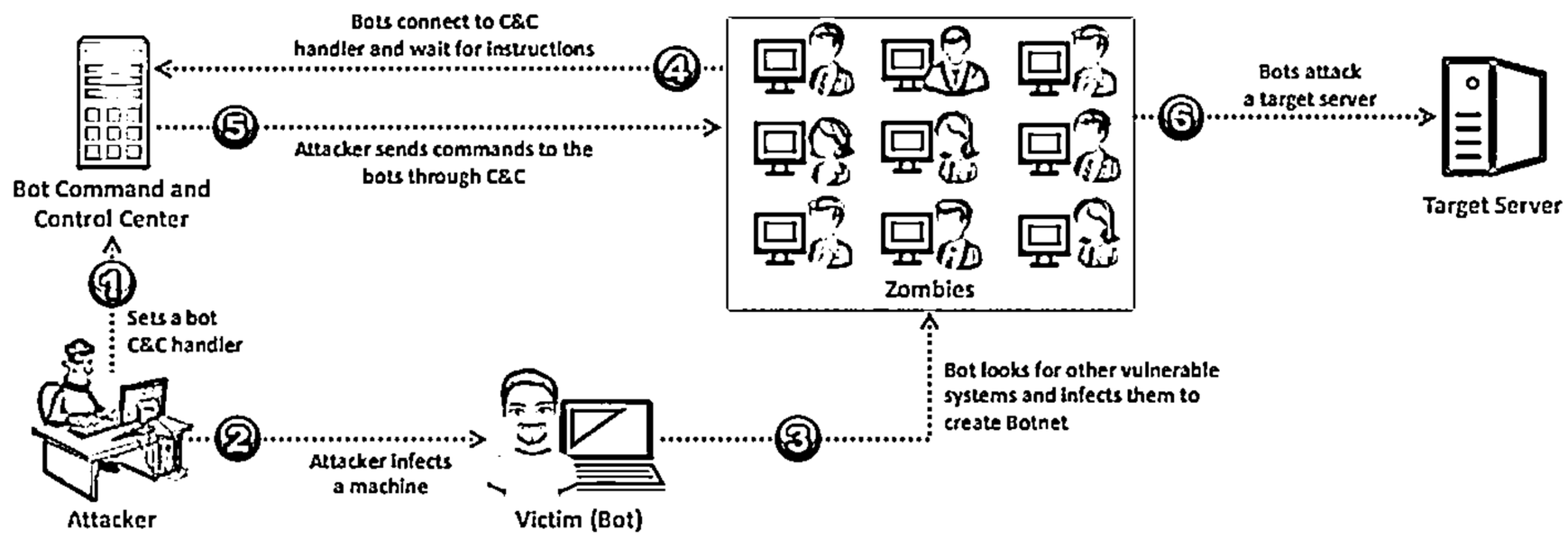


Figure 10.16: Hierarchical setup of a cybercrime organization

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

Botnets

- Bots are software applications that run automated tasks over the Internet and perform simple, repetitive tasks, such as web spidering and search engine indexing
- A botnet is a huge network of compromised systems and can be used by an attacker to launch denial-of-service attacks



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

Botnets

Bots are used for benign data collection or data mining activities, such as "web spidering," as well as to coordinate DoS attacks. The main purpose of a bot is to collect data. There are different types of bots, such as Internet bots, IRC bots, and chatter bots. Examples for IRC bots are Supybot, Sopel, EnergyMech, and Eggdrop.

A botnet (a contraction of "roBOT NETwork") is a group of computers "infected" by bots; however, botnets can be used for both positive and negative purposes. As a hacking tool, a botnet is composed of a huge network of compromised systems. A relatively small botnet of 1,000 bots has a combined bandwidth larger than the bandwidth of most corporate systems.

The advent of botnets led to an enormous increase in cybercrime. Botnets form the core of the cybercriminal activity center that links and unites various parts of the cybercriminal world. Cybercriminal service suppliers are a part of a cybercrime network. They offer services such as malicious code development, bulletproof hosting, the creation of browser exploits, and encryption and packing.

Malicious code is the primary tool used by criminal organizations to commit cybercrimes. Botnet owners order both bots and other malicious programs such as Trojans, viruses, worms, keyloggers, and specially crafted applications to attack remote computers via networks. Developers offer malware services on public sites or closed Internet resources.

Botnets are agents that an intruder can send to a server system to perform an illegal activity. Botnets run hidden programs that allow the identification of system vulnerabilities. Attackers can use botnets to perform the tedious tasks involved in probing a system for known vulnerabilities.

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

Attackers can use botnets to perform the following:

- **DDoS attacks**: Botnets can generate DDoS attacks, which consume the bandwidth of the victim's computers. Botnets can also overload a system, wasting valuable host system resources and destroying network connectivity.
- **Spamming**: Attackers use a SOCKS proxy for spamming. They harvest email addresses from web pages or other sources.
- **Sniffing traffic**: A packet sniffer observes the data traffic entering a compromised machine. It allows an attacker to collect sensitive information such as credit card numbers and passwords. The sniffer also allows an attacker to steal information from one botnet and use it against another botnet. In other words, botnets can rob one another.
- **Keylogging**: Keylogging is a method of recording the keys typed on a keyboard, and it provides sensitive information such as system passwords. Attackers use keylogging to harvest account login information for services such as PayPal.
- **Spreading new malware**: Botnets can be used to spread new bots.
- **Installing advertisement add-ons**: Botnets can be used to perpetrate a "click fraud" by automating clicks.
- **Google AdSense abuse**: Some companies permit showing Google AdSense ads on their websites for economic benefits. Botnets allow an intruder to automate clicks on an ad, producing a percentage increase in the click queue.
- **Attacks on IRC chat networks**: Also called clone attacks, these attacks are similar to a DDoS attack. A master agent instructs each bot to link to thousands of clones within an IRC network, which can flood the network.
- **Manipulating online polls and games**: Every botnet has a unique address, enabling it to manipulate online polls and games.
- **Mass identity theft**: Botnets can send a large number of emails while impersonating a reputable organization such as eBay. This technique allows attackers to steal information for identity theft.

The below figure illustrates how an attacker launches a botnet-based DoS attack on a target server. The attacker sets up a bot C&C center, following which they infect a machine (bot) and compromises it. Later, they use this bot to infect and compromise other vulnerable systems available in the network, resulting in a botnet. The bots (also known as zombies) connect to the C&C center and awaits instructions. Subsequently, the attacker sends malicious commands to the bots through the C&C center. Finally, as per the attacker's instructions, the bots launch a DoS attack on a target server, making its services unavailable to legitimate users in the network.

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

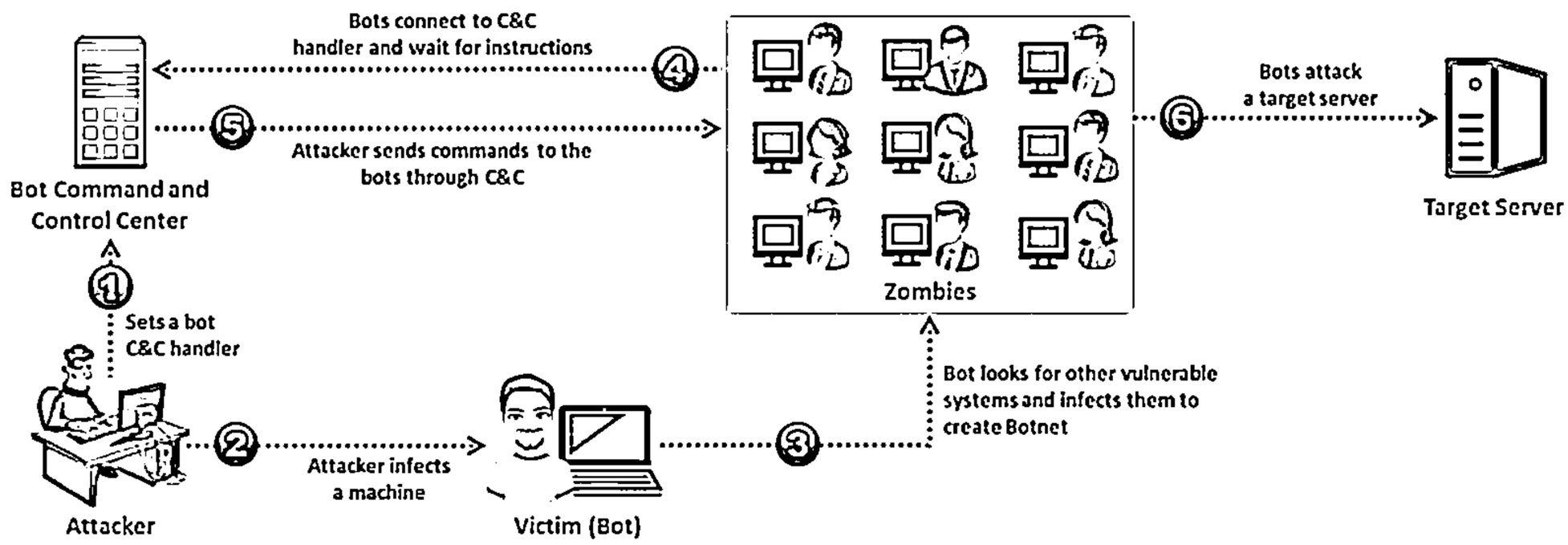
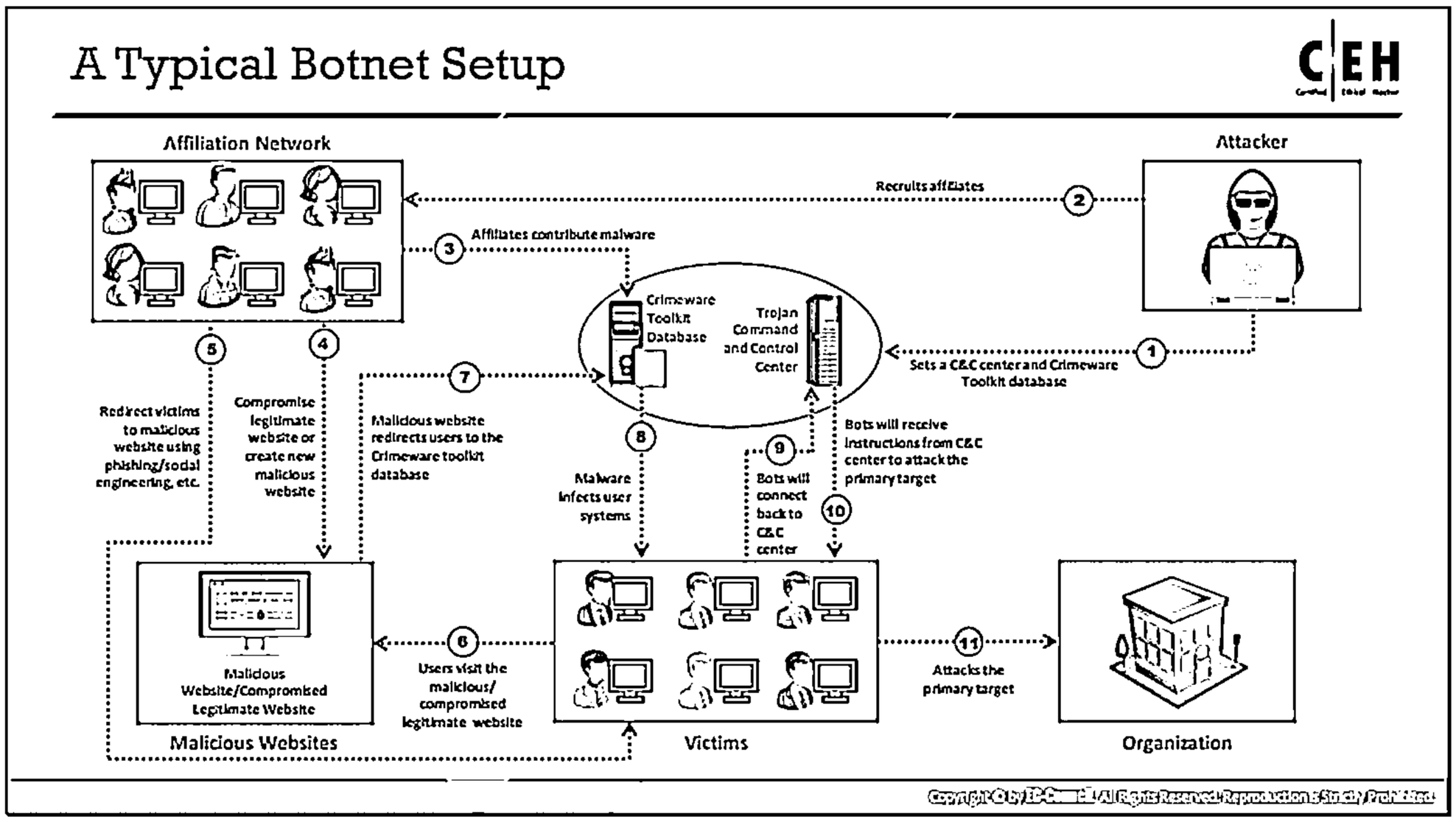


Figure 10.17: Botnet-based DDoS attack

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



A Typical Botnet Setup

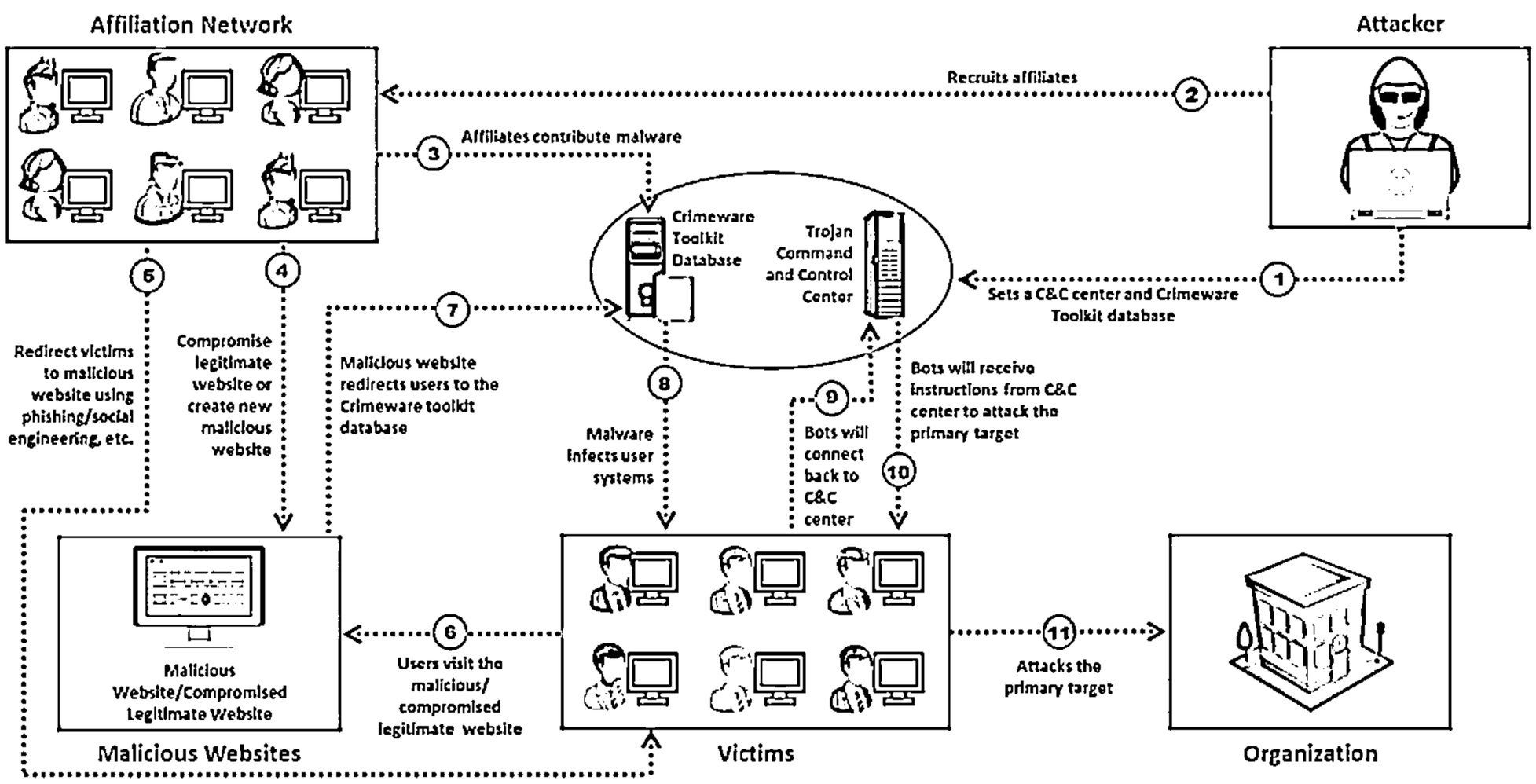
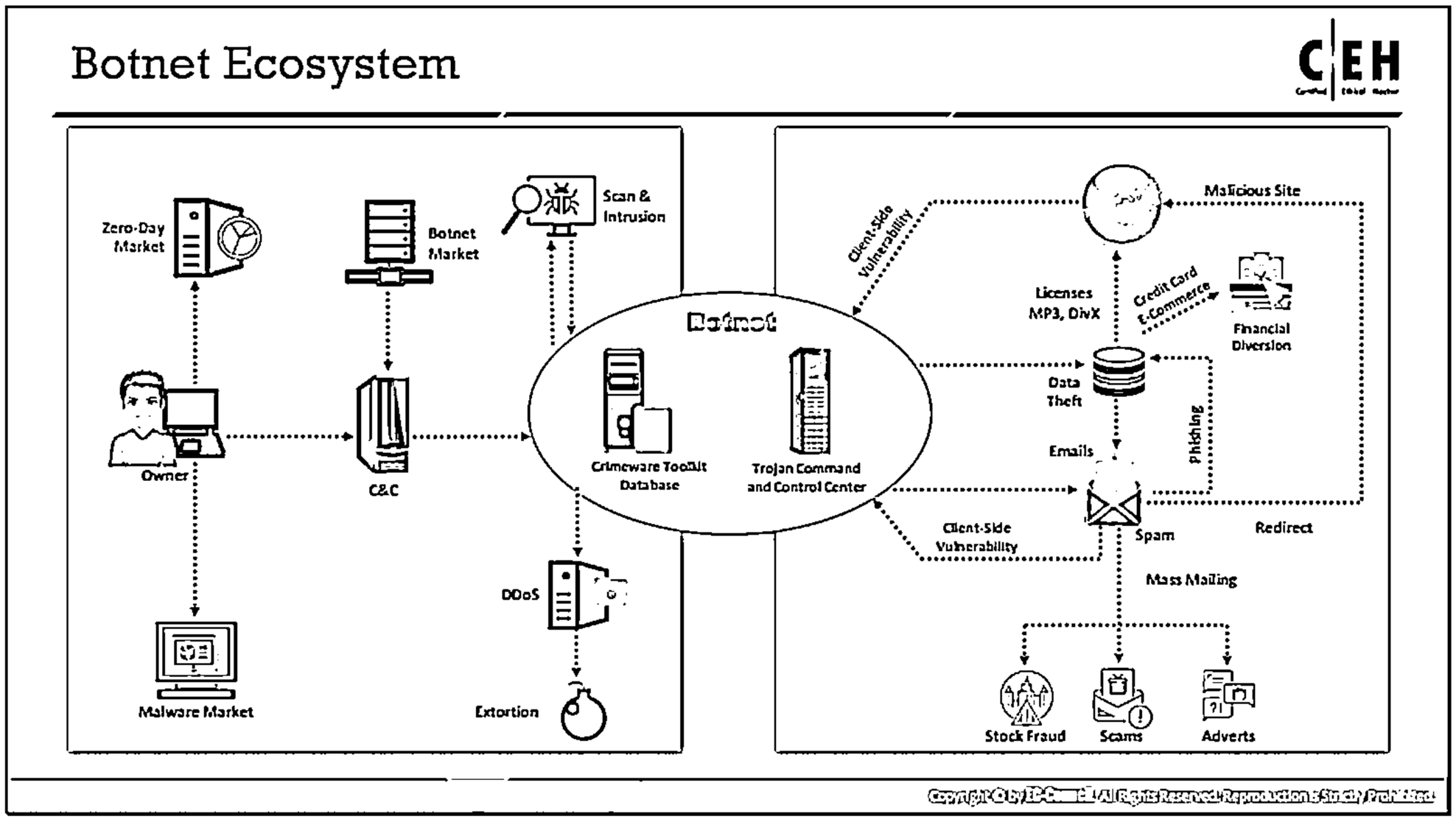


Figure 10.18: Typical botnet setup

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



Botnet Ecosystem

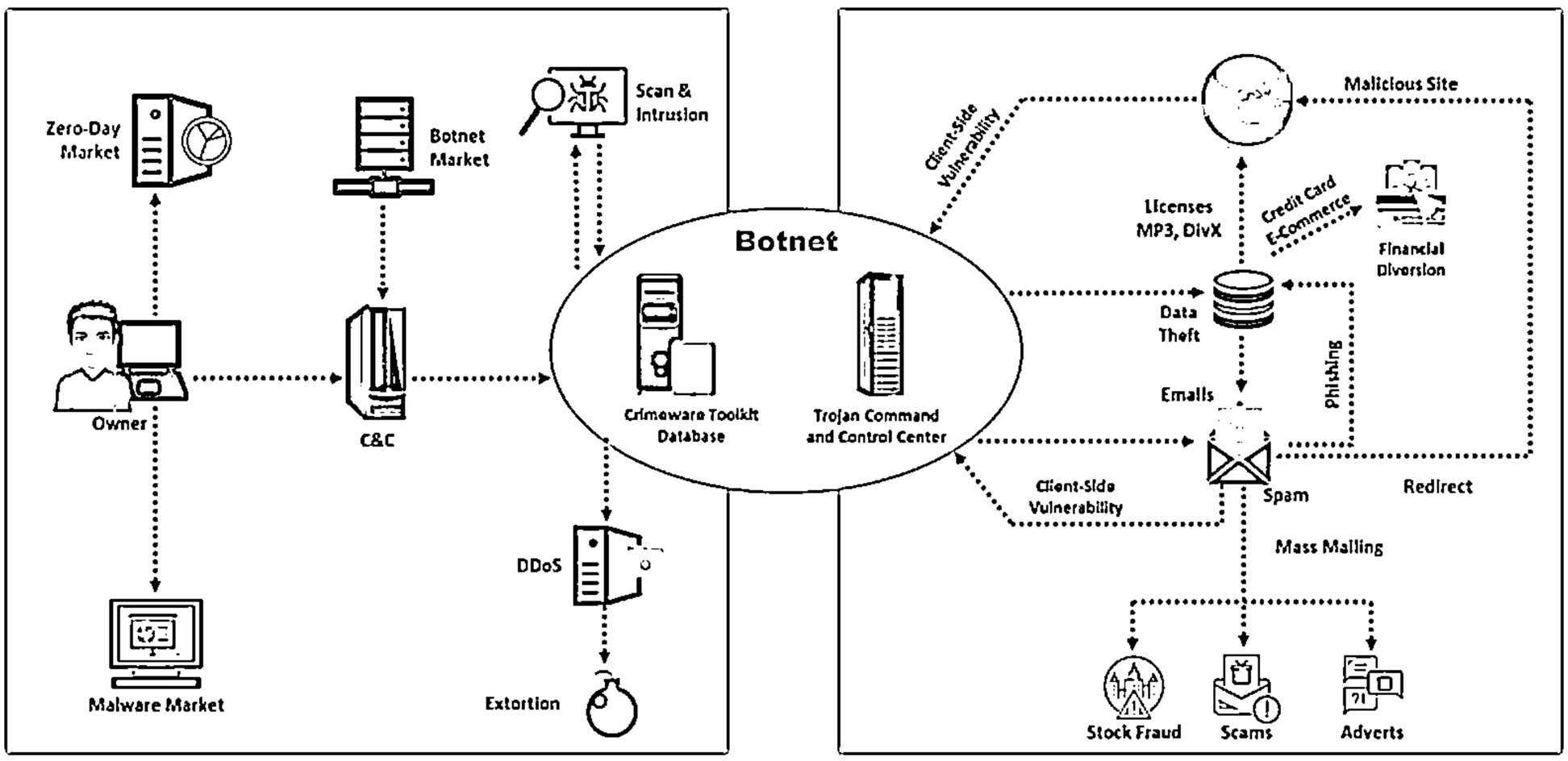


Figure 10.19: Botnet ecosystem

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

Scanning Methods for Finding Vulnerable Machines

Random Scanning	❑ The infected machine probes IP addresses randomly from the target network IP range and checks for vulnerabilities
Hit-list Scanning	❑ An attacker first collects a list of potentially vulnerable machines and then scans them to find vulnerable machines
Topological Scanning	❑ It uses information obtained from an infected machine to find new vulnerable machines
Local Subnet Scanning	❑ The infected machine looks for new vulnerable machines in its own local network
Permutation Scanning	❑ It uses a pseudorandom permutation list of IP addresses to find new vulnerable machines

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

Scanning Methods for Finding Vulnerable Machines

Discussed below are scanning methods used by an attacker to find vulnerable machines in a network:

- **Random Scanning**

  In this technique, the infected machine (an attacker's machine or a zombie) probes IP addresses randomly in the target network's IP range and checks their vulnerability. On finding a vulnerable machine, it hacks and attempts to infect the vulnerable machine by installing the same malicious code installed on it. This technique generates significant traffic because many compromised machines probe and check the same IP addresses. Malware propagates quickly in the initial stage, and the speed of propagation reduces as the number of new IP addresses available decreases with time.

- **Hit-list Scanning**

  Through scanning, an attacker first collects a list of potentially vulnerable machines and then creates a zombie army. Subsequently, the attacker scans the list to find a vulnerable machine. On finding one, the attacker installs malicious code on it and divides the list in half. The attacker continues to scan one half, whereas the other half is scanned by the newly compromised machine. This process keeps repeating, causing the number of compromised machines to increase exponentially. This technique ensures the installation of malicious code on all the potentially vulnerable machines in the hit list within a short time.

- **Topological Scanning**

  This technique uses the information obtained from an infected machine to find new vulnerable machines. An infected host checks for URLs in the hard drive of a machine

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

that it wants to infect. Subsequently, it shortlists URLs and targets, and it checks their vulnerability. This technique yields accurate results, and its performance is similar to that of the hit-list scanning technique.

- **Local Subnet Scanning**

  In this technique, an infected machine searches for new vulnerable machines in its local network, behind a firewall, by using the information hidden in the local addresses. Attackers use this technique in combination with other scanning mechanisms.

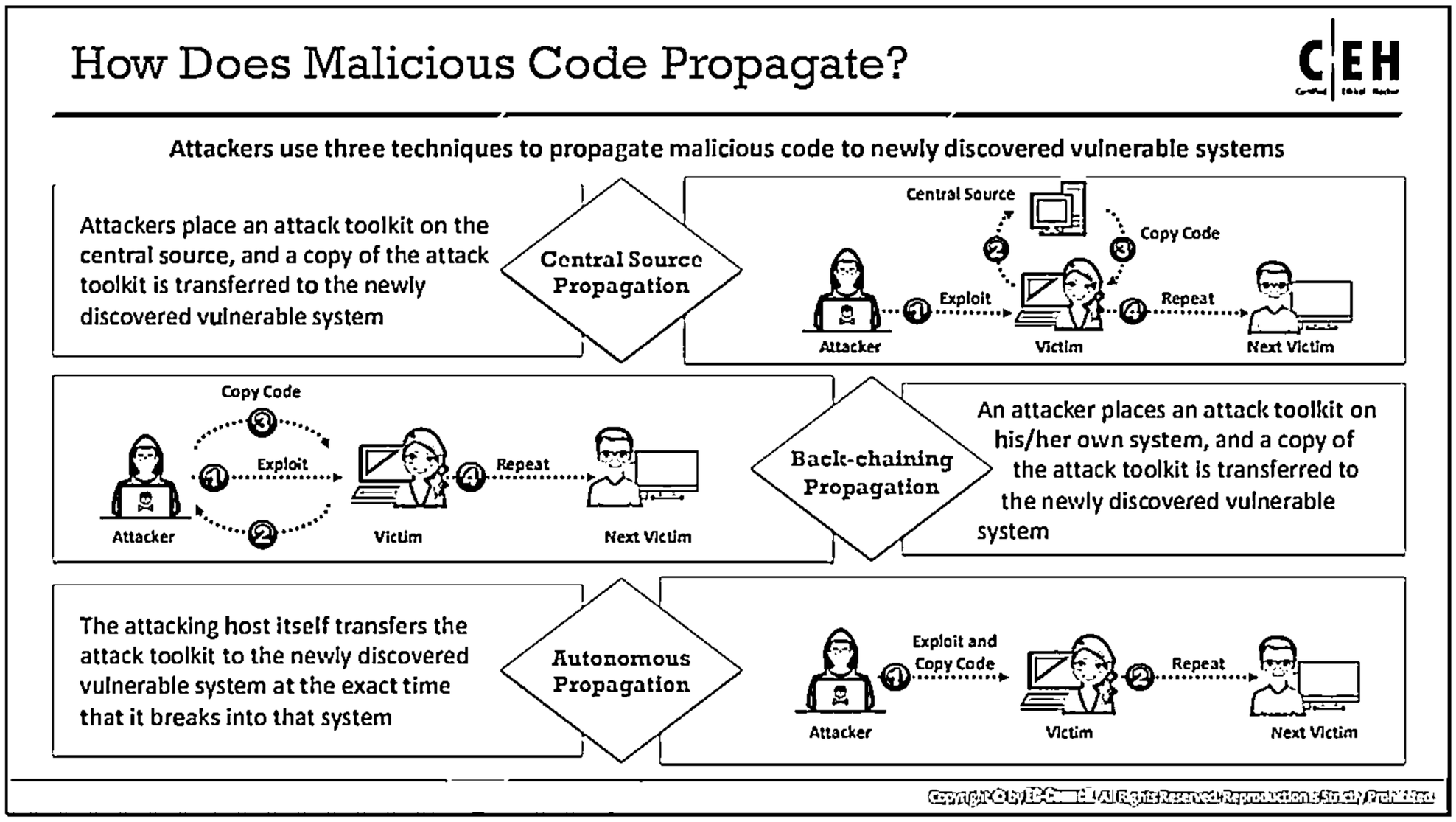
- **Permutation Scanning**

  In this technique, attackers share a common pseudorandom permutation list of IP addresses of all machines. The list is created using a block cipher of 32 bits and a preselected key. If a compromised host is infected during either hit-list scanning or local subnet scanning, the list is scanned from immediately after the point of the compromised host to identify new targets. If a compromised host is infected during permutation scanning, scanning restarts from a random point. If an already infected machine is encountered, scanning restarts from a new random start point in the permutation list. The process of scanning stops when the compromised host consecutively encounters a predefined number of already infected machines and fails to find new targets. Thereafter, a new permutation key is generated to initiate a new scanning phase.

  Permutation scanning has the following advantages:

  - The reinfection of a target is avoided.
  - New targets are scanned at random, thereby ensuring a high scanning speed.

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



How Does Malicious Code Propagate?

Discussed below are three techniques used by an attacker to propagate malicious code and build attack networks:

- **Central Source Propagation**

  In this technique, the attacker places an attack toolkit on a central source and a copy of the attack toolkit is transferred to a newly discovered vulnerable system. Once the attacker finds a vulnerable machine, they instruct the central source to transfer a copy of the attack toolkit to the newly compromised machine, on which attack tools are automatically installed under management by a scripting mechanism. This initiates a new attack cycle, in which the newly infected machine searches for other vulnerable machines and repeats the process to install the attack toolkit. In general, this technique uses HTTP, FTP, and RPC protocols.

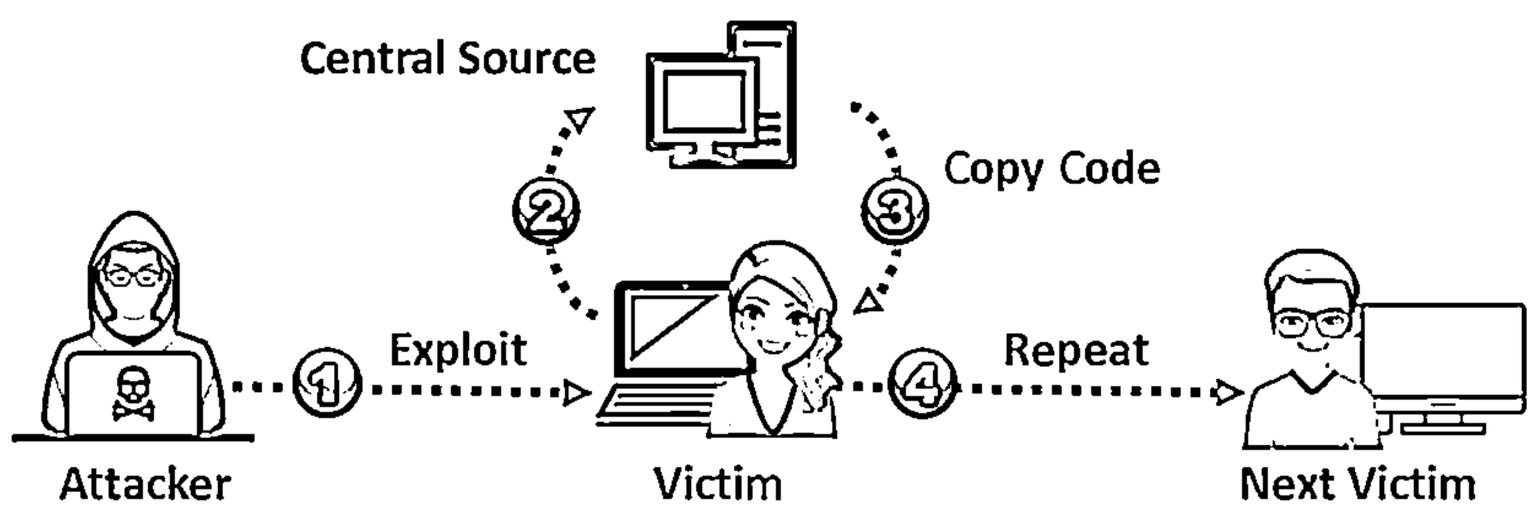


Figure 10.20: Central source propagation

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

- **Back-chaining Propagation**

  In this technique, the attacker places an attack toolkit on their own system, and a copy of the attack toolkit is transferred to a newly discovered vulnerable system. The attack tools installed on the attacking machine use some special methods to accept a connection from the compromised system and then transfer a file containing the attack tools to it. Simple port listeners containing a copy of this file or full intruder-installed web servers, both of which use the Trivial File Transfer Protocol (TFTP), support this back-channel file copy.

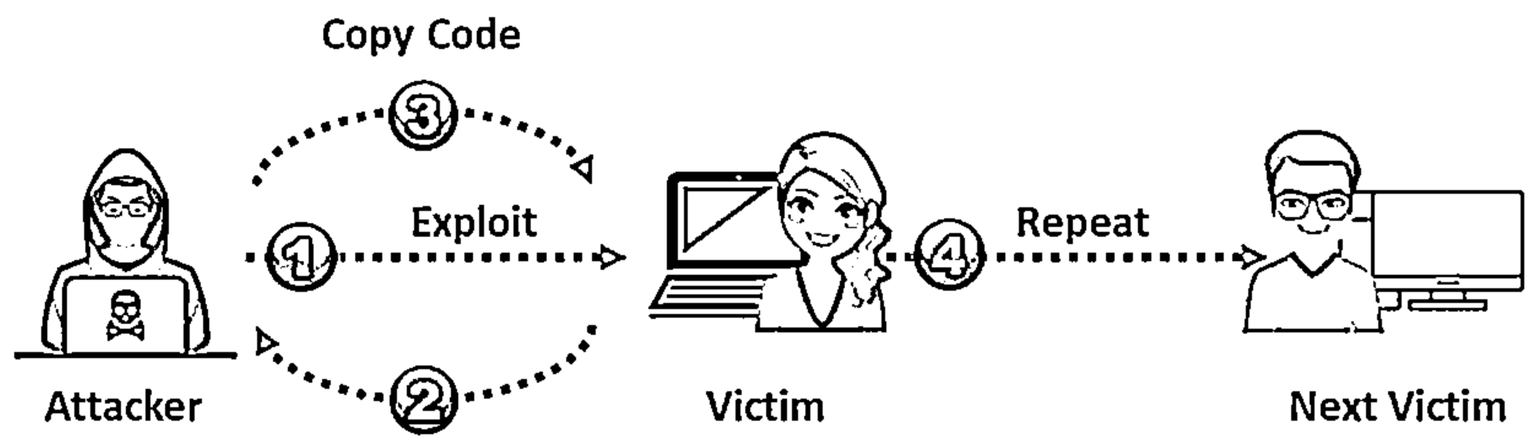


Figure 10.21: Back-chaining propagation

- **Autonomous Propagation**

  Unlike the previously discussed mechanisms, in which an external file source transfers the attack toolkit, in autonomous propagation, the attacking host itself transfers the attack toolkit to a newly discovered vulnerable system, exactly at the time it breaks into that system.

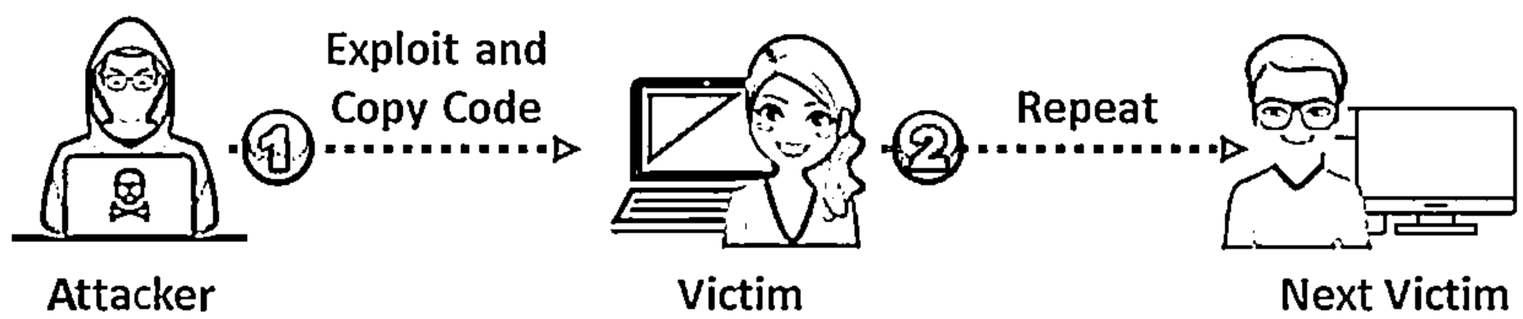
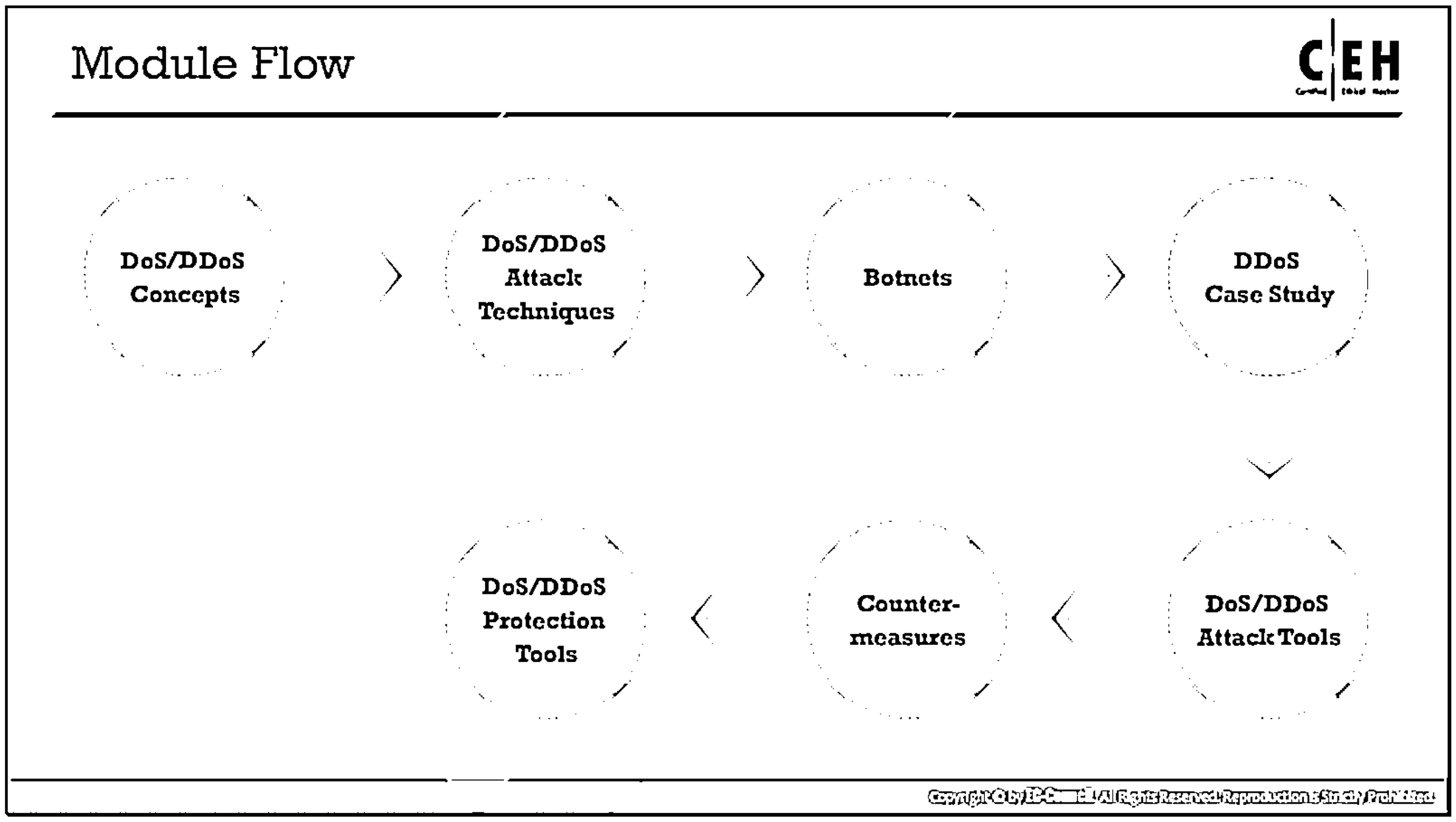


Figure 10.22: Autonomous Propagation

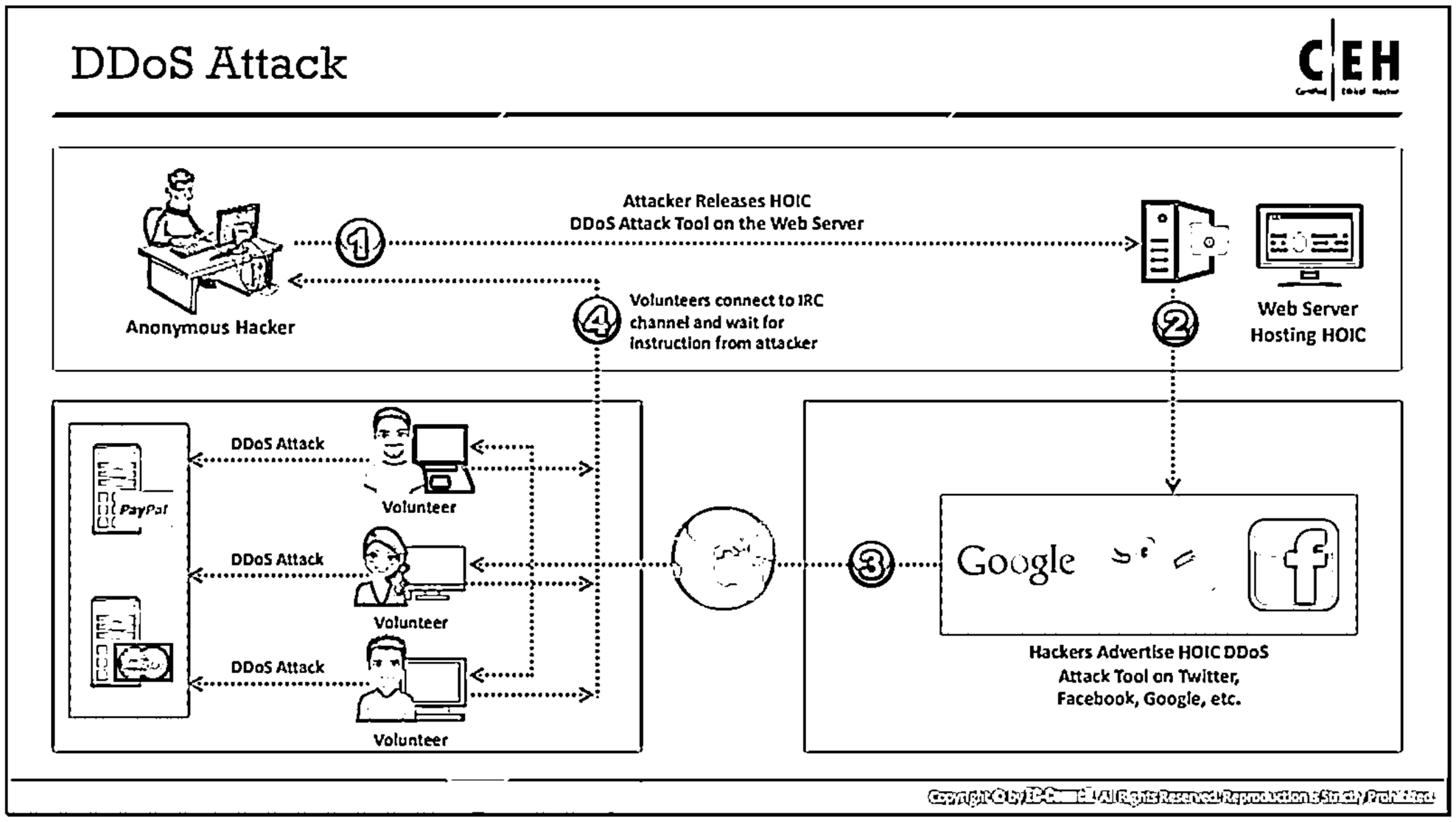
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



DDoS Case Study

DDoS attacks are sophisticated and complex attacks based on DoS and multiple distributed attack sources. In a DDoS attack, a large number of compromised computers (zombies) interrupt or suspend network services. This section presents a case study of a DDoS attack.

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



DDoS Attack

In a DDoS attack, attackers use a group of compromised systems (bots or zombies) usually infected with Trojans to perform a DoS attack on a target system or network resource.

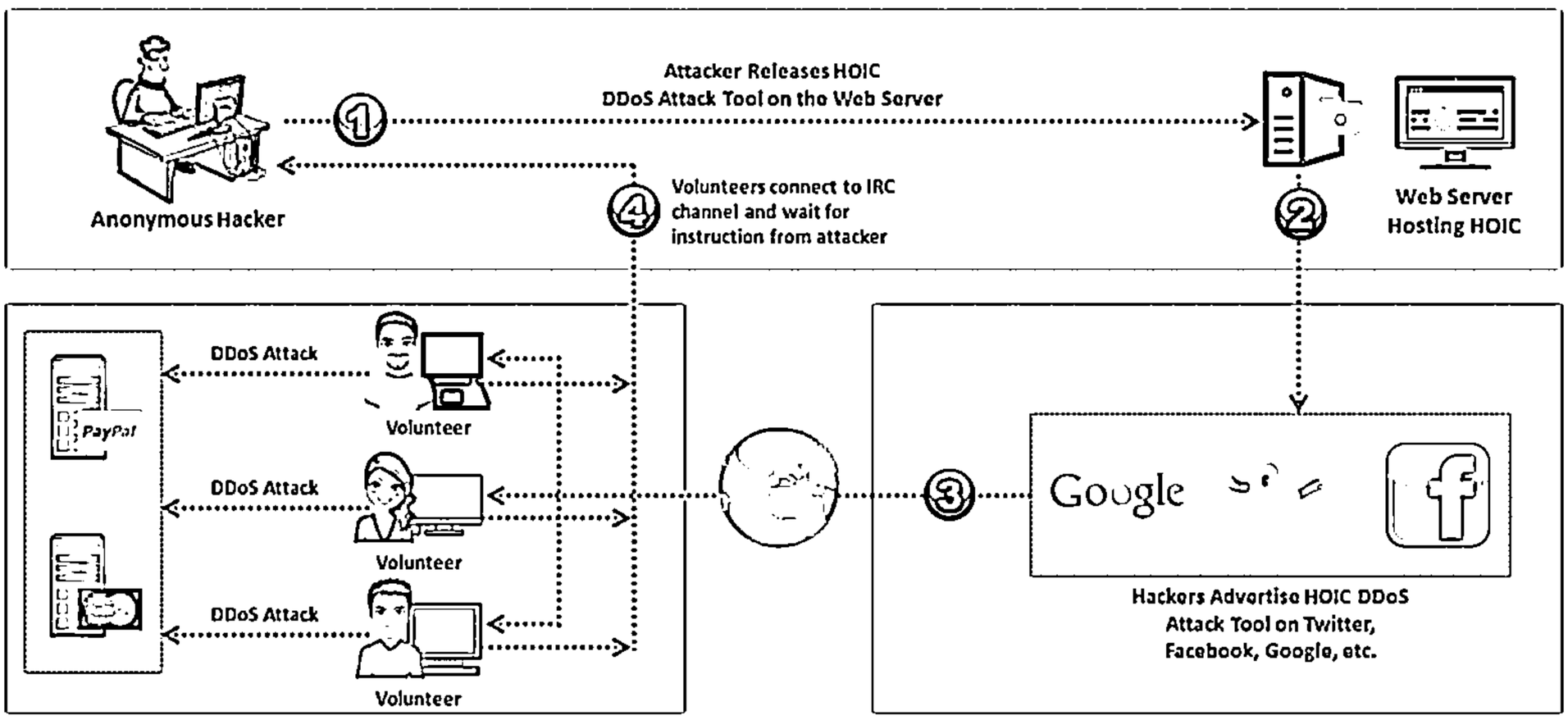


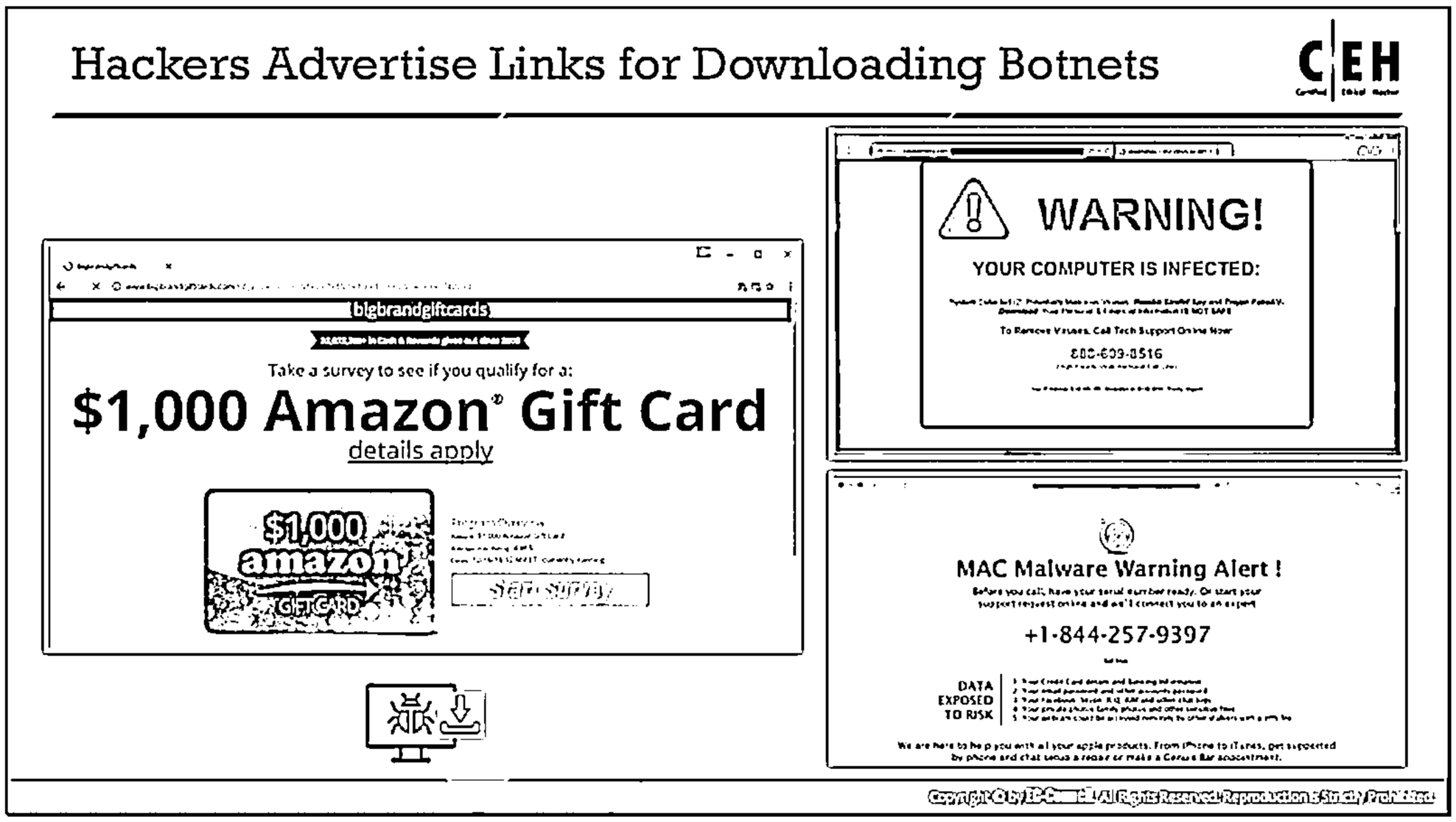
Figure 10.23: DDoS attack scenario

As shown in the figure, an anonymous hacker hosts a High Orbit Ion Cannon (HOIC) DDoS attack tool on a web server they own or on a compromised web server. The hacker then advertises the HOIC DDoS attack tool on social networking sites or search engines such as Twitter, Facebook, and Google with a malicious download link.

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

Users who desire to perform the DDoS attack may download the HOIC DDoS attack tool by clicking on the malicious download link provided by the hacker. These users are termed "volunteers." All the volunteers connect via an IRC channel to the anonymous hacker and await instructions to proceed further. The hacker instructs the volunteers to flood the target web server (e.g., PayPal, MasterCard, and PAYBACK) with multiple requests. On receiving instructions, the volunteers act accordingly. Consequently, the target server becomes overwhelmed and stops responding to requests from even legitimate users.

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



Hackers Advertise Links for Downloading Botnets

Hackers advertise botnets on various blogs, search engines, social networking sites, emails, and so on with download links. Hackers also use fake updates and security alerts to trick the victim into downloading the malware. The intention in doing so is to spread the botnet and increase the size of the attack network. This method of attack is very quick and effective. The below figure shows examples for ads hosted by hackers on the Internet to download botnets.

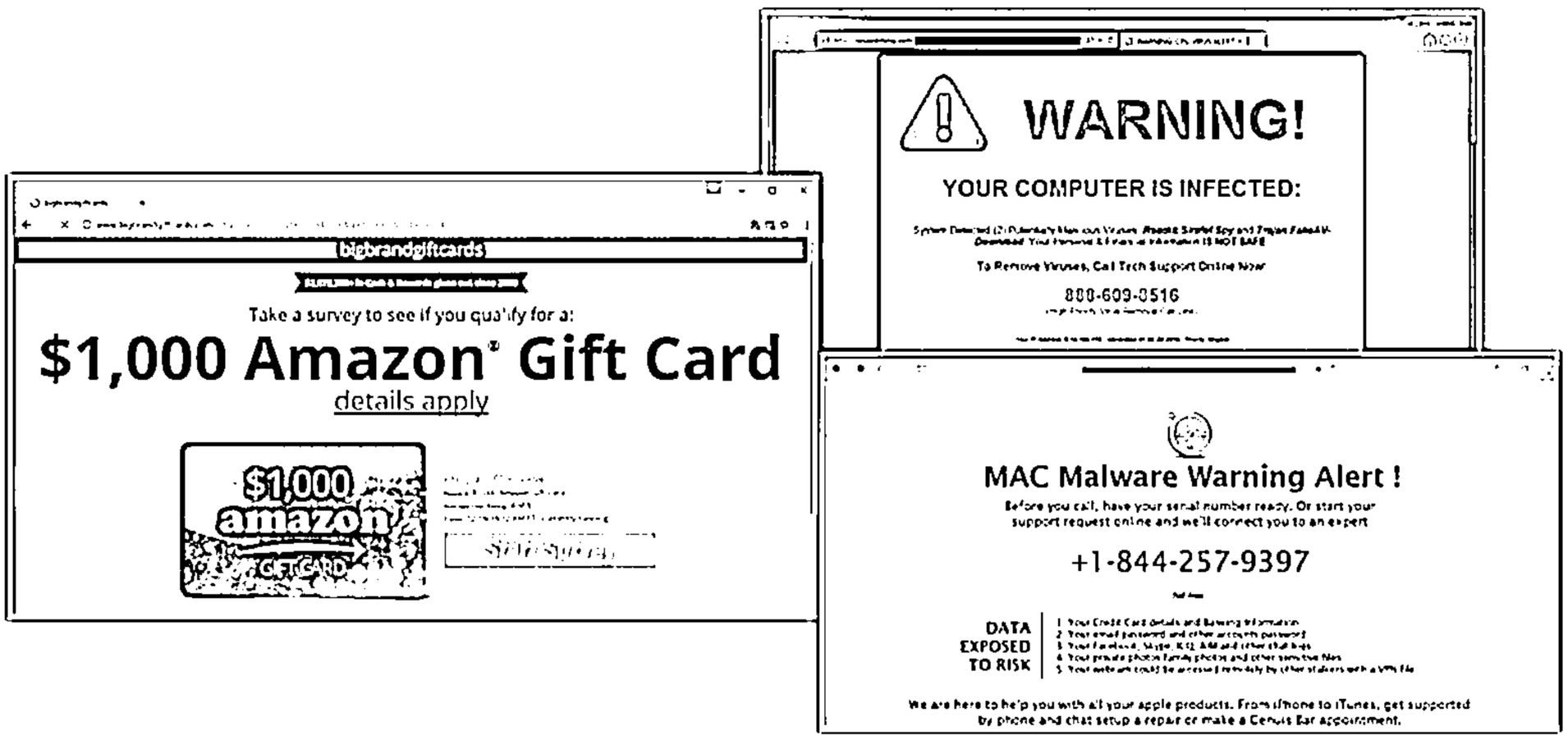


Figure 10.24: Advertisements with links to download botnets

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

Use of Mobile Devices as Botnets for Launching DDoS Attacks

- Android devices are passively vulnerable to various malware such as Trojan, bots, and RATs, which are often found in third-party application stores
- These unsecured Android devices are becoming primary targets for attackers to enlarge their botnet because they are highly vulnerable to malware
- Malicious Android applications found in the Google Play store and drive-by downloads are just a few examples of infection methods
- The attacker binds the malicious APK server to the Android application package (APK file), encrypts it, and removes unwanted features and permissions before distributing the malicious package to a third-party app store like the Google Play Store
- Once the user is tricked into downloading and installing such an application, the attacker can gain full control of the victim's device, enslaving the targeted device into the attacker's mobile botnet to perform malicious activities such as launching DDoS attacks and web injections

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

Use of Mobile Devices as Botnets for Launching DDoS Attacks

Android devices are passively vulnerable to various malware such as Trojans, bots, Remote Access Trojans (RATs), and so on, which are often found in third-party application stores. These unsecured android devices are becoming the primary targets for attackers to enlarge their botnet network because they are highly vulnerable to malware. Malicious android applications found in the Google Play Store and as drive-by downloads are examples for infection methods. The attacker binds a malicious server to the android application package (APK) file, encrypts it, and removes unwanted features and permissions before distributing the malicious package to a third-party app store such as Google Play Store. Once the victims are tricked into downloading and installing such applications, the victim's device is taken over by the attacker and integrated into the attacker's mobile botnet to perform malicious activities such as DDoS attacks and web injections.

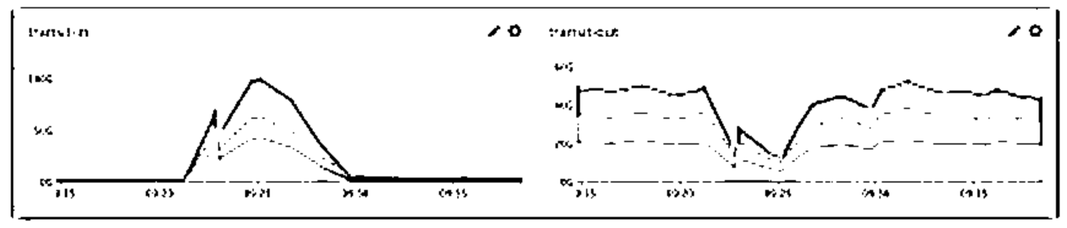
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

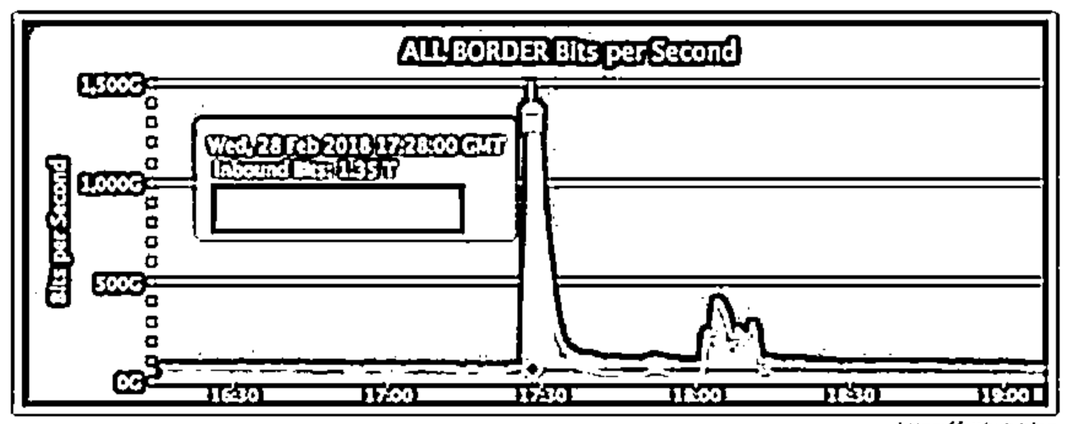
DDoS Case Study: DDoS Attack on GitHub

- In February 2018, GitHub encountered a devastating volumetric DDoS attack, which made its service unavailable to its users for 4 minutes
- This is the world's largest DDoS attack ever recorded

Attack Timeline

- The attack took place on Wednesday, 28 February 2018
- The attack made GitHub.com unavailable from 17:21 to 17:26 UTC and intermittently unavailable from 17:26 to 17:30 UTC due to a heavy inflow of data packets
- The first portion of the attack peaked at 1.35 Tbps via 126.9 million packets per second, and a second 400 Gbps spike occurred a little after 18:00 UTC





https://github.blog

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

DDoS Case Study: DDoS Attack on GitHub (Cont'd)

Attack Mechanism

- It was an amplification attack using a Memcached-based approach that peaked at 1.35 Tbps
- The attack originated from over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints
- The attack worked by abusing instances of Memcached servers that are inadvertently accessible on the public internet with UDP support enabled
- The spoofing of IP addresses allowed the responses of Memcached servers to be redirected to target a different address and send more data toward the target than needs to be sent by the unspoofed source
- The vulnerability arising from this misconfiguration caused an amplification factor of up to 51,000, meaning that for each byte sent by the attacker, up to 51 kB was sent toward the target
- This large amplification factor caused a devastating inflow of 1.3 Tbps of data toward GitHub, interrupting its normal operations

https://github.blog

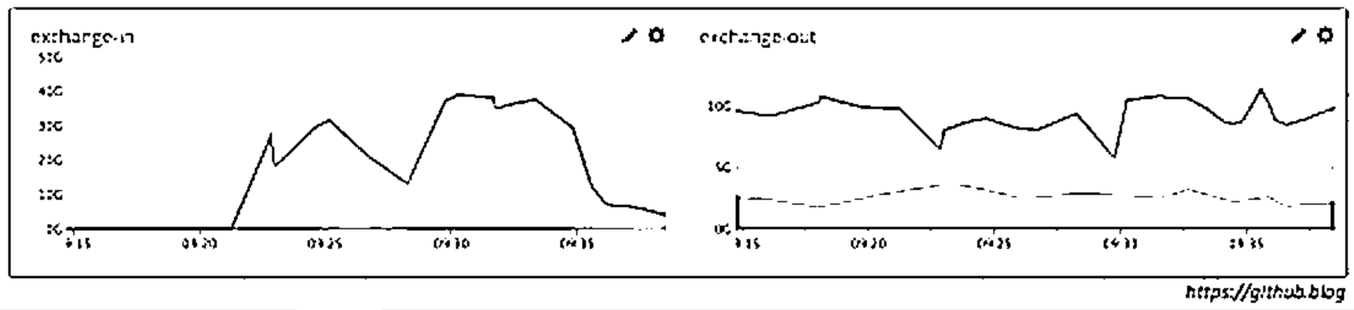
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

DDoS Case Study: DDoS Attack on GitHub (Cont'd)

GitHub's Response

- Given the increase in inbound transit bandwidth to over 100 Gbps in one of GitHub's facilities, GitHub personnel made the decision to move incoming traffic to Akamai
- At 17:26 UTC, the command was initiated via GitHub's ChatOps tooling to withdraw BGP announcements over transit providers and announce AS36459 exclusively over GitHub's links to Akamai
- Routes reconverged in the next few minutes and access control lists mitigated the attack at their border
- Monitoring of transit bandwidth levels and load balancer response codes indicated a full recovery at 17:30 UTC
- At 17:34 UTC, routes to internet exchanges were withdrawn as a follow-up to shift an additional 40 Gbps away from GitHub's Network



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

DDoS Case Study: DDoS Attack on GitHub

Source: *https://github.blog*

GitHub is a renowned open-source cloud platform used as a repository by many companies, businesses, and researchers with wide areas of interest. In February 2018, GitHub encountered a devastating DDoS attack, which made its service unavailable to users for 4 min. This was the world's largest DDoS attack ever recorded.

- **Attack Timeline**

  The DDoS attack occurred on Wednesday, February 28, 2018. This volumetric DDoS attack made GitHub.com unavailable from 17:21 to 17:26 UTC and intermittently unavailable from 17:26 to 17:30 UTC owing to a heavy inflow of data packets.

  At 17:21 UTC, GitHub's network monitoring system detected an anomaly in the ratio of ingress to egress traffic, and they notified the on-call engineer and others. The below figure shows inbound versus outbound throughput over transit links.

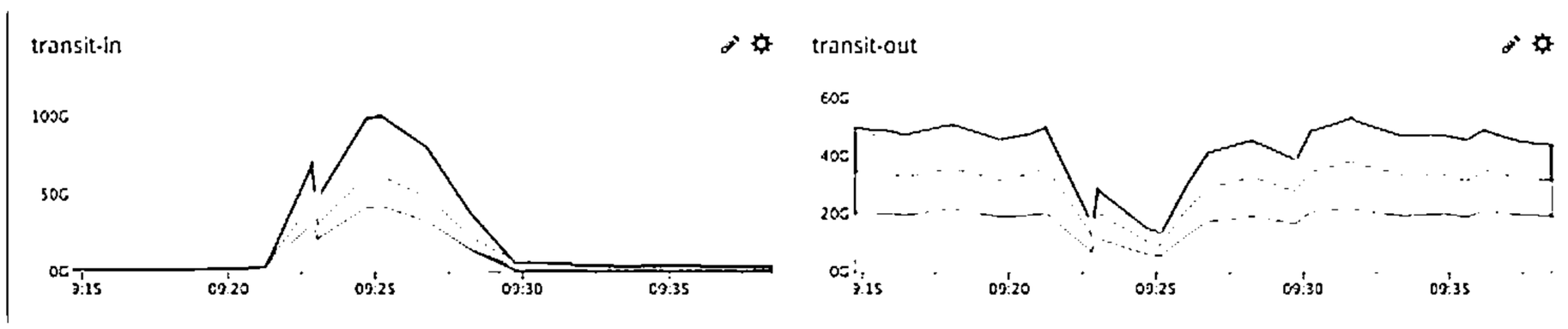


Figure 10.25: Inbound versus outbound throughput over transit links

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

The first portion of the attack peaked at 1.35 Tbps via 126.9 million packets per second (pps), and a second 400 Gbps spike occurred a little after 18:00 UTC. The below figure, provided by Akamai, shows inbound traffic in bits per second (bps).

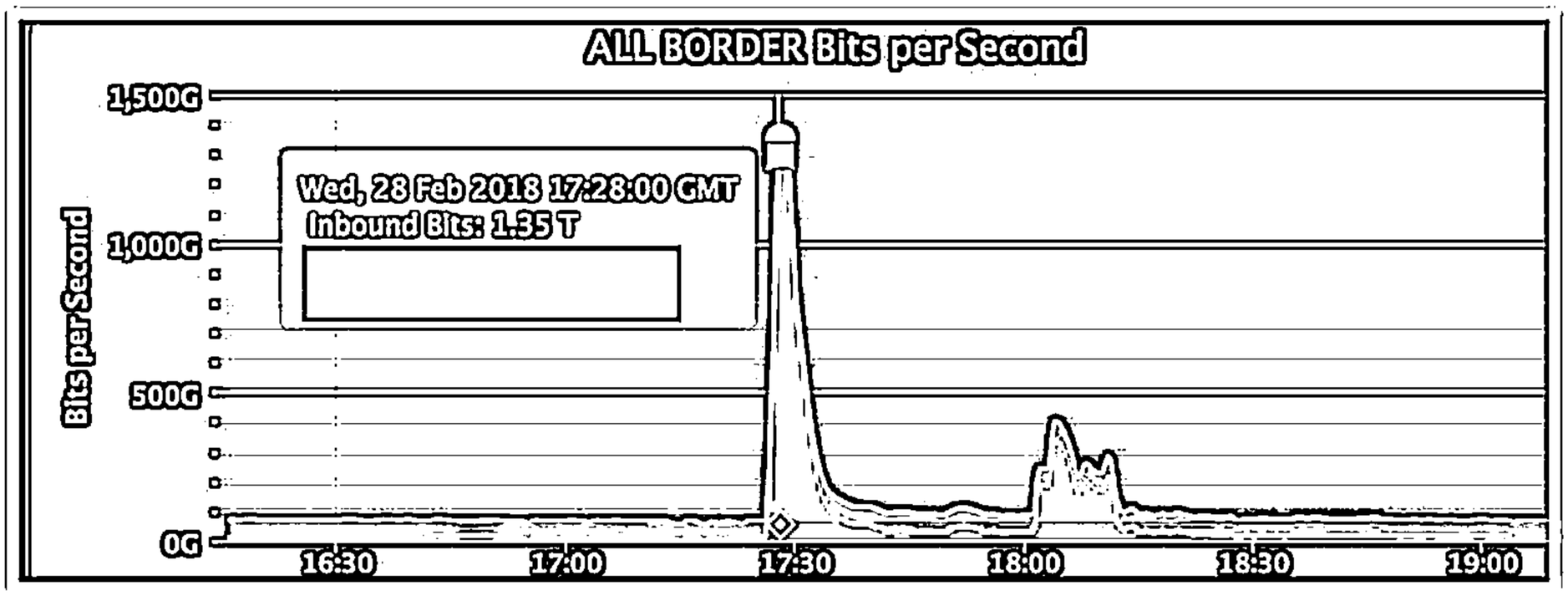


Figure 10.26: Inbound traffic in bits per second

- **Attack Mechanism**

  This attack was an amplification attack using a Memcached-based approach that peaked at 1.35 Tbps. The attack originated from over a thousand different autonomous system numbers (ASNs) across tens of thousands of unique endpoints. The attack worked by abusing Memcached instances that were inadvertently accessible on the public Internet with UDP support enabled. The spoofing of IP addresses allowed Memcached's responses to be targeted against another address and more data than necessary to be sent toward the target by the unspoofed source. The vulnerability due to this misconfiguration caused an amplification factor of up to 51,000, implying that up to 51 KB was sent toward the target for each byte sent by the attacker. This large amplification factor caused the devastating inflow of 1.3 Tbps data towards GitHub, interrupting its normal operations.

- **GitHub's Response**

  Given the increase in inbound transit bandwidth to over 100 Gbps in one of GitHub's facilities, GitHub personnel decided to move the incoming traffic to Akamai. At 17:26 UTC, a command was initiated via GitHub's ChatOps tooling to withdraw Border Gateway Protocol (BGP) announcements over transit providers and announce AS36459, the autonomous system belonging to GitHub, exclusively over GitHub's links to Akamai.

  Routes reconverged in the next few minutes, and access control lists mitigated the attack at their border. The monitoring of transit bandwidth levels and load balancer response codes indicated a full recovery at 17:30 UTC. At 17:34 UTC, routes to Internet exchanges were withdrawn as a follow-up to shift an additional 40 Gbps away from GitHub's network.

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

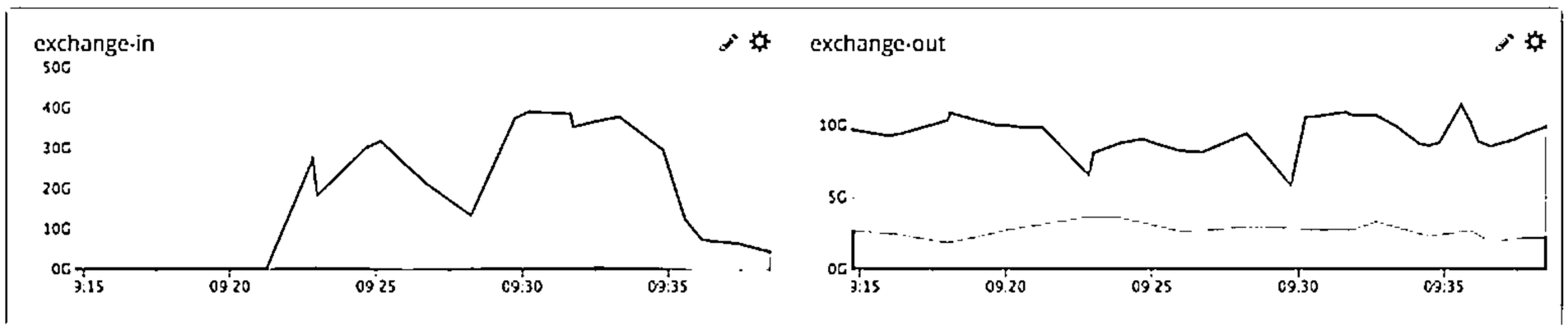
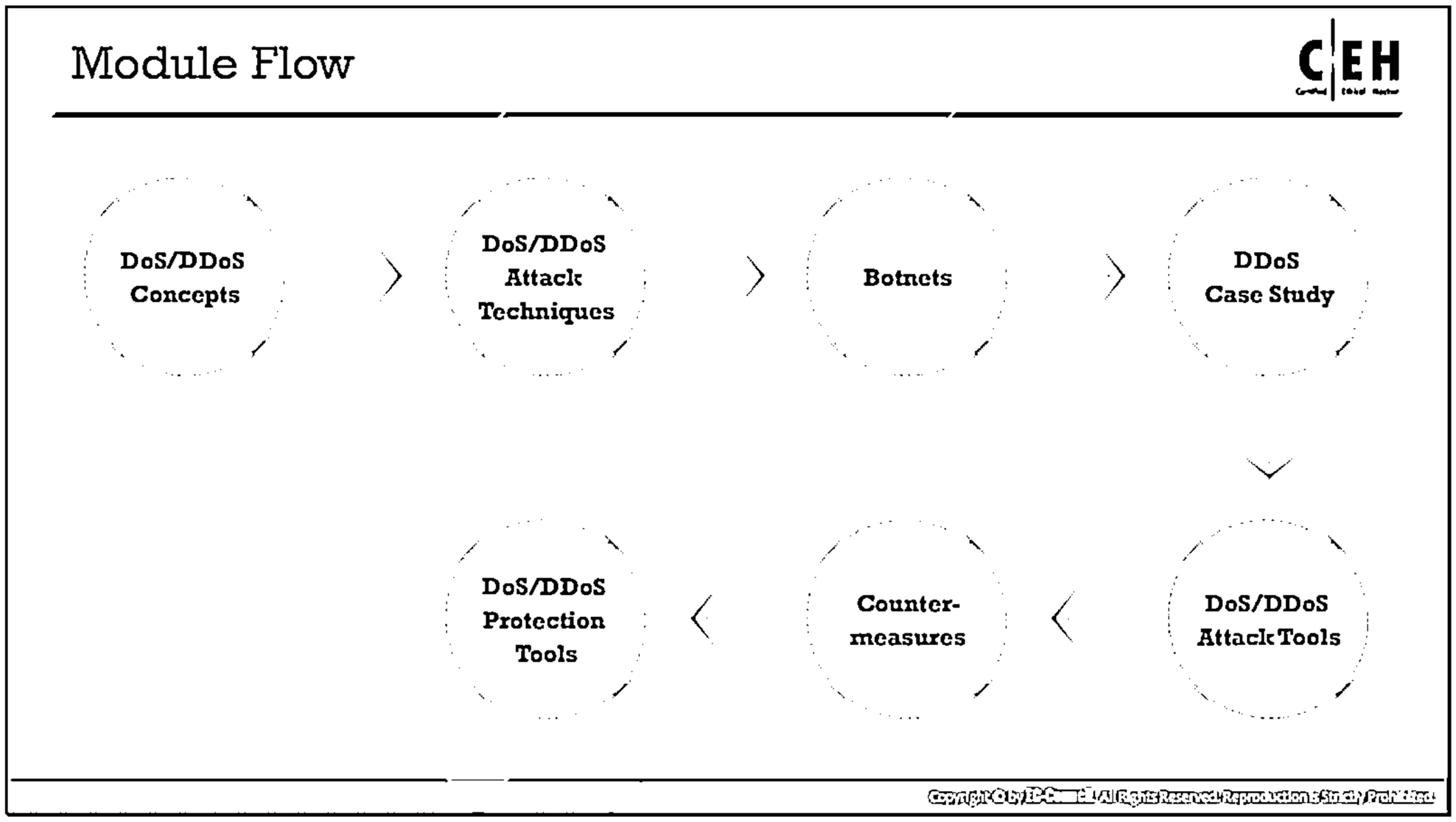


Figure 10.27: Inbound versus outbound throughput over transit links

After this incident, GitHub revealed that they were investigating the use of their monitoring infrastructure to automate DDoS mitigation providers and would continue to measure response times to similar incidents with a goal of reducing the mean time to recovery (MTTR).

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



DoS/DDoS Attack Tools

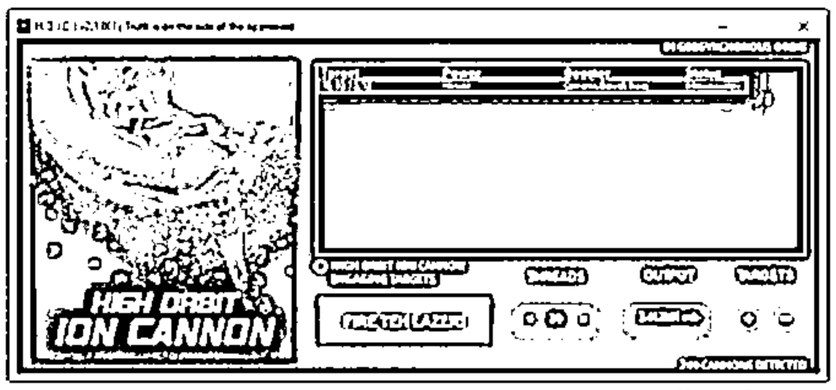
This section deals with various DoS/DDoS attack tools used to take over a single or multiple network system to exhaust their computing resources or render them unavailable to their intended users.

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

DoS/DDoS Attack Tools

High Orbit Ion Cannon (HOIC)

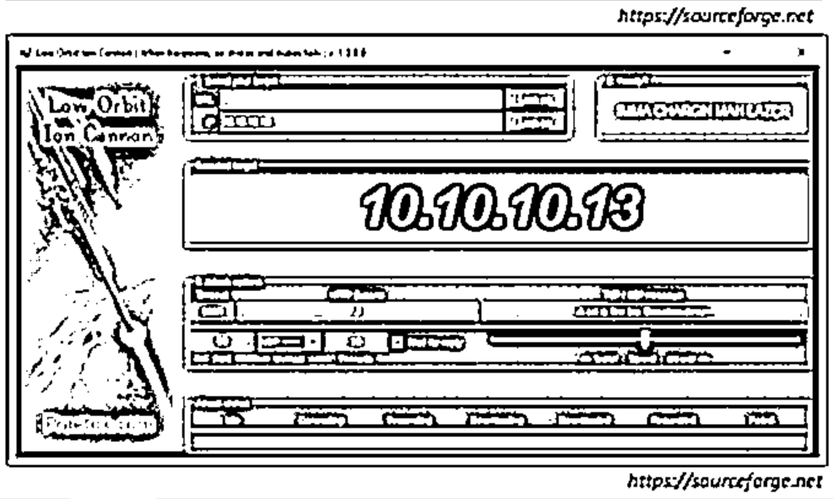
HOIC carries out a DDoS to attack any IP address with a user selected port and a user selected protocol



https://sourceforge.net

Low Orbit Ion Cannon (LOIC)

LOIC can be used on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host



https://sourceforge.net

DoS/DDoS Attack Tools

- XOIC (*http://anonhacktivism.blogspot.com*)
- HULK (*https://siberianlaika.ru*)
- Tor's Hammer (*https://sourceforge.net*)
- Slowloris (*https://github.com*)
- PyLoris (*https://sourceforge.net*)
- R-U-Dead-Yet (*https://sourceforge.net*)

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

DoS/DDoS Attack Tools

- **High Orbit Ion Cannon (HOIC)**

  Source: *https://sourceforge.net*

  HOIC is a network stress and DoS/DDoS attack application written in BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP POST and GET requests to a computer that uses lulz-inspired GUIs. Its features are summarized as follows:

  - High-speed multi-threaded HTTP flooding
  - Simultaneous flooding of up to 256 websites
  - Built-in scripting system to allow the deployment of "boosters," which are scripts designed to thwart DDoS countermeasures and increase DoS output
  - Portability to Linux/Mac with a few bug fixes
  - Ability to select the number of threads in an ongoing attack
  - Ability to throttle attacks individually with three settings: LOW, MEDIUM, and HIGH

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

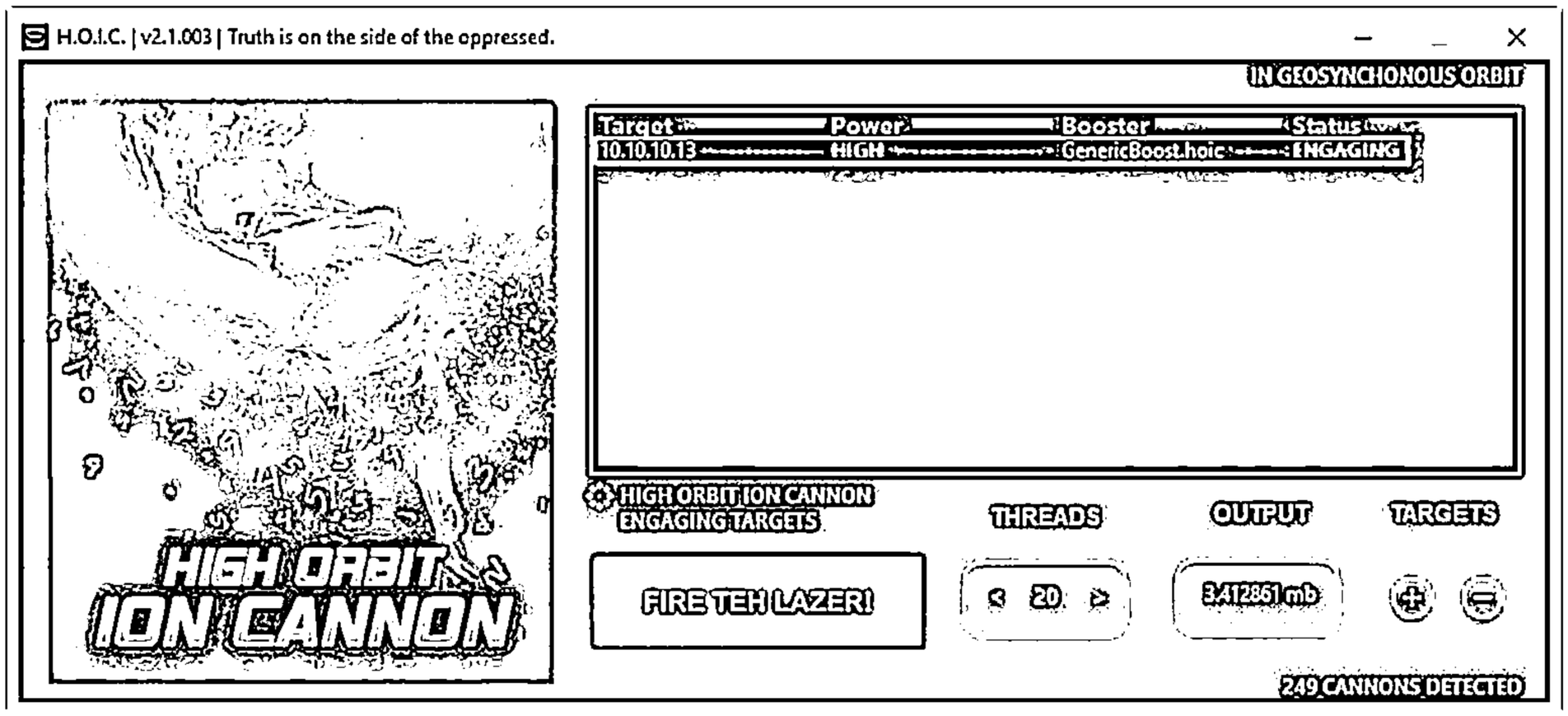


Figure 10.28: Screenshot of HOIC DoS attack tool

- **Low Orbit Ion Cannon (LOIC)**

  Source: *https://sourceforge.net*

  LOIC is a network stress testing and DoS attack application. LOIC attacks can be called application-based DOS attacks because they primarily target web applications. LOIC can be used on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service.

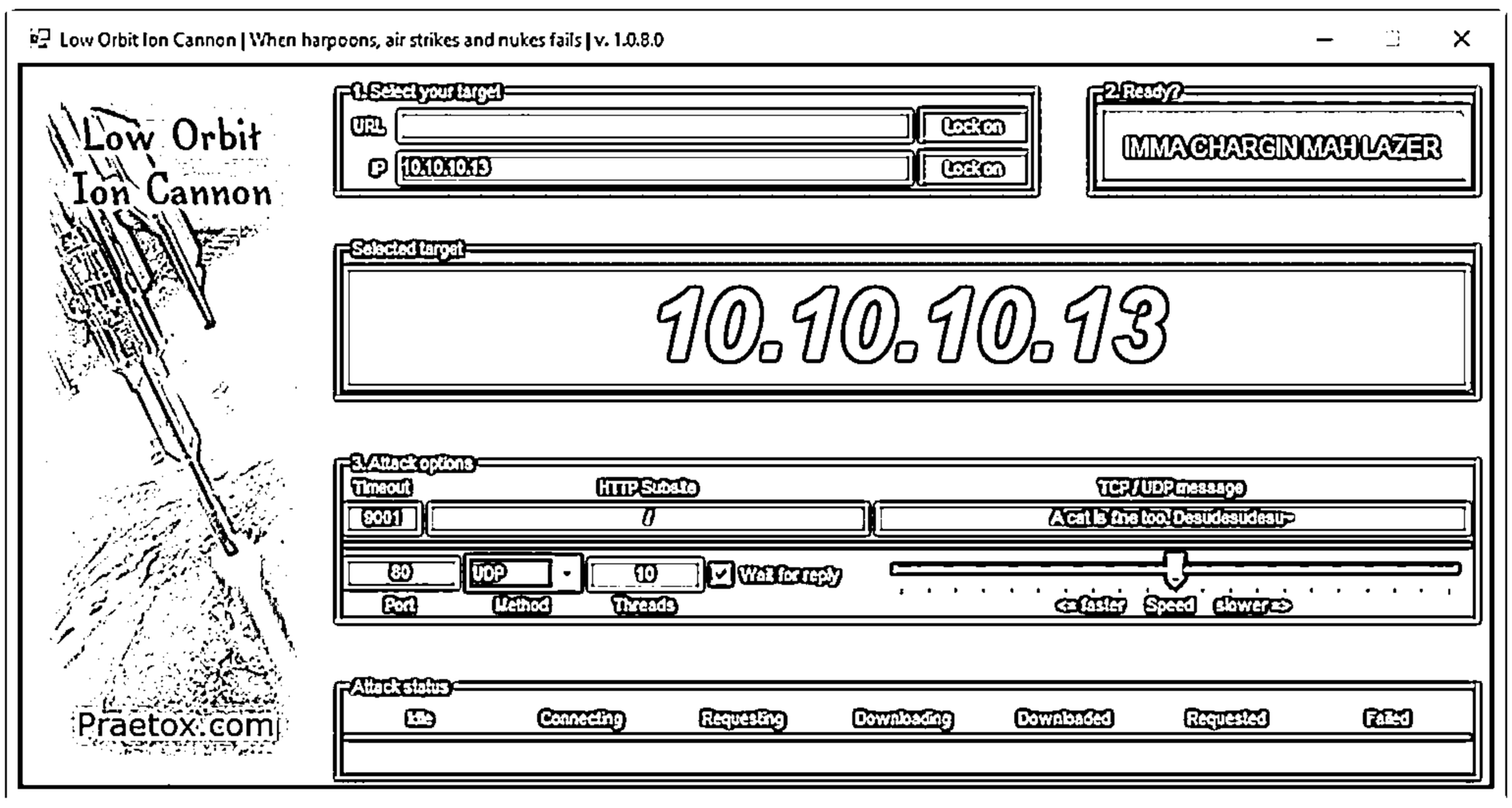


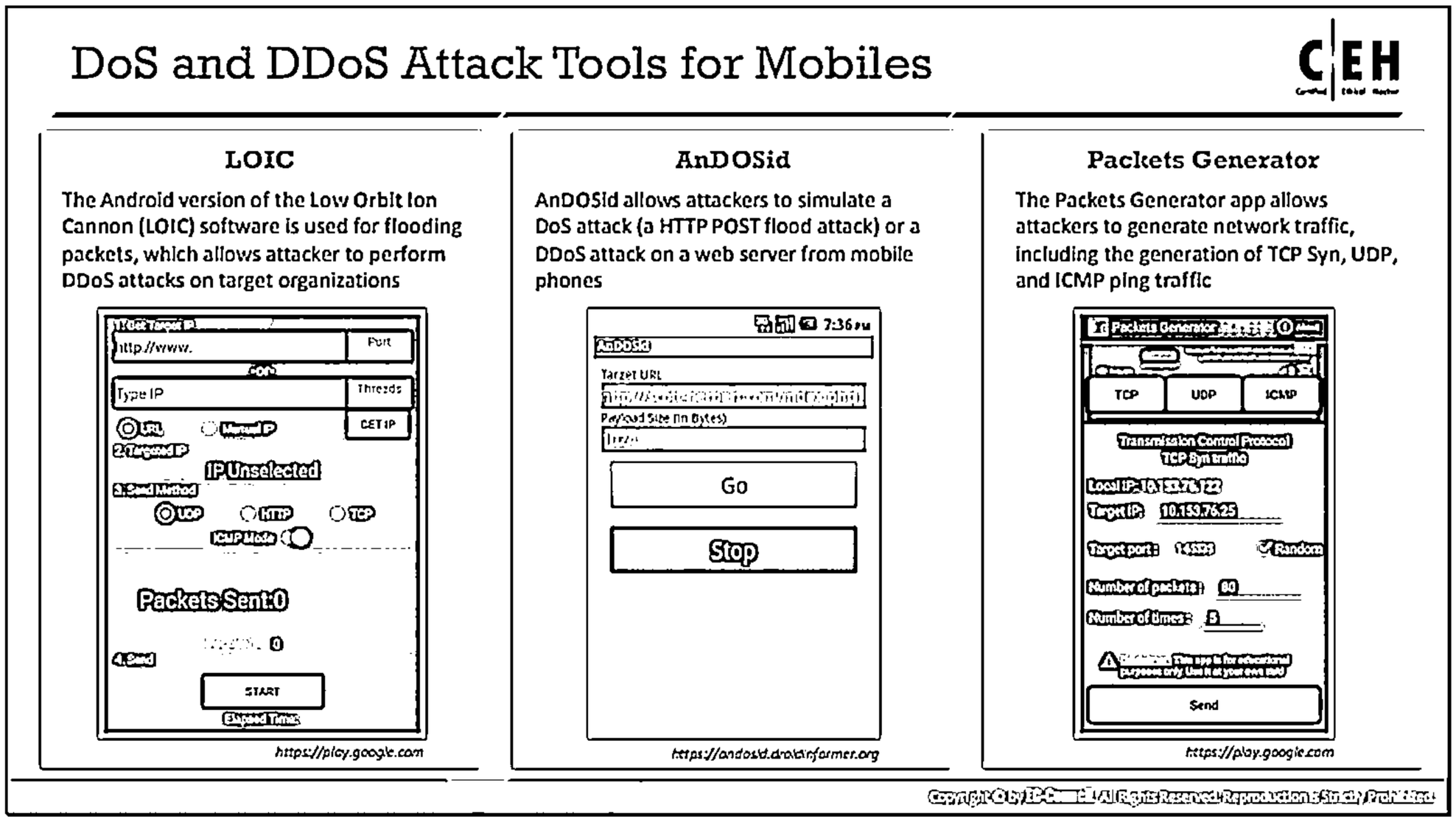
Figure 10.29: Screenshot of LOIC DoS attack tool

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

The following are some of the additional DoS/DDoS attack tools:

- XOIC (*http://anonhacktivism.blogspot.com*)
- HULK (*https://siberianlaika.ru*)
- Tor's Hammer (*https://sourceforge.net*)
- Slowloris (*https://github.com*)
- PyLoris (*https://sourceforge.net*)
- R-U-Dead-Yet (*https://sourceforge.net*)

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



DoS/DDoS Attack Tools for Mobiles

- **LOIC**

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

  The Android version of LOIC software is used for flooding packets, which allows the attacker to perform a DDoS attack on the target organization. This application can perform UPD, HTTP, or TCP flood attacks.

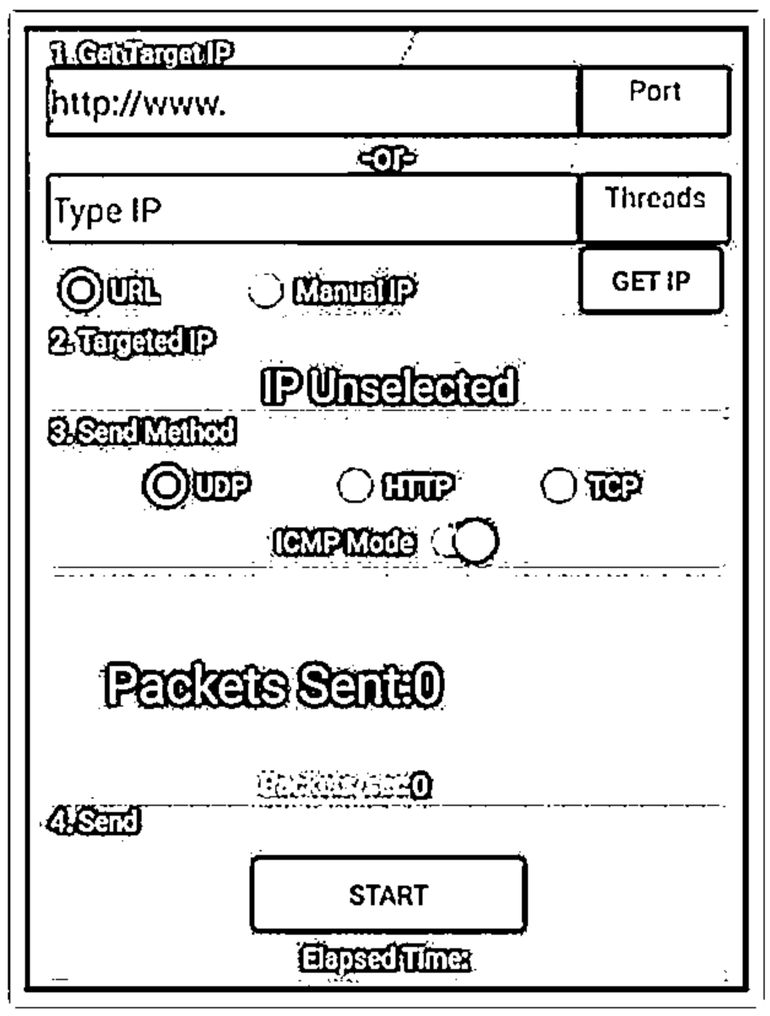


Figure 10.30: Screenshot of LOIC DoS attack tool for mobile

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

- **AnDOSid**

  Source: *https://andosid.droidinformer.org*

  AnDOSid allows the attacker to simulate a DoS attack (an HTTP POST flood attack to be precise) and DDoS attack on a web server from mobile phones.

Figure 10.31: Screenshot of AnDOSid DoS attack tool for mobile

- **Packets Generator**

  Source: https://play.google.com

  The Packets Generator app allows attackers to generate network traffic including TCP SYN, UDP, and ICMP ping traffic. It is effectively used for testing a firewall's filtering rules, an intrusion detection system's attack signatures, and a router's access-control lists (ACLs) by sending a series of generated packets towards a target.

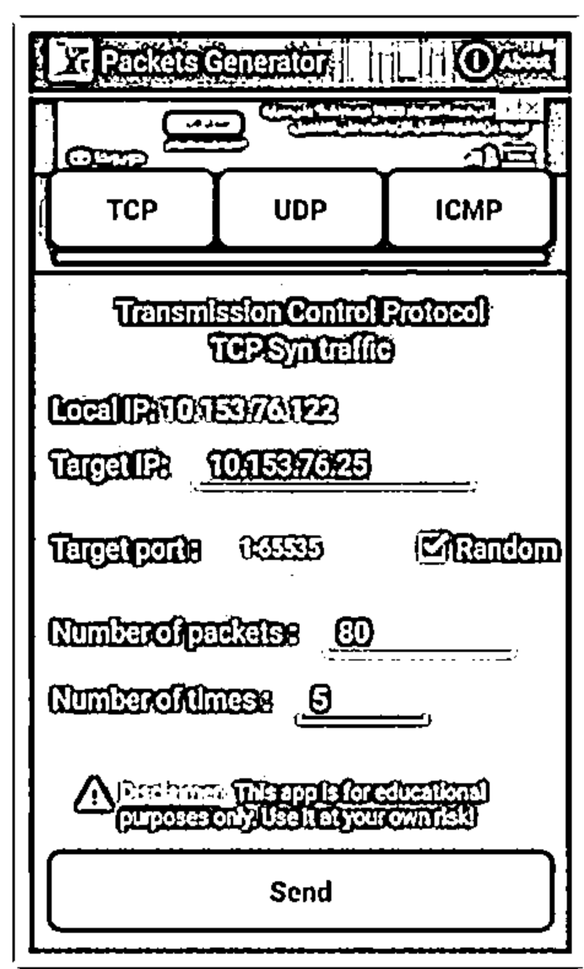
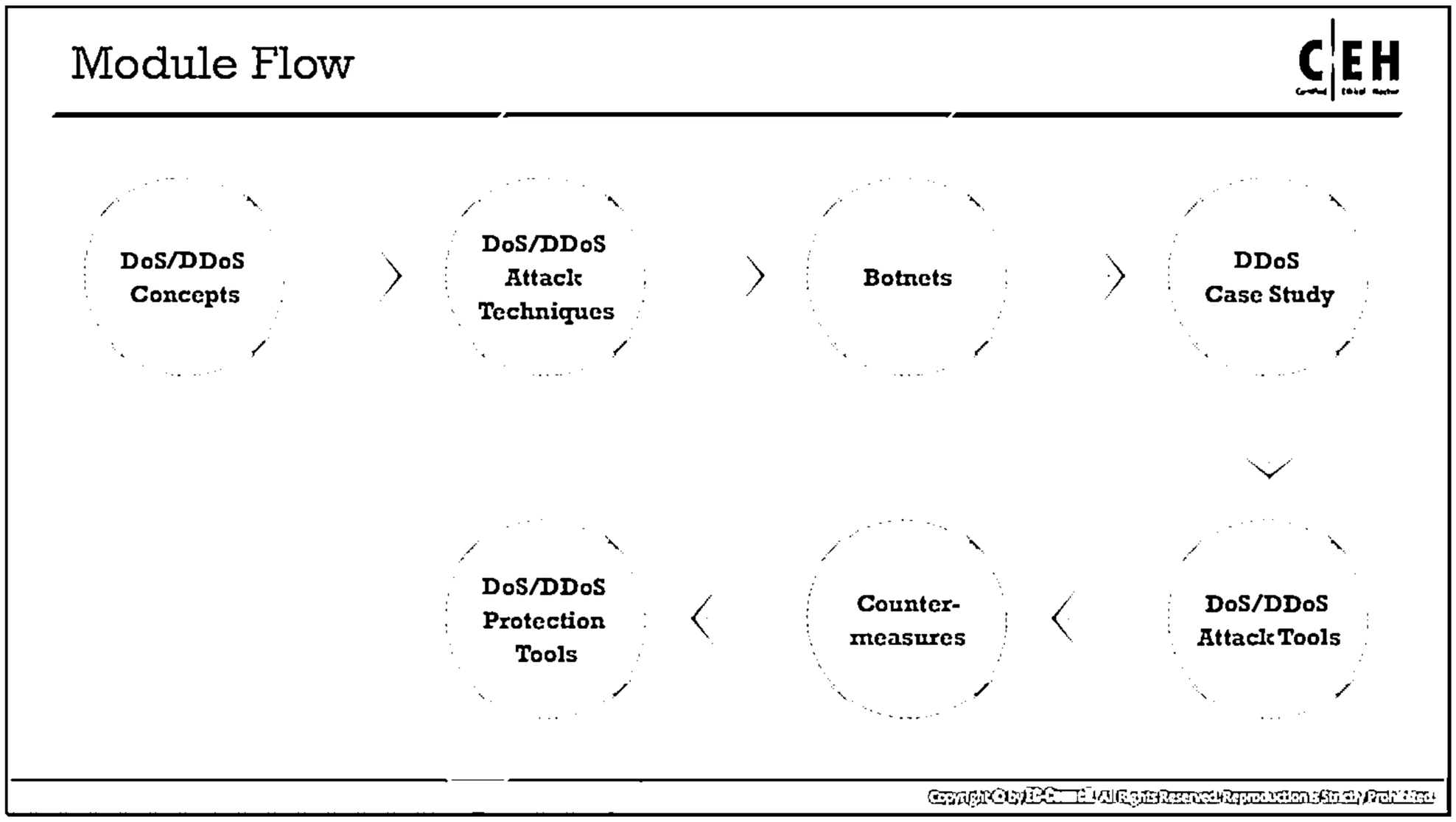


Figure 10.32: Screenshot of Packets Generator tool for mobile

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



Countermeasures

DoS/DDoS is one of the foremost security threats on the Internet; thus, there is a great necessity for solutions to mitigate these attacks. This section discusses detection methods, various preventive measures, and responses to DoS/DDoS attacks.

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

Detection Techniques

- Detection techniques are based on identifying and discriminating illegitimate traffic increases and flash events from legitimate packet traffic
- All detection techniques define an attack as an abnormal and noticeable deviation from a threshold of normal network traffic statistics

Activity Profiling

- Activity profiling is done based on the average packet rate for a network flow, which consists of consecutive packets with similar packet fields
- Activity profiles are obtained by monitoring network packet header information
- An attack is indicated by the following:
  - An increase in activity levels among the network flow clusters
  - An increase in the overall number of distinct clusters (DDoS attack)

Sequential Change-Point Detection

- Change-point detection algorithms isolate changes in network traffic statistics and in the traffic flow rate caused by attacks
- The algorithms filter the target traffic data by address, port, or protocol and store the resultant flow as a time series
- The sequential change-point detection technique uses the Cusum algorithm to identify and locate DoS attacks
- This technique can also be used to identify the typical scanning activities of network worms

Wavelet-Based Signal Analysis

- Wavelet analysis describes an input signal in terms of spectral components
- Analyzing each spectral window's energy determines the presence of anomalies
- Wavelet-based signal analysis filters out the anomalous traffic flow input signals from background noise

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

Detection Techniques

Early detection techniques help prevent DoS/DDoS attacks. Detecting a DoS/DDoS attack is a tricky task. A DoS/DDoS attack traffic detector needs to distinguish between a genuine and a bogus data packet, which is not always possible. Therefore, the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS/DDoS attack. Detection techniques are based on the identification and discrimination of an illegitimate traffic increase and flash events from legitimate packet traffic.

One problem in filtering bogus traffic from legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS/DDoS attack.

All the detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve the statistical analysis of deviations to categorize malicious and genuine traffic.

The following are the three types of detection techniques:

- **Activity Profiling**

  Activity profiling is performed based on the average packet rate for network flow, which consists of consecutive packets with similar packet header information. The packet header information includes the IP addresses of the destination and sender, ports, and transport protocols used. An attack is indicated by

  - An increase in activity levels among the network flow clusters
  - An increase in the overall number of distinct clusters (DDoS attack)

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

For a higher average packet rate or activity level of a flow, the time between consecutive matching packets is lower. Randomness in the average packet rate or activity level can indicate suspicious activity. The entropy calculation method measures randomness in activity levels. If a network is under attack, the entropy of network activity levels increases.

One of the major hurdles in the activity profiling method is the huge volume of traffic. This problem can be overcome by clustering packet flows with similar characteristics. Because DoS attacks generate a large number of data packets that are very similar, an increase in the average packet rate or an increase in the diversity of packets could indicate a DoS attack.

- **Sequential Change-Point Detection**

  In the sequential change-point detection technique, network traffic is filtered by IP addresses, targeted port numbers, and communication protocols used, and the traffic flow data are stored in a graph that shows the traffic flow rate versus time. Change-point detection algorithms isolate changes in network traffic statistics and in traffic flow rate caused by attacks. If there is a drastic change in traffic flow rate, a DoS attack may be occurring.

  This technique uses the cumulative sum (CUSUM) algorithm to identify and locate DoS attacks. The algorithm calculates deviations in the actual versus expected local average in the traffic time series. The sequential change-point detection technique identifies the typical scanning activities of network worms.

- **Wavelet-Based Signal Analysis**

  The wavelet analysis technique analyzes network traffic in terms of spectral components. It divides incoming signals into various frequencies and analyzes different frequency components separately. Analyzing each spectral window's energy reveals the presence of anomalies. These techniques check frequency components present at a specific time and provide a description of those components. The presence of an unfamiliar frequency indicates suspicious network activity.

  A network signal consists of a time-localized data packet flow signal and background noise. Wavelet-based signal analysis filters out the input signals of anomalous traffic flow from background noise. Normal network traffic is generally low-frequency traffic. During an attack, the high-frequency components of a signal increase.

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

DoS/DDoS Countermeasure Strategies

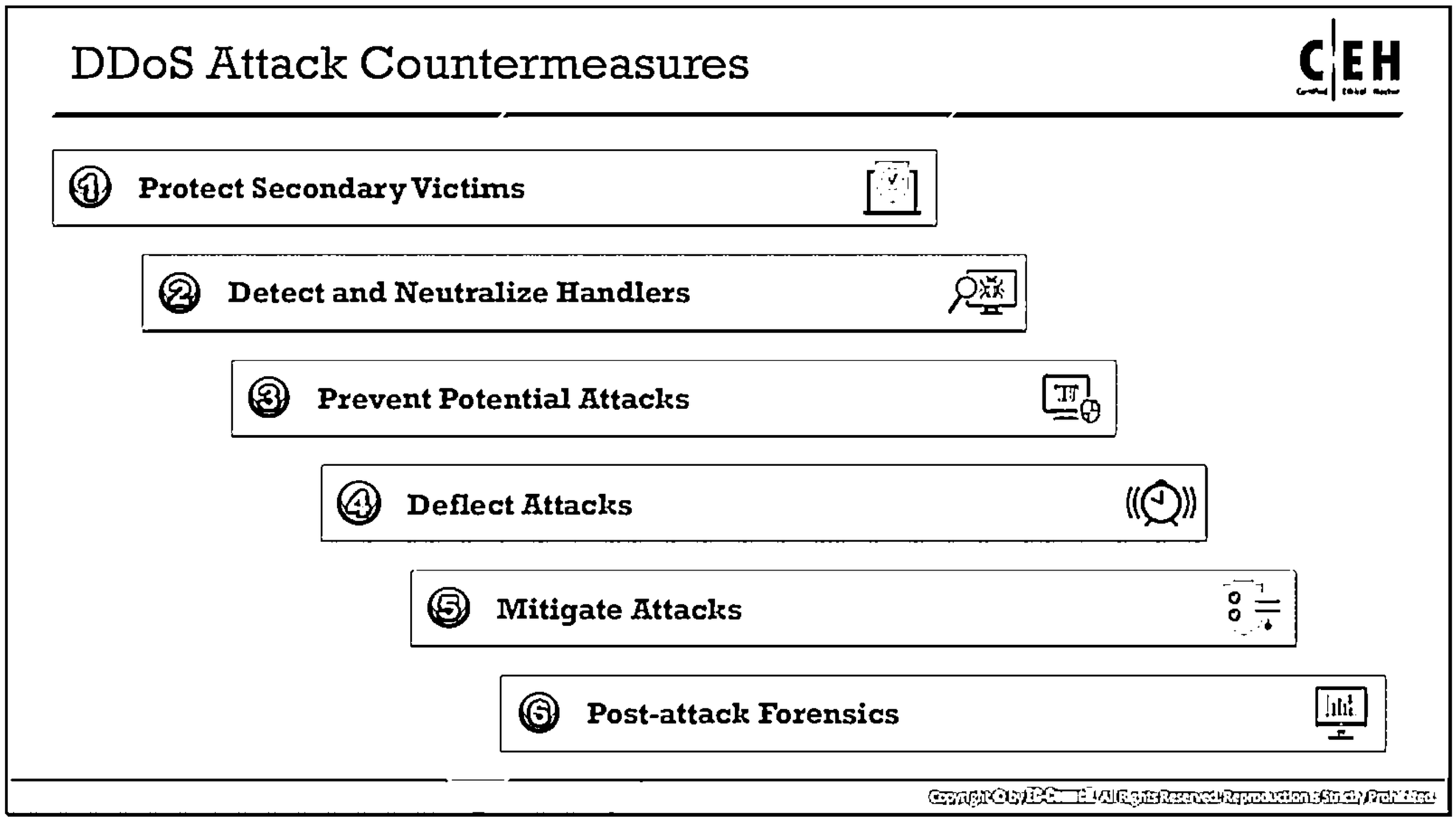
Absorbing the Attack	⊖ Use additional capacity to absorb the attack ⊖ Requires preplanning and additional resources
Degrading Services	⊖ Identify critical services to maintain functionality while stopping non-critical services
Shutting Down the Services	⊖ Shut down all services until the attack has subsided

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

DoS/DDoS Countermeasure Strategies

- **Absorbing the Attack**: In this strategy, additional capacity is used to absorb an attack, which requires preplanning. It also requires additional resources. One disadvantage associated with this strategy is the cost of additional resources, which is incurred even when no attacks are underway.
- **Degrading Services**: If it is not possible to keep all services functioning during an attack, it is a good idea to keep at least the critical services functional. For this, the critical services are first identified, following which the network, systems, and application designs are customized to cut down the noncritical services. This strategy may help keep the critical services functional.
- **Shutting Down Services**: In this strategy, all services are shut down until an attack has subsided. Though it may not be the ideal choice, it may be a reasonable response in some cases.

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



DDoS Attack Countermeasures

Many solutions have been proposed for mitigating the effects of a DDoS attack. However, no single complete solution exists that can protect all known forms of DDoS attacks. Moreover, attackers continually devise new methods to perform DDoS attacks to bypass the security solutions employed.

The following are examples for DDoS attack countermeasures:

- Protect secondary victims
- Neutralize handlers
- Prevent potential attacks
- Deflect attacks
- Mitigate attacks
- Post-attack forensics

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

Protect Secondary Victims and Detect and Neutralize Handlers

Protect Secondary Victims

- Monitor security regularly to remain protected from DDoS agent software
- Install anti-virus and anti-Trojan software and keep them up-to-date
- Increase awareness regarding security issues and prevention techniques among all Internet users
- Disable unnecessary services, uninstall unused applications, and scan all files received from external sources
- Properly configure and regularly update the built-in defensive mechanisms in the core hardware and software of systems

Detect and Neutralize Handlers

Network Traffic Analysis

- Analyze communication protocols and traffic patterns between handlers and clients or handlers and agents in order to identify the network nodes that might be infected by the handlers

Neutralize Botnet Handlers

- There are usually fewer DDoS handlers deployed compared to the number of agents. Neutralizing a few handlers can possibly render multiple agents useless, thus thwarting DDoS attacks

Spoofed Source Address

- There is a decent probability that the spoofed source address of DDoS attack packets will not represent a valid source address of the definite sub-network

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

Protect Secondary Victims

- **Individual Users**

  The best method to prevent DDoS attacks is for secondary victim systems to prevent themselves from taking part in the attack. This demands intensified security awareness and prevention techniques. Secondary victims must monitor their security regularly to remain protected from DDoS agent software. It must be ensured that the system does not install any DDoS agent program; further, DDoS agent traffic must not be transferred into the network.

  Antivirus and anti-Trojan software must be installed and updated regularly, as well as software patches to fix known vulnerabilities. Moreover, awareness of security issues and prevention techniques must be increased among all Internet users. It is important to disable unnecessary services, uninstall unused applications, and scan all files received from external sources. Because these tasks may appear daunting to the average web user, the core hardware and software of computing systems come with integrated mechanisms that defend against malicious code insertion. Therefore, the built-in defensive mechanisms in the core hardware and software of the systems must be properly configured and regularly updated to avoid DDoS attacks. Employing the above countermeasures will leave attackers with no DDoS attack network through which they can launch DDoS attacks.

- **Network Service Providers**

  Service providers and network administrators can adopt dynamic pricing for their network usage to charge potential secondary victims for accessing the Internet and

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

thereby encourage them to become more active in preventing themselves from becoming a part of a DDoS attack.

Detect and Neutralize Handlers

An important method used to stop DDoS attacks is to detect and neutralize handlers. This can be achieved by network traffic analysis, neutralizing botnet handlers, and identifying spoofed source addresses. In the agent-handler DDoS attack-tool arsenal, the handler works as an intermediary for the attacker to initiate attacks. Analyzing communication protocols and traffic patterns between handlers and clients or handlers and agents can reveal the network nodes infected by the handlers. Discovering the handlers in the network and disabling them can be a quick method of disrupting the DDoS attack network. Because the number of DDoS handlers deployed in the network is much less than the number of agents, neutralizing a few handlers can possibly render multiple agents useless, thereby thwarting DDoS attacks.

Furthermore, there is a reasonable probability that the spoofed source address of DDoS attack packets will not represent a valid source address of the definite sub-network. Identifying spoofed source addresses will prevent DDoS attacks with thorough comprehension of communication protocols and traffic among handlers, clients, and agents.

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

Prevent Potential Attacks

Egress Filtering	Ingress Filtering	TCP Intercept	Rate Limiting
❑ Egress filtering scans the headers of IP packets leaving a network ❑ Egress filtering ensures that unauthorized or malicious traffic never leaves the internal network ❑ The packets will not reach the targeted address if they do not meet the necessary specifications	❑ Ingress filtering prevents the source address spoofing of Internet traffic ❑ It protects against flooding attacks originating from valid prefixes (IP addresses) ❑ It allows the originator to be traced to its true source	❑ TCP intercept features in routers protect TCP servers from TCP SYN-flooding attacks ❑ Configuring TCP Intercept features prevents DoS attacks by intercepting and validating TCP connection requests	❑ Rate limiting controls the rate of outbound or inbound traffic of a network interface controller ❑ It reduces the high-volume inbound traffic caused by DDoS attacks

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

Prevent Potential Attacks

- **Egress Filtering**

  Egress filtering scans the headers of IP packets leaving a network. If the packets meet specifications, they can be routed out of the sub-network from which they originated. On the other hand, the packets do not reach the targeted address if they fail to meet the necessary specifications. Egress filtering ensures that unauthorized or malicious traffic never leaves the internal network.

  DDoS attacks generate spoofed IP addresses. Establishing protocols to require any legitimate packet that leaves a company's network to have a source address in which the network portion matches the internal network can help mitigate attacks. A properly developed firewall for the sub-network can filter out many DDoS packets with spoofed IP source addresses.

  If a web server is vulnerable to a zero-day attack known only to the underground hacker community, a server can be vulnerable even after applying all available patches. However, if the user enables egress filtering, they can save the integrity of a system by keeping the server from establishing a connection back to the attacker. This would also limit the effectiveness of many payloads used in common exploits. Outbound exposure can be restricted to the required traffic, thereby limiting the attacker's ability to connect to other systems and gain access to tools that can enable further access into the network.

- **Ingress Filtering**

  Ingress filtering is a packet filtering technique used by many Internet Service Providers (ISPs) to prevent the source address spoofing of Internet traffic. Thus, ingress filtering

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

can indirectly combat several types of net abuse by making Internet traffic traceable to its true source. It protects against flooding attacks that originate from valid prefixes (IP addresses) and enables the originator to be traced to its true source.

- **TCP Intercept**

  TCP intercept is a traffic-filtering feature in routers to protect TCP servers from a TCP SYN-flooding attack, which is a kind of DoS attack. In a SYN-flooding attack, the attacker sends a huge volume of requests to connect with unreachable return addresses. As the addresses are not reachable, the connections cannot be established and remain unresolved. This huge volume of unresolved open connections overwhelms the server and may cause it to deny service even to valid requests. Consequently, legitimate users may not be able to connect to a website, access email, use an FTP service, and so on.

  In the TCP intercept mode, a router intercepts the SYN packets sent by clients to a server and matches them with an extended access list. If a match is obtained, then on behalf of the destination server, the intercept software establishes a connection with the client. Similarly, the intercept software also establishes a connection with the destination server on behalf of the client. Once the two half connections are established, the intercept software combines them transparently. Thus, the TCP intercept software prevents fake connection attempts from reaching the server by acting as a mediator between the server and client throughout the connection.

- **Rate limiting**

  Rate limiting is a technique used to control the rate of outbound or inbound traffic of a network interface controller. This technique effectively reduces the high volume of inbound traffic that causes a DDoS attack. It is especially important to employ this technique in hardware appliances, in which the technique is configured to limit the rate of requests on layers 4 and 5 of the Open Systems Interconnection (OSI) model.

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

Deflect Attacks

- Systems that are set up with limited security, also known as Honeypots, act as an enticement for an attacker
- Honeypots serve as a means of gaining information about attackers, attack techniques, and tools by storing a record of the system activities
- The defense-in-depth approach is used with IPSes at different network points to divert suspicious DoS traffic to several honeypots

KFSensor | KFSensor acts as a honeypot, designed to attract and detect hackers and worms by simulating vulnerable system services and Trojans

http://www.keyfocus.net

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

Deflect Attacks

Systems set up with limited security, also known as honeypots, act as enticement for an attacker. Recent research reveals that a honeypot can imitate all aspects of a network, including its web servers, mail servers, and clients. Honeypots are intentionally set up with low security to gain the attention of DDoS attackers and serve as a means for gaining information about attackers, attack techniques, and tools by storing a record of the system activities. DDoS attackers attracted by a honeypot install handlers or agent code within the honeypot. This avoids compromising systems that are more sensitive. Honeypots not only protect the actual system from attackers but also keep track of details on the attackers' activities by recording the activity information. Consequently, the honeypot owner can keep a record of the handler and/or agent activity. Users can employ this knowledge to defend against any future DDoS installation attacks. A defense-in-depth approach with Internet Protocol Security (IPSec) can be used at different network points to divert suspicious DoS traffic to several honeypots.

There are two different types of honeypots:

- Low-interaction honeypots
- High-interaction honeypots

An example for high-interaction honeypots is a honeynet. Honeynets form the security infrastructure; in other words, they simulate the complete layout of a network of computers but are originally intended for "capturing" attacks. The goal is to develop a network wherein all activities are controlled and tracked. This network contains potential victim decoys, and the network even has real computers running real applications.

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

- **KFSensor**

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

  KFSensor is a Windows-based honeypot intrusion detection system (IDS). It acts as a honeypot designed to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By responding with an emulation of a real service, KFSensor can reveal the nature of an attack while maintaining total control and avoiding the risk of compromise. By acting as a decoy server, it can divert attacks from critical systems and provide a higher level of information than can be achieved using firewalls and a network IDS (NIDS) alone.

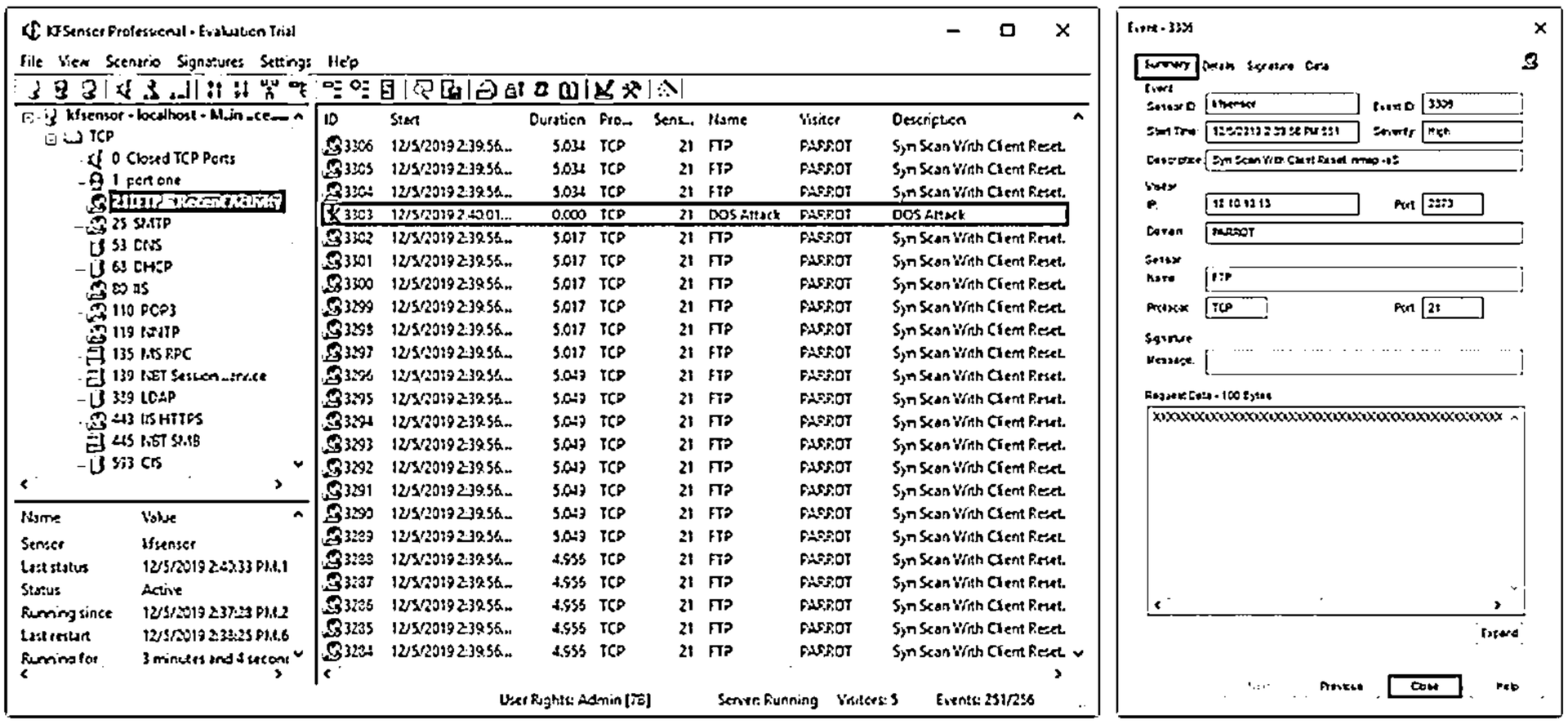


Figure 10.33: Screenshot of KFSensor

The following are examples for additional DoS/DDoS countermeasure (honeypot) tools:

- SSHHiPot (*https://github.com*)
- Artillery (*https://github.com*)

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

Mitigate Attacks

Load Balancing

- Increase bandwidth on critical connections to absorb additional traffic generated by an attack
- Replicate servers to provide additional failsafe protection
- Balance loads on each server in a multiple-server architecture to mitigate DDoS attacks

Throttling

- Set routers to access a server with a logic that throttles incoming traffic levels to be safe for the server
- Throttling helps in preventing damage to servers by controlling DoS traffic
- This method helps routers manage heavy incoming traffic, so that the server can handle it
- It filters legitimate user traffic from fake DDoS attack traffic

Drop Requests

- In this technique, servers and routers drop packets when load increases
- System causes requester to drop the request by making it to solve a difficult puzzle that requires a lot of memory or computing power before it can continue with the request

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

Mitigate Attacks

- **Load Balancing**

  Bandwidth providers can increase bandwidth on critical connections in case of a DDoS attack to prevent their servers from shutting down. Using a replicated server model provides additional failsafe protection. Replicated servers help in better load management by balancing loads on each server in a multiple-server architecture; they also increase normal network performance and mitigate the effect of a DDoS attack.

- **Throttling**

  Throttling entails the setting up of routers for server access with a logic to throttle incoming traffic levels that are safe for the server. "Min-max fair server-centric router" throttles (minimum and maximum throughput controls) help users prevent their servers from shutting down. Throttling helps in preventing damage to servers by controlling the DoS traffic. This method helps routers manage heavy incoming traffic so that the server can handle it. It also filters legitimate user traffic from fake DDoS attack traffic and can be extended to throttle DDoS attack traffic while allowing legitimate user traffic for better results.

  A major limitation of this method is that it may trigger false alarms. Occasionally, it may allow malicious traffic to pass through while dropping some legitimate traffic.

- **Drop Requests**

  Another method is to drop packets when the load increases. Usually, the router or server performs this task. However, before continuing with a request, the system induces the requester to drop the request by making them solve a difficult puzzle that requires a lot of memory or computing power. Consequently, users of zombie systems

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

detect a performance degradation and could possibly be dissuaded from taking part in transferring DDoS attack traffic.

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

Post-Attack Forensics

Traffic Pattern Analysis	⊖ Traffic pattern analysis can help network administrators to develop new filtering techniques for preventing attack traffic from entering or leaving their networks ⊖ The output of traffic pattern analysis helps in updating load balancing and throttling countermeasures to enhance efficiency and protection ability
Packet Traceback	⊖ Packet Traceback is similar to reverse engineering ⊖ It helps in identifying the true source of attack and taking necessary steps to block further attacks
Event Log Analysis	⊖ Event log analysis helps in identifying the source of DoS traffic ⊖ This allows network administrators to recognize the type of DDoS attack or a combination of attacks used

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

Post-Attack Forensics

- **Traffic Pattern Analysis**

  During a DDoS attack, the traffic pattern tool stores post-attack data, which users analyze to identify characteristics unique to the attacking traffic. These data are helpful in updating load balancing and throttling countermeasures to enhance their efficiency and protection ability. Moreover, DDoS attack traffic patterns can help network administrators develop new filtering techniques to prevent DDoS attack traffic from entering or leaving their networks. Analyzing DDoS traffic patterns can also help network administrators ensure that an attacker cannot use their servers as a DDoS platform to break into other sites.

- **Zombie Zapper Tool**

  When a company is unable to ensure the security of its servers and a DDoS attack starts, the network IDS notices the high volume of traffic, which indicates a potential problem. The targeted victim can run Zombie Zapper to stop packets from flooding the system.

  There are two versions of Zombie Zapper: one runs on UNIX, while the other runs on Windows. Currently, this tool acts as a defense mechanism against Trinoo, Tribe Flood Network (TFN), Shaft, and Stacheldraht.

- **Packet Traceback**

  Packet traceback refers to tracing back attack traffic. It is similar to reverse engineering. In this method, the targeted victim works backward by tracing the packet to its source. Once the victim identifies the true source, they can take steps to block further attacks from that source by developing the necessary preventive techniques. In addition, packet traceback can assist in gaining knowledge of the various tools and techniques that an

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

attacker uses. This information can help in developing and implementing different filtering techniques to block attacks.

- **Event Log Analysis**

  DDoS event logs assist in forensic investigation and the enforcement of laws, which are helpful when an attacker causes severe financial damage. Providers can use honeypots and other network security mechanisms such as firewalls, packet sniffers, and server logs to store all the events that occurred during the setup and execution of the attack. This allows network administrators to recognize the type of DDoS attack or the combination of attacks used. Routers, firewalls, and IDS logs can be analyzed to identify the source of the DoS traffic. Further, network administrators can attempt to trace back the attacker's IP address with the help of intermediary ISPs and law enforcement agencies.

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

Techniques to Defend against Botnets

RFC 3704 Filtering	Cisco IPS Source IP Reputation Filtering	Black Hole Filtering	DDoS Prevention Offerings from ISP or DDoS Service
❑ RFC 3704 filtering limits the impact of DDoS attacks by denying traffic with spoofed addresses ❑ Any traffic coming from unused or reserved IP addresses is bogus and should be filtered at the ISP before it enters the Internet link	❑ Reputation services help in determining if an IP or service is a source of threat ❑ Cisco IPS regularly updates its database with known threats such as botnets, botnet harvesters, and malwares, and helps in filtering DoS traffic	❑ A "black hole" refers to a network node where incoming traffic is discarded or dropped without informing the source that the data did not reach its intended recipient ❑ Black hole filtering refers to discarding packets at the routing level	❑ Enable IP Source Guard (in CISCO) or similar features in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings, preventing a bot from succeeding with spoofed packets

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

Techniques to Defend against Botnets

There are four techniques to defend against botnets:

- **RFC 3704 Filtering**

  RFC 3704 is a basic access-control list (ACL) filter, which limits the impact of DDoS attacks by blocking traffic with spoofed addresses. This filter requires packets sourced from valid, allocated address space that is consistent with the topology and space allocation. A "bogon list" consists of all unused or reserved IP addresses that should not come from the Internet. If a packet is sourced from any of the IP addresses from the bogon list, then the packet is from a spoofed source IP, and the filter should drop it. System administrators should check whether the ISP performs RFC 3704 filtering in the cloud before traffic enters the system. Because the bogon list changes regularly, in case the ISP does not perform RFC 3704 filtering, the system administrator must manage their own bogon ACL rules or switch to another ISP.

- **Cisco IPS Source IP Reputation Filtering**

  Reputation services help in determining whether an IP or service is a source of threat. Cisco Global Correlation, a new security capability of Cisco IPS 7.0, uses immense security intelligence. The Cisco SensorBase Network contains information about all known threats on the Internet, such as botnets, malware outbreaks, dark nets, and botnet harvesters. The Cisco IPS makes use of this network to filter DoS traffic before it damages critical assets. To detect and prevent malicious activity even earlier, it incorporates global threat data into its system.

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

- **Black Hole Filtering**

  Black-hole filtering is a common technique to defend against botnets and, thus, to prevent DoS attacks. Black holes refer to network nodes wherein incoming traffic is discarded or dropped without informing the source that the data did not reach the intended recipient. Undesirable traffic can be dropped before it enters a protected network with a technique called remotely triggered black-hole (RTBH) filtering. As this is a remotely triggered process, this filtering must be performed in conjunction with the ISP. It uses Border Gateway Protocol (BGP) host routes to route traffic to the victim's servers to a "null0" next hop.

- **DDoS Prevention Offerings from ISP or DDoS Service**

  This method is effective in preventing IP spoofing at the ISP level. Here, the ISP scrubs/cleans traffic before allowing it to enter a user's Internet link. Because this service runs in the cloud, DDoS attacks do not saturate the Internet links. In addition, some third parties offer cloud DDoS prevention services.

  IP Source Guard (in CISCO) or similar features can be enabled in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings, which prevent bots from sending spoofed packets.

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

Additional DoS/DDoS Countermeasures

1. Use strong encryption mechanisms such as WPA2 or AES 256 for broadband networks to protect against eavesdropping
2. Ensure that the software and protocols are up-to-date, and scan the machines thoroughly to detect any anomalous behavior
3. Disable unused and unsecure services
4. Block all inbound packets originating from service ports to block the traffic from reflection servers
5. Update each kernel to its latest release
6. Prevent the transmission of fraudulently addressed packets at the ISP level
7. Implement cognitive radios in the physical layer to handle jamming and scrambling attacks
8. Configure the firewall to deny external ICMP traffic access
9. Secure any remote administration and connectivity testing
10. Perform thorough input validation
11. Prevent the use of unnecessary functions such as gets, and strcpy
12. Prevent return addresses from being overwritten

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

Additional DoS/DDoS Countermeasures

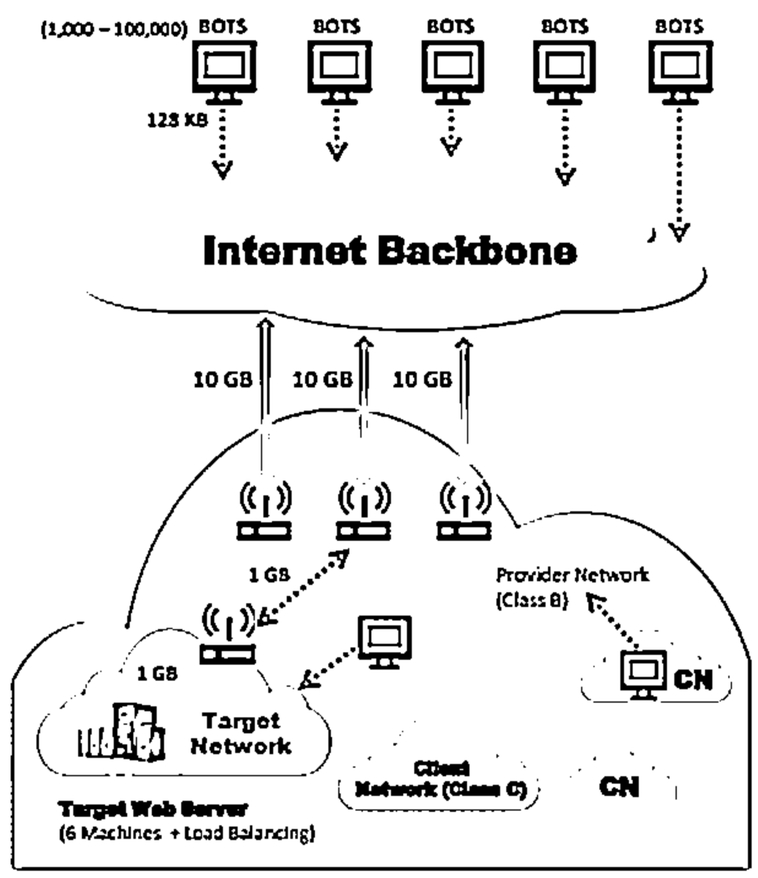
Implementing defensive mechanisms at proper places by following proper measures allows the heightening of organizational network security. The following is a list of countermeasures for combating DoS/DDoS attacks:

- Use strong encryption mechanisms such as WPA2 and AES 256 for broadband networks to defend against eavesdropping
- Ensure that the software and protocols are up-to-date and scan the machines thoroughly to detect any anomalous behavior
- Update the kernel to the latest release and disable unused and insecure services
- Block all inbound packets originating from the service ports to block the traffic from reflection servers
- Enable TCP SYN cookie protection
- Prevent the transmission of fraudulently addressed packets at the ISP level
- Implement cognitive radios in the physical layer to handle jamming and scrambling attacks
- Configure the firewall to deny external ICMP traffic access
- Secure remote administration and connectivity testing
- Perform thorough input validation
- Stop data processed by the attacker from being executed
- Prevent the use of unnecessary functions such as gets and strcpy
- Prevent the return addresses from being overwritten

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

DoS/DDoS Protection at ISP Level

1. Most ISPs simply block all requests during a DDoS attack, denying even the legitimate traffic from accessing the service
2. ISPs offer in-the-cloud DDoS protection for Internet links so that they do not become saturated by the attack
3. In-the-cloud DDoS protection redirects attack traffic to the ISP during the attack and sends it back
4. Administrators can request ISPs to block the original affected IP and move their site to another IP after performing DNS propagation



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

DoS/DDoS Protection at ISP Level

One of the best ways to defend against DoS attacks is to block them at the gateway. This task is performed by the contracted ISP. ISPs offer a "clean pipes" service-level agreement that provides an assured bandwidth of genuine traffic, rather than the total bandwidth of all traffic. Most ISPs simply block all requests during a DDoS attack, denying even legitimate traffic from accessing the service. If an ISP does not provide clean-pipes services, subscription services provided by many cloud service providers can be used. The subscription services serve as an intermediary, receive traffic destined for the network, filter it, and then pass on only trusted connections. Vendors such as Imperva and VeriSign offer services for cloud protection against DoS attacks.

ISPs offer in-the-cloud DDoS protection for Internet links to avoid saturation due to an attack. This type of protection redirects attack traffic to the ISP during an attack. Administrators can request ISPs to block the original affected IP and move their site to another IP after performing DNS propagation.

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

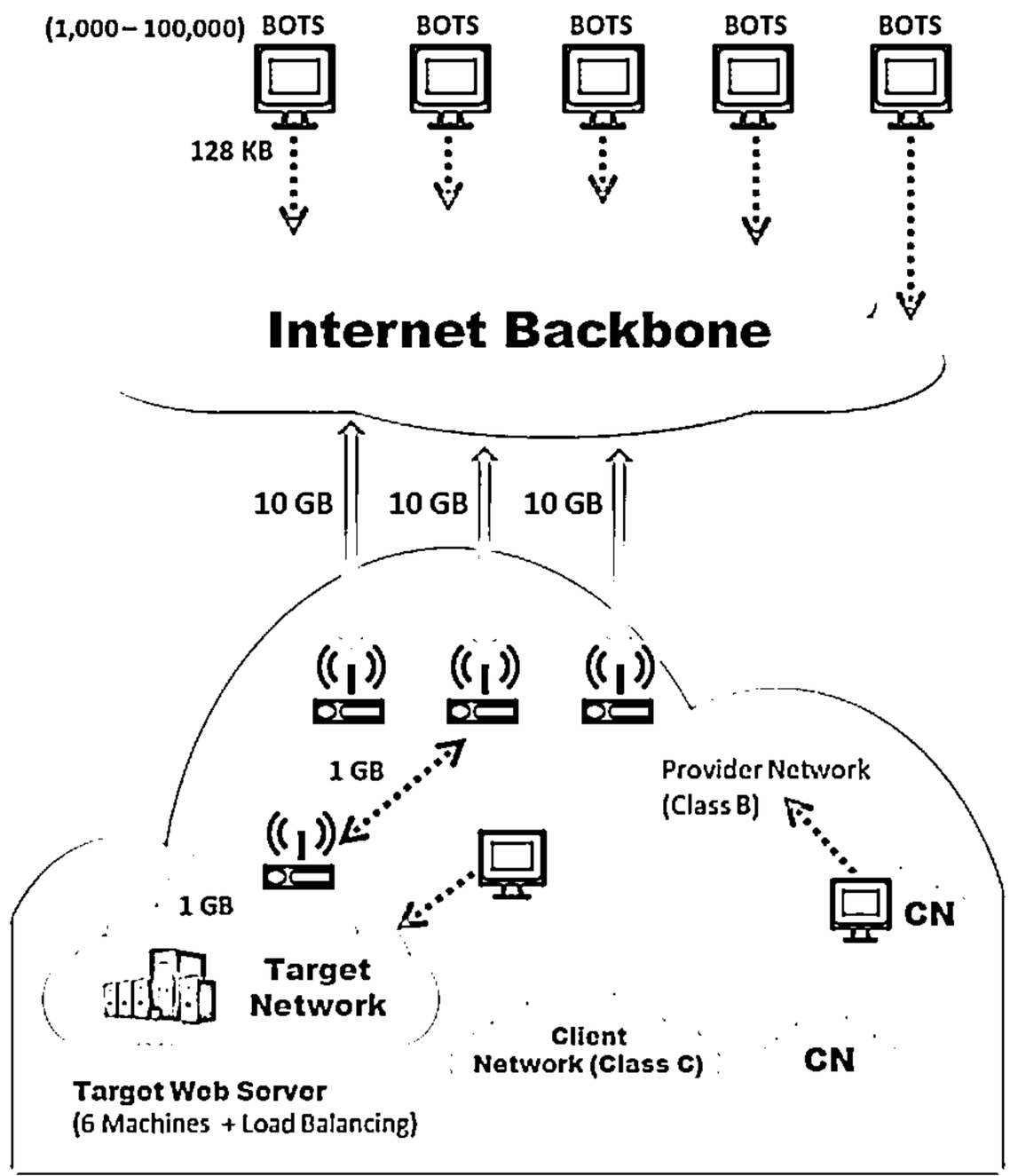


Figure 10.34: DoS/DDoS protection at the ISP level

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

Enabling TCP Intercept on Cisco IOS Software

- To enable TCP Intercept on CISCO IOS, use these commands in the global configuration mode:

Step	Command	Purpose
1	access-list access-list-number {deny | permit} tcp any destination destination-wildcard	Define an IP extended access list
2	ip tcp Intercept list *access-list-number*	Enable TCP Intercept

- TCP intercept can operate in either the active intercept mode or the passive watch mode. The default is the intercept mode
- The command to set the TCP Intercept mode in the global configuration is as follows:

Command	Purpose
ip tcp intercept mode {intercept | watch}	Set the TCP intercept mode

https://www.cisco.com

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

Enabling TCP Intercept on Cisco IOS Software

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

TCP intercept can be enabled by executing the commands given in the below table in the global configuration mode.

Step	Command	Purpose
1	`access-list access-list-number {deny | permit} tcp any destination destination-wildcard`	Defines an IP extended access list
2	`ip tcp intercept list access-list-number`	Enables TCP intercept

Table 10.1: Steps to enable TCP intercept on Cisco IOS

An access list achieves three purposes:

1. Interception of all requests
2. Interception of only requests originating from specific networks
3. Interception of only requests destined for specific servers

Typically, an access list defines the source as any source and the destination as specific networks or servers. As it is unimportant to know who to intercept packets from, the source addresses are not filtered. Rather, the destination server or network to be protected is identified. TCP intercept can operate in either the active intercept mode or passive watch mode. The default is the intercept mode.

In the active intercept mode, the Cisco IOS software actively intercepts all inbound connection requests (SYN) and replies with a SYN-ACK on behalf of the server, following which it waits for

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

an acknowledge (ACK) from the client. On receiving the ACK from the client, the server sends the original SYN, and the software makes a three-way handshake with the server. Once the three-way handshake is complete, the two half connections are linked.

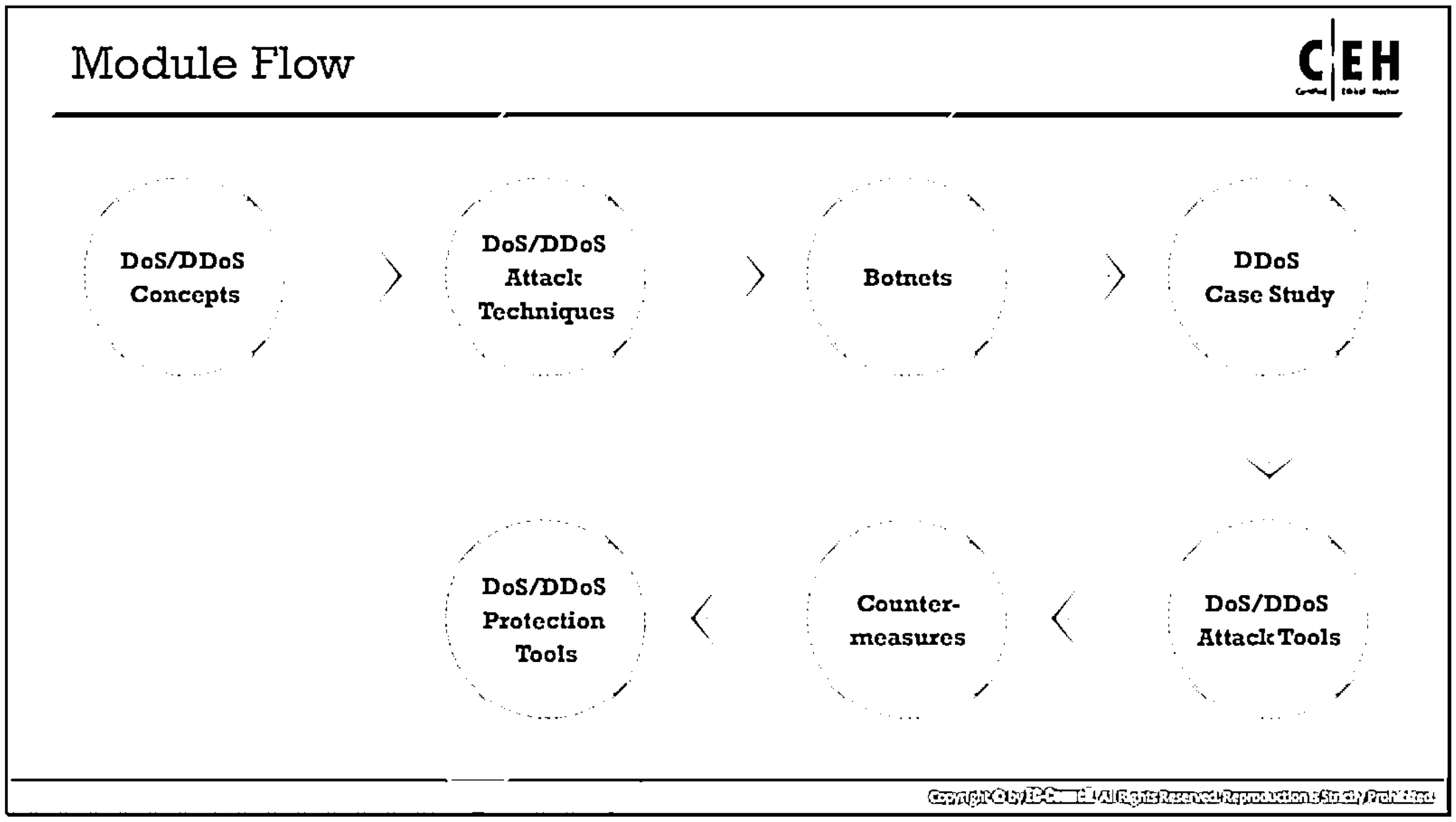
In the passive watch mode, the user sends connection requests that pass through the server, but they need to wait until the connection is established. If connection requests fail to establish within 30 s, the software sends a reset request to the server to clear its state.

Below table presents the command to set the TCP intercept mode in the global configuration mode.

Command	Purpose
`ip tcp intercept mode {intercept | watch}`	Set the TCP intercept mode

Table 10.2: Command to set the TCP intercept mode in the global configuration mode

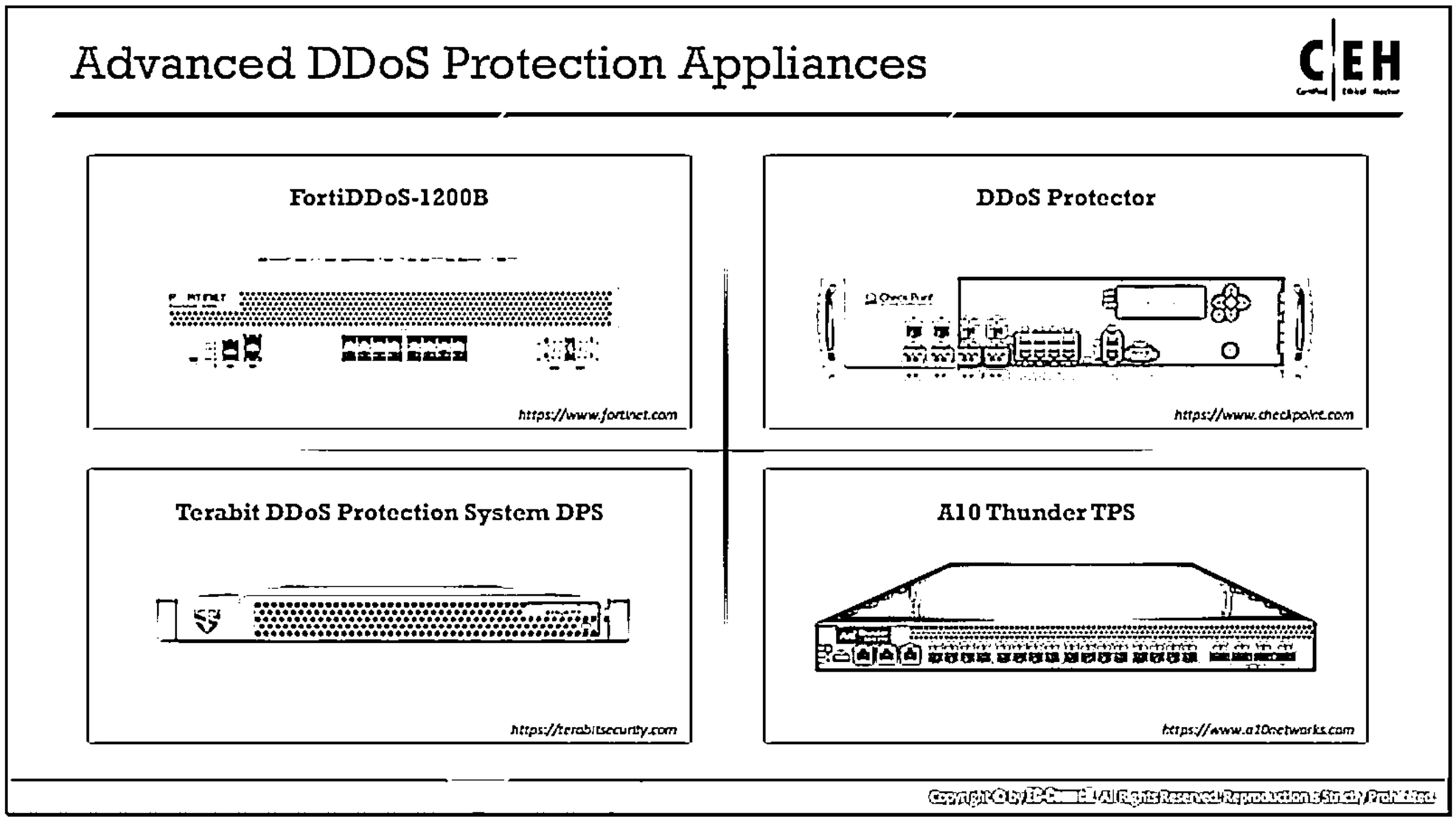
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



DoS/DDoS Protection Tools

This section discusses various hardware and software DoS/DDoS protection tools such as FortiDDoS, DDoS Protector, Imperva Incapsula, and Anti DDoS Guardian that are effective in safeguarding networks from DoS/DDoS attacks.

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



Advanced DDoS Protection Appliances

The following are examples for appliances that provide advanced protection against DDoS attacks.

- **FortiDDoS-1200B**

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

  FortiDDoS provides comprehensive protection against DDoS attacks. It helps protect Internet infrastructure from threats and service disruptions by surgically removing network and application layer DDoS attacks while letting legitimate traffic flow without being impacted.

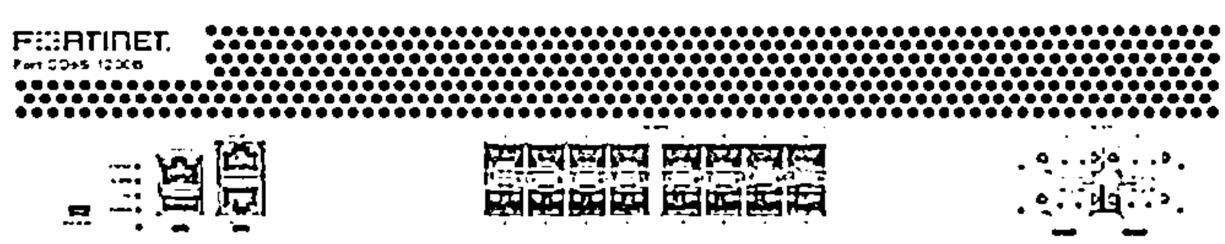


Figure 10.35: FortiDDoS-1200B

- **DDoS Protector**

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

  Check Point DDoS Protector blocks DDoS attacks with multi-layered protection. Its advantages are listed as follows:

  - Blocks a wide range of attacks with customized multi-layered protection

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

- Behavioral protection base-lining multiple elements and blocking abnormal traffic
- Automatically generated and predefined signatures
- Use of advanced challenge/response techniques

- Fast response time to protect against attacks within seconds
  - Automatically defends against network flood and application layer attacks
  - Customized protection optimized to meet the security needs of a specific network environment
  - Quic kly filters traffic before it reaches the firewall to protect networks and servers as well as block exploits
- Flexible deployment options to protect any business
- Integrated with Check Point Security Management

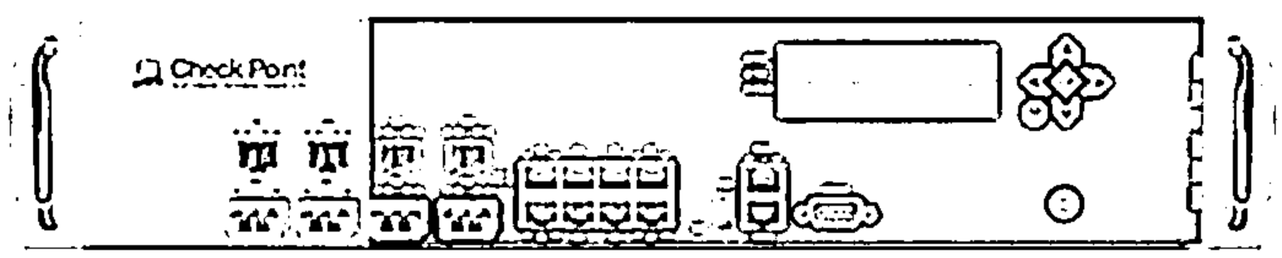


Figure 10.36: DDoS Protector

- **Terabit DDoS Protection System**

  Source: *https://terabitsecurity.com*

  Terabit DDoS Protection System (DPS) is a solution for the detection and subsequent treatment of DDoS attacks. Terabit DPS helps ensure the maximum availability of a network and eliminates any disruptions caused by DoS/DDoS attacks. It can be used for large networks of bandwidth up to 1 Tbps. It can also provide protection for bandwidth up to 6.4 Tbps.

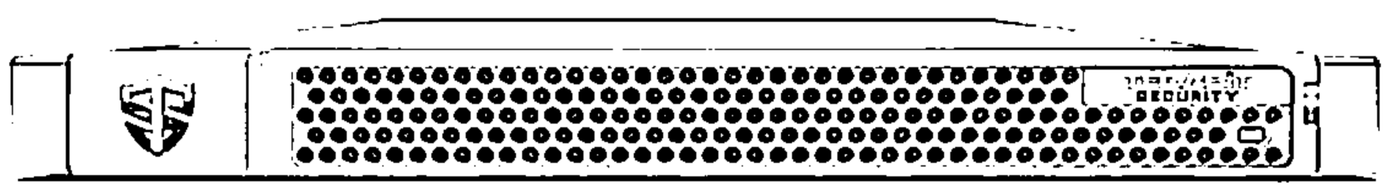


Figure 10.37: Terabit DPS appliance

- **A10 Thunder TPS**

  Source: *https://www.a10networks.com*

  A10 Thunder Threat Protection System (TPS) ensures reliable access to key network services by detecting and blocking external threats such as DDoS and other cyber-attacks before they escalate into costly service outages. Its features are listed as follows:

  - Custom protection with immediate blocking

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

- Proactive DDoS detection and mitigation
- Combined on-premises and cloud-based DDoS protection
- Built-in SSL inspection to block encrypted traffic
- Inbound reputation-based DDoS protection
- Inbound and outbound advanced threat protection

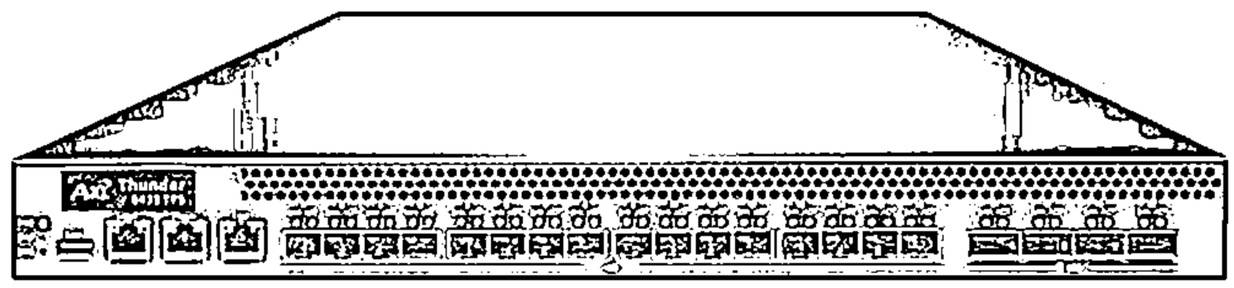
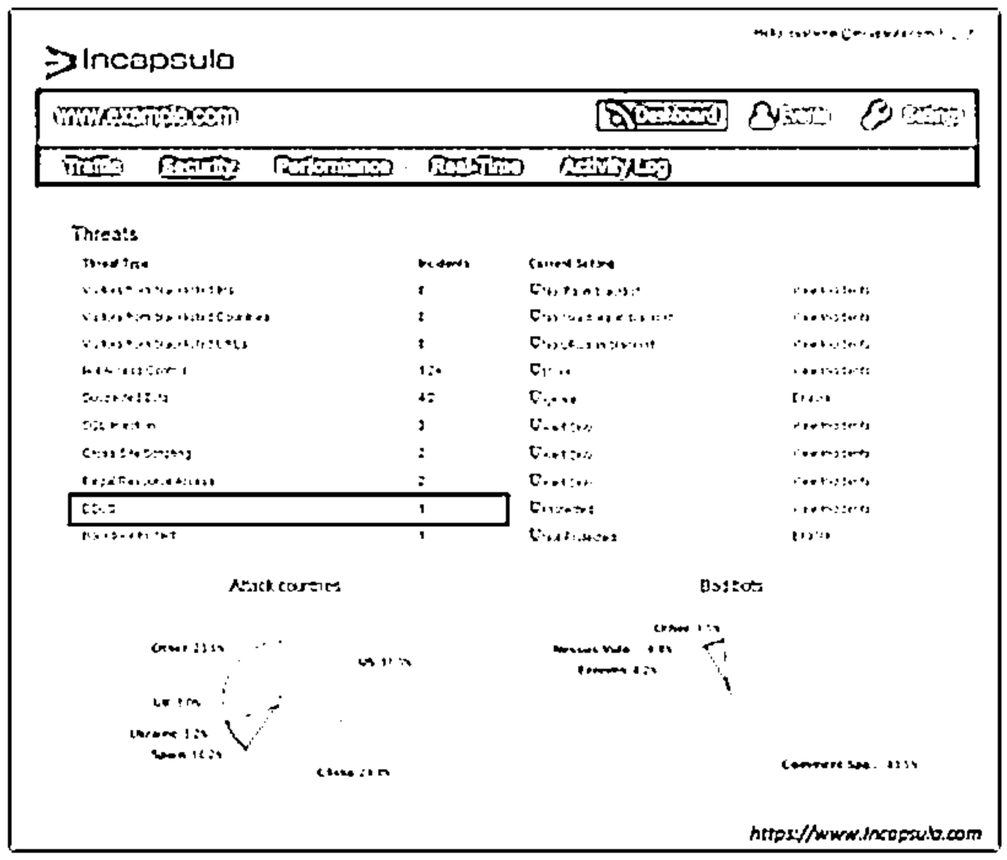


Figure 10.38: A10 Thunder TPS

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

DoS/DDoS Protection Tools



Imperva Incapsula DDoS Protection

Imperva Incapsula DDoS protection quickly mitigates attacks of any size without affecting legitimate traffic or increasing latency

DoS/DDoS Protection Tools

- Anti DDoS Guardian (*http://www.beethink.com*)
- DOSarrest's DDoS protection service (*https://www.dosarrest.com*)
- DDoS-GUARD (*https://ddos-guard.net*)
- Cloudflare (*https://www.cloudflare.com*)
- F5 (*https://f5.com*)

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

DoS/DDoS Protection Tools

- **Imperva Incapsula DDoS Protection**

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

  Imperva Incapsula DDoS protection quickly mitigates any size attack without disrupting legitimate traffic or increasing latency. It is designed to provide multiple DDoS protection options and supports unicast and anycast technologies to power a many-to-many defense methodology. It automatically detects and mitigates attacks exploiting application and server vulnerabilities, hit-and-run events, and large botnets.

  Incapsula proxies all web requests to block DDoS attacks from being relayed to client origin servers. Incapsula detects and mitigates any type of attack, including TCP SYN + ACK, TCP FIN, TCP RESET, TCP ACK, TCP ACK + PSH, TCP fragmentation, UDP, Slowloris, spoofing, ICMP, IGMP, HTTP flood, brute force, connection flood, DNS flood, NXDomain, mixed SYN + UDP or ICMP + UDP flood, ping of death, reflected ICMP & UDP, and Smurf.

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

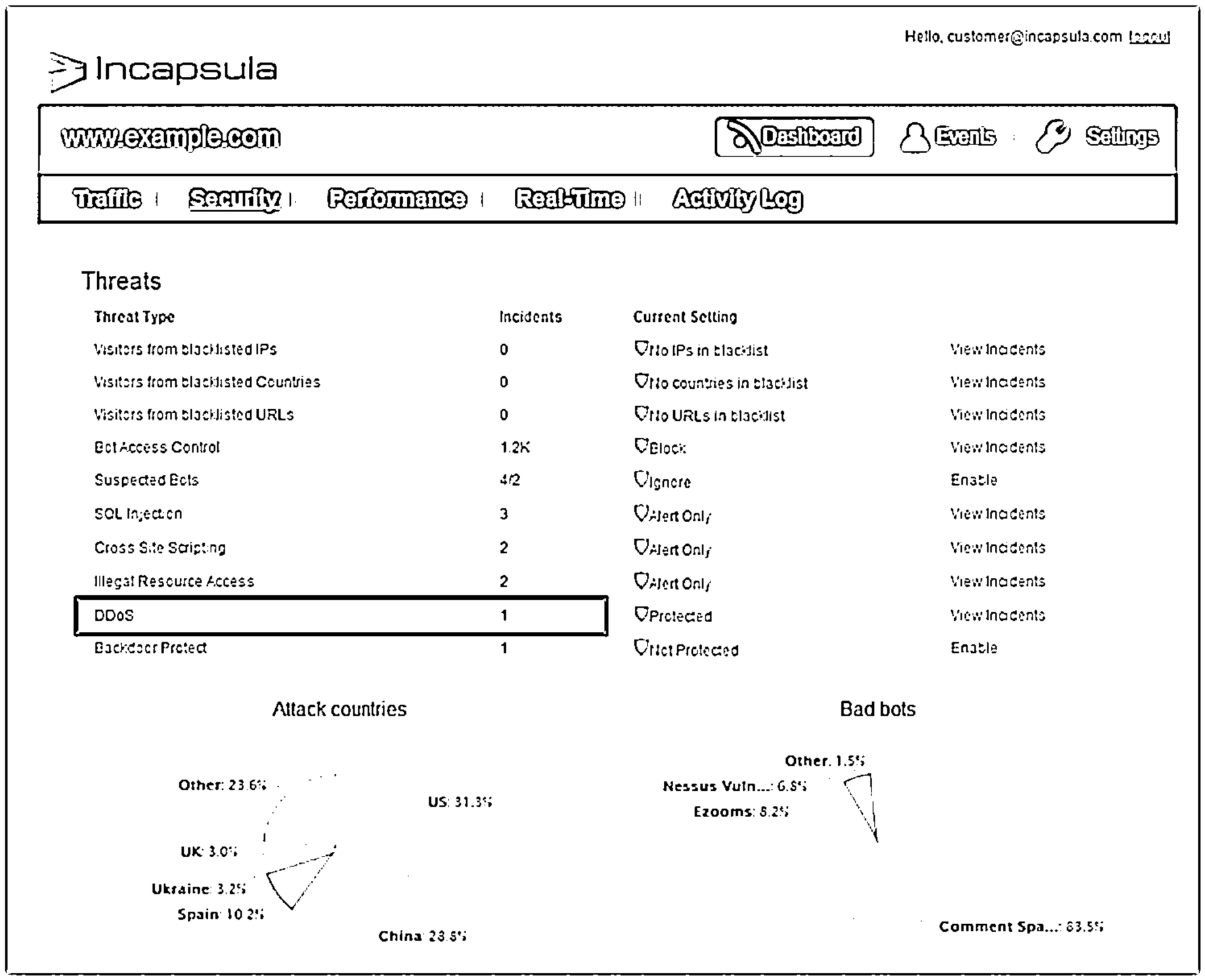


Figure 10.39: Screenshot of Incapsula DDoS protection tool

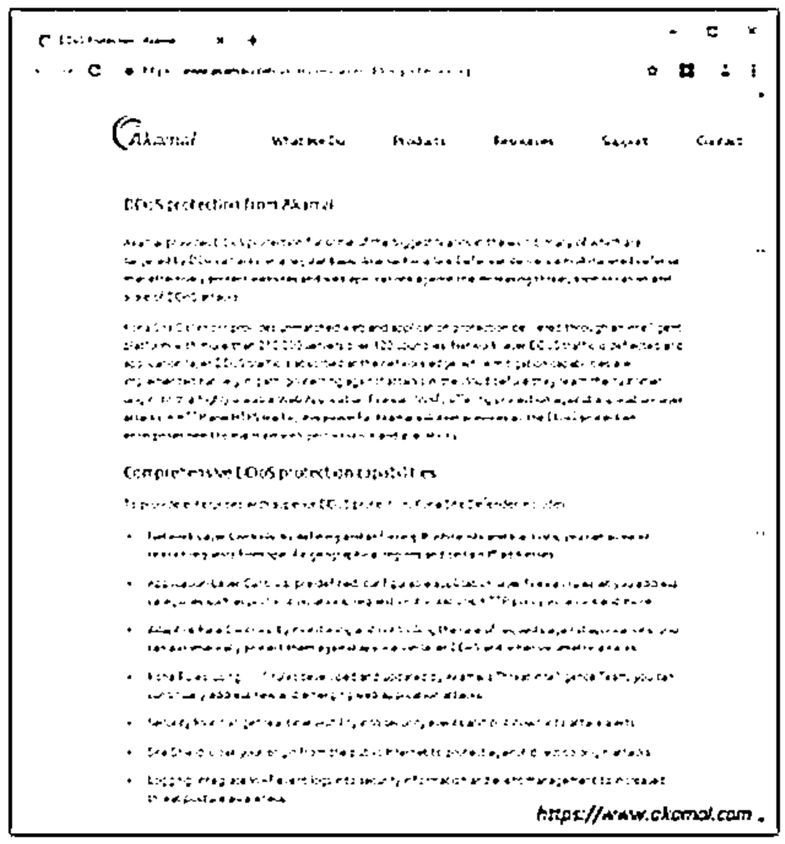
The following are examples for additional DDoS protection tools:

- Anti DDoS Guardian (*http://www.beethink.com*)
- DOSarrest's DDoS protection service (*https://www.dosarrest.com*)
- DDoS-GUARD (*https://ddos-guard.net*)
- Cloudflare (https://www.cloudflare.com)
- F5 (*https://f5.com*)

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

DoS/DDoS Protection Services

Akamai DDoS Protection



Kaspersky DDoS Protection Tool
https://www.kaspersky.com

Stormwall PRO
https://stormwall.pro

Corero Network Security
https://www.corero.com

Nexusguard
https://www.nexusguard.com

BlockDoS
https://www.blockdos.net

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

DoS/DDoS Protection Services

- **Akamai DDoS Protection**

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

  Akamai provides DDoS protection for enterprises regularly targeted by DDoS attacks. Akamai Kona Site Defender delivers multi-layered defense that effectively protects websites and web applications against the increasing threat, sophistication, and scale of DDoS attacks.

  Kona Site Defender provides unmatched web and application protection, which is delivered through an intelligent platform with more than 210,000 servers over 120 countries. Network-layer DDoS traffic is deflected and application layer DDoS traffic is absorbed in the network edge, while mitigation capabilities are implemented natively in-path, protecting against attacks in the cloud before they reach the client origin. Kona Site Defender has a highly scalable web application firewall (WAF) offering protection against application layer attacks in HTTP and HTTPS traffic, providing a complete DDoS protection solution for enterprises to maintain web performance and availability.

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

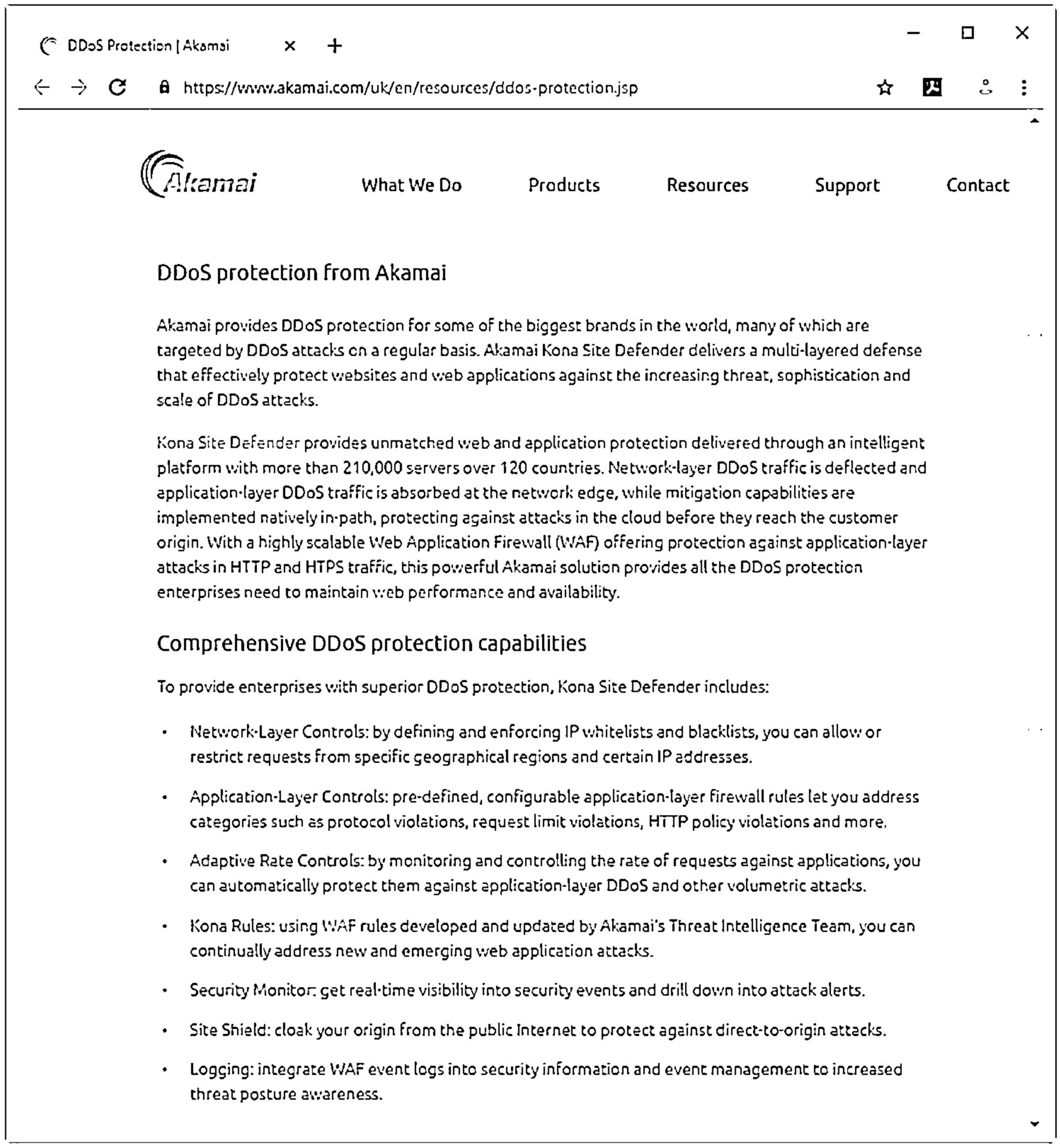


Figure 10.40: Akamai DDoS protection service

The following are examples for additional DDoS protection services:

- Kaspersky DDoS Protection Tool (*https://www.kaspersky.com*)
- Stormwall PRO (*https://stormwall.pro*)
- Corero Network Security (*https://www.corero.com*)
- Nexusguard (*https://www.nexusguard.com*)
- BlockDoS (*https://www.blockdos.net*)

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:
  - Concepts of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks
  - Various types of DoS/DDoS attacks
  - Concepts of botnets along with the botnet ecosystem
  - DDoS case study in detail, namely, the DDoS Attack on GitHub
  - Various DoS/DDoS attack tools
  - We concluded with a detailed discussion on various countermeasures that are to be employed to prevent DoS/DDoS attacks along with various hardware and software DoS/DDoS protection tools
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform session hijacking to steal a valid session ID

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

Module Summary

In this module, we discussed concepts related to denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. We also discussed various types of DoS/DDoS attacks. Additionally, this module discussed concepts related to botnets along with the botnet ecosystem. Further, a detailed case study of a DDoS attack on GitHub was presented. Moreover, this module illustrated various DoS/DDoS attack tools and concluded with a detailed discussion on various countermeasures to prevent DoS/DDoS attacks, along with various hardware and software DoS/DDoS protection tools.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform session hijacking to steal a valid session ID.

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

C|EH™

Certified Ethical Hacker

Module 11: Session Hijacking

Module Objectives

- Understanding Session Hijacking Concepts
- Understanding Application Level Session Hijacking
- Understanding Network Level Session Hijacking
- Overview of Session Hijacking Tools
- Understanding Different Session Hijacking Countermeasures

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

Module Objectives

Session hijacking allows attackers to take over an active session by bypassing the authentication process. Thereafter, they can perform any action on the hijacked system.

This module aims to provide comprehensive information on session hijacking. It starts with an introduction to session hijacking concepts and provides insight into session hijacking at the application and network levels. Later, the module discusses tools used to hijack a session between a client and server. It also discusses various countermeasures to defend against session hijacking attacks.

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

- Describe session hijacking concepts
- Perform application level session hijacking
- Perform network level session hijacking
- Use different session hijacking tools
- Apply session hijacking countermeasures

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

Module Flow

01	Session Hijacking Concepts	03	Network Level Session Hijacking
02	Application Level Session Hijacking	04	Session Hijacking Tools
05	Countermeasures		

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

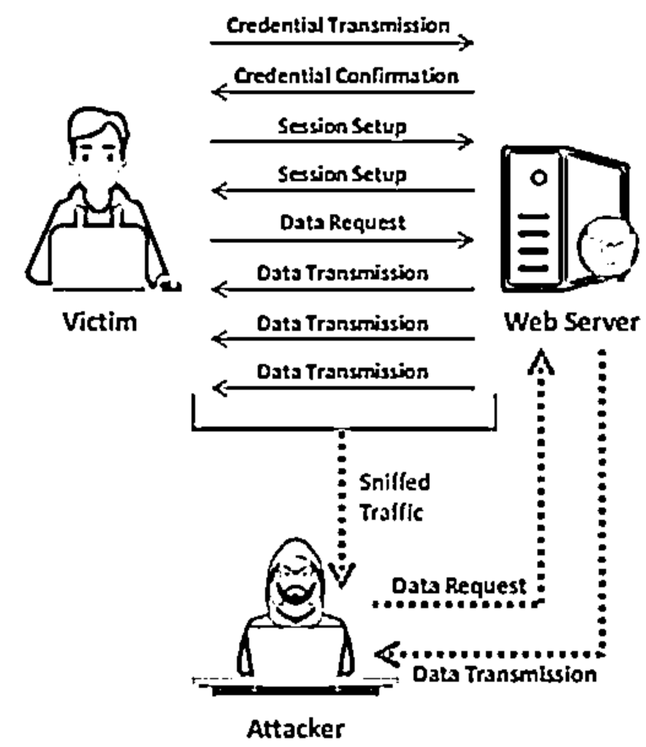
Session Hijacking Concepts

Familiarization with basic concepts related to session hijacking is important to attain a comprehensive understanding. This section explains what session hijacking is as well as the reasons why session hijacking succeeds. It also discusses the session hijacking process, packet analysis of a local session hijack, types of session hijacking, session hijacking in an Open Systems Interconnection (OSI) model, and differences between spoofing and hijacking.

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

What is Session Hijacking?

- Session hijacking refers to an attack in which an attacker seizes control of a valid TCP communication session between two computers
- As most authentications only occur at the start of a TCP session, this allows the attacker to gain access to a machine
- Attackers can sniff all the traffic from the established TCP sessions and perform identity theft, information theft, fraud, etc.
- The attacker steals a valid session ID and uses it to authenticate himself with the server



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

What is Session Hijacking?

A web server sends a session identification token or key to a web client after successful authentication. These session tokens differentiate multiple sessions that the server establishes with clients. Web servers use various mechanisms to generate random tokens and controls to secure the tokens during transmission.

Session hijacking is an attack in which an attacker takes over a valid Transmission Control Protocol (TCP) communication session between two computers. Because most types of authentication are performed only at the start of a TCP session, an attacker can gain access to a machine while a session is in progress. Attackers can sniff all the traffic from established TCP sessions and perform identity theft, information theft, fraud, etc.

A session hijacking attack exploits a session-token generation mechanism or token security controls so that the attacker can establish an unauthorized connection with a target server. The attacker can guess or steal a valid session ID, which identifies authenticated users, and use it to establish a session with the server. The web server responds to the attacker's requests under the impression that it is communicating with an authenticated user.

Attackers can use session hijacking to launch various kinds of attacks, such as man-in-the-middle (MITM) and denial-of-service (DoS) attacks. In an MITM attack, an attacker places themselves between an authorized client and a server by performing session hijacking to ensure that information flowing in either direction passes through them. However, the client and server believe they are directly communicating with each other. Attackers can also sniff sensitive information and disrupt sessions to launch a DoS attack.

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

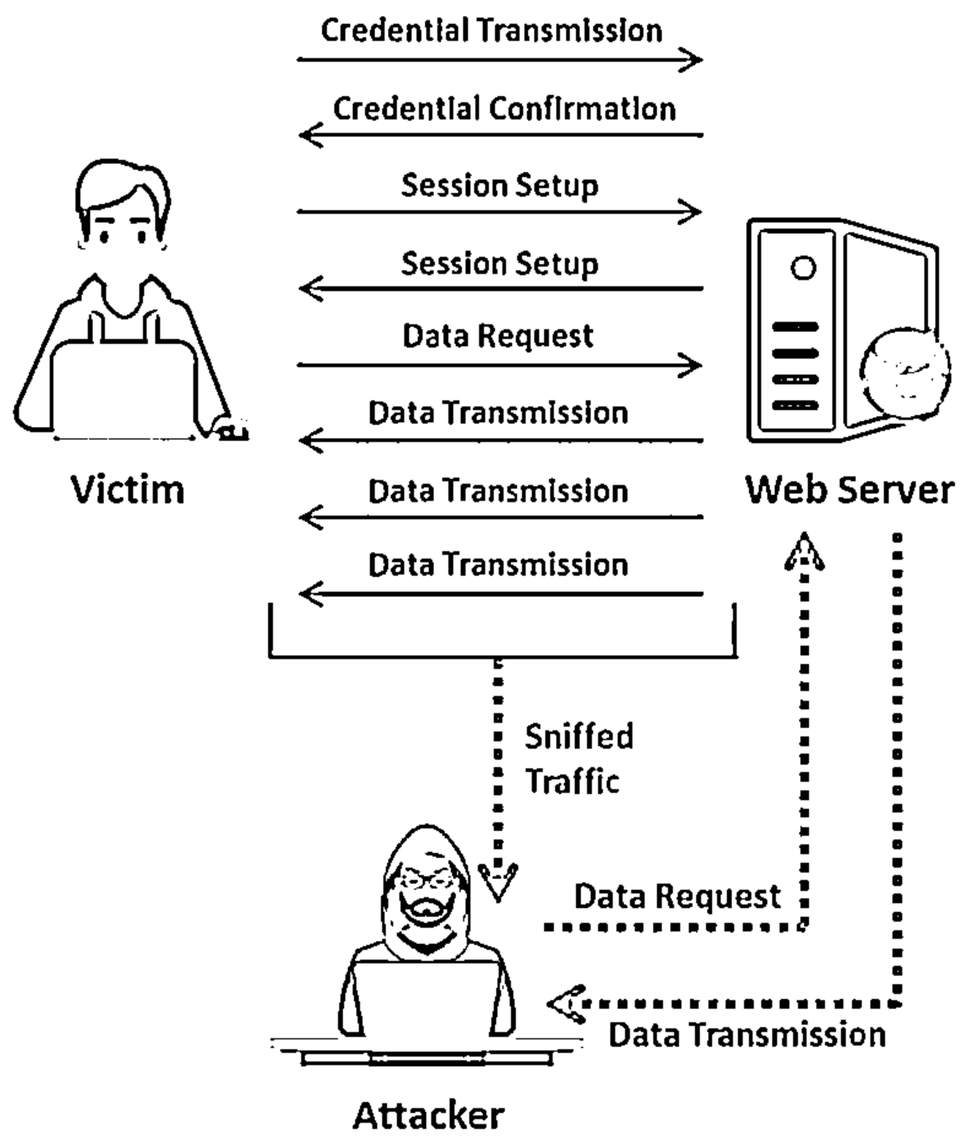


Figure 11.1: Example of session hijacking

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

Why is Session Hijacking Successful?

- Absence of account lockout for invalid session IDs
- Indefinite session timeout
- Weak session-ID generation algorithm or small session IDs
- Most computers using TCP/IP are vulnerable
- Insecure handling of session IDs
- Most countermeasures do not work without encryption

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

Why is Session Hijacking Successful?

Session hijacking succeeds because of the following factors.

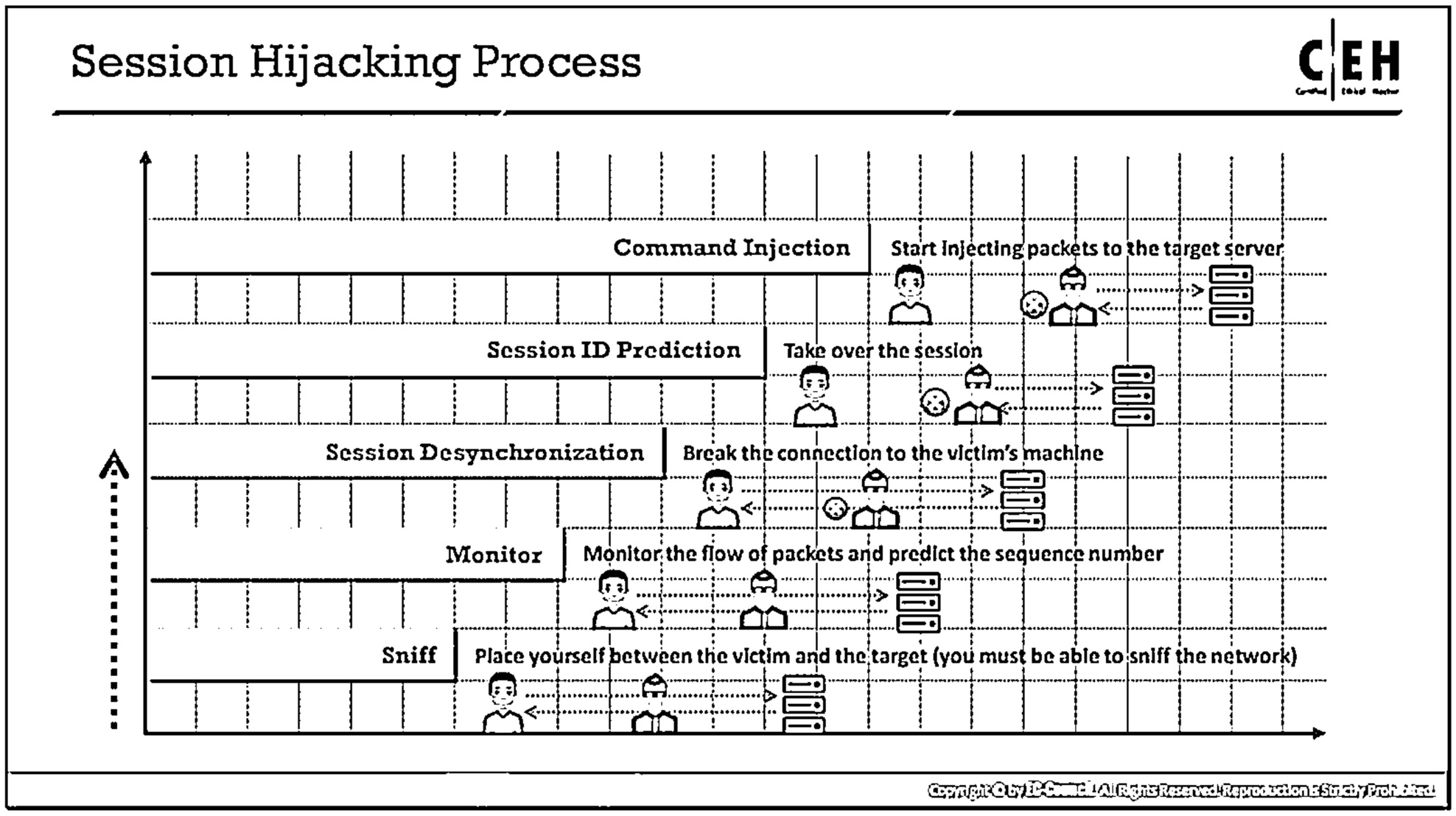
- **Absence of account lockout for invalid session IDs**: If a website does not implement account lockout, an attacker can make several attempts to connect with varying session IDs embedded in a genuine URL. The attacker can continue making attempts until the actual session ID is determined. This attack is also known as a brute-force attack. During a brute-force attack, the web server does not display a warning message or complaint, allowing the attacker to determine the valid session ID.
- **Weak session-ID generation algorithm or small session IDs**: Most websites use linear algorithms to predict variables such as time or IP address for generating session IDs. By studying the sequential pattern and generating multiple requests, an attacker can easily narrow the search space necessary to forge a valid session ID. Even if a strong session-ID generation algorithm is used, an active session ID can be easily determined if the string is short.
- **Insecure handling of session IDs**: An attacker can retrieve stored session-ID information by misleading the user's browser into visiting another site. Before the session expires, the attacker can exploit the information in many ways, such as Domain Name System (DNS) poisoning, cross-site scripting exploitation, and the exploitation of a bug in the browser.
- **Indefinite session timeout**: Session IDs with an indefinite expiration time provides an attacker with unlimited time to guess a valid session ID. An example of this is the "remember me" option in many websites. The attacker can use static session IDs to the user's web account after capturing the user's cookie file. The attacker can also perform

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

session hijacking if they can break into a proxy server, which potentially logs or caches session IDs.

- **Most computers using TCP/Internet Protocol (IP) are vulnerable**: All machines running TCP/IP are vulnerable to session hijacking because of the design flaws inherent in TCP/IP.
- **Most countermeasures do not work without encryption**: It is easy to sniff session IDs in a flat network if transport security is not set up properly during the transmission of session ID cookies, even if a web application uses Secure Sockets Layer (SSL) encryption. An attacker's task becomes even easier if they capture session IDs containing actual login information.

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



Session Hijacking Process

It is easier for an attacker to sneak into a system as a genuine user than to enter a system directly. An attacker can hijack a genuine user's session by finding an established session and taking it over after user authentication. After hijacking the session, the attacker can stay connected for hours without arousing suspicion. During this period, all traffic intended for the user's IP address goes to the attacker's system instead, and the attacker can plant backdoors or gain additional access to the system. Here, we examine how an attacker hijacks a session.

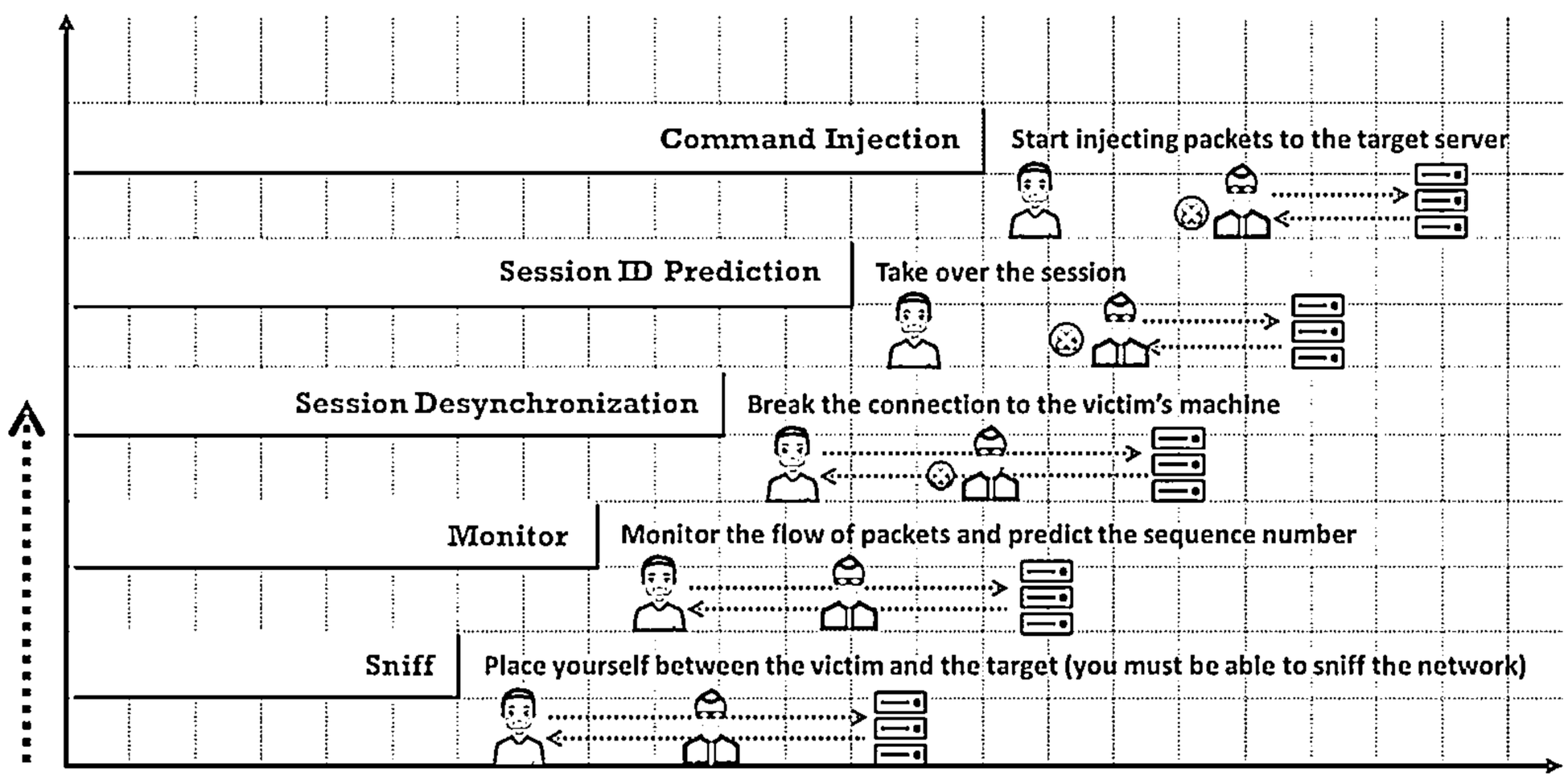


Figure 11.2: Session hijacking process

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

Session hijacking can be divided into three broad phases.

- **Tracking the connection**

  The attacker uses a network sniffer to track a victim and host or uses a tool such as Nmap to scan the network for a target with a TCP sequence that is easy to predict. After identifying a victim, the attacker captures the sequence and acknowledgment numbers of the victim because TCP checks these numbers. The attacker then uses these numbers to construct packets.

- **Desynchronizing the connection**

  A desynchronized state occurs when a connection between a target and host is established, or stable with no data transmission or the server's sequence number is not equal to the client's acknowledgment number, or vice versa.

  To desynchronize the connection between the target and host, the attacker must change the sequence number or acknowledgment number (SEQ/ACK) of the server. For this purpose, the attacker sends null data to the server; consequently, the server's SEQ/ACK numbers advance, while the target machine does not register the increment. For example, before desynchronization, the attacker monitors the session without any interference, following which they send a large amount of null data to the server. These data change the ACK number on the server without affecting anything else, thereby desynchronizing the server and target.

  Another approach is to send a reset flag to the server to break the connection on the server side. Ideally, this occurs in the early setup stage of the connection. The attacker's goal is to break the connection on the server side and create a new connection with a different sequence number.

  The attacker waits for a SYN/ACK packet from the server to the host. On detecting a packet, the attacker immediately sends an RST packet and a SYN packet with identical parameters, such as a port number with a different sequence number, to the server. The server, on receiving the RST packet, closes the connection with the target and initiates another one based on the SYN packet but with a different sequence number on the same port. After opening a new connection, the server sends a SYN/ACK packet to the target for acknowledgement. The attacker detects (but does not intercept) this packet and sends an ACK packet to the server. Now, the server is in the established state. The aim is to keep the target conversant and ensure that it switches to the established state on receiving the first SYN/ACK packet from the server. Consequently, both the server and target are desynchronized but in an established state.

  An attacker can also use a FIN flag, but this will make the server respond with an ACK packet, thus revealing the attack through an ACK storm. The attack is revealed because of a flaw in this method of hijacking a TCP connection. While receiving an unacceptable packet, the host acknowledges it by sending the expected sequence number. This unacceptable packet generates an ACK packet, thereby creating an endless loop for every data packet. The mismatch in SEQ/ACK numbers results in excess network traffic

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

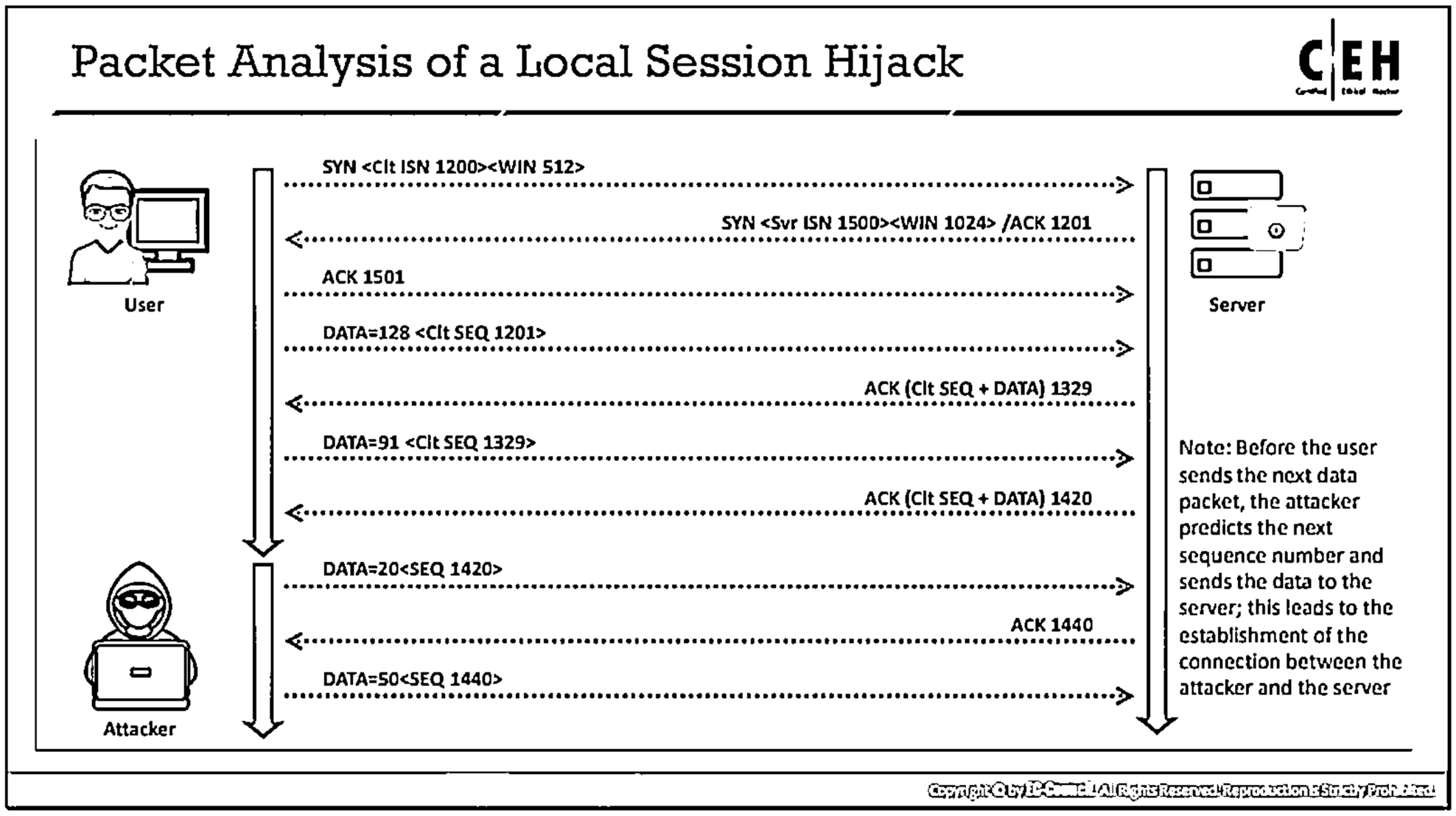
with both the server and target attempting to verify the correct sequence. Because these packets carry no data, retransmission does not occur if the packet is lost. However, because TCP uses IP, the loss of a single packet ends the unwanted conversation between the server and target.

An attacker can add a desynchronizing stage to the hijack sequence to deceive the target host. Without desynchronizing, the attacker injects data into the server while keeping their identity hidden by spoofing an IP address. However, the attacker should ensure that the server responds to the target host as well.

- **Injecting the attacker's packet**

  Once the attacker has interrupted the connection between the server and target, they can either inject data into the network or actively participate as the man in the middle, passing data from the target to the server and vice-versa while reading and injecting data at will.

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



Packet Analysis of a Local Session Hijack

Session hijacking involves high-level attack vectors, which affect many systems. TCP is used for transmitting data by many systems that establish LAN or Internet connections. For establishing a connection between two systems and for the successful transmission of data, the two systems should perform a three-way handshake. Session hijacking involves the exploitation of this three-way handshake method to take control over the session.

To conduct a session hijacking attack, the attacker performs three activities:

- Tracking of a session
- Desynchronization of the session
- Injection of commands during the session

By sniffing network traffic, an attacker can monitor or track a session. The next step in session hijacking is to desynchronize the session. It is easy to accomplish this attack if the attacker knows the next sequence number (NSN) used by the client. A session can be hijacked by using that sequence number before the client uses it. There are two possibilities to determine sequence numbers: one is to sniff the traffic, find an ACK packet, and then determine the NSN based on the ACK packet. The other is to transmit data with guessed sequence numbers, which is not a reliable method. If the attacker can access the network and sniff the TCP session, they can easily determine the sequence number. This type of session hijacking is called "local session hijacking."

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

The below figure shows the packet analysis of a local session hijack.

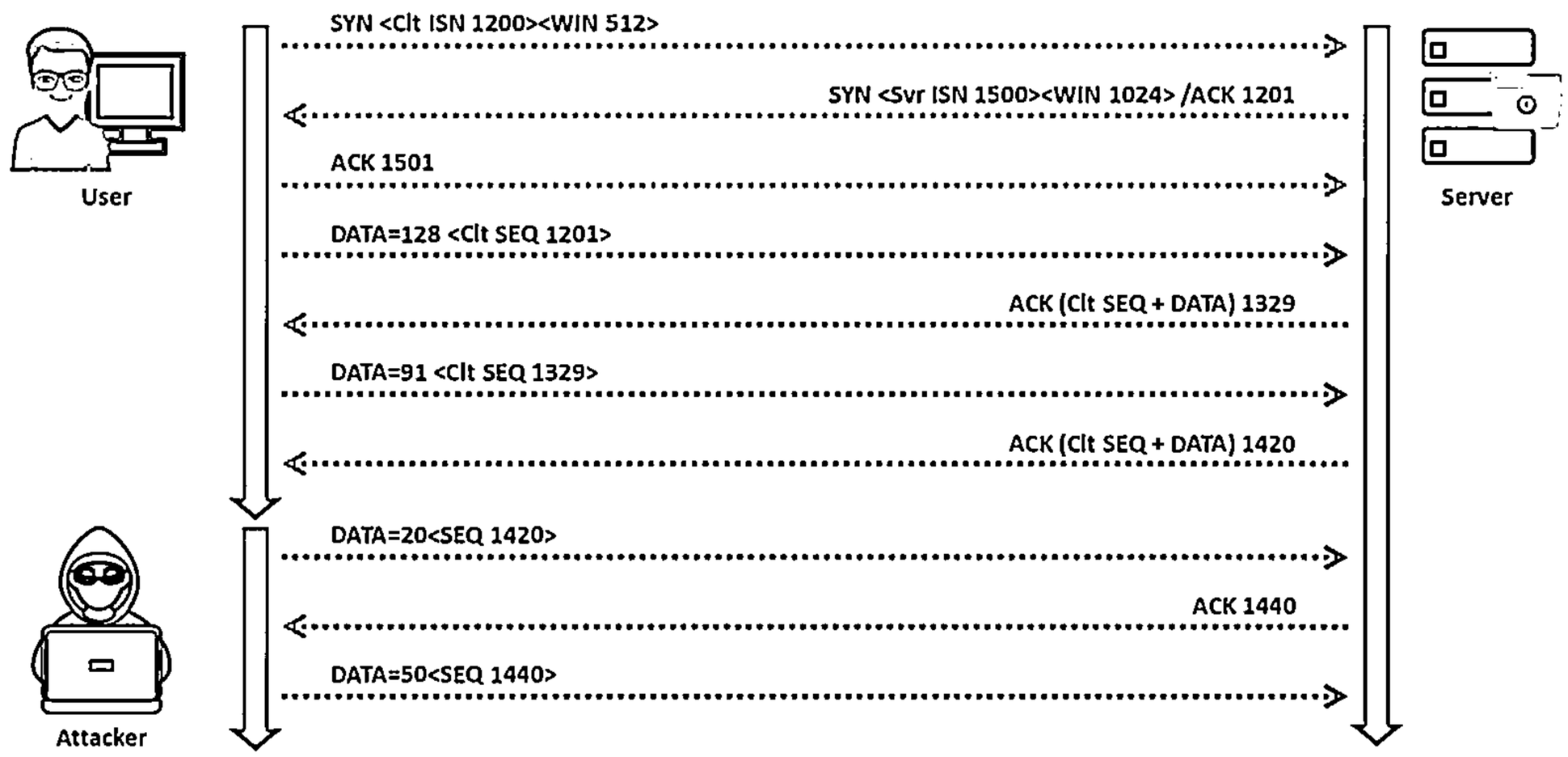


Figure 11.3: Packet analysis of a local session hijack

According to above figure, the next expected sequence number is 1420. If the attacker transmits that packet sequence number before the user does, they can desynchronize the connection between the user and server.

If the attacker sent the data with the expected sequence number before the user could, the server would be synchronized with the attacker. This leads to the establishment of a connection between the attacker and server. Then, the server would drop the data sent by the user with the correct sequence number, believing it to be a resent packet. The user is unaware of the attacker's action and may resend the data packet because the user does not receive an ACK for their TCP packet. However, the server would drop all the packets resent by the user. Thus, the local session hijacking attack is successfully completed.

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

Types of Session Hijacking

Passive	❑ In a passive attack, an attacker hijacks a session but sits back, watches, and records all the traffic in that session
Active	❑ In an active attack, an attacker finds an active session and seizes control of it

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

Types of Session Hijacking

Session hijacking can be either active or passive, depending on the degree of involvement of the attacker. The essential difference between an active and passive hijack is that while an active hijack takes over an existing session, a passive hijack monitors an ongoing session.

- **Passive Session Hijacking**

  In a passive attack, after hijacking a session, an attacker only observes and records all the traffic during the session. A passive attack uses sniffers on the network, allowing attackers to obtain information such as user IDs and passwords. The attacker can later use this information to log in as a valid user and enjoy the user's privileges. Password sniffing is the simplest attack to obtain raw access to a network. Countering this attack involves methods that range from identification schemes (for example, one-time password systems such as S/KEY) to ticketing identification (for example, Kerberos). These techniques help in protecting data from sniffing attacks, but they cannot protect against active attacks if the data are unencrypted or do not carry a digital signature.

- **Active Session Hijacking**

  In an active attack, an attacker takes over an existing session either by breaking the connection on one side of the conversation or by actively participating. An example of an active attack is a man-in-the-middle (MITM) attack. To perform a successful MITM attack, the attacker must guess the sequence number before the target responds to the server. On most current networks, sequence-number prediction does not work, because operating-system (OS) vendors use random values for the initial sequence number, which makes it difficult to predict sequence numbers.

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

Figure 11.4: Attacker sniffing a victim's traffic

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

Session Hijacking in OSI Model

Network Level Hijacking

- Network level hijacking can be defined as the interception of packets during the transmission between a client and the server in a TCP or UDP session

Application Level Hijacking

- Application level hijacking refers to gaining control over the HTTP's user session by obtaining the session IDs

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

Session Hijacking in OSI Model

There are two levels of session hijacking in the OSI model: the network level and application level.

- **Network Level Hijacking**

  Network level hijacking is the interception of packets during the transmission between a client and server in a TCP/User Datagram Protocol (UDP) session. A successful attack provides the attacker with crucial information, which can be further used to attack application level sessions. Attackers most likely perform network level hijacking because they do not need to modify the attack on a per-web-application basis. This attack focuses on the data flow of the protocol shared across all web applications.

- **Application Level Hijacking**

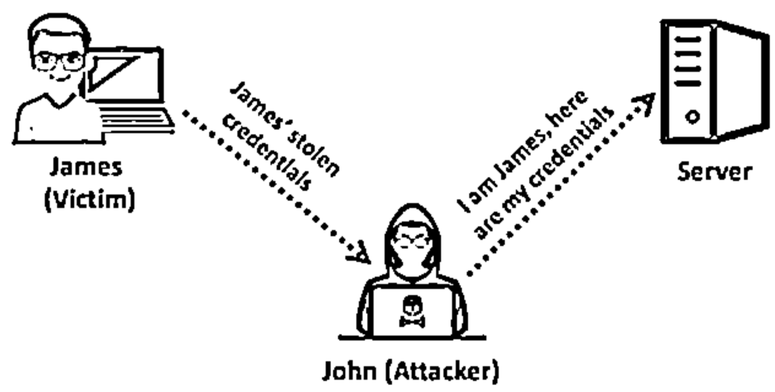
  Application level hijacking involves gaining control over the Hypertext Transfer Protocol (HTTP) user session by obtaining the session IDs. At the application level, the attacker gains control of an existing session and can create new unauthorized sessions by using stolen data. In general, both occur together, depending on the system being attacked.

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

Spoofing vs. Hijacking

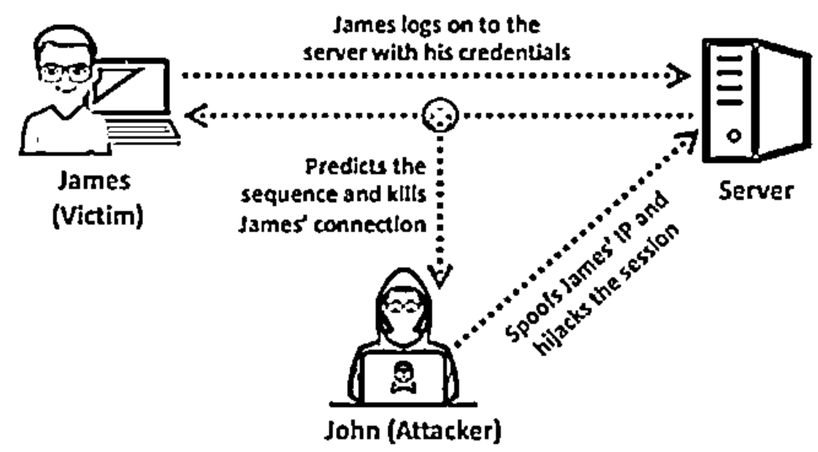
Spoofing Attack

- An attacker pretends to be another user or machine (victim) to gain access
- The attacker does not seize control of an existing active session; instead, he or she initiates a new session using the victim's stolen credentials



Hijacking

- Session hijacking is the process of seizing control of an existing active session
- The attacker relies on the legitimate user to create a connection and authenticate



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

Spoofing vs. Hijacking

In blind hijacking, an attacker predicts the sequence numbers that a victim host sends to create a connection that appears to originate from the host or a blind spoof. To understand blind hijacking, it is important to understand sequence-number prediction. TCP sequence numbers, which are unique per byte in a TCP session, provide flow control and data integrity. TCP segments provide the initial sequence number (ISN) as a part of each segment header. ISNs do not start at zero for each session. As part of the handshake process, each participant needs to state the ISN, and bytes are numbered sequentially from that point.

Blind session hijacking relies on the attacker's ability to predict or guess sequence numbers. An attacker is unable spoof a trusted host on a different network and observe the reply packets because no route exists for the packets to return to the attacker's IP address. Moreover, the attacker is unable resort to Address Resolution Protocol (ARP) cache poisoning because routers do not broadcast ARP across the Internet. Because the attacker is unable to observe the replies, they must anticipate the responses from the victim and prevent the host from sending a TCP/RST packet to the victim. The attacker predicts sequence numbers that the remote host expects from the victim and then hijacks the communication. This method is useful to exploit the trust relationships between users and remote machines.

In a spoofing attack, an attacker pretends to be another user or machine (victim) to gain access. Instead of taking over an existing active session, the attacker initiates a new session using the victim's stolen credentials. Simple IP spoofing is easy to perform and is useful in various attack methods. To create new raw packets, the attacker must have root access on the machine. However, to establish a spoofed connection using this session hijacking technique, an attacker must know the sequence numbers used by a target machine. IP spoofing forces the attacker to

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

forecast the NSN. When an attacker uses blind hijacking to send a command, they cannot view the response.

In the case of IP spoofing without a session hijack, guessing the sequence number is unnecessary because no currently open session exists with that IP address. In a session hijack, the traffic returns to the attacker only if source routing is used. Source routing is a process that allows the sender to specify the route to be taken by an IP packet to the destination. The attacker performs source routing and then sniffs the traffic as it passes by the attacker. In session spoofing, captured authentication credentials are used to establish a session. In contrast, active hijacking eclipses a pre-existing session. As a result of this attack, a legitimate user may lose access or the normal functionality of their established Telnet session because an attacker hijacks the session and acts with the user's privileges. Because most authentication mechanisms are enforced only at the initiation of a session, the attacker can gain access to a target machine without authentication while a session is in progress.

Another method is to use source routed IP packets. This type of MITM attack allows an attacker to become a part of the target–host conversation by deceptively guiding IP packets to pass through their system.

Session hijacking is the process of taking over an existing active session. An attacker relies on a legitimate user to make a connection and authenticate. Session hijacking is more difficult than IP address spoofing. In session hijacking, John (an attacker) would seek to insert himself into a session that James (a legitimate user) already had set up with \\Mail. John would wait until James establishes a session, displace James from the established session by some means, such as a DoS attack, and then pick up the session as though he were James. Subsequently, John would send a scripted set of packets to \\Mail and observe the responses. For this purpose, John needs to know the sequence number in use when he hijacked the session. To calculate the sequence number, he must know the ISN and the number of packets involved in the exchange process.

Successful session hijacking is difficult without the use of known tools and is only possible when several factors are under the attacker's control. Knowledge of the ISN is the least of John's challenges. For instance, John needs a method to displace James from the active session as well as a method to know the exact status of James's session at the moment that James is displaced. Both these tasks require John to have far more knowledge and control over the session than would normally be possible.

However, IP address spoofing attacks can only be successful if an attacker uses IP addresses for authentication. They cannot perform IP address spoofing or session hijacking if per-packet integrity checking is executed. In the same manner, IP address spoofing or session hijacking is not possible if the session uses encryption methods such as Secure Sockets Layer (SSL) or Point-to-Point Tunneling Protocol (PPTP). Consequently, the attacker cannot participate in the key exchange.

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

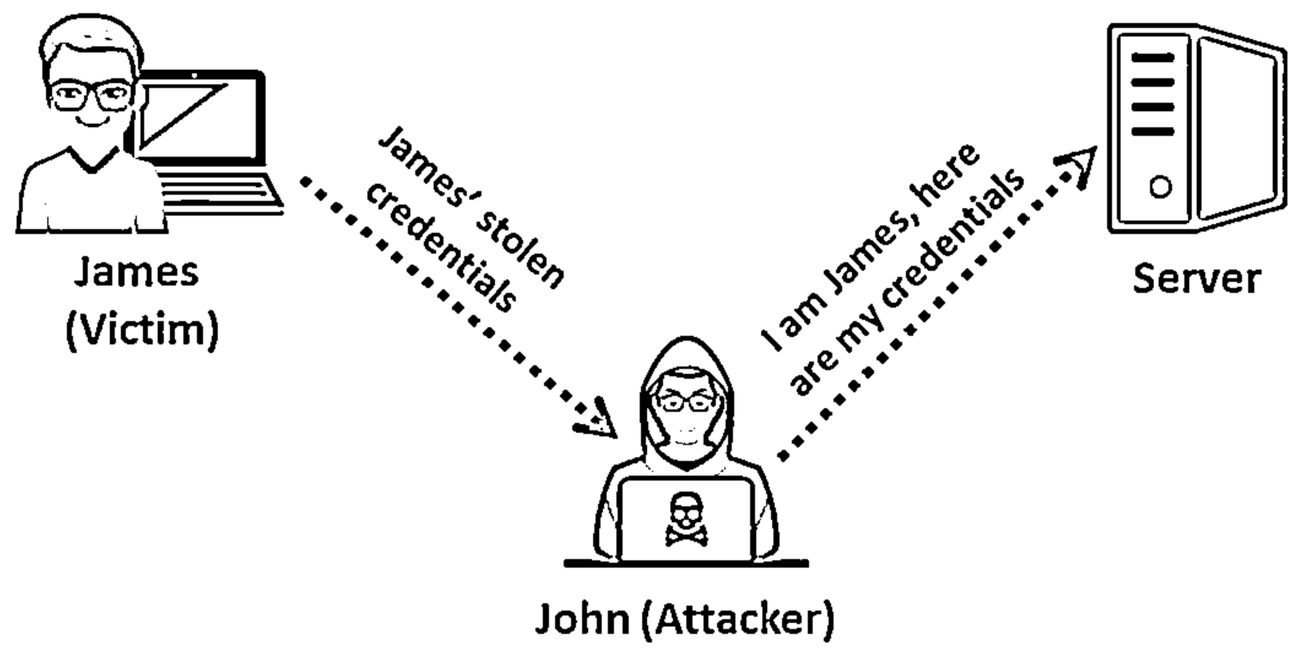


Figure 11.5: Spoofing attack

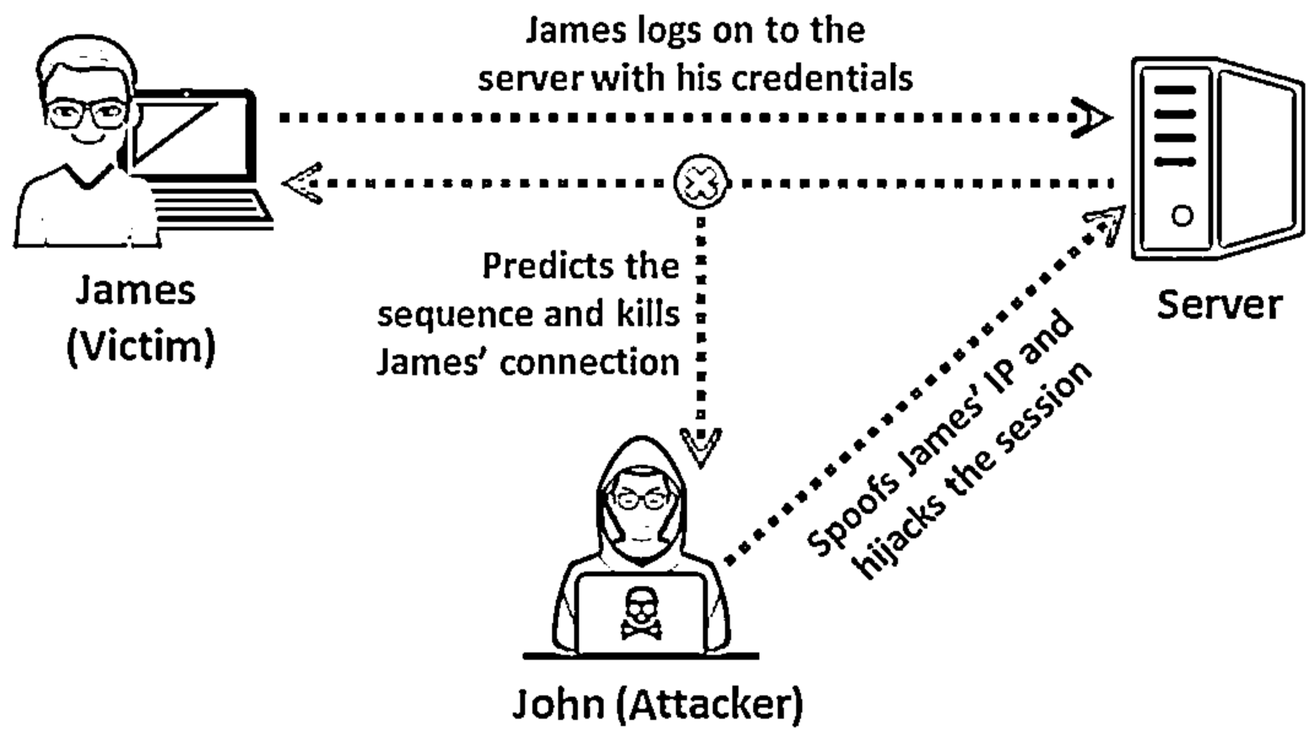


Figure 11.6: Session hijacking

In summary, the hijacking of non-encrypted TCP communications requires the presence of non-encrypted session-oriented traffic, the ability to recognize TCP sequence numbers from which the next sequence number (NSN) can be predicted, and the ability to spoof a host's media access control (MAC) or IP address to receive communications that are not destined for the attacker's host. If the attacker is on the local segment, they can sniff and predict the ISN + 1 number and route the traffic back to them by poisoning the ARP caches on the two legitimate hosts participating in the session.

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

Module Flow

01	Session Hijacking Concepts
03	Network Level Session Hijacking
02	Application Level Session Hijacking
04	Session Hijacking Tools
05	Countermeasures

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

Application Level Session Hijacking

- In a session hijacking attack, a session token is stolen or a valid session token is predicted to gain unauthorized access to the web server

A session token can be compromised in various ways

1. Session sniffing
2. Predictable session token
3. Man-in-the-middle attack
4. Man-in-the-browser attack
5. Cross-site scripting (XSS) attack
6. Cross-site request forgery attack
7. Session replay attack
8. Session fixation attack
9. CRIME attack
10. Forbidden attack
11. Session donation attack

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

Application Level Session Hijacking

In application level hijacking, the attacker obtains the session IDs to gain control over an existing session or to create a new unauthorized session. This section discusses application level session hijacking and various methods to compromise the session token, such as session sniffing and the use of predictable session tokens.

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

In application level session hijacking, an attacker steals or predicts a valid session to gain unauthorized access to a web server. Usually, network level and application level session hijacking occur together because a successful network level session hijack provides an attacker with ample information to perform application level session hijacking. Application level session hijacking relies on HTTP sessions.

An attacker implements various techniques such as stealing, guessing, and brute forcing to obtain a valid session ID, which helps in acquiring control over a valid user's session while it is in progress.

- **Stealing**: Attackers use different techniques to steal session IDs. An attacker can steal the session key through physical access by, for example, acquiring the files containing session IDs or memory contents of either the user's system or the server. The attacker can also use sniffing tools such as Wireshark or SteelCentral Packet Analyzer to sniff the traffic between the client and server to extract the session IDs from the packets.
- **Guessing**: An attacker attempts to guess the session IDs by observing session variables. In the case of session hijacking, the range of session ID values that can be guessed is limited. Thus, guessing techniques are effective only when servers use weak or flawed session-ID generation mechanisms.
- **Brute forcing**: In the brute-force technique, an attacker obtains session IDs by attempting all possible permutations of session ID values until finding one that works. An attacker using a digital subscriber line (DSL) can generate up to 1,000 session IDs per second. This technique is most useful when the algorithm that produces session IDs is non-random.

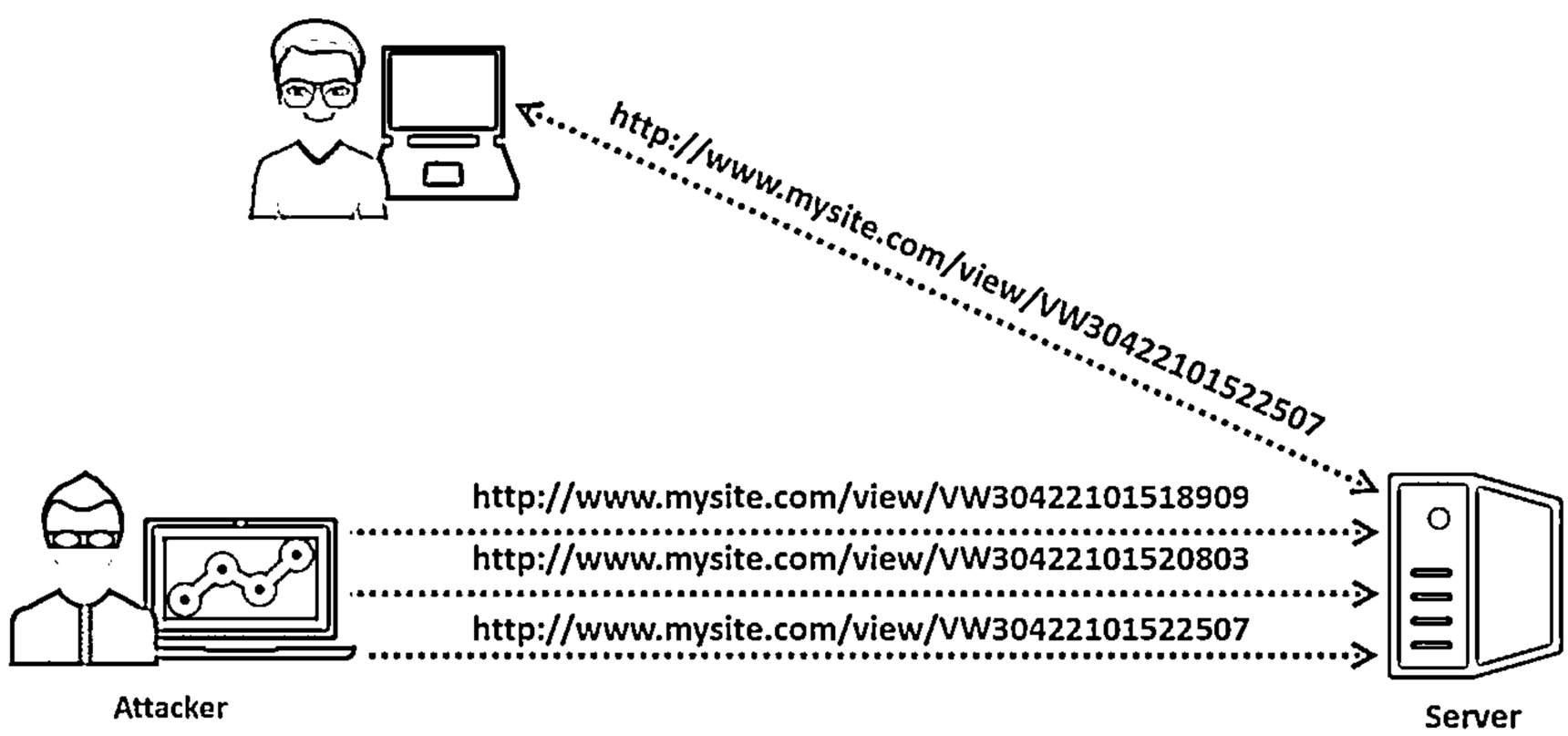


Figure 11.7: Brute-forcing attack on the session ID of a user

As shown in the above figure, a legitimate user connects to a server with session ID VW30422101522507. Employing various combinations such as VW30422101518909 and VW30422101520803, an attacker attempts to brute force the session ID in the hope of eventually arriving at the correct session ID. Once the attacker obtains the correct

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

session ID, they gain complete access to the user's data and can perform operations on behalf of the legitimate user.

Note: A session ID brute-forcing attack is known as a session prediction attack if the predicted range of values for a session ID is very small.

A session token can be compromised in various ways:

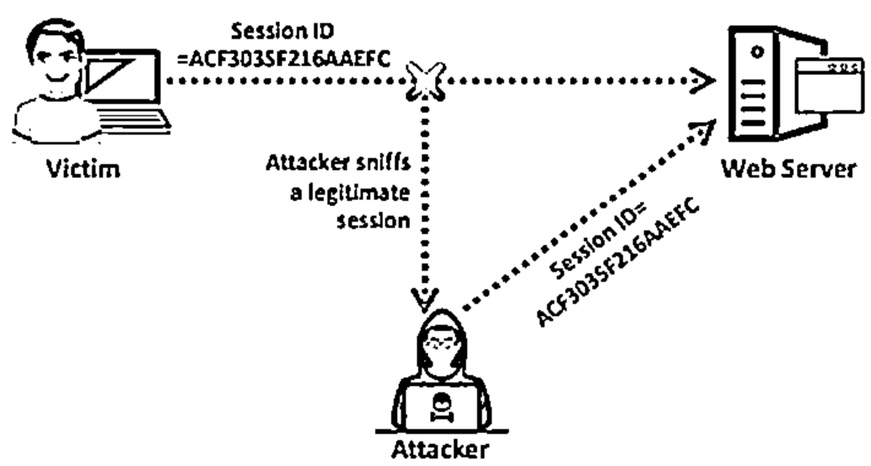
- Session sniffing
- Predictable session token
- Man-in-the-middle (MITM) attack
- Man-in-the-browser attack
- Cross-site scripting (XSS) attack
- Cross-site request forgery attack
- Session replay attack
- Session fixation attack
- CRIME attack
- Forbidden attack
- Session donation attack

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

Compromising Session IDs using Sniffing and by Predicting Session Token

Compromising Session IDs using Sniffing

- An attacker uses a sniffer to capture a valid session token or session ID
- The attacker then uses the valid token session to gain unauthorized access to the web server



Compromising Session IDs by Predicting Session Token

- Attackers can predict session IDs generated by weak algorithms and impersonate a website user
- Attackers analyze variable sections of session IDs to determine a pattern
- The analysis is performed manually or using various cryptanalytic tools
- Attackers collect a high number of simultaneous session IDs to gather samples in the same time window and keep the variable constant

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

Compromising Session IDs Using Sniffing

A web server identifies a user's connection through a unique session ID (also known as a session token). The web server sends a session token to the client browser after the successful authentication of client login. Usually, a session token comprises a string of variable width that is useful in various ways, such as in the header of an HTTP requisition (cookie), in a URL, or in the body of an HTTP requisition.

An attacker uses packet sniffing tools such as Wireshark and SteelCentral Packet Analyzer to intercept the HTTP traffic between a victim and web server. The attacker then analyzes the data in the captured packets to identify valuable information such as session IDs and passwords. Once the session ID is determined, the attacker masquerades as the victim and sends the session ID to the web server before the victim does. The attacker uses the valid token session to gain unauthorized access to the web server. In this manner, the attacker takes control over an existing legitimate session.

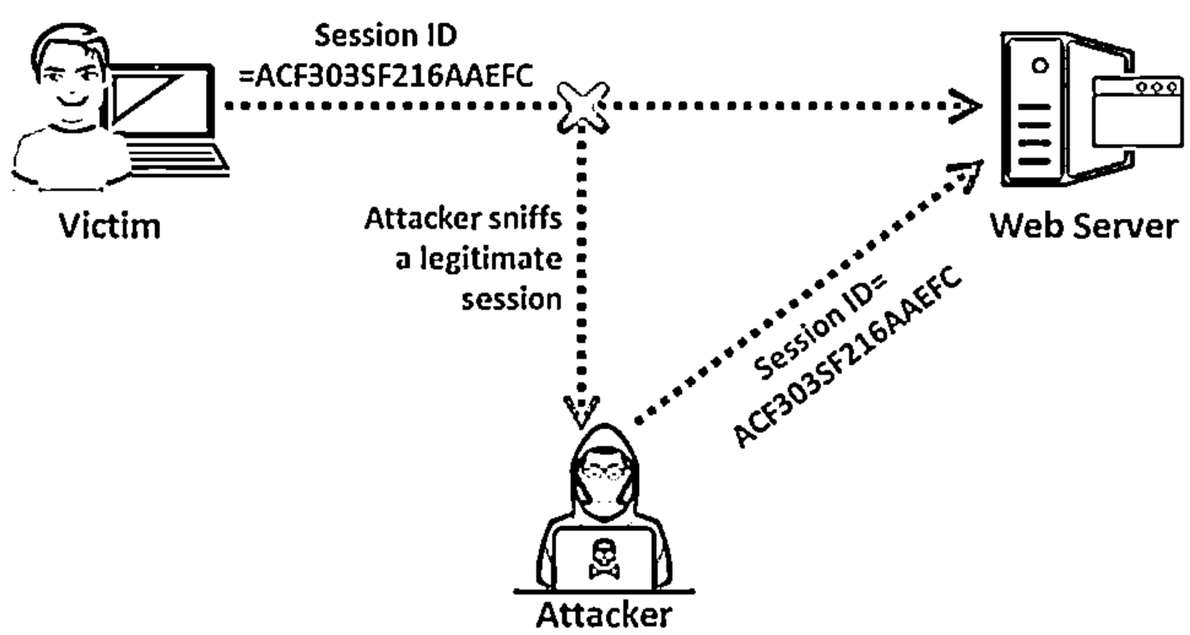


Figure 11.8: Prediction of session ID by sniffing

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

Compromising Session IDs by Predicting Session Token

A session ID is tagged as proof of an authenticated session established between a user and web server. Thus, if an attacker can guess or predict the session ID of the user, fraudulent activity is possible. Session prediction enables an attacker to bypass the authentication schema of an application. Usually, attackers can predict session IDs generated by weak algorithms and impersonate a website user. Attackers analyze a variable section of session IDs to determine the existence of a pattern. This analysis is performed either manually or by using various cryptanalytic tools.

An attacker collect a high number of simultaneous session IDs to gather samples in the same time window and keep the variable constant. First, the attacker collects some valid session IDs that are useful in identifying authenticated users. The attacker then studies the session ID structure, the information used to generate it, and the algorithm used by the web application to secure it. From these findings, the attacker can predict the session ID.

Attackers can also guess session IDs by using a brute-force technique, in which they generate and test different session ID values until they succeed in gaining access to the application.

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

How to Predict a Session Token

- Most web servers use custom algorithms or a predefined pattern to generate session IDs
- An attacker guesses the unique session value or deduces the session ID to hijack the session

Captures

An attacker captures several session IDs and analyzes the pattern

```
http://www.certifiedhacker.com/view/JBEX18082019152820
http://www.certifiedhacker.com/view/JBEX18082019153020
http://www.certifiedhacker.com/view/JBEX18082019160020
http://www.certifiedhacker.com/view/JBEX18082019164020
```

Constant Date Time

Predicts

At 16:25:55 on August 23, 2019, the attacker can successfully predict the session ID

```
http://www.certifiedhacker.com/view/JBEX23082019162555
```

Constant Date Time

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

How to Predict a Session Token

Most web servers generate session IDs using custom algorithms or a pre-defined pattern that might simply increase static numbers, whereas others use more complex procedures such as factoring in time and other computer-specific variables. Thus, attackers can identify session IDs generated in the following ways:

- Embedding in the URL, which is received by a GET request in the application when the links embedded within a page are clicked by clients
- Embedding in a form as a hidden field, which is submitted to the HTTP's POST command
- Embedding in cookies on the client's local machine

An attacker guesses the unique session value or deduces the session ID to hijack the session. As shown in the below figure, an attacker first captures several session IDs and analyzes the pattern.

```
http://www.certifiedhacker.com/view/JBEX18082019152820
http://www.certifiedhacker.com/view/JBEX18082019153020
http://www.certifiedhacker.com/view/JBEX18082019160020
http://www.certifiedhacker.com/view/JBEX18082019164020
```

Constant Date Time

Figure 11.9: Sample sessions captured by an attacker

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

On analyzing the pattern, at 16:25:55 on August 23, 2019, the attacker successfully predicts the session ID, as shown in the below figure.

```
http://www.certifiedhacker.com/view/JBEX23082019162555
                                    Constant  Date      Time
```

Figure 11.10: Session ID predicted by the attacker

Now, the attacker can mount an attack through the following steps.

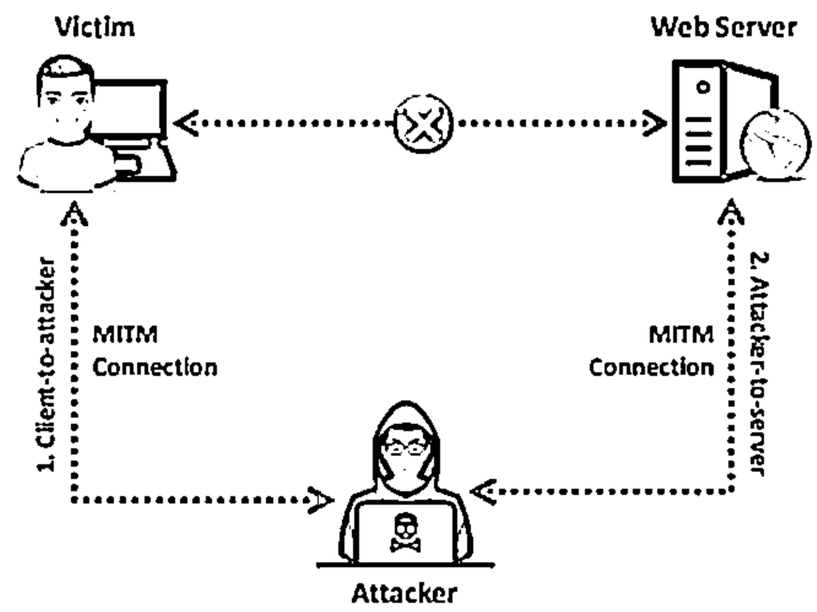
- The attacker acquires the current session ID and connects to the web application.
- The attacker implements a brute-force technique or calculates the next session ID.
- The attacker modifies the current value in the cookie/URL/hidden form field and assumes the next user's identity.

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

Compromising Session IDs Using Man-in-the-Middle Attack

- The man-in-the-middle attack is used to intrude into an existing connection between systems and intercept the messages being exchanged

- Attackers use different techniques and split the TCP connection into two connections:
  - Client-to-attacker connection
  - Attacker-to-server connection
- After the interception of the TCP connection, an attacker can read, modify, and insert fraudulent data into the intercepted communication
- In the case of an http transaction, the TCP connection between the client and the server becomes the target



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

Compromising Session IDs Using Man-in-the-Middle Attack

A man-in-the-middle (MITM) attack is used to intrude into an existing connection between systems and to intercept messages being transmitted. In this attack, attackers use different techniques and split a TCP connection into two: a client-to-attacker connection and an attacker-to-server connection. After the successful interception of a TCP connection, an attacker can read, modify, and insert fraudulent data into the intercepted communication. In the case of an HTTP transaction, the TCP connection between the client and server is the target.

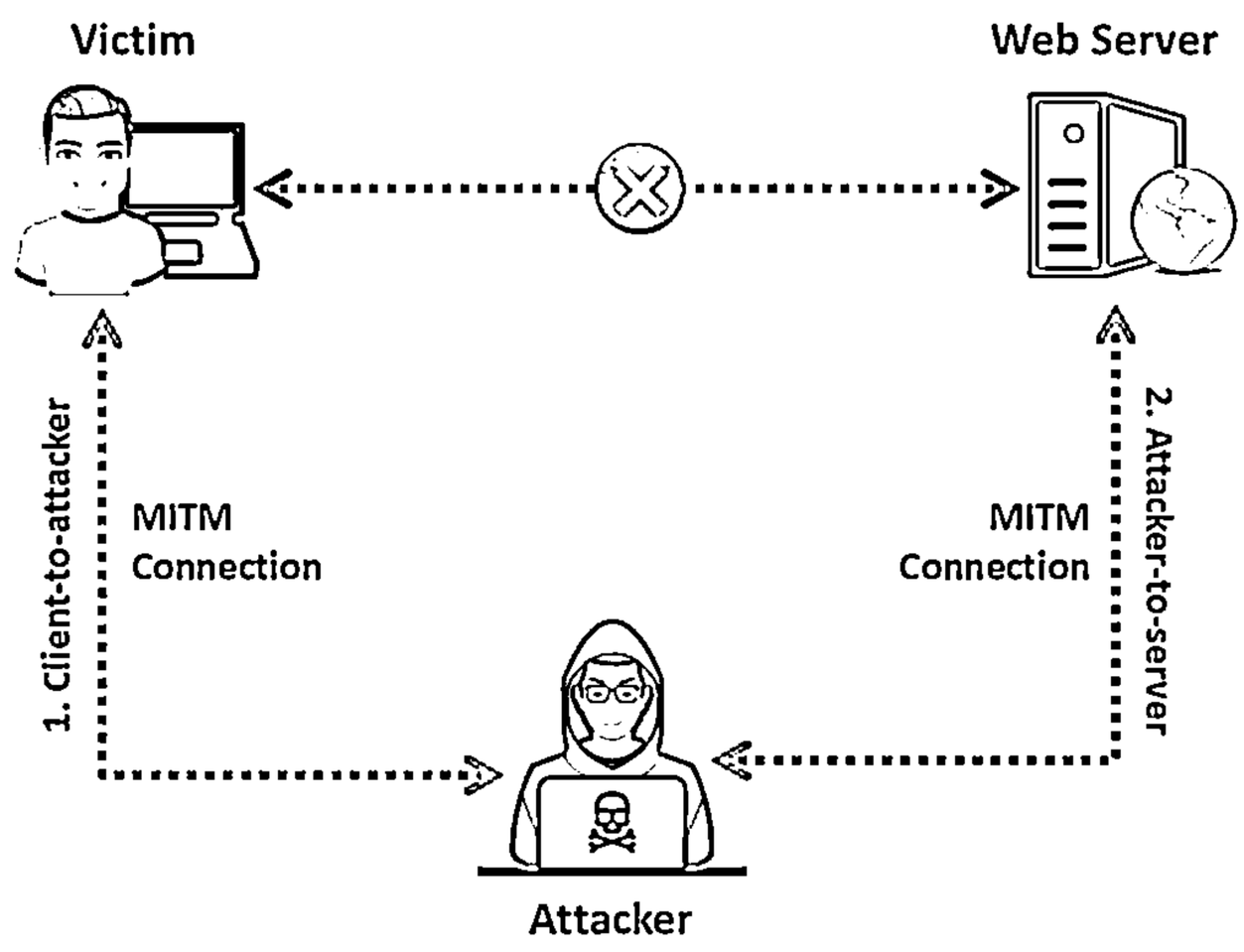


Figure 11.11: Prediction of session ID using a man-in-the-middle (MITM) attack

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

Compromising Session IDs Using Man-in-the-Browser Attack

- The man-in-the-browser attack uses a Trojan horse to intercept the calls between the browser and its security mechanisms or libraries
- It works with an already installed Trojan horse and acts between the browser and its security mechanisms
- Its main objective is to cause financial deceptions by manipulating transactions of Internet banking systems

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

Steps to Perform Man-in-the-Browser Attack

1. The Trojan first infects the computer's software (OS or application)
2. The Trojan installs malicious code (extension files) and saves it into the browser configuration
3. After the user restarts the browser, the malicious code in the form of extension files is loaded
4. The extension files register a handler for every visit to the webpage
5. When the page is loaded, the extension uses the URL and matches it with a list of known sites targeted for attack
6. The user logs in securely to the website
7. The Trojan registers a button event handler when a specific page load is detected for a specific pattern and compares it with its targeted list
8. When the user clicks on the button, the extension uses DOM interface and extracts all the data from all form fields and modifies the values
9. The browser sends the form and modified values to the server
10. The server receives the modified values but cannot distinguish between the original and the modified values
11. After the server performs the transaction, a receipt is generated
12. Now, the browser receives the receipt for the modified transaction
13. The browser displays the receipt with the original details
14. The user thinks that the original transaction was received by the server without any interceptions

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

Compromising Session IDs Using Man-in-the-Browser Attack

A man-in-the-browser attack is similar to an MITM attack. The difference between the two is that a man-in-the-browser attack uses a Trojan horse to intercept and manipulate calls between a browser and its security mechanisms or libraries. An attacker positions a previously installed Trojan between the browser and its security mechanism, and the Trojan can modify web pages and transaction content or insert additional transactions. All of the Trojan's activities are invisible to both the user and web application.

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

The main objective of this attack is financial theft by manipulating transactions made using Internet banking systems. A man-in-the-browser attack can succeed even in the presence of security mechanisms such as SSL, public key infrastructure (PKI), and two-factor authentication because all the expected controls and security mechanisms would seem to function normally.

Steps to Perform Man-in-the-Browser Attack:

- The Trojan first infects the computer's software (OS or application).
- The Trojan installs malicious code (extension files) and saves it in the browser configuration.
- After the user restarts the browser, the malicious code in the form of extension files is loaded.
- The extension files register a handler for every visit to a webpage.
- When a page is loaded, the extension matches its URL with a list of known sites targeted for attack.
- The user logs in securely to the website.
- The extension registers a button event handler when a specific page load is detected with a specific pattern and compares it with its targeted list.
- When the user clicks on the button, the extension uses the Document Object Model (DOM) interface and extracts all the data from all form fields and modifies the values.
- The browser sends the form and modified values to the server.
- The server receives the modified values but cannot distinguish between the original and modified values.
- After the server performs the transaction, a receipt is generated.
- Now, the browser receives the receipt for the modified transaction.
- The browser displays the receipt with the original details.
- The user believes that the original transaction was received by the server without any interception.

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

Compromising Session IDs Using Client-side Attacks

Cross-Site Scripting (XSS)

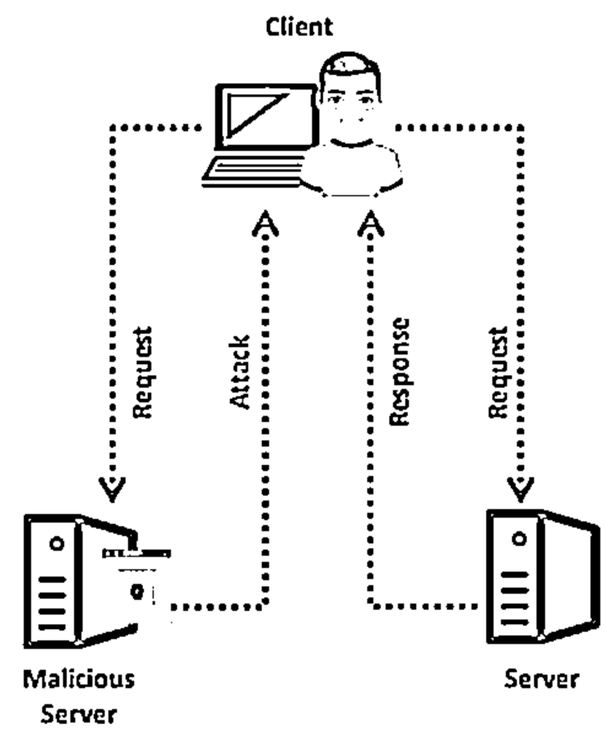
- XSS enables attackers to inject malicious client-side scripts into the web pages viewed by other users

Malicious JavaScript Codes

- A malicious script can be embedded in a web page that does not generate any warning, but it captures session tokens in the background and sends them to the attacker

Trojans

- A Trojan horse can change the proxy settings in the user's browser to send all the sessions through the attacker's machine



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

Compromising Session IDs Using Client-side Attacks

Client-side attacks target vulnerabilities in client applications that interact with a malicious server or process malicious data. Depending on the nature of vulnerabilities, an attacker can exploit an application by sending an email with a malicious link or otherwise tricking a user into visiting a malicious website. Vulnerable client-side applications include unprotected websites, Java Runtime Environment, and browsers; of these, browsers are the major target. Client-side attacks occur when clients establish connections with malicious servers and process potentially harmful data from them. If no interaction occurs between the client and server, then there is no scope for a client-side attack. One such example is running a File Transfer Protocol (FTP) client without establishing a connection to an FTP server. In the case of instant messaging, the application is configured in such a way that it makes clients to log in to a remote server, making it susceptible to client-side attacks. The following client-side attacks can be used to compromise session IDs.

- **Cross-site scripting (XSS)**: XSS enables attackers to inject malicious client-side scripts into web pages viewed by other users.
- **Malicious JavaScript codes**: An attacker can embed in a web page a malicious script that does not generate any warning but captures session tokens in the background and sends them to the attacker.
- **Trojans**: A Trojan horse can change the proxy settings in the user's browser to send all sessions through an attacker's machine.

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

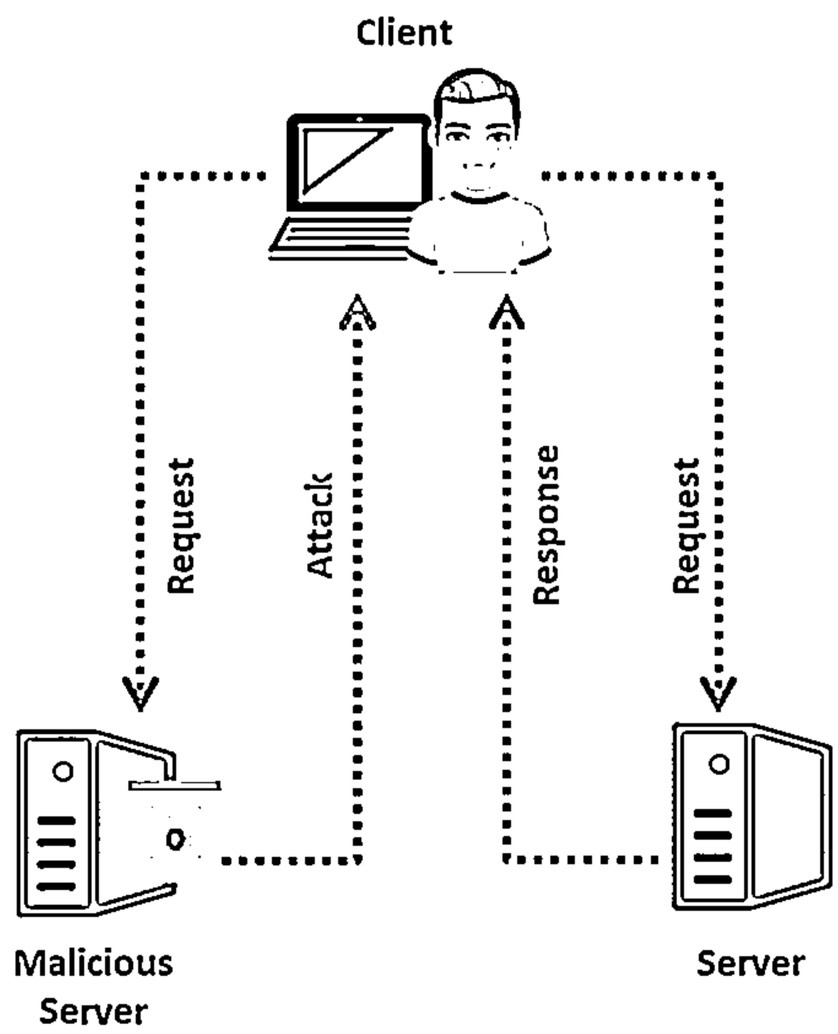
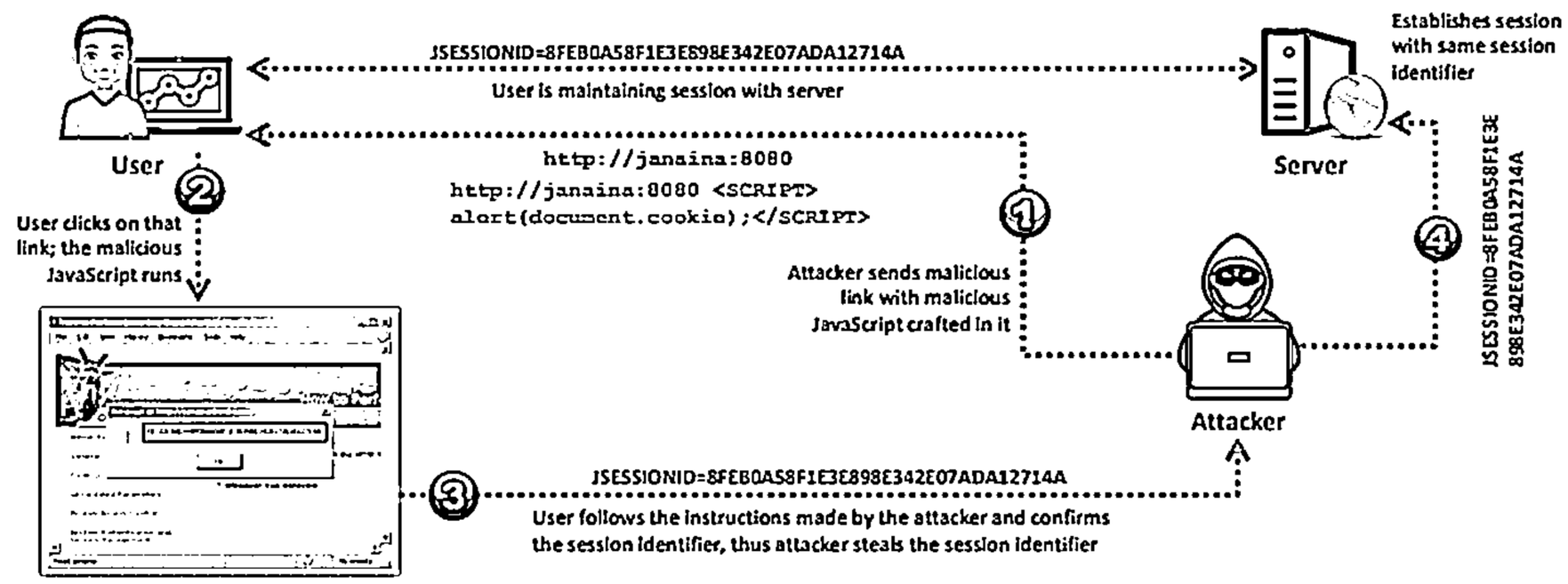


Figure 11.12: Prediction of session ID using a client-side attack

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

Compromising Session IDs Using Client-side Attacks: Cross-site Script Attack

- If an attacker sends a crafted link to the victim with malicious JavaScript, the JavaScript will run and complete the instructions made by the attacker when the victim clicks on the link



Compromising Session IDs Using Client-side Attacks: Cross-site Script Attack

A cross-site script attack is a client-side attack in which the attacker compromises a session token by using malicious code or programs. This type of attack occurs when a dynamic web page receives malicious data from the attacker and executes it on the user's system.

Web sites that create dynamic pages do not have control over how the clients read their output. Thus, attackers can insert a malicious JavaScript, VBScript, ActiveX, Hypertext Markup Language (HTML), or Flash applet into a vulnerable dynamic page. That page then executes the script on the user's machine and collects personal information of the user, steals cookies, redirects users to unexpected web pages, or executes any malicious code on the user's system.

As shown in the below figure, a user first establishes a valid session with a server. An attacker sends a crafted link to the victim with malicious JavaScript. When the user clicks on the link, the JavaScript runs automatically and performs the instructions set by the attacker. The result displays the current session ID of the user. Using the same technique, the attacker can create specific JavaScript code that fetches the user's session ID:

```
<SCRIPT>alert(document.cookie);</SCRIPT>
```

Thereafter, the attacker uses the stolen session ID to establish a valid session with the server.

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

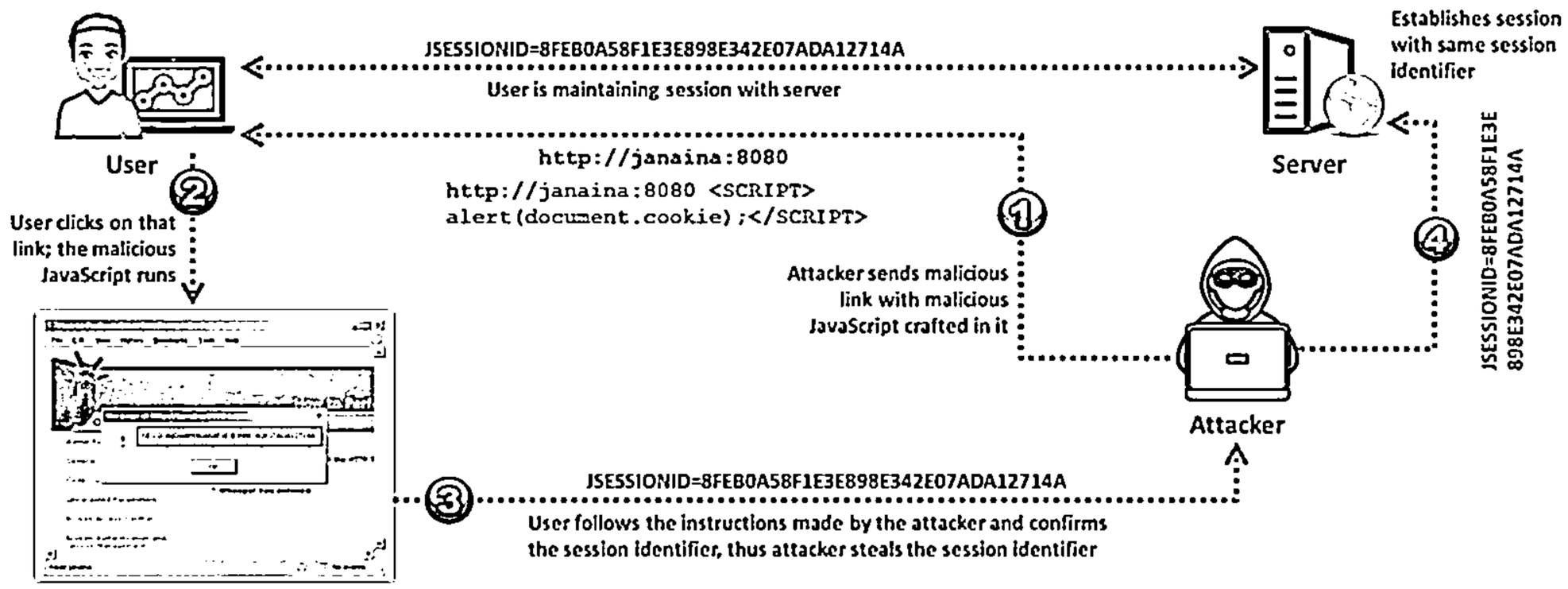
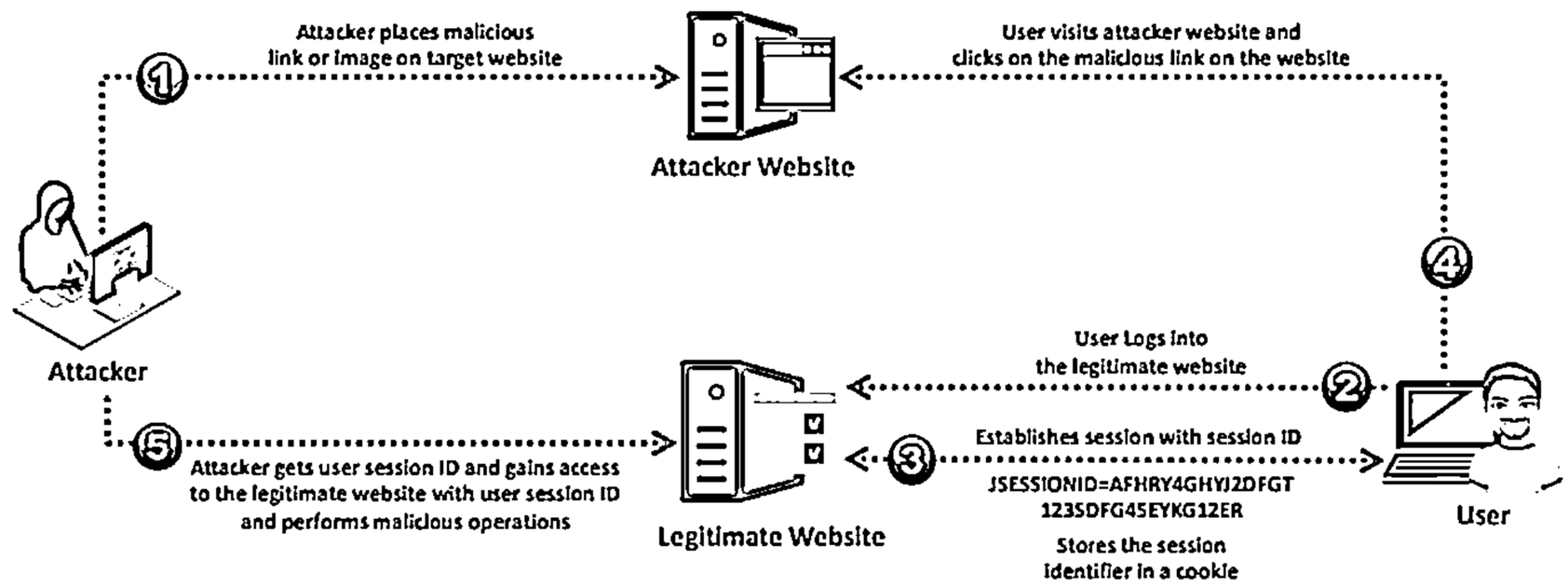


Figure 11.13: Prediction of session ID using a cross-site script attack

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

Compromising Session IDs Using Client-side Attacks: Cross-site Request Forgery Attack

- The Cross-Site Request Forgery (CSRF) attack exploits the victim's active session with a trusted site to perform malicious activities



Compromising Session IDs Using Client-side Attacks: Cross-site Request Forgery Attack

Cross-site request forgery (CSRF), also known as a one-click attack or session riding, is an attack in which the attacker exploits the victim's active session with a trusted site to perform malicious activities such as item purchases and the modification or retrieval of account information. In CSRF web attacks, the attacker creates a host form, containing malicious information, and sends it to the authorized user. The user fills in the form and sends it to the web server. Because the data originates from a trusted user, the web server accepts the data. Unlike an XSS attack, which exploits the trust a user has for a particular website, CSRF exploits the trust that a website has on a user's browser. A CSRF attack involves the following steps.

- The attacker hosts a web page with a form that appears legitimate. This page already contains the attacker's request.
- A user, believing the form to be the original, enters a login and password.
- Once the user completes the form, that page is submitted to the real site.
- The real site's server accepts the form, assuming that it was sent by the user based on the authentication credentials.

In this manner, the server accepts the attacker's request.

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

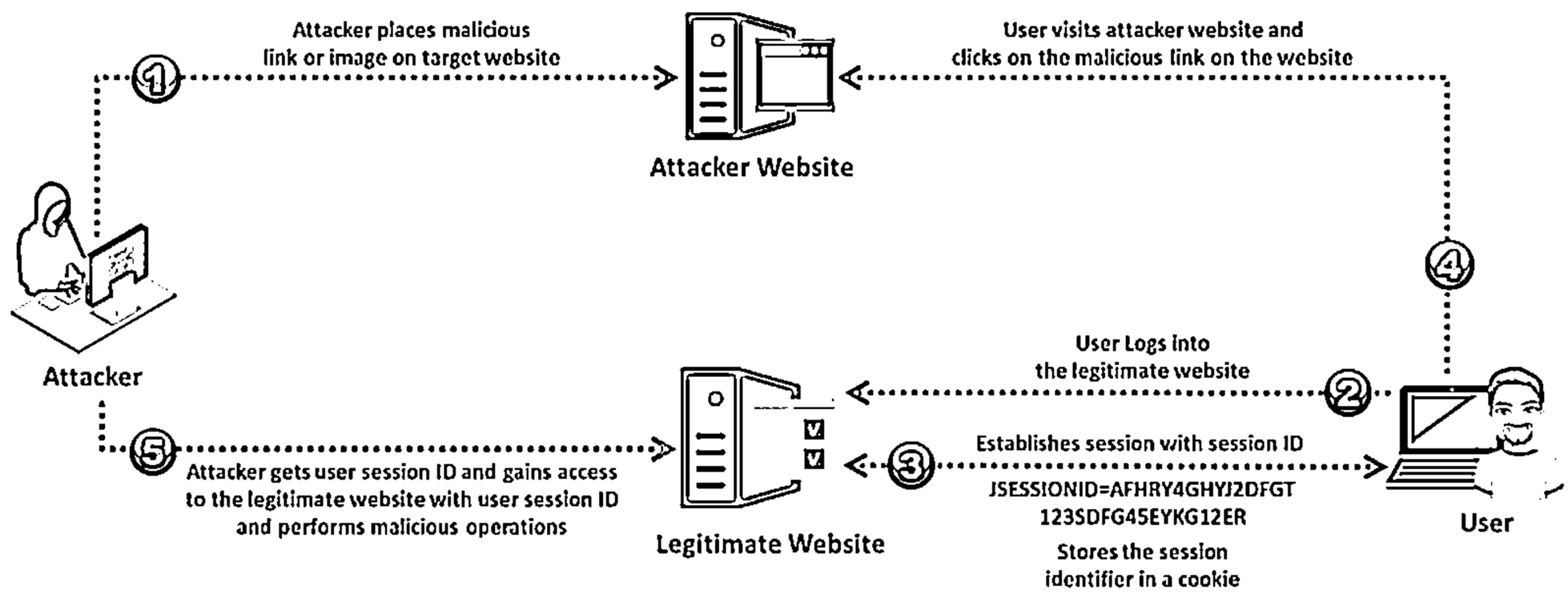
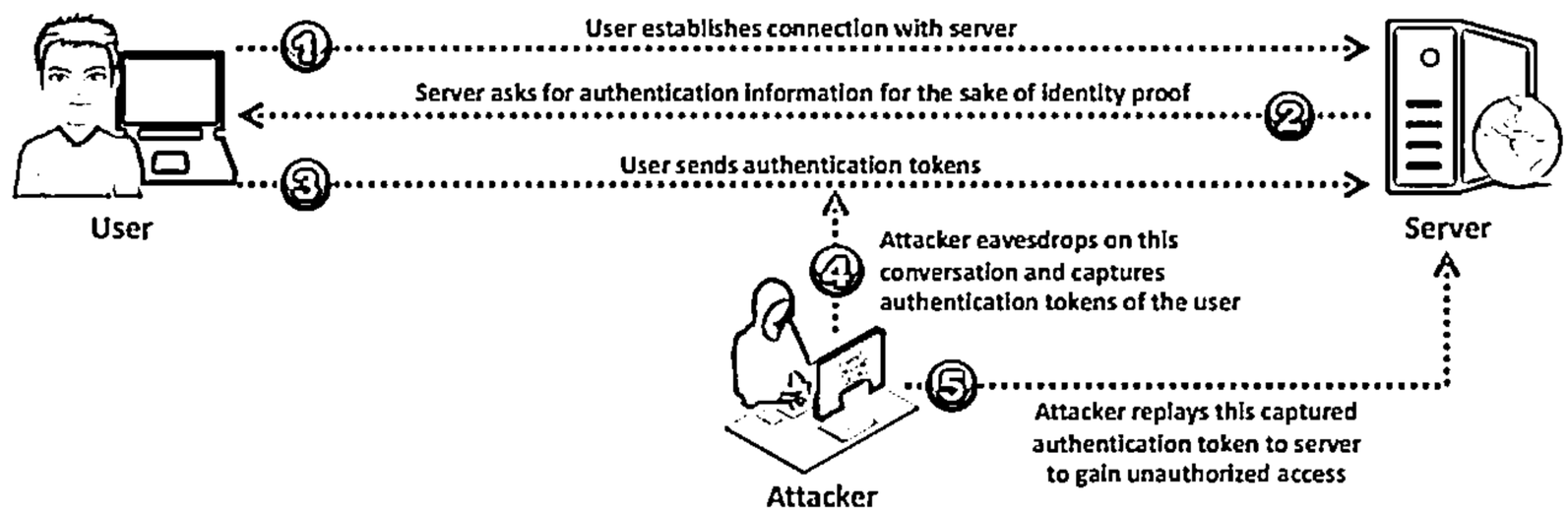


Figure 11.14: Prediction of session ID using a cross-site request forgery attack

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

Compromising Session IDs Using Session Replay Attacks

- In a session replay attack, the attacker listens to the conversation between the user and the server and captures the authentication token of the user
- Once the authentication token is captured, the attacker replays the request to the server with the captured authentication token and gains unauthorized access to the server



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

Compromising Session IDs Using Session Replay Attacks

In a session replay attack, the attacker captures the authentication token of a user by listening to a conversation between the user and server. Once the authentication token is captured, the attacker replays the authentication request to the server with the captured authentication token to dodge the server; consequently, they gain unauthorized access to the server. A session replay attack involves the following steps.

- The user establishes a connection with the web server.
- The server asks the user for authentication information as identity proof.
- The user sends authentication tokens to the server. In this step, an attacker captures the authentication token of the user by eavesdropping on the conversation between the user and server.
- Once the authentication token is captured, the attacker replays the request to the server with the captured authentication token and gains unauthorized access to the server.

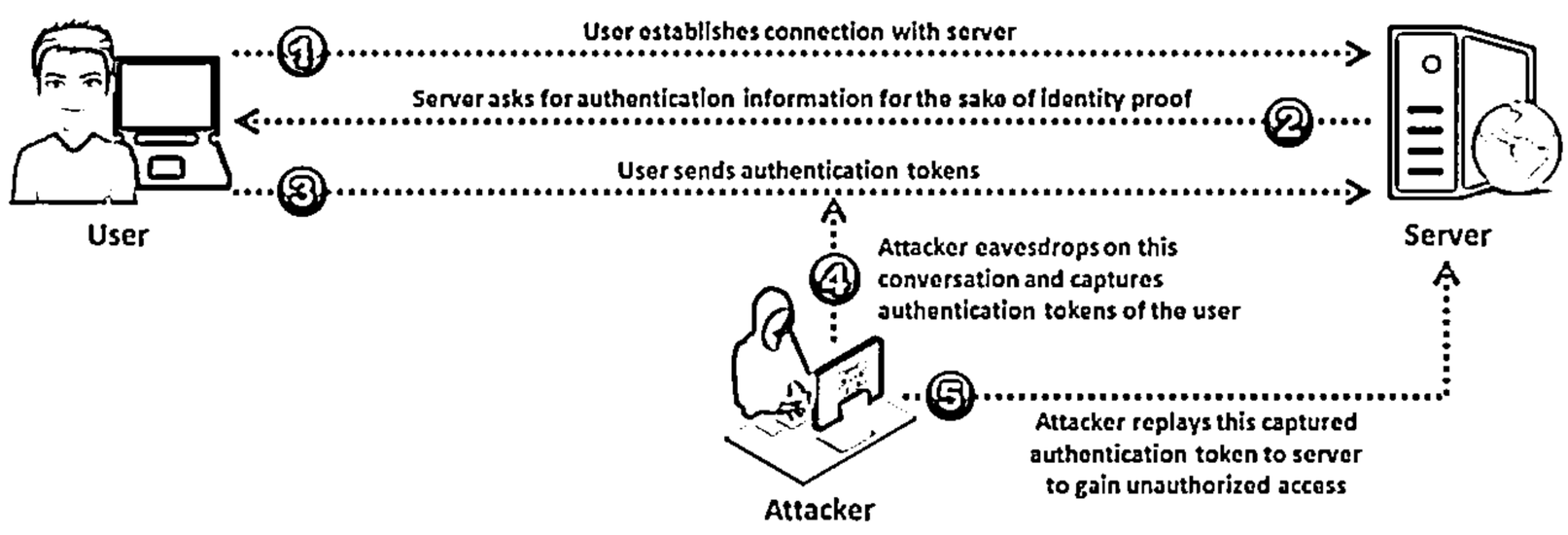


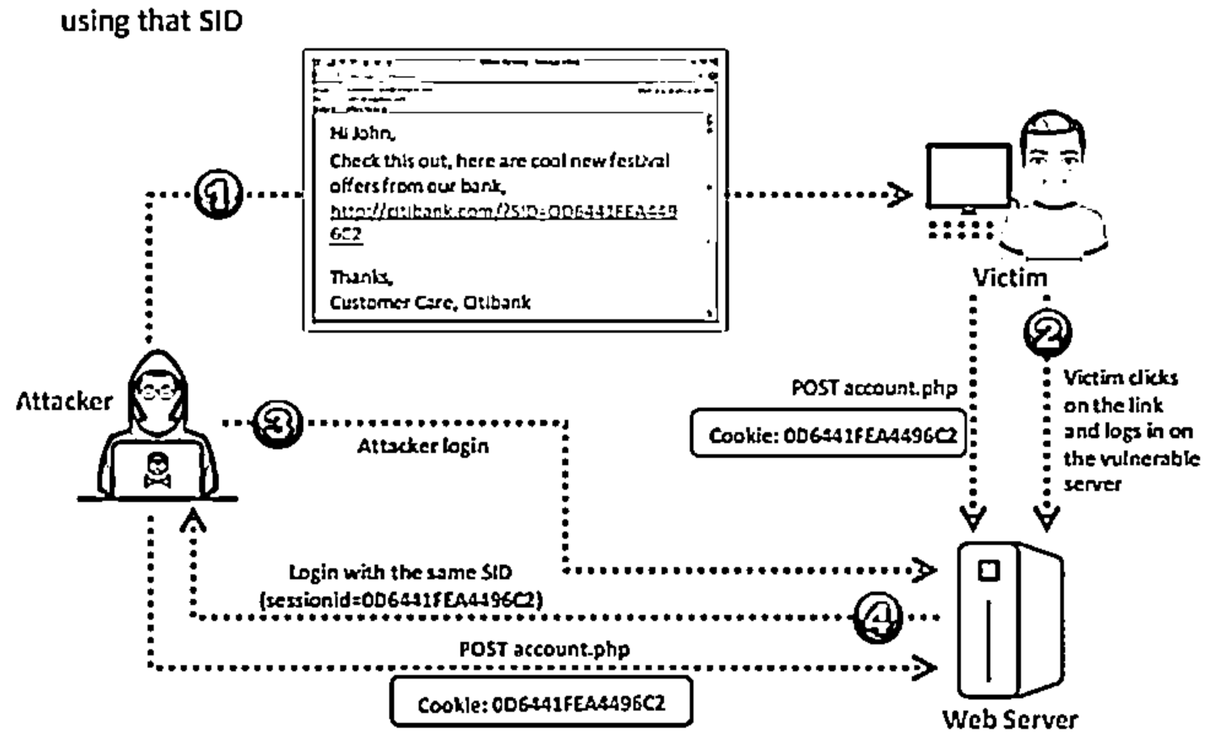
Figure 11.15: Prediction of session ID using a session replay attack

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

Compromising Session IDs Using Session Fixation

- Session fixation is an attack that allows an attacker to hijack a valid user session
- An attacker attempts to lure a user to authenticate himself or herself with a known session ID and then hijacks the user-validated session with the knowledge of the used session ID
- The attacker has to provide a legitimate web application session ID and attempt to lure the victim's browser to use it
- Some techniques for executing session fixation attacks are as follows:
  - Session token in the URL argument
  - Session token in a hidden form field
  - Session ID in a cookie

- The attacker exploits the vulnerability of a server that allows a user to use a fixed SID
- The attacker provides a valid SID to a victim and lures him or her to authenticate using that SID



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

Compromising Session IDs Using Session Fixation

Web session security prevents an attacker from intercepting, brute forcing, or predicting the session ID issued by a web server to a user's browser as proof of an authenticated session. However, this approach ignores the possibility of the attacker issuing a session ID to the user's browser, forcing it to use the chosen session ID. This type of attack is called a session fixation attack because an attacker fixes the user's session ID in advance, instead of generating it randomly at the time of login.

The attacker performs a session fixation attack to hijack a valid user session. The attacker takes advantage of limitations in web-application session ID management. Web applications allow the user to authenticate themselves using an existing session ID, instead of generating a new session ID. In this type of attack, the attacker provides a legitimate web-application session ID and lures the victim to use it. If the victim's browser uses that session ID, then the attacker can hijack the user-validated session because the attacker is already aware of the session ID used by the victim.

A session fixation attack is a kind of session hijack. However, instead of stealing the session established between a user and web server after the user logs in, a session fixation attack fixes an established session on the user's browser; thus, the attack is initiated before the user logs in. An attacker uses various techniques to perform a session fixation attack:

- Session token in the URL argument
- Session token in a hidden form field
- Session ID in a cookie

The attacker must choose a technique based on how the target web application uses session tokens. The attacker exploits the vulnerability of a server that allows a user to use a fixed

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

session ID. Then, the attacker provides a valid session ID to a victim and lures him to authenticate themselves using that session ID. A session fixation attack has the following three phases.

- **Session set-up phase:** In this phase, the attacker first obtains a legitimate session ID by establishing a connection with the target web server. Few web servers support the idle session time-out feature. If the target web server supports this feature, the attacker needs to send requests repeatedly to keep the established trap session ID alive.
- **Fixation phase:** In this phase, the attacker introduces the session ID to the victim's browser, thereby fixing the session.
- **Entrance phase:** In this phase, the attacker waits for the victim to log in to the target web server using the trap session ID and then enters the victim's session.

A session fixation attack is performed through the following steps.

- First, the attacker establishes a legitimate connection with the target web server.
- The target web server (e.g., *http://citibank.com/*) issues a session ID, say 0D6441FEA4496C2, to the attacker.
- The attacker sends a link with the established session ID, say *http://citibank.com/?SID=0D6441FEA4496C2*, to the victim and lures the victim to click on it to access the website.
- The victim clicks on the link, believing it to be a legitimate link sent by the bank. This opens the server's login page in the victim's browser for SID=0D6441FEA4496C2.
- The web server checks that the session ID 0D6441FEA4496C2 is already established and is in an active state; hence, it does not create the new session.
- Finally, the victim enters their login credentials in the login script, and the server grants them access to the bank account.
- At this point, knowing the session ID, the attacker can also access the victim's bank account via *http://citibank.com/? SID=0D6441FEA4496C2*.

Because the session ID is set by the attacker before the user logged in, the user can be said to have logged into the attacker's session.

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

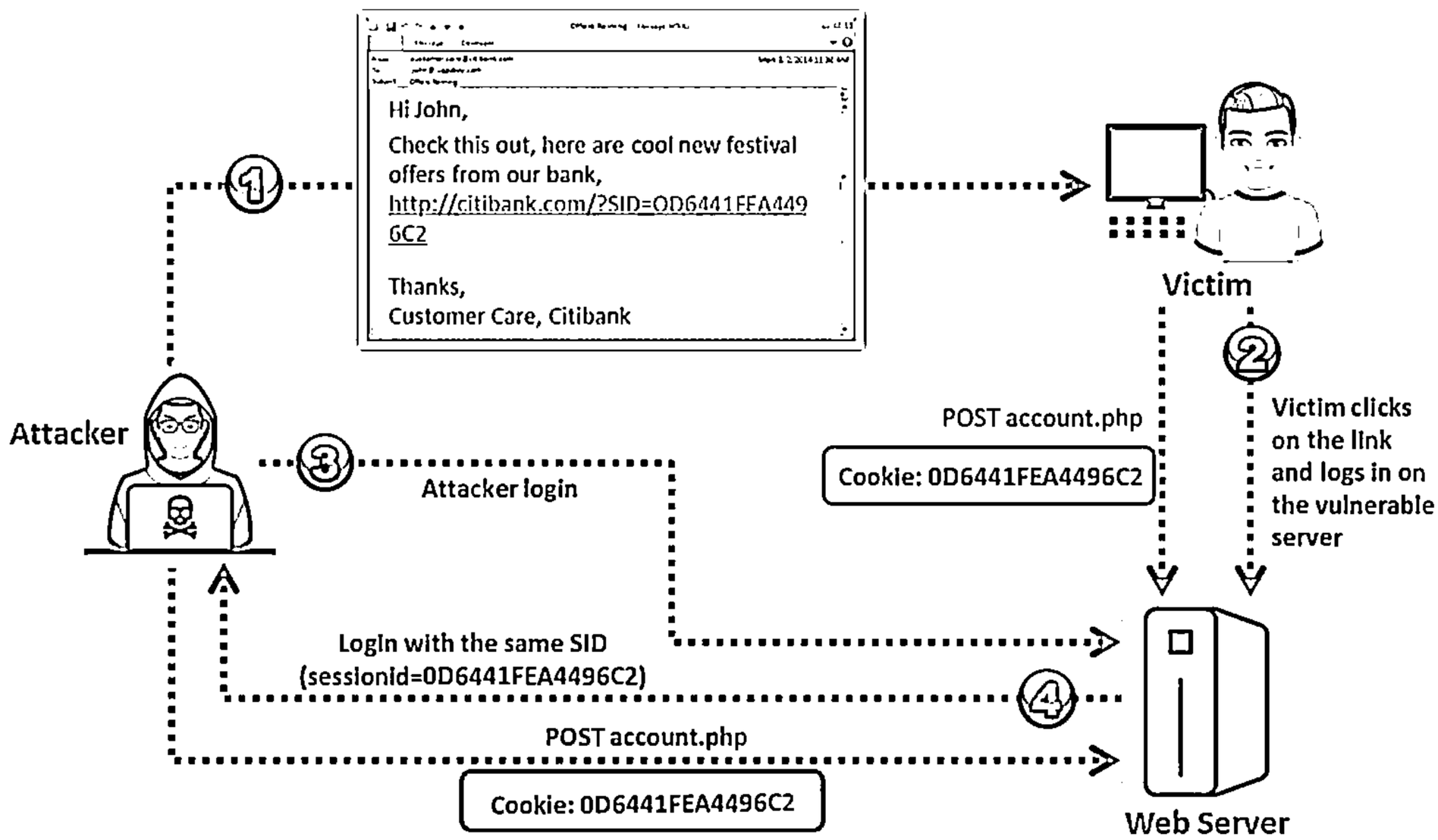
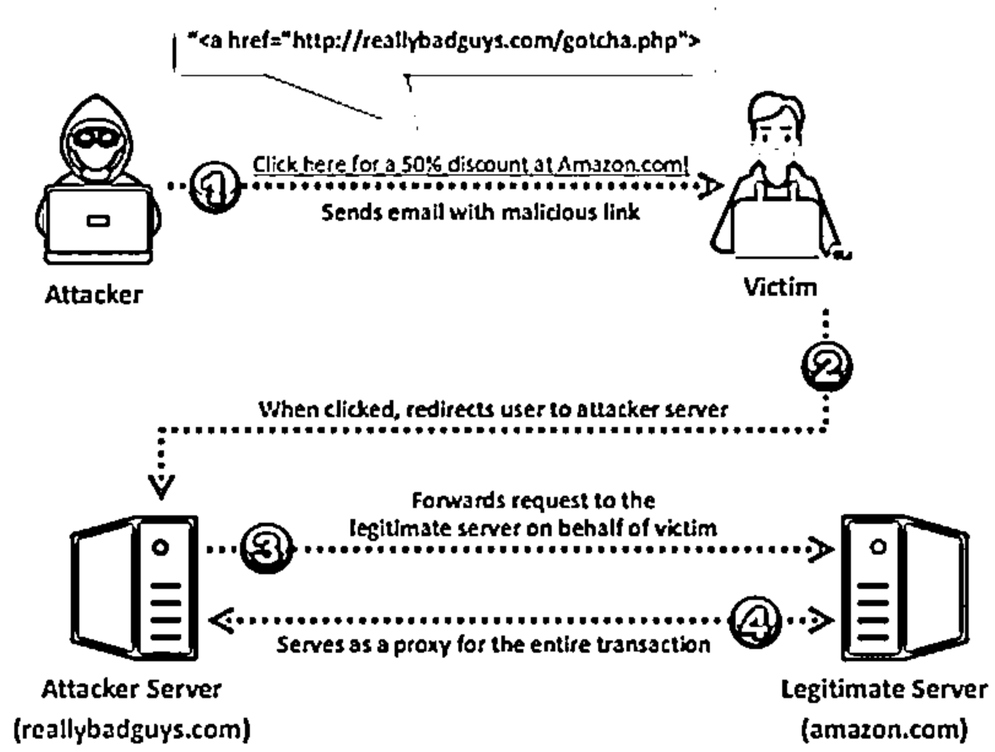


Figure 11.16: Session fixation attack

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

Session Hijacking Using Proxy Servers

- An attacker lures the victim to click on a bogus link, which looks legitimate but redirects the user to the attacker server
- The attacker forwards the request to the legitimate server on behalf of the victim and serves as a proxy for the entire transaction
- The attacker then captures the session's information during the interaction of the legitimate server and user



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

Session Hijacking Using Proxy Servers

An attacker lures the victim to click on a fake link, which appears legitimate but redirects the user to the attacker's server. The attacker then forwards the request to the legitimate server on behalf of the victim and serves as a proxy for the entire transaction. Acting as a proxy, the attacker captures the session information during the interaction between the legitimate server and user.

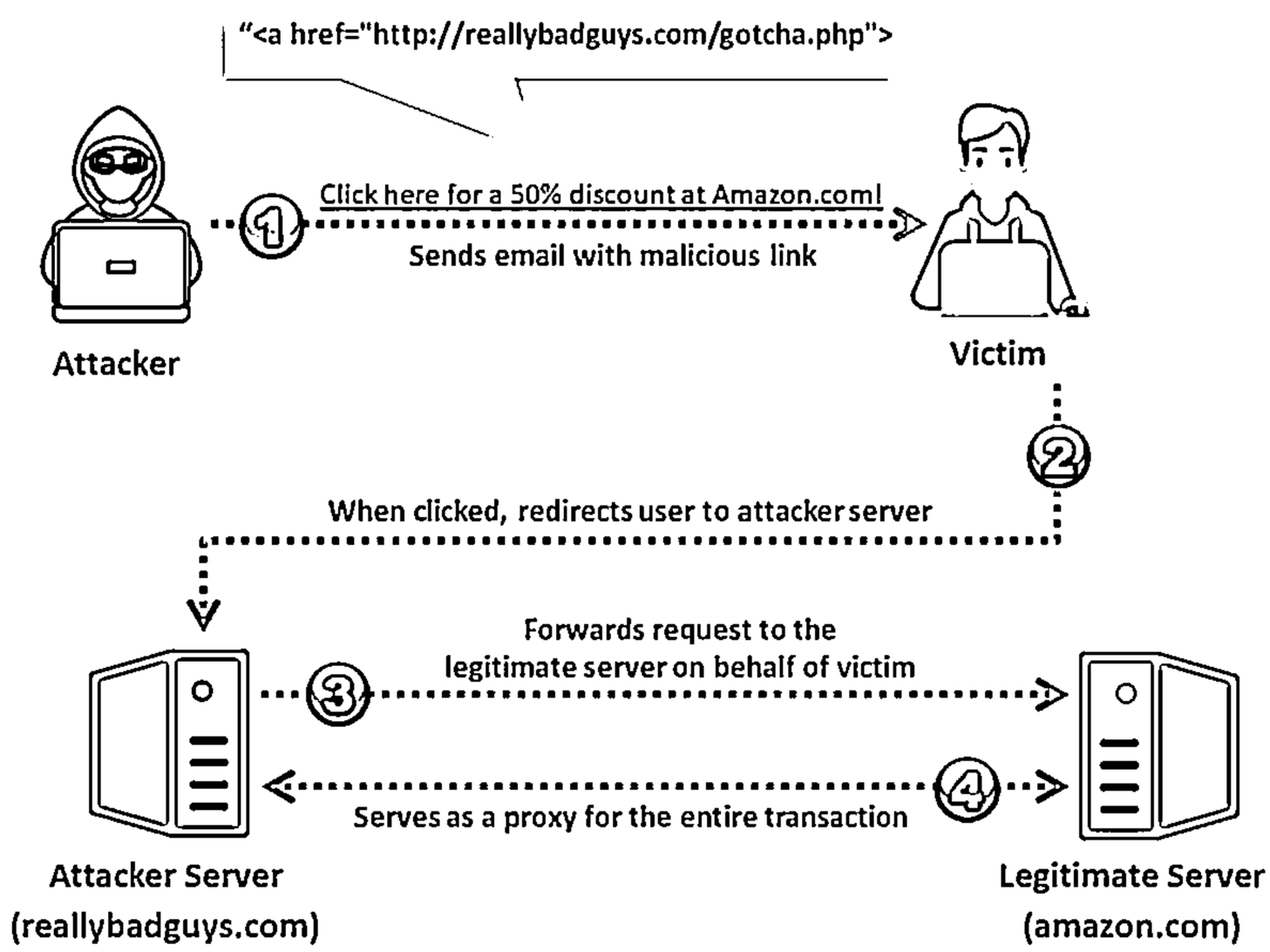
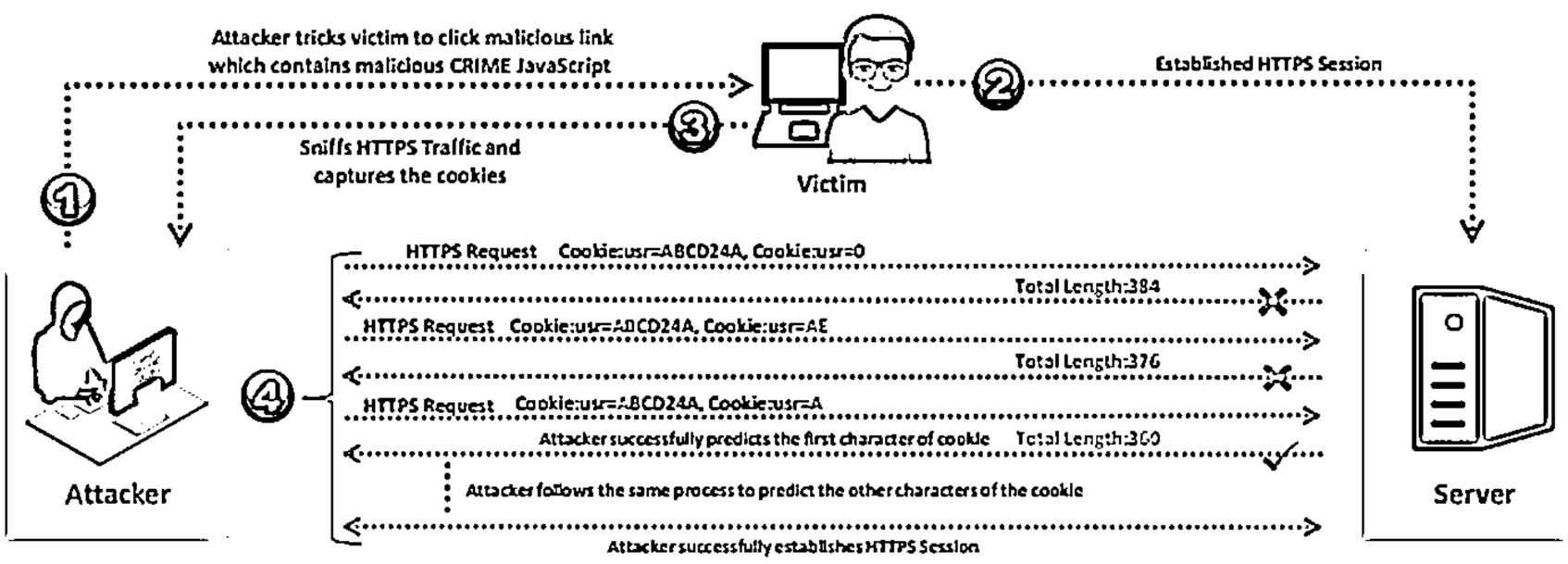


Figure 11.17: Session hijacking using proxy servers

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

Session Hijacking Using CRIME Attack

- Compression Ratio Info-Leak Made Easy (CRIME) is a client-side attack that exploits the vulnerabilities present in the data compression feature of protocols, such as SSL/TLS, SPDY, and HTTPS
- Attackers hijack the session by decrypting secret session cookies
- The authentication information obtained from the session cookies is used to establish a new session with the web application



Session Hijacking Using CRIME Attack

Compression Ratio Info-Leak Made Easy (CRIME) is a client-side attack that exploits vulnerabilities in the data-compression feature of protocols such as SSL/Transport Layer Security (TLS), SPDY, and HTTP Secure (HTTPS). The possibility of mitigation against HTTPS compression is low, which makes this vulnerability even more dangerous than other compression vulnerabilities.

When two hosts on the Internet establish a connection using HTTPS, a TLS session is established, and the data are transmitted in an encrypted form. Hence, it is difficult for an attacker to read or modify the messages between the two hosts. When a user logs into a web application, authentication data are stored in a cookie. Whenever the browser sends an HTTPS request to the web application, the stored cookie is used for authentication. In this attack, the attacker attempts to access the authentication cookie to hijack the victim's session.

In HTTPS, cookies are compressed using a lossless data compression algorithm (DEFLATE) and then encrypted. Hence, it is difficult for an attacker to obtain the value of the cookie with simple sniffing.

To perform a CRIME attack, an attacker must use social engineering techniques to trick the victim into clicking on a malicious link. When the victim clicks on the malicious link, it either injects malicious code into the victim's system or redirects the victim to a malicious website. If the victim has already established an HTTPS connection with a secured web application, the attacker sniffs the victim's HTTPS traffic using techniques such as ARP spoofing. Through sniffing, the attacker captures the cookie value from the HTTPS messages and sends multiple HTTPS requests to the web application with that cookie prepended with a few random characters. Subsequently, the attacker monitors the traffic between the victim and web application to obtain the compressed and encrypted value of the cookie. After capturing the

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

cookie, the attacker analyzes the cookie length and predicts the actual value of the authentication cookie.

After obtaining the authentication cookie, the attacker impersonates the victim and hijacks the victim's session with the secure web application to steal confidential information such as passwords, social security numbers, and credit card numbers. Attackers use tools such as CrimeCheck to detect whether a web server has TLS or HTTP compression enabled and are thus vulnerable to CRIME attacks.

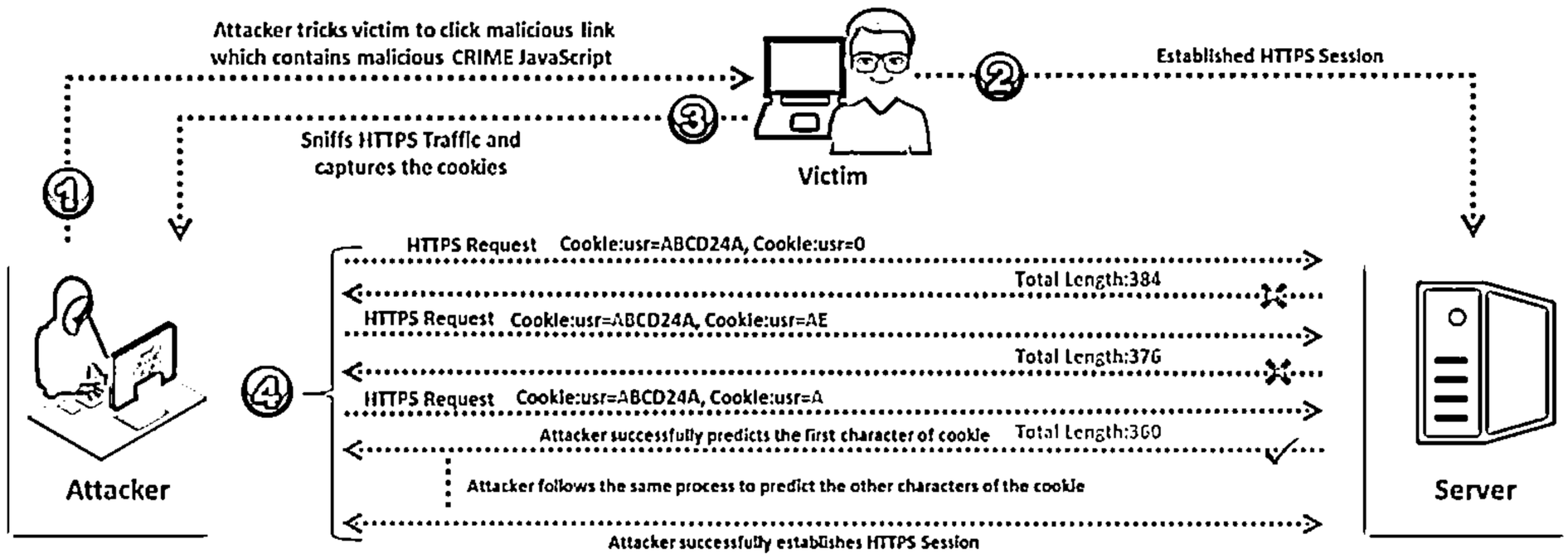
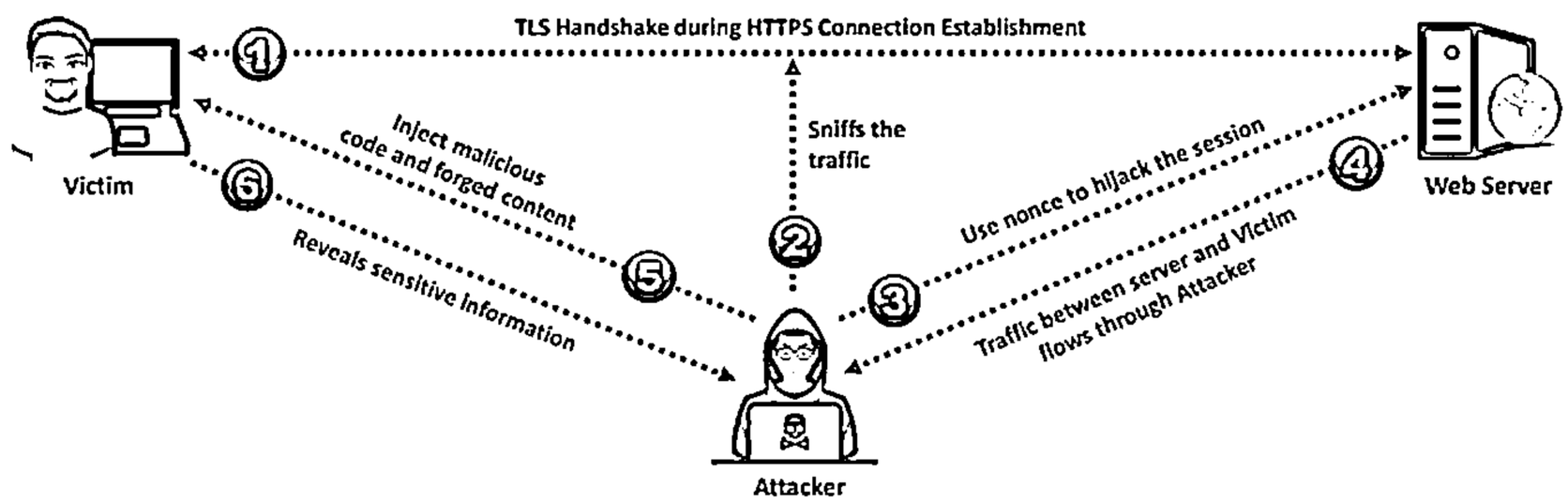


Figure 11.18: Session hijacking using a CRIME attack

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

Session Hijacking Using Forbidden Attack

- A forbidden attack is a type of man-in-the-middle attack used to hijack HTTPS sessions
- It exploits the reuse of cryptographic nonce during the TLS handshake
- After hijacking the HTTPS session, the attackers inject malicious code and forged content that prompts the victim to disclose sensitive information, such as bank account numbers, passwords, and social security numbers



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

Session Hijacking Using Forbidden Attack

A forbidden attack is a type of MITM attack that can be executed when a cryptographic nonce is reused while establishing an HTTPS session with a server. According to the TLS specification, these arbitrary pieces of data must be used once. This attack exploits the vulnerability that the TLS implementation incorrectly reuses the same nonce when data are encrypted using the Advanced Encryption Standard–Galois/Counter Mode (AES-GCM) during the TLS handshake. Attackers exploit this vulnerability to perform an MITM attack by generating cryptographic keys used for authentication. Repeating the same nonce during the TLS handshake allows an attacker to monitor and hijack the connection. After hijacking the HTTPS session and bypassing the protection, attackers inject malicious code and forged content into the transmission, such as JavaScript code or web fields that prompt the user to disclose passwords, social security numbers, or other confidential information. A forbidden attack involves the following steps.

- The attacker monitors the connection between the victim and web server and sniffs the nonce from the TLS handshake messages.
- The attacker generates authentication keys using the nonce and hijacks the connection.
- All the traffic between the victim and web server flows through the attacker's machine.
- The attacker injects JavaScript code or web fields into the transmission towards the victim.
- The victim reveals sensitive information such as bank account numbers, passwords, and social security numbers to the attacker.

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

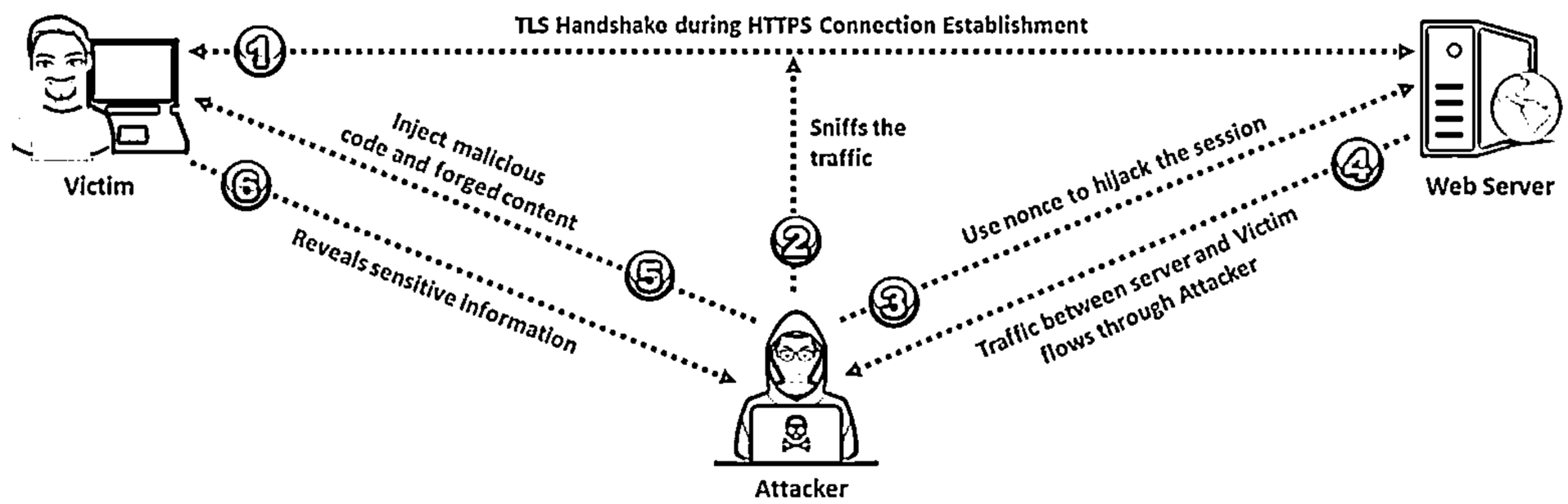
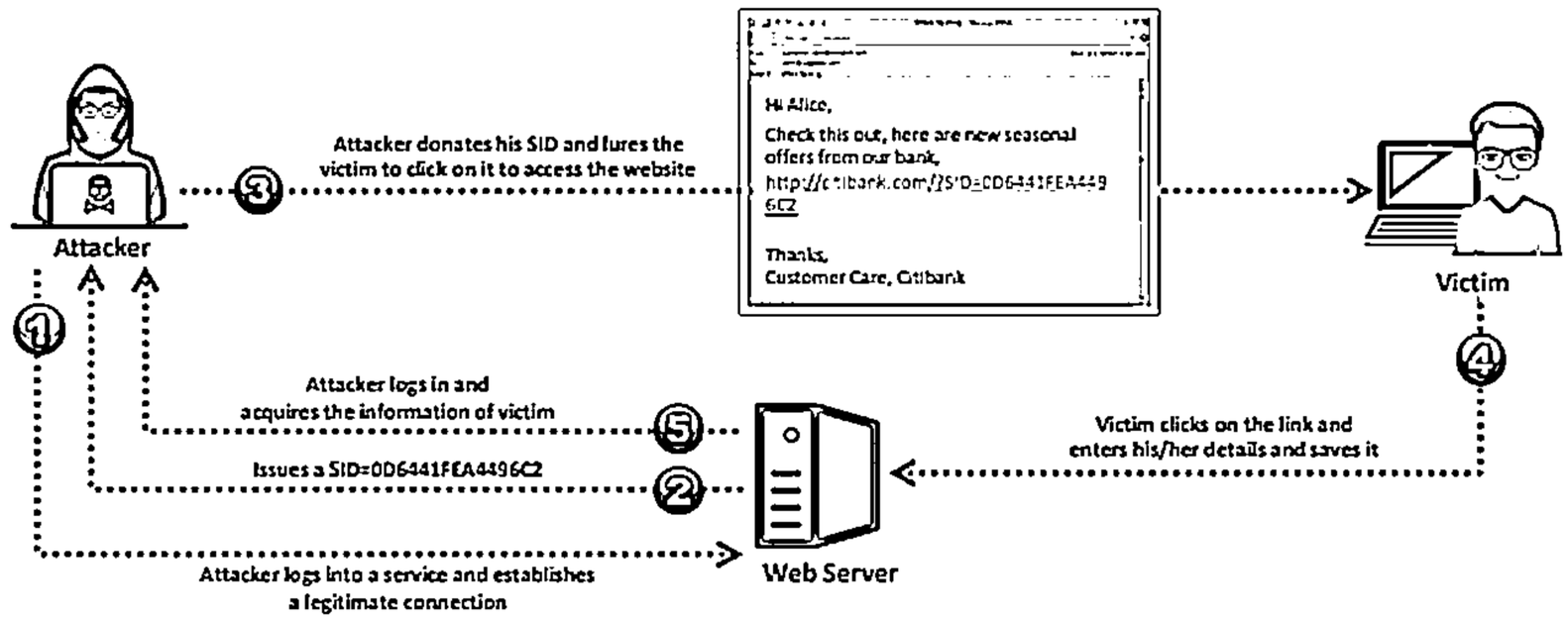


Figure 11.19: Session hijacking using a forbidden attack

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

Session Hijacking Using Session Donation Attack

- In a session donation attack, an attacker donates his/her own session identifier (SID) to the target user
- The attacker first obtains a valid SID by logging into a service and later feeds the same SID to the target user
- This SID links a target user back to the attacker's account page without any information to the victim



Session Hijacking Using Session Donation Attack

In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation. A session donation attack involves the following steps.

- First, the attacker logs into a service, establishes a legitimate connection with the target web server, and deletes the stored information.
- The target web server (e.g., *http://citibank.com/*) issues a session ID, say 0D6441FEA4496C2, to the attacker.
- The attacker then donates their session ID, say *http://citibank.com/?SID=0D6441FEA4496C2*, to the victim and lures the victim to click on it to access the website.
- The victim clicks on the link, believing it to be a legitimate link sent by the bank. This opens the server's page in the victim's browser with SID=0D6441FEA4496C2. Finally, the victim enters their information in the page and saves it.
- The attacker can now login as themselves and acquire the victim's information.

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

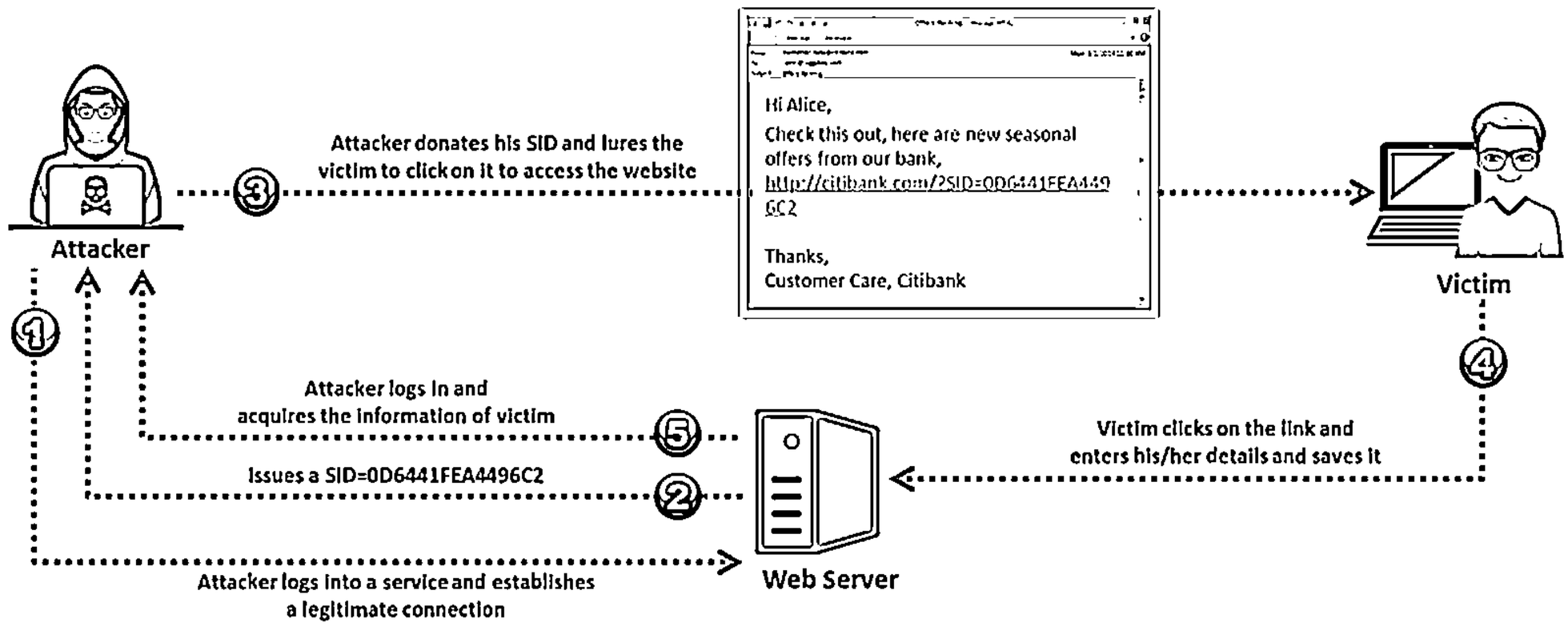


Figure 11.20: Session hijacking using a session donation attack

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

Module Flow

01	Session Hijacking Concepts
03	Network Level Session Hijacking
02	Application Level Session Hijacking
04	Session Hijacking Tools
05	Countermeasures

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

Network Level Session Hijacking

1. The network level hijacking relies on hijacking transport and Internet protocols used by web applications in the application layer
2. By attacking the network level sessions, the attacker gathers some critical information, which are used to attack the application level sessions

Network level hijacking includes:

1. Blind hijacking
2. UDP hijacking
3. TCP/IP hijacking
6. RST hijacking
7. Man-in-the-middle: Packet sniffer
8. IP spoofing: Source routed packets

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

Network Level Session Hijacking

Attackers especially focus on network level session hijacking because it does not require host access, in contrast to host-level session hijacking, or a need to tailor their attacks on a per-application basis, in contrast to application level hijacking.

This section discusses network level session hijacking, concepts related to network communications, and various techniques used to perform network level session hijacking.

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

Network level hijacking relies on hijacking transport and Internet protocols used by web applications in the application layer. By attacking network level sessions, the attacker gathers some critical information that is used to attack application level sessions.

The following are different types of network level hijacking:

- Blind hijacking
- UDP hijacking
- TCP/IP hijacking
- RST hijacking
- Man-in-the-middle: packet sniffer
- IP spoofing: source routed packets

Three-way Handshake

When two parties establish a connection using TCP, they perform a three-way handshake. A three-way handshake starts the connection and exchanges all the parameters needed for the two parties to communicate. TCP uses a three-way handshake to establish a new connection.

Initially, the client-side connection is in the closed state and the server-side in the listening state. The client initiates the connection by sending the initial sequence number (ISN) and setting the SYN flag. The client is now in the SYN-SENT state.

When the server receives this packet, it acknowledges the client sequence number and sends its own ISN with the SYN flag set. The server's state is now SYN-RECEIVED. On receipt of this packet, the client acknowledges the server sequence number by incrementing it and setting the ACK flag. The client is now in the established state. At this point, the two machines have established a session and can communicate.

On receiving the client's acknowledgement, the server enters the established state and sends an acknowledgment, incrementing the client's sequence number. The connection can be closed either by using the FIN or RST flag or through a time out.

If the RST flag of a packet is set, the receiving host enters the CLOSED state and frees all resources associated with this connection. This leads to the connection drop of any additional incoming packets.

If the packet is sent with the FIN flag turned on, the receiving host closes the connection because it enters the CLOSE-WAIT state. The packets sent by the client are accepted in an established connection if the sequence number is within the range and follows its predecessor.

If the sequence number is beyond the range of the acceptable sequence numbers, it drops the packet and sends an ACK packet using the expected sequence number.

For the three parties to communicate, the following information is required:

- IP address
- Port numbers
- Sequence numbers

It is easy for an attacker to determine the IP address and port number; these are available in the IP packets, which do not change throughout the session. However, the sequence numbers change. Therefore, the attacker must successfully guess the sequence numbers for a blind

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

hijack. If the attacker can fool the server into receiving their spoofed packets and executing them, the attacker is successful in hijacking the session.

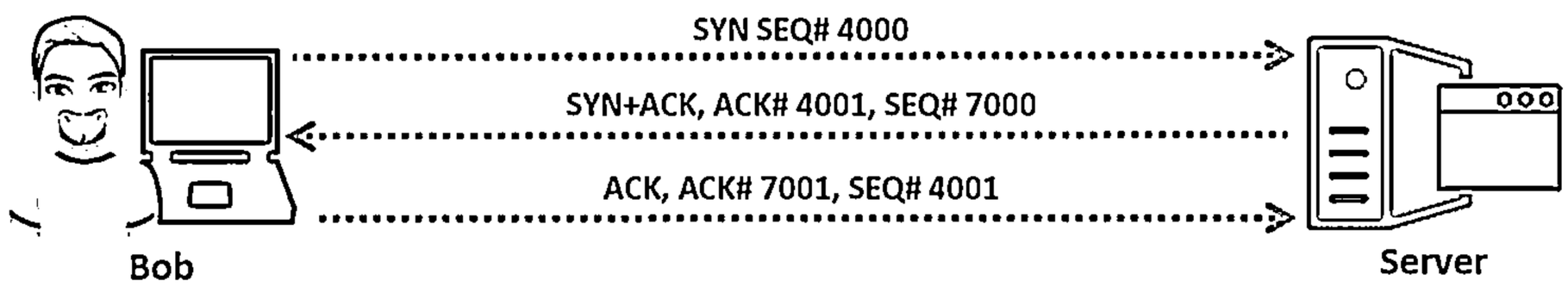


Figure 11.21: Three-way handshake

The three-way handshake shown in the above figure involves the following steps.

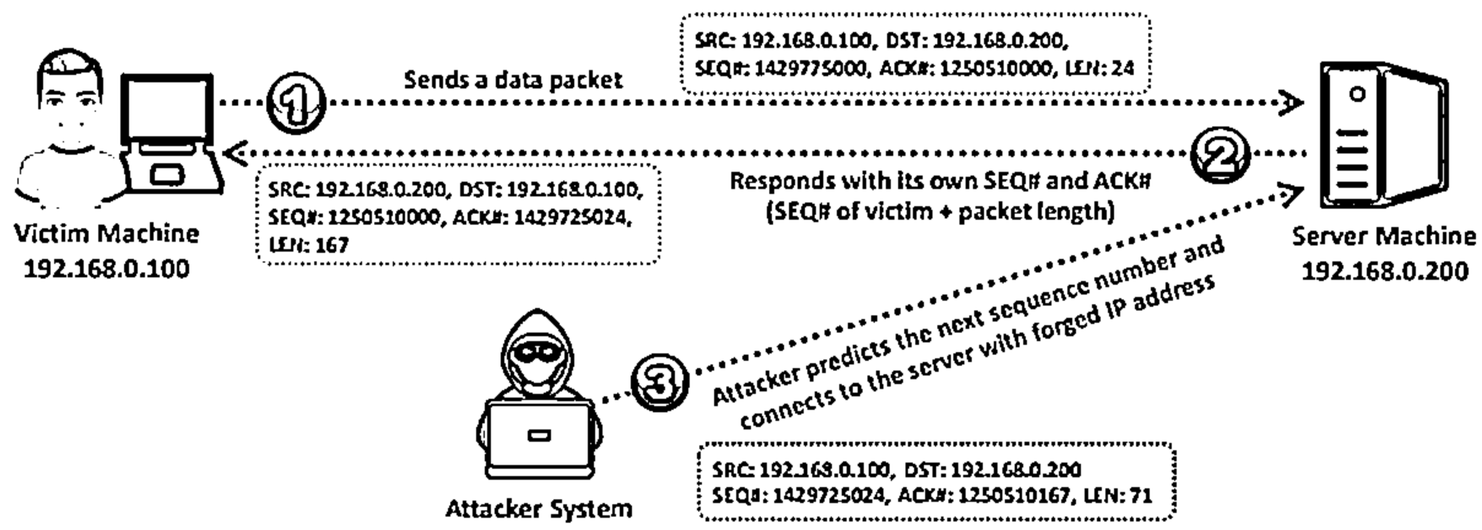
1. Bob initiates a connection with the server and sends a packet to the server with the SYN flag set.
2. The server receives this packet and sends a packet with the SYN + ACK flag and an initial sequence number (ISN) for the server.
3. Bob sets the ACK flag acknowledging the receipt of the packet and increments the sequence number by 1.
4. The two machines have successfully established a session.

If the attacker can anticipate the next sequence number and ACK number that Bob will send, they can spoof Bob's address and start communication with the server.

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

TCP/IP Hijacking

- TCP/IP hijacking involves using spoofed packets to seize control of a connection between a victim and target machine
- A victim's connection hangs, and an attacker is then able to communicate with the host's machine as if the attacker is the victim
- To launch a TCP/IP hijacking attack, the attacker must be on the same network as the victim
- The target server and the victim machines can be located anywhere



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

TCP/IP Hijacking

In TCP/IP hijacking, an attacker intercepts an established connection between two communicating parties by using spoofed packets and then pretends to be one of those parties. In this approach, the attacker uses spoofed packets to redirect the TCP traffic to their own machine. Once this is successful, the victim's connection hangs, and the attacker is able to communicate with the host's machine on behalf of the victim. To launch a TCP/IP hijacking attack, both the victim and attacker must be on the same network. The target server and the victim machines can be located anywhere. By using this technique, an attacker can easily attack systems that use one-time passwords. As illustrated in the below figure, TCP/IP hijacking involves the following processes.

- The hacker sniffs the communication between the victim and host to obtain the victim's ISN.
- By using this ISN, the attacker sends a spoofed packet from the victim's IP address to the host system.
- The host machine responds to the victim, assuming that the packet arrived from it. This increments the sequence number.

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

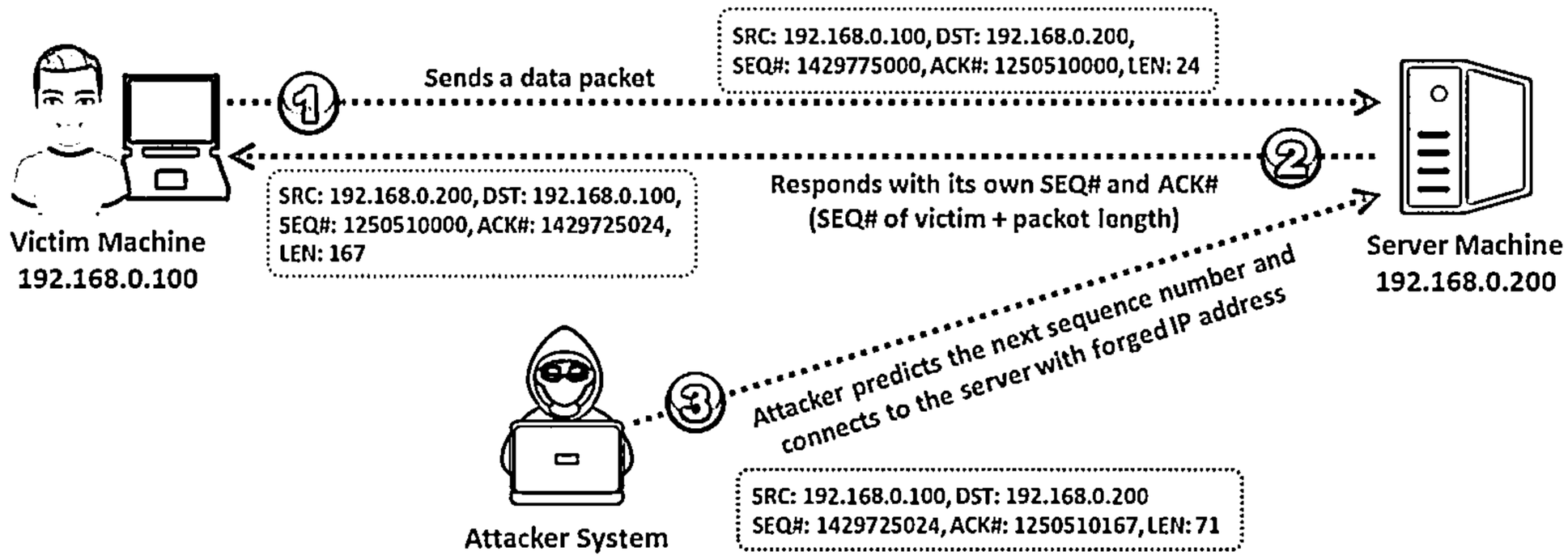


Figure 11.22: TCP/IP hijacking process

TCP/IP hijacking is performed through the following steps.

- The attacker sniffs the victim's connection and uses the victim's IP address to send a spoofed packet with the predicted sequence number.
- The receiver processes the spoofed packet, increments the sequence number, and sends an acknowledgement to the victim's IP address.
- The victim machine is unaware of the spoofed packet. Therefore, it ignores the receiver machine's ACK packet and turns off sequence number count.
- Consequently, the receiver receives packets with the incorrect sequence number.
- The attacker forces the victim's connection with the receiver machine into a desynchronized state.
- The attacker tracks sequence numbers and continuously spoofs packets that originate from the victim's IP address.
- The attacker continues to communicate with the receiver machine, while the victim's connection hangs.

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

IP Spoofing: Source Routed Packets

1. The packet source routing technique is used for gaining unauthorized access to a computer with the help of a trusted host's IP address
2. An attackers spoofs the host's IP address so that the server managing a session with the host accepts the packets from the attacker
3. When the session is established, the attacker injects forged packets before the host responds to the server
4. The original packet from the host is lost as the server receives the packet with a sequence number already used by the attacker
5. The packets from the attacker are source-routed through the host with the destination IP specified by the attacker

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

IP Spoofing: Source Routed Packets

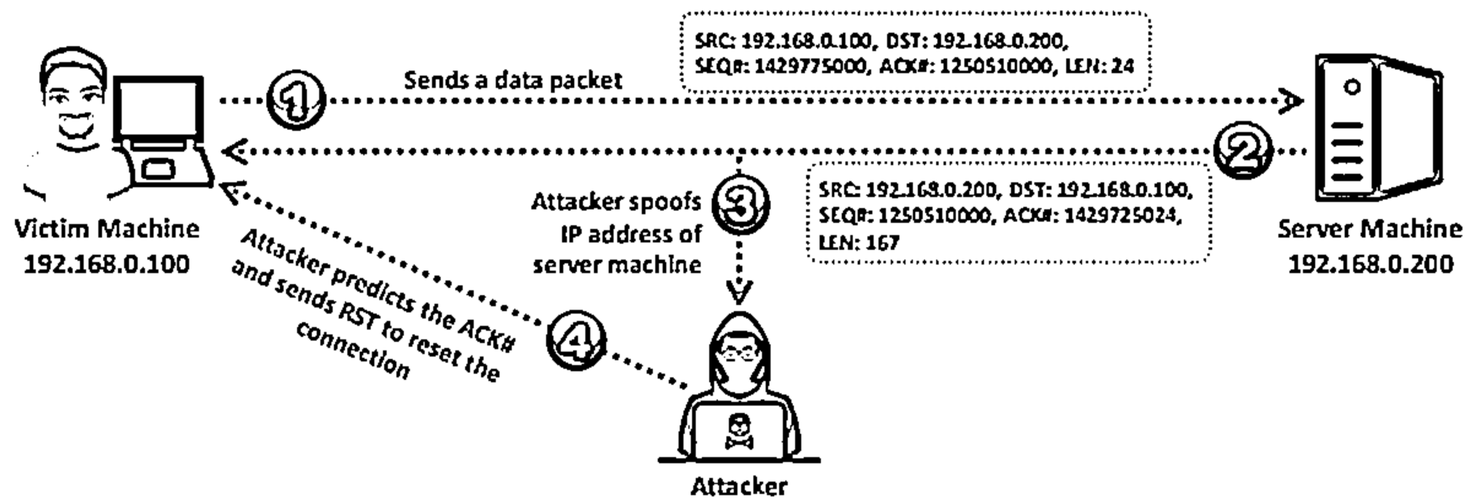
Source routed packets are useful in gaining unauthorized access to a computer with the help of a trusted host's IP address. This type of hijack allows attackers to create their own acceptable packets to insert into a TCP session. First, an attacker spoofs a trusted host's IP address so that the server managing a session with the host accepts the packets from the attacker. The packets are source routed; therefore, the sender specifies the path for packets from the source to the destination IP. By using this source-routing technique, attackers fool the server into believing that it is communicating with the user.

After spoofing the IP address successfully, the hijacker alters the sequence and acknowledgment numbers. Once these numbers are changed, the attacker injects forged packets into the TCP session before the client can respond. This leads to a desynchronized state because there the sequence and ACK numbers are not synchronized. The original packets are lost, and the server receives a packet with the new ISN. These packets are source routed to a patched destination IP address specified by the attacker.

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

RST Hijacking

- RST hijacking involves injecting an authentic-looking reset (RST) packet using a spoofed source address and predicting the acknowledgment number
- A hacker can reset a victim's connection if it uses an accurate acknowledgment number
- The victim would believe that the source sent the reset packet, and reset the connection
- RST Hijacking can be performed using a packet crafting tool, such as Colasoft Packet Builder, and TCP/IP analysis tools, such as tcpdump



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

RST Hijacking

RST hijacking involves injecting an authentic-looking reset (RST) packet by using a spoofed source IP address and predicting the acknowledgment number. The hacker can reset the victim's connection if it uses an accurate acknowledgment number. The victim believes that the source has sent the reset packet and resets the connection. RST hijacking can be performed using packet-crafting tools such as Colasoft Packet Builder and TCP/IP analysis tools such as tcpdump.

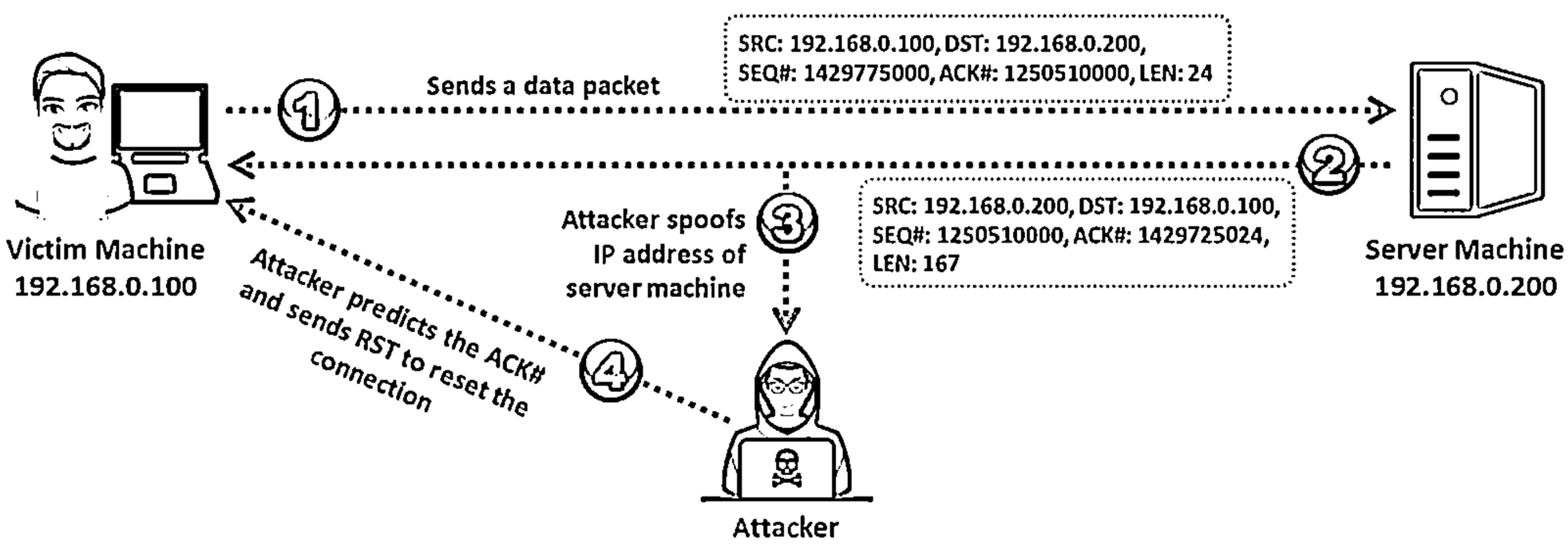


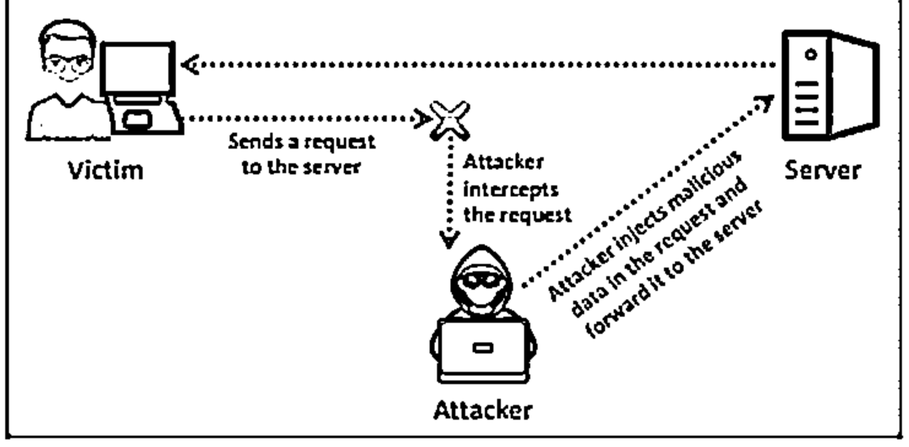
Figure 11.23: RST hijacking process

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

Blind and UDP Hijacking

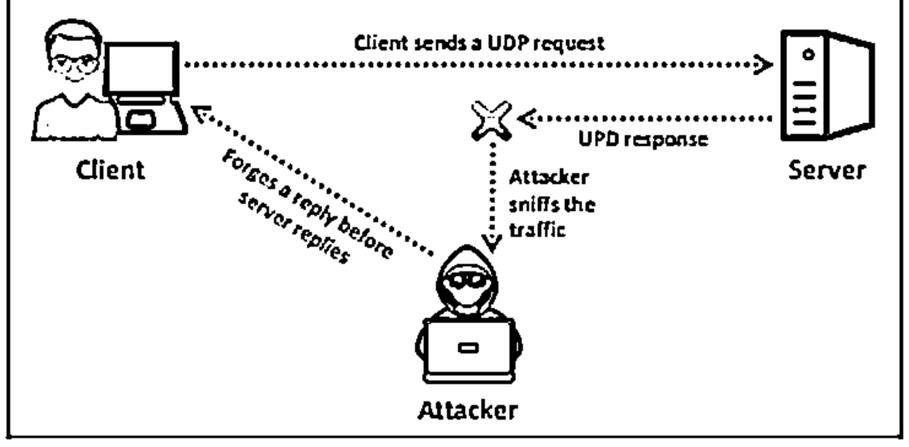
Blind Hijacking

- An attacker can inject malicious data or commands into the intercepted communications in the TCP session even if the source-routing is disabled
- The attacker can send the data or commands but has no access to see the response



UDP Hijacking

- A network-level session hijacking where the attacker sends forged server reply to a victim's UDP request before the intended server replies to it
- The attacker uses a man-in-the-middle attack to intercept the server's response to the client and sends a forged reply



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

Blind Hijacking

In blind hijacking, an attacker can inject malicious data or commands into intercepted communications in a TCP session, even if the victim disables source routing. For this purpose, the attacker must correctly guess the next ISN of a computer attempting to establish a connection. Although the attacker can send malicious data or a command, such as a password setting to allow access from another location on the network, the attacker cannot view the response. To be able to view the response, an MITM attack is a much better option.

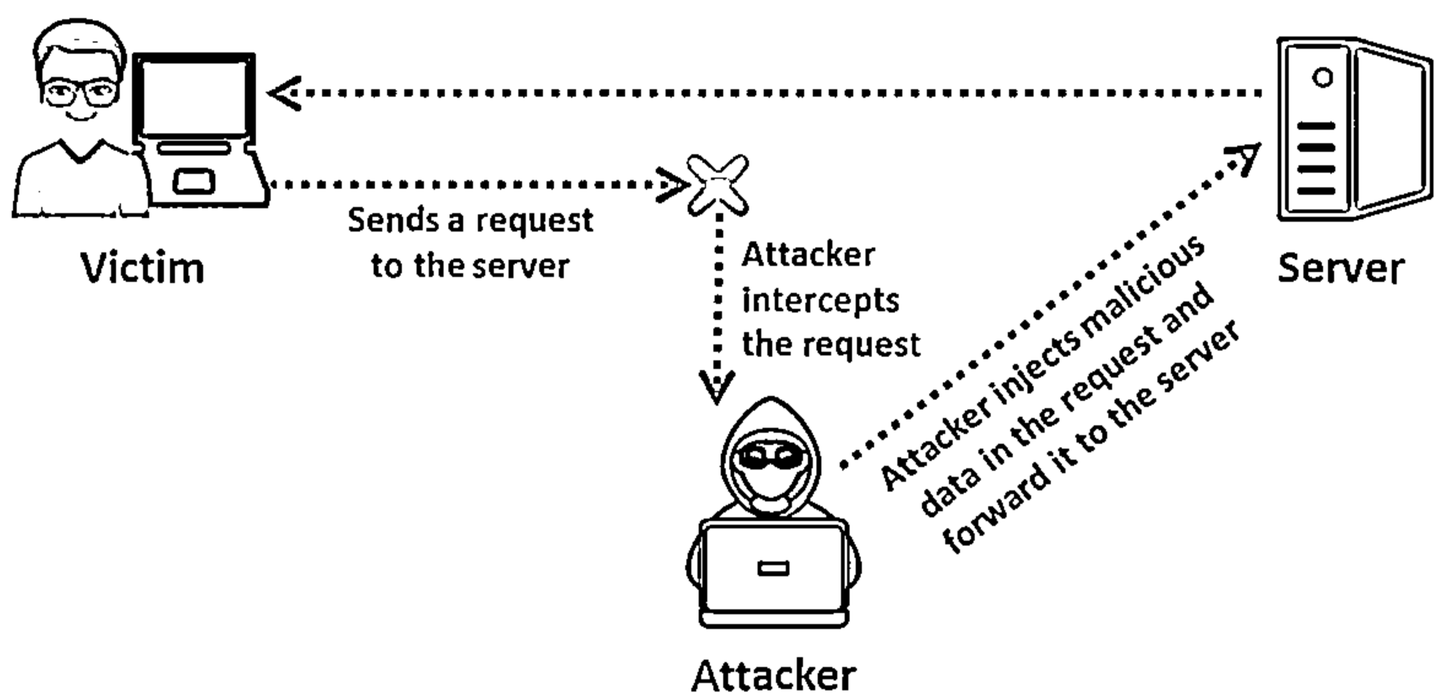


Figure 11.24: Blind hijacking process

UDP Hijacking

The User Datagram Protocol (UDP) does not use packet sequencing or synchronizing. Therefore, a UDP session can be attacked more easily than a TCP session. Because UDP is connectionless, it is easy to modify data without the victim noticing. In network level session hijack, the hijacker forges a server reply to a client UDP request before the server can respond. Thus, the attacker

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

takes control of the session. No packets are exchanged between the server and client, because the server's sequence number fails to match the client's acknowledgement number.

The server's reply can be easily restricted if sniffing is used. An MITM attack in UDP hijacking can minimize the task of the attacker because it can stop the server's reply from reaching the client in the first place.

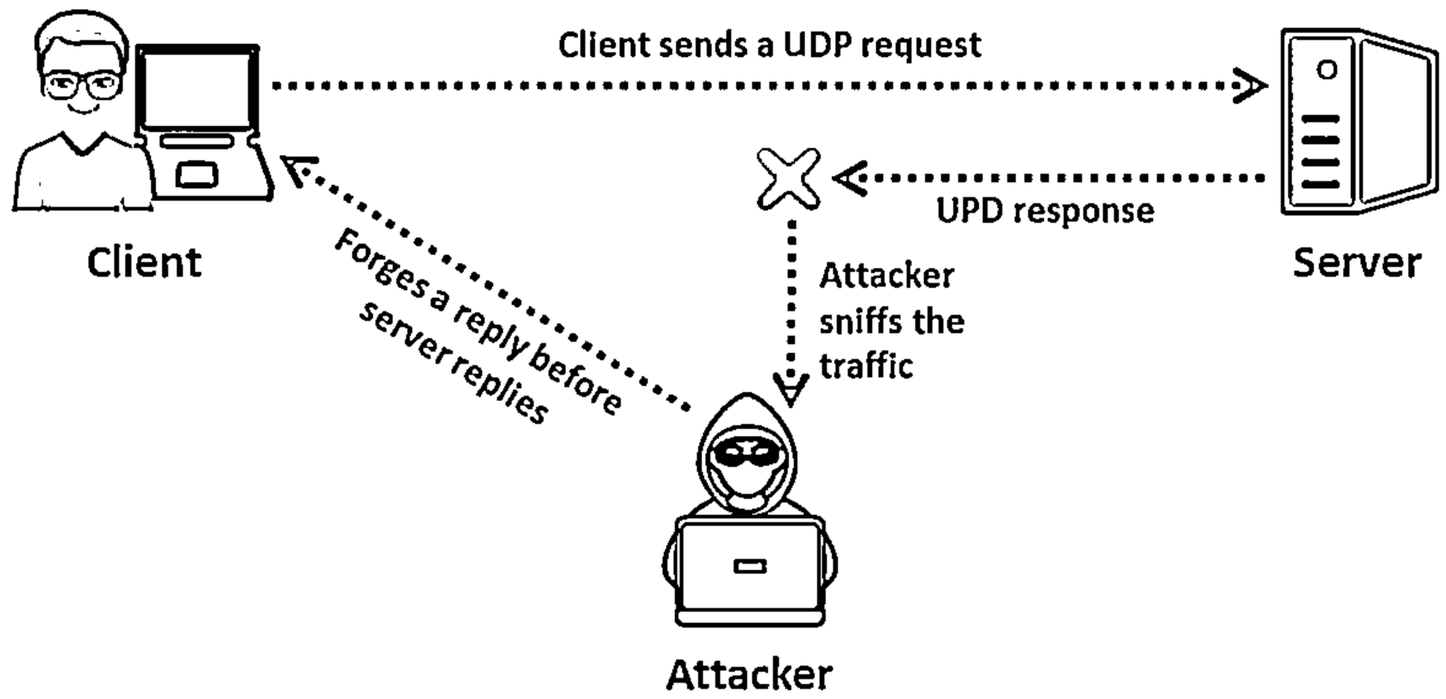
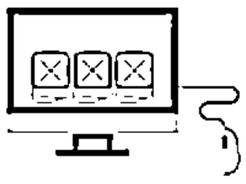


Figure 11.25: Hijacking a UDP session

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

MiTM Attack Using Forged ICMP and ARP Spoofing

- In this attack, the packet sniffer is used as an interface between the client and server
- An attacker changes the default gateway of the client's machine and attempts to reroute packets
- The packets between the client and server are routed through the hijacker's host using two techniques, as shown below:



Forged Internet Control Message Protocol (ICMP)

- It is an extension of IP to send error messages where the attacker can send messages to fool the client and server

Address Resolution Protocol (ARP) Spoofing

- ARP is used to map the network layer addresses (IP address) to link layer addresses (MAC address)

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

MITM Attack Using Forged ICMP and ARP Spoofing

An MITM attack uses a packet sniffer to intercept communication between a client and server. The attacker changes the default gateway of the client's machine and attempts to reroute packets. The packets between the client and server are routed through the hijacker's host by using the following two techniques.

- **Forged Internet Control Message Protocol (ICMP)**

  The Internet Control Message Protocol (ICMP) is an extension of IP used to send error messages. An attacker can use ICMP to send messages to fool the client and server. In this technique, ICMP packets are forged to redirect traffic between the client and host through the hijacker's host. The hacker's packets send error messages indicating problems in processing packets through the original connection. This fools the server and client into routing through the hijacker's path instead.

- **Address Resolution Protocol (ARP) Spoofing**

  Hosts use Address Resolution Protocol (ARP) tables to map local network layer addresses (IP addresses) to hardware addresses or MAC addresses. This technique involves fooling the host by broadcasting the ARP request and changing its ARP tables by sending forged ARP replies. The attacker sends forged ARP replies that update the ARP tables of the host that is broadcasting ARP requests. This routes the traffic to the attacker's host instead of the legitimate IP address.

In both techniques, an attacker routes the packets in transit between the client and server through their machine.

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

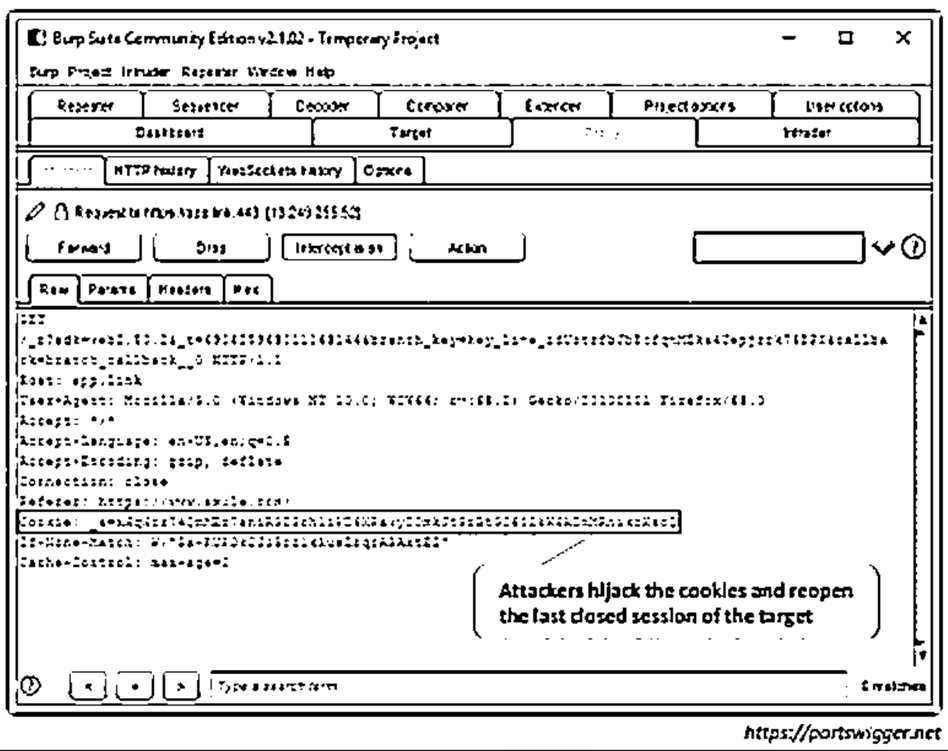
Module Flow

01	Session Hijacking Concepts
03	Network Level Session Hijacking
02	Application Level Session Hijacking
04	Session Hijacking Tools
05	Countermeasures

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

Session Hijacking Tools

Burp Suite | Burp Suite allows an attacker to inspect and modify traffic between the browser and target application



https://portswigger.net

OWASP ZAP
https://www.owasp.org

bettercap
https://www.bettercap.org

netool toolkit
https://sourceforge.net

WebSploit Framework
https://sourceforge.net

sslstrip
https://pypi.python.org

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

Session Hijacking Tools

Attackers can use tools such as Burp Suite, OWASP ZAP, and bettercap to hijack a session between a client and server. This section discusses various tools that help perform session hijacking.

- **Burp Suite**

  Source: *https://portswigger.net*

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

Burp Suite is an integrated platform for the security testing of web applications. It allows attackers to inspect and modify traffic between a browser and target application.

Burp Suite contains the following key components.

- An intercepting proxy, which allows the user to inspect and modify traffic between their browser and the target application
- An application-aware spider that crawls content and functionality
- An advanced web application scanner that automates the detection of numerous types of vulnerability
- An intruder tool for performing powerful customized attacks to find and exploit unusual vulnerabilities
- A repeater tool for manipulating and resending individual requests
- A sequencer tool for testing the randomness of session tokens
- The CSRF PoC Generator function, which generates proof-of-concept cross-site request forgery (CSRF) attacks for a given request

As shown in the figure, attackers can use this tool to capture a session cookie of a victim and later use that cookie to reopen a closed session of the victim.

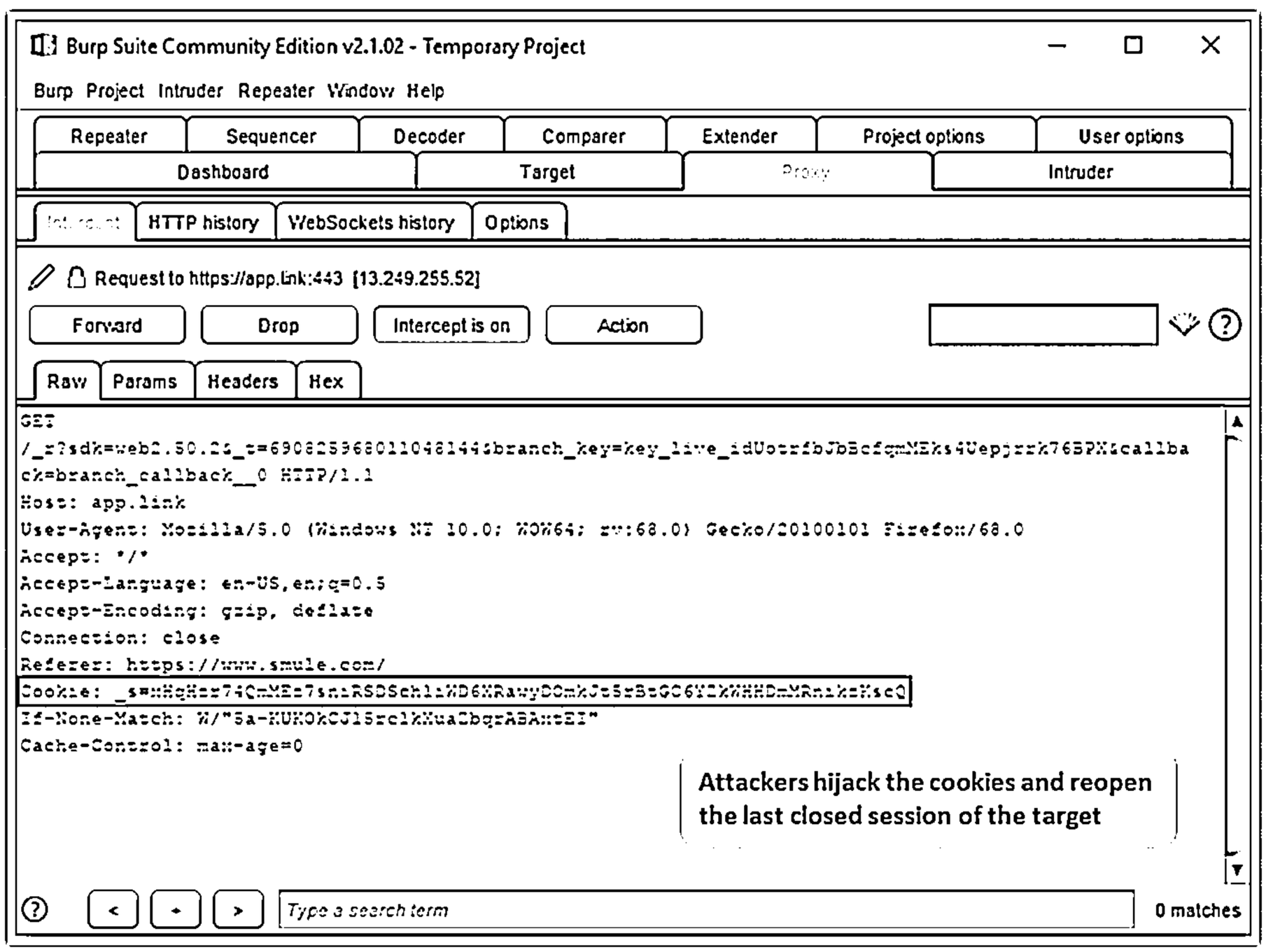


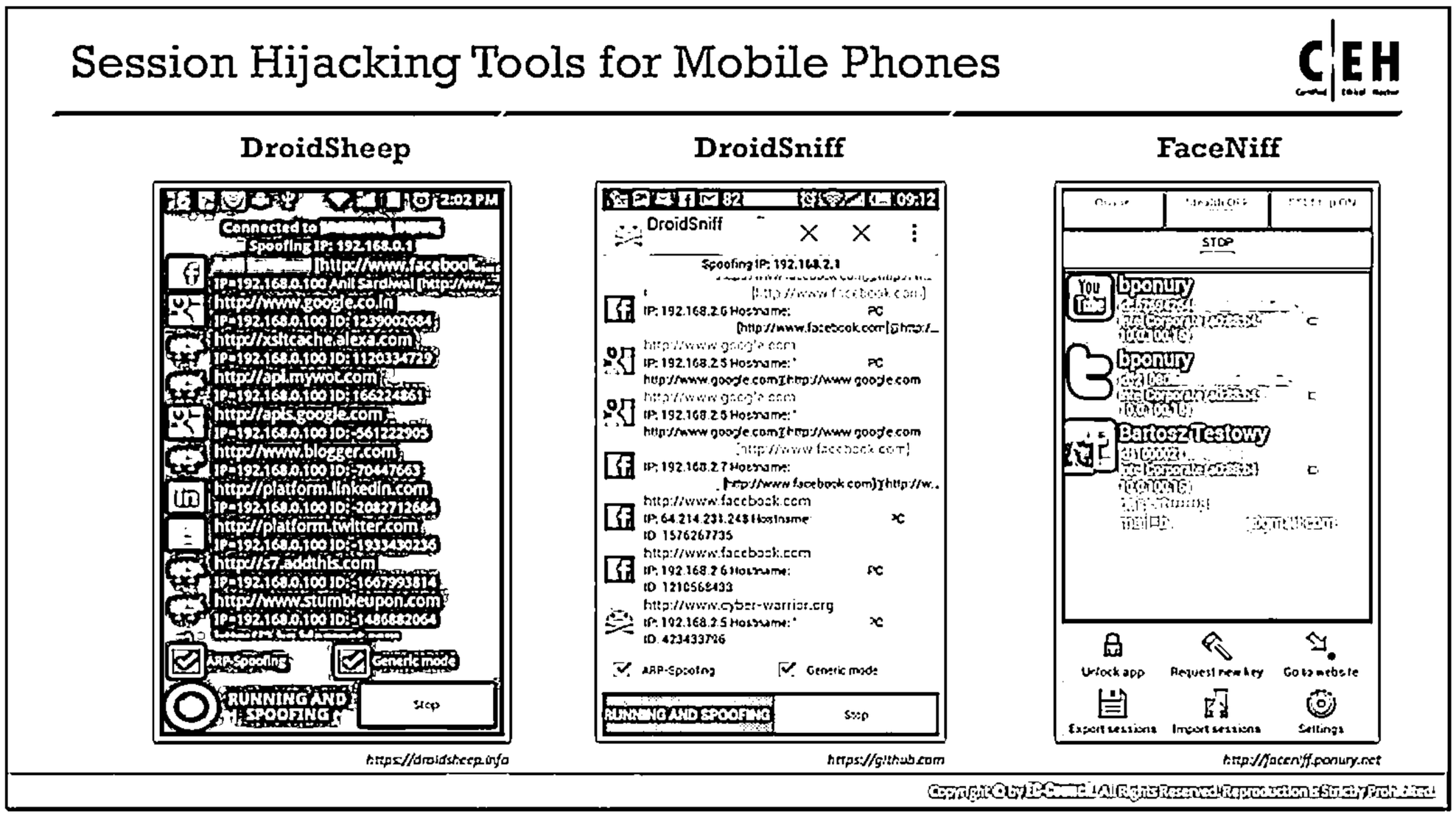
Figure 11.26: Screenshot of Burp Suite

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

The following are some additional session hijacking tools:

- OWASP ZAP (*https://www.owasp.org*)
- bettercap (*https://www.bettercap.org*)
- netool toolkit (*https://sourceforge.net*)
- WebSploit Framework (*https://sourceforge.net*)
- sslstrip (*https://pypi.python.org*)

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



Session Hijacking Tools for Mobile Phones

- **DroidSheep**

  Source: *https://droidsheep.info*

  The DroidSheep tool is used for session hijacking on Android devices connected to a common wireless network. It obtains the session ID of active users on the Wi-Fi network and uses it to access a website as an authorized user. A DroidSheep user can easily observe the activities of authorized users on websites. It can also hijack social accounts by obtaining the session ID.

Figure 11.27: Screenshot of DroidSheep

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

- **DroidSniff**

  Source: *https://github.com*

  DroidSniff is an Android app for security analysis in wireless networks that can capture Facebook, Twitter, LinkedIn, and other accounts. This tool is used for testing the security of user accounts. It identifies the poor security properties of network connections without encryption.

Figure 11.28: Screenshot of DroidSniff

- **FaceNiff**

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

  FaceNiff is an Android app that allows a user to sniff and intercept web-session profiles over the WiFi network that the user's mobile device is connected to. Although FaceNiff can hijack sessions only when the WiFi network does not use the Extensible Authentication Protocol (EAP), it works on any private network, including open, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access–pre-shared key (WPA-PSK), and WPA2-PSK networks.

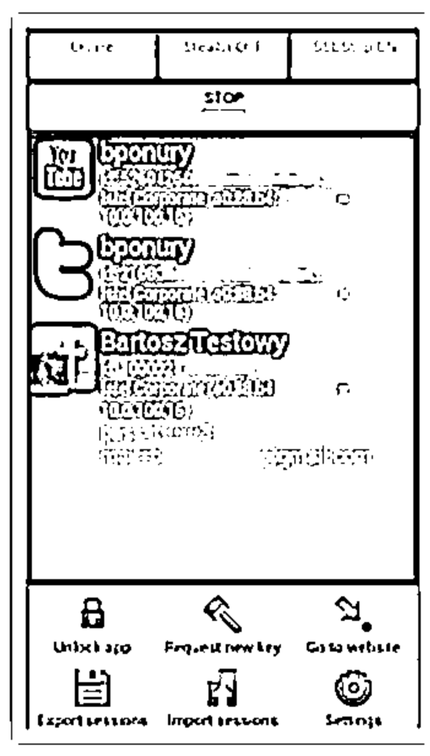
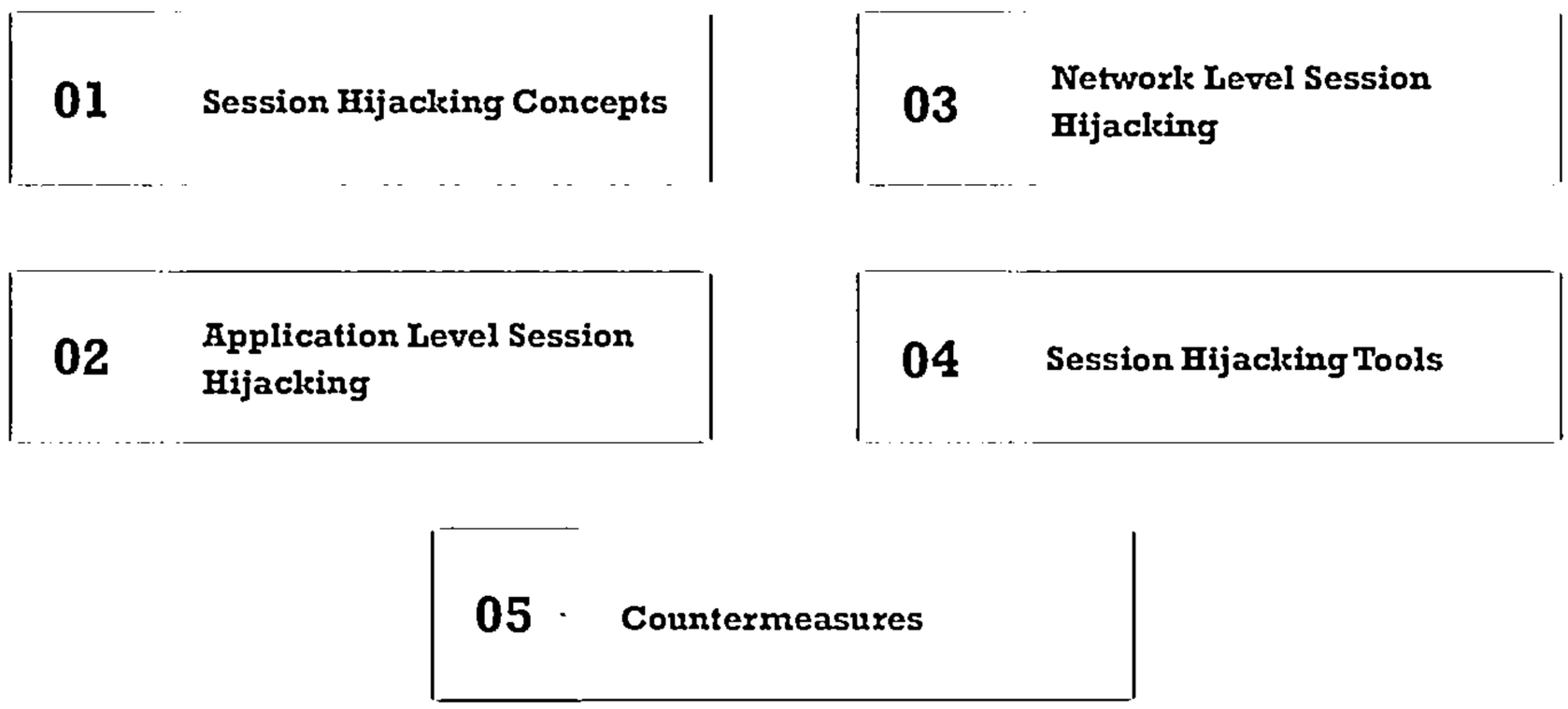


Figure 11.29: Screenshot of FaceNiff

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

Module Flow



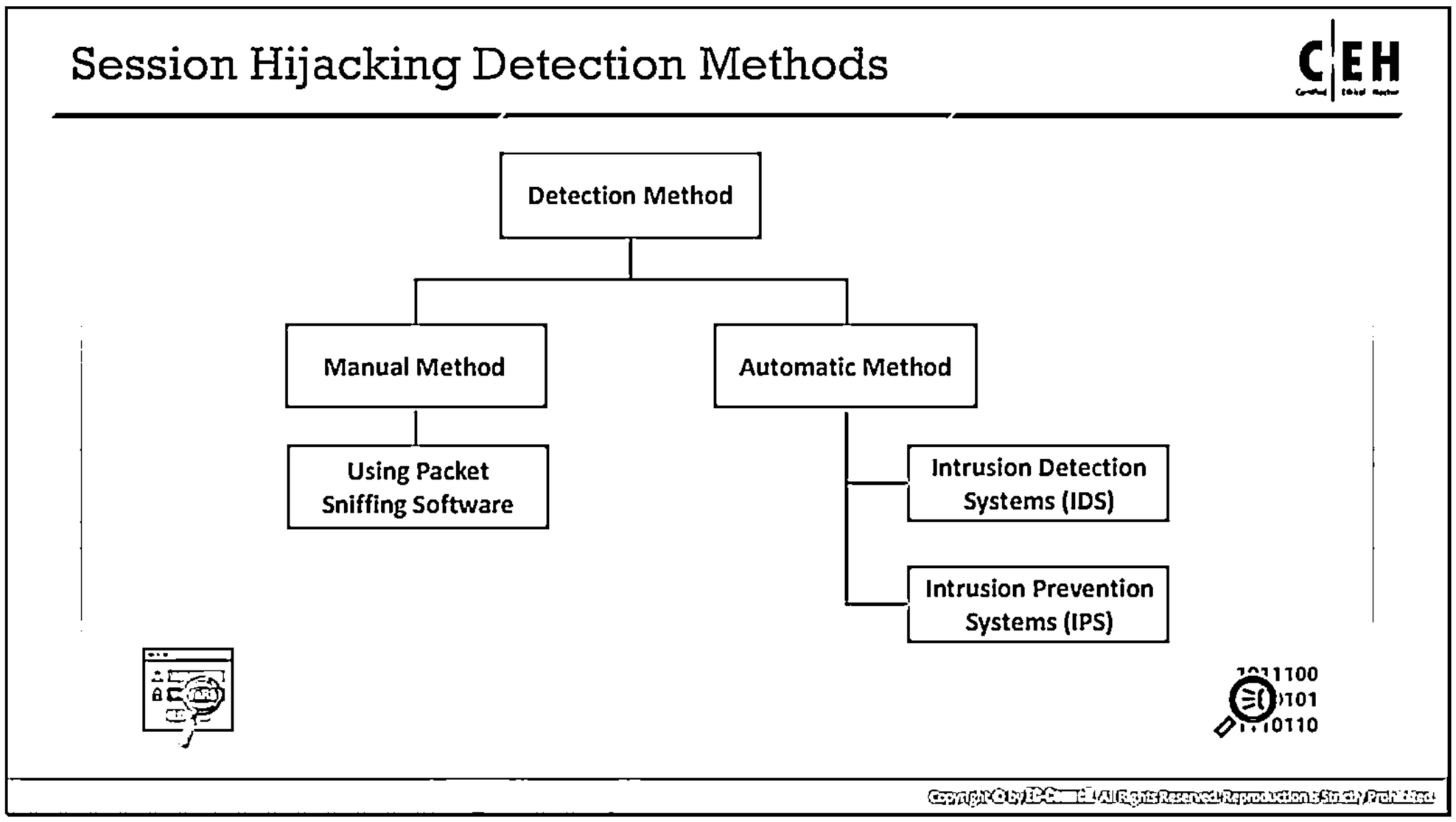
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasures

In general, hijacking is a dangerous attack because the victim is at risk of identity theft, fraud, and loss of sensitive information. All networks using TCP/IP are vulnerable to the different types of session hijacking attacks discussed earlier. However, following best practices might protect against session hijacking attacks.

This section discusses session hijacking detection methods, session hijacking detection tools, various countermeasures to combat session hijacking attacks, and approaches causing vulnerability to session hijacking and their preventative solutions such as IP Security (IPsec).

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



Session Hijacking Detection Methods

Session hijacking attacks are exceptionally difficult to detect, and users often overlook them unless the attacker causes severe damage.

The following are some symptoms of a session hijacking attack:

- A burst of network activity for some time, which decreases the system performance
- Busy servers resulting from requests sent by both the client and hijacker

Methods to detect session hijacking

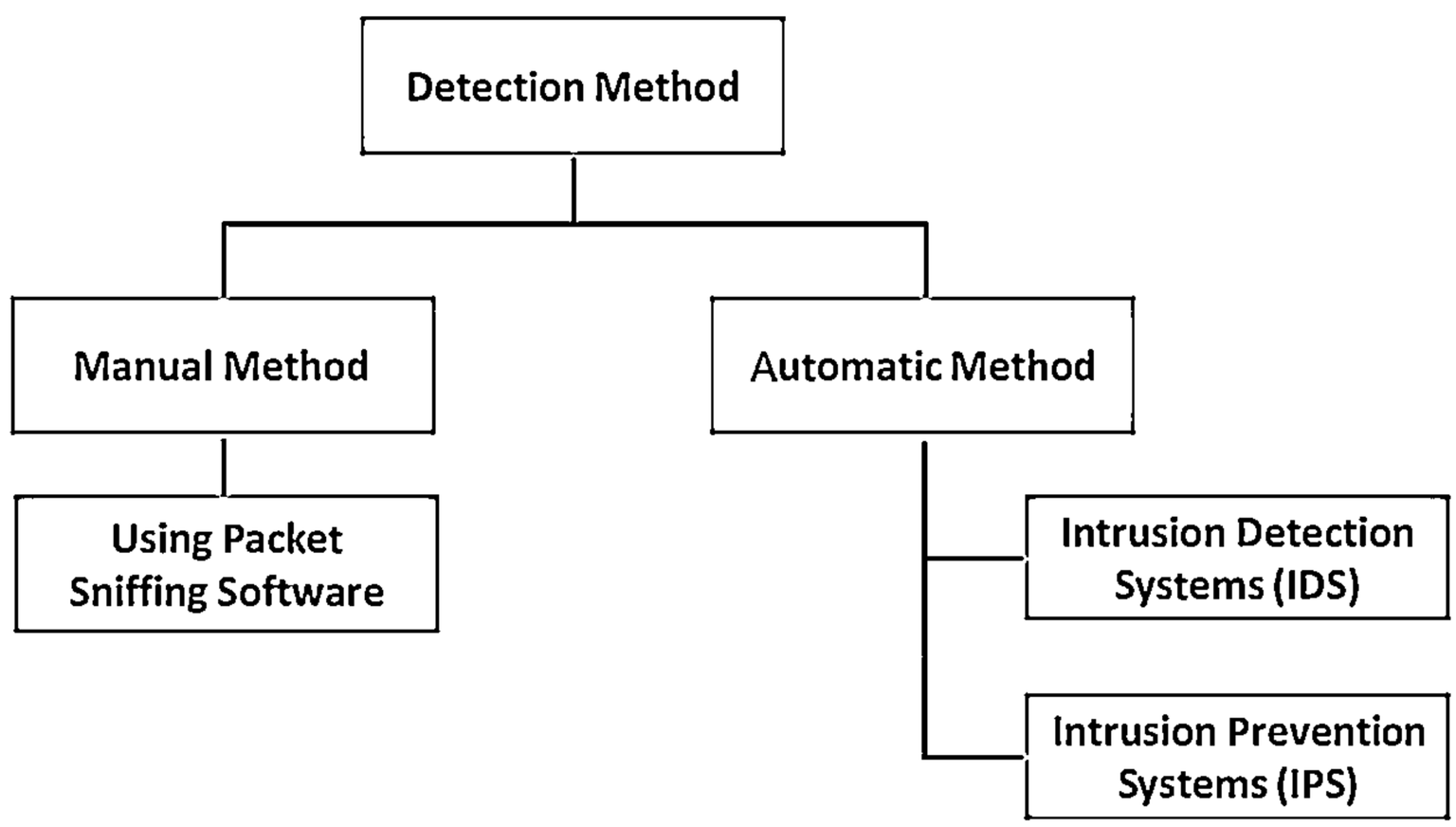


Figure 11.30: Session hijacking detection methods

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

- **Manual Method**

  The manual method involves the use of packet sniffing software such as Wireshark and SteelCentral Packet Analyzer to monitor session hijacking attacks. The packet sniffer captures packets in transit across the network, which is then analyzed using various filtering tools.

  Forced ARP Entry

  A forced ARP entry involves replacing the MAC address of a compromised machine in the ARP cache of the server with a different one in order to restrict network traffic to the compromised machine.

  A forced ARP entry should be performed in the case of the following:

  - Repeated ARP updates
  - Frames sent between the client and server with different MAC addresses
  - ACK storms

- **Automatic Method**

  The automatic method involves the use of an intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor incoming network traffic. If the packet matches any of the attack signatures in the internal database, the IDS generates an alert, whereas the IPS blocks the traffic from entering the database.

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

Protecting against Session Hijacking

1. Use Secure Shell (SSH) to create a secure communication channel
2. Implement the log-out functionality for the user to end the session
3. Generate the session ID after a successful login and accept only session IDs generated by the server only
4. Ensure that data in transit is encrypted and implement the defense-in-depth mechanism
5. Use string or a long random number as a session key
6. Use different usernames and passwords for different accounts
7. Implement timeout() to destroy the session when expired
8. Do not transport session ID in query string
9. Ensure that client-side and server-side protection software are active and up-to-date
10. Use strong authentication (e.g., Kerberos) or peer-to-peer virtual private networks (VPNs)
11. Configure the appropriate internal and external spoof rules on gateways
12. Use IDS products or ARPwatch for monitoring ARP cache poisoning
13. Use HTTP Public Key Pinning (HPKP) to allow users authenticate web servers
14. Enable browsers to verify website authenticity using network notary servers

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

Protecting against Session Hijacking

- Use the Secure Shell (SSH) to create a secure communication channel.
- Pass authentication cookies over HTTPS connections.
- Implement the log-out functionality for the user to end the session.
- Generate a session ID after a successful login and accept session IDs generated by the server only.
- Ensure that data in transit are encrypted and implement the defense-in-depth mechanism.
- Use strings or long random numbers as session keys.
- Use different usernames and passwords for different accounts.
- Educate employees and minimize remote access.
- Implement `timeout()` to destroy sessions when expired.
- Avoid including the session ID in the URL or query string.
- Use switches rather than hubs and limit incoming connections.
- Ensure client-side and server-side protection software are in the active state and up to date.
- Use strong authentication (such as Kerberos) or peer-to-peer virtual private networks (VPNs).
- Configure appropriate internal and external spoof rules on gateways.

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

- Use IDS products or ARPwatch for monitoring ARP cache poisoning.
- Use encrypted protocols available in the OpenSSH suite.
- Use firewalls and browser settings to confine cookies.
- Protect authentication cookies with SSL.
- Regularly update platform patches to fix TCP/IP vulnerabilities (e.g., predictable packet sequences).
- Use IPsec to encrypt session information.
- Use HTTP Public Key Pinning (HPKP) to allow users to authenticate web servers.
- Enable browsers to verify website authenticity using network notary servers.
- Implement DNS-based authentication of named entities.
- Disable compression mechanisms of HTTP requests.
- Use cipher-chaining block (CBC) ciphers incorporating random padding up to 255 bytes, thereby making the extraction of confidential information difficult for an attacker.
- Restrict the cross-site scripts known as cross-site request forgery (CSRF) from the client side.
- Upgrade web browsers to the latest versions.
- Use vulnerability scanners such as masscan to detect any insecure configuration of HTTPS session settings on sites.

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

Web Development Guidelines to Prevent Session Hijacking

1. Create session keys with lengthy strings or random numbers to make it difficult for an attacker to guess a valid session key
2. Regenerate the session ID after a successful login to prevent session fixation attacks
3. Encrypt the data and session key transferred between the user and web servers
4. Expire the session as soon as the user logs out
5. Prevent eavesdropping within the network
6. Reduce the life span of a session or cookie
7. Do not create sessions for unauthenticated users until it is necessary
8. Ensure HTTPOnly while using cookies for Session IDs
9. Check whether all the requests received for the current session are coming from the same IP address and User-Agent
10. Implement continuous device verification to identify whether the user who established the session is still in control
11. Implement risk-based authentication at different levels before giving access to sensitive information
12. Perform authentication and integrity verification between VPN endpoints

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

Web Development Guidelines to Prevent Session Hijacking

An attacker usually hijacks a session by exploiting the vulnerabilities in mechanisms used for session establishment. Web developers often ignore security. During the development process, web developers should consider the following guidelines to minimize/eliminate the risk of session hijacking.

- Create session keys with lengthy strings or random numbers so that it is difficult for an attacker to guess a valid session key.
- Regenerate the session ID after a successful login to prevent session fixation attacks.
- Encrypt the data and session key transferred between the user and web servers.
- Implement the Secure Sockets Layer (SSL) to encrypt all the information in transit via the network.
- Make the session expire as soon as the user logs out.
- Prevent eavesdropping within the network.
- Reduce the life span of a session or cookie.
- Use restrictive cache directives for all the web traffic through HTTP and HTTPS, such as the "**Cache-Control: no-cache, no-store**" and "**Pragma: no-cache**" HTTP headers and/or equivalent META tags on all or (at least) sensitive web pages.
- Do not create sessions for unauthenticated users unless necessary.
- Ensure HTTPOnly while using cookies for session IDs.
- Use a secure flag to send cookies in HTTPS requests and encrypt them before sending across the network.

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

- Check whether all the requests received for the current session originate from the same IP address and user agent.
- Implement continuous device verification to identify whether the user who established the session is still in control.
- Implement risk-based authentication at different levels before granting access to sensitive information.
- Perform authentication and integrity verification between VPN endpoints.

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

Web User Guidelines to Prevent Session Hijacking

1. Do not click on links received through emails or IMs
2. Use firewalls to prevent malicious content from entering the network
3. Use firewalls and browser settings to restrict cookies
4. Ensure that the website is certified by the certifying authorities
5. Ensure that you clear history, offline content, and cookies from your browser after every confidential and sensitive transaction
6. Prefer https, a secure transmission, over http when transmitting sensitive and confidential data
7. Logout from the browser by clicking on the logout button instead of closing the browser

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

Web User Guidelines to Prevent Session Hijacking

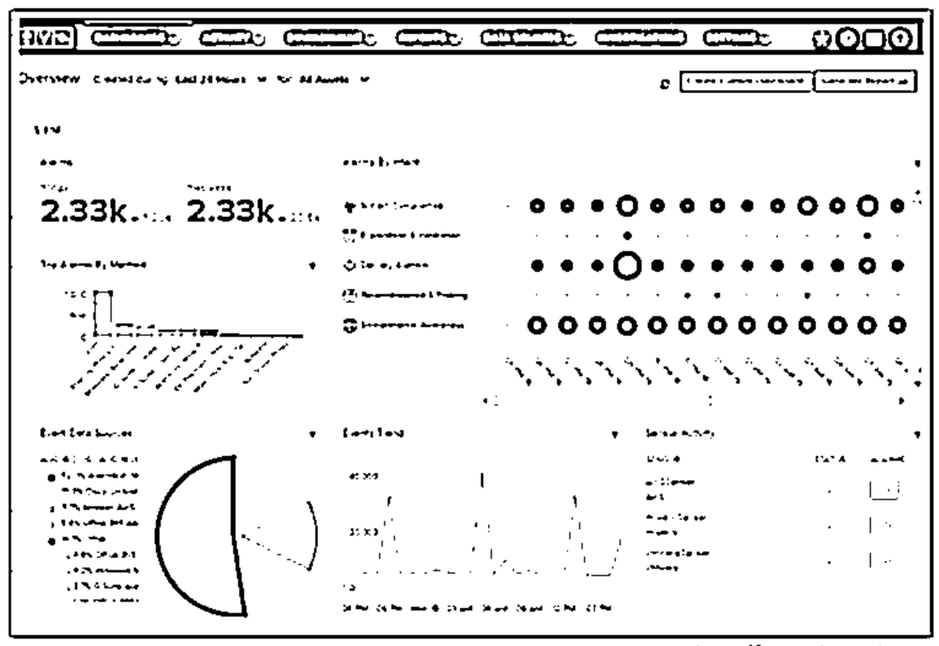
The following are some guidelines for web users to defend against session hijacking.

- Do not click on links received through emails or instant messages (IMs).
- Use firewalls to prevent malicious content from entering the network.
- Use firewalls and browser settings to restrict cookies.
- Ensure that the website is certified by appropriate certifying authorities.
- Ensure that the history, offline content, and cookies are cleared from the browser after every confidential and sensitive transaction.
- Give preference to HTTPS, a secure transmission protocol, over HTTP when transmitting sensitive and confidential data.
- Logout from the browser by clicking on the logout button instead of closing the browser.
- Verify and disable add-ons from untrusted sites. Enable add-ons only if necessary.
- Practice using a one-time password for critical data transactions (e.g., credit card transactions).
- Frequently update anti-virus signatures to prevent the automatic installation of malware that attempts to steal cookies.

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

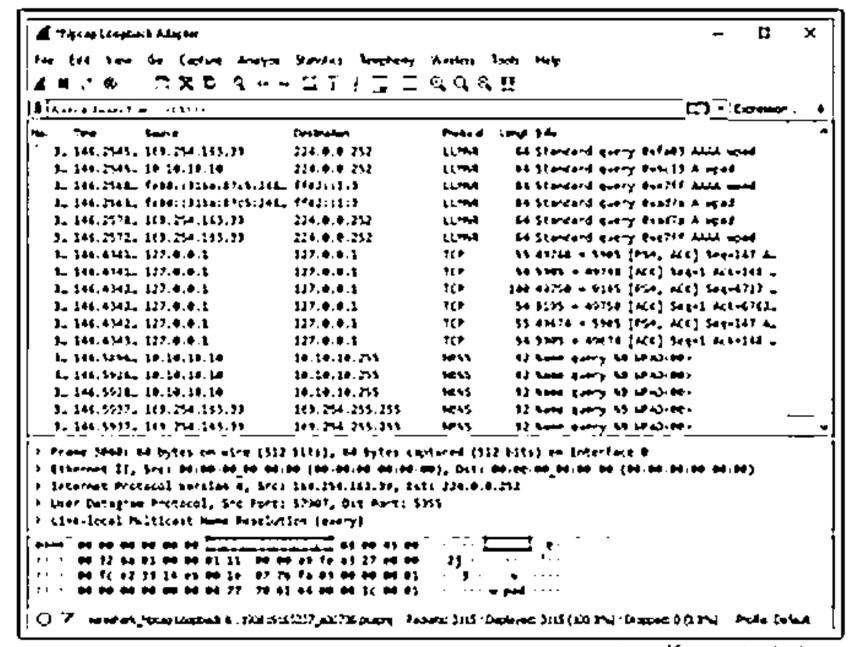
Session Hijacking Detection Tools

AlienVault USM	AlienVault USM delivers threat detection, incident response, and compliance management across cloud, on-premises, etc.



https://www.alienvault.com

Wireshark	Wireshark allows you to capture and interactively browse the traffic running on a computer network



https://www.wireshark.org

Session Hijacking Detection Tools: ⊖ Check Point IPS Software Blade (*https://www.checkpoint.com*) ⊖ LogRhythm (*https://logrhythm.com*)

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

Session Hijacking Detection Tools

Session hijacking attacks are difficult to detect, and in most cases, attacks go unnoticed, causing severe leakage of confidential data. Tools such as packet sniffers, IDSs, and security information and event management (SIEM) can be used to detect session hijacking attacks.

- **AlientVault USM**

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

  AlienVault Unified Security Management (USM) offers powerful threat detection, incident response, and compliance management across cloud, on-premises, and hybrid environments. Security professionals can use this tool for detecting session hijacking attempts and perform asset discovery, intrusion detection, security automation, SIEM and log management, endpoint detection and response, threat detection, threat intelligence, and vulnerability assessment.

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

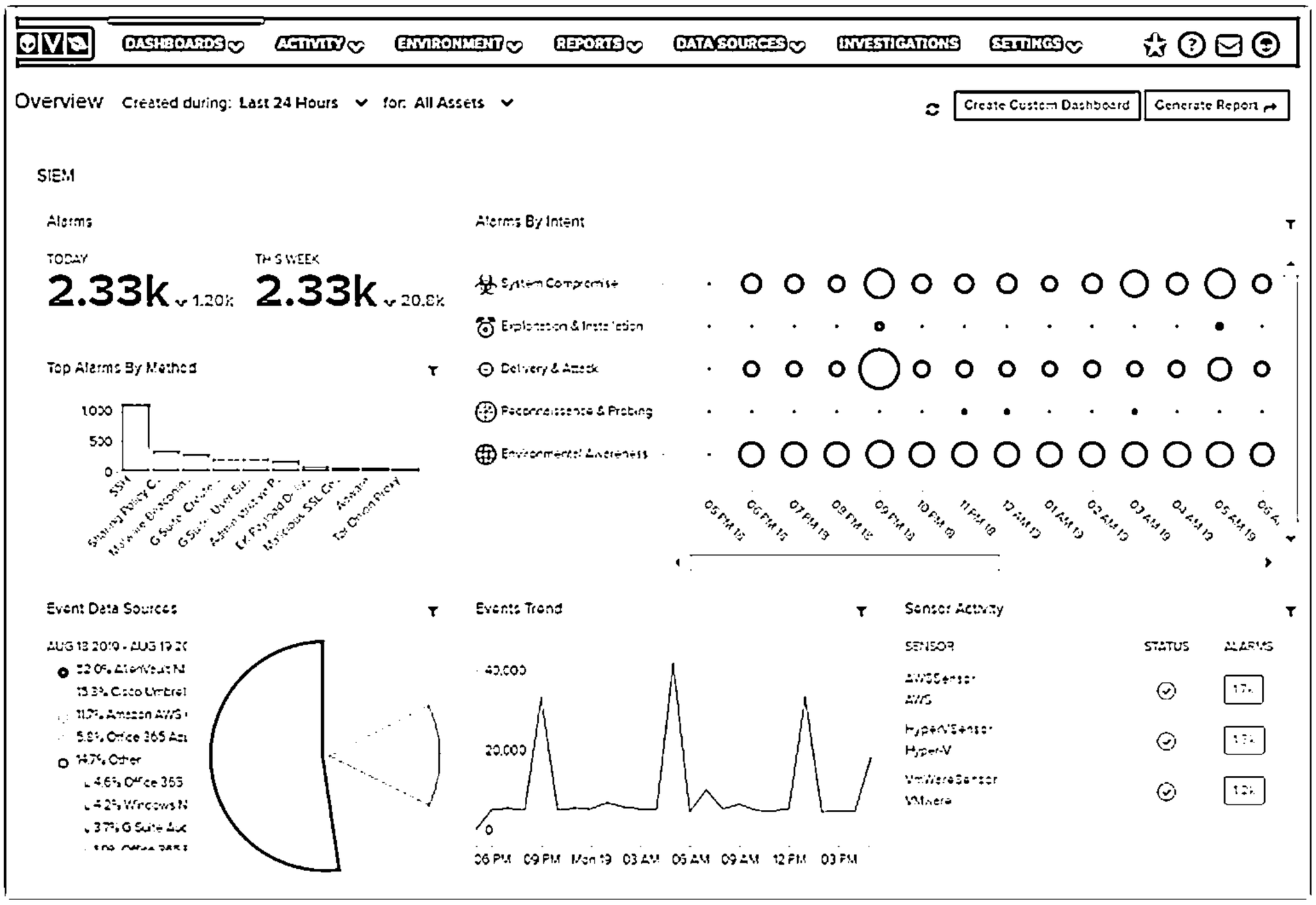


Figure 11.31: Screenshot of AlientVault USM

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

- **Wireshark**

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

  Wireshark allows users to capture and interactively browse the traffic on a network. This tool uses Winpcap to capture packets. Therefore, it can only capture packets on the networks supported by Winpcap. It captures live network traffic from Ethernet, IEEE 802.11, Point-to-Point Protocol/High-level Data Link Control (PPP/HDLC), Asynchronous Transfer Mode (ATM), Bluetooth, Universal Serial Bus (USB), Token Ring, Frame Relay, and Fiber Distributed Data Interface (FDDI) networks. Security professionals use Wireshark to monitor and detect session hijacking attempts.

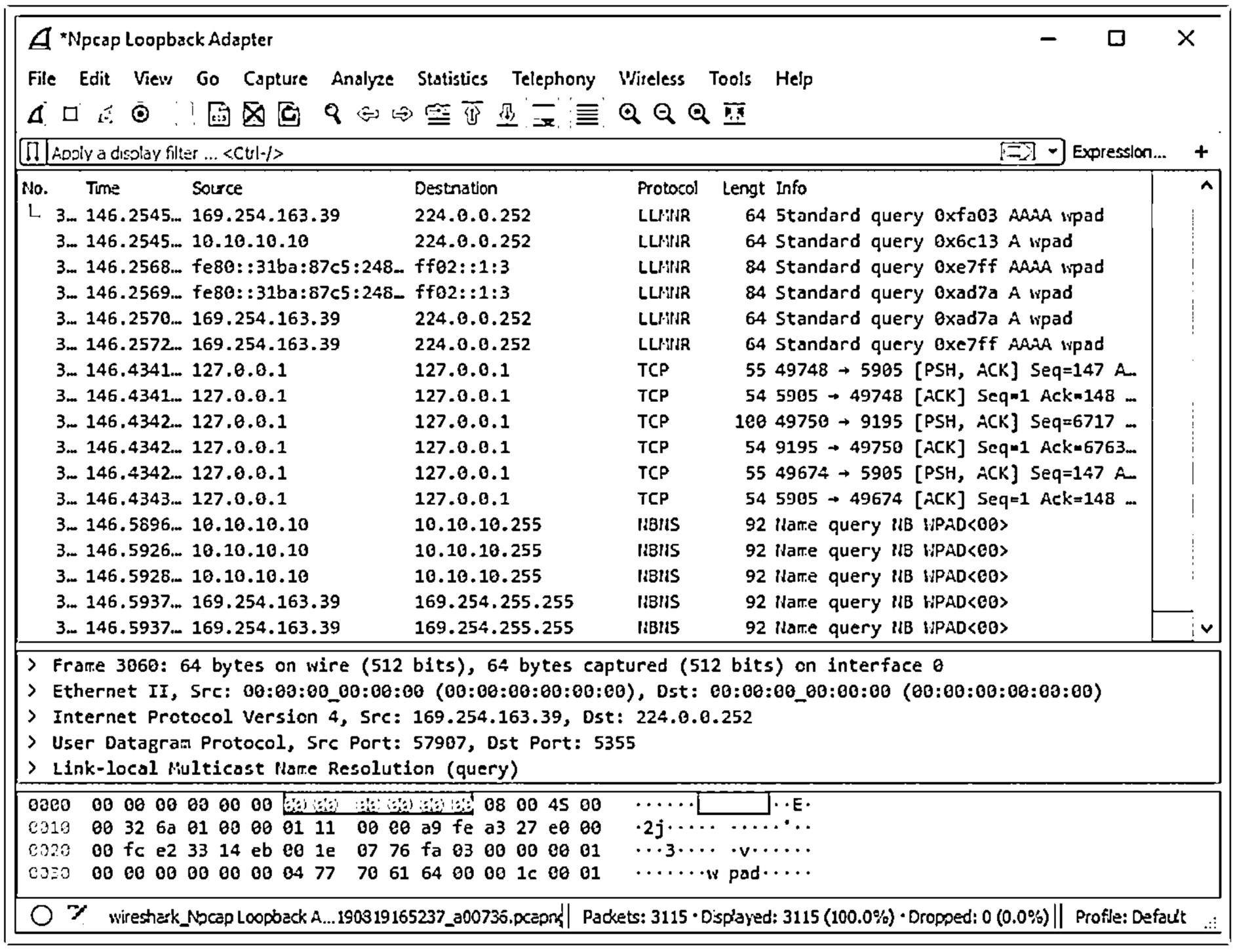


Figure 11.32: Screenshot of Wireshark

The following are some additional session hijacking detection tools:

- Check Point IPS Software Blade (*https://www.checkpoint.com*)
- LogRhythm (*https://logrhythm.com*)
- SolarWinds Log & Event Manager (*https://www.solarwinds.com*)
- IBM Security Network Intrusion Prevention System (*https://www.ibm.com*)

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

Approaches Causing Vulnerability to Session Hijacking and their Preventative Solutions

Issue	Solution	Notes
Telnet, rlogin	OpenSSH or ssh (Secure Shell)	It sends encrypted data and makes it difficult for an attacker to send the correctly encrypted data if a session is hijacked
FTP	SFTP, AS2, MFT, FTPS	Implementing these protocols reduces the chance of a successful hijack by sending data using encryption and digital certificates
HTTP	SSL (Secure Socket Layer) or TLS (Transport Layer Security)	It reduces the chances of a successful hijack
IP	IPSec	It prevents hijacking by securing IP communications
Any Remote Connection	VPN	Implementing encrypted VPNs, such as PPTP, L2PT, and IPSec, for remote connection prevents session hijacking
SMB (Server Message Block)	SMB signing	It improves the security of the SMB protocol and reduces the chances of session hijacking
Hub Network	Switch Network	It mitigates the risk of ARP spoofing and other session hijacking attacks

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

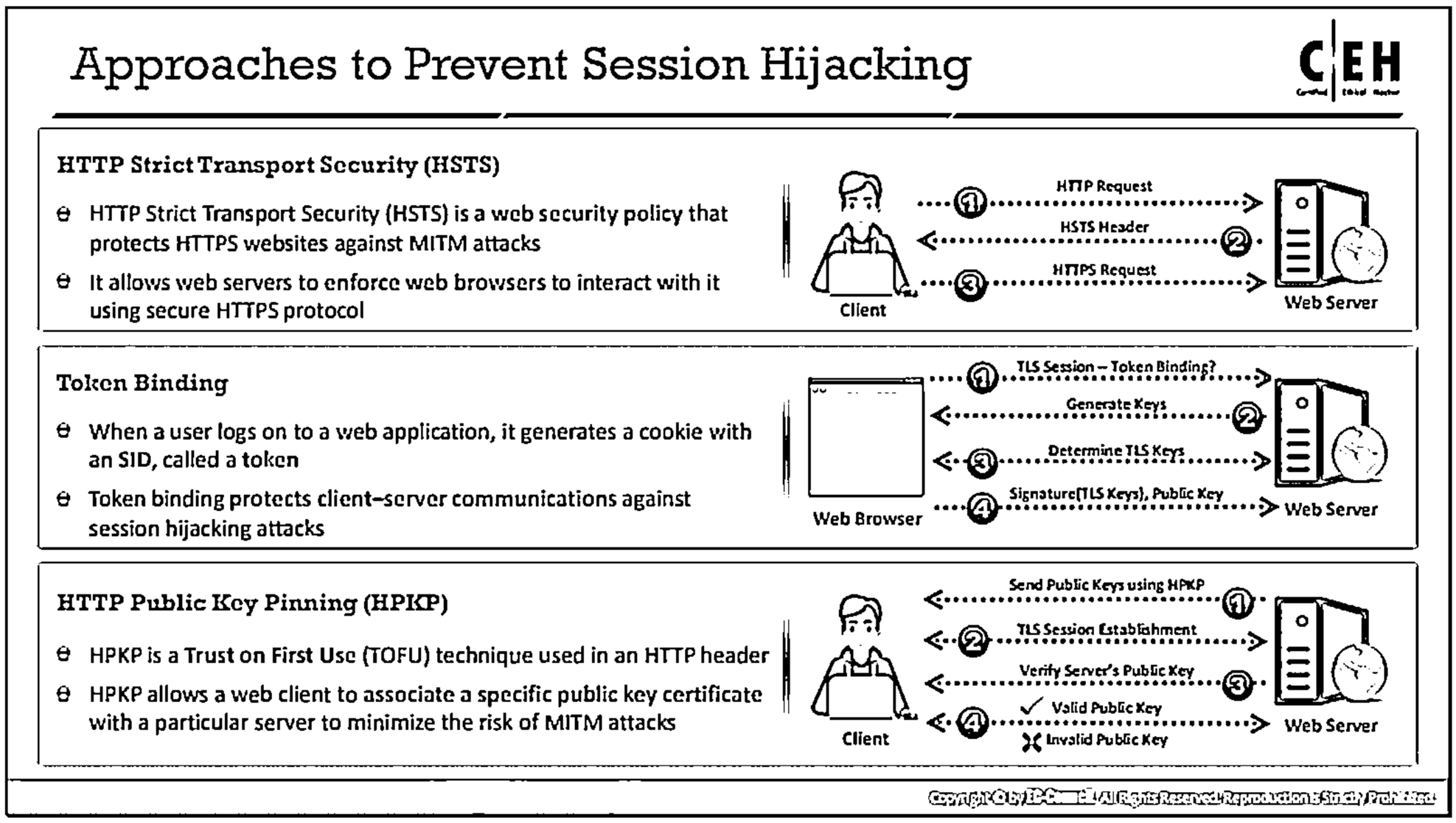
Approaches Causing Vulnerability to Session Hijacking and their Preventative Solutions

Implementing encryption and signing protocols prevents attackers from hijacking sessions. Below table lists various issues and their respective solutions that, upon implementation, prevent or impede the hijacking of a valid session.

Issue	Solution	Notes
Telnet, rlogin	Secure Shell (SSH) or OpenSSH	It sends encrypted data and makes it difficult for an attacker to send correctly encrypted data if a session is hijacked.
FTP	SSH FTP (SFTP), Applicability Statement 2 (AS2), managed file transfer (MFT), FTP Secure (FTPS)	Implementing these protocols reduces the chance of a successful hijack by sending data using encryption and digital certificates.
HTTP	Secure Sockets Layer (SSL) or Transport Layer Security (TLS)	It reduces the chances of a successful hijack.
IP	IPsec	It prevents hijacking by securing IP communications.
Any Remote Connection	Virtual private network (VPN)	Implementing encrypted VPNs such as PPTP, Layer 2 Protocol Tunneling (L2PT), and IPsec, for remote connections prevents session hijacking.
Server Message Block (SMB)	SMB signing	It improves the security of the SMB protocol and reduces the chances of session hijacking.
Hub Network	Switch network	It mitigates the risk of ARP spoofing and other session hijacking attacks.

Table 11.1: Approaches causing vulnerability to session hijacking and their preventative solutions

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



Approaches to Prevent Session Hijacking

- **HTTP Strict Transport Security (HSTS)**

  HTTP Strict Transport Security (HSTS) is a web security policy that protects HTTPS websites against MITM attacks. The HSTS policy helps web servers force web browsers to interact with them using HTTPS. With the HSTS policy, all insecure HTTP connections are automatically converted into HTTPS connections. This policy ensures that all the communication between a web server and web browser is encrypted and that all responses that are delivered and received originate from an authenticated server.

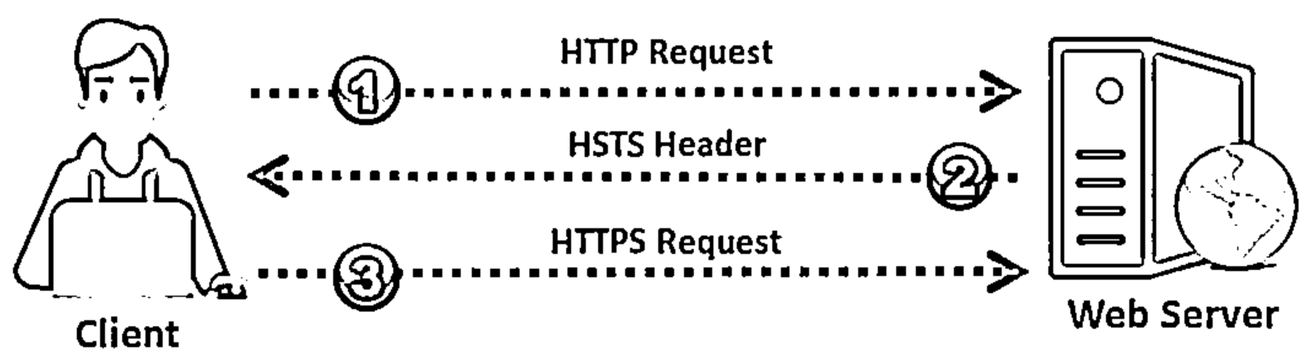


Figure 11.33: Implementation of HSTS

- **Token Binding**

  When a user logs into a web application, a cookie with a session ID, called a token, is generated. The user utilizes this random token to send requests to the server and access resources. An attacker can impersonate the user and hijack the connection by capturing and reusing a valid session ID. Token binding protects client–server communication against session hijacking attacks. The client creates a public–private key pair for every connection to a remote server. When a client connects to the server, it generates a signature using a private key and sends this signature along with its public key to the server. The server verifies the signature using the client's public key. This ensures that

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

the message was sent by an authentic client because only the client has its private key. Even if an attacker captures the signature, it is not possible for them to regenerate the signature or reuse it for another connection. For every new connection, a new pair of public and private keys are used.

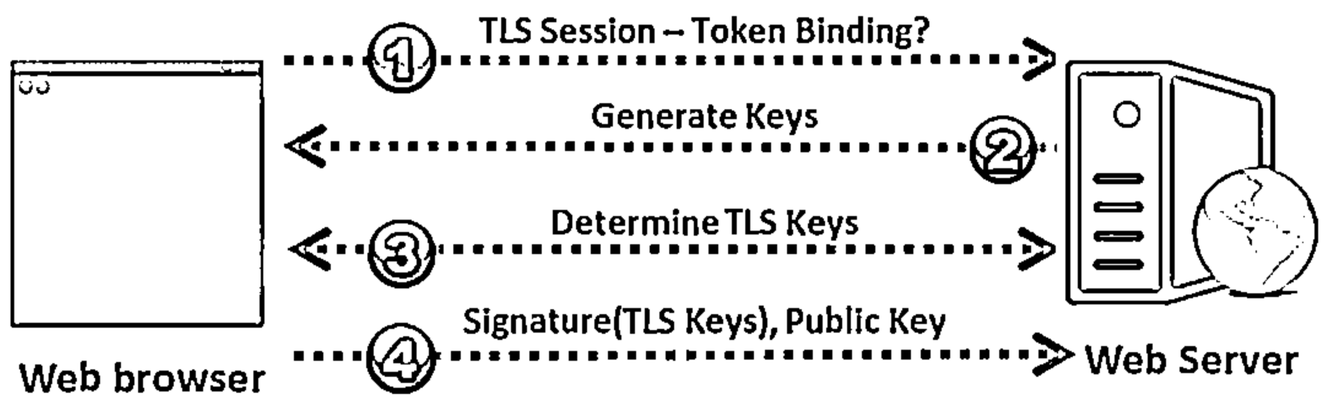


Figure 11.34: Implementation of token binding

- **HTTP Public Key Pinning (HPKP)**

  HTTP Public Key Pinning (HPKP) is a trust on first use (TOFU) technique used in an HTTP header that allows a web client to associate a specific public key certificate with a particular server to minimize the risk of MITM attacks based on fraudulent certificates. In TLS sessions, to verify the authenticity of a server's public key, the public key is enclosed in an X.509 digital certificate, which is signed by a certification authority (CA). By compromising any CA, attackers can perform MITM attacks on various TLS sessions. HPKP protects TLS sessions from such attacks by delivering to the client the list of public keys owned by a web server. When the client connects to the web server, it verifies the server's certificate in the certificate chain obtained using HPKP. If the server sends any unidentified public key, the client issues a warning message to the user.

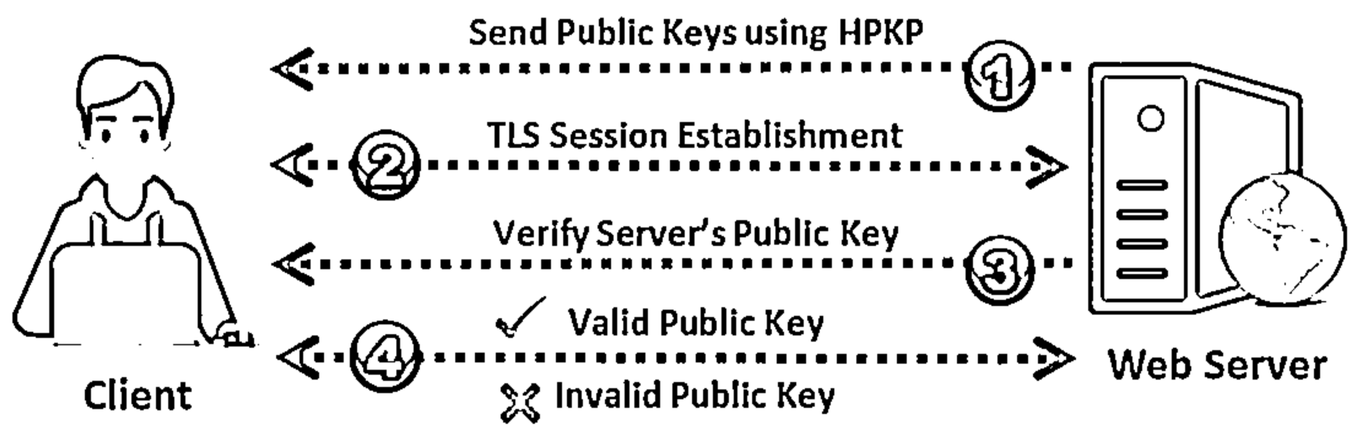


Figure 11.35: Implementation of HPKP

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

Approaches to Prevent MITM Attacks

WEP/WPA Encryption

- WEP and WPA are the different wireless protocols that are intended to protect the traffic that is sent and received by users over a wireless network
- The implementation of these protocols can thwart unwanted users connecting to the network and prevent MITM attacks

VPN

- A VPN creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information
- The implementation of VPN in the network prevents attackers from decrypting the data flowing between the endpoints

Two-Factor Authentication

- A two-factor authentication provides an extra layer of protection as it provides another vector of authentication in addition to a user's password
- The implementation of two-factor authentication can prevent attackers from performing session hijacking and brute-forcing their way into a user's account

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

Approaches to Prevent MITM Attacks

Man-in-the-middle (MITM) attacks are the most common attacks in which the attackers can intercept the traffic between two endpoints. The victim may not realize the effect of this attack, because it is mostly passive in nature. Because the detection of MITM attacks is difficult, they can only be prevented using various measures. The following are some approaches to prevent MITM attacks:

- **WEP/WPA Encryption**

  Wired Equivalent Privacy (WEP) and Wireless Protected Access (WPA) are wireless protocols that are intended to protect the traffic that is sent and received by users over a wireless network. The implementation of these protocols can thwart the attempts of unwanted users to connect to the network. A weak encryption mechanism enables attackers to brute force credentials and enter the target network to perform an MITM attack.

- **VPN**

  A VPN creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information. It creates a subnet by using key-based encryption for secure communication between endpoints. The implementation of a VPN in the network prevents attackers from decrypting the data flowing between the endpoints.

- **Two-Factor Authentication**

  Two-factor authentication provides an extra layer of protection because it serves as a vector of authentication in addition to a user's password. Therefore, the implementation of two-factor authentication can prevent attackers from performing session hijacking and brute forcing to compromise a user's account.

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

IPSec

- IPSec is a protocol suite developed by the IETF for securing IP communications by authenticating and encrypting each IP packet of a communication session
- It is deployed widely to implement VPNs and for remote user access through dial-up connection to private networks

Components of IPsec

- IPsec Driver
- Internet Key Exchange (IKE)
- Internet Security Association Key Management Protocol
- Oakley
- IPsec Policy Agent

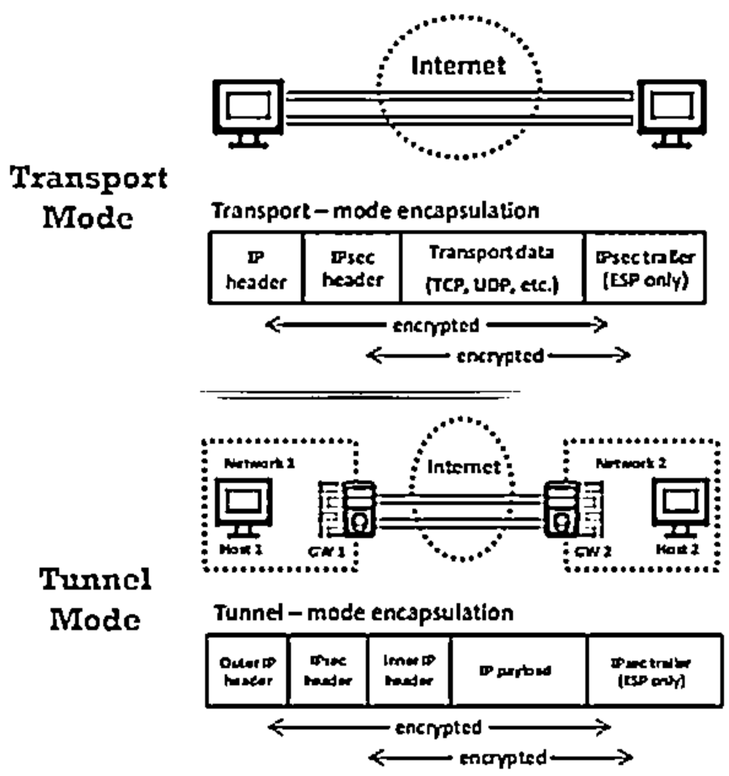
Benefits of IPSec

- Network-level peer authentication
- Data origin authentication
- Data integrity
- Data confidentiality (encryption)
- Replay protection

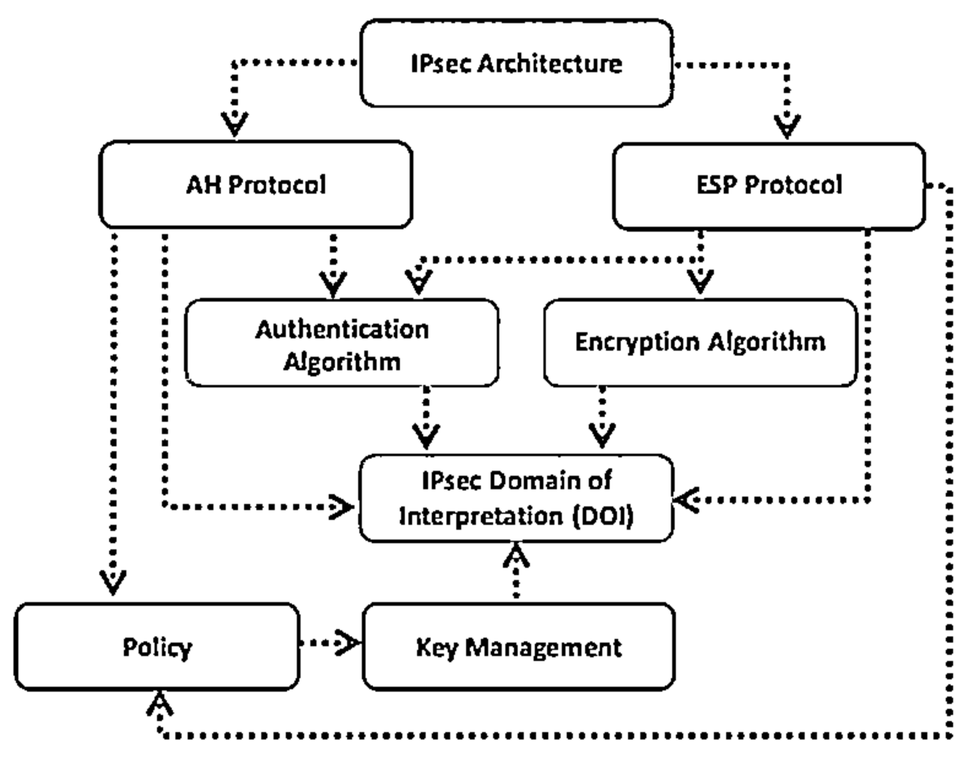
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

IPSec (Cont'd)

Modes of IPsec



IPsec Architecture



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

IPsec

Internet Protocol Security (IPsec) is a set of protocols that the Internet Engineering Task Force (IETF) developed to support the secure exchange of packets at the IP layer. It ensures interoperable cryptographically based security for IPv4 and IPv6, and it supports network level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. It is widely used to implement VPNs and for remote user access through

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

dial-up connection to private networks. It supports transport and tunnel encryption modes, although sending and receiving devices must share a public key.

IPsec policies can be assigned through the Group Policy configuration of Active Directory domains, organizational units, and IPsec deployment policies at the domain, site, or organizational-unit level. The security services offered by IPsec include the following:

- Rejection of replayed packets (a form of partial sequence integrity)
- Data confidentiality (encryption)
- Access control
- Connectionless integrity
- Data origin authentication
- Data integrity
- Limited traffic-flow confidentiality
- Network level peer authentication
- Replay protection

At the IP layer, IPsec provides all the above-mentioned services, offering the protection of IP and/or upper-layer protocols such as TCP, UDP, ICMP, and Border Gateway Protocol (BGP).

Components of IPsec

- **IPsec driver**: Software that performs protocol-level functions required to encrypt and decrypt packets.
- **Internet Key Exchange (IKE)**: An protocol that produces security keys for IPsec and other protocols.
- **Internet Security Association and Key Management Protocol (ISAKMP)**: Software that allows two computers to communicate by encrypting the data exchanged between them.
- **Oakley**: A protocol that uses the Diffie–Hellman algorithm to create a master key and a key that is specific to each session in IPsec data transfer.
- **IPsec Policy Agent**: A service included in Windows OS that enforces IPsec policies for all the network communications initiated from that system.

The following are the steps involved in the IPsec process.

- A consumer sends a message to a service provider.
- The consumer's IPsec driver attempts to match the outgoing packet's address or the packet type against the IP filter.
- The IPsec driver notifies ISAKMP to initiate security negotiations with the service provider.
- The service provider's ISAKMP receives the security negotiation request.

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

- Both principles initiate a key exchange, establishing an ISAKMP Security Association (SA) and a shared secret key.
- Both principles discuss the security level for the information exchange, establishing both IPsec SAs and keys.
- The consumer's IPsec driver transfers packets to the appropriate connection type for transmission to the service provider.
- The provider receives the packets and transfers them to the IPsec driver.
- The provider's IPsec uses the inbound SA and key to check the digital signature and begin decryption.
- The provider's IPsec driver transfers decrypted packets to the OSI transport layer for further processing.

Modes of IPsec

The configuration of IPsec involves two different modes: the tunnel mode and transport mode. These modes are associated with the functions of two core protocols: the Encapsulation Security Payload (ESP) and Authentication Header (AH). The model selection depends on the requirements and implementation of IPsec.

- **Transport Mode**

  In the transport mode (also ESP), IPsec encrypts only the payload of the IP packet, leaving the header untouched. It authenticates two connected computers and provides the option of encrypting data transfer. It is compatible with network address translation (NAT); therefore, it can be used to provide VPN services for networks utilizing NAT.

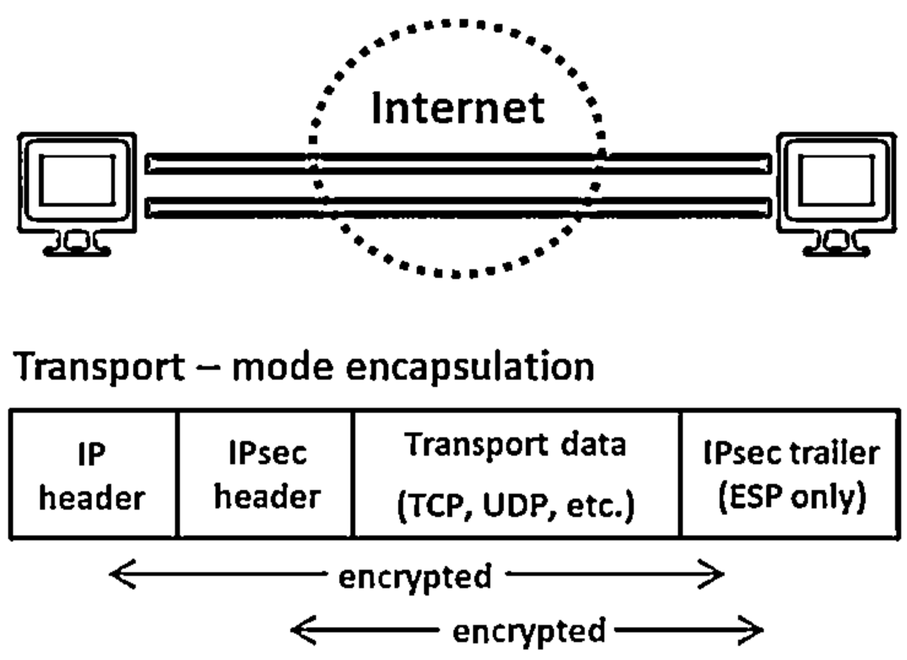


Figure 11.36: Transport mode encapsulation

- **Tunnel Mode**

  In the tunnel mode (also AH), the IPsec encrypts both the payload and header. Hence, in the tunnel mode has higher security than the transport mode. After receiving the data, the IPsec-compliant device performs decryption. The tunnel model is used to create VPNs over the Internet for network-to-network communication (e.g., between routers and link sites), host-to-network communication (e.g., remote user access), and host-to-

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

host communication (e.g., private chat). It is compatible with NAT and supports NAT traversal.

In the tunnel mode, the system encrypts entire IP packets (payload and IP header) and encapsulates the encrypted packets into a new IP packet with a new header. In this mode, ESP encrypts and optionally authenticates entire inner IP packets, whereas AH authenticates entire inner IP packets and selected fields of outer IP headers. The tunnel mode is usually useful between two gateways or between a host and gateway.

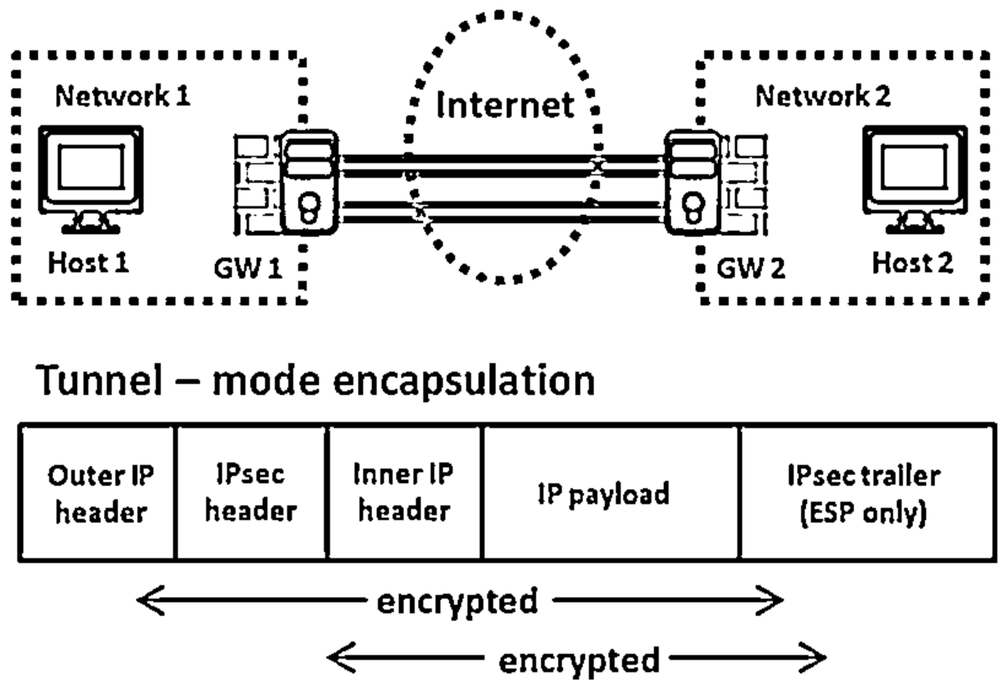


Figure 11.37: Tunnel mode encapsulation

IPsec Architecture

IPsec offers security services at the network layer. This provides the freedom to select the required security protocols as well as the algorithms used for services. To provide the requested services, the corresponding cryptographic keys can be employed, if required. Security services offered by IPsec include access control, data origin authentication, connectionless integrity, anti-replay, and confidentiality. To meet these objectives, IPsec uses two traffic security protocols, AH and ESP, as well as cryptographic key management protocols and procedures.

The protocol structure of the IPsec architecture is as follows.

- **Authentication Header (AH)**: It offers integrity and data origin authentication, with optional anti-replay features.
- **Encapsulating Security Payload (ESP)**: It offers all the services offered by AH as well as confidentiality.
- **IPsec Domain of Interpretation (DOI)**: It defines the payload formats, types of exchange, and naming conventions for security information such as cryptographic algorithms or security policies. IPsec DOI instantiates ISAKMP for use with IP when IP uses ISAKMP to negotiate security associations.
- **Internet Security Association and Key Management Protocol (ISAKMP)**: It is a key protocol in the IPsec architecture that establishes the required security for various communications over the Internet, such as government, private, and commercial

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

communications, by combining the security concepts of authentication, key management, and security associations.

- **Policy**: IPsec policies are useful in providing network security. They define when and how to secure data, as well as security methods to use at different levels in the network. One can configure IPsec policies to meet the security requirements of a system, domain, site, organizational unit, and so on.

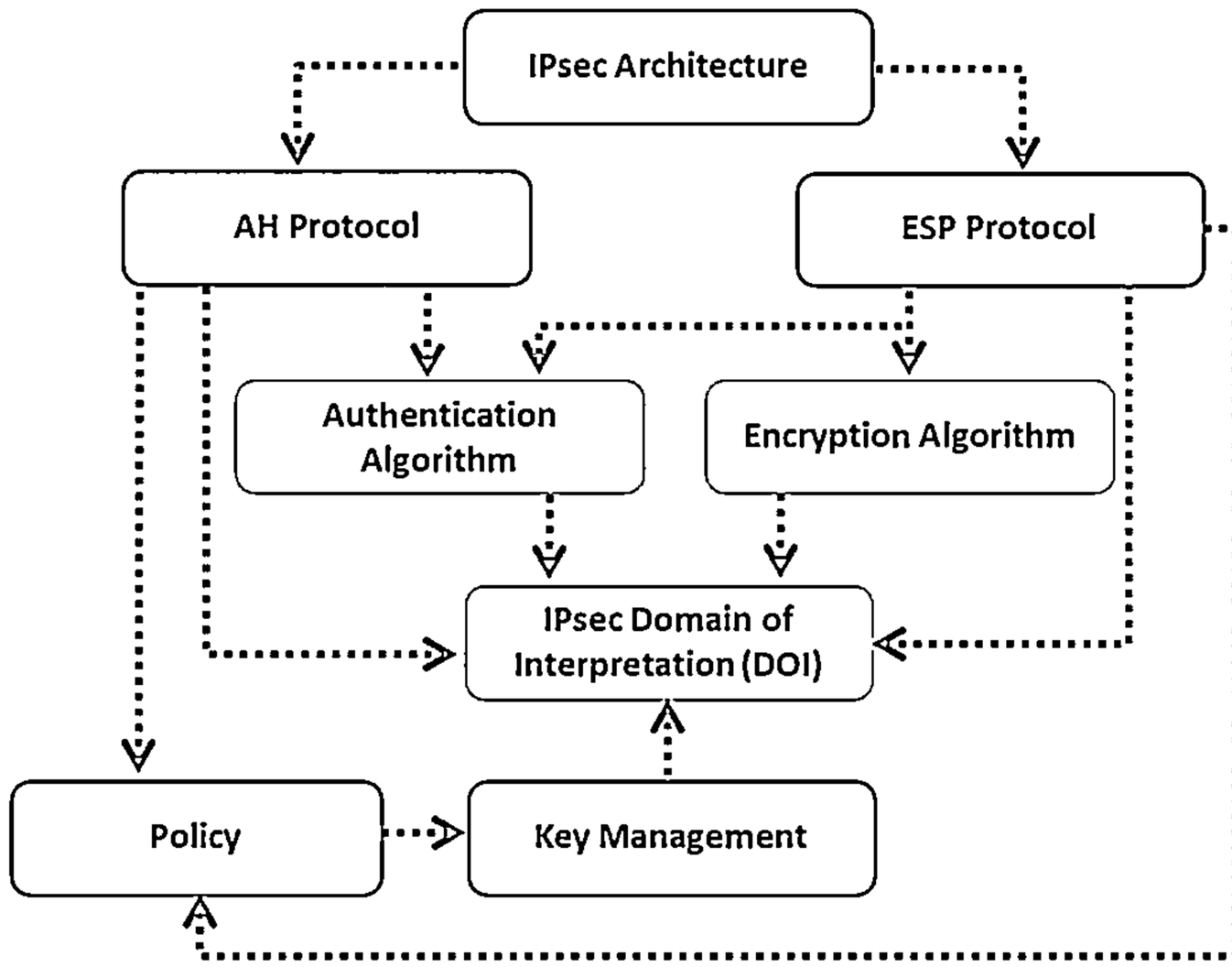
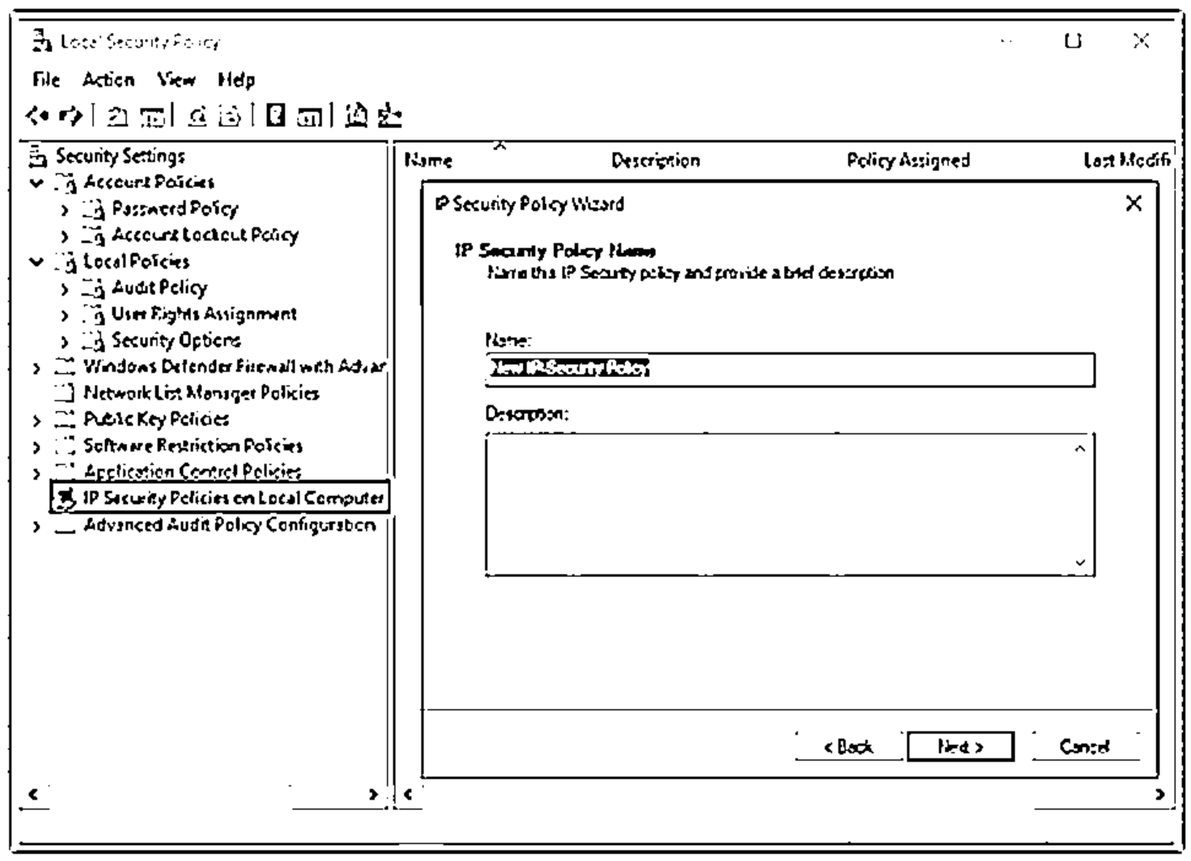


Figure 11.38: IPsec architecture

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

IPsec Authentication and Confidentiality

- IPsec uses two different security services for authentication and confidentiality
  - Authentication Header (AH): Provides the data authentication of the sender
  - Encapsulation Security Payload (ESP): Provides both the data authentication and encryption (confidentiality) of the sender



IPsec Authentication and Confidentiality

IPsec uses two different security services for authentication and confidentiality.

- **Authentication Header (AH)**: It is useful in providing connectionless integrity and data origin authentication for IP datagrams and anti-replay protection for the data payload and some portions of the IP header of each packet. However, it does not support data confidentiality (no encryption). A receiver can select the service to protect against replays, which is an optional service on establishing a security association (SA).
- **Encapsulation Security Payload (ESP)**: In addition to the services (data origin authentication, connectionless integrity, and anti-replay service) provided by AH, the ESP protocol offers confidentiality. Unlike AH, ESP does not provide integrity and authentication for the entire IP packet in the transport mode. ESP can be applied alone, in conjunction with AH, or in a nested manner. It protects only the IP data payload in the default setting. In the tunnel mode, it protects both the payload and IP header.

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

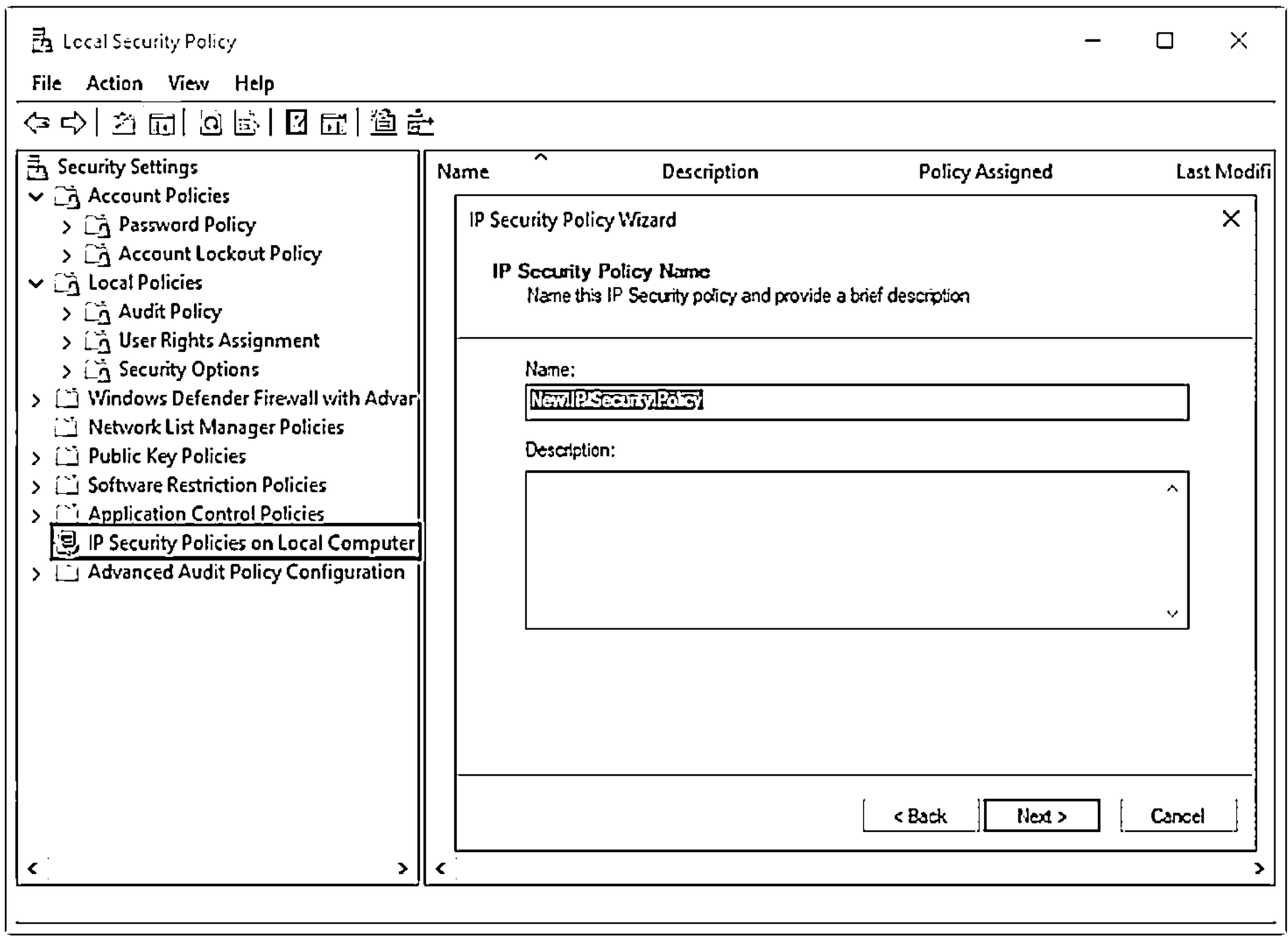


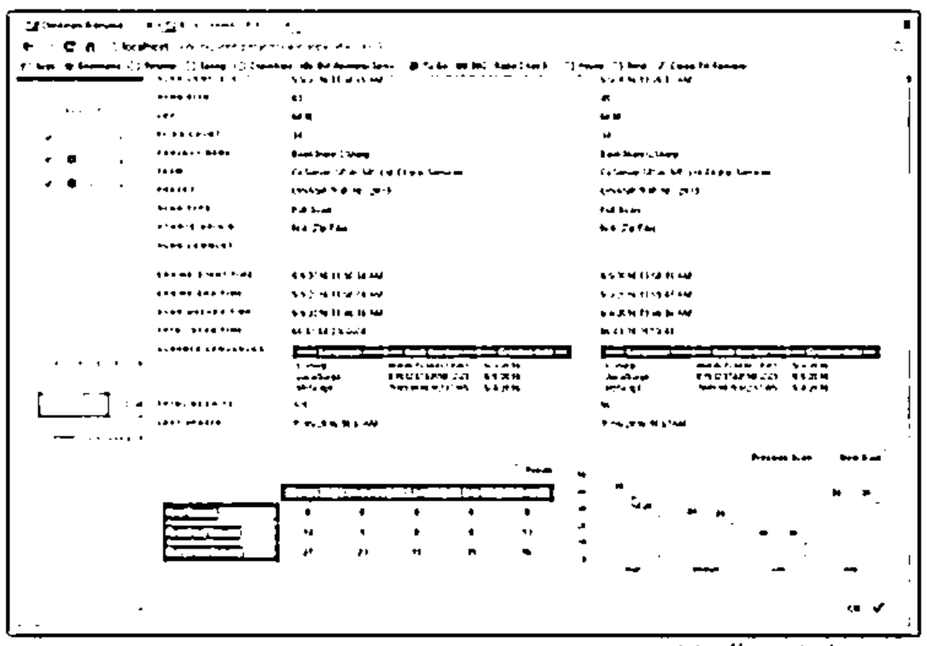
Figure 11.39: Screenshot of local IPsec policy on Windows

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

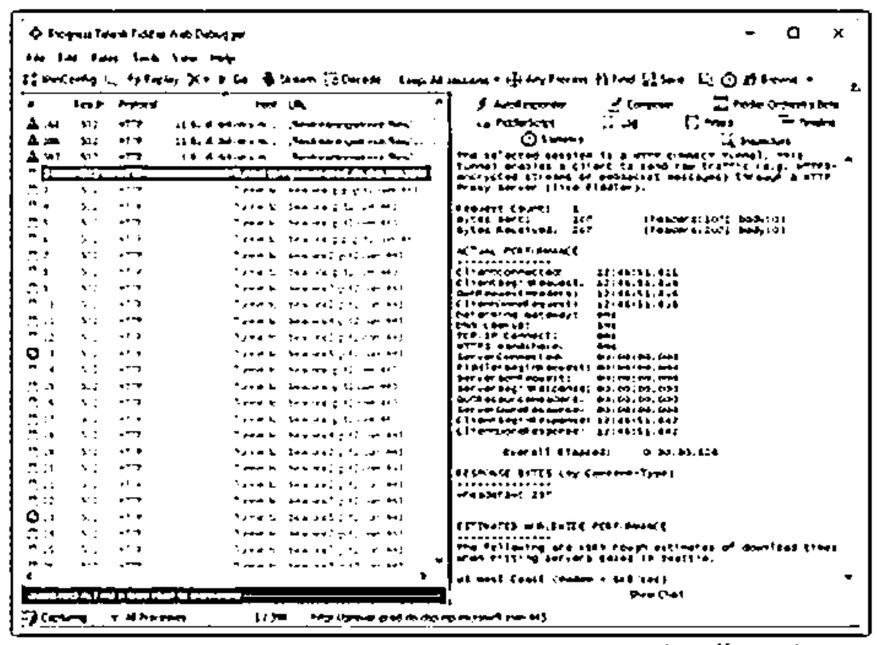
Session Hijacking Prevention Tools

CxSAST | CxSAST is a unique source code analysis solution that provides tools to identify, track, and repair technical and logical flaws in the source code

Fiddler | Fiddler is used for the security testing of web applications, such as decrypting HTTPS traffic and manipulating requests using a MITM decryption technique



https://www.checkmarx.com



https://www.telerik.com

Session Hijacking Prevention Tools:
- Nessus (*https://www.tenable.com*)
- Netsparker (*https://www.netsparker.com*)

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

Session Hijacking Prevention Tools

To prevent session hijacking, the security testing of web applications and the analysis of static code to identify vulnerabilities in web applications are required. Identifying vulnerabilities at an early stage helps in implementing security measures to protect against session hijacking attacks.

- **CxSAST**

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

  Checkmarx CxSAST is a unique source-code analysis solution that provides tools for identifying, tracking, and repairing technical and logical flaws in source code, such as security vulnerabilities, compliance issues, and business logic problems. CxSAST supports open-source analysis (CxOSA), enabling licensing and compliance management, vulnerability alerts, policy enforcement, and reporting. This tool supports a wide range of OS platforms, programming languages, and frameworks.

  Security professionals can use this tool to prevent various session hijacking attacks such as MITM attacks, session fixation attacks, and XSS attacks.

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

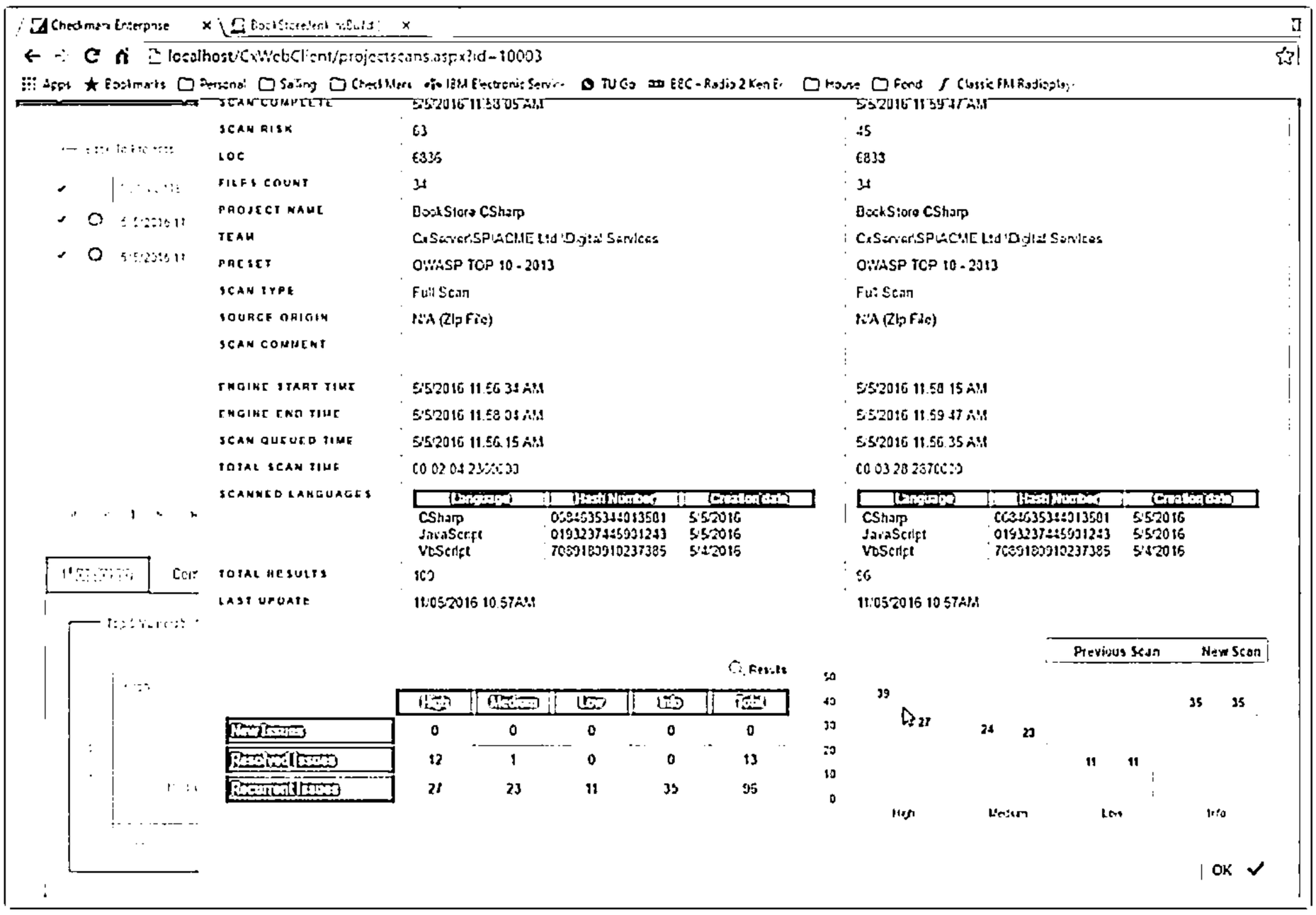


Figure 11.40: Screenshot of CxSAST

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

- **Fiddler**

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

  Fiddler is used for performing web-application security tests such as the decryption of HTTPS traffic and manipulation of requests using an MITM decryption technique. Fiddler is a web debugging proxy that logs all HTTP(S) traffic between a computer and the Internet.

  Security professionals can use Fiddler to test web applications by debugging the traffic from systems as well as manipulating and editing web sessions.

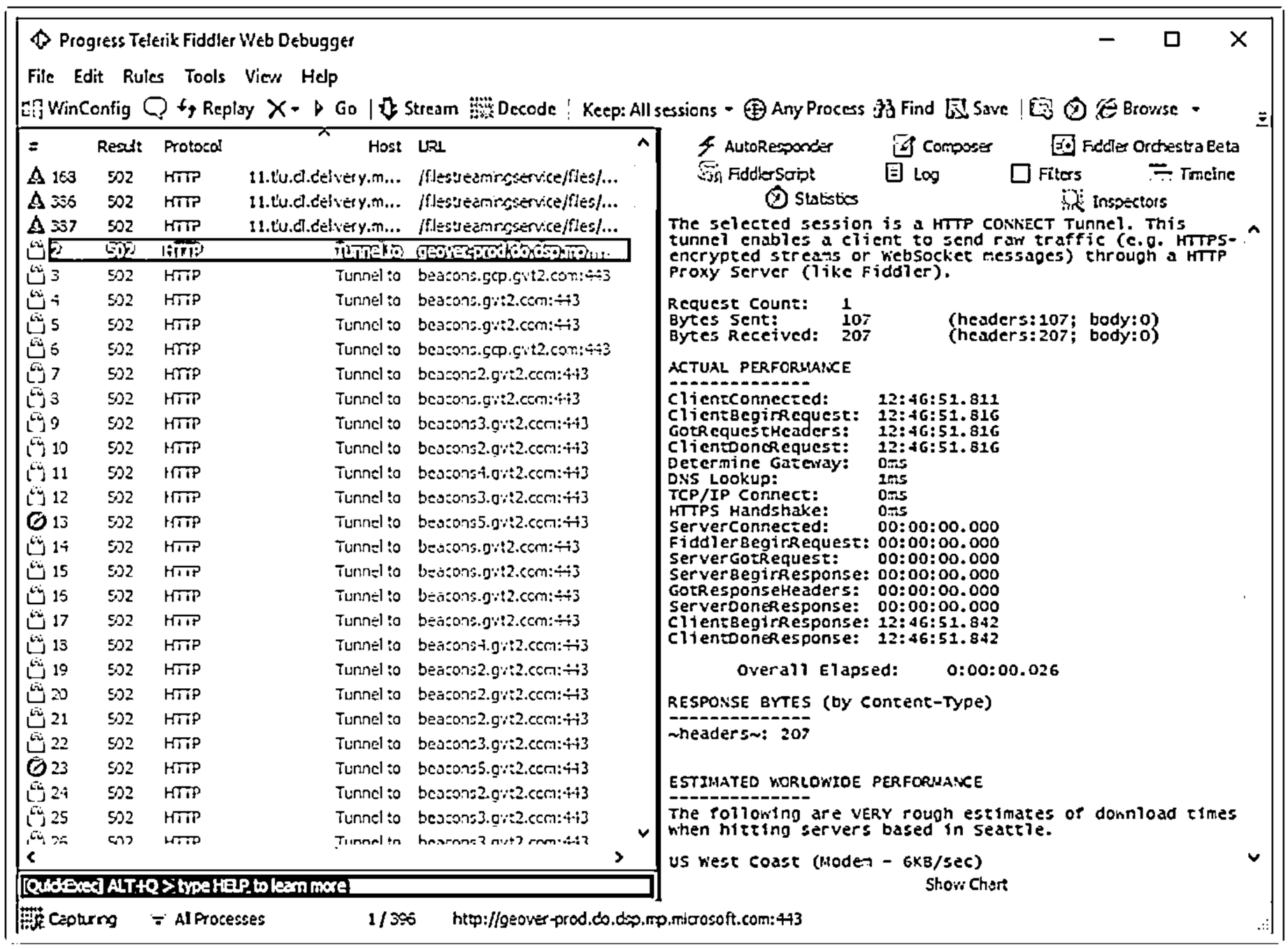


Figure 11.41: Screenshot of Fiddler

The following are some additional session hijacking prevention tools:

- Nessus (*https://www.tenable.com*)
- Netsparker (*https://www.netsparker.com*)
- Wapiti (*http://wapiti.sourceforge.net*)
- WebWatchBot (*https://www.exclamationsoft.com*)

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:
  - Session hijacking concepts and different types of session hijacking
  - Application level and network level session hijacking attacks
  - Various session hijacking tools
  - How to detect, protect, and defend against session hijacking attacks, as well as various session hijacking detection and prevention tools
  - We concluded with a detailed discussion on various countermeasures to be employed to prevent session hijacking attempts by threat actors
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, evade network security components, such as IDS and firewalls to compromise the infrastructure

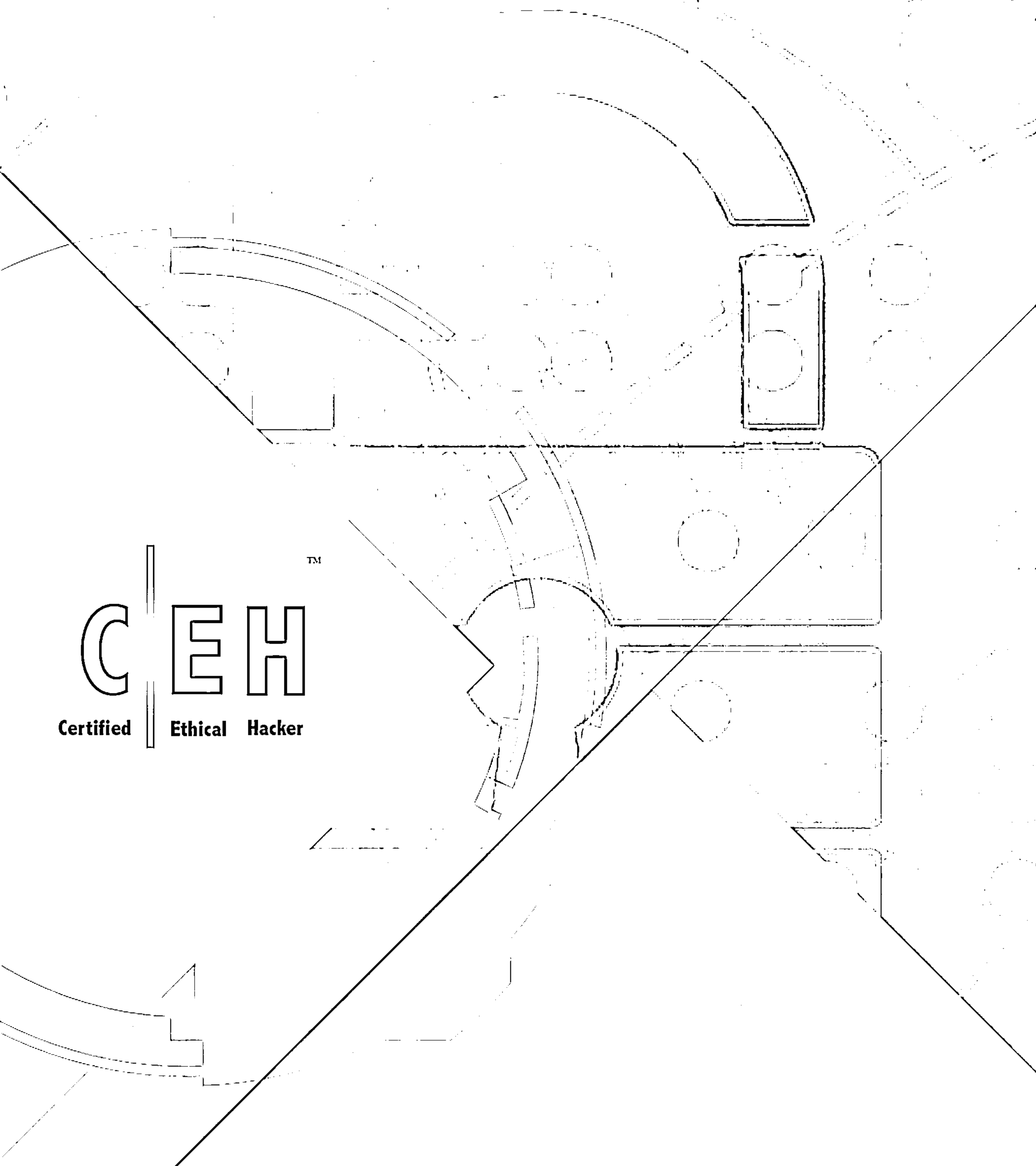
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

In this module, we discussed concepts related to session hijacking, along with different types of session hijacking. We also discussed in detail application level and network level session hijacking attacks. Furthermore, this module presented various session hijacking tools. It also discussed how to detect, protect, and defend against session hijacking attacks, in addition to various session hijacking detection and prevention tools. This module ended with a detailed discussion on various countermeasures to be employed to prevent session hijacking attempts by threat actors.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, evade network security components such as IDSs and firewalls to compromise network infrastructure.

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



C|EH™

Certified | Ethical Hacker

Module 12:
Evading IDS, Firewalls, and Honeypots

Module Objectives

- Understanding IDS, IPS, Firewall, and Honeypot Concepts
- IDS, IPS, Firewall, and Honeypot Solutions
- Understanding different Techniques to Bypass IDS
- Understanding different Techniques to Bypass Firewalls
- IDS/Firewall Evading Tools
- Understanding different Techniques to Detect Honeypots
- IDS/Firewall Evasion Countermeasures

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

Module Objectives

The widespread use of the Internet throughout the business world has boosted network usage in general. Organizations adopt various network security measures such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and "honeypots" to protect their networks. Networks are the most preferred targets of hackers for compromising an organization's security, and attackers continue to find new ways to evade network security measures and attack these targets.

This module provides deep insights into various network security technologies, such as IDS, IPS, firewalls, and honeypots. It explains the operations of these components as well as the various techniques used by attackers to evade them. Further, it describes the countermeasures necessary to prevent such attacks.

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

- Describe IDS, IPS, firewall, and honeypot concepts
- Use different IDS, IPS, firewall, and honeypot solutions
- Explain different techniques to bypass IDS
- Explain various techniques to bypass firewalls
- Use different tools to evade IDS/firewalls
- Explain different techniques to detect honeypots
- Adopt countermeasures against IDS/firewall evasion

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

Module Flow

1. IDS, IPS, Firewall, and Honeypot Concepts
2. IDS, IPS, Firewall, and Honeypot Solutions
3. Evading IDS
4. Evading Firewalls
5. IDS/Firewall Evading Tools
6. Detecting Honeypots
7. IDS/Firewall Evasion Countermeasures

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

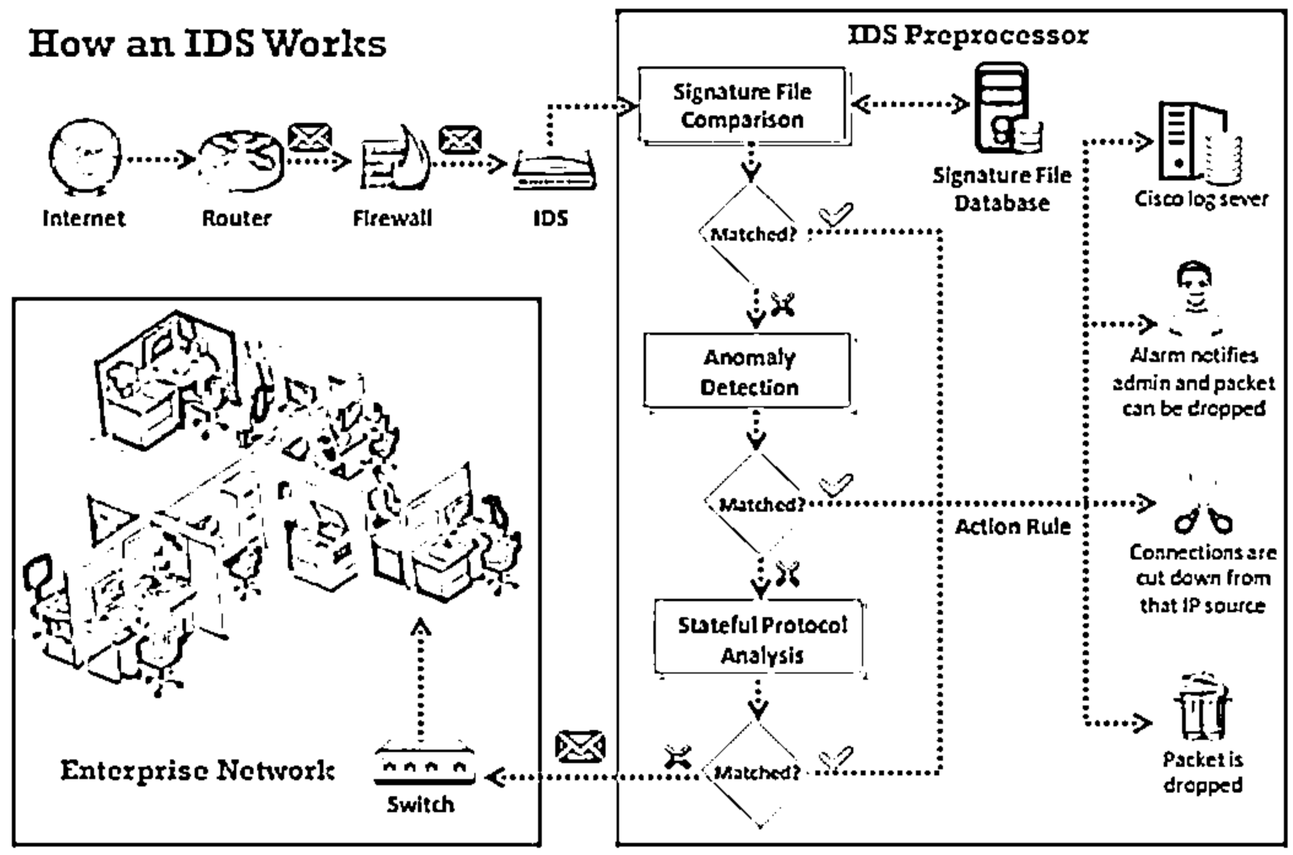
IDS, IPS, Firewall, and Honeypot Concepts

Ethical hackers should have an idea about the function, role, placement, and design of firewalls, IDS, IPS, and honeypots to protect an organization's network by understanding how an attacker evades such security measures. This section provides an overview of these basic concepts.

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

Intrusion Detection System (IDS)

- An intrusion detection system (IDS) is a software system or hardware device that inspects all inbound and outbound network traffic for suspicious patterns that may indicate a network or system security breach
- The IDS checks traffic for signatures that match known intrusion patterns and signals an alarm when a match is found
- Depending on the traffic to be monitored, the IDS is placed outside/inside the firewall to monitor suspicious traffic originating from outside/inside the network



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

Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a security software or hardware device used to monitor, detect, and protect networks or systems from malicious activities; it alerts the concerned security personnel immediately upon detecting intrusions. IDS are extremely useful as they monitor the inbound/outbound traffic of the network and check for suspicious activities continuously to detect a network or system security breach. Specifically, they check traffic for signatures that match known intrusion patterns and raise an alarm when a match is detected. IDS can be categorized into active and passive IDS depending on their functionality. A passive IDS generally only detects intrusions while an active IPS not only detects intrusions in the network but also prevents them.

Main Functions of IDS:

- An IDS gathers and analyzes information from within a computer or a network to identify possible violations of the security policy, including unauthorized access, as well as misuse.
- An IDS is also referred to as a "packet sniffer," which intercepts packets traveling via various communication media and protocols, usually TCP/IP.
- The packets are analyzed after they are captured.
- An IDS evaluates traffic for suspected intrusions and raises an alarm upon detecting such intrusions.

Where IDS resides in the network

One of the most common places to deploy an IDS is near the firewall. Depending on the traffic to be monitored, an IDS is placed outside/inside the firewall to monitor suspicious traffic

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

originating from outside/inside the network. When placed inside, the IDS will be ideal if it is near a DMZ; however, the best practice is to use a layered defense by deploying one IDS in front of the firewall and another one behind the firewall in the network.

Before deploying the IDS, it is essential to analyze the network topology, understand how the traffic flows to and from the resources that an attacker can use to gain access to the network, and identify the critical components that will be possible targets of various attacks against the network. After the position of the IDS in the network is determined, the IDS must be configured to maximize its network protection effect.

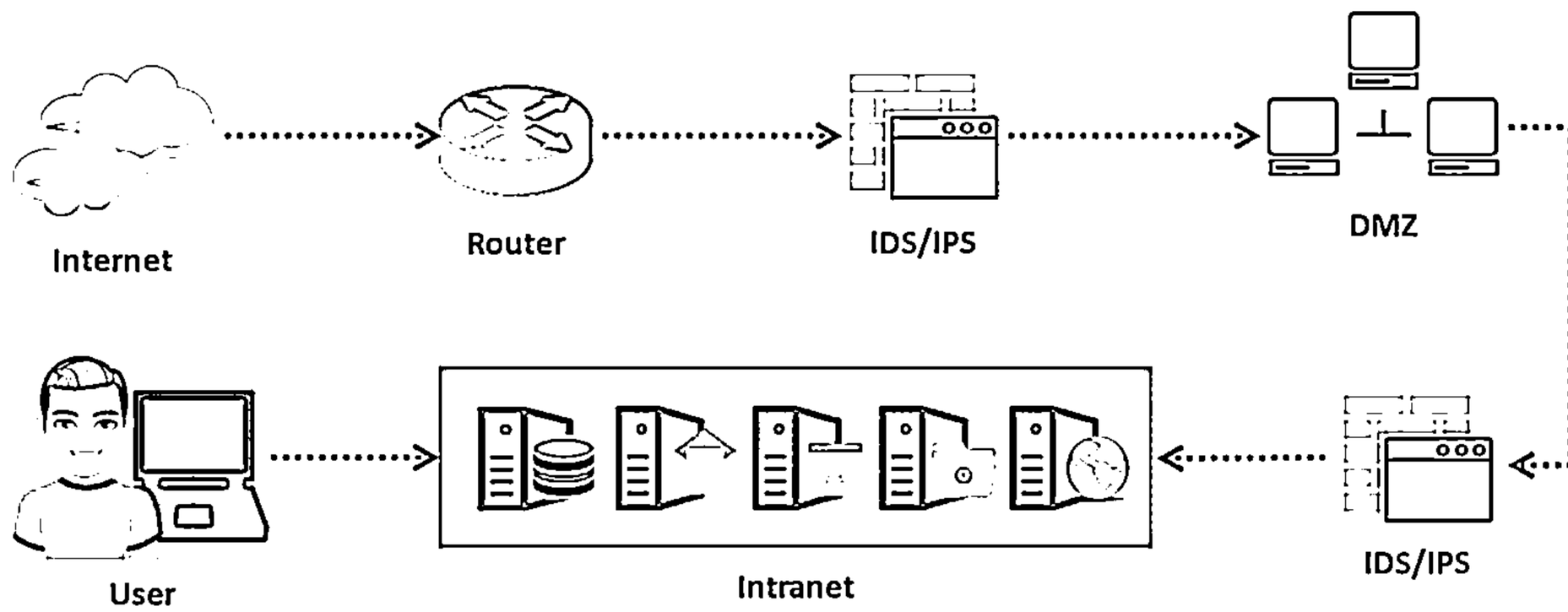


Figure 12.1: Placement of IDS

How an IDS Works

The primary purpose of the IDS is to provide real-time monitoring and detection of intrusions. Additionally, reactive IDS (and IPS) can intercept, respond to, and/or prevent intrusions.

An IDS works as follows:

- IDS have sensors to detect malicious signatures in data packets, and some advanced IDS include behavioral activity detection to detect malicious traffic behavior. Even if the packet signatures do not match perfectly with the signatures in the IDS signature database, the activity detection system can alert administrators about possible attacks.
- If the signature matches, the IDS performs predefined actions such as terminating the connection, blocking the IP address, dropping the packet, and/or raising an alarm to notify the administrator.
- When signature matches, anomaly detection will be skipped; otherwise, the sensor may analyze traffic patterns for an anomaly.
- When the packet passes all the tests, the IDS will forward it to the network.

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

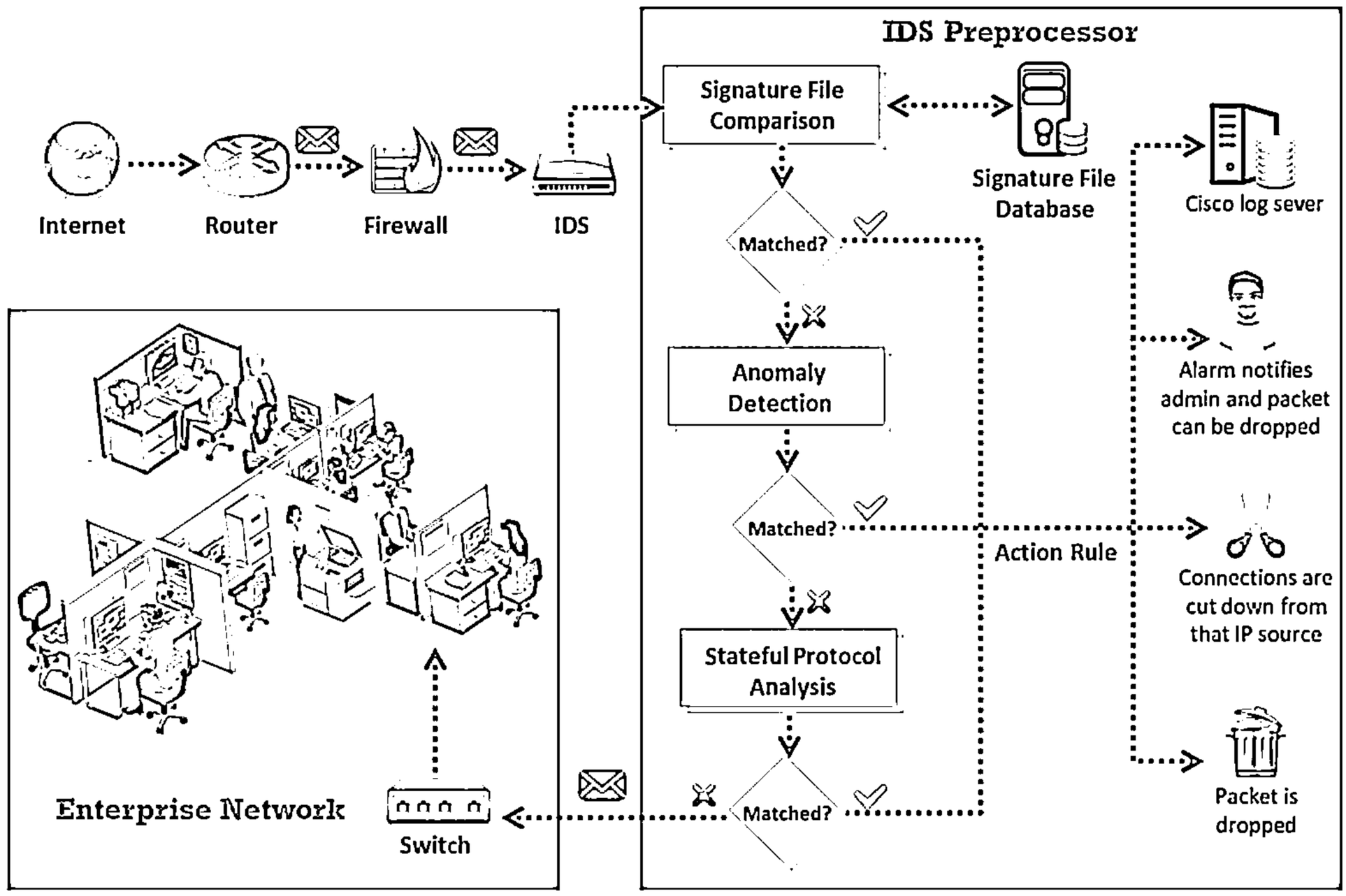


Figure 12.2: Working of IDS

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

How an IDS Detects an Intrusion?

Signature Recognition	Signature recognition, also known as misuse detection, tries to identify events that indicate an abuse of a system or network resource
Anomaly Detection	It detects the intrusion based on the fixed behavioral characteristics of the users and components in a computer system
Protocol Anomaly Detection	In this type of detection, models are built to explore anomalies in the way in which vendors deploy the TCP/IP specification

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

How an IDS Detects an Intrusion?

An IDS uses three methods to detect intrusions in the network.

- **Signature Recognition**

  Signature recognition, also known as misuse detection, tries to identify events that indicate an abuse of a system or network. This technique involves first creating models of possible intrusions and then comparing these models with incoming events to make a detection decision. The signatures for IDS were created under the assumption that the model must detect an attack without disturbing normal system traffic. Only attacks should match the model; otherwise, false alarms could occur.

  - Signature-based intrusion detection compares incoming or outgoing network packets with the binary signatures of known attacks using simple pattern-matching techniques to detect intrusions. Attackers can define a binary signature for a specific portion of the packet, such as TCP flags.
  - Signature recognition can detect known attacks. However, there is a possibility that other innocuous packets contain the same signature, which will trigger a false positive alert.
  - Improper signatures may trigger false alerts. To detect misuse, a massive number of signatures are required. The more the signatures, the greater are the chances are of the IDS detecting attacks; however, the traffic may incorrectly match with the signatures, thus impeding system performance.
  - A large amount of signature data requires more network bandwidth. IDS compare signatures of data packets against those in the signature database. An increase in

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

the number of signatures in the database could result in the dropping of certain packets.

- New virus attacks such as URSNIF and VIRLOCK have driven the need for multiple signatures for a single attack. Changing a single bit in some attack strings can invalidate a signature generated for that attack. Therefore, entirely new signatures are required to detect a similar attack.
- Despite the problems with signature-based IDS, such systems are popular, and they work well when configured correctly and monitored closely.

- **Anomaly Detection**

  Anomaly detection, or "**not-use detection,**" differs from signature recognition. Anomaly detection involves a database of anomalies. An anomaly is detected when an event occurs outside the tolerance threshold of normal traffic. Therefore, any deviation from regular use is an attack. Anomaly detection detects intrusions based on the fixed behavioral characteristics of the users and components in a computer system. Establishing a model of normal use is the most challenging step in creating an anomaly detector.

  - In the traditional method of anomaly detection, essential data are kept for checking variations in network traffic. However, in reality, there is some unpredictability in network traffic, and there are too many statistical variations, thus making these models imprecise. Some events labeled as anomalies might only be irregularities in network usage.
  - In this type of approach, the inability to construct a model thoroughly on a regular network is a concern. These models should be used to check specific networks.

- **Protocol Anomaly Detection**

  Protocol anomaly detection depends on the anomalies specific to a protocol. It identifies particular flaws in vendors' deployment of the TCP/IP protocol. Protocols are designed according to RFC specifications, which dictate standard handshakes to permit universal communication. The protocol anomaly detector can identify new attacks.

  - There are new attack methods and exploits that violate protocol standards.
  - Malicious anomaly signatures are becoming increasingly common. By contrast, the network protocol is well defined and is changing slowly. Therefore, the signature database should frequently be updated to detect attacks.
  - Protocol anomaly detectors are different from traditional IDS in terms of how they present alarms.
  - The best way to present alarms is to explain which part of the state system is compromised. For this purpose, IDS operators must have thorough knowledge of protocol design.

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

General Indications of Intrusions

File System Intrusions

- The presence of new or unfamiliar files, or programs
- Changes in file permissions
- Unexplained changes in a file's size
- Rogue files on the system that do not correspond to the master list of signed files
- Missing files

Network Intrusions

- Repeated probes of the available services on your machines
- Connections from unusual locations
- Repeated login attempts from remote hosts
- A sudden influx of log data

System Intrusions

- Short or incomplete logs
- Unusually slow system performance
- Missing logs or logs with incorrect permissions or ownership
- Modifications to system software and configuration files
- Unusual graphic displays or text messages
- Gaps in system accounting
- System crashes or reboots
- Unfamiliar processes

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

General Indications of Intrusions

Intrusion attempts on networks, systems, or file systems can be identified by following some general indicators:

- **File System Intrusions**

  By observing system files, the presence of an intrusion can be identified. System files record the activities of the system. Any modification or deletion of the file attributes or the file itself is a sign that the system has been a target of an attack:

  - If you find new, unknown files/programs on your system, then there is a possibility that the system has been intruded into. The system can be compromised to the extent that it can, in turn, compromise other network systems.
  - When an intruder gains access to a system, he or she tries to escalate privileges to gain administrative access. When the intruder obtains administrator privileges, he/she could change file permissions, for example, from read-only to write.
  - Unexplained modifications in file size are also an indication of an attack. Make sure you analyze all your system files.
  - The presence of rogue suid and sgid files on your Linux system that do not match your master list of suid and sgid files could indicate an attack.
  - You can identify unfamiliar file names in directories, including executable files with strange extensions and double extensions.
  - Missing files are also a sign of a probable intrusion/attack.

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

- **Network Intrusions**

  Similarly, general indications of network intrusions include:

  - A sudden increase in bandwidth consumption
  - Repeated probes of the available services on your machines
  - Connection requests from IPs other than those in the network range, which imply that an unauthenticated user (intruder) is attempting to connect to the network
  - Repeated login attempts from remote hosts
  - A sudden influx of log data, which could indicate attempts at DoS attacks, bandwidth consumption, and DDoS attacks

- **System Intrusions**

  Similarly, general indications of system intrusions include:

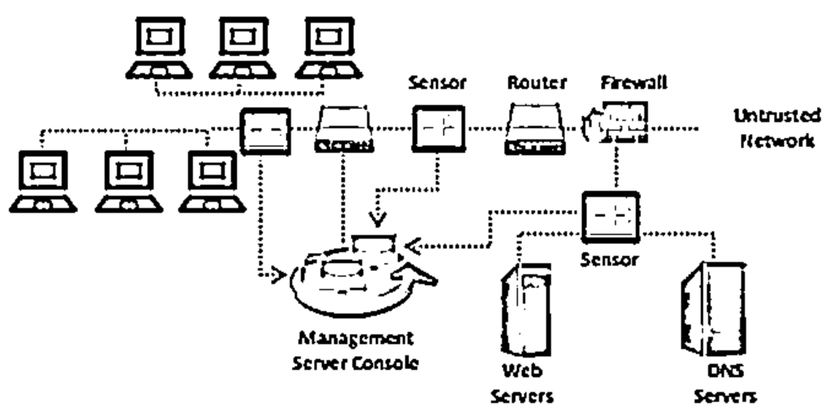
  - Sudden changes in logs such as short or incomplete logs
  - Unusually slow system performance
  - Missing logs or logs with incorrect permissions or ownership
  - Modifications to system software and configuration files
  - Unusual graphic displays or text messages
  - Gaps in system accounting
  - System crashes or reboots
  - Unfamiliar processes

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

Types of Intrusion Detection Systems

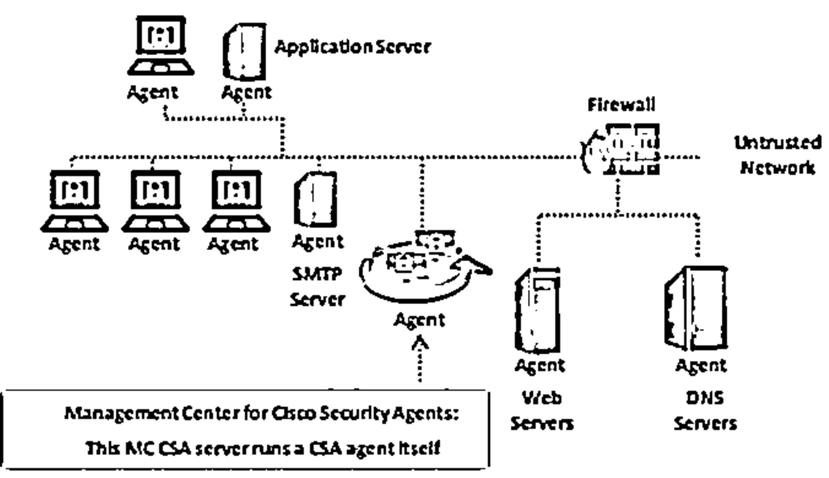
Network-Based Intrusion Detection Systems

- These systems typically consist of a black box that is placed on the network in a promiscuous mode, listening for patterns indicative of an intrusion
- It detects malicious activity such as Denial-of-Service attacks, port scans, or even attempts to crack into computers by monitoring network traffic



Host-Based Intrusion Detection Systems

- These systems usually include auditing for events that occur on a specific host
- These are not as common, due to the overhead they incur by having to monitor each system event



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

Types of Intrusion Detection Systems

There are two types of intrusion detection systems:

- **Network-Based Intrusion Detection Systems**

  Network-based intrusion detection systems (NIDS) check every packet entering the network for the presence of anomalies and incorrect data. By limiting the firewall to drop large numbers of data packets, the NIDS checks every packet thoroughly. A NIDS captures and inspects all traffic. It generates alerts at the IP or application level based on the content. NIDS are more distributed than host-based IDS. The NIDS identifies the anomalies at the router and host levels. It audits the information contained in the data packets and logs the information of malicious packets; furthermore, it assigns a threat level to each risk after receiving the data packets. The threat level enables the security team to remain on alert. These mechanisms typically consist of a black box placed on the network in a promiscuous mode, listening for patterns indicative of an intrusion. It detects malicious activity such as DoS attacks, port scans, or even attempts to break into computers by monitoring network traffic.

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

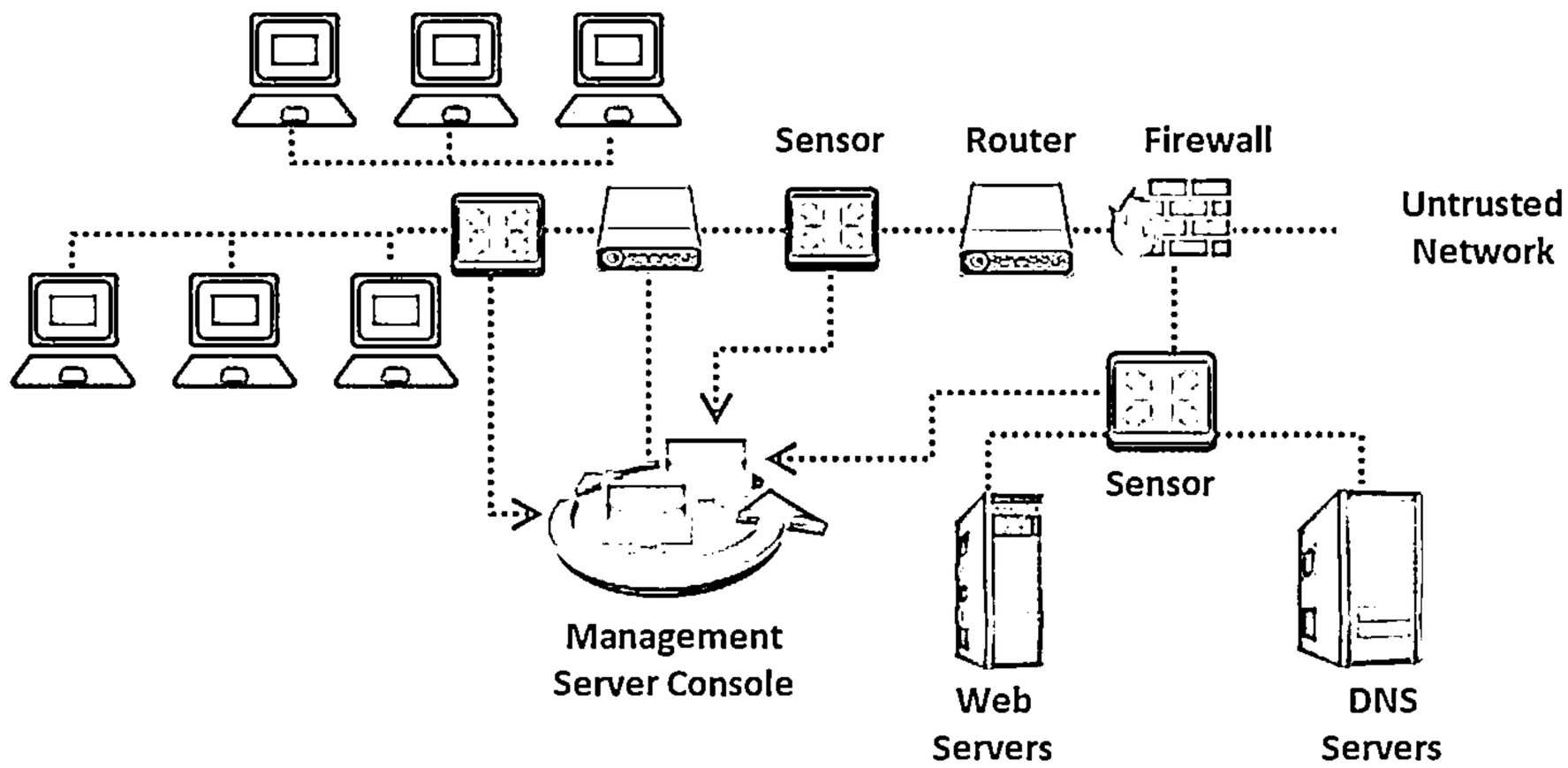


Figure 12.3: Network-based IDS (NIDS)

- **Host-Based Intrusion Detection Systems**

  A host-based IDS (HIDS) analyzes each system's behavior. The HIDS can be installed on any system ranging from a desktop PC to a server. It is more versatile than the NIDS. In addition to detecting unauthorized insider activity, host-based systems are also effective in detecting unauthorized file modification. The HIDS focuses on the changing aspects of local systems. It is also more platform-centric, with a greater focus on the Windows OS; nevertheless, other HIDS are available for UNIX platforms. These mechanisms usually include auditing events that occur on a specific host. They are not very common because of the overhead they incur by having to monitor each system event.

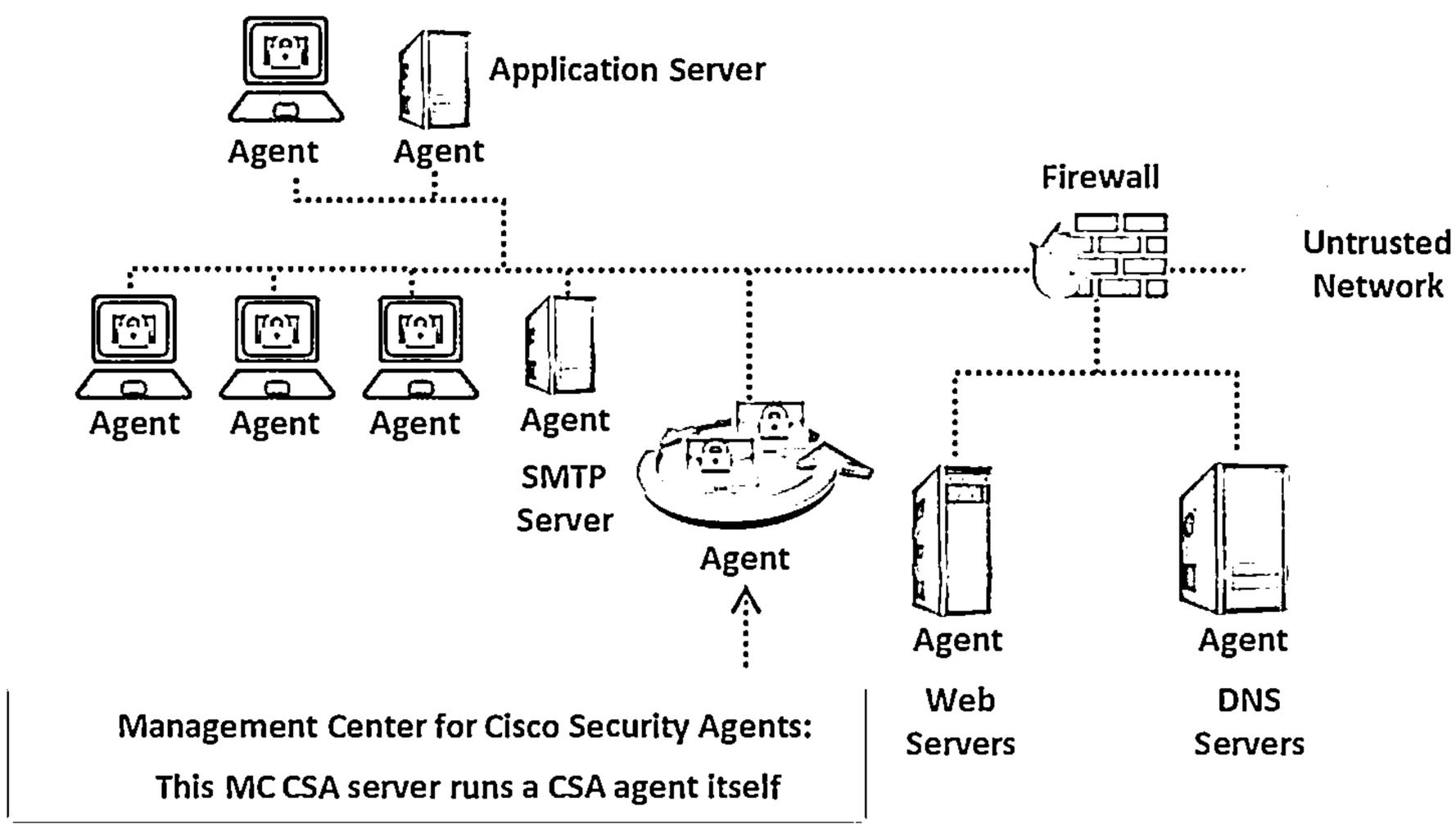


Figure 12.4: Host-based IDS (HIDS)

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

Types of IDS Alerts

True Positive (Attack - Alert)	An IDS raises an alarm when a legitimate attack occurs ✓✓
False Positive (No Attack - Alert)	An IDS raises an alarm when no attack has taken place ✗✓
False Negative (Attack - No Alert)	An IDS does not raise an alarm when a legitimate attack has taken place ✗✗
True Negative (No Attack - No Alert)	An IDS does not raise an alarm when an attack has not taken place ✓✗

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

Types of IDS Alerts

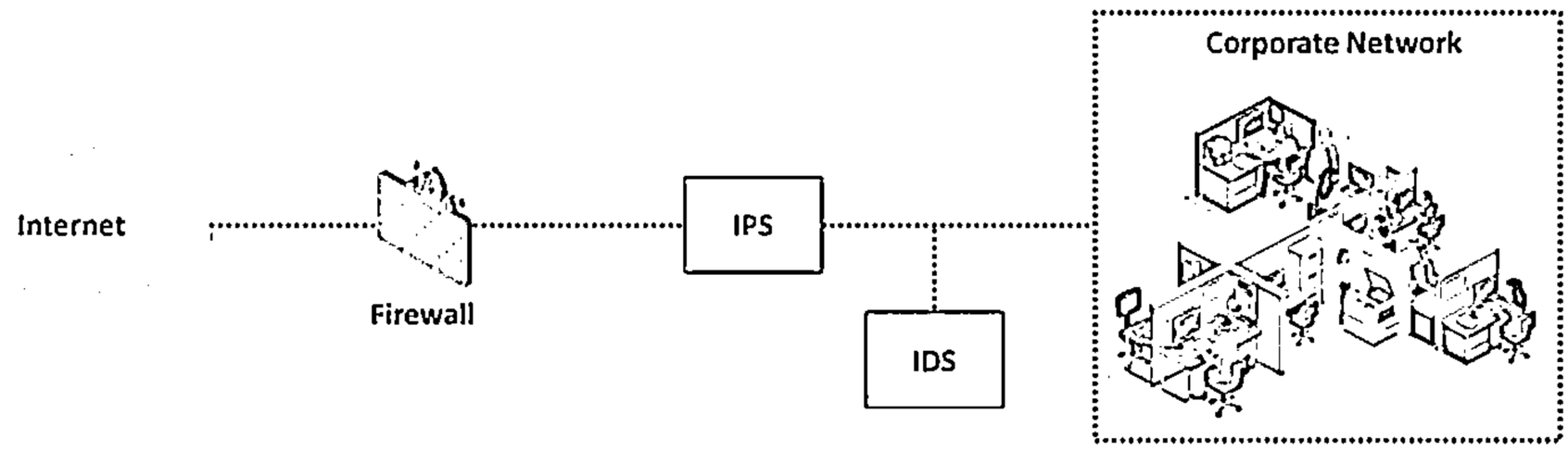
An IDS generates four types of alerts: True Positive, False Positive, False Negative, and True Negative.

- **True Positive (Attack - Alert)**: A true positive is a condition that occurs when an event triggers an alarm and causes the IDS to react as if a real attack is in progress. The event may be an actual attack, in which case an attacker attempts to compromise the network, or it may be a drill, in which case security personnel use hacker tools to test a network segment.
- **False Positive (No attack - Alert)**: A false positive occurs if an event triggers an alarm when no actual attack is in progress. It occurs when an IDS treats regular system activity as an attack. False positives tend to make users insensitive to alarms and weaken their reactions to actual intrusion events. While testing the configuration of an IDS, administrators use false positives to determine whether the IDS can distinguish between false positives and real attacks.
- **False Negative (Attack - No Alert)**: A false negative is a condition that occurs when an IDS fails to react to an actual attack event. This condition is the most dangerous failure, as the purpose of an IDS is to detect and respond to attacks.
- **True Negative (No attack - No Alert)**: A true negative is a condition that occurs when an IDS identifies an activity as acceptable behavior and the activity is acceptable. A true negative means successfully ignoring acceptable behavior. It is not harmful, as the IDS performs as expected in this case.

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

Intrusion Prevention System (IPS)

- An intrusion prevention system (IPS) is also considered as an active IDS since it is capable of not only detecting the intrusions but also preventing them
- It is a continuous monitoring system that often sits behind the firewalls as an additional layer of protection
- Unlike an IDS, which is passive, an IPS is placed inline in the network, between the source and destination to actively analyze the network traffic and to automatically take decisions on the traffic that is entering the network



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

Intrusion Prevention System (IPS)

Intrusion prevention systems (IPS) are considered as active IDS, as they are capable of not only detecting intrusions but also preventing them. IPS are continuous monitoring systems that often sit behind firewalls as an additional layer of protection. Unlike IDS, which are passive, IPS are placed inline in the network, between the source and the destination, to actively analyze the network traffic and make automated decisions regarding the traffic that is entering the network.

Some of the actions that an IPS is meant to perform are as follows:

- Generate alerts if any abnormal traffic is detected in the network
- Continuously record real-time logs of network activities
- Block and filter malicious traffic
- Detect and eliminate threats quickly, as it is placed inline in the operational network
- Identify threats accurately without generating false positives

An IPS takes actions based on certain rules and policies configured into it. In other words, the IPS can identify, log, and prevent the occurrence of any intrusion or attack in the network. IPS can also be employed to detect critical issues in corporate security policies such as notorious insider threats, malicious network guests, etc.

Classification of IPS:

Like IDS, IPS are also classified into two types:

- Host-based IPS
- Network-based IPS

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

Advantages of IPS over IDS:

- Unlike IDS, IPS can block as well as drop illegal packets in the network
- IPS can be used to monitor activities occurring in a single organization
- IPS can prevent the occurrence of direct attacks in the network by controlling the amount of network traffic

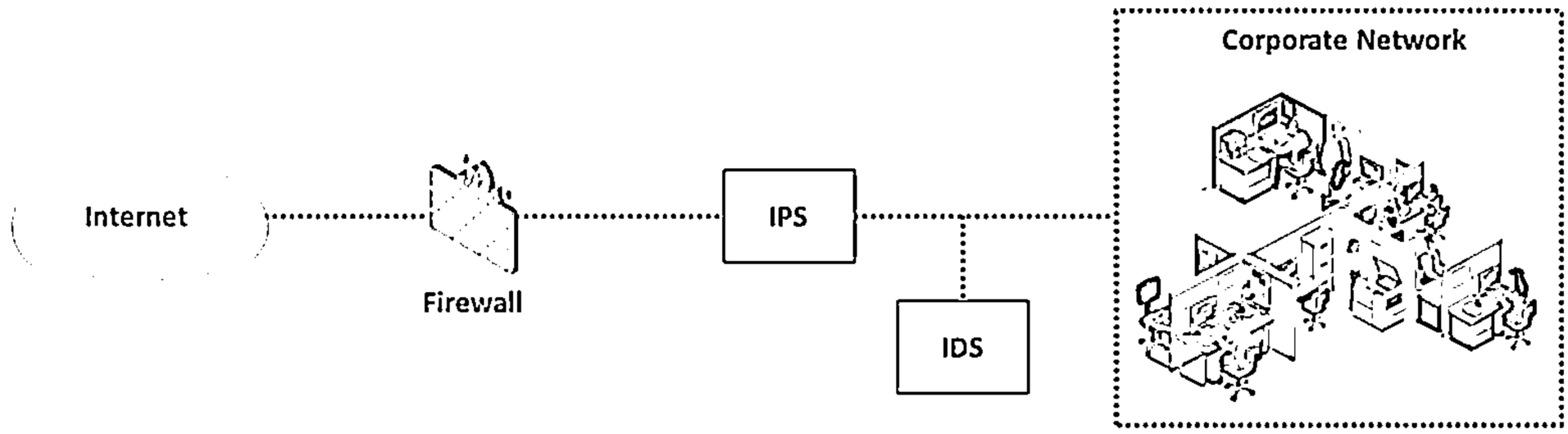
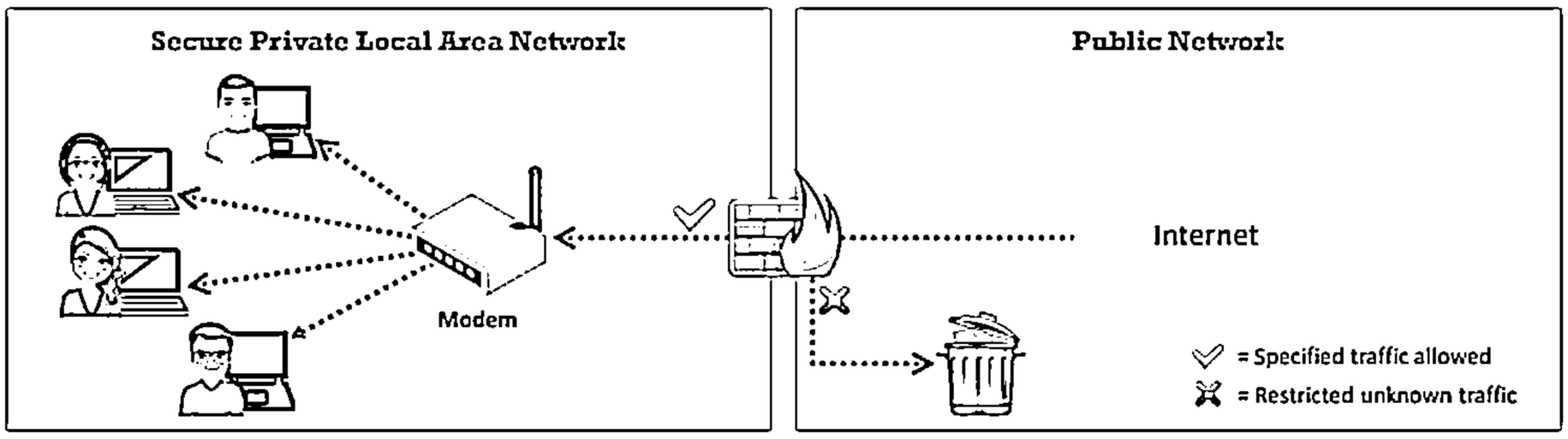


Figure 12.5: Example of an IPS placement

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

Firewall

- Firewalls are hardware and/or software designed to prevent unauthorized access to or from a private network
- They are placed at the junction or gateway between two networks, which is usually between a private network and a public network such as the Internet
- Firewalls examine all messages entering or leaving the Intranet (or private network) and block those that do not meet the specified security criteria



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

Firewall

A firewall is a software- or hardware-based system located at the network gateway that protects the resources of a private network from unauthorized access by users on other networks. They are placed at the junction or gateway between two networks, usually a private network and a public network such as the Internet. Firewalls examine all the messages entering or leaving the intranet and block those that do not meet the specified security criteria. Firewalls may be concerned with the type of traffic or with the source or destination addresses and ports. They include a set of tools that monitor the flow of traffic between networks. A firewall placed at the network level and working closely with the router filters all the network packets to determine whether to forward them toward their destinations. Always install firewalls away from the rest of the network, so that none of the incoming requests can gain direct access to a private network resource. If appropriately configured, the firewall protects systems on one side of it from systems on the other side.

- A firewall is an intrusion detection mechanism that is designed by an organization's security policy. Its settings can change to make appropriate changes to its functionality.
- Firewalls can be configured to restrict incoming traffic to POP and SMTP and to enable email access. Certain firewalls block specific email services to avoid spam.
- A firewall can be configured to check inbound traffic at a "checkpoint," where a security audit is performed. It can also act as an active "phone tap" tool for identifying an intruder's attempt to dial into modems in a secured network. Firewall logs consist of logging information that notifies the administrator about all attempts to access various services.

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

- The firewall verifies the incoming and outgoing traffic against its rules and acts as a router to move data between networks. The firewall allows or denies access requests made from one side of it to services on the other side.
- Identify all the attempts to log into the network for auditing. Unauthorized attempts can be identified by embedding an alarm that is triggered when an unauthorized user attempts to log in. Firewalls can filter packets based on the address and type of traffic. They recognize the source and destination addresses as well as port numbers during address filtering, and they identify the types of network traffic during protocol filtering. Firewalls can identify the state and attributes of data packets.

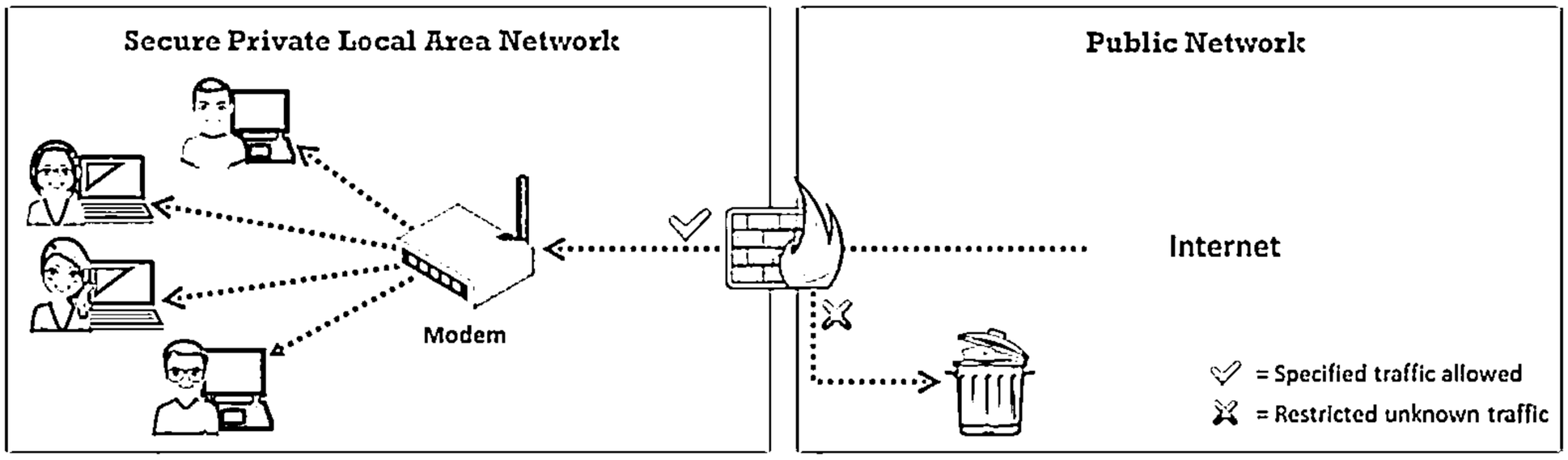
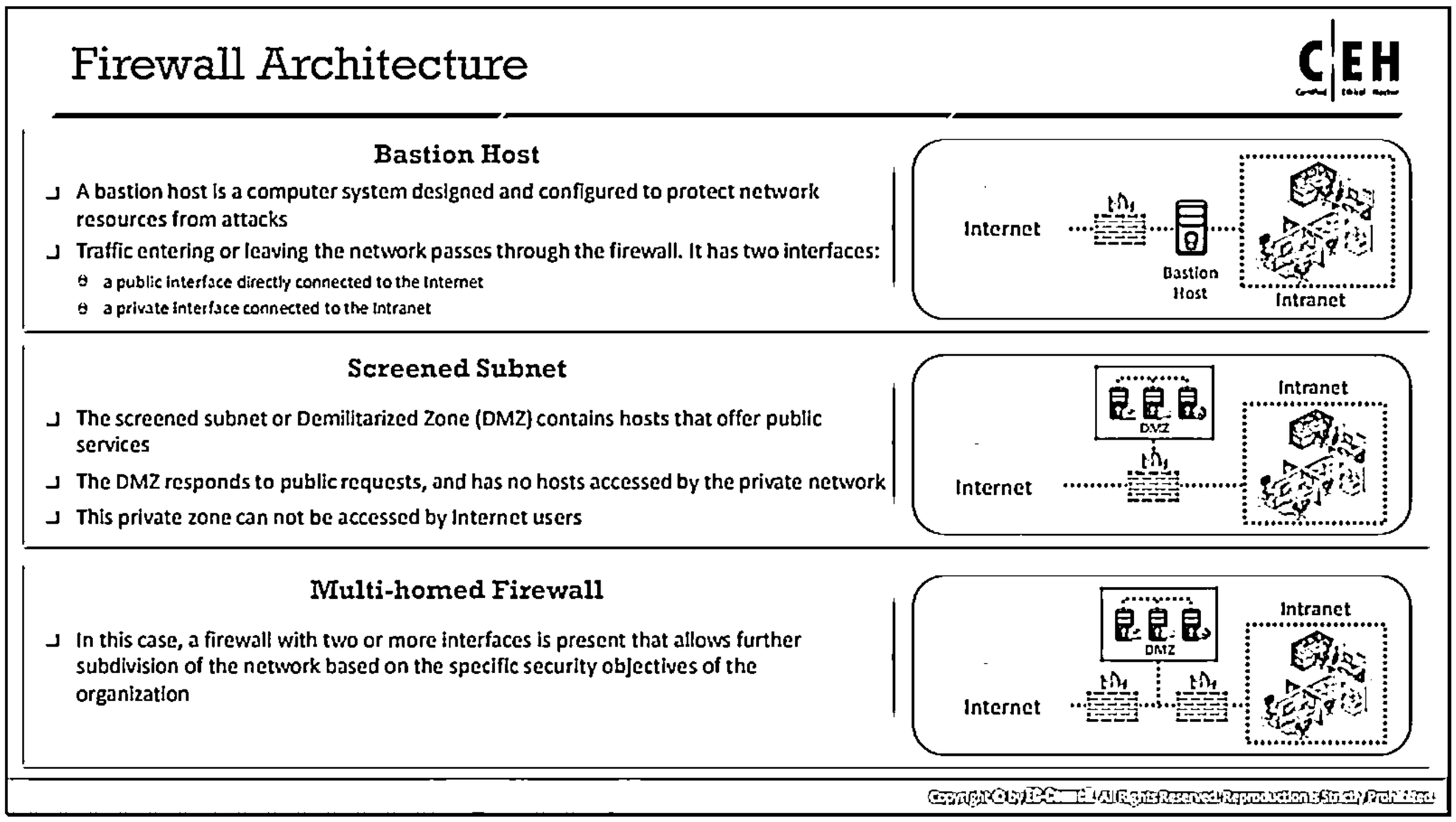


Figure 12.6: Example of a Firewall

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



Firewall Architecture

The firewall architecture consists of the following elements:

- **Bastion Host**

  The bastion host is designed for defending the network against attacks. It acts as a mediator between inside and outside networks. A bastion host is a computer system designed and configured to protect network resources from attacks. Traffic entering or leaving the network passes through the firewall. It has two interfaces:

  - Public interface directly connected to the Internet
  - Private interface connected to the intranet

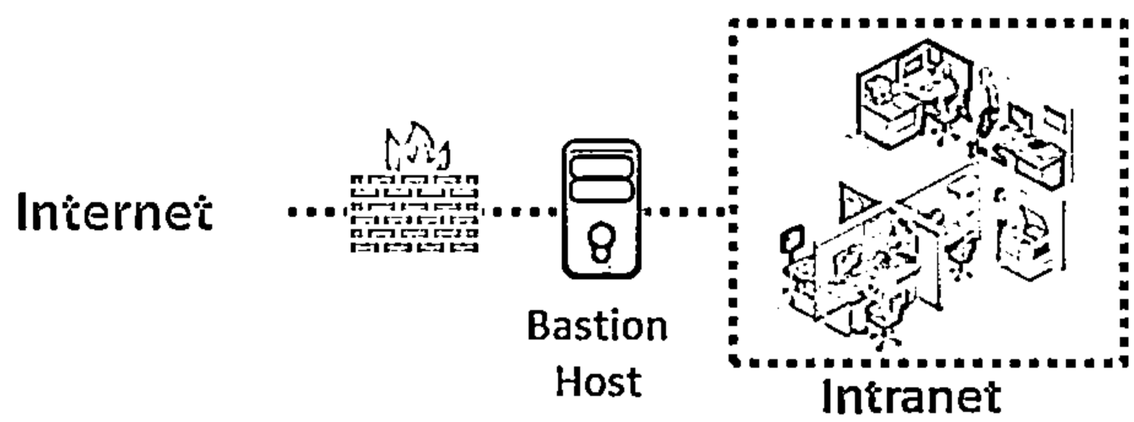


Figure 12.7: Bastion Host Firewall

- **Screened Subnet**

  A screened subnet (DMZ) is a protected network created with a two- or three-homed firewall behind a screening firewall, and it is a term that is commonly used to refer to the DMZ. When using a three-homed firewall, connect the first interface to the Internet, the second to the DMZ, and the third to the intranet. The DMZ responds to public

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

requests and has no hosts accessed by the private network. Internet users cannot access the private zone.

The advantage of screening a subnet away from the intranet is that public requests can be responded to without allowing traffic into the intranet. A disadvantage of the three-homed firewall is that if it is compromised, both the DMZ and the intranet could also be compromised. A safer technique is to use multiple firewalls to separate the Internet from the DMZ, and to then separate the DMZ from the intranet.

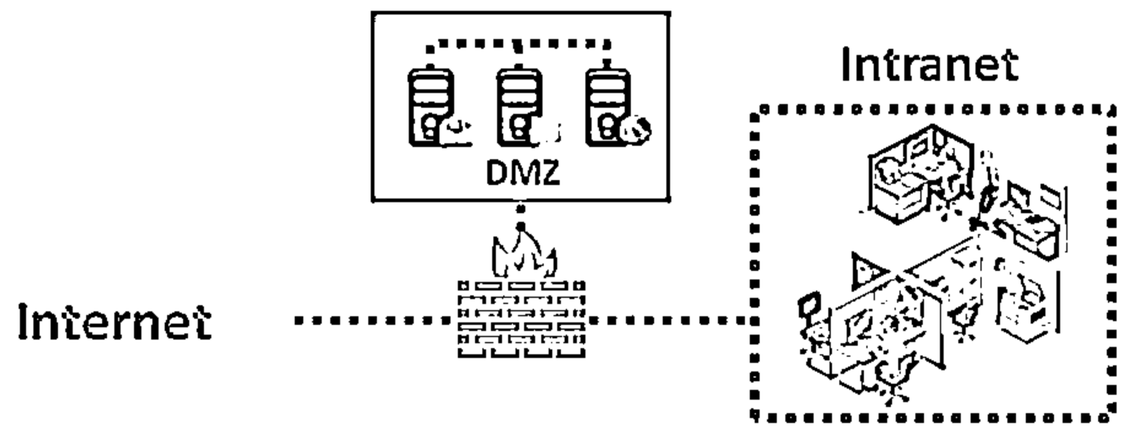


Figure 12.8: Screened Subnet Firewall

- **Multi-homed Firewall**

  A multi-homed firewall is a node with multiple NICs that connects to two or more networks. It connects each interface to separate network segments logically and physically. A multi-homed firewall helps in increasing the efficiency and reliability of an IP network. The multi-homed firewall has more than three interfaces that allow for further subdividing the systems based on the specific security objectives of the organization. However, the model that provides deeper protection is the back-to-back firewall.

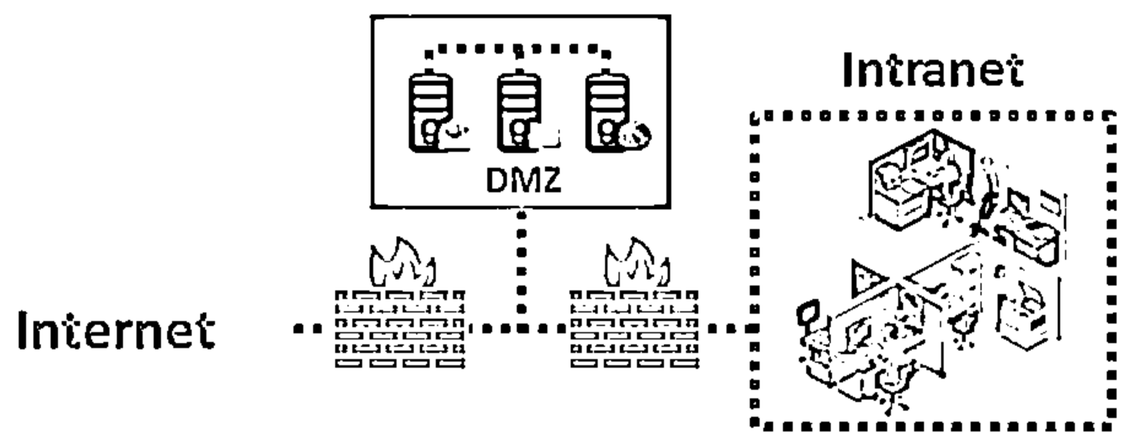
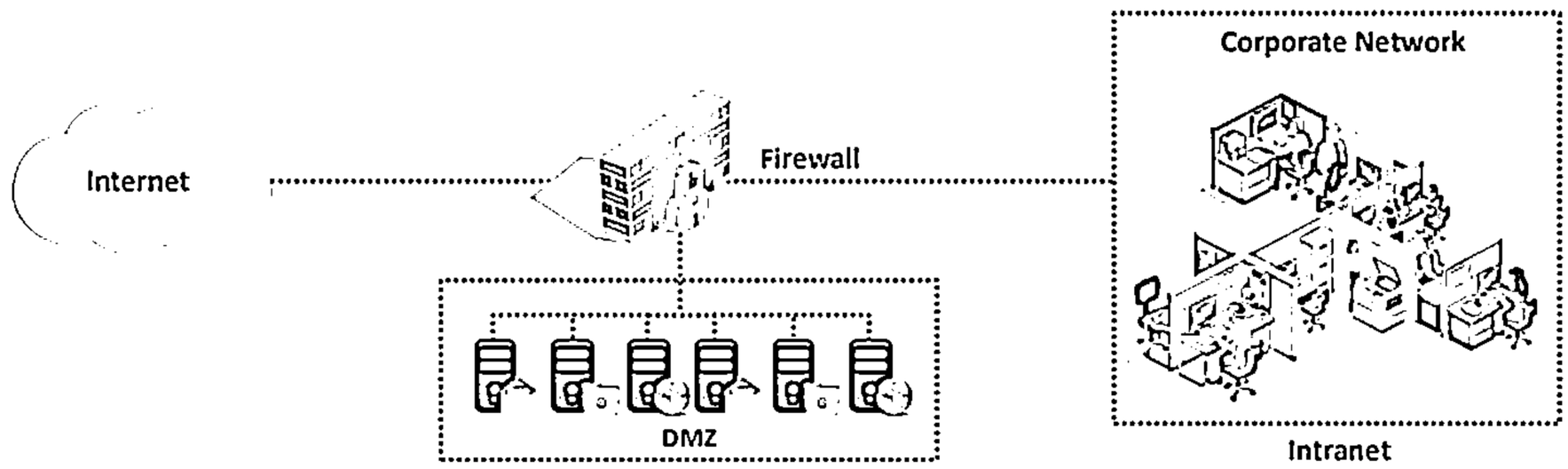


Figure 12.9: Multi-homed Firewall

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

Demilitarized Zone (DMZ)

- The DMZ is a network that serves as a buffer between the internal secure network and the insecure Internet
- It can be created using a firewall with three or more network interfaces, assigned with specific roles such as the internal trusted network, the DMZ network, and the external un-trusted network



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

Demilitarized Zone (DMZ)

In computer networks, the demilitarized zone (DMZ) is an area that hosts computer(s) or a small sub-network placed as a neutral zone between a particular company's internal network and an untrusted external network to prevent outsider access to a company's private data. The DMZ serves as a buffer between the secure internal network and the insecure Internet, as it adds a layer of security to the corporate LAN, thus preventing direct access to other parts of the network.

A DMZ is created using a firewall with three or more network interfaces that are assigned specific roles, such as an internal trusted network, a DMZ network, or an external untrusted network (Internet). Any service such as email, web, or FTP that provides access to external users can be placed in the DMZ. However, web servers that communicate with database servers cannot reside in the DMZ, as they could give outside users direct access to sensitive information. There are many ways in which the DMZ can be configured according to specific network topologies and company requirements.

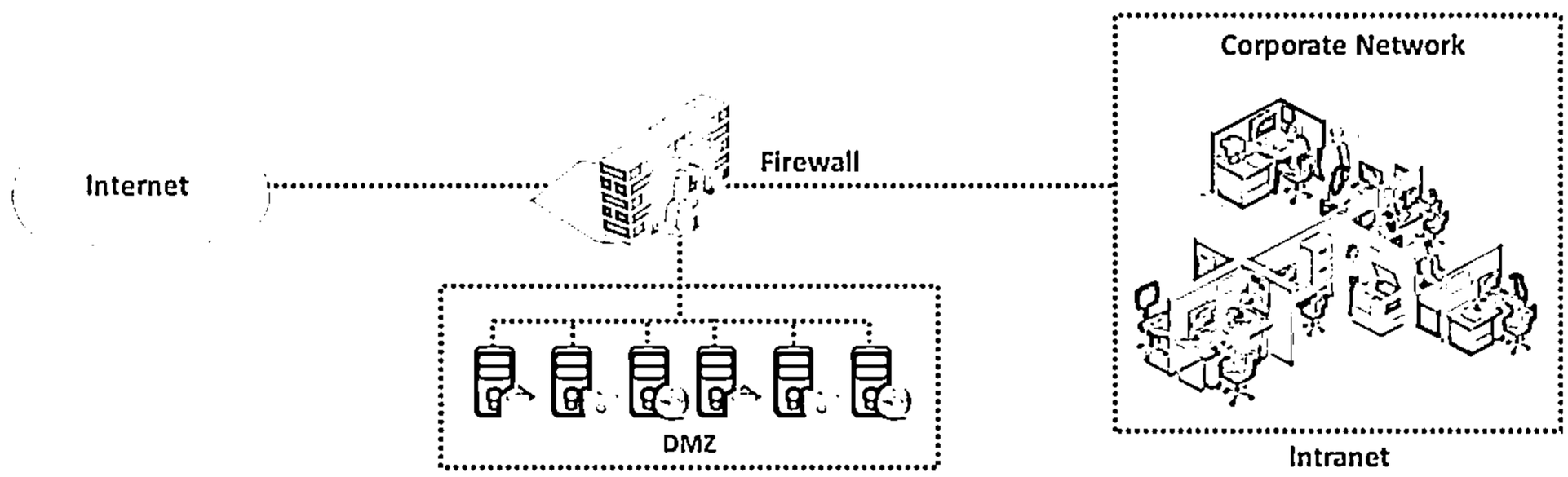
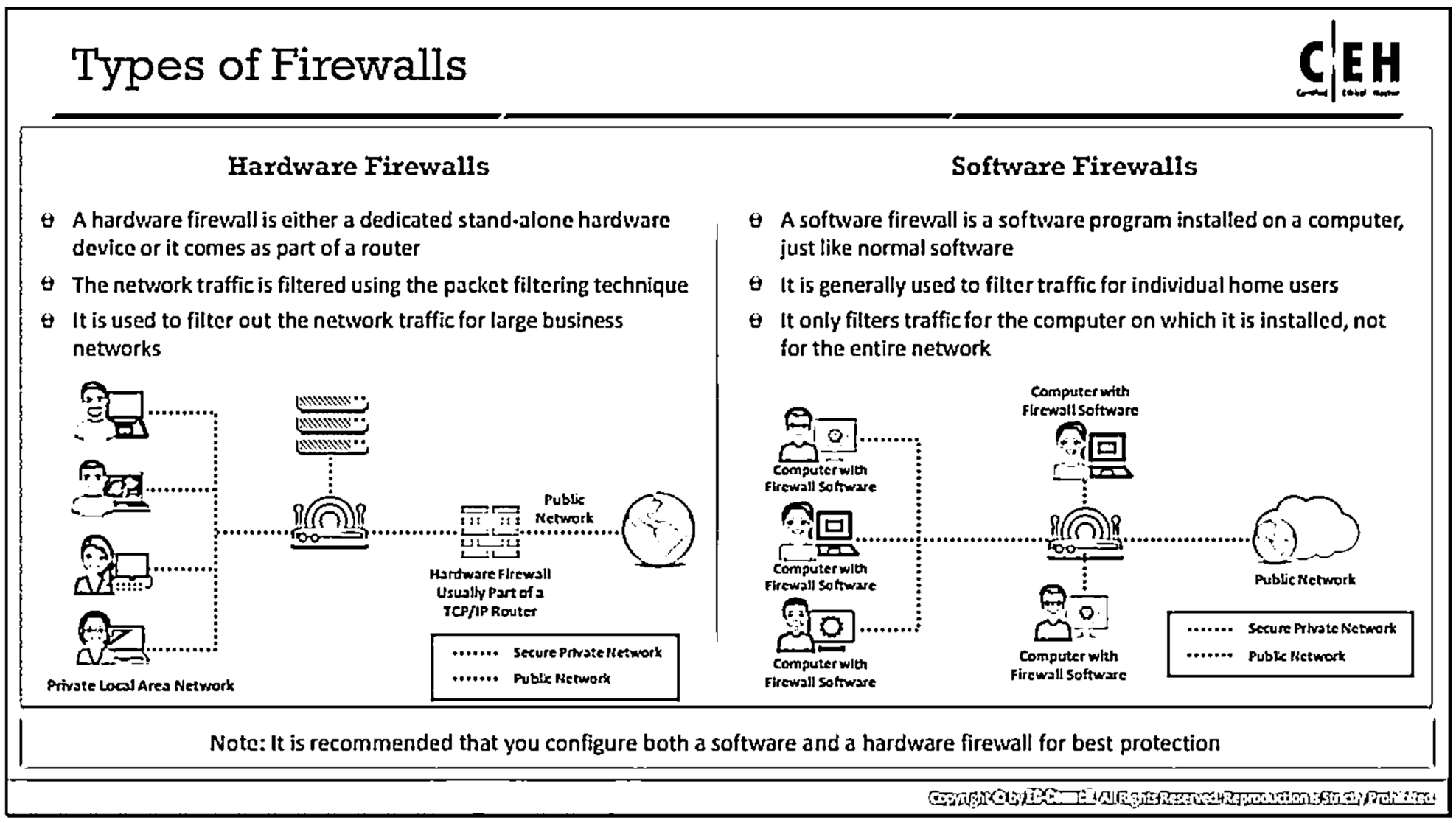


Figure 12.10: Demilitarized Zone (DMZ)

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



Types of Firewalls

There are two types of firewalls.

- **Hardware Firewalls**

  A hardware firewall is a dedicated firewall device placed on the perimeter of the network. It is an integral part of the network setup and is also built into broadband routers or used as a standalone product. A hardware firewall helps to protect systems on the local network and performs effectively with little or no configuration. It employs the technique of packet filtering. It reads the header of a packet to find out the source and destination addresses, and compares them with a set of predefined and/or user-created rules that determine whether it should forward or drop the packet. A hardware firewall functions on an individual system or a particular network connected using a single interface. Examples of hardware firewalls include Cisco ASA and FortiGate. Hardware firewalls protect the private local area network.

  However, hardware firewalls are expensive as well as difficult to implement and upgrade.

  Advantages:

  - Security: A hardware firewall with its operating system (OS) is considered to reduce security risks and increase the level of security controls.
  - Speed: Hardware firewalls initiate faster responses and enable more traffic.
  - Minimal Interference: Since a hardware firewall is a separate network component, it enables better management and allows the firewall to shut down, move, or be reconfigured without much interference in the network.

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

Disadvantages:

- More expensive than a software firewall.
- Difficult to implement and configure.
- Consumes more space and involves cabling.

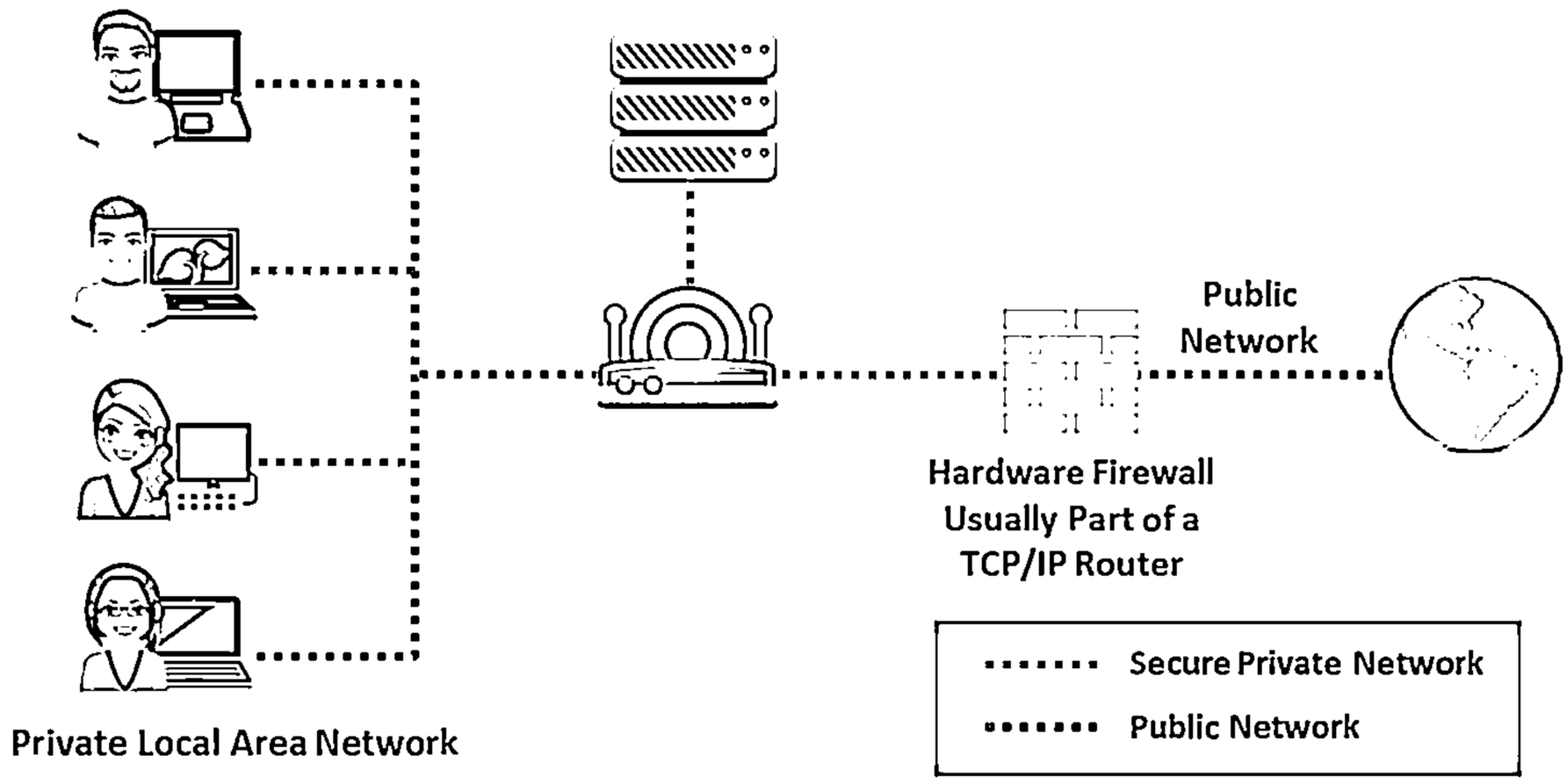


Figure 12.11: Hardware Firewall

- **Software Firewalls**

  A software firewall is similar to a filter. It sits between a regular application and the networking components of the OS. It is more useful for individual home users and it is suitable for mobile users who need digital security when working outside the corporate network. Further, it is easy to install on an individual's PC, notebook, or workgroup server. It helps protect your system from outside attempts at unauthorized access and provides protection against everyday Trojans and email worms. It includes privacy controls, web filtering, and more. A software firewall implants itself in the critical area of the application/network path. It analyzes the data flow against the rule set.

  The configuration of a software firewall is simple compared to that of a hardware firewall. A software firewall intercepts all requests from a network to the computer to determine if they are valid and protects the computer from attacks and unauthorized access. It incorporates user-defined controls, privacy controls, web filtering, content filtering, etc., to restrict unsafe applications from running on an individual system. Software firewalls use more resources than hardware firewalls, which reduces the speed of the system. Examples of software firewalls include those produced by Norton, McAfee, and Kaspersky.

  Advantages:

  - Less expensive than hardware firewalls.
  - Ideal for personal or home use.

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

- Easier to configure and reconfigure.

Disadvantages:

- Consumes system resources.
- Difficult to uninstall.
- Not appropriate for environments requiring faster response times.

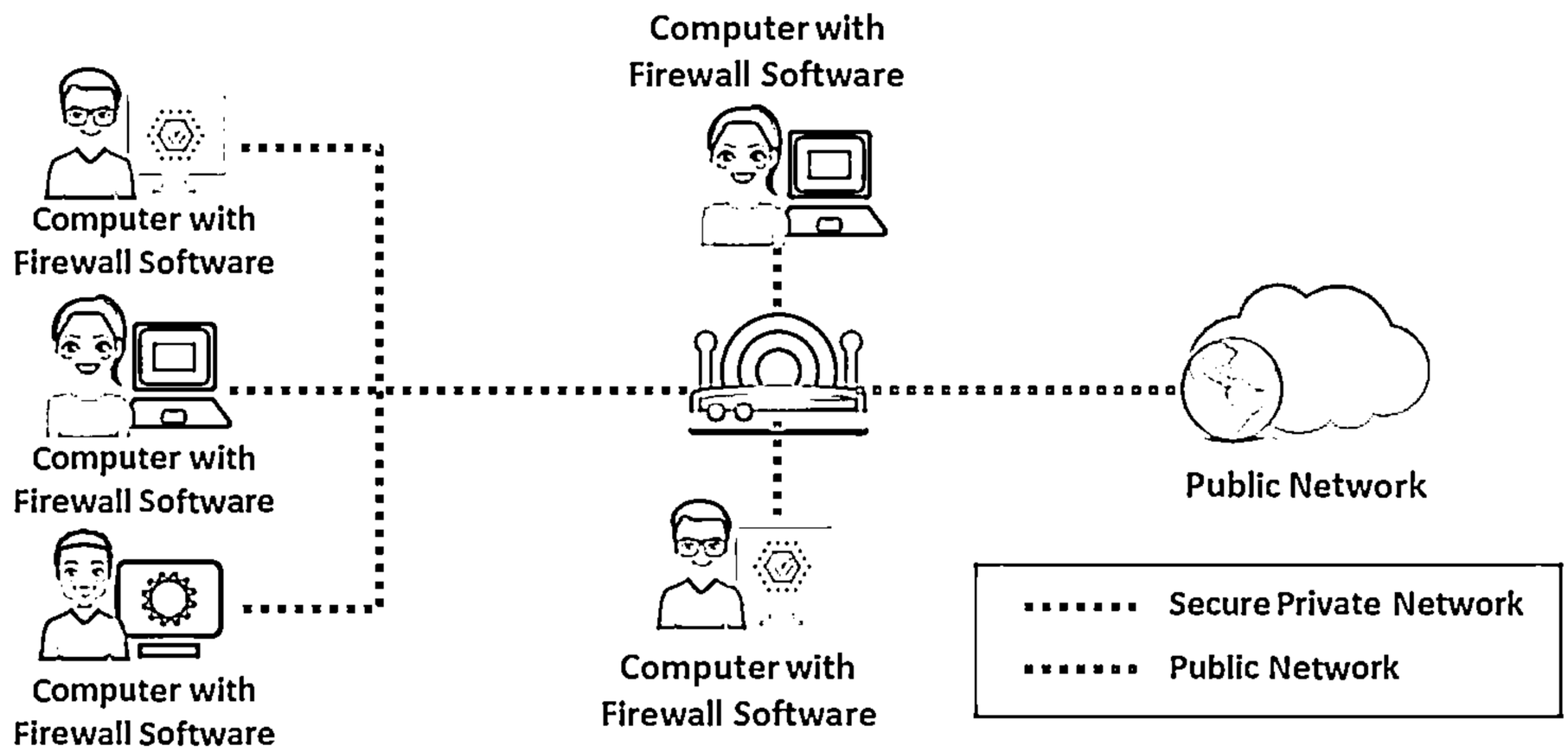


Figure 12.12: Software Firewall

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

Firewall Technologies

- Firewalls are designed and developed with the help of different firewall services
- Each firewall service provides security, depending on its efficiency and sophistication

Technologies used for creating a firewall service

1. Packet Filtering
2. Circuit Level Gateways
3. Application Level Firewall
4. Stateful Multilayer Inspection
5. Application Proxies
6. Virtual Private Network
7. Network Address Translation

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

Firewall Technologies

Firewalls are designed and developed with the help of different firewall services. Each firewall service provides security depending on its efficiency and sophistication. There are different types of firewall technologies depending on where the communication is taking place, where the traffic is intercepted in the network, the state that is traced, and so on. Considering the capabilities of different firewalls, it is easy to choose and place an appropriate firewall to meet the security requirements in the best possible way. Each type of firewall has its advantages.

Several firewall technologies are available for organizations to implement their security measures. Sometimes, firewall technologies are combined with other technologies to build another firewall technology. For example, NAT is a routing technology; however, when it is combined with a firewall, it is considered a firewall technology.

The various firewall technologies are listed below:

- Packet Filtering
- Circuit-Level Gateways
- Application-Level Firewall
- Stateful Multilayer Inspection
- Application Proxies
- Virtual Private Network
- Network Address Translation

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

The table below summarizes technologies operating at each OSI layer:

OSI Layer	Firewall Technology
Application	▪ Virtual Private Network (VPN) ▪ Application Proxies
Presentation	▪ Virtual Private Network (VPN)
Session	▪ Virtual Private Network (VPN) ▪ Circuit-Level Gateways
Transport	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Network	▪ Virtual Private Network (VPN) ▪ Network Address Translation (NAT) ▪ Packet Filtering ▪ Stateful Multilayer Inspection
Data Link	▪ Virtual Private Network (VPN) ▪ Packet Filtering
Physical	▪ Not Applicable

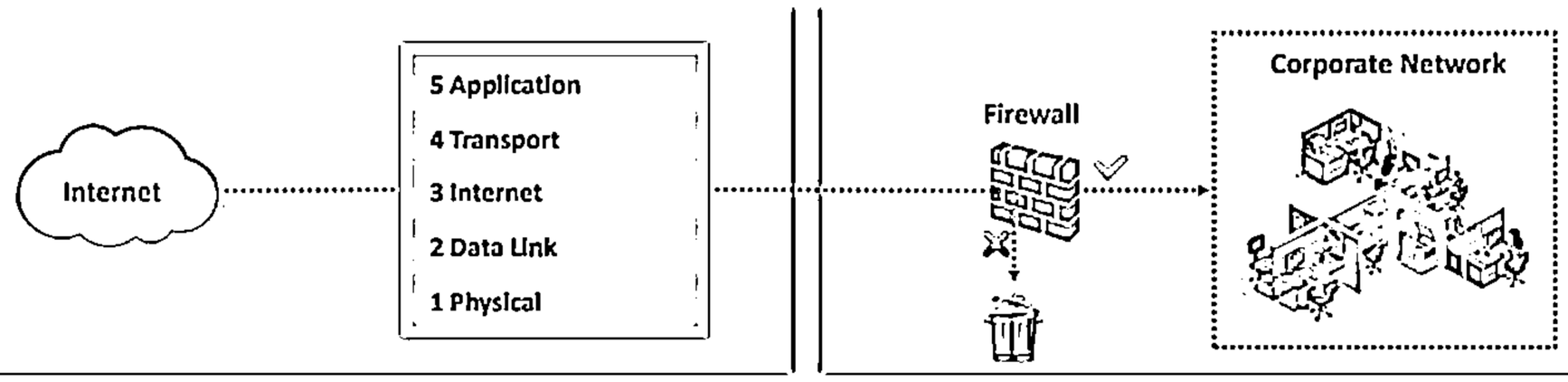
Table 12.1: Firewall Technologies

The security levels of these technologies vary according to their efficiency levels. A comparison of these technologies can be made by allowing them to pass through the OSI layer between the hosts. The data passes through the intermediate layers from a higher layer to a lower layer. Each layer adds additional information to the data packets. The lower layer now sends the obtained information through the physical network to the upper layers and then to its destination.

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

Packet Filtering Firewall

- Packet filtering firewalls work at the network layer of the OSI model (or the internet layer of TCP/IP). They usually form part of a router
- In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded
- Depending on the packet and the criteria, the firewall can drop the packet, forward it, or send a message to the originator
- Rules can include the source and destination IP address, the source and destination port number, and the protocol used



✓ = Traffic allowed based on source and destination IP address, packet type, and port number
✗ = Disallowed Traffic

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

Packet Filtering Firewall

In a packet filtering firewall, each packet is compared with a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet and transmit it or send a message to the originator. The rules can include the source and the destination IP address, the source and the destination port number, and the protocol used. It works at the internet layer of the TCP/IP model or the network layer of the OSI model. Packet filtering firewalls focus on individual packets, analyze their header information, and determine which way they need to be directed. Traditional packet filters make this decision according to the following information in a packet:

- **Source IP address**: Used to check whether the packet is coming from a valid source. The information about the source IP address can found from the IP header of the packet.
- **Destination IP address**: Checks if the packet is going to the correct destination and if the destination accepts these types of packets. The information about the destination IP address can found from the IP header of the packet.
- **Source TCP/UDP port**: Used to check the source port of the packet
- **Destination TCP/UDP port**: Used to monitor the destination port regarding the services to be allowed and the services to be denied.
- **TCP flag bits**: Used to check whether the packet has SYN, ACK, or other bits set for the connection to be made.
- **Protocol in use**: Used to check whether the protocol that the packet is carrying should be allowed.
- **Direction**: Used to check whether the packet is entering or leaving the private network.

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

- **Interface:** Used to check whether the packet is coming from an unreliable zone.

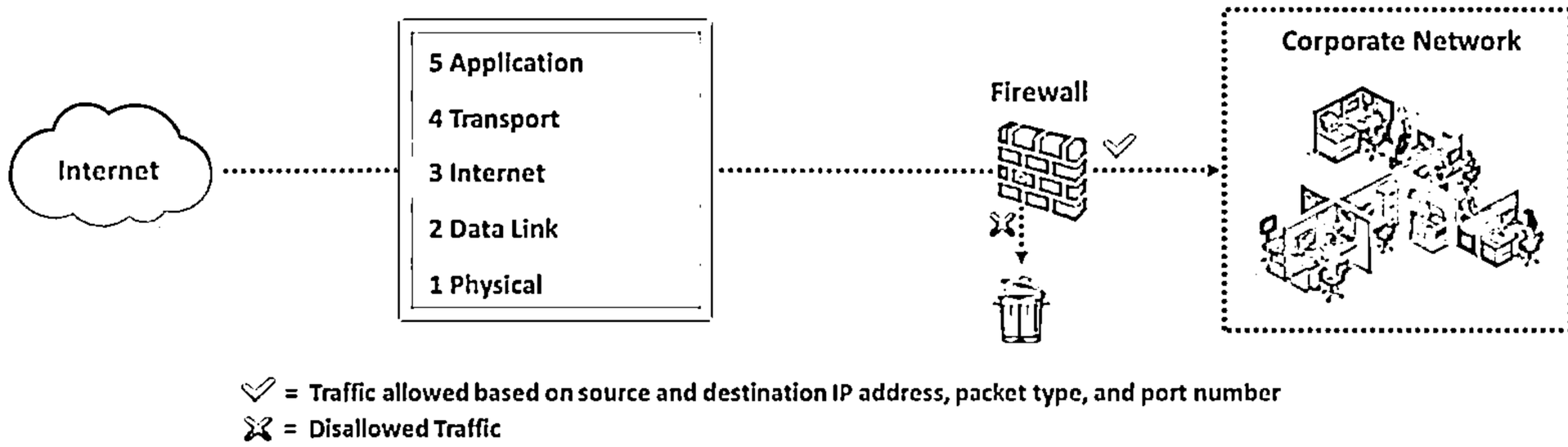
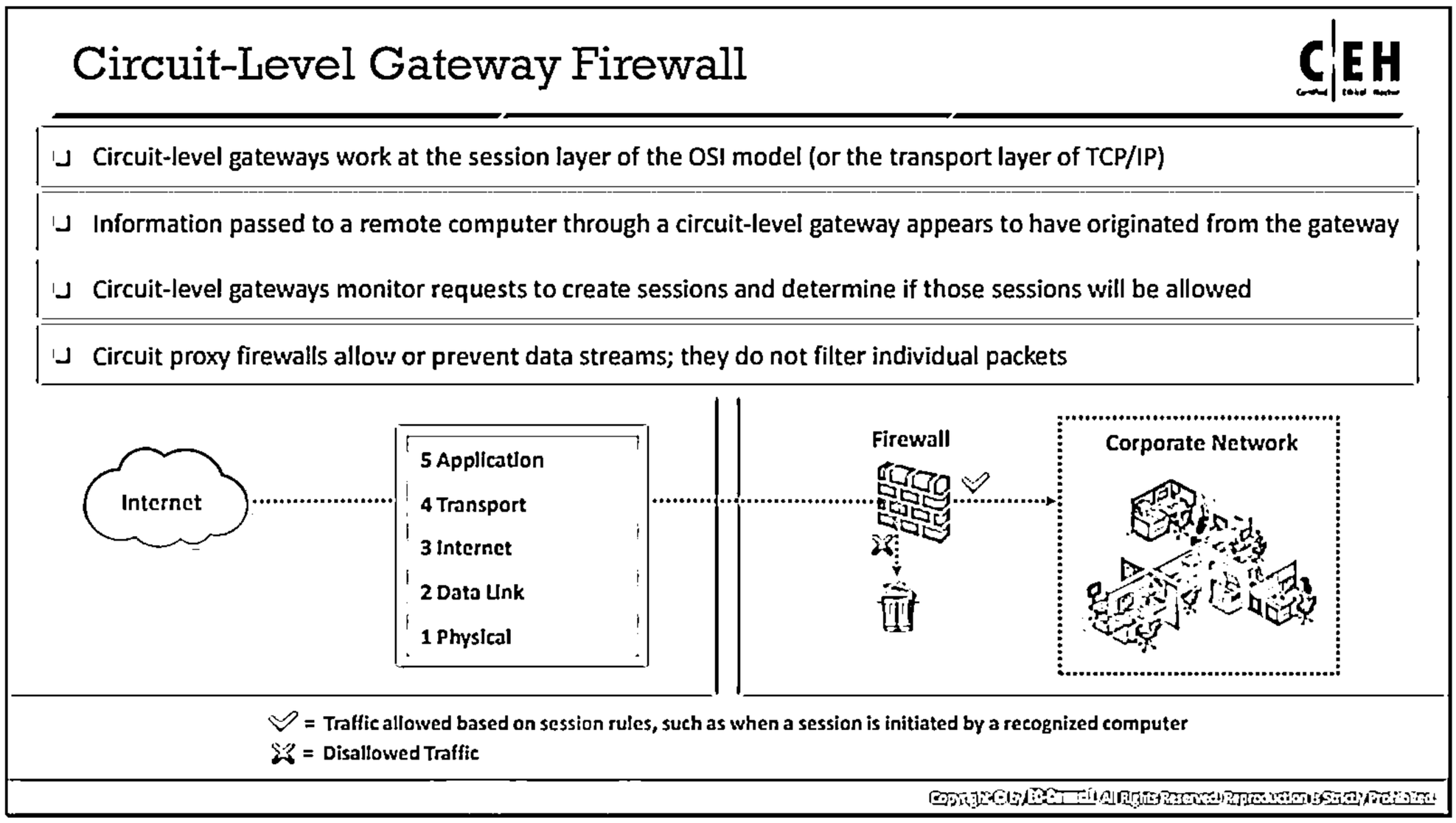


Figure 12.13 Example of Packet Filtering Firewall

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



Circuit-Level Gateway Firewall

A circuit-level gateway firewall works at the session layer of the OSI model or transport layer of TCP/IP. It forwards data between networks without verification and blocks incoming packets from the host but allows the traffic to pass through itself. Information passed to remote computers through a circuit-level gateway will appear to have originated from the gateway, as the incoming traffic carries the IP address of the proxy (circuit-level gateway). Such firewalls monitor requests to create sessions and determine if those sessions will be allowed.

A circuit-level gateway gives controlled access to network services and host requests. To determine whether a requested session is valid, it checks the TCP handshake between packets. Circuit proxy firewalls allow or prevent data streams; they do not filter individual packets. They are relatively inexpensive and hide the information about the private network that they protect.

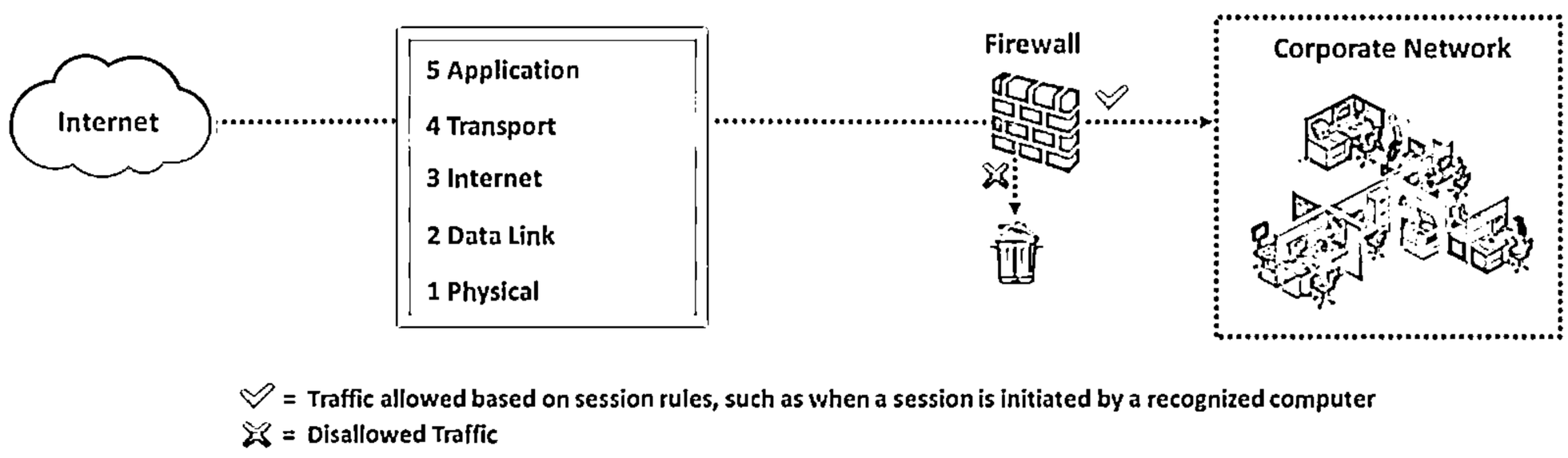
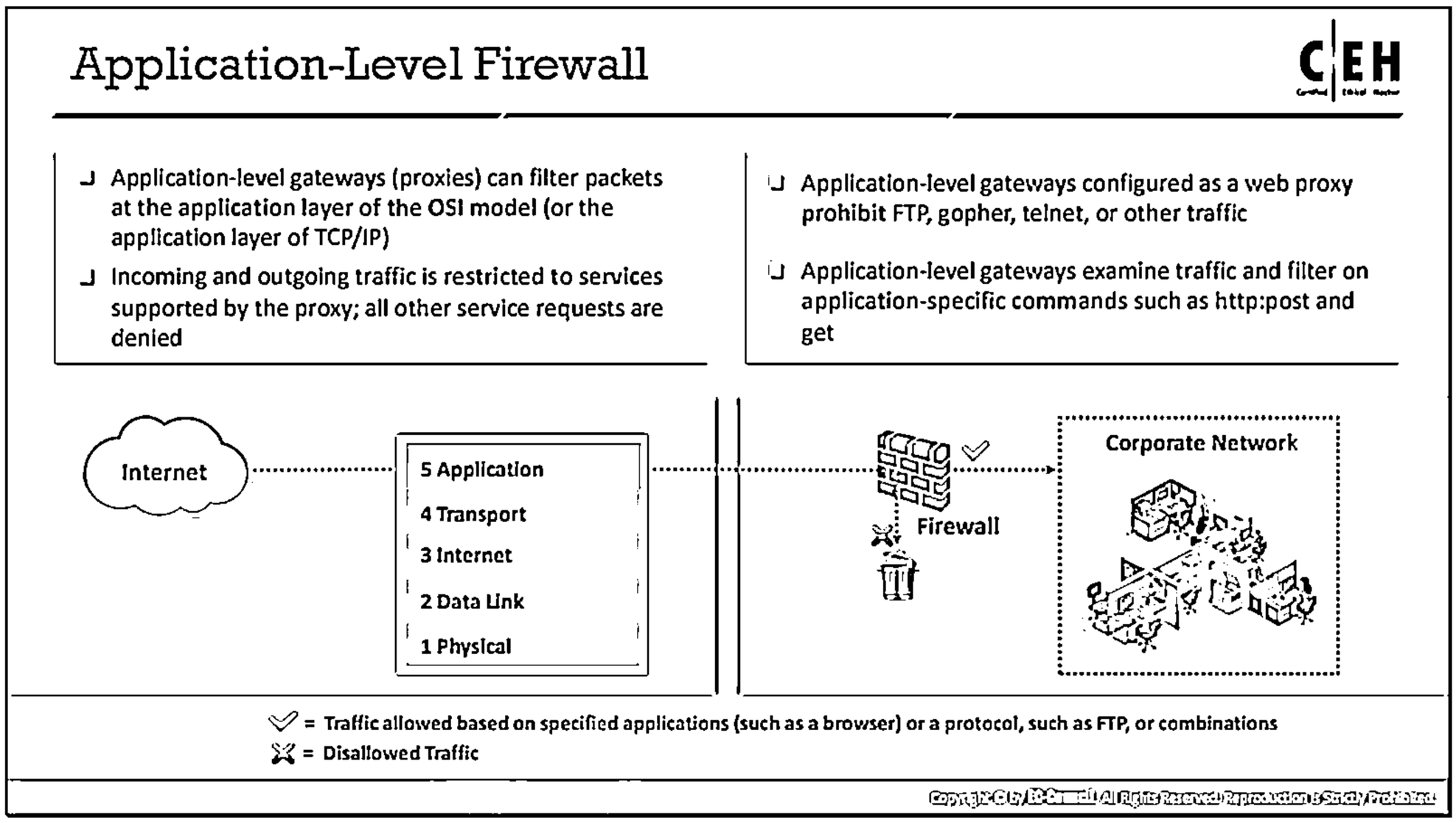


Figure 12.14 Example of Circuit-Level Gateway Firewall

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



Application-Level Firewall

Application-based proxy firewalls focus on the application layer rather than just the packets. Application-level gateways (proxies) can filter packets at the application layer of the OSI model (or the application layer of TCP/IP). Incoming and outgoing traffic is restricted to services supported by the proxy; all other service requests are denied. The need for an application-level firewall arises from the tremendous amount of voice, video, and collaborative traffic in the data-link layer and network layer, which may be used for unauthorized access to internal and external networks. Application-level gateways configured as web proxies prohibit FTP, gopher, telnet, or other traffic. They examine traffic and filter application-specific commands such as HTTP: post and get.

Traditional firewalls are unable to filter such types of traffic. They can inspect, find, and verify malicious traffic that is missed by stateful inspection firewalls to make decisions as to whether to allow access, and they improve the overall security of the application layer. For example, worms that send malicious code in legitimate protocols cannot be detected by stateful firewalls, as proxy firewalls focus on packet headers in the network layer. However, deep packet inspection firewalls can find such attacks with the help of informative signatures added inside packets.

Some of the features of application-level firewalls are as follows:

- They analyze the application information to make decisions as to whether to permit traffic.
- Being proxy-based, they can permit or deny traffic according to the authenticity of the user or process involved.

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

- A content-caching proxy optimizes performance by caching frequently accessed information rather than sending new requests to the servers for the same old data.

Application-layer firewalls can function in one of two modes: active or passive.

- **Active application-level firewalls**: They examine all incoming requests, including the actual message that is exchanged, against known vulnerabilities, such as SQL injection, parameter and cookie tampering, and cross-site scripting. The requests that are deemed genuine are allowed to pass through them.
- **Passive application-level firewalls**: They work similarly to IDS in that they also check all incoming requests against known vulnerabilities, but they do not actively reject or deny those requests if a potential attack is discovered.

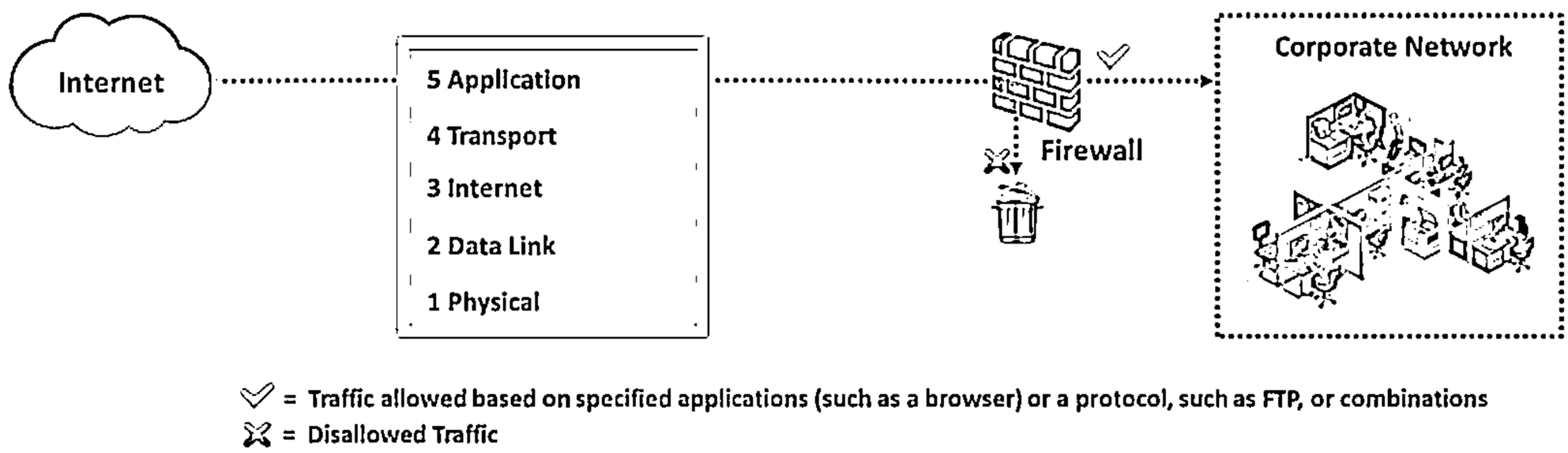
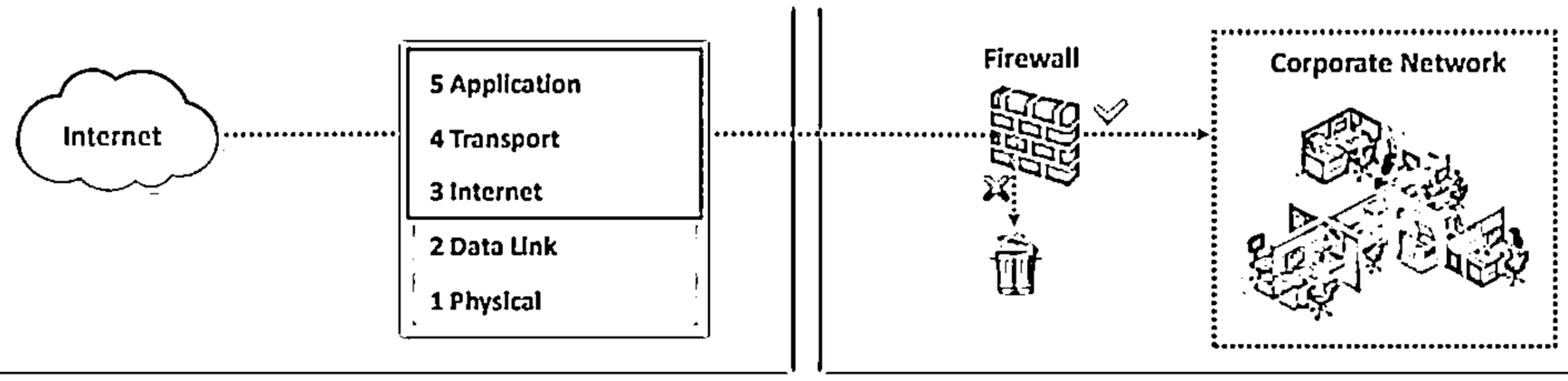


Figure 12.15: Example of Application-Level Firewall

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

Stateful Multilayer Inspection Firewall

- Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls (Packet Filtering, Circuit-Level Gateways, and Application-Level Firewalls)
- They filter packets at the network layer of the OSI model (or the internet layer of TCP/IP), to determine whether session packets are legitimate, and they evaluate the contents of packets at the application layer



✓ = Traffic is filtered at three layers based on a wide range of the specified application, session, and packet filtering rules
✗ = Disallowed Traffic

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

Stateful Multilayer Inspection Firewall

Stateful multilayer inspection firewalls combine the aspects of the three above-mentioned types of firewalls (packet filtering, circuit-level gateways, and application-level firewalls). They filter packets at the network layer of the OSI model (or the internet layer of the TCP/IP model) to determine whether session packets are legitimate, and they evaluate the contents of the packets at the application layer.

Using stateful packet filtering, you can overcome the limitation of packet firewalls, which can only filter the IP address, port, protocol, and so on. This multilayer firewall can perform deep packet inspection.

Features of the Stateful Multilayer Inspection Firewall:

- This type of firewall can remember the packets that passed through it earlier and make decisions about future packets accordingly.
- These firewalls combine the best features of both packet filtering and application-based filtering.
- Cisco PIX firewalls are stateful.
- These firewalls track and log slots or translations.

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

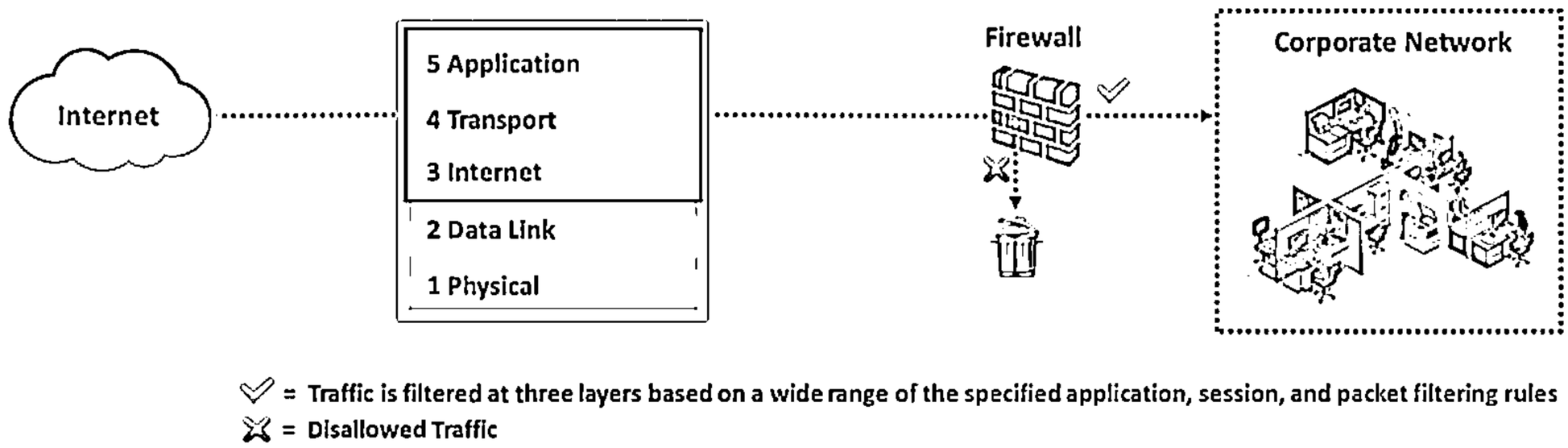


Figure 12.16: Example of Stateful Multilayer Inspection Firewall

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

Application Proxy

- An application-level proxy works as a proxy server and filters connections for specific services
- It filters connections based on the services and protocols appropriate to that application
- For example, an FTP proxy will only allow FTP traffic to pass through, and all other services and protocols will be blocked

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

Application Proxy

An application-level proxy works as a proxy server and filters connections for specific services. It filters connections based on the services and protocols when acting as a proxy. For example, an FTP proxy will only allow FTP traffic to pass through while all other services and protocols will be blocked. It is a type of server that acts as an interface between the user workstation and the Internet. It correlates with the gateway server and separates the enterprise network from the Internet. It receives a request from a user to provide the Internet service and responds to the original request only. A proxy service is an application or program that helps forward user requests (for example, FTP or Telnet) to the actual services. A proxy is also known as an application-level gateway, as it renews the connections and act as a gateway to the services. Proxies run on a firewall host that is either a dual-homed host or some other bastion host for security purposes. Some proxies, namely caching proxies, improve network efficiency. They keep copies of the requested data of the hosts that they proxy. Such proxies can provide the data directly when multiple hosts request the same data. Caching proxies help in reducing the load on network connections, whereas proxy servers provide both security and caching.

A proxy service is available to the user in the internal network and the service in the outside network (Internet), and it is transparent. Instead of direct communication, it talks with the proxy and it handles all the communication between users and Internet services. Transparency is the main advantage of proxy services. To the user, a proxy server presents an illusion that it is dealing directly with the real server, whereas to a real server, the proxy server gives the illusion that it is dealing directly with the user.

Advantages

- Proxy services are useful for logging because they can understand application protocols and effectively allow logging.

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

- Proxy services reduce the load on network links as they are capable of caching copies of frequently requested data and allow it to be directly loaded from the system instead of the network.
- Proxy systems perform user-level authentication, as they are involved in the connection.
- Proxy systems automatically protect weak or faulty IP implementations as they sit between the client and the Internet and generate new IP packets for the client.

Disadvantages

- Proxy services lag behind non-proxy services until suitable proxy software is available.
- Each service in a proxy may use different servers.
- Proxy services may require changes in the client, applications, and procedures.

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

Network Address Translation (NAT)

1. Network address translation separates IP addresses into two sets and enables the LAN to use these addresses for internal and external traffic separately
2. It also works with a router, similar to packet filtering. NAT also modifies the packets the router sends simultaneously
3. It has the ability to change the address of the packet and make it appear to have arrived from a valid address
4. It limits the number of public IP addresses an organization can use
5. It can act as a firewall filtering technique where it allows only those connections which originate on the inside network and will block the connections which originate on the outside network

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

Network Address Translation (NAT)

Network address translation (NAT) separates IP addresses into two sets and enables the LAN to use these addresses for internal and external traffic. The NAT helps hide an internal network layout and force connections to go through a choke point. It also works with a router, and similarly to packet filtering, it will also modify the packets that the router sends simultaneously. When the internal machine forwards the packet to the external machine, the NAT modifies the source address of the packet to make it appear as if it is coming from a valid address. When the external machine sends the packet to the internal machine, the NAT modifies the destination address to turn the visible address into the correct internal address. The NAT can also change the source and destination port numbers. It limits the number of public IP addresses that an organization can use. It can act as a firewall filtering technique whereby it allows only those connections that originate in the internal network and blocks the connections that originate in the external network.

NAT systems use different schemes for translation between internal and external addresses:

- Assign one external host address for each internal address and always apply the same translation. This slows down connections and does not provide any savings in address space.
- Dynamically allocate an external host address without modifying the port numbers when the internal host initiates a connection. This restricts the number of internal hosts that can simultaneously access the Internet to the number of available external addresses.
- Create a fixed mapping from internal addresses to externally visible addresses but use a port mapping so that multiple internal machines use the same external address.

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

- Dynamically allocate an external host address and port pair each time an internal host initiates a connection. This makes the most efficient possible use of the external host addresses.

Advantages

- Network address translation helps to enforce the firewall's control over outbound connections.
- It restricts incoming traffic and allows only packets that are part of a current interaction initiated from the inside.
- It helps hide the internal network's configuration and thus lowers the success rate of attacks on the network or system.

Disadvantages

- The NAT system has to guess how long it should keep a particular translation, which is not always possible.
- The NAT interferes with encryption and authentication systems to ensure the security of the data.
- Dynamic allocation of ports may interfere with packet filtering.

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

Virtual Private Network

1. A VPN is a private network constructed using public networks, such as the Internet
2. It is used for the secure transmission of sensitive information over an untrusted network, using encapsulation and encryption
3. It establishes a virtual point-to-point connection through the use of dedicated connections
4. Only the computing device running the VPN software can access the VPN

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

Virtual Private Network

A virtual private network (VPN) is a network that provides secure access to the private network through the Internet. VPNs are used for connecting wide area networks (WAN). They allow computers on one network to connect to computers on another network. They are used for the secure transmission of sensitive information over an untrusted network via encapsulation and encryption. They employ encryption and integrity protection, enabling you to use a public network as a private network. A VPN performs encryption and decryption outside the packet-filtering perimeter to allow the inspection of packets coming from other sites. It establishes a virtual point-to-point connection through the use of dedicated connections. A VPN also encapsulates packets sent over the Internet. It combines the advantages of both public and private networks. VPNs have no relation to firewall technology, but firewalls are convenient for adding VPN features as they help in providing secure remote services. The computing device running the VPN software can only access the VPN.

All VPNs that run over the Internet adopt the following principles:

- Encrypts the traffic
- Checks for integrity protection
- Encapsulates new packets, which are sent across the Internet to some destination that reverses the encapsulation
- Checks the integrity
- Decrypts the traffic eventually

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

Advantages

- A VPN hides all the traffic that flows over it, ensures encryption, and protects data from snooping.
- It provides remote access for protocols while avoiding attackers from the Internet at large.

Disadvantages

- As the VPN runs on a public network, the user will be vulnerable to an attack on the destination network.

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

Firewall Limitations

1. A firewall does not protect the network from new viruses, backdoors, or insider attacks
2. A firewall cannot do anything if the network design or configuration is faulty
3. A firewall is not an alternative to antivirus or antimalware protection
4. A firewall cannot prevent social engineering threats
5. A firewall does not prevent password misuse
6. A firewall does not block attacks from a higher level of the protocol stack
7. A firewall does not protect against attacks from dial-in connections or attacks originating from common ports and applications
8. A firewall is unable to understand tunneled traffic

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

Firewall Limitations

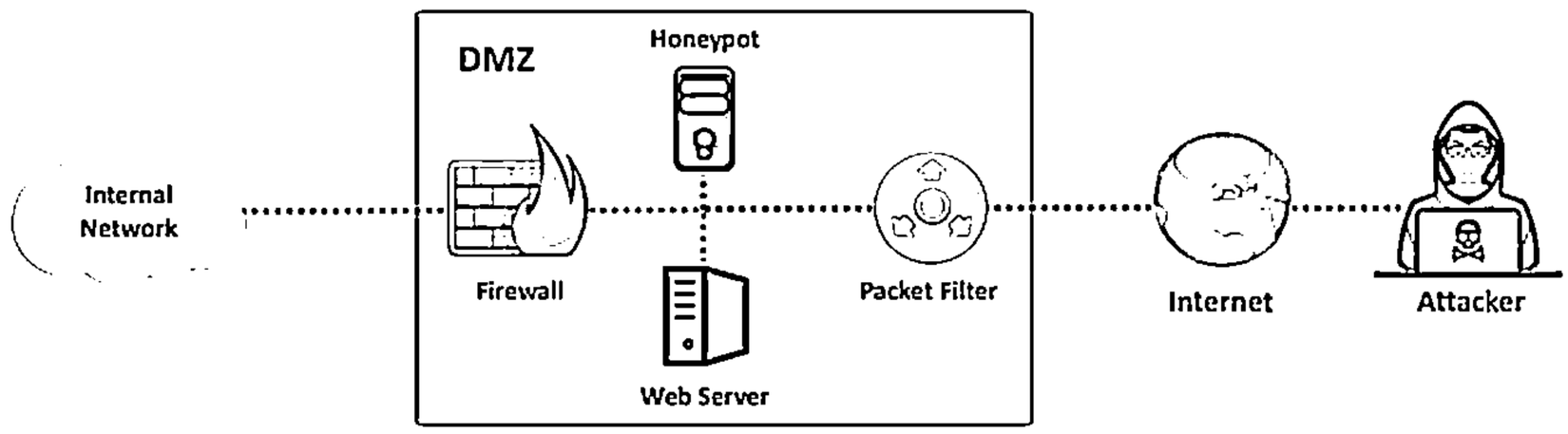
Although firewalls are essential to your security strategy, they have the following limitations:

- Firewalls can restrict users from accessing valuable services such as FTP, Telnet, NIS, etc., and they sometimes restrict Internet access as well.
- The firewall cannot prevent internal attacks (backdoor) in a network, e.g., a disgruntled employee who cooperates with the external attacker.
- The firewall focuses its security at a single point, which makes other systems within the network prone to security attacks.
- A bottleneck could occur if all the connections pass through the firewall.
- The firewall cannot protect the network from social engineering and data-driven attacks whereby the attacker sends malicious links and emails to employees inside the network.
- If external devices such as laptops, mobile phones, portable hard drives, etc., are already infected and connected to the network, then a firewall cannot protect the network from these devices.
- The firewall is unable to adequately protect the network from all types of zero-day viruses that try to bypass it.
- A firewall cannot do anything if the network design and configuration is faulty.
- A firewall is not an alternative to antivirus or antimalware tools.
- A firewall does not block attacks from a higher level of the protocol stack.
- A firewall does not prevent attacks originating from common ports and applications.
- A firewall does not prevent attacks from dial-in connections.
- A firewall is unable to understand tunneled traffic.

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

Honeypot

1. A honeypot is an information system resource that is expressly set up to attract and trap people who attempt to penetrate an organization's network
2. It has no authorized activity, does not have any production value, and any traffic to it is likely to be a probe, attack, or compromise
3. A honeypot can log port access attempts or monitor an attacker's keystrokes. These could be early warnings of a more concerted attack



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

Honeypot

A honeypot is a computer system on the Internet intended to attract and trap those who attempt unauthorized or illicit utilization of the host system to penetrate an organization's network. It is a fake proxy run to frame attackers by logging traffic through it and then sending complaints to the victims' ISPs. It has no authorized activity or production value, and any traffic to it is likely a probe, attack, or compromise. Whenever there is any interaction with a honeypot, it is most likely to be malicious. Honeypots are unique; they do not solve a specific problem. Instead, they are a highly flexible tools with many different security applications. Honeypots help in preventing attacks, detecting attacks, and information gathering and research. A honeypot can log port access attempts or monitor an attacker's keystrokes; these could be early warnings of a more concerted attack. It requires a considerable amount of effort to maintain a honeypot.

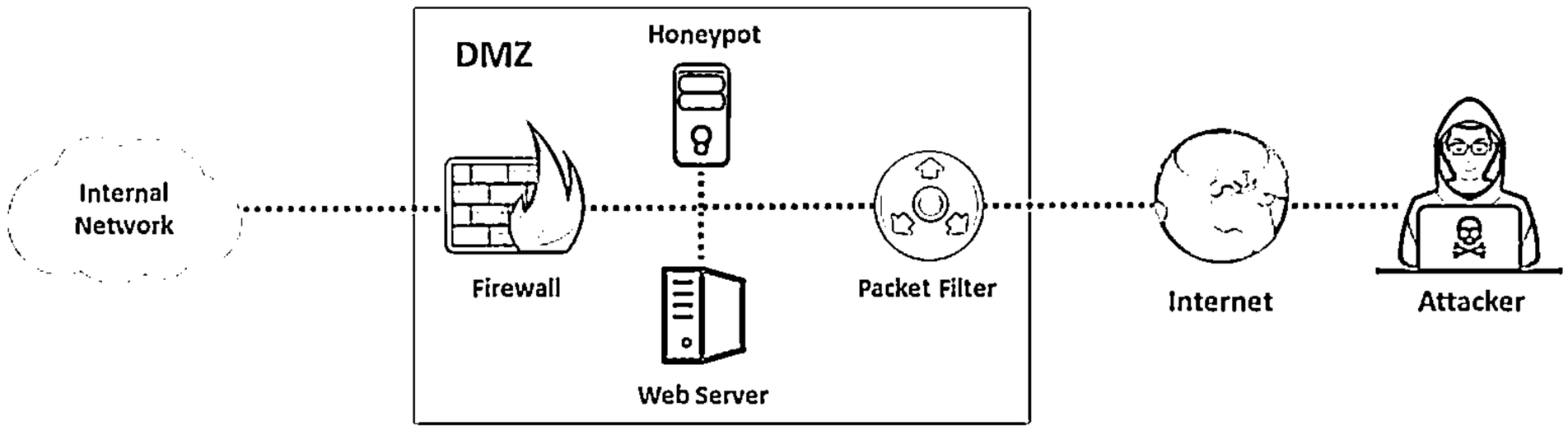


Figure 12.17: Example of Honeypot

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

Types of Honeypots

Classification of honeypots based on their design criteria:

Low-interaction Honeypots	These honeypots simulate only a limited number of services and applications of a target system or network
Medium-interaction Honeypots	These honeypots simulate a real operating system, applications, and services of a target network
High-interaction Honeypots	These honeypots simulate all services and applications of a target network
Pure Honeypots	These honeypots emulate the real production network of a target organization

Classification of honeypots based on their deployment strategy:

- Production Honeypots
- Research Honeypots

Classification of honeypots based on their deception technology:

- Malware Honeypots
- Database Honeypots
- Spam Honeypots
- Email Honeypots
- Spider Honeypots
- Honeynets

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

Types of Honeypots

Honeypots are classified into the following types based on their design criteria:

- **Low-interaction Honeypots**

  Low-interaction honeypots emulate only a limited number of services and applications of a target system or network. If the attacker does something that the emulation does not expect, the honeypot will simply generate an error. They capture limited amounts of information, i.e., mainly transactional data, and some limited interactions. These honeypots cannot be compromised completely. They are set to collect higher-level information about attack vectors such as network probes and worm activities. Some examples are Specter, KFSensor, and Honeytrap.

  KFSensor is a low-interaction honeypot used to attract and identify penetrations. It implements vulnerable system services and Trojans to attract hackers. This honeypot can be used to monitor all TCP, UDP, and ICMP ports and services. KFSensor identifies and raises alerts about port scanning and DoS attacks.

  A honeytrap is a low-interaction honeypot used to observe attacks against TCP and UDP services. It runs as a daemon and starts server processes dynamically on requested ports. Attackers are tricked into sending responses to the honeytrap server process. The data that is received by the honeypot is concatenated into a string and stored in a database file. This string is called the attack string. Honeytraps parse attack strings for a command requesting the server to download a file from another host in the network. If such a command is detected, the server tries to access the corresponding file automatically. It supports only FTP and TFTP protocols. It also identifies and logs HTTP_URIs.

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

- **Medium-interaction Honeypots**

  Medium-interaction honeypots simulate a real OS as well as applications and services of a target network. They provide greater misconception of an OS than low-interaction honeypots. Therefore, it is possible to log and analyze more complex attacks. These honeypots capture more useful data than low-interaction honeypots. They can only respond to preconfigured commands; therefore, the risk of intrusion increases. The main disadvantage of medium-interaction honeypots is that the attacker can quickly discover that the system behavior is abnormal. Some examples of medium-interaction honeypots include HoneyPy, Kojoney2, and Cowrie.

  Kojoney2 is a medium-interaction honeypot that emulates a real SSH environment. This honeypot listens on port 21 for incoming SSH connections. If a connection request is initiated, Kojoney2 will verify users against an internal list of fake users. Usually, the connections are accepted by granting access to the SSH shell. It simulates many shell commands to trick attackers. Using Kojoney2, attackers can download files using wget and curl commands.

- **High-Interaction Honeypots**

  Unlike their low- and medium-interaction counterparts, high-interaction honeypots do not emulate anything; they run actual vulnerable services or software on production systems with real OS and applications. These honeypots simulate all services and applications of a target network. They can be completely compromised by attackers to gain full access to the system in a controlled area. They capture complete information about an attack vector such as attack techniques, tools, and intent. The honeypotized system is more prone to infection, as attack attempts can be carried out on real production systems.

  A honeynet is a prime example of a high-interaction honeypot. It is neither a product nor a software solution that a user installs. Instead, it is an architecture—an entire network of computers designed to attack. The idea is to have an architecture that creates a highly controlled network with real computers running real applications, in which all activities are monitored and logged.

  "**Bad guys**" find, attack, and break into these systems through their own initiative. When they do, they do not realize that they are in a honeynet. Without the knowledge of the attackers, all their activities and actions, from encrypted SSH sessions to email and file uploads, are captured by inserting kernel modules into their systems.

  At the same time, the honeynet controls the attacker's activity. Honeynets do this by using a honeywall gateway, which allows inbound traffic to the victim's systems but controls the outbound traffic using intrusion prevention technologies. This gives the attacker the flexibility to interact with the victim's systems but prevents the attacker from harming other non-honeynet computers.

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

- **Pure Honeypots**

  Pure honeypots emulate the real production network of a target organization. They cause attackers to devote their time and resources toward attacking the critical production system of the company. Attackers uncover and discover the vulnerabilities and trigger alerts that help network administrators to provide early warnings of attacks and hence reduce the risk of an intrusion.

Honeypots are classified into the following types based on their deployment strategy:

- **Production Honeypots**

  Production honeypots are deployed inside the production network of the organization along with other production servers. Although such honeypots improve the overall state of security of the organization, they effectively capture only a limited amount of information related to the adversaries. Such honeypots fall under the low-interaction honeypot category and are extensively employed by large organizations and corporations. As production honeypots are deployed internally, they also help to find out internal flaws and attackers within an organization.

- **Research Honeypots**

  Research honeypots are high-interaction honeypots primarily deployed by research institutes, governments, or military organizations to gain detailed knowledge about the actions of intruders. By using such honeypots, security analysts can obtain in-depth information about how an attack is performed, vulnerabilities are exploited, and attack techniques and methods are used by the attackers. This analysis, in turn, can help an organization to improve attack prevention, detection, and security mechanisms and develop a more secure network infrastructure.

  The main drawback of research honeypots is that they do not contribute to the direct security of the company. If a company is looking to improve its production infrastructure, it should opt for production honeypots.

Honeypots are classified into the following types based on their deception technology:

- **Malware Honeypots**

  Malware honeypots are used to trap malware campaigns or malware attempts over the network infrastructure. These honeypots are simulated with known vulnerabilities such as outdated APIs, vulnerable SMBv1 protocols, etc., and they also emulate different Trojans, viruses, and backdoors that encourage adversaries to perform exploitation activities. These honeypots lure the attacker or malware into performing attacks, from which the attack pattern, malware signatures, and malware threat actors can be identified effectively.

- **Database Honeypots**

  Database honeypots employ fake databases that are vulnerable to perform database-related attacks such as SQL injection and database enumeration. These fake databases trick the attackers by making them think that these databases contain crucial sensitive

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

information such as credit card details of all the customers and employee databases. However, all the information present in the database are fake and simulated. Such databases lure the attacker to perform attacks, with their vulnerabilities; from the attacks, the attack pattern and the threat actor's TTP's towards database attacks can be identified effectively.

- **Spam Honeypots**

  Spam honeypots specifically target spammers who abuse vulnerable resources such as open mail relays and open proxies. Basically, spam honeypots consist of mail servers that deliberately accept emails from any random source from the Internet. They provide crucial information about spammers and their activities.

- **Email Honeypots**

  Email honeypots are also called email traps. They are nothing but fake email addresses that are specifically used to attract fake and malicious emails from adversaries. These fake email IDs will be distributed across the open Internet and dark web to lure threat actors into performing various malicious activities to exploit the organization. By constantly monitoring the incoming emails, the adversary's deception techniques can be identified by the administrators and internal employees can be warned to avoid falling into such email traps.

- **Spider Honeypots**

  Spider honeypots are also called spider traps. These honeypots are specifically designed to trap web crawlers and spiders. Many threat actors perform web crawling and spidering to extract important information from web applications. Such crucial information includes URLs, contact details, directory details, etc. Spider honeypots are employed to trap such adversaries. A fake website will be emulated and presented as a legitimate one. Threat actors attempting to perform web crawling on such traps will be identified and blacklisted.

- **Honeynets**

  Honeynets are networks of honeypots. They are very effective in determining the entire capabilities of the adversaries. Honeynets are mostly deployed in an isolated virtual environment along with a combination of vulnerable servers. The various TTPs employed by different attackers to enumerate and exploit networks will be recorded, and this information can be very effective in determining the complete capabilities of the adversary.

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

Module Flow

1. IDS, IPS, Firewall, and Honeypot Concepts
2. IDS, IPS, Firewall, and Honeypot Solutions
3. Evading IDS
4. Evading Firewalls
5. IDS/Firewall Evading Tools
6. Detecting Honeypots
7. IDS/Firewall Evasion Countermeasures

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

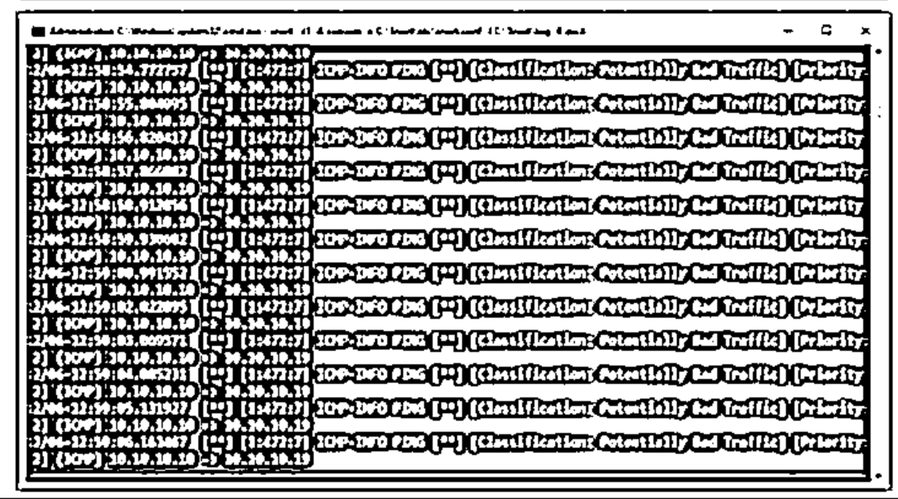
IDS, IPS, Firewall, and Honeypot Solutions

The previous section discussed the function, role, and placement of IDS, IPS, firewalls, and honeypots for securing networks. A number of easy-to-use and feature-enriched solutions (hardware, software, or both) are available for the implementation of IDS, IPS, firewalls, and honeypots. This section discusses some commercially available solutions that simplify the usage of IDS, IPS, firewalls, and honeypots.

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

Intrusion Detection Tools: Snort

1. Snort is an open-source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks
2. It can perform protocol analysis and content searching/matching, and is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, and OS fingerprinting attempts
3. It uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug-in architecture
4. Uses of Snort:
   - Straight packet sniffer like tcpdump
   - Packet logger (useful for network traffic debugging, etc.)
   - Network intrusion prevention system



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

Snort Rules

- Snort's rule engine allows custom rules to be established to meet the needs of the network
- Snort rules help in differentiating between normal Internet activities and malicious activities
- Snort rules must be contained on a single line; the Snort rule parser does not handle rules on multiple lines
- Snort rules come with two logical parts:
  - Rule header: Identifies the rule's actions, such as alert, log, pass, activate, and dynamic
  - Rule options: Identifies the rule's alert messages

Example

Rule Protocol

Rule Port

```
alert tcp any any -> 192.168.1.0/24 111 (content: "|00 01 86 a5|"; msg: "mountd access";)
```

Rule Action

Rule Format Direction

Rule IP Address

Alert Message

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

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

Snort Rules: Rule Actions and IP Protocols

Rule Actions

- The rule header stores the complete set of rules to identify a packet and determines the action to be performed or the rule to be applied
- The rule action alerts Snort when it finds a packet that matches the rule criteria
- There are three available actions in Snort:
  - Alert - Generate an alert using the selected alert method, and then log the packet
  - Log - Log the packet
  - Pass - Drop (ignore) the packet

IP Protocols

There are three available IP protocols that Snort supports for suspicious behavior:

1. TCP
2. UDP
3. ICMP

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

Snort Rules: The Direction Operator and IP Addresses

The Direction Operator

- This operator indicates the direction of interest for the traffic; traffic can flow in either a single direction or bi-directionally
- Example of a Snort rule using the bidirectional operator:

```
log !192.168.1.0/24 any <> 192.168.1.0/24 23
```

IP Addresses

- Identify the IP address and the port that the rule applies to
- Use the keyword "any" to define the IP address
- Use numeric IP addresses qualified with a CIDR netmask
- Example of an IP Address Negation Rule:

```
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 (content:
"|00 01 86 a5|"; msg: "external mountd access";)
```

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

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

Snort Rules: Port Numbers

- Port numbers can be listed in different ways, including "any" ports, static port definitions, port ranges, and by negation
- Port ranges are indicated with the range operator ":"
- Example of a Port Negation

```
log tcp any any -> 192.168.1.0/24 !6000:6010
```

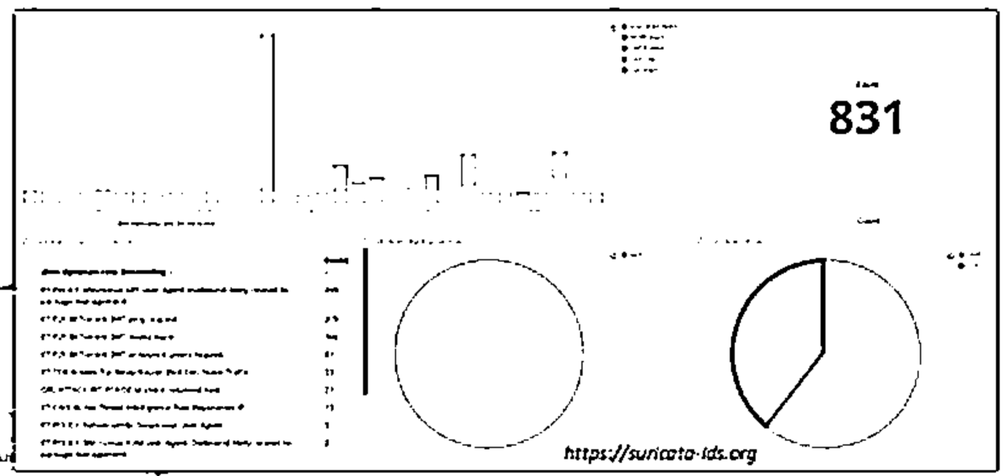
Protocols	IP Address	Action
Log UDP any any ->	192.168.1.0/24 1:1024	Log UDP traffic coming from any port and destination ports ranging from 1 to 1024
Log TCP any any ->	192.168.1.0/24 :5000	Log TCP traffic from any port going to ports less than or equal to 5000
Log TCP any :1024 ->	192.168.1.0/24 400:	Log TCP traffic from the well-known ports and going to ports greater than or equal to 400

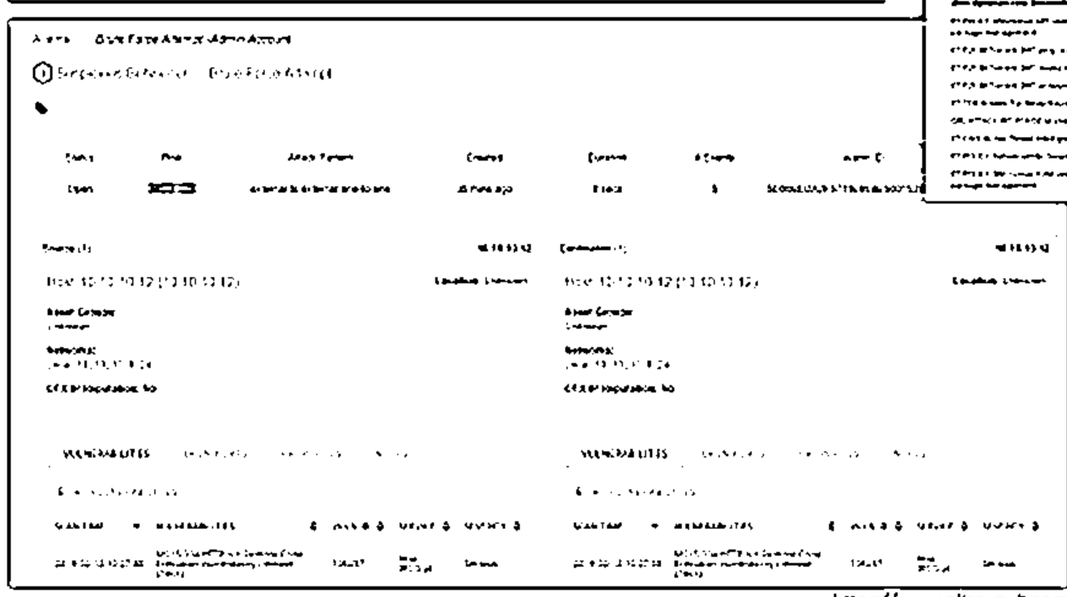
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Intrusion Detection Tools: Suricata and AlienVault® OSSIM™

Suricata

- Suricata is a robust network threat detection engine capable of real-time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM), and offline pcap processing





AlienVault® OSSIM™

- AlienVault® OSSIM™ provides you with a feature-rich open source security information and event management (SIEM) system complete with event collection, normalization, and correlation

Intrusion Detection Tools

- SolarWinds Security Event Manager (*https://www.solarwinds.com*)
- OSSEC (*https://www.ossec.net*)
- BroIDS/Zeek IDS (*https://www.zeek.org*)

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

Intrusion Detection Tools

Intrusion detection tools detect anomalies. These tools, when running on a dedicated workstation, read all network packets, reconstruct user sessions, and scan for possible intrusions by looking for attack signatures and network traffic statistical anomalies. Moreover, these tools offer real-time, zero-day protection from network attacks and malicious traffic, and they prevent malware, spyware, port scans, viruses, DoS, and DDoS from compromising hosts.

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

- **Snort**

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

  Snort is an open-source network intrusion detection system capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, and it is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. It uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that uses a modular plug-in architecture.

  Uses of Snort:

  - Straight packet sniffer such as tcpdump
  - Packet logger (useful for network traffic debugging, etc.)
  - Network intrusion prevention system

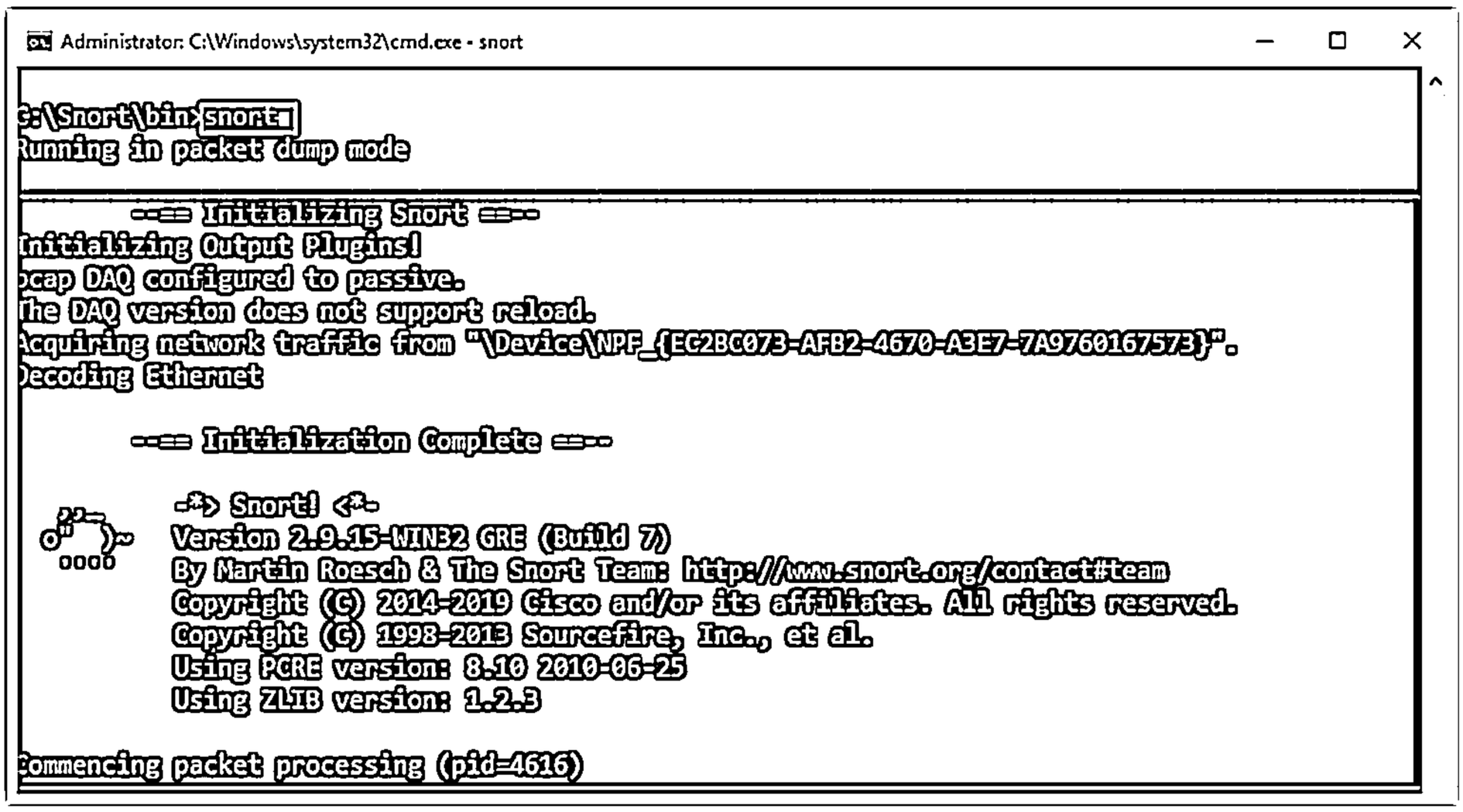


Figure 12.18: Screenshot of Snort

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

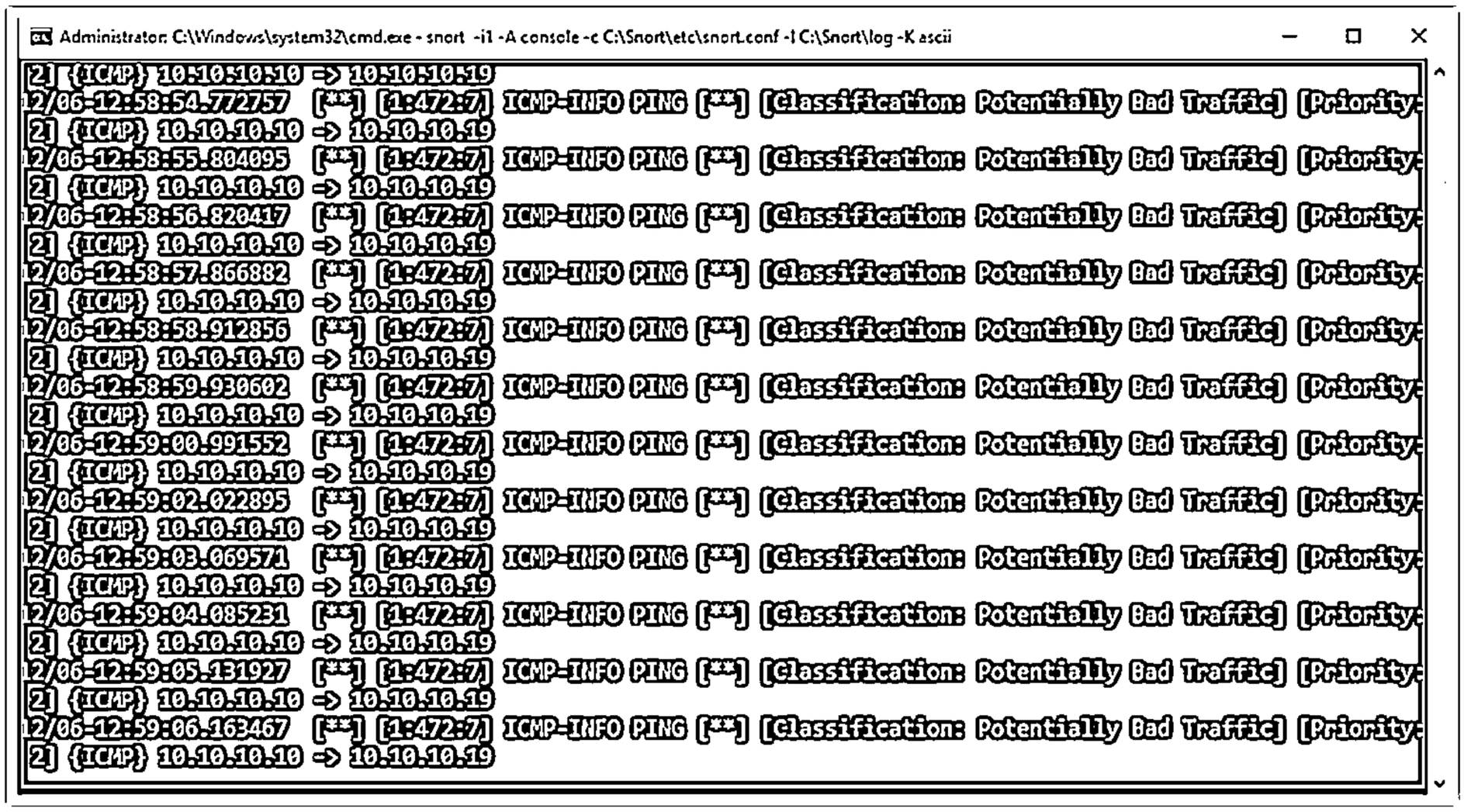


Figure 12.19: Snort output

Snort Rules

Snort's rule engine allows custom rules to meet the needs of the network. Snort rules help in differentiating between normal Internet activities and malicious activities. Snort uses the popular **libpcap library** (for UNIX/Linux) or **Winpcap** (for Windows), the same library that tcpdump uses to perform its packet sniffing. Attaching Snort in the promiscuous mode to the network media decodes all the packets passing through the network. It generates alerts according to the content of individual packets and rules defined in the configuration file.

Snort allows users to write their own rules. However, each of these Snort rules must describe the following:

- Any violation of the security policy of the company that might be a threat to the security of the company's network and other valuable information
- All well-known and frequent attempts to exploit the vulnerabilities in the company's network
- The conditions in which a user thinks that a network packet(s) is unusual (i.e., if the identity of the packet is not authentic)

Snort rules, written for both protocol analysis and content searching and matching, should be robust and flexible. The rules should be "**robust**": the system should maintain a hard check on the activities taking place on the network and notify the administrator of any potential intrusion attempt. The rules should be "**flexible**": the system must be sufficiently compatible to act immediately and take necessary remedial measures according to the nature of the intrusion.

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

Both flexibility and robustness can be achieved using an easy-to-understand and lightweight rule-description language that aids in writing simple Snort rules. Consider the following two primary principles while writing Snort rules:

- No written rule must extend beyond a single line; thus, rules should be short, precise, and easy to understand.
- Each rule should be divided into two logical sections:
  - The rule header
  - The rule options

The rule header contains the rule's action, the protocol, the source and destination IP addresses, the source and destination port information, and the **Classless Inter-Domain Routing (CIDR) block**. The rule option section includes alert messages in addition to information about the inspected part of the packet to determine whether to take any rule action.

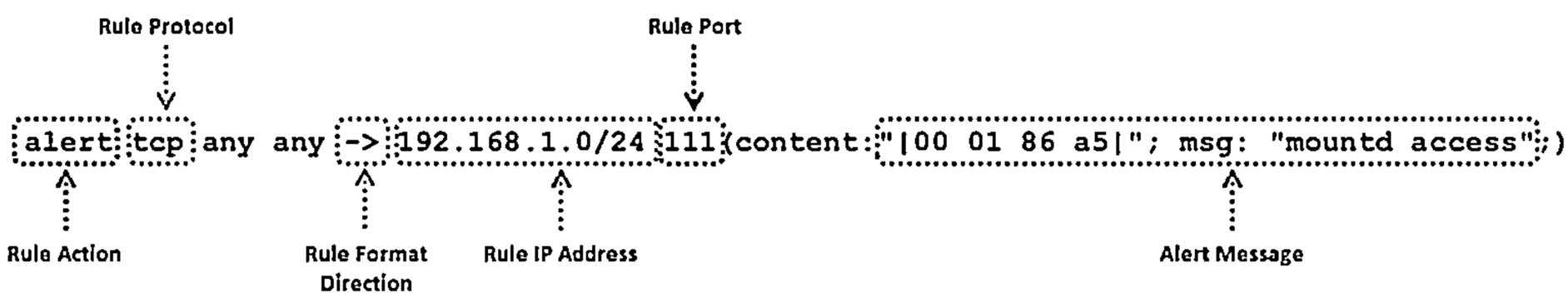


Figure 12.20: Example of Snort rules

Snort Rules: Rule Actions and IP Protocols

The rule header stores a complete set of rules to identify a packet and determines the action to be performed or rule to be applied. It contains information that defines the who, where, and what of a packet, as well as what to do if a packet with all the attributes indicated in the rule should show up. The first item in a rule is the rule action, which tells Snort "what to do" when it finds a packet that matches the rule criteria. There are five available default actions in Snort: alert, log, pass, activate, and dynamic. Furthermore, if Snort is running in the inline mode, you have additional options, which include drop and reject.

The IP sends data from one system to another via the Internet. It supports unique addressing for every computer on a network. Organize data on the IP network into packets. Each packet contains message data, source, destination, and more.

Snort supports three available IP protocols to tackle suspicious behavior:

- **TCP**: The Transmission Control Protocol (TCP) is a part of the IP. It is used to connect two different hosts and exchange data between them.
- **UDP**: **The** User Datagram Protocol (UDP) is used for broadcasting messages over a network.
- **ICMP**: The Internet Control Message Protocol (ICMP) is a part of the IP. The OS uses ICMP in a network to send error messages, for example.

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

Snort Rules: Direction Operator and IP Addresses

- **Direction Operator**

  This operator indicates the direction of interest for the traffic; traffic can flow either in a single direction or bidirectionally.

  Example of a Snort rule using the Bidirectional Operator:

  ```
  log !192.168.1.0/24 any <> 192.168.1.0/24 23
  ```

- **IP Addresses**
  - Identify the IP address and port that the rule applies to
  - Use keyword "any" to define the IP address
  - Use numeric IP addresses qualified with a CIDR netmask
  - Example of IP Address Negation Rule:

    ```
    alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111
    (content: "|00 01 86 a5|"; msg: "external mountd access";)
    ```

Snort Rules: Port Numbers

Port numbers can be listed in different ways, including the use of "any" ports, static port definitions, port ranges, and by negation. Port ranges are indicated by the range operator ":." The direction operator "-$>$" indicates the orientation or direction of the traffic to which the rule applies. Consider an IP address and port number on the left side of the direction operator as the traffic coming from the source host and the address and port information on the right side of the operator as the destination host. There is also a bidirectional operator, indicated by "$<>$". This tells Snort to consider the address/port pairs in either the source or the destination orientation, and it is handy for recording/analyzing both sides of a conversation, such as telnet or POP3 sessions. Further, note that there is no "$<$-" operator. In Snort versions before version 1.8.7, the direction operator did not provide proper error checking; hence, many people used invalid tokens. Note that "$<$-" does not exist so that rules always read consistently.

The next fields in a Snort rule specify the source and destination IP addresses and ports of the packet, as well as the direction in which the packet is traveling. Snort can accept a single IP address or a list of addresses. When specifying a list of IP address, you should separate each one with a comma and then enclose the list within square brackets as follows:

[192.168.1.1,192.168.1.45,10.1.1.24]

When doing this, be careful not to use any whitespaces. You can also specify the ranges of IP addresses using CIDR notation or even include CIDR ranges within lists. Snort also allows you to apply the logical NOT operator ("!") to an IP address or CIDR range to specify that the rule should match all but that address or range of addresses. For example, an easy modification to the initial example is to change it such that an alert is

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

raised upon detecting any traffic that has originated outside the local net using the negation operator.

Example of a Port Negation:

```
log tcp any any -> 192.168.1.0/24 !6000:6010
```

Protocols	IP Address	Action
Log UDP any any ->	192.168.1.0/24 1:1024	Log UDP traffic coming from any port and destination ports ranging from 1 to 1024
Log TCP any any ->	192.168.1.0/24 :5000	Log TCP traffic from any port going to ports less than or equal to 5000
Log TCP any :1024 ->	192.168.1.0/24 400:	Log TCP traffic from the well-known ports and going to ports greater than or equal to 400

Table 12.2: Examples of a Port Negation

- **Suricata**

  Source: *https://suricata-ids.org*

  Suricata is a robust network threat detection engine capable of real-time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM), and offline pcap processing. It inspects the network traffic using powerful and extensive rules and a signature language, and it provides powerful Lua scripting support for the detection of complex threats. With standard input and output formats such as YAML and JSON, integrations with existing tools such as SIEMs, Splunk, Logstash/Elasticsearch, Kibana, and other databases become effortless.

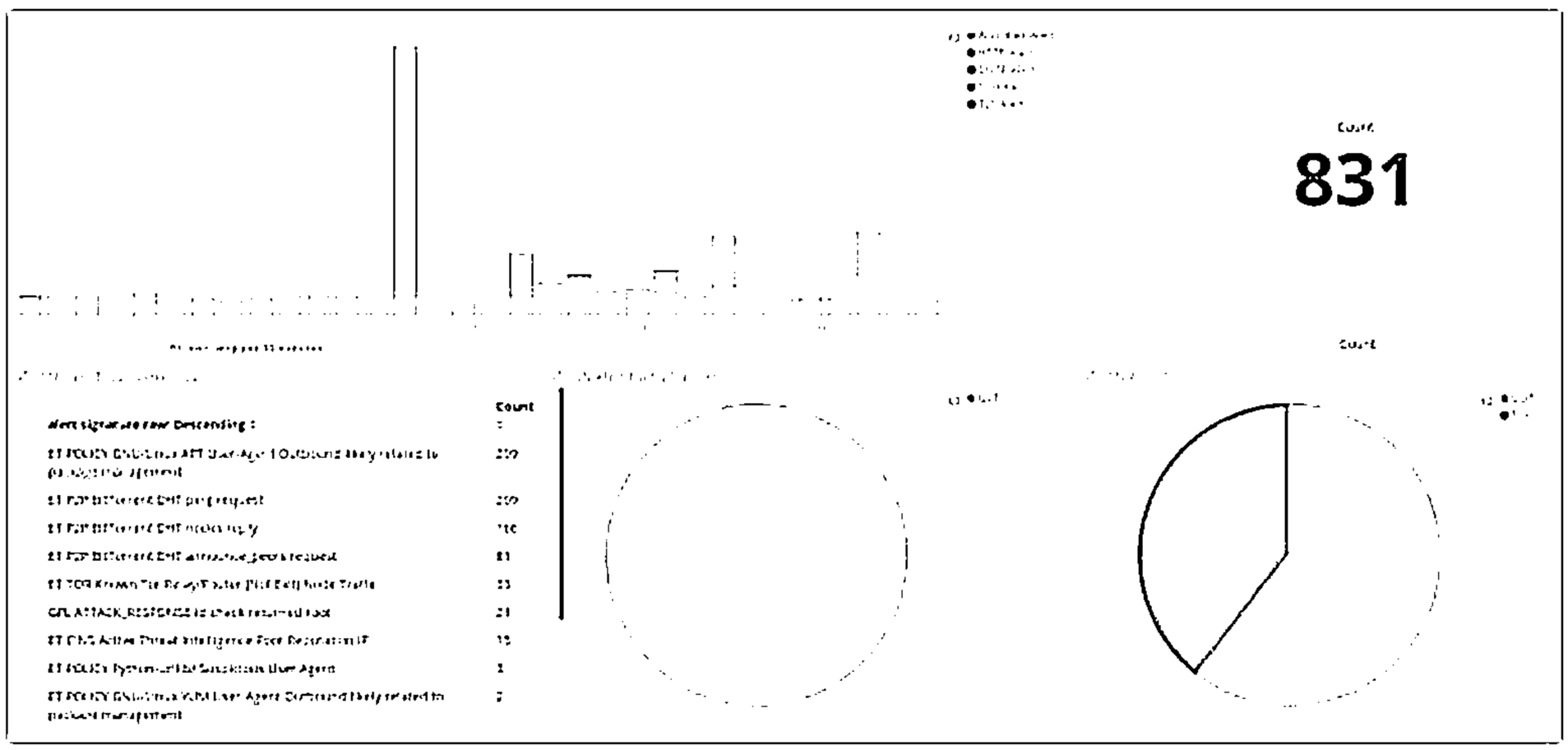


Figure 12.21: Screenshot of TippingPoint

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

- **AlienVault® OSSIM™**

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

  AlienVault® OSSIM™, Open Source Security Information and Event Management (SIEM), provides you with a feature-rich open-source SIEM complete with event collection, normalization, and correlation.

  OSSIM provides a unified platform with many essential security capabilities such as:

  - Asset discovery
  - Vulnerability assessment and intrusion detection
  - Behavioral monitoring
  - SIEM event correlation

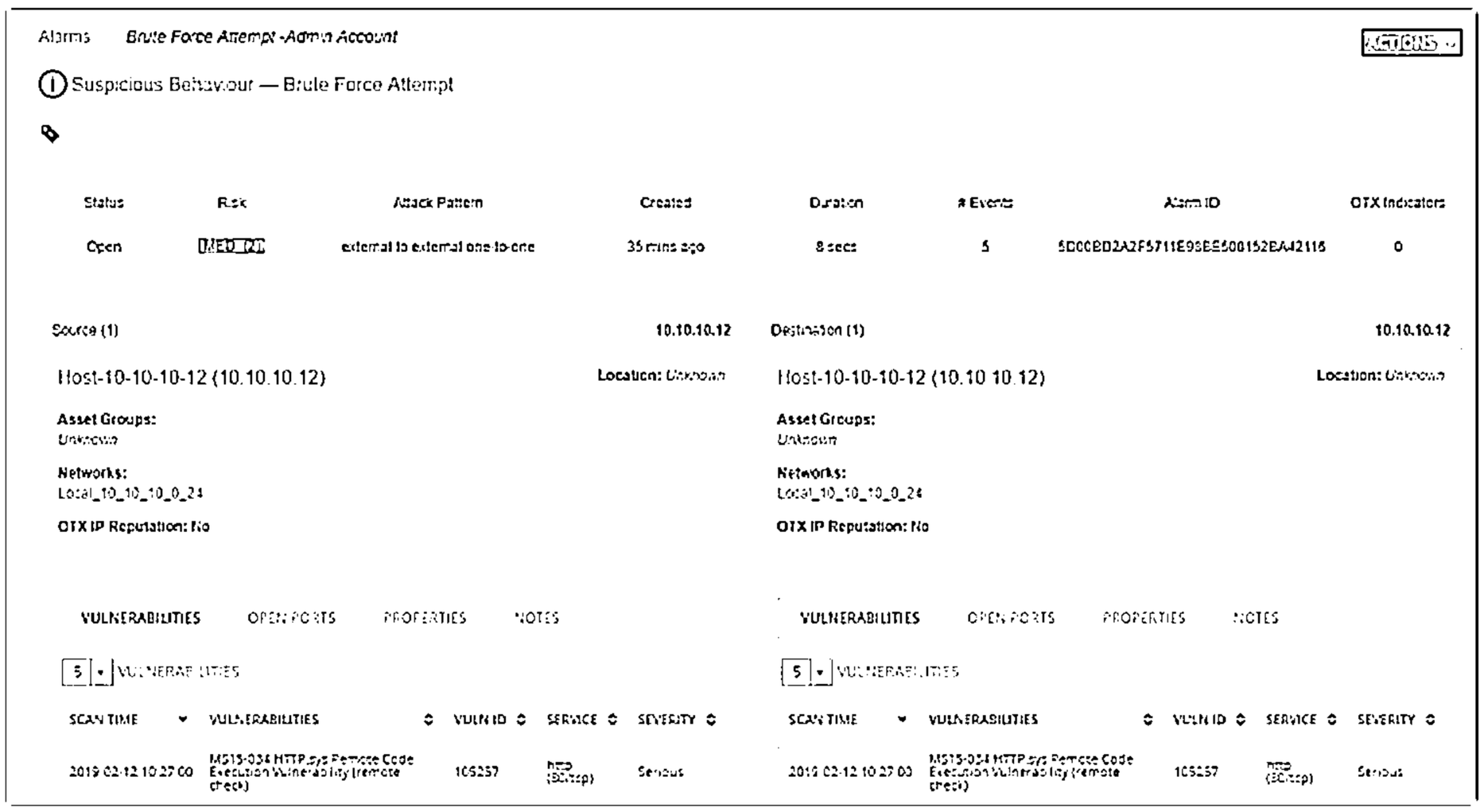
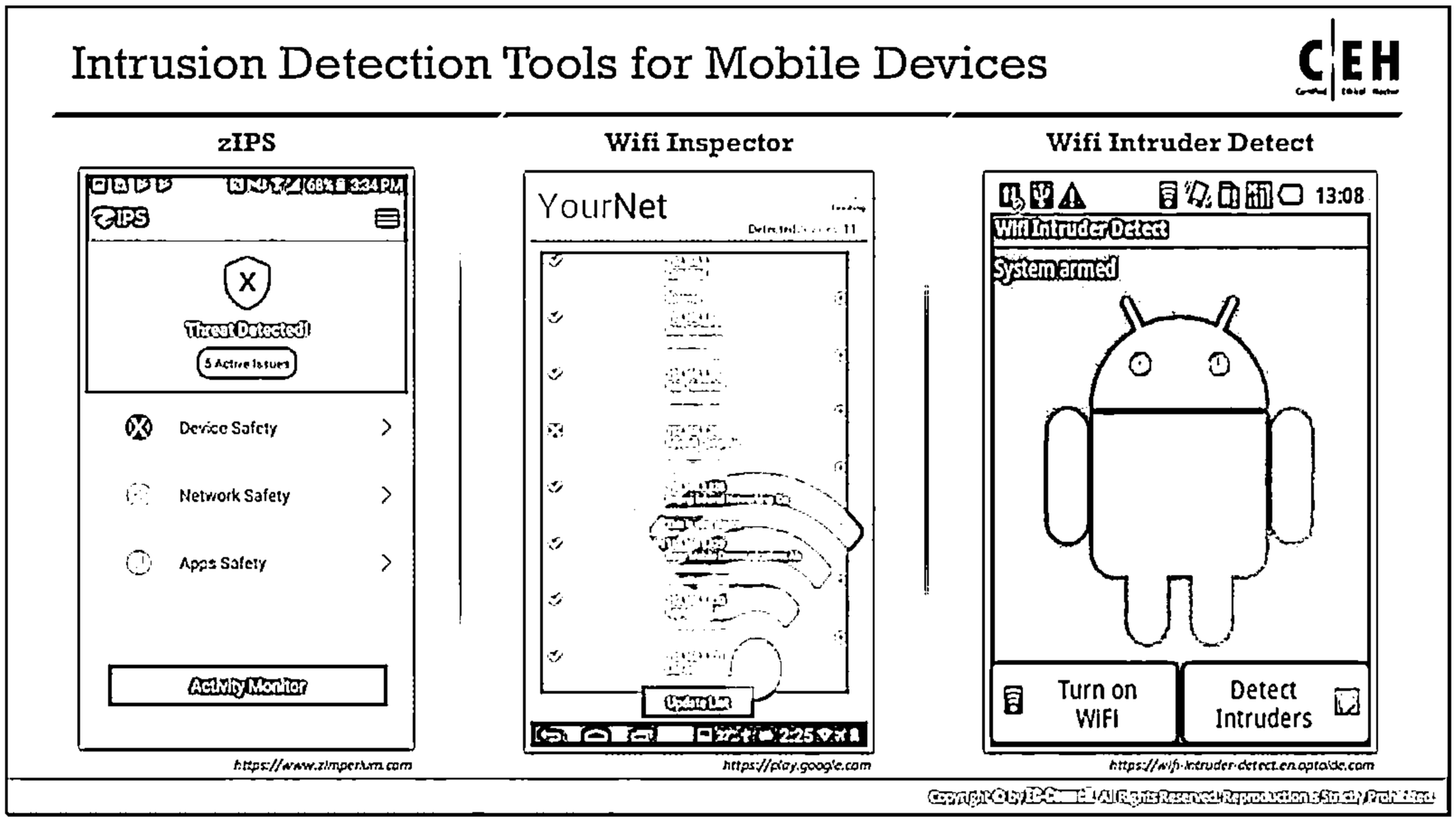


Figure 12.22: Screenshot of AlienVault® OSSIM™

Some additional intrusion detection tools are listed below:

- SolarWinds Security Event Manager (*https://www.solarwinds.com*)
- OSSEC (*https://www.ossec.net*)
- BroIDS/Zeek IDS (*https://www.zeek.org*)

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



Intrusion Detection Tools for Mobile Devices

Intrusion detection tools are also available for mobile devices to help you detect and prevent intrusion attempts.

- **zIPS**

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

  Zimperium's zIPS™ is a mobile intrusion prevention system app that provides comprehensive protection for iOS and Android devices against mobile network, device, and application cyber-attacks. It can detect both known and unknown threats by analyzing the behavior of your mobile device. By examining slight deviations from the mobile device's OS statistics, memory, CPU, and other system parameters, the z9™ detection engine can accurately identify not only the specific type of malicious attack but also the forensics associated with the who, what, where, when, and how of an attack occurrence.

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

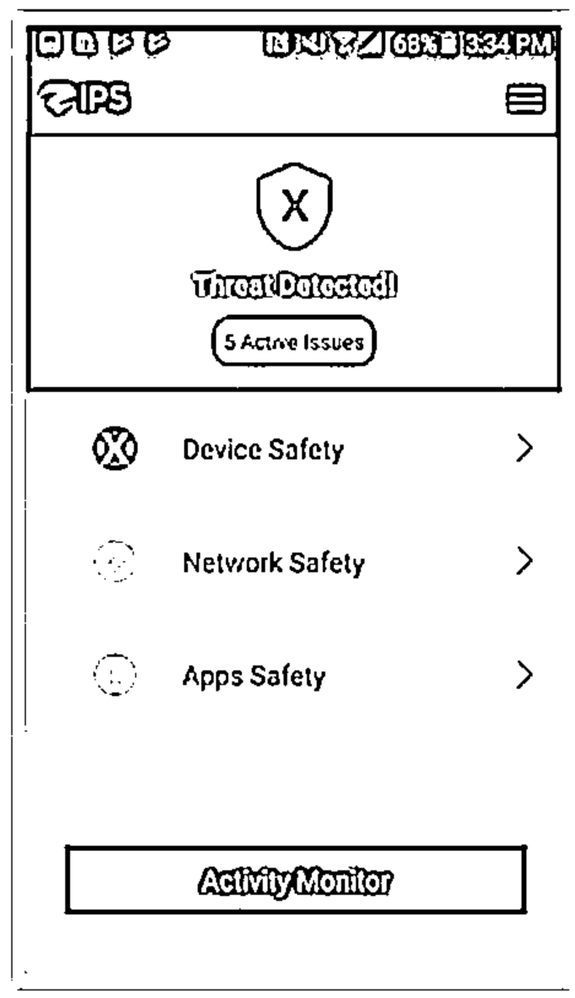


Figure 12.23: Screenshot of zIPS

- **Wifi Inspector**

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

  Wifi Inspector allows you to find all the devices connected to the network (via both wired and Wi-Fi connections, including consoles, TVs, PCs, tablets, and phones); it gives relevant data such as the IP addresses, manufacturer names, device names, and MAC addresses of connected devices. It also allows you to save a list of known devices with a custom name and finds intruders in a short period.

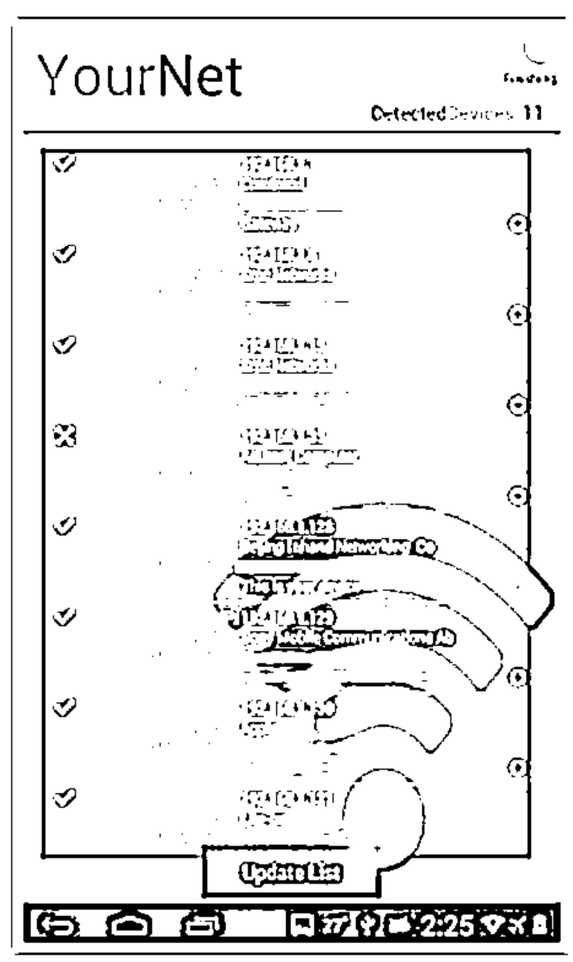


Figure 12.24: Screenshot of Wifi Inspector

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

- **Wifi Intruder Detect**

  Source: *https://wifi-intruder-detect.en.aptoide.com*

  Wifi Intruder Detect helps to find security leaks in the Wi-Fi network Internet connection. It allows you to detect an intruder who is accessing the network, Wi-Fi, or Internet connection without your consent.

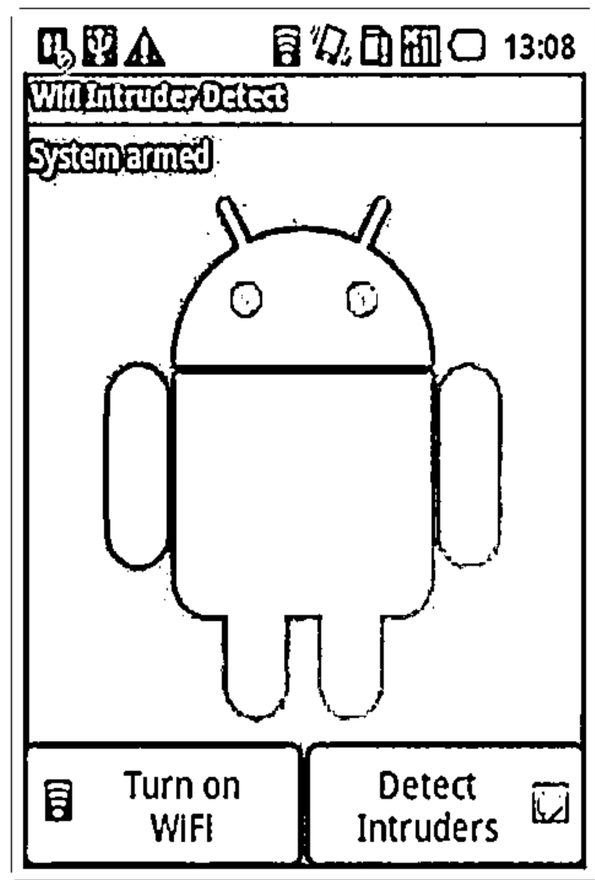


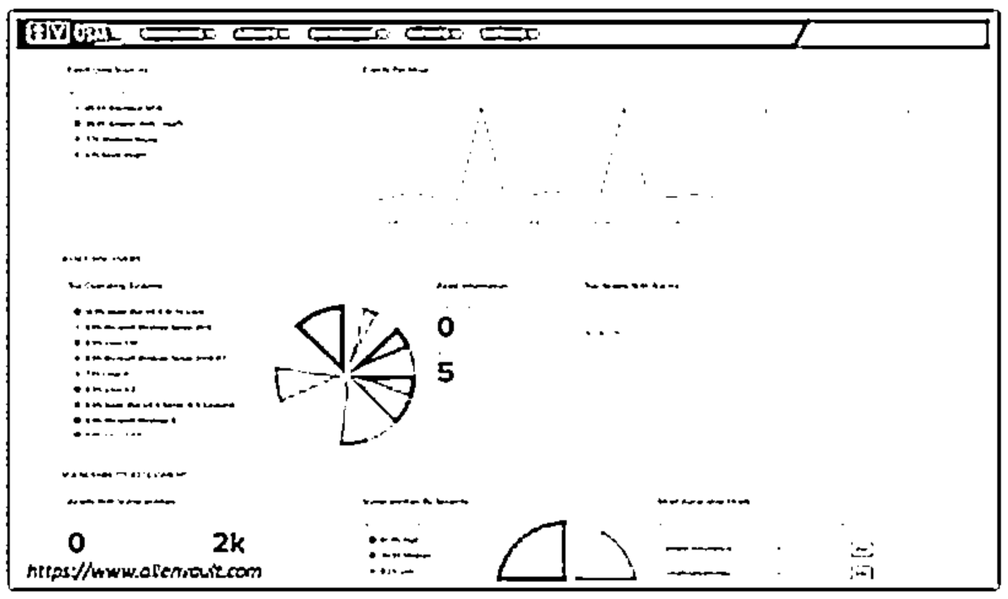
Figure 12.25: Screenshot of Wifi Intruder Detector Pro

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

Intrusion Prevention Tools

AlienVault® Unified Security Management® (USM)

- AlienVault USM offers threat detection, incident response, and compliance management across the cloud, on-premises, and in hybrid environments
- It can be integrated with AlienVault Open Threat Exchange (OTX) to protect the network from intrusions



- **IBM Security Network Intrusion Prevention System** *https://www.ibm.com*
- **Cyberoam Intrusion Prevention System** *https://www.cyberoam.com*
- **McAfee Host Intrusion Prevention for Desktops** *https://www.mcafee.com*
- **Cisco Intrusion Prevention Systems** *https://www.cisco.com*
- **Check Point IPS Software Blade** *https://www.checkpoint.com*

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

Intrusion Prevention Tools

- **AlienVault® Unified Security Management® (USM)**

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

  AlienVault USM can perform threat detection, incident response, and compliance management across cloud, on-premises, and hybrid environments. It can be integrated with AlienVault Open Threat Exchange (OTX), which is an open threat intelligence community with more than 100,000 participants who contribute over 19 million threat indicators daily to protect the network from intrusions.

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

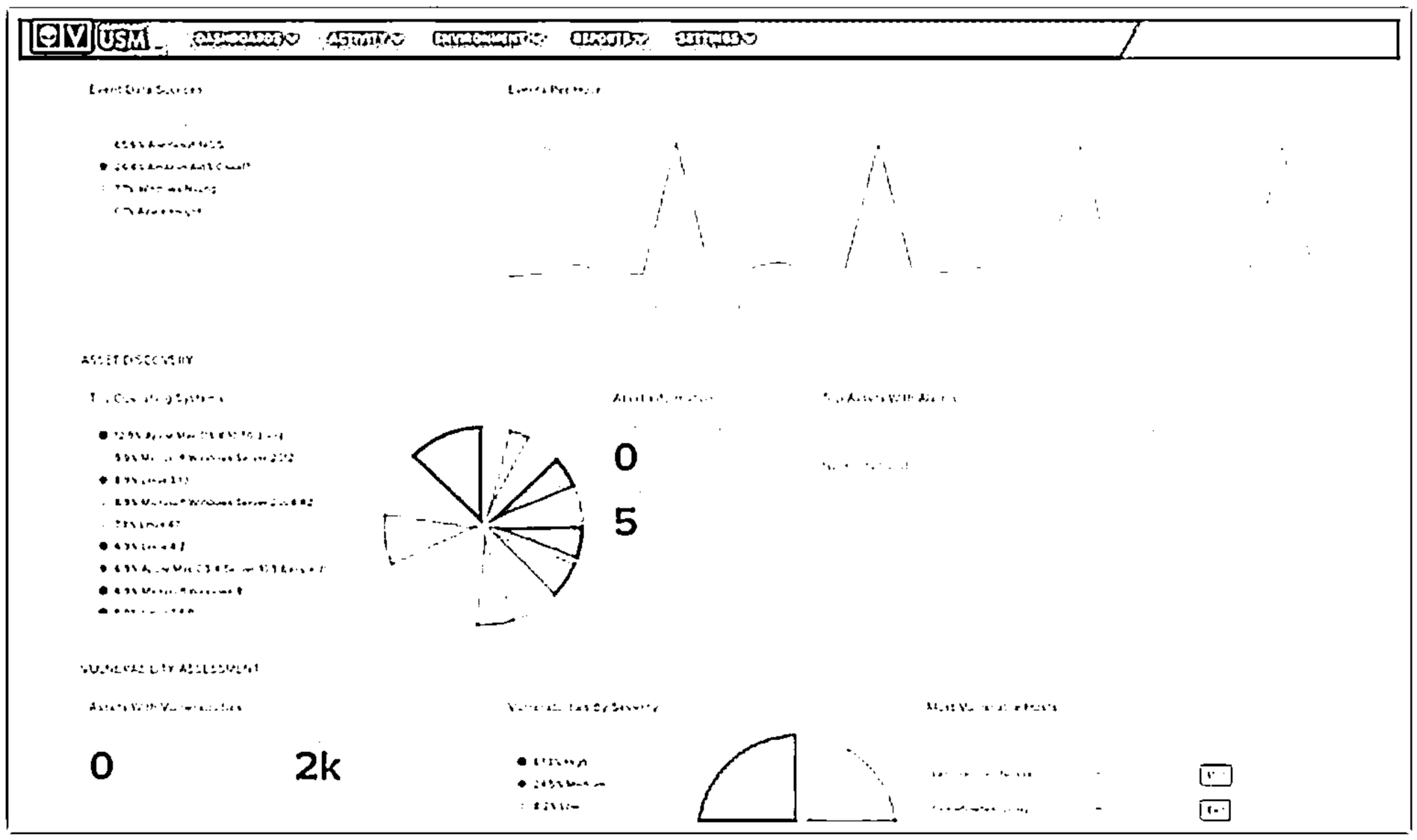


Figure 12.26: Screenshot of AlienVault USM

Some additional intrusion prevention tools are listed below:

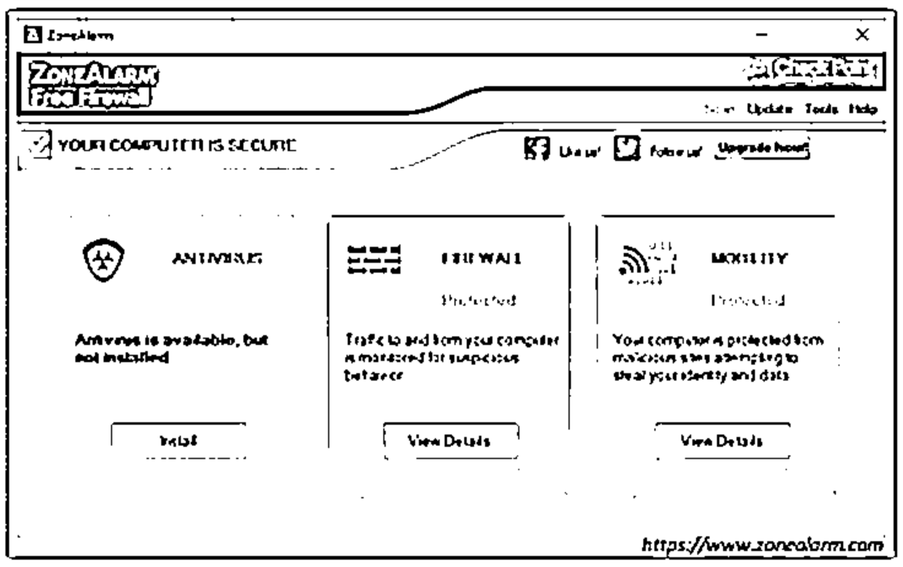
- IBM Security Network Intrusion Prevention System (*https://www.ibm.com*)
- Cyberoam Intrusion Prevention System (*https://www.cyberoam.com*)
- McAfee Host Intrusion Prevention for Desktops (*https://www.mcafee.com*)
- Cisco Intrusion Prevention Systems (*https://www.cisco.com*)
- Check Point IPS Software Blade (*https://www.checkpoint.com*)

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

Firewalls: ZoneAlarm Free Firewall 2019 and ManageEngine Firewall Analyzer

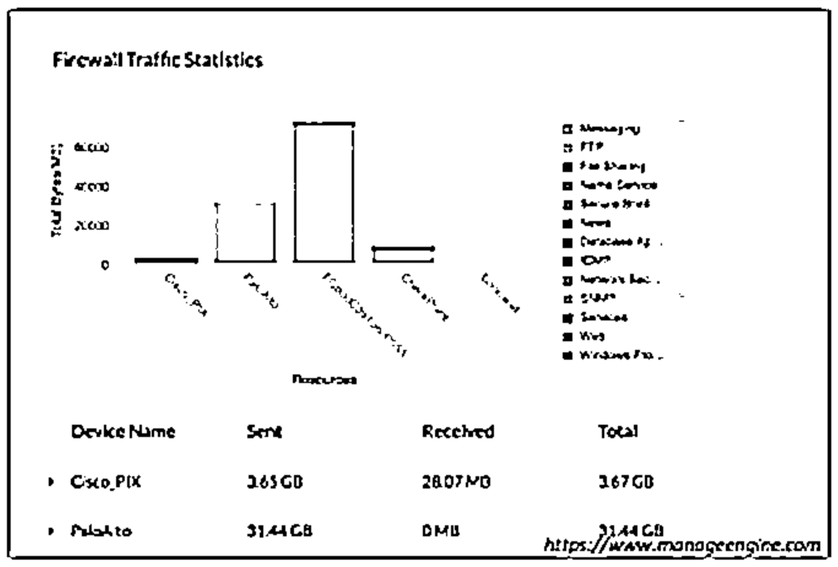
ZoneAlarm Free Firewall 2019

ZoneAlarm Free Firewall 2019 manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that put network privacy at risk



ManageEngine Firewall Analyzer

ManageEngine Firewall Analyzer offers a rich set of pre-defined reports that help in analyzing bandwidth usage and understanding network security



Firewalls

- pfSense (*https://www.pfsense.org*)
- Sophos XG Firewall (*https://www.sophos.com*)
- Comodo Firewall (*https://personalfirewall.comodo.com*)
- Palo Alto Network Wildfire (*https://www.paloaltonetworks.com*)

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

Firewalls

Firewalls provide essential protection to computers against viruses, privacy threats, objectionable content, hackers, and malicious software when connected to the Internet. A firewall monitors running applications that access the network. It analyzes downloads, raises an alert when downloading a malicious file, and stops it from infecting a PC.

- **ZoneAlarm Free Firewall 2019**

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

  ZoneAlarm Free Firewall 2019 prevents attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that may compromise network privacy. It monitors programs for suspicious behavior, spotting and stopping new attacks that bypass traditional anti-virus protection. Moreover, it prevents identity theft by guarding your data. It also erases your tracks, allowing you to surf the web in complete privacy. Furthermore, it locks out attackers, blocks intrusions, and makes your PC invisible online. In addition, it filters out annoying and potentially dangerous emails.

  Features:

  - Two-way firewall that monitors and blocks inbound as well as outbound traffic
  - Allows users to browse the web privately using the Full Stealth Mode
  - Identity protection services help to prevent identify theft by guarding crucial data of the users. It also offers PC protection and data encryption
  - Public network protection and wireless network protection are other key features of this firewall

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

- Provides quick real-time security updates

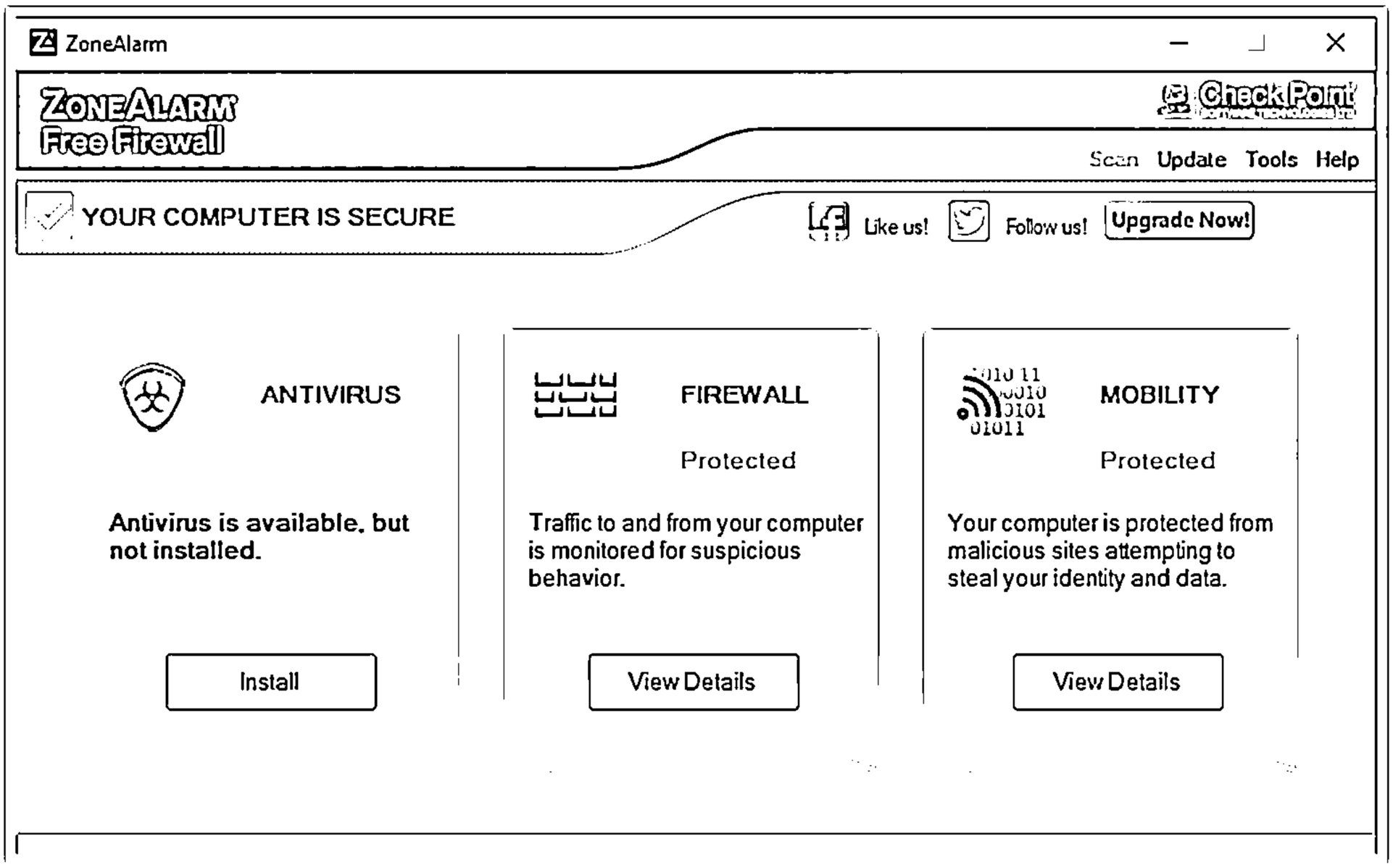


Figure 12.27: Screenshot of ZoneAlarm PRO FIREWALL 2017

- **ManageEngine Firewall Analyzer**

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

  ManageEngine Firewall Analyzer is an agent-less log analytics and configuration management software that helps network administrators to understand how the bandwidth is being used in their network. ManageEngine Firewall Analyzer is vendor-agnostic and supports nearly all open-source and commercial network firewalls such as Check Point, Cisco, Juniper, Fortinet, and Palo Alto.

  Features:

  - Compliance and Change Management
  - User Internet Activity Monitoring
  - Network Traffic and Bandwidth Monitoring
  - Firewall Policy Management
  - Real-time VPN and Proxy Server Monitoring
  - Network Security Management
  - Network Forensic Audits
  - Log Analysis

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

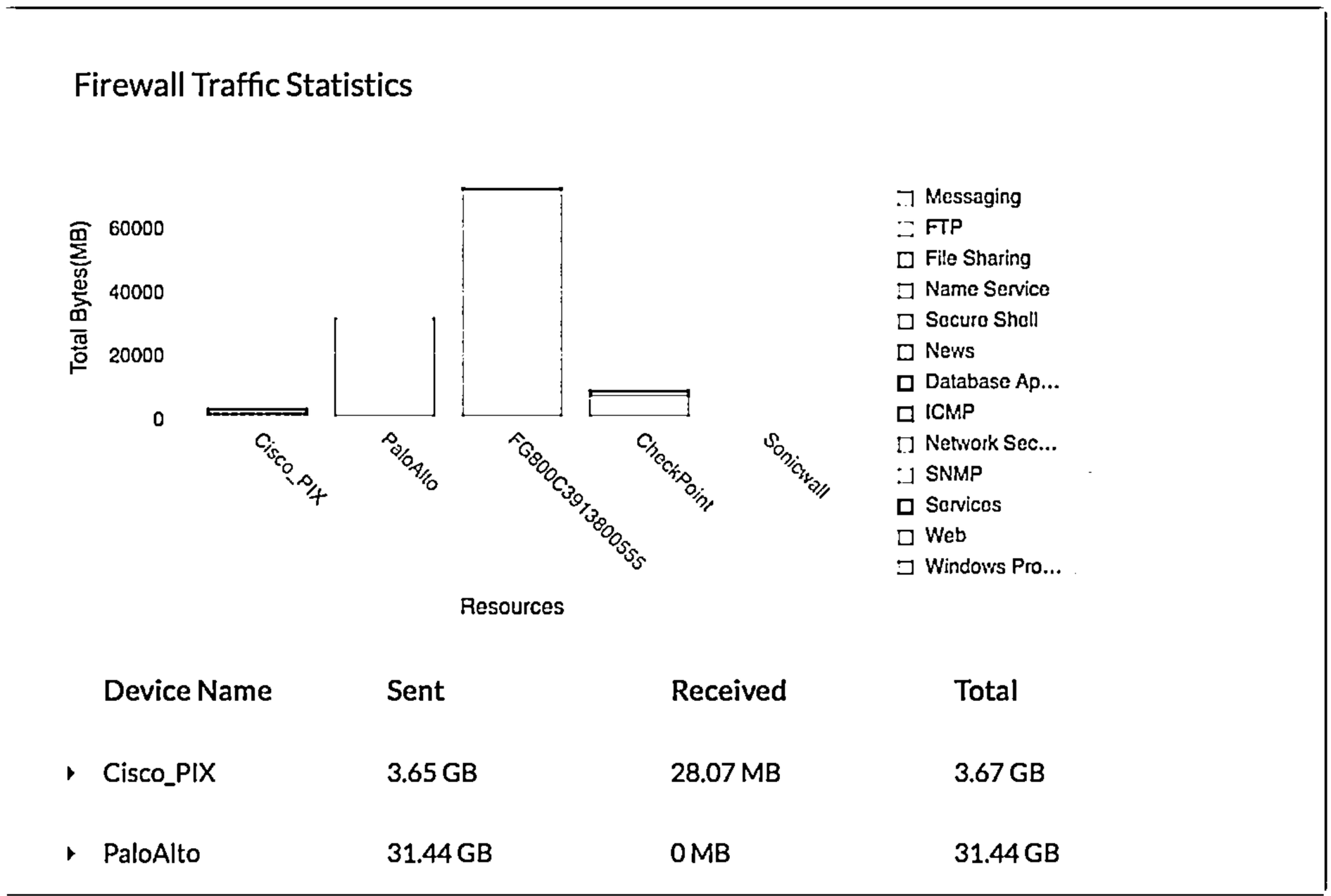
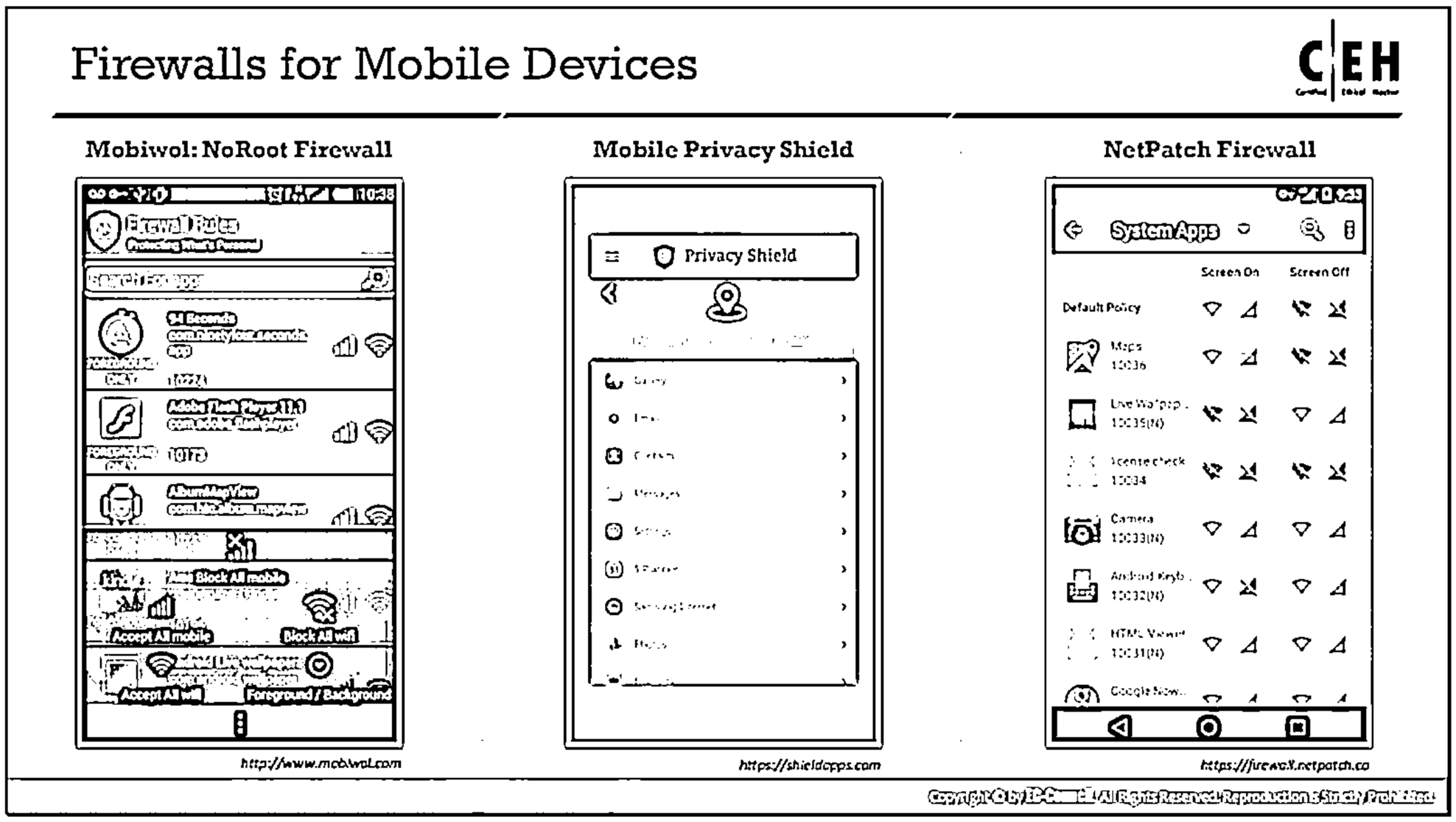


Figure 12.28: Screenshot of ManageEngine Firewall Analyzer

Some additional firewall solutions are listed below:

- pfSense (*https://www.pfsense.org*)
- Sophos XG Firewall (*https://www.sophos.com*)
- Comodo Firewall (*https://personalfirewall.comodo.com*)
- Palo Alto Network Wildfire (*https://www.paloaltonetworks.com*)

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



Firewalls for Mobile Devices

The firewalls discussed previously are used for securing personal computers and networks. Similarly, some firewalls can secure mobile devices.

- **Mobiwol: NoRoot Firewall**

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

  Mobiwol NoRoot Firewall helps to take control of mobile apps, easily allow/block app connectivity, and block background app activity. It generates alerts when new apps access the Internet.

  Features:

  - Automatic launches on device startup
  - Automatically identifies applications currently installed on your mobile device
  - Identifies and notifies when newly installed apps access the web
  - Sets allow/block on a per-application basis
  - Disables background activity for selected apps

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

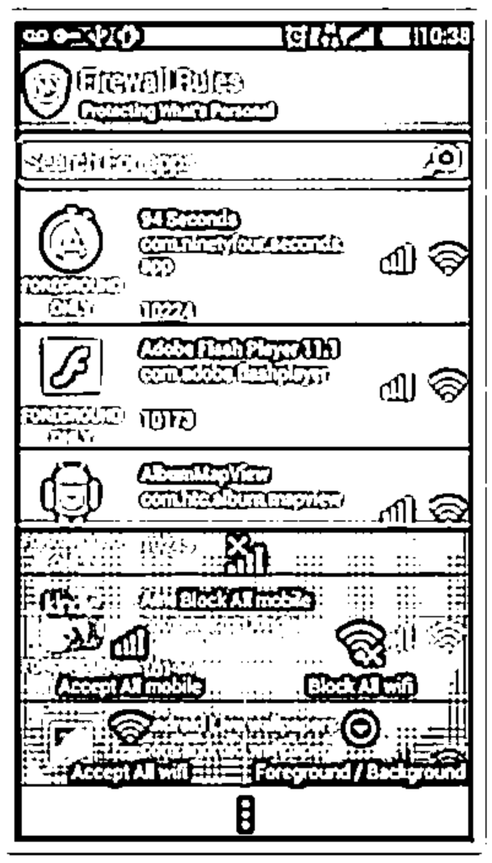


Figure 12.29: Screenshot of Mobiwol: NoRoot Firewall

- **Mobile Privacy Shield**

  Source: *https://shieldapps.com*

  Mobile Privacy Shield is an application for people on the move, i.e., people who store necessary information on their smartphones and use their devices for banking, shopping, business, and more. Mobile Privacy Shield's Privacy Advisor monitors application permissions, sorting them into three categories by the privacy-risk level. Each report is packed with detailed information and a response is suggested per case. Mobile Privacy Shield centralizes all permissions, allowing you to review and assess their validity and need conveniently. It also allows you to remove each threat from within the interface.

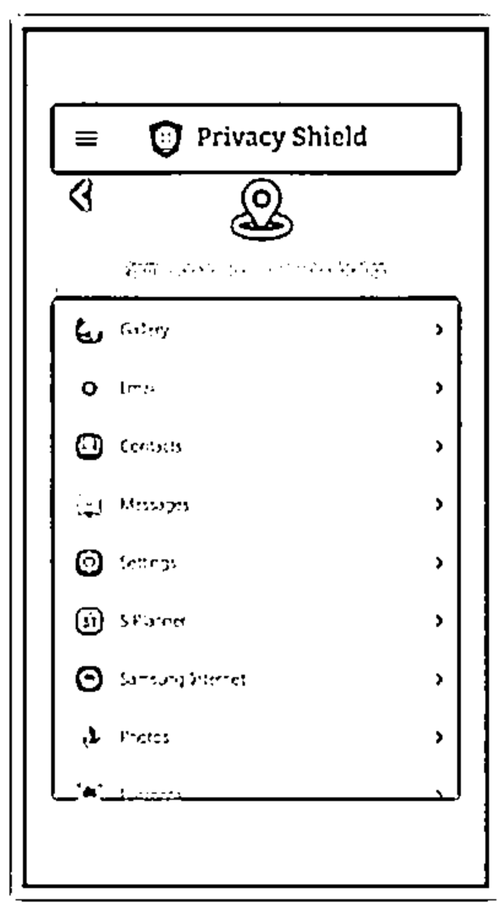


Figure 12.30: Screenshot of Mobile Privacy Shield

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

- **NetPatch Firewall**

  Source: *https://firewall.netpatch.co*

  NetPatch Firewall is a full-featured advanced Android no-root firewall. It can be used to fully control a mobile device network. Using NetPatch Firewall, you can create network rules based on apps, IP addresses, domain names, etc. This firewall is designed to reduce a mobile device's network traffic and battery consumption, improve network security, and ensure privacy.

  Features:

  - Block network access per app, screen on/off, Wi-Fi/mobile (3G & 4G), block roaming
  - Shadowsocks secure proxy, support TCP and UDP (a better VPN proxy)
  - Custom DNS, change your DNS server, support DNS query through Shadowsocks proxy, and set the DNS cache time
  - Notify when new apps installed
  - Export/import configure

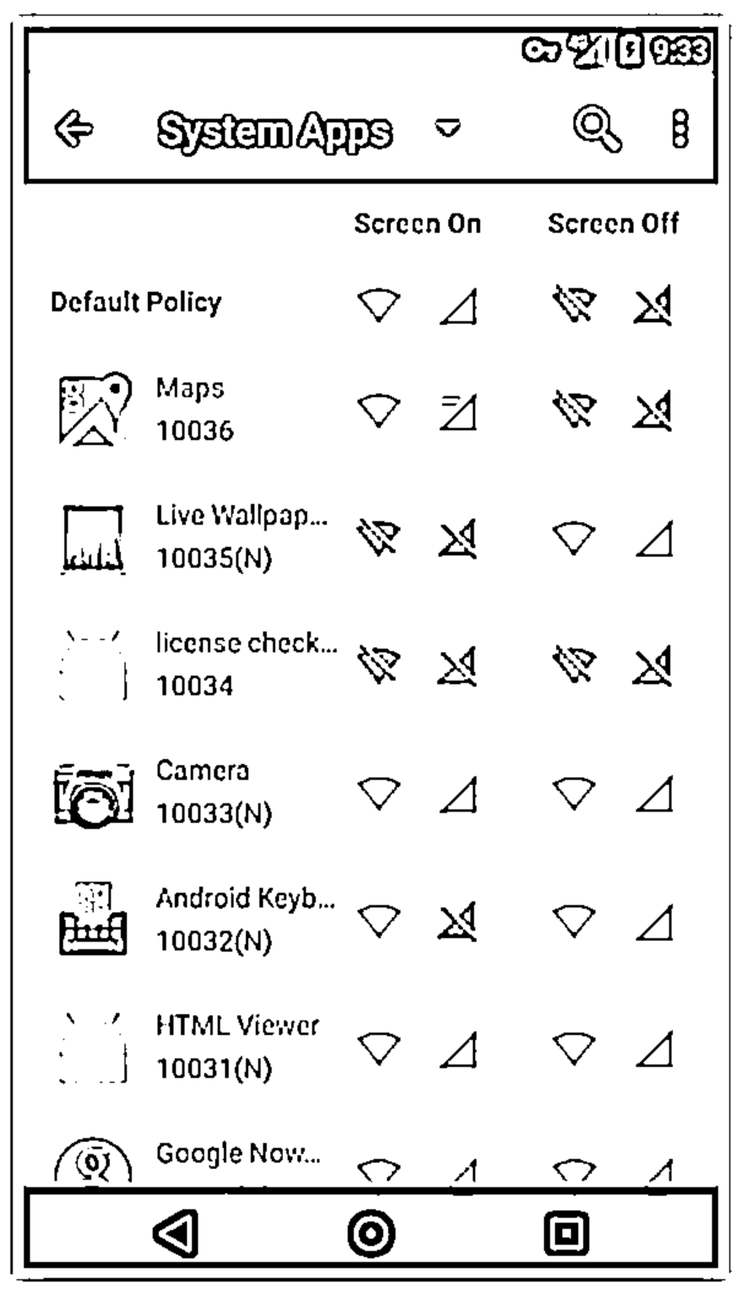


Figure 12.31: Screenshot of NetPatch Firewall

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

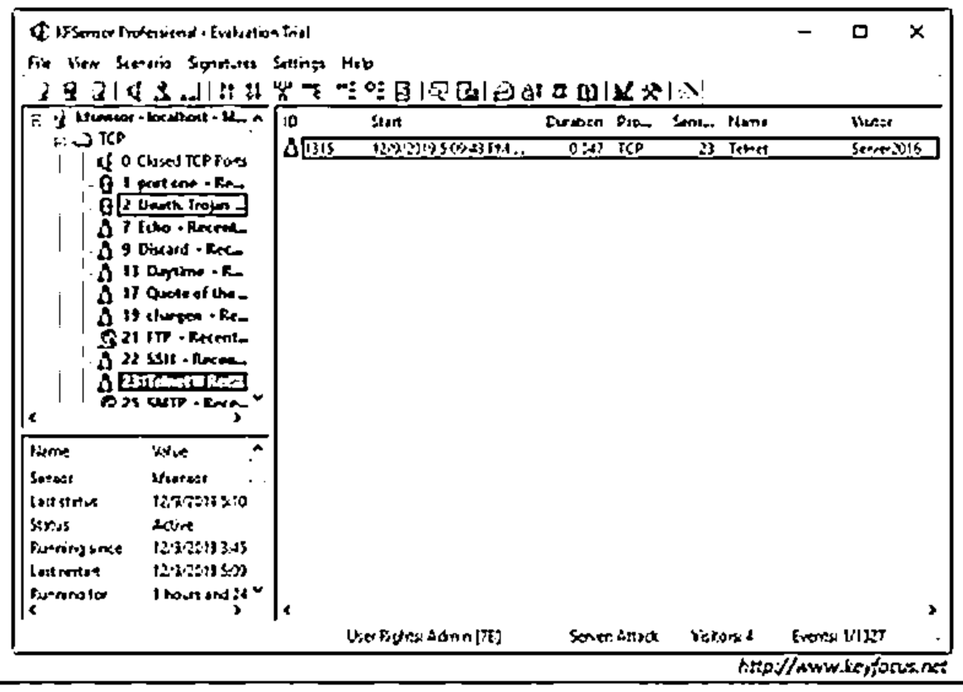
Honeypot Tools: KFSensor and SPECTER

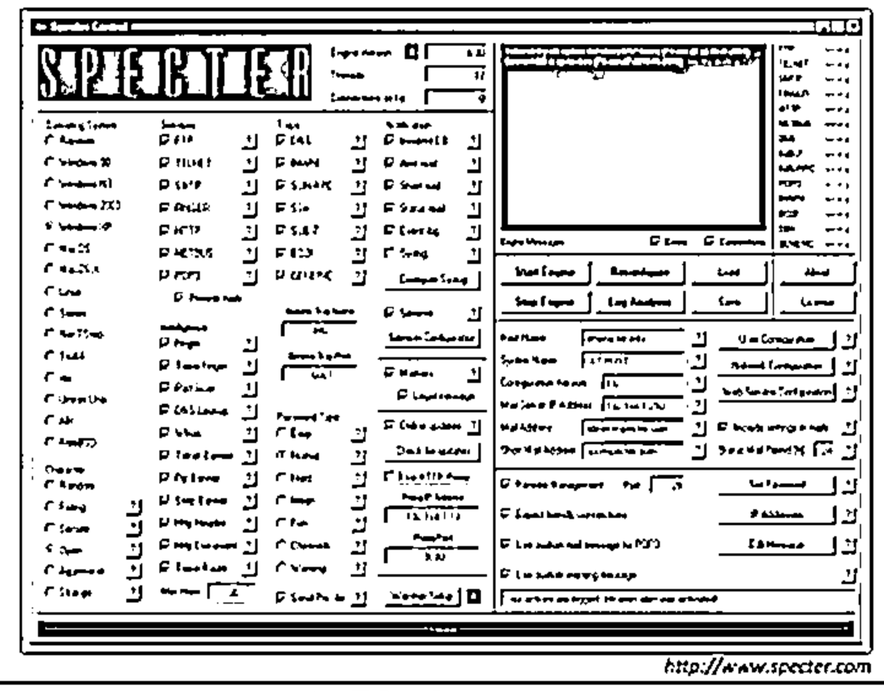
KFSensor

KFSensor is a host-based Intrusion Detection System (IDS) that acts as a honeypot to attract and detect hackers and worms by simulating vulnerable system services and Trojans

SPECTER

SPECTER is a honeypot-based intrusion detection system that offers common Internet services such as SMTP, FTP, POP3, HTTP, and TELNET which appear perfectly normal to the attackers but in fact are traps





Honeypot Tools

Honeypots are security tools that allow the security community to monitor attackers' tricks and exploits by logging all their activity so that it can respond to such exploits quickly before the attacker can misuse or compromise the system.

- **KFSensor**

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

  KFSensor is a host-based IDS that acts as a honeypot to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By acting as a decoy server, it can divert attacks from critical systems and provide a higher level of information than that achieved using firewalls and NIDS alone.

  You can use KFSensor in a Windows-based corporate environment. It includes many innovative and unique features such as remote management, a Snort-compatible signature engine, and emulations of Windows networking protocols.

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

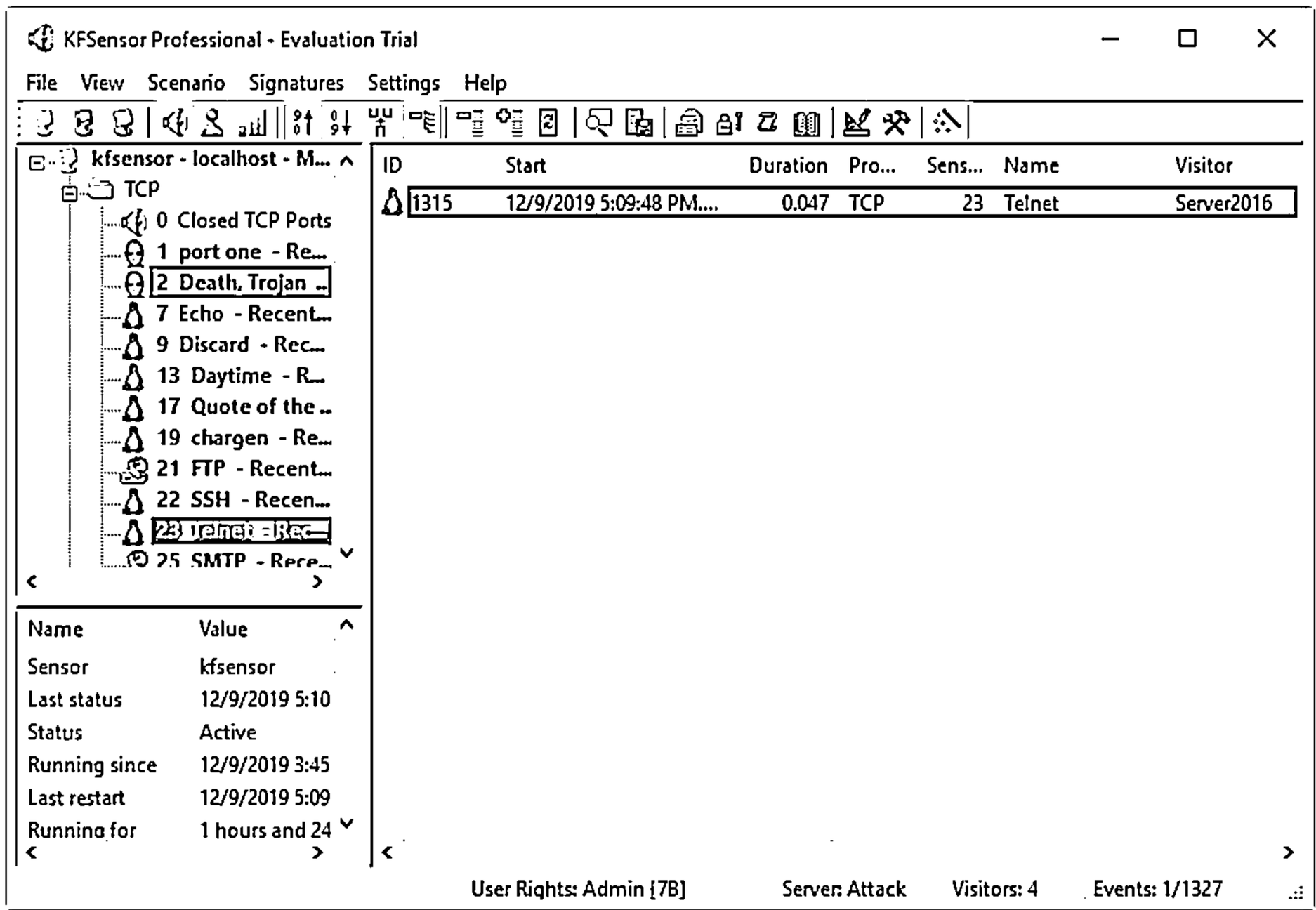


Figure 12.32: Screenshot of KFSensor

- **SPECTER**

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

  SPECTER is a honeypot or deception system. It simulates a complete system and provides an appealing target to lure hackers away from production systems. It offers typical Internet services such as SMTP, FTP, POP3, HTTP, and TELNET, which appear perfectly normal to attackers. However, it traps attackers by tricking them into leaving some traces that show that they had connected to a decoy system that does none of the things it appears to but instead logs everything and notifies the appropriate people.

  Furthermore, SPECTER automatically investigates attackers while they are still trying to break in. It provides massive amounts of decoy content and generates decoy programs that do not leave traces on the attacker's computer. Automated weekly online updates of the honeypot's content and vulnerability databases allow the honeypot to change regularly without user interaction.

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

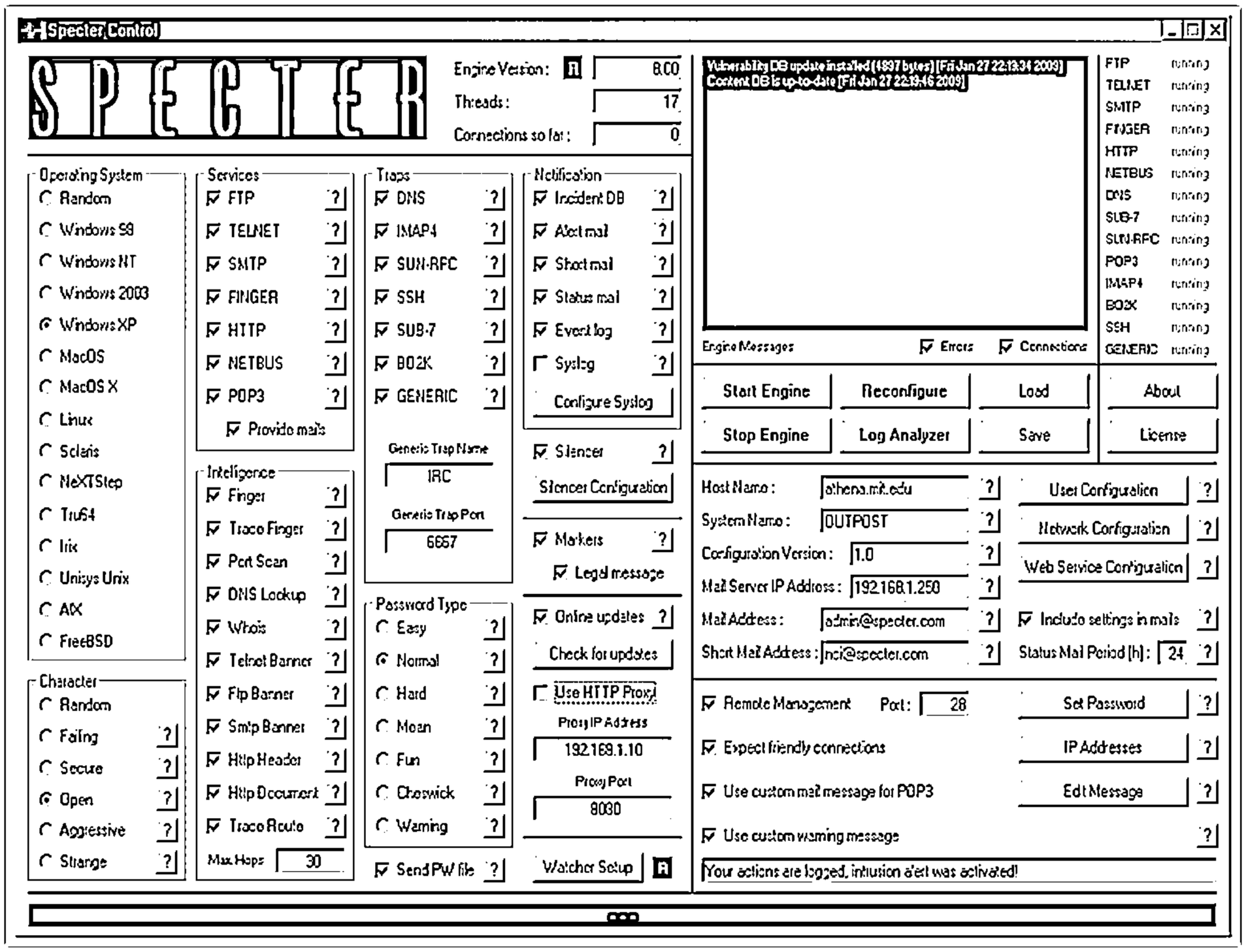


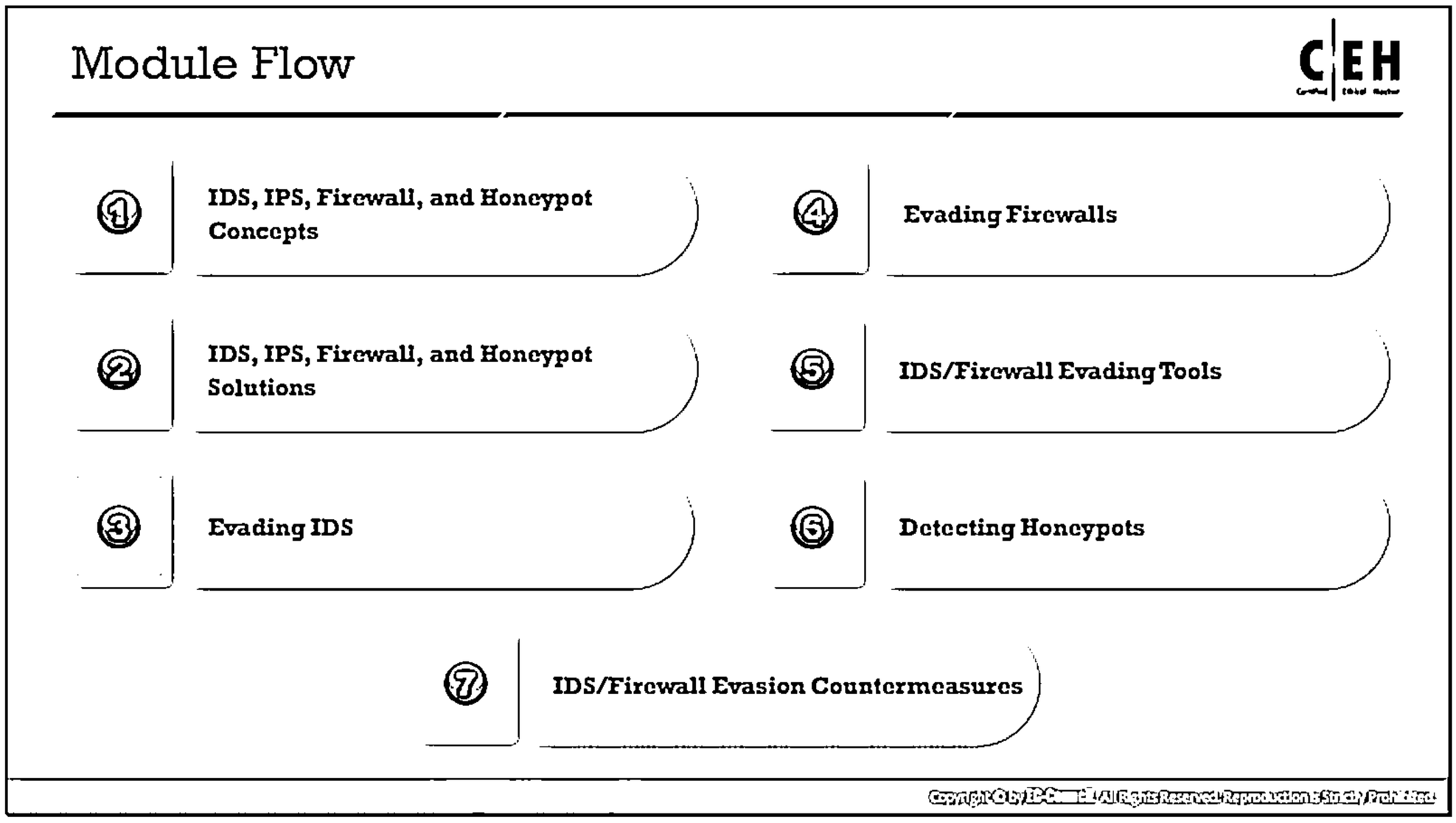
Figure 12.33: Screenshot of SPECTER

Some additional honeypot tools are listed below:

- HoneyBOT (*https://www.atomicsoftwaresolutions.com*)
- MongoDB-HoneyProxy (*https://github.com*)
- Modern Honey Network (*https://github.com*)
- Honeyd (*http://www.honeyd.org*)

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

Module Flow



Evading IDS

The previous sections helped us to understand IDS, IPS, their roles and functions, how they protect your network from intruders, and the various IDS solutions available. Even though IDS thwart attempts to breach the network security, attackers can still evade IDS. This section explains various ways in which attackers evade IDS.

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

IDS Evasion Techniques

1 Insertion Attack	7 Unicode Evasion	13 Polymorphic Shellcode
2 Evasion	8 Fragmentation Attack	14 ASCII Shellcode
3 Denial-of-Service Attack	9 Overlapping Fragments	15 Application-Layer Attacks
4 Obfuscating	10 Time-To-Live Attacks	16 Desynchronization
5 False Positive Generation	11 Invalid RST Packets	17 Encryption
6 Session Splicing	12 Urgency Flag	18 Flooding

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

IDS Evasion Techniques

IDS that provide an extra layer of security to the organization's infrastructure are interesting targets for attackers. Attackers implement various IDS evasion techniques to bypass such security mechanisms and compromise the infrastructure. IDS evasion is the process of modifying attacks to fool the IDS/IPS into interpreting that the traffic is legitimate and thus prevent the IDS from triggering an alert. Many IDS evasion techniques can perform IDS evasion in different and effective ways.

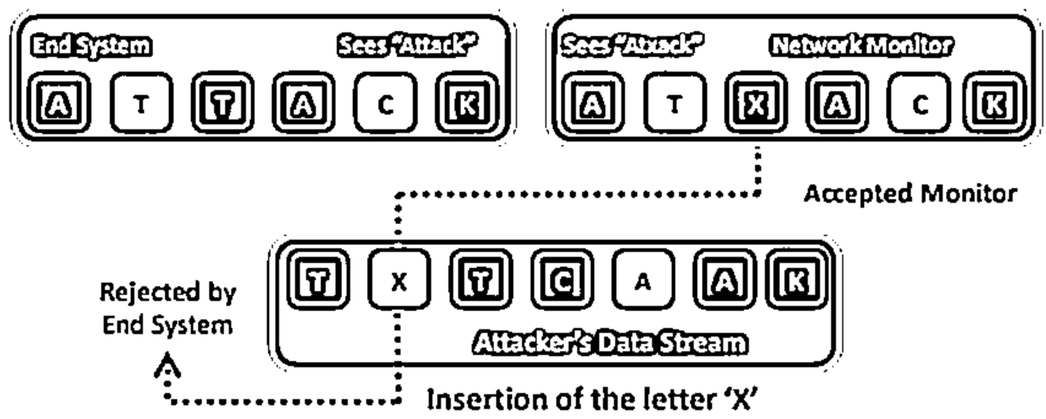
Some IDS evasion techniques are as follows

- Insertion Attack
- Evasion
- DoS Attack
- Obfuscating
- False Positive Generation
- Session Splicing
- Unicode Evasion
- Fragmentation Attack
- Overlapping Fragments
- Time-To-Live Attacks
- Invalid RST Packets
- Urgency Flag
- Polymorphic Shellcode
- ASCII Shellcode
- Application-Layer Attacks
- Desynchronization
- Encryption
- Flooding

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

Insertion Attack

1. Insertion is the process by which the attacker confuses the IDS by forcing it to read invalid packets
2. An IDS blindly believes and accepts a packet that an end system rejects, and an attacker exploits this condition and inserts data into the IDS
3. This attack occurs when the NIDS is less strict in processing packets than the internal network
4. The attacker obscures extra traffic and the IDS concludes that the traffic is harmless. Hence, the IDS gets more packets than the destination



- An attacker sends one-character packets to the target system via the IDS with varying TTL such that some packets reach the IDS but not the target system
- This will result in the IDS and the target system having two different character strings

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

Insertion Attack

Insertion is the process by which the attacker confuses the IDS by forcing it to read invalid packets (i.e., the system may not accept the packet addressed to it). An IDS blindly trusts and accepts a packet that an end system rejects. If a packet is malformed or if it does not reach its actual destination, the packet is invalid. If the IDS reads an invalid packet, it gets confused. An attacker exploits this condition and inserts data into the IDS. This attack occurs when the NIDS is less strict in processing packets than the internal network. The attacker obscures extra traffic and the IDS concludes that the traffic is harmless. Hence, the IDS gets more packets than the destination.

To understand how insertion becomes a problem for a network IDS, it is important to understand how the IDS detects attacks. It employs pattern-matching algorithms to look for specific patterns of data in a packet or stream of packets. For example, it might search for the "phf" string in an HTTP request to discover a PHF **Common Gateway Interface (CGI)** attack. An attacker who can insert packets into the IDS can prevent pattern matching from working. For instance, an attacker can send the string "phf" to a web server, attempting to exploit the CGI vulnerability, but force the IDS to read "phoneyf" (by "inserting" the string "oney") instead. A straightforward insertion attack involves intentionally corrupting the IP checksum. Every packet transmitted on an IP network has a checksum that verifies the corrupted packets. IP checksums are 16-bit numbers computed by examining the information in the packet. If the checksum on an IP packet does not match the actual packet, the addressed host will not accept it, while the IDS might consider it as part of the effective stream.

For example, the attacker can send packets whose time-to-live (TTL) fields are crafted to reach the IDS but not the target computers. This will result in the IDS and the target system having two different character strings. An attacker confronts the IDS with a stream of one-character

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

packets (the attacker-originated data stream), in which one of the characters (the letter "X") will be accepted only by the IDS. As a result, the IDS and the end system reconstruct two different strings.

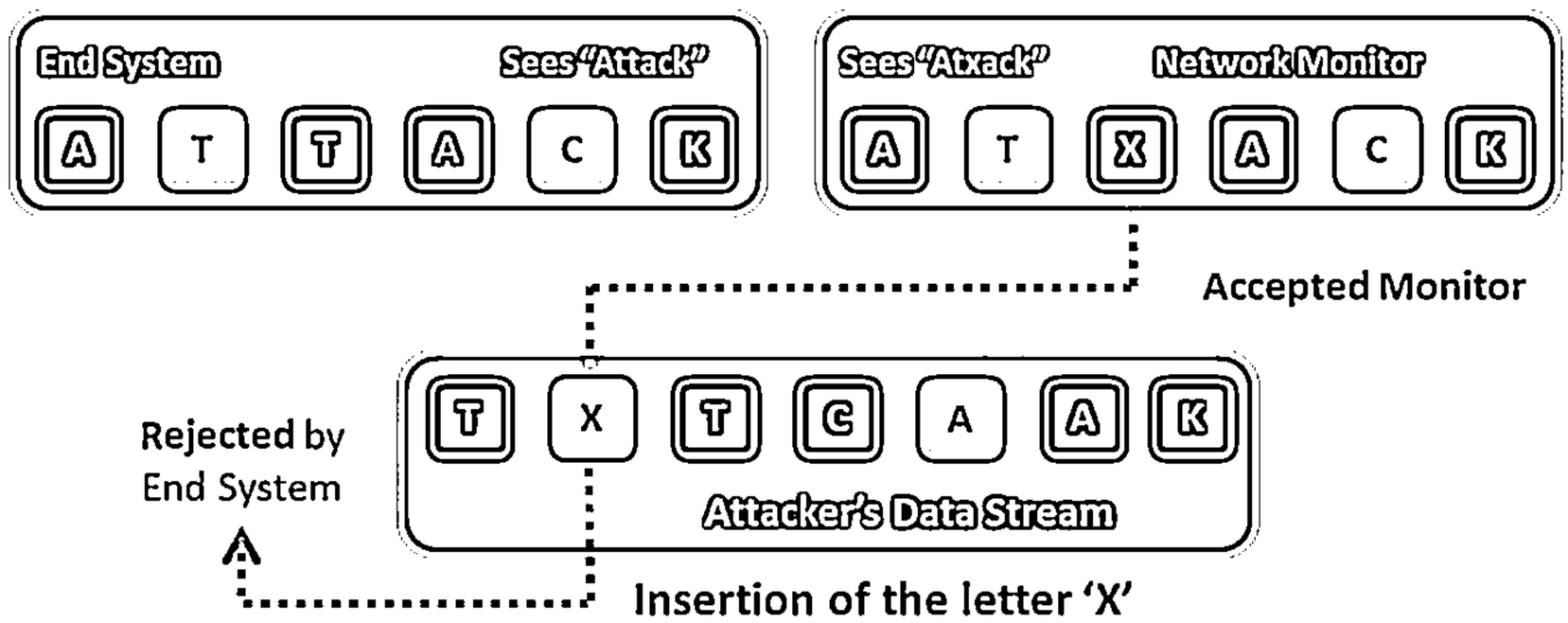
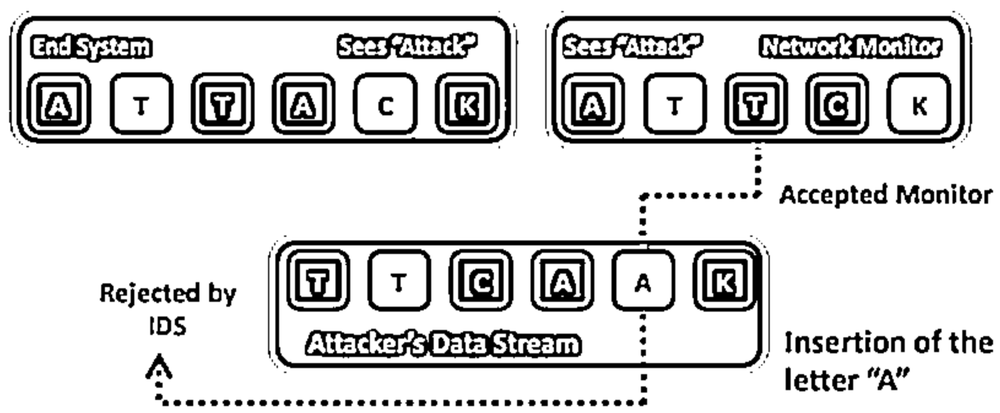


Figure 12.34: Evading IDS using Insertion attack

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

Evasion

- In this evasion technique, an end system accepts a packet that an IDS rejects
- Using this technique, an attacker exploits the host computer without the IDS ever realizing it
- The attacker sends portions of the request in packets that the IDS mistakenly rejects, allowing the removal of parts of the stream from the IDS



- For example, if the malicious sequence is sent byte-by-byte and one byte is rejected by the IDS, the IDS cannot detect the attack
- Here, the IDS gets fewer packets than the destination

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

Evasion

An "evasion" attack occurs when the IDS discards packets while the host that has to get the packets accepts them. Using this technique, an attacker exploits the host computer. Evasion attacks have an adverse effect on the accuracy of the IDS. An evasion attack at the IP layer allows an attacker to attempt arbitrary attacks against hosts on a network without the IDS ever realizing it. The attacker sends portions of the request in packets that the IDS mistakenly rejects, allowing the removal of parts of the stream from the ID system's view. For example, if the attacker sends a malicious sequence byte by byte, and if the IDS rejects only one byte, it cannot detect the attack. Here, the IDS gets fewer packets than the destination.

One example of an evasion attack is when an attacker opens a TCP connection with a data packet. Before any TCP connection can be used, it must be "**opened**" with a handshake between the two endpoints of the connection. An essential fact about TCP is that the handshake packets can themselves bear data. The IDS that does not accept the data in these packets is vulnerable to an evasion attack.

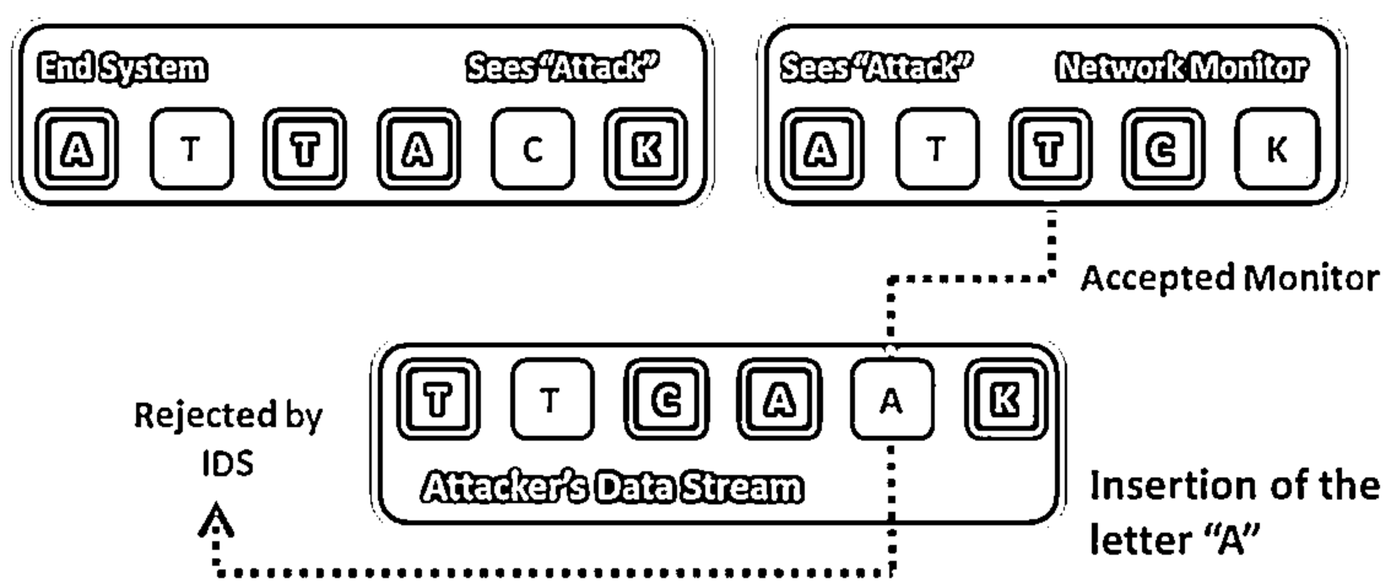


Figure 12.35: Illustration of Evasion technique

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

Denial-of-Service Attack (DoS)

- Many IDSs use a centralized server for logging alerts
- If the attackers know the IP address of the centralized server, they can perform DoS or other hacks to slow down or crash the server
- As a result, the attackers' intrusion attempts will not be logged

Using this evasion technique, an attacker

1. Causes the device to lock up
2. Causes personnel to be unable to investigate all the alarms
3. Causes more alarms than can be handled by management systems (such as databases)
4. Fills up disk space causing attacks not to be logged
5. Consumes the device's processing power and allows attacks to sneak by

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

Denial-of-Service Attack (DoS)

Multiple types of DoS attack will work against IDS. The attacker identifies a point of network processing that requires the allocation of a resource, causing a condition to occur in which all of that resource is consumed. The resources affected by the attacker are CPU cycles, memory, disk space, and network bandwidth. Attackers monitor and attack the CPU capabilities of the IDS. This is because the IDS needs half of a CPU cycle to read the packets, detect the purpose of their existence, and then compare them with some location in the saved network state. An attacker can verify the most computationally expensive network processing operations and then compel the IDS to spend all its time in carrying out useless work.

An IDS requires memory for a variety of tasks such as generating a match for the patterns, saving the TCP connections, maintaining reassembly queues, and producing buffers for the data. In the initial phase, the system requires memory to read the packets. The system will allocate the memory for network processing operations. An attacker can verify the processing operations that require the IDS to allocate memory and force the IDS to assign all of its memory for meaningless information.

In certain circumstances, the IDS store activity logs on the disk. The stored events occupy most of the disk space. Most computers have limited disk space. The attackers can occupy a significant part of the disk space on the IDS by creating and storing a large number of useless events. This renders the IDS useless in terms of storing real events.

Network IDS record the activity on the networks they monitor. They are competent because networks are rarely used to their full capacity; few monitoring systems can cope with an extremely busy network.

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

The IDS, unlike an end system, must read everyone's packets, not just those explicitly sent to it. An attacker can overload the network with meaningless information and prevent the IDS from keeping up with what is happening on the network.

Many IDS today employ central logging servers that are used exclusively to store IDS alert logs. The central server's function is to centralize alert data so that it is viewed as a whole rather than on a system-by-system basis.

However, if attackers know the central log server's IP address, they could slow it down or even crash it using a DoS attack. After shutting down the server, attacks could go unnoticed because the alert data is now no longer logged.

Using this evasion technique, an attacker

- Causes the device to lock up
- Causes personnel to be unable to investigate all the alarms
- Causes more alarms than can be handled by management systems (such as databases, etc.)
- Fills up disk space, preventing attacks from being logged
- Consumes the device's processing power and allows attacks to sneak by

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

Obfuscating

1. Obfuscating is an IDS evasion technique used by attackers who encode the attack packet payload in such a way that the destination host can decode the packet but not the IDS
2. Attackers manipulate the path referenced in the signature to fool the HIDS
3. Attackers can encode attack patterns in unicode to bypass IDS filters, but be understood by an IIS web server
4. Polymorphic code is another means to circumvent signature-based IDSs by creating different attack patterns, so that the attack does not have just one unique detectable signature
5. Attacks on encrypted protocols such as HTTPS are obfuscated if the attack is encrypted

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

Obfuscating

Obfuscation means to make code more difficult to understand or read, generally for privacy or security purposes. A tool called an obfuscator converts a straightforward program into one that works in the same way but which is much more difficult to understand.

Obfuscating is an IDS evasion technique used by attackers to encode the attack packet payload in such a way that the destination host can only decode the packet but not the IDS. An attacker manipulates the path referenced in the signature to fool the HIDS. Using Unicode characters, an attacker can encode attack packets that the IDS would not recognize but which an IIS web server can decode. Polymorphic code is another means to circumvent signature-based IDS by creating unique attack patterns so that the attack does not have a single detectable signature. Attackers perform obfuscated attacks on encrypted protocols such as HTTPS. Attackers can also use obfuscation techniques such as digital steganography to bypass IDS and deploy malware on to the target system lying beyond the IDS.

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

False Positive Generation

1. Attackers with knowledge of the target IDS craft malicious packets just to generate alerts
2. These packets are sent to the IDS to generate many false positive alerts
3. Attackers then use these false positive alerts to hide the real attack traffic
4. Attackers can bypass the IDS unnoticed as it is difficult to differentiate the attack traffic from the large volume of false positives

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

False Positive Generation

This mode does not attack the target; instead, it does something relatively ordinary. In this mode, the IDS generates an alarm when no condition is present to warrant one. Another attack similar to the DoS method is to create a significant amount of alert data that the IDS will log. Attackers construct malicious packets known to trigger alerts within the IDS, forcing it to generate a large number of false reports. Such an attack creates a large amount of log "noise" in an attempt to blend real attacks with fake ones. Attackers know all too well that when looking at log data, it can be challenging to differentiate between legitimate attacks and false positives. If attackers know the IDS, they can even generate false positives specific to that IDS. Attackers then use these false positive alerts to hide real attack traffic. Attackers can bypass IDS unnoticed, as it is difficult to differentiate the attack traffic from the large volume of false positives.

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

Session Splicing

1. Session splicing is a technique used to bypass the IDS where an attacker splits the attack traffic into many packets such that no single packet triggers the IDS
2. It is effective against IDSs that do not reconstruct packets before checking them against intrusion signatures
3. If attackers are aware of a delay in packet reassembly at the IDS, they can add delays between packet transmissions to bypass the reassembly
4. Many IDSs stop reassembly if they do not receive packets within a certain time
5. The IDS will stop working if the target host keeps the session active for a time longer than the IDS reassembly time
6. Any attack attempt after a successful splicing attack will not be logged by the IDS

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

Session Splicing

Session splicing is an IDS evasion technique that exploits how some IDS do not reconstruct sessions before pattern-matching the data. It is a network-level evasion method used to bypass IDS where an attacker splits the attack traffic into an excessive number of packets such that no single packet triggers the IDS. The attacker divides the data in the packets into small portions of a few bytes and evades the string match while delivering the data. The IDS cannot handle an excessive number of small-sized packets and fails to detect the attack signatures. If attackers know what IDS is in use, they could add delays between packets to bypass reassembly checking. This approach is effective against IDS that do not reconstruct packets before checking them against intrusion signatures. If attackers are aware of the delay in packet reassembly at the IDS, they can add delays between packet transmissions to bypass the reassembly.

Many IDS reassemble communication streams; hence, if a packet is not received within a reasonable period, many IDS stop reassembling and handling that stream. If the application under attack keeps a session active for a longer time than that spent by the IDS on reassembling it, the IDS will stop. As a result, any session after the IDS stops reassembling the sessions will be susceptible to malicious data theft by attackers. The IDS will not log any attack attempt after a successful splicing attack. Attackers can use tools such as **Nessus** for session-splicing attacks.

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

Unicode Evasion Technique

1. Unicode is a character coding system to support the worldwide interchange, processing, and display of written texts
2. In the Unicode code space, all the code points are treated differently but it is possible that there could be multiple representations of a single character

   For example, / → %u2215, e → %u00e9 (UTF-16) and © → %c2%a9, ≠ → %e2%89%a0 (UTF-8)
3. Because of this complexity, some IDS systems handle Unicode improperly as Unicode allows multiple interpretations of the same characters
4. Taking this as an advantage, attackers can convert attack strings to Unicode characters to avoid pattern and signature matching at the IDS

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

Unicode Evasion Technique

Unicode is a character coding system that supports encoding, processing, and displaying of written texts for universal languages to maintain consistency in a computer representation. Several standards, such as Java, LDAP, and XML, require Unicode, and many OS and applications support it. Attackers can implement an attack by different character encodings known as "**code points**" in the Unicode code space. The most commonly used character encodings are Unicode Transformation Format (UTF)-8 and UTF-16.

For Example: In UTF-16, the character "/" can be represented as "%u2215" and "e" as "%u00e9"; in UTF- 8, "©" can be represented as "%c2%a9" and "≠" as "%e2%89%a0."

Problems with Unicode:

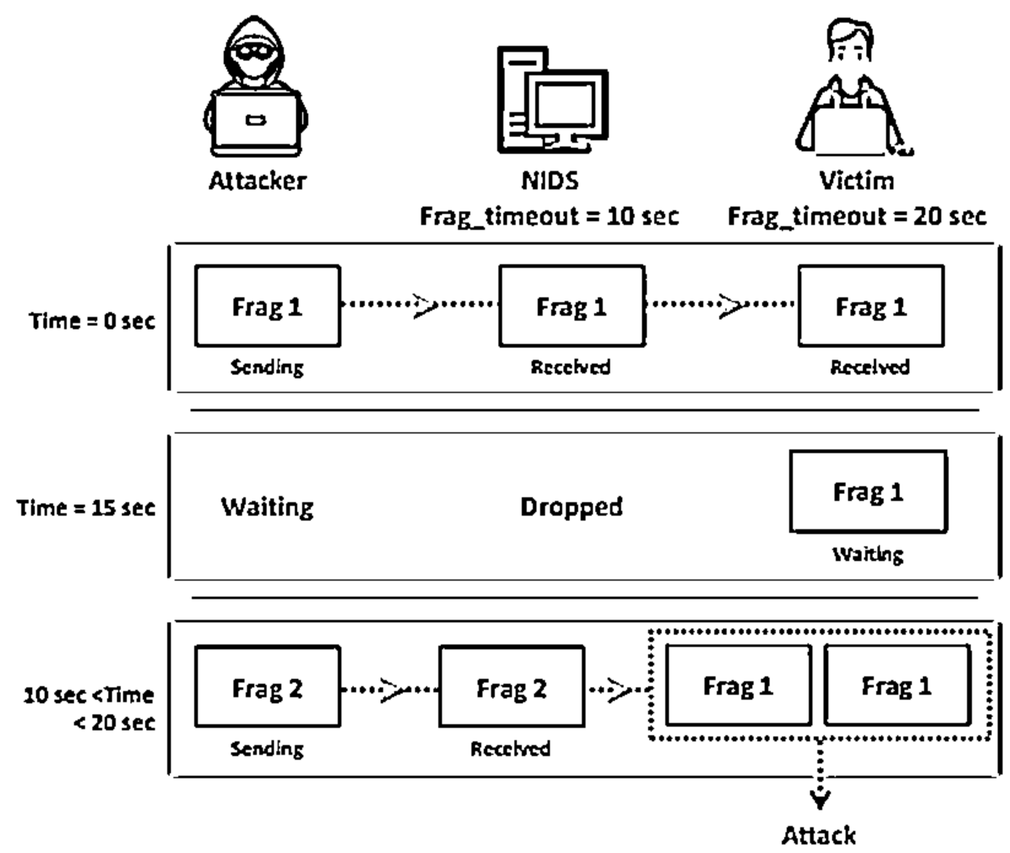
In the Unicode code space, all the code points are treated differently, but it is possible that there are multiple representations of a single character. There are also code points that alter the previous code points. Moreover, applications or OS may assign the same representation to different code points. Because of this complexity, some IDS mishandle Unicode, as Unicode allows multiple interpretations of the same characters.

For example, "\" represents 5C, C19C, and E0819C, which makes writing pattern-matching signatures very difficult. Taking advantage of this fact, attackers can convert attack strings into Unicode characters to avoid pattern and signature matching in the IDS. Attackers can also encode URLs in HTTP requests using Unicode characters to bypass HTTP-based attack detection at the IDS.

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

Fragmentation Attack

- Fragmentation can be used as an attack vector when fragmentation timeouts vary between the IDS and the host
- If the fragment reassembly timeout is 10 sec at the IDS and 20 sec at the target system, attackers will send the second fragment 15 sec after sending the first fragment
- In this scenario, the IDS will drop the fragments as the second fragment is received after its reassembly time, but the target system will reassemble the fragments
- Attackers will keep sending the fragments with 15 sec delays until all the attack payload is reassembled at the target system

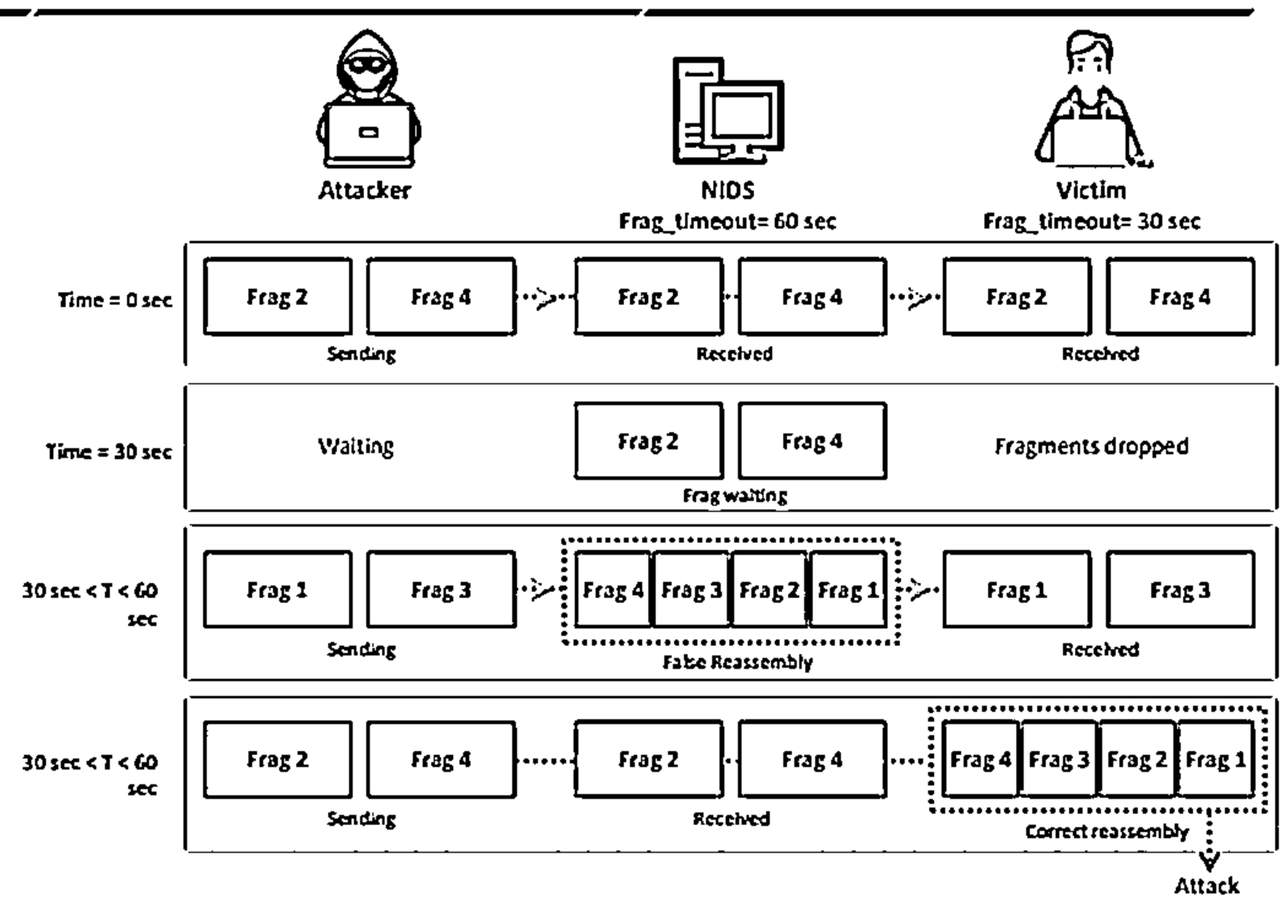


Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Fragmentation Attack (Cont'd)

A similar fragmentation attack works when the IDS timeout exceeds that of the victim

- The victim and the IDS both receive frags 2 and 4 out of the 4 fragments, both carrying a false payload
- The victim drops these two fragments after 30 sec and does not send an ICMP as frag 1 was never received
- The victim and the IDS receive frags 1 and 3 out of the 4 fragments
- The IDS reassembles the 4 received fragments, but the computed net checksum is invalid, so the packet is dropped
- The victim and the IDS receive real frags 2 and 4 out of the 4 fragments
- The victim reassembles the 4 received fragments and is attacked; the IDS times out frags 2 and 4 and drops the fragments



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

Fragmentation Attack

IP packets must follow the standard **Maximum Transmission Unit (MTU)** size while traveling across the network. If the packet size is exceeded, it will be split into multiple fragments ("fragmentation"). The IP header contains of a fragment ID, fragment offset, fragment length, fragments flags, and others besides the original data. In a network, the flow of packets is irregular; hence, systems need to keep fragments around, wait for future fragments, and then reassemble them in order. Fragmentation can be used as an attack vector when fragmentation

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

timeouts vary between the IDS and the host. Through the process of fragmenting and reassembling, attackers can send malicious packets over the network to exploit and attack systems. To avoid detection by an IDS, attackers may exploit fragmentation by using the fragment reassembly timeout, which varies from system to system.

- **Attack Scenario - 1**

  If, for example, the fragment reassembly timeout is 10 s at the IDS and 20 s at the target system, attackers will send the second fragment 15 s after sending the first fragment. In this scenario, the IDS will drop the fragment on receiving the second fragment after its reassembly timeout, but the target host will reassemble the fragments. Attackers will continue sending fragments with intervals of 15 s until the attack payload is reassembled at the target system. Thus, the victim will reassemble the fragments and receive the attack code, whereas the IDS will not detect this or generate alerts as the IDS drops the fragments.

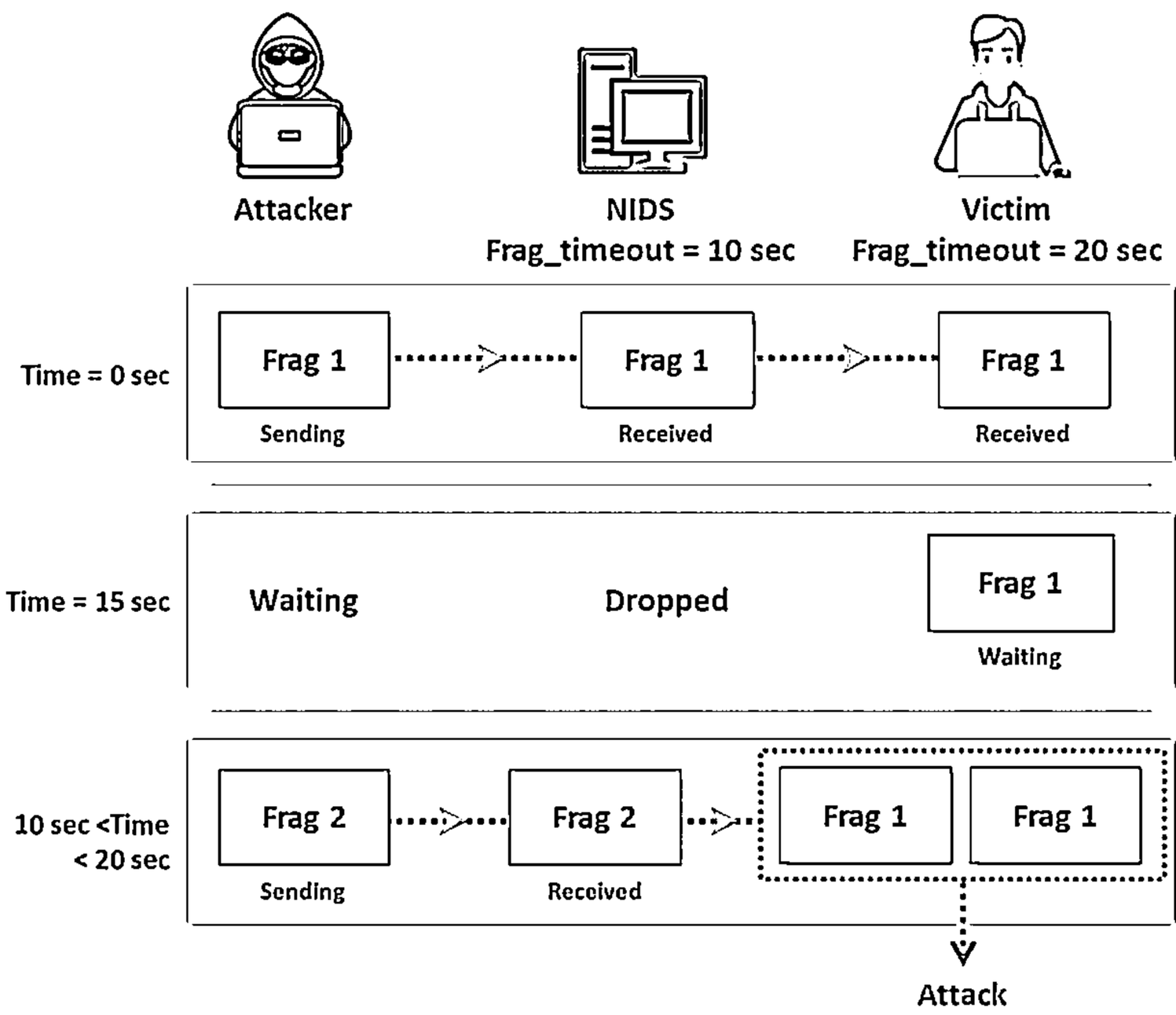


Figure 12.36: Fragmentation attack scenario-1

The figure above illustrates the discussed scenario (Attack Scenario-1). The attacker will successfully perform a fragmentation attack on a host. The attacker manipulates the order and time of the fragments and sends those fragments to the victim machine. The attack will succeed when the NIDS fragmentation reassembly timeout is less than the victim's fragmentation reassembly timeout.

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

- **Attack Scenario - 2**

  A similar fragmentation attack works when the IDS timeout exceeds that of the victim. Sometimes, the IDS fragmentation reassembly timeout is greater than that of a host. In this scenario, consider that the attacker has fragmented the attack packet into four fragments: frag-1, frag-2, frag-3, and frag-4. Here, the IDS fragmentation reassembly timeout is 60 s, and the fragmentation reassembly timeout for the host is 30 s.

  Initially, the attacker sends frag-2 and frag-4 with a false payload referred to as frag-2' and frag-4', which are received by both the IDS and the victim. The attacker waits until the fragments' reassembly timeout occurs at the victim's system. In this attack, the victim has not received frag-1, so it will drop the fragments without generating an ICMP error message. The attacker then sends a packet (frag-1, frag-3) with a legitimate payload. Now, the victim has only frag-1 and frag-3, whereas the IDS has frag-1, frag-2', frag-3, and frag-4'. Here, frag-2' and frag-4' have false payloads. With the four received fragments, the IDS will perform a TCP reassembly but drop the packet, as the computed checksum for frag-2' and frag-4' will be invalid. If the attacker now sends frag-2 and frag-4 again with a valid payload, the IDS will have only these two fragments with a valid payload, as the previous fragments will have been reassembled and dropped. The victim will have all fragments (frag-1, frag-3, frag-2, frag-4)—with valid payloads that will reassemble—and read the packet as valid.

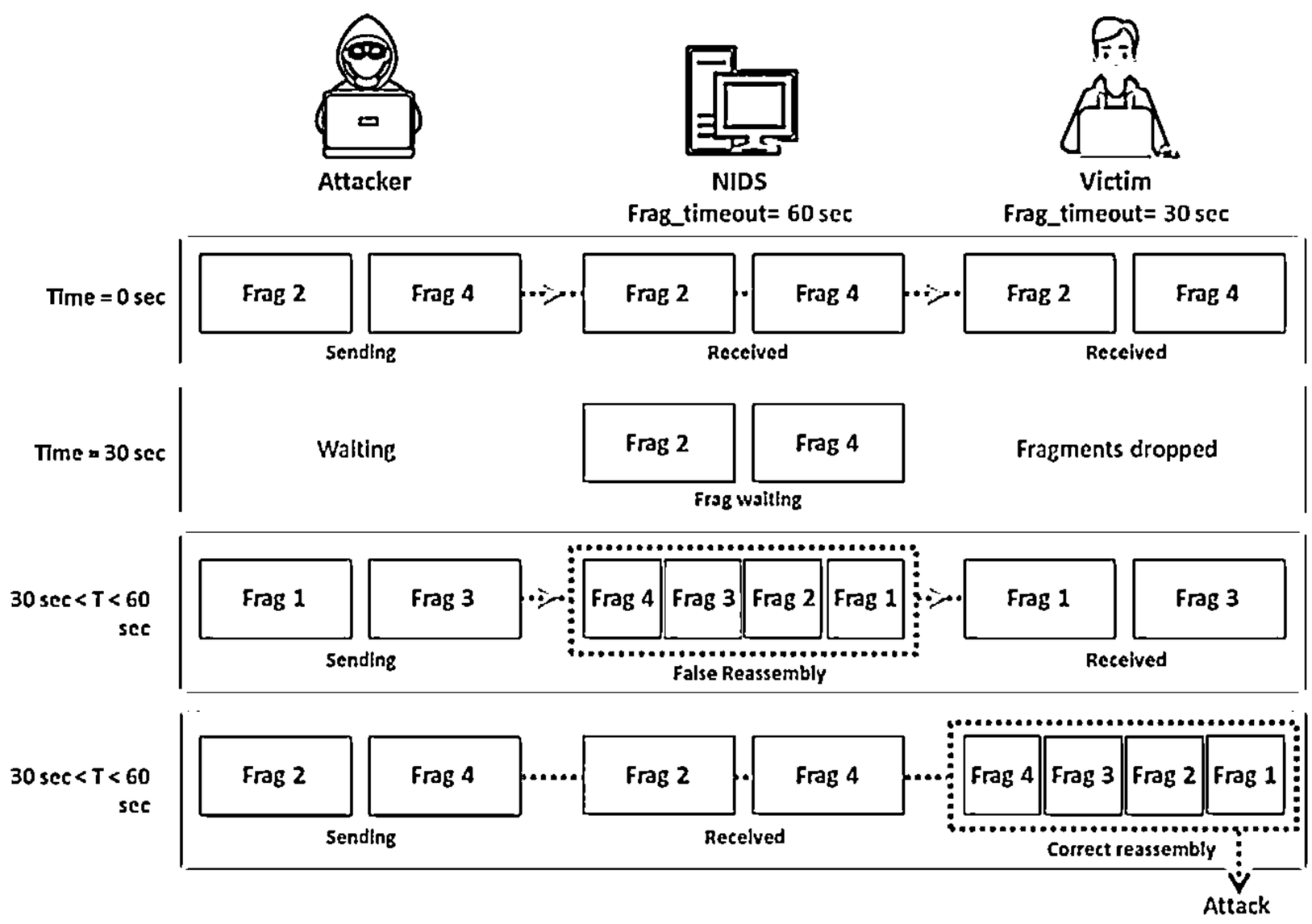


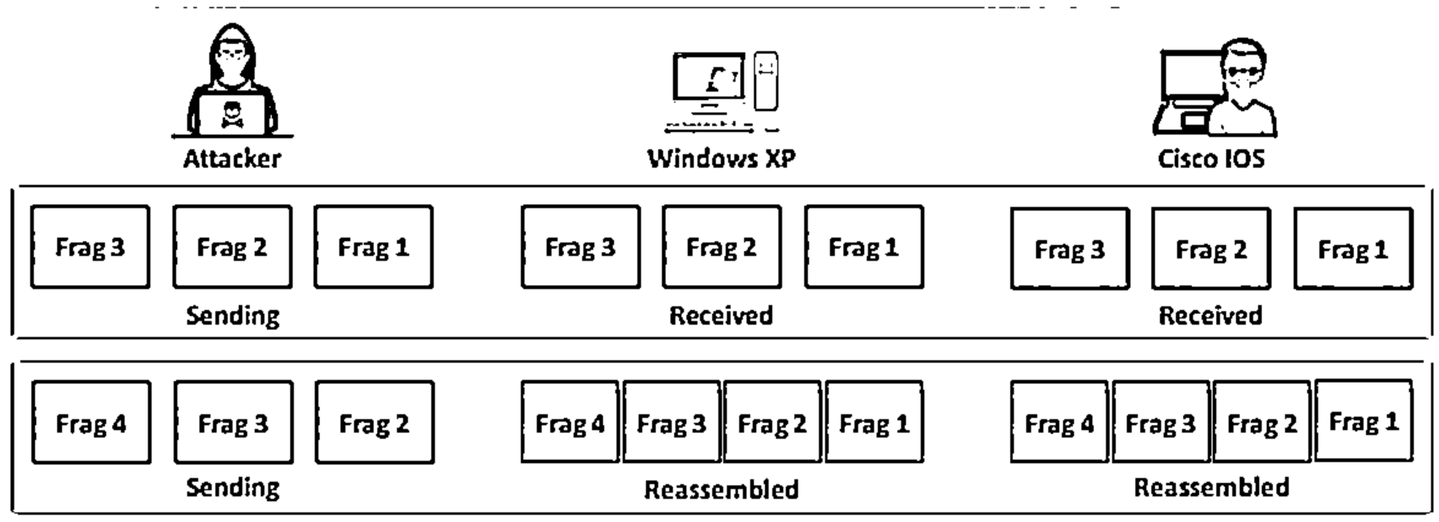
Figure 12.37: Fragmentation attack scenario-2

The figure above illustrates the discussed scenario (Attack Scenario-2). The attacker sends the malicious payload that will falsely reassemble fragments at the IDS and successfully performs a fragmentation attack on a host when the NIDS fragmentation reassembly timeout exceeds the victim's fragmentation reassembly timeout.

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

Overlapping Fragments

- An IDS evasion technique in which the attackers generate a series of tiny fragments with overlapping TCP sequence numbers
- For example, the initial fragment consists of 100 bytes of payload with a sequence number 1; the second fragment consists of 96 bytes and includes an overlapping sequence, and so on
- At the time of reassembling the packet the destination host must know how to assemble the overlapping TCP fragments
- Some OSs will take the original fragments with a given offset (e.g., Windows W2K/XP/2003) and some operating systems will take the subsequent fragments with a given offset (e.g., Cisco IOS)



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

Overlapping Fragments

Attackers use overlapping fragments to evade IDS. In this technique, attackers generate a series of tiny fragments with overlapping TCP sequence numbers. For example, the initial fragment consists of 100 bytes of payload with the sequence number of 1, the second fragment includes an overlapping sequence of 96 bytes, and so on. At the time of reassembling the packet, the destination host must know how to assemble the overlapping TCP fragments. Some OS will take the original fragments with a given offset (e.g., Windows W2K/XP/2003) and some OS will take the subsequent fragments with a given offset (e.g., Cisco IOS).

Consider a scenario in which the attacker carries out this attack by breaking the packet into four fragments, sending frag-1, frag-2, and frag-3 first, accepted by both OSs. Then, the attacker sends frag-2', frag-3', and frag-4. Here, the payloads of frag-2' and frag-3' are different from those of frag-2 and frag-3, respectively, but the fragment offset and its length, along with the other fields in the IP header, remain the same. In such a scenario, an OS such as Windows XP will reassemble frag-1, frag-2, frag-3, and frag-4, whereas an OS such as Cisco IOS will reassemble frag-1, frag-2', frag-3', and frag-4.

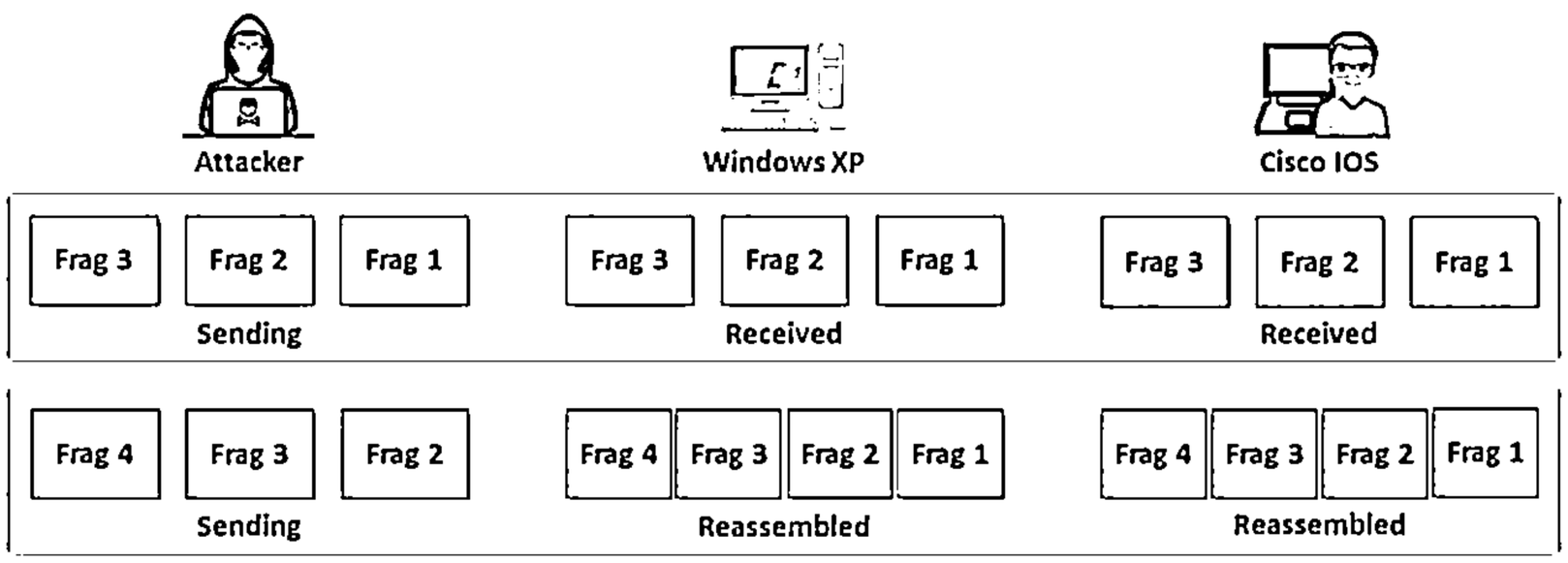


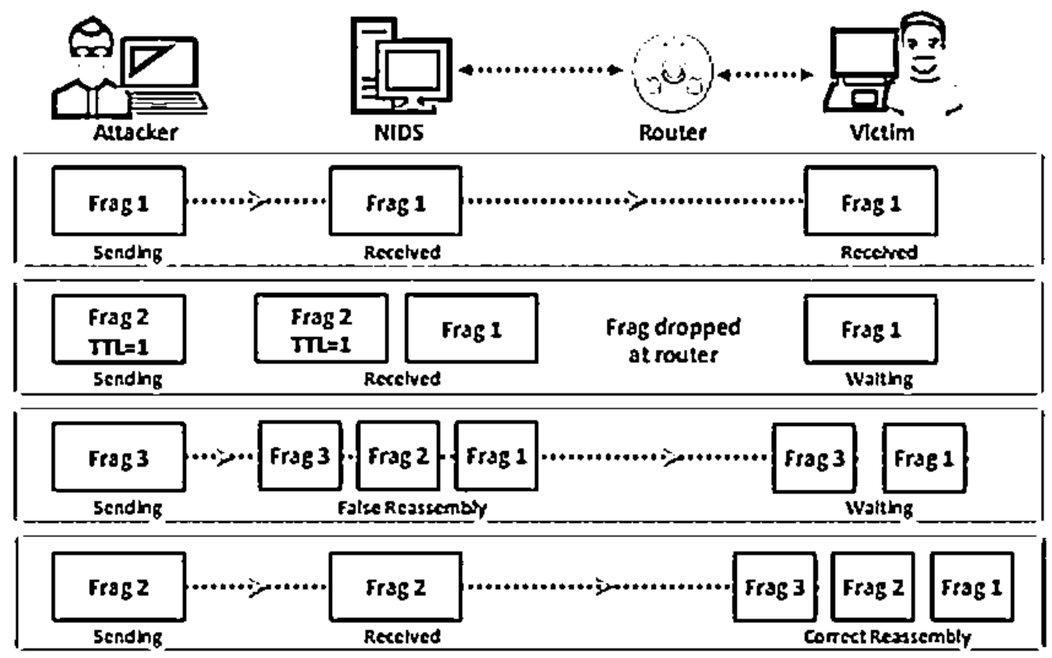
Figure 12.38: Evading IDS using Overlapping Fragments

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

Time-To-Live Attacks

- These attacks require the attacker to have a prior knowledge of the topology of the victim's network
- This information can be obtained using tools such as traceroute which give information on the number of routers between the attacker and the victim

1. The attacker breaks malicious traffic into 3 fragments
2. The attacker sends frag 1 with a high TTL, and a false frag 2 with a low TTL
3. The IDS receives both fragments, but the victim receives the first fragment only
4. The attacker sends frag 3 with a high TTL
5. The IDS reassembles the 3 fragments into a meaningless packet and drops the packet
6. The victim receives real frag 2, and suffers from an attack, while no log entry created



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

Time-To-Live Attacks

Each IP packet has a field called **Time to Live (TTL)**, which indicates how many hops the packet can take before a network node discards it. Each router along a data path decrements this value by 1. When the TTL reaches 0, the packet is dropped, and an ICMP alert notification is sent to the sender. Typically, when a host sends a packet, it sets the TTL to a high value such that it can reach its destination under normal circumstances. Different OS use different default initial values for the TTL. Therefore, attackers can guess the number of routers between them and a sending machine, and make assumptions as to what the initial TTL was, thereby guessing which OS a host is running, as a prelude to an attack. To prevent such detection, **SmartDefense** can change the TTL field of all packets (or all outgoing packets) to a given number. These attacks require the attacker to have prior knowledge of the topology of the victim's network. This information can be obtained using tools such as traceroute, which gives information on the number of routers between the attacker and the victim.

Consider a scenario in which a router is present between the IDS and a victim. Attackers need to acquire this information before launching the TTL attack by breaking the malicious data packet into three fragments. It is assumed that the attacker has prior knowledge about the topology of the target network (i.e., how many routers are there between the attacker and victim machines). The attacker fragments the packet and sends frag 1 with the TTL set to a higher value. It is then received by the victim and the IDS. Then, the attacker sends frag-2' with a false payload and a TTL value of 1, which is received by the IDS; however, the victim will not receive it, because the router discards it and the TTL value is reduced to 0. Next, the attacker sends frag-3 with a correct payload and a higher TTL value, which enables it to reach the IDS and the victim. After receiving frag-3, the IDS performs a TCP reassembly on fragments 1, 2', and 3, and the victim waits for frag-2. Finally, the attacker sends frag-2 with a valid payload. The victim, after receiving frag-2, reassembles fragments 1, 2, and 3 and gets the attack code

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

embedded in a malicious payload. Here, the IDS has only frag-2, as it has already reassembled the fragments and the stream has cleared.

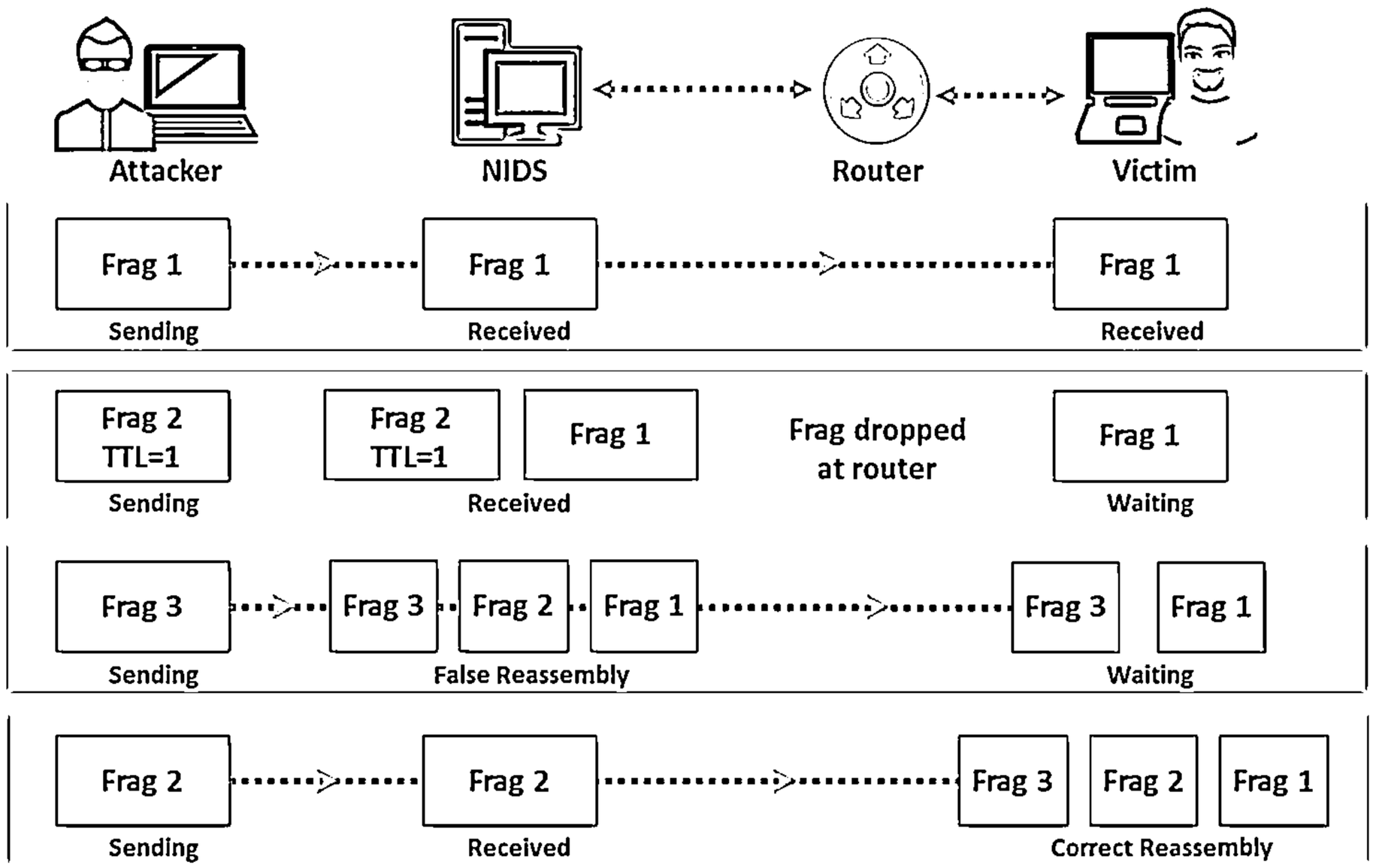


Figure 12.39: Evading IDS using Time-To-Live attack

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

Invalid RST Packets

1. TCP uses a 16-bit checksum field for error-checking of the header and data
2. The reset (RST) flag in a TCP header is used to close a TCP connection
3. In an invalid reset attack, the attackers send the RST packet to the IDS with an invalid checksum
4. The IDS stops processing the packet thinking that the TCP communication session has ended but the target system will receive the packet
5. The target system checks the RST packet's checksum and drops it
6. The attack enables the attackers to communicate with the target system while the IDS thinks that the communication has ended

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

Invalid RST Packets

The TCP uses 16-bit checksums for error checking of the header and data and to ensure that communication is reliable. It adds a checksum to every transmitted segment that is checked at the receiving end. When a checksum differs from the checksum expected by the receiving host, the TCP drops the packet at the receiver's end. The TCP also uses an RST packet to end two-way communications. Attackers can use this feature to elude detection by sending RST packets with an invalid checksum, which causes the IDS to stop processing the stream because the IDS thinks that the communication session has ended. However, the end host checks this packet, verifies the checksum value, and then drops the packet if it is invalid.

Some IDS might interpret this packet as an actual termination of the communication and stop reassembling the communication. Such instances allow attackers to continue to communicate with the end host while confusing the IDS because the end host accepts the packets that follow the RST packet with an invalid checksum value.

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

Urgency Flag

1. The urgent (URG) flag in the TCP header is used to mark the data that requires urgent processing at the receiving end
2. If the URG flag is set, the TCP protocol sets the urgent pointer field to a 16-bit offset value that points to the last byte of urgent data in the segment
3. Many IDSs do not consider the urgent pointer and process all the packets in the traffic, whereas the target system processes the urgent data only
4. This results in the IDS and the target systems having different sets of packets, which can be exploited by attackers to pass the attack traffic

Urgency Flag Attack Example

```
"When a TCP packet contains both urgent data and normal
data then 1-byte data after the urgent data is lost"
Packet 1: XYZ
Packet 2: LMN Urgency Pointer: 3
Packet 3: PQR
End result: XYZLMNQR
```

- The above example demonstrates the working of an urgency flag in a TCP packet
- According to RFC 1122, when a TCP segment consists of an urgency pointer, one byte of data after the urgent data will be lost

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

Urgency Flag

The urgency flag in the TCP marks data as urgent. TCP uses an urgency pointer that points to the beginning of urgent data within a packet. When the user sets the urgency flag, the TCP ignores all data before the urgency pointer, and the data to which the urgency pointer points is processed. If the URG flag is set, the TCP sets the Urgent Pointer field to a 16-bit offset value that points to the last byte of urgent data in the segment. Some IDS do not consider the TCP's urgency feature and process all the packets in the traffic, whereas the target system processes only the urgent data. Attackers exploit this feature to evade the IDS, as seen in other evasion techniques. Attackers can place garbage data before the urgency data. The pointer and the IDS read that data without consideration of the end host's urgency flag handling. This means that the IDS have more data than the end host processes. This results in the IDS and the target systems having different sets of packets, which can be exploited by attackers to pass the attack traffic.

Example:

```
"When a TCP packet contains both urgent data and normal data then 1-
byte data after the urgent data is lost"

Packet 1: XYZ

Packet 2: LMN Urgency Pointer: 3

Packet 3: PQR

End result: XYZLMNQR
```

The above example demonstrates the working of an urgency flag in a TCP packet. According to RFC 1122, if a TCP segment consists of an urgency pointer, then one byte of data after the urgent data will be lost.

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

Polymorphic Shellcode

1. A signature-based network intrusion detection system (NIDS) identifies an attack by matching attack signatures with incoming and outgoing data packets
2. Many IDSs identify signatures for the commonly used strings embedded in the shellcode
3. Polymorphic shellcode attacks include multiple signatures, making it difficult to detect the signature
4. Attackers encode the payload using certain techniques and then place a decoder before the payload
5. As a result of this the shellcode is completely rewritten each time it is sent, thus evading detection
6. This technique also evades the commonly used shellcode strings, thus making shellcode signatures unusable

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

Polymorphic Shellcode

A signature-based network intrusion detection system (NIDS) identifies an attack by matching attack signatures with incoming and outgoing data packets. Many IDS identify signatures for commonly used strings embedded in the shellcode. Polymorphic shellcode attacks include multiple signatures, making it difficult to detect the signature. Attackers encode the payload using some technique and then place a decoder before the payload. As a result, the shellcode is completely rewritten each time it is sent, thereby evading detection.

With polymorphic shellcodes, attackers hide their shellcode (attack code) by encrypting it with an unknown encryption algorithm and including the decryption code as part of the attack packet. To carry out polymorphic shellcode attacks, they use an existing buffer-overflow exploit and set the "return" memory address on the overflowed stack to the entrance point of the decryption code. This makes it difficult for the IDS to identify it as a shellcode. Therefore, when attackers modify/transform their attacks in this way, the NIDS cannot recognize them. This technique also evades commonly used shellcode strings, thus making shellcode signatures unusable.

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

ASCII Shellcode

1. An ASCII shellcode includes characters which are present only in the ASCII standard
2. Attackers can use an ASCII shellcode to bypass the IDS signature as the pattern matching does not work effectively with the ASCII values
3. The scope of an ASCII shellcode is limited as not all assembly instructions can be converted to ASCII values directly
4. This limitation can be overcome by using other sets of instructions for converting to ASCII values properly

The following is an example of an ASCII shellcode:

```
char shellcode[] =
"LLLLYhb0pLX5b0pLHSSPPWQPPaPWSUTBRDJfh5tDS"
"RajYX0Dka0TkafhN9fYf1Lkb0TkdjfY0Lkf0Tkgfh"
"6rfYf1Lki0tkkh95h8Y1LkmjpY0Lkq0tkrh2wnuXl"
"Dks0tkwjfX0Dkx0tkx0tkyCjnY0LkzC0TkzCCjtX0"
"DkzC0tkzCj3X0Dkz0TkzC0tkzChjG3IY1LkzCCCC0"
"tkzChpfcMX1DkzCCCC0tkzCh4pCnY1Lkz1TkzCCCC"
"fhJGfXf1Dkzf1tkzCCjHX0DkzCCCCjvY0LkzCCCjd"
"X0DkzC0TkzCjWX0Dkz0TkzCjdX0DkzCjXY0Lkz0tk"
"zMdgvvn9F1r8F55h8pG9wnuvjrNfrVx2LGkG3IDpf"
"cM2KgmnJGgbinYshdvD9d";
```

When executed, the shellcode above executes a "/bin/sh" shell. "bin" and "sh" are contained in the last few bytes of the shellcode

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

ASCII Shellcode

ASCII shellcodes contain only characters from the ASCII standard. Such shellcodes allow attackers to bypass commonly enforced character restrictions within the string input code. They also help attackers bypass IDS pattern matching signatures because they hide strings similarly to polymorphic shellcodes. The IDS pattern matching mechanism does not work efficiently with ASCII values.

Using ASCII for shellcode is very restrictive in that it limits what the shellcode can do under some circumstances, as not all assembly instructions convert directly into ASCII values. This restriction bypasses using other instructions, or a combination of instructions, which convert to ASCII character representation, serving the same purpose as those instructions that convert improperly.

An ASCII shellcode example is given below:

```
char shellcode[] =
"LLLLYhb0pLX5b0pLHSSPPWQPPaPWSUTBRDJfh5tDS"
"RajYX0Dka0TkafhN9fYf1Lkb0TkdjfY0Lkf0Tkgfh"
"6rfYf1Lki0tkkh95h8Y1LkmjpY0Lkq0tkrh2wnuXl"
"Dks0tkwjfX0Dkx0tkx0tkyCjnY0LkzC0TkzCCjtX0"
"DkzC0tkzCj3X0Dkz0TkzC0tkzChjG3IY1LkzCCCC0"
"tkzChpfcMX1DkzCCCC0tkzCh4pCnY1Lkz1TkzCCCC"
"fhJGfXf1Dkzf1tkzCCjHX0DkzCCCCjvY0LkzCCCjd"
"X0DkzC0TkzCjWX0Dkz0TkzCjdX0DkzCjXY0Lkz0tk"
"zMdgvvn9F1r8F55h8pG9wnuvjrNfrVx2LGkG3IDpf"
"cM2KgmnJGgbinYshdvD9d";
```

When executed, the shellcode above runs a "/bin/sh" shell. "bin" and "sh" are contained in the last few bytes of the shellcode.

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

Application-Layer Attacks

- Applications accessing media files (audio, video and images) compress them to a smaller size for maximizing the data transfer rate
- The IDS cannot verify the signature of the compressed file format
- This enables an attacker to exploit the vulnerabilities in compressed data
- The IDS can recognize conditions favorable for attack, but alternative forms of attack are also possible, for example, various integer values can be used to exploit integer overflow vulnerabilities
- This makes the detection of attack traffic extremely difficult at the IDS

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

Application-Layer Attacks

Media files such as images, audios, and videos can be compressed so that they can be rapidly transferred as smaller chunks. Attackers find flaws in this compressed data and perform attacks; even the IDS signatures cannot identify the attack code within data thus compressed.

Many applications that deal with such media files employ some form of compression to increase the data transfer speed. When you find a flaw in these applications, the entire attack can occur within the compressed data, and the IDS will have no way to check the compressed file format for signatures. This enables an attacker to exploit the vulnerabilities in the compressed data. Many IDS look for specific conditions that allow for an attack. However, there are times when the attack can take many different forms. For example, attackers can exploit the integer overflow vulnerabilities using several different integer values. This fact, combined with compressed data, makes signature detection extremely difficult.

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

Desynchronization

Pre-Connection SYN

- This attack is performed by sending an initial SYN before the real connection is established, but with an invalid TCP checksum
- If a SYN packet is received after the TCP control block is opened, the IDS resets the appropriate sequence number to match that of the newly received SYN packet
- Attackers send fake SYN packets with a completely invalid sequence number to desynchronize the IDS
- This stops the IDS from monitoring all legitimate and attack traffic

Post-Connection SYN

- In this technique, attackers attempt to desynchronize the IDS from the actual sequence numbers that the kernel is honoring
- Attackers send a post connection SYN packet in the data stream, which will have divergent sequence numbers
- However, the target host will ignore this SYN packet, as it references an already established connection
- The intent of this attack is to get the IDS to resynchronize its notion of the sequence numbers to the new SYN packet
- It will then ignore any data that is a legitimate part of the original stream, because it will be awaiting a different sequence number
- After successfully resynchronizing the IDS with a SYN packet, attackers send an RST packet with the new sequence number and thus close its notion of the connection

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

Desynchronization

- **Pre-Connection SYN**

  This attack is performed by sending an initial SYN before the real connection is established, but with an invalid TCP checksum. The IDS can ignore or accept subsequent SYNs in a connection. If a SYN packet is received after the TCP control block is opened, the IDS resets the appropriate sequence number to match the newly received SYN packet. Attackers send fake SYN packets with a completely invalid sequence number to desynchronize the IDS. This stops the IDS from monitoring all legitimate and attack traffic. If the IDS is smart, it does not check the TCP checksum. If the IDS checks the checksum, the attack is synchronized and a bogus sequence number is sent to the IDS before the real connection occurs.

- **Post-Connection SYN**

  In this technique, attackers attempt to desynchronize the IDS from the actual sequence numbers that the kernel is honoring. Send a post-connection SYN packet in the data stream, which will have divergent sequence numbers but otherwise meet all the necessary criteria to be accepted by the target host. However, the target host will ignore this SYN packet, as it references an already established connection. This attack intends to get the IDS to resynchronize its notion of the sequence numbers to the new SYN packet. It will then ignore any data that is a legitimate part of the original stream because it will be waiting for a different sequence number. Once you succeed in resynchronizing the IDS with a SYN packet, send an RST packet with the new sequence number and close down its notion of the connection.

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

Other Types of Evasion

Encryption

- When the attacker has already established an encrypted session with the victim, it results in the most effective evasion attack

Flooding

- The attacker sends loads of unnecessary traffic to produce noise, and if the IDS does not analyze the noise traffic well, then the true attack traffic may go undetected

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

Other Types of Evasion

- **Encryption**

  Network-based intrusion detection analyzes traffic in the network from the source to the destination. If an attacker succeeds in establishing an encrypted session with his/her target host using a secure shell (SSH), secure socket layer (SSL), or virtual private network (VPN) tunnel, the IDS will not analyze the packets going through these encrypted communications. Thus, an attacker sends malicious traffic using such secure channels, thereby evading IDS security.

- **Flooding**

  IDS use resources such as memory and processor speed to analyze the traffic going through them. To bypass IDS security, attackers flood IDS resources with noise or fake traffic to exhaust them with having to analyze flooded traffic. Once such attacks succeed, attackers send malicious traffic toward the target system behind the IDS, which offers little or no intervention. Thus, true attack traffic might go undetected.

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

Module Flow

1. IDS, IPS, Firewall, and Honeypot Concepts
2. IDS, IPS, Firewall, and Honeypot Solutions
3. Evading IDS
4. Evading Firewalls
5. IDS/Firewall Evading Tools
6. Detecting Honeypots
7. IDS/Firewall Evasion Countermeasures

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

Evading Firewalls

The previous section explained how attackers use various techniques to bypass IDS. Similarly, they can also use various tricks and techniques to bypass firewalls. This section discusses the different techniques used by attackers to bypass firewall security.

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

Firewall Evasion Techniques

1 Firewalking	6 Using an IP Address in Place of a URL	11 SSH and DNS Tunneling
2 Banner Grabbing	7 Using a Proxy Server	12 Through External Systems
3 IP Address Spoofing	8 ICMP Tunneling	13 Through MITM Attack
4 Source Routing	9 ACK Tunneling	14 Through Content
5 Tiny Fragments	10 HTTP Tunneling	15 Through XSS Attack

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

Firewall Evasion Techniques

Bypassing a firewall is a technique whereby an attacker manipulates the attack sequence to avoid being detected by the underlying security firewall. The firewall operates on a predefined set of rules, and with thorough knowledge and skill, an attacker can bypass the firewall by employing various firewall bypassing techniques. Using these techniques, the attacker tricks the firewall into not filtering the malicious traffic generated by the attacker.

Some firewall bypassing techniques are as follows:

- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Using an IP Address in Place of a URL
- Using Anonymous Website Surfing Sites
- Using a Proxy Server
- ICMP Tunneling
- ACK Tunneling
- HTTP Tunneling
- SSH Tunneling
- DNS Tunneling
- Through External Systems
- Through MITM Attack
- Through Content
- Through XSS Attack

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

Firewall Identification

Port Scanning

- Port scanning is used to identify open ports and services running on these ports
- Open ports can be further probed to identify the version of services, which helps in finding vulnerabilities in these services
- Some firewalls will uniquely identify themselves in response to simple port scans
- For example: Check Point's FireWall-1 listens on TCP ports 256, 257, 258, and 259. Microsoft's Proxy Server listens on TCP ports 1080 and 1745

Firewalking

- Firewalking is a technique that uses TTL values to determine gateway ACL filters and it maps networks by analyzing the IP packet responses
- Attackers send a TCP or UDP packet to the targeted firewall with a TTL set to one hop greater than that of the firewall
- If the packet makes it through the gateway, it is forwarded to the next hop where the TTL equals one and elicits an ICMP "TTL exceeded in transit" to be returned, as the original packet is discarded
- This method helps locate a firewall. Additional probing permits fingerprinting and identification of vulnerabilities

Banner Grabbing

- Banners are service announcements provided by services in response to connection requests, and often carry vendor version information
- Banner grabbing is a simple method of fingerprinting that helps in detecting the vendor of a firewall, and the firmware's version
- The three main services which send out banners are FTP, telnet, and web servers
- An example of SMTP banner grabbing is: telnet mail.targetcompany.org 25

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

Firewall Identification

- **Port Scanning**

  Ports are points from which computers send or accept information from network resources. Port scanning is used to identify open ports and the services running on these ports. Finding open ports is an attacker's first step toward gaining access to the target system. To do so, the attacker systematically scans the target's ports to identify the versions of services, which helps in finding vulnerabilities in these services. Attackers sometimes use automated port-scanning utilities to do so, many of which are easily available.

  How Attackers Scan Ports

  Port scanning consists of sending messages to each port, one at a time. The kind of response received indicates whether the system is using the port, leaving it exposed to the discovery of weaknesses. Some firewalls will uniquely identify themselves using simple port scans. For example, Check Point's FireWall-1 listens on TCP ports 256, 257, 258, and 259, and Microsoft's Proxy Server usually listens on TCP ports 1080 and 1745.

- **Firewalking**

  Firewalking is a method of collecting information about remote networks behind firewalls. It is a technique that uses TTL values to determine gateway ACL filters and map networks by analyzing the IP packet response. It probes ACLs on packet filtering routers/firewalls using the same method as tracerouting. Firewalking involves sending TCP or UDP packets into the firewall where the TTL value is one hop greater than the targeted firewall. If the packet makes it through the gateway, the system forwards it to the next hop, where the TTL equals one, and prompts an ICMP error message at the

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

point of rejection with a "TTL exceeded in transit" message. This method helps locate a firewall; additional probing facilitates fingerprinting and identification of vulnerabilities.

Firewalk is a well-known application used for firewalking. It has two phases: a network discovery phase and a scanning phase. It comes with various open-source Linux distributions. Nmap has a firewalk script that can be used to perform firewalking.

- **Banner Grabbing**

  Banners are service announcements provided by services in response to connection requests, and they often carry vendor version information. Banner grabbing is a simple method of fingerprinting that helps in detecting the vendor of a firewall and the firmware version. It identifies the service running on the system. Attackers use banner grabbing to fingerprint services and thus discover the services running on firewalls. The three primary services that send out banners are FTP, Telnet, and web servers.

  A firewall does not block banner grabbing because the connection between the attacker's system and the target system appears legitimate. An example of SMTP banner grabbing is `telnet mail.targetcompany.org 25`.

  The syntax is "`<service name > <service running > <port number>`"

  Banner grabbing is used for specifying banners and application information. For example, when the user opens a telnet connection to a known port on the target server and presses Enter a few times, if required, it displays the following result:

```
C:\>telnet www.corleone.com 80
HTTP/1.0 400 Bad Request
Server: Netscape - Commerce/1.12
```

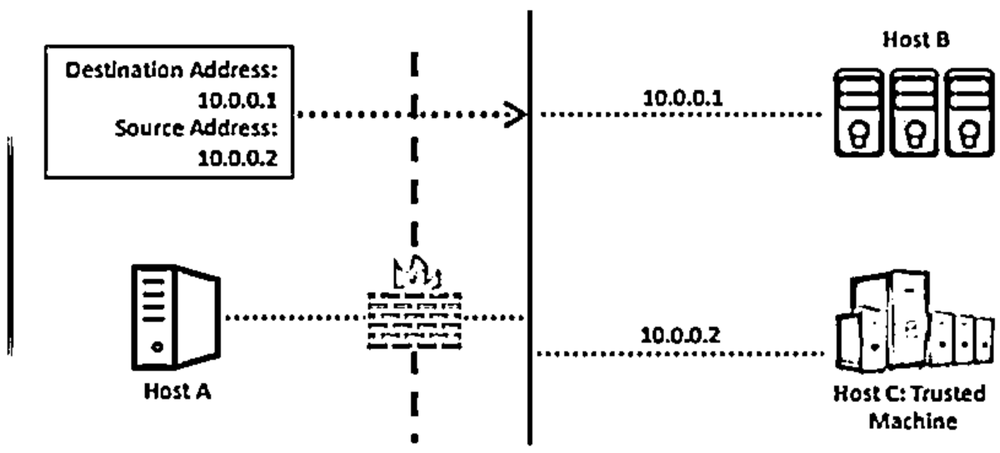
  This system works with many other common applications that respond to a set port. The information generated through banner grabbing can boost the attacker's efforts to further compromise the system. With information about the version and the vendor of the web server, the attacker can further focus on employing platform-specific exploit techniques. Services on ports such as FTP, Telnet, and web servers should not remain open, as they are vulnerable to banner grabbing.

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

IP Address Spoofing

- IP address spoofing is a hijacking technique in which an attacker masquerades as a trusted host to conceal his/her identity. It can be used to spoof a website, hijack browsers, or gain unauthorized access to a network
- Attackers modify the addressing information in the IP packet header and the source address bits field in order to bypass the firewall

- For example, let's consider three hosts: A, B and C
- Host C is a trusted machine of host B
- Host A masquerades as host C by modifying the IP address of the malicious packets that he intends to send to host B
- When the packets are received, host B thinks that they are from host C, but they are in fact from host A



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

IP Address Spoofing

Most firewalls filter packets based on the source IP address. These firewalls examine the source IP address and determine whether the packet is coming from a legitimate source or an illegitimate source. The IDS filters packets from illegitimate sources. Attackers use the IP spoofing technique to bypass such firewalls.

IP address spoofing is a hijacking technique in which an attacker masquerades as a trusted host to conceal his identity, spoof a website, hijack browsers, or gain unauthorized access to a network. In IP spoofing, the attacker creates IP packets by using a forged IP address and gains access to the system or network without authorization. Attackers modify the addressing information in the IP packet header and the source address bits field to bypass the firewall. The attacker spoofs the message; therefore, the destination host thinks that it has come from a reliable source. Thus, the attacker succeeds in impersonating others with the help of IP spoofing. Hackers use this technique to avoid detection during spamming and various other activities.

For example, let us consider three hosts: A, B, and C. Host C is a trusted machine of host B. Host A masquerades as host C by modifying the IP address of the malicious packets that it intends to send to host B. When the packets are received, host B thinks that they are from host C, but they are actually from host A.

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

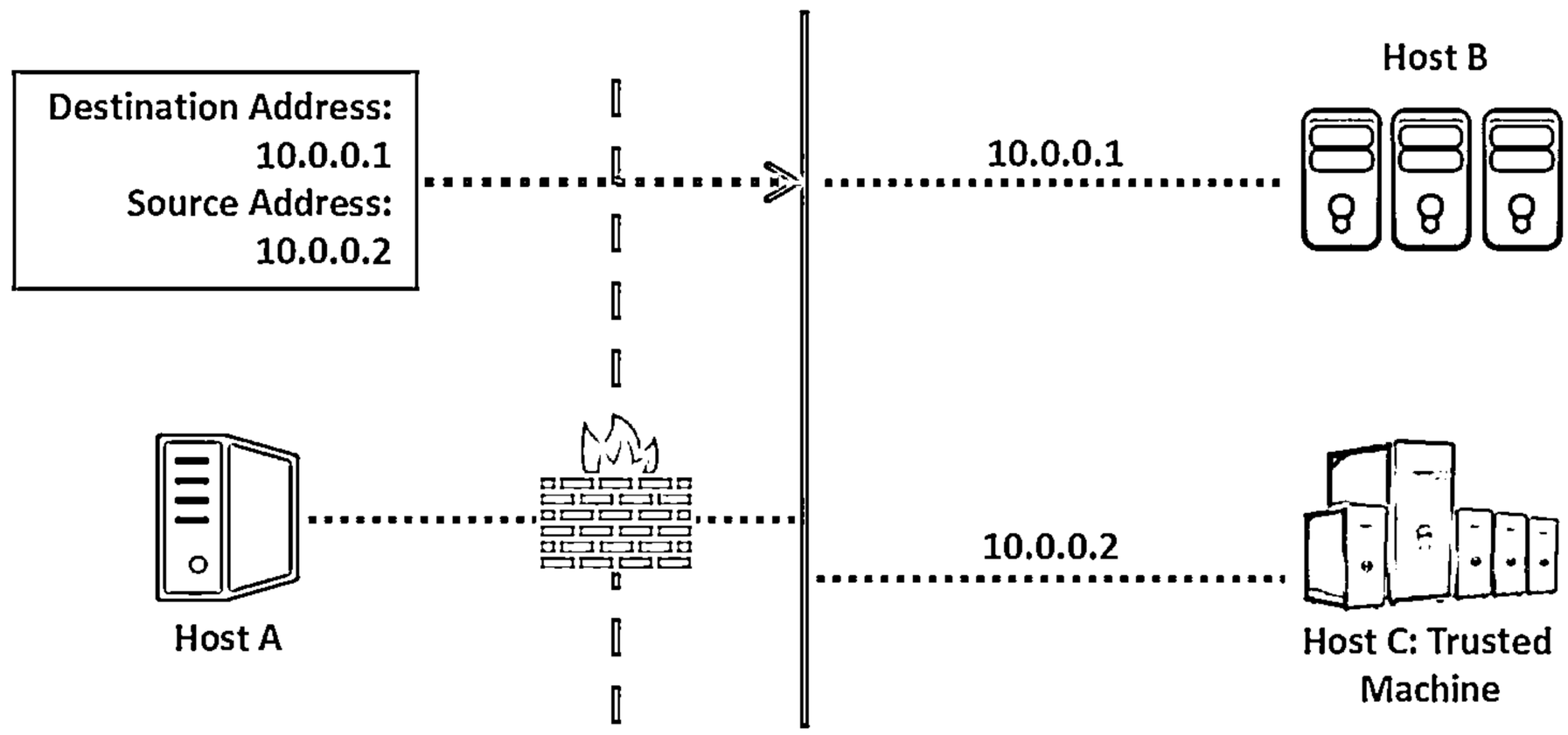


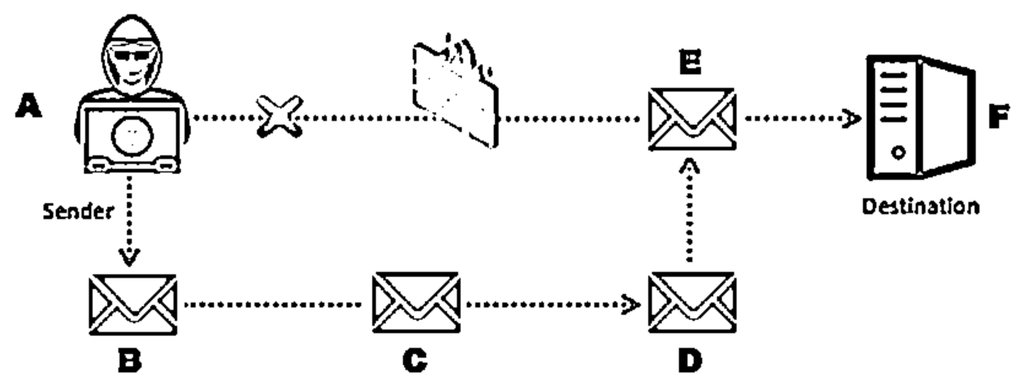
Figure 12.40: Evading Firewall using IP Address Spoofing

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

Source Routing

- Source routing allows the sender of a packet to partially or completely specify the route the packet takes through the network
- As the packet travels through the nodes in the network, each router examines the destination IP address and chooses the next hop to direct the packet to the destination
- In source routing, the sender makes some or all of these decisions on the router

The figure shows source routing, where the originator dictates the eventual route of the traffic



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

Source Routing

Using this technique, the sender of the packet designates the route (partially or entirely) that a packet should take through the network such that the designated route should bypass the firewall node. Thus, the attacker can evade firewall restrictions.

When these packets travel through the network nodes, each router examines the destination IP address and chooses the next hop to direct the packet to the destination. In source routing, the sender makes some or all of these decisions on the router.

Source routing is categorized into two approaches: loose source routing and strict source routing. In loose source routing, the sender specifies one or more stages that the packet must go through, whereas in strict source routing, the sender specifies the exact route the packet must go through.

The figure below shows source routing, where the originator dictates the eventual route of the traffic.

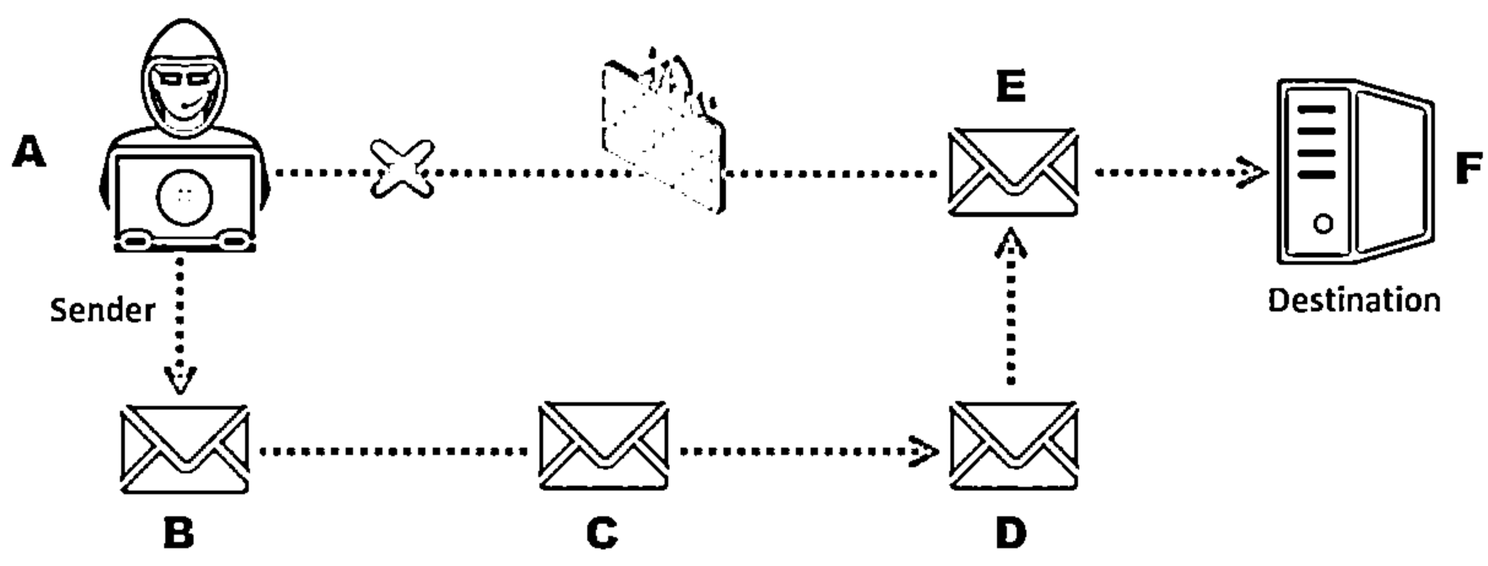


Figure 12.41: Evading Firewall using Source Routing

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

Tiny Fragments

- Attackers create tiny fragments of outgoing packets forcing some of the TCP packet's header information into the next fragment
- The IDS filter rules that specify patterns will not match with the fragmented packets due to broken header information
- The attack will succeed if the filtering router examines only the first fragment and allows all the other fragments to pass through
- This attack is used to avoid user defined filtering rules and works when the firewall checks only for the TCP header information

IP-3ar0JI0B0K			MK=1, Fragment Offset=0					
Source Port				Destination Port				
Sequence Number								
Acknowledgement Sequence Number								
Data Offset	Reserved	-	ACK	-	-	-	-	Window
Checksum								Urgent Pointer=0
0								

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

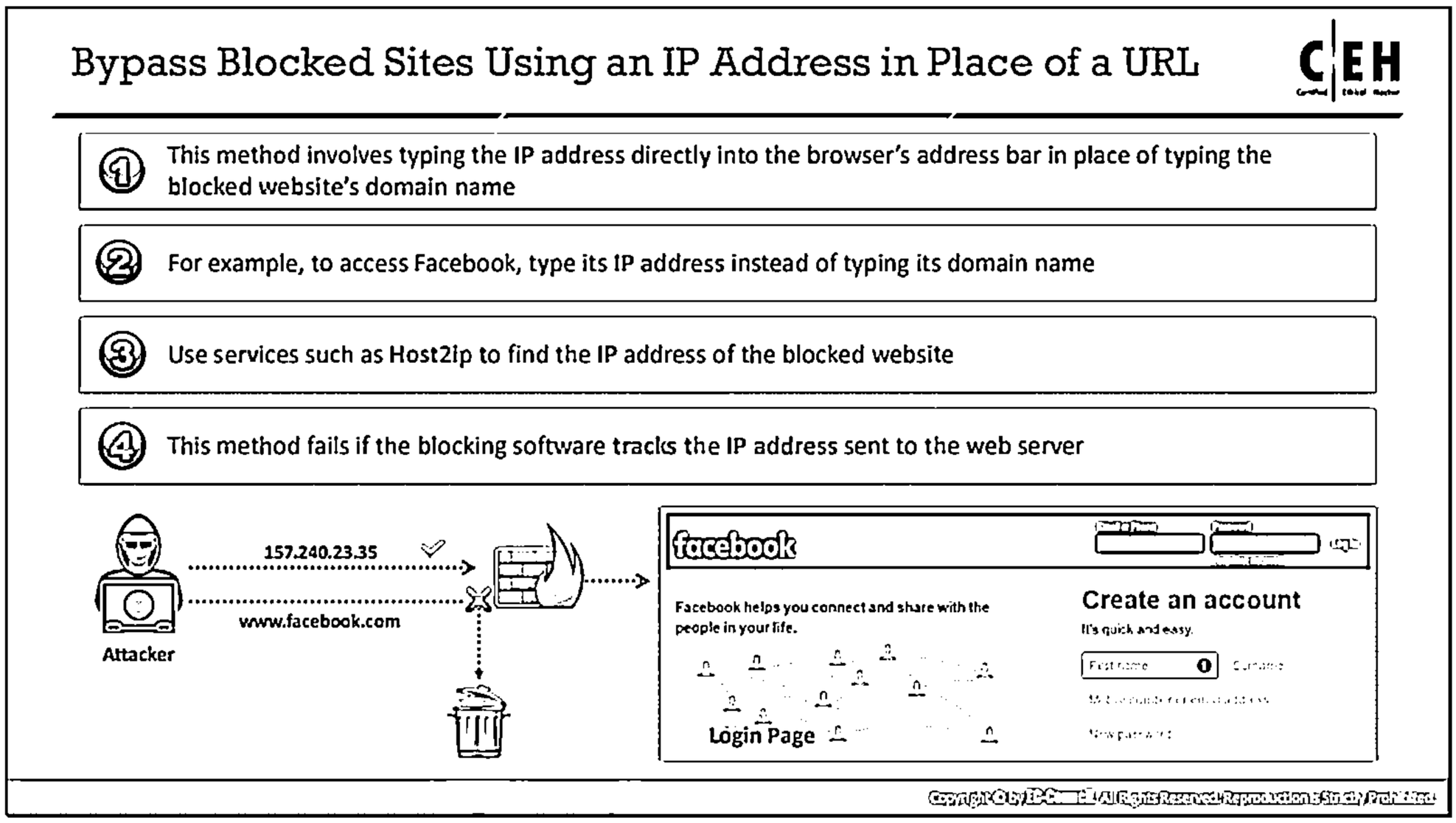
Tiny Fragments

Attackers create tiny fragments of outgoing packets, forcing some of the TCP packet's header information into the next fragment. The IDS filter rules that specify patterns will not match with the fragmented packets owing to the broken header information. The attack will succeed if the filtering router examines only the first fragment and allows all the other fragments to pass through. This attack is used to avoid user-defined filtering rules and works when the firewall checks only for the TCP header information.

IP-3ar0JI0B0K			MK=1, Fragment Offset=0					
Source Port				Destination Port				
Sequence Number								
Acknowledgement Sequence Number								
Data Offset	Reserved	-	ACK	-	-	-	-	Window
Checksum								Urgent Pointer=0
0								

Figure 12.42: TCP header format

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



Bypass Blocked Sites Using an IP Address in Place of a URL

This method involves typing a blocked website's IP address directly in the browser's address bar instead of the domain name. For example, to access Facebook, type its IP address instead of typing its domain name. Use services such as Host2ip to find the IP address of the blocked website. This method fails if the blocking software tracks the IP address sent to the web server.

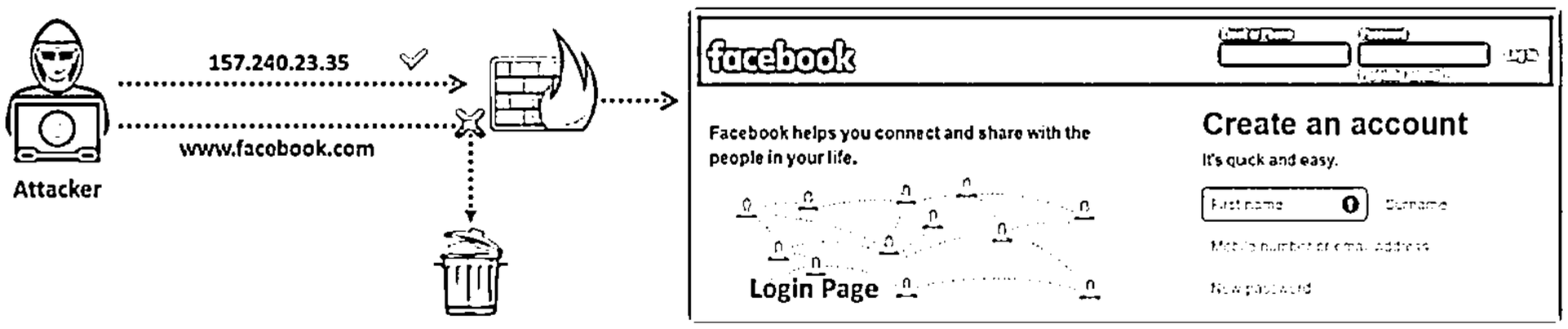


Figure 12.43: Bypass blocked sites using the IP address instead of the URL

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

Bypass Blocked Sites Using Anonymous Website Surfing Sites

- There are many online anonymizer services that enable anonymous surfing on the Internet
- Some websites provide options to encrypt the URL's of the websites
- These services hide the actual IP address of the surfer and enable bypassing the IP-based firewall filter rules

Anonymizers

1 *https://www.anonymizer.com*	6 *http://www.guardster.com*
2 *https://www.free-proxy.com*	7 *http://anonymouse.org*
3 *https://anonymous-proxy-servers.net*	8 *https://www.boomproxy.com*
4 *https://zendproxy.com*	9 *http://ww7.onype.com*
5 *https://proxify.com*	10 *https://www.spysurfing.com*

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

Bypass Blocked Sites Using Anonymous Website Surfing Sites

Anonymous web-surfing sites help to browse the Internet anonymously and unblock blocked sites (i.e., evade firewall restrictions). By using these sites, you can surf restricted sites anonymously without revealing your IP address. Various anonymous web-surfing sites available, some of which provide options to encrypt website URLs.

The following is the list of proxy servers that can help you to access blocked websites. These proxy websites will hide the actual IP address and show another IP address, which could prevent the website from being blocked, thereby allowing access.

Anonymizer

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

Anonymizer's VPN routes all the traffic through an encrypted tunnel directly from your laptop to secure and harden servers and networks. It then masks the real IP address to ensure complete and continuous anonymity for all online activities.

Some online anonymizers include:

- *https://www.free-proxy.com*
- *https://anonymous-proxy-servers.net*
- *https://zendproxy.com*
- *https://proxify.com*
- *http://www.guardster.com*
- *http://anonymouse.org*
- *https://www.boomproxy.com*
- *http://ww7.anype.com*
- *https://www.spysurfing.com*

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

Bypass a Firewall Using a Proxy Server

1. Find an appropriate proxy server
2. On the Tools menu of any Internet browser, go to "Proxy Settings" and in the Internet Properties dialog box under the Connections tab, click "LAN settings"
3. Under LAN Settings, click on the "Use a proxy server for your LAN" check box
4. In the Address box, type the IP address of the proxy server
5. In the Port box, type the port number that is used by the proxy server for client connections (by default, 8080)
6. Click to select "Bypass proxy server for local addresses" check box if you do not want the proxy server computer to be used when connected to a computer on the local network
7. Click OK to close the LAN Settings dialog box
8. Click OK again to close the Internet Properties dialog box

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

Bypass a Firewall Using a Proxy Server

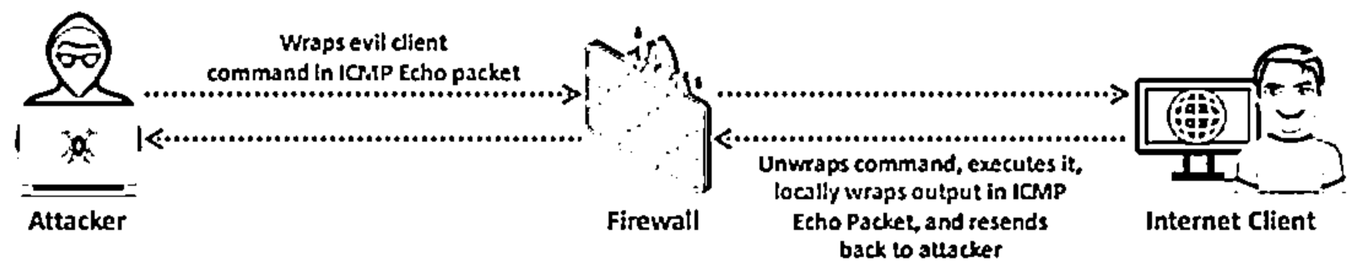
Steps to be followed to bypass a firewall using a proxy server:

1. Find an appropriate proxy server
2. In the Tools menu of any Internet browser, go to "**Proxy Settings,**" and in the **Internet Properties** dialog box under **Connections** tab, click "**LAN settings**"
3. Under **LAN Settings**, click on the "**Use a proxy server for your LAN**" checkbox
4. In the **Address** box, type the **IP address** of the proxy server
5. In the **Port** box, type the **port number** that is used by the proxy server for client connections (by default, 8080)
6. Click to select the "**Bypass proxy server for local addresses**" checkbox if you do not want the proxy server computer to be used when connected to a computer on the local network
7. Click **OK** to close the **LAN Settings** dialog box
8. Click **OK** again to close the **Internet Properties** dialog box

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

Bypassing Firewalls through the ICMP Tunneling Method

- ICMP tunneling allows tunneling a backdoor shell in the data portion of ICMP Echo packets
- RFC 792, which delineates ICMP operations, does not define what should go in the data portion
- The payload portion is arbitrary and is not examined by most of the firewalls, thus any data can be inserted in the payload portion of the ICMP packet, including a backdoor application
- Some administrators keep ICMP open on their firewall because it is useful for tools like ping and traceroute
- Assuming that ICMP is allowed through a firewall, use Loki ICMP tunneling (*https://tools.cisco.com*) to execute commands of choice by tunneling them inside the payload of the ICMP echo packets



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

Bypassing Firewalls through the ICMP Tunneling Method

The ICMP protocol is used to send an error message to the client. As it is a required service for network communication, users often enable this service on their networks. Moreover, it does not entail a significant threat from the security perspective. The attacker takes advantage of the enabled ICMP protocol on the network and performs ICMP tunneling to send his/her malicious data into the target network. The ICMP tunnel provides attackers with full access to target networks.

It allows tunneling of a backdoor shell in the data portion of ICMP Echo packets. RFC 792, which delineates ICMP operation, does not define what should go in the data portion. The payload portion is arbitrary and is not examined by most firewalls. Thus, any data can be inserted in the payload portion of the ICMP packet, including a backdoor application. Some administrators keep ICMP open on their firewall because it is useful for tools such as ping and traceroute. Assuming that ICMP is allowed through a firewall, use Loki ICMP tunneling (*https://tools.cisco.com*) to execute commands of choice by tunneling them inside the payload of ICMP echo packets.

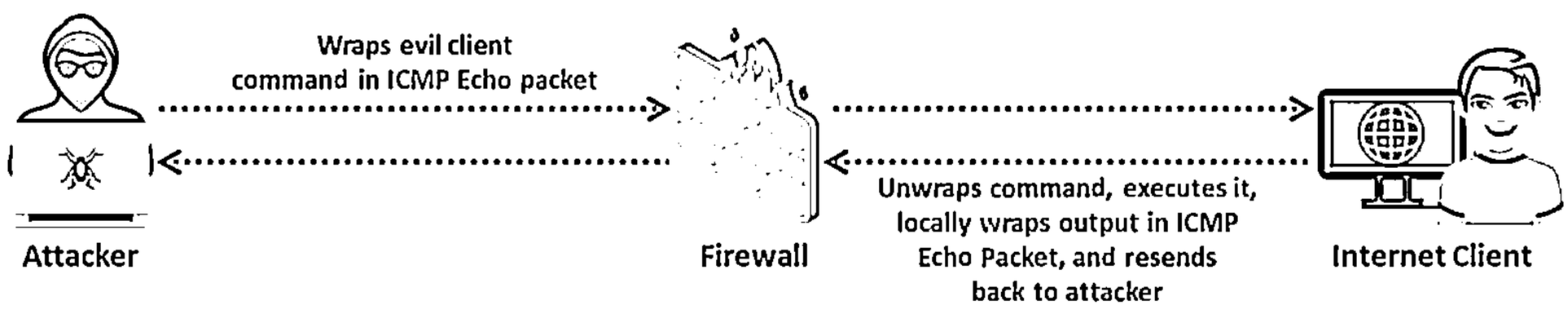
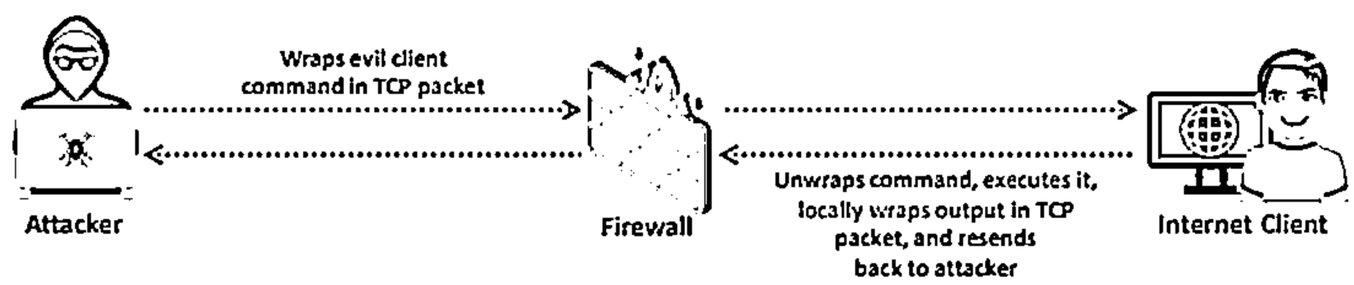


Figure 12.44: Bypassing firewall through ICMP tunneling

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

Bypassing Firewalls through the ACK Tunneling Method

- ACK tunneling allows tunneling a backdoor application with TCP packets with the ACK bit set
- The ACK bit is used to acknowledge the receipt of a packet
- Some firewalls do not check packets with the ACK bit set because ACK bits are supposed to be used in response to legitimate traffic
- Tools such as AckCmd (*http://ntsecurity.nu*) can be used to implement ACK tunneling



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

Bypassing Firewalls through the ACK Tunneling method

Ordinary packet filtering firewalls define their rule sets based on the SYN packet when TCP level communication is to be established. This is because such a firewall assumes that only the SYN packet is coming from the client and is thus likely to contain malicious code in the SYN packet. These firewalls ignore the possibility that the attacker can also inject malicious code in the ACK packet. As ACK packets are sent after establishing a session, ACK traffic is considered legitimate. In addition, the filtering of ACK packets is ignored to reduce the workload of firewalls, as there can be many ACK packets for one SYN packet. ACK tunneling allows tunneling of a backdoor application with TCP packets with the ACK bit set. The ACK bit acknowledges the receipt of a packet. As stated earlier, some firewalls do not check packets with the ACK bit set, because ACK bits are supposed to be used in response to legitimate traffic that has already been allowed to pass through. Attackers exploit this fact in ACK tunneling. Tools such as **AckCmd** (*http://ntsecurity.nu*) use ACK tunneling.

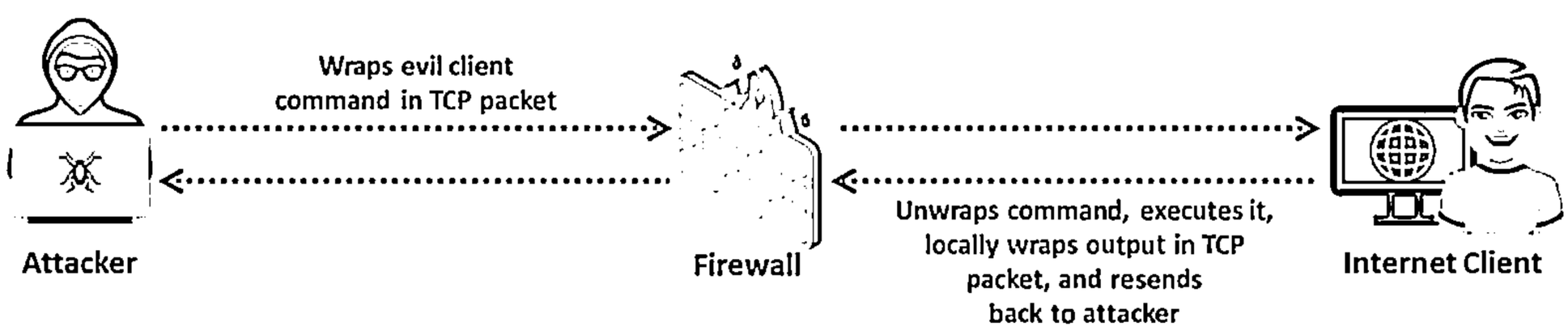
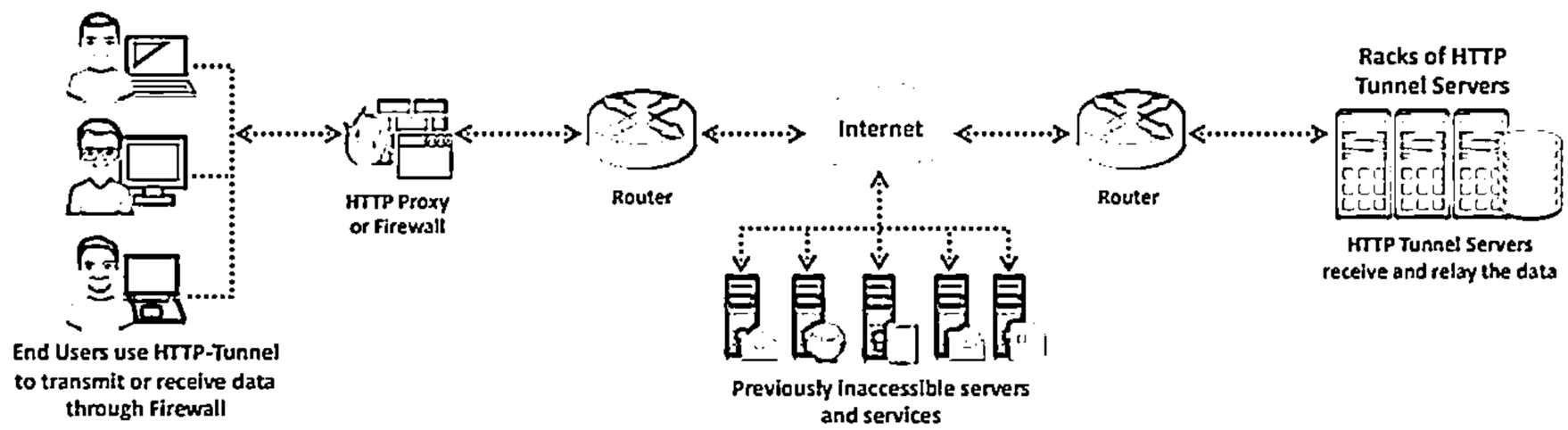


Figure 12.45: Bypassing firewall through ACK tunneling

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

Bypassing Firewalls through the HTTP Tunneling Method

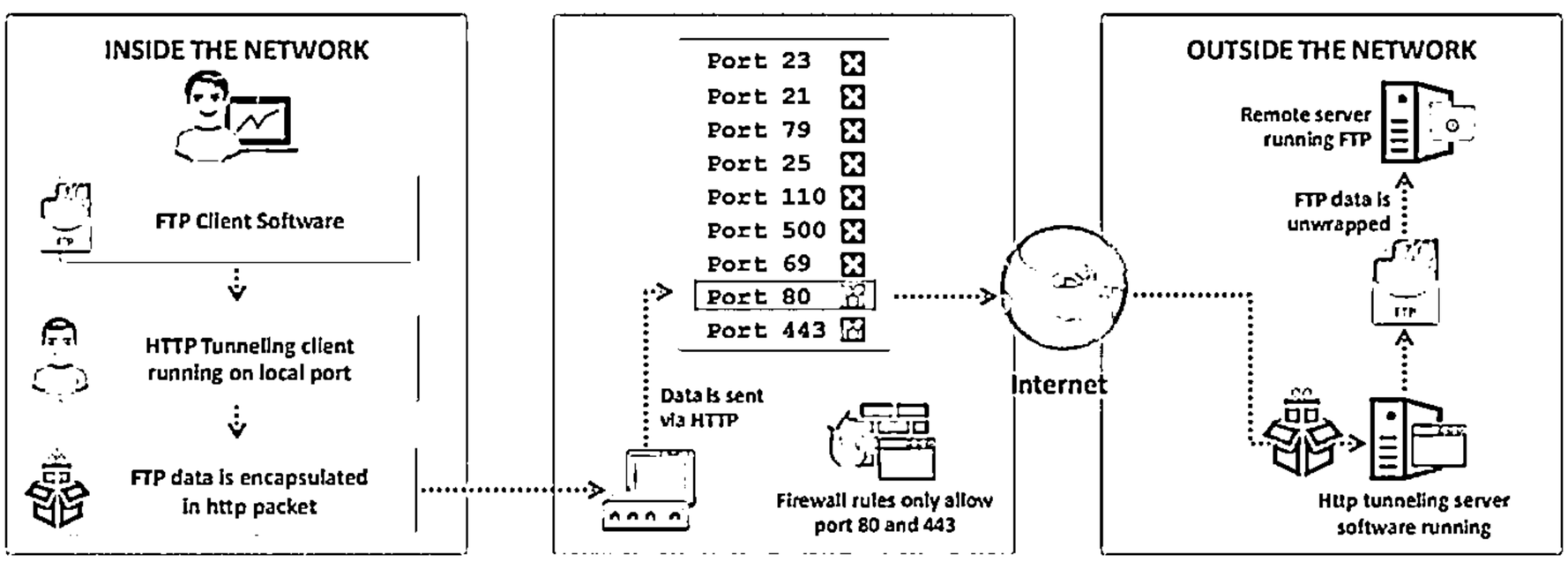
1. HTTP Tunneling technology allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls
2. This method can be implemented if the target company has a public web server, with port 80 used for HTTP traffic, that is unfiltered on its firewall
3. Encapsulates data inside HTTP traffic (port 80)



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

Why do I Need HTTP Tunneling?

- For instance, consider that an organization's firewalls restrict users from accessing all ports except 80 and 443, and a user may want to use FTP
- HTTP tunneling will enable the use of FTP via the HTTP protocol



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

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

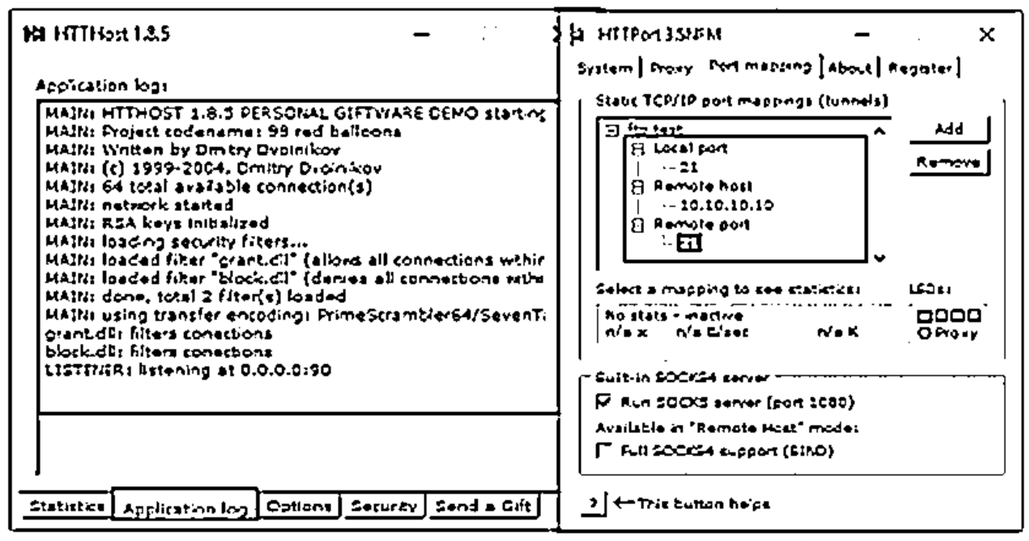
HTTP Tunneling Tools

HTTPort and HTTHost

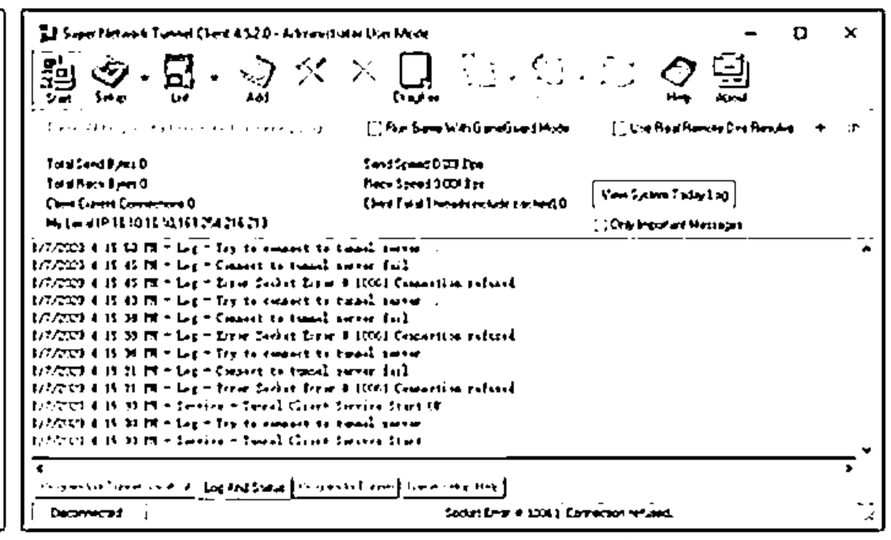
- HTTPort allows you to bypass your HTTP proxy, which is blocking you from the Internet
- It allows you to use various Internet software from behind the proxy, such as e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, or IRC

Super Network Tunnel

- A two-way http tunnel software connecting two computers
- It works like VPN tunneling but uses HTTP protocol to establish a connection



https://www.targeted.org



http://www.networktunnel.net

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

Bypassing Firewalls through the HTTP Tunneling Method

HTTP tunneling allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls. This method can be implemented if the target company has a public web server in which port 80 is used for HTTP traffic that is unfiltered by its firewall. The attacker encapsulates data inside HTTP traffic (via port 80). Many firewalls do not examine the payload of an HTTP packet to confirm that it is legitimate. Thus, it is possible to tunnel traffic via TCP port 80.

Tools such as **HTTPTunnel** (*http://http-tunnel.sourceforge.net*) use this technique of tunneling traffic across TCP port 80. HTTPTunnel is a client/server application, the client application is htc, and the server is hts. Upload the server to the target system and redirect it through TCP port 80.

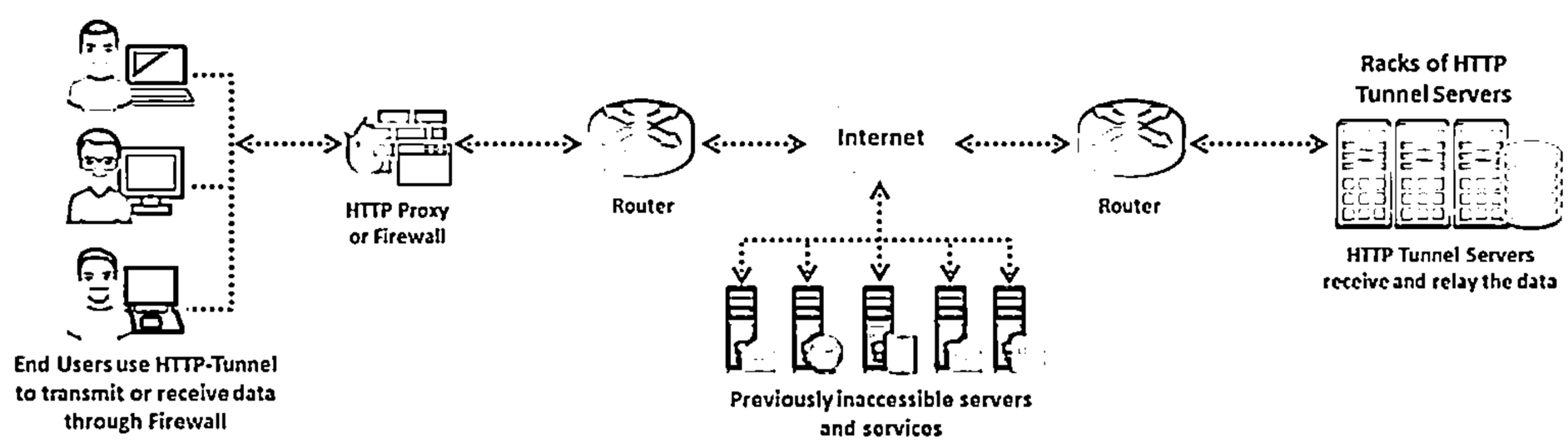


Figure 12.46: Bypassing firewall through HTTP tunneling

Why do I Need HTTP Tunneling?

HTTP tunneling is used in scenarios in which network users are granted restricted connectivity through a firewall or proxy; in such conditions, some applications may also lack native communications support.

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

These restrictions include:

- Blocking of TCP/IP ports, traffic initiated from outside the network, and network protocols except for a few commonly used protocols, etc.
- Surfing blocked websites
- Posting in forums anonymously by hiding the IP address
- Using an application such as chatting through ICQ or IRC, instant messengers, games, browsers, etc.
- Sharing of confidential resources over HTTP securely
- Downloading files with filtered extensions and/or with malicious code

For instance, consider that organization firewalls restrict users to access all ports except 80 and 443, and a user may want to use FTP. HTTP tunneling enables FTP use via the HTTP protocol. The HTTP tunnel creates a bidirectional virtual data connection tunneled in HTTP traffic. It works with the help of FTP client software to perform protocol encapsulation by enclosing data packets of one protocol such as SOAP or JRMP within HTTP packets on, e.g., local port 80. These packets are sent through the firewall or proxy server as normal Internet traffic, which is then directed to the HTTP tunneling server software located outside the network. Upon receiving the packets, this server unwraps the FTP data and redirects the packet to the remote FTP server.

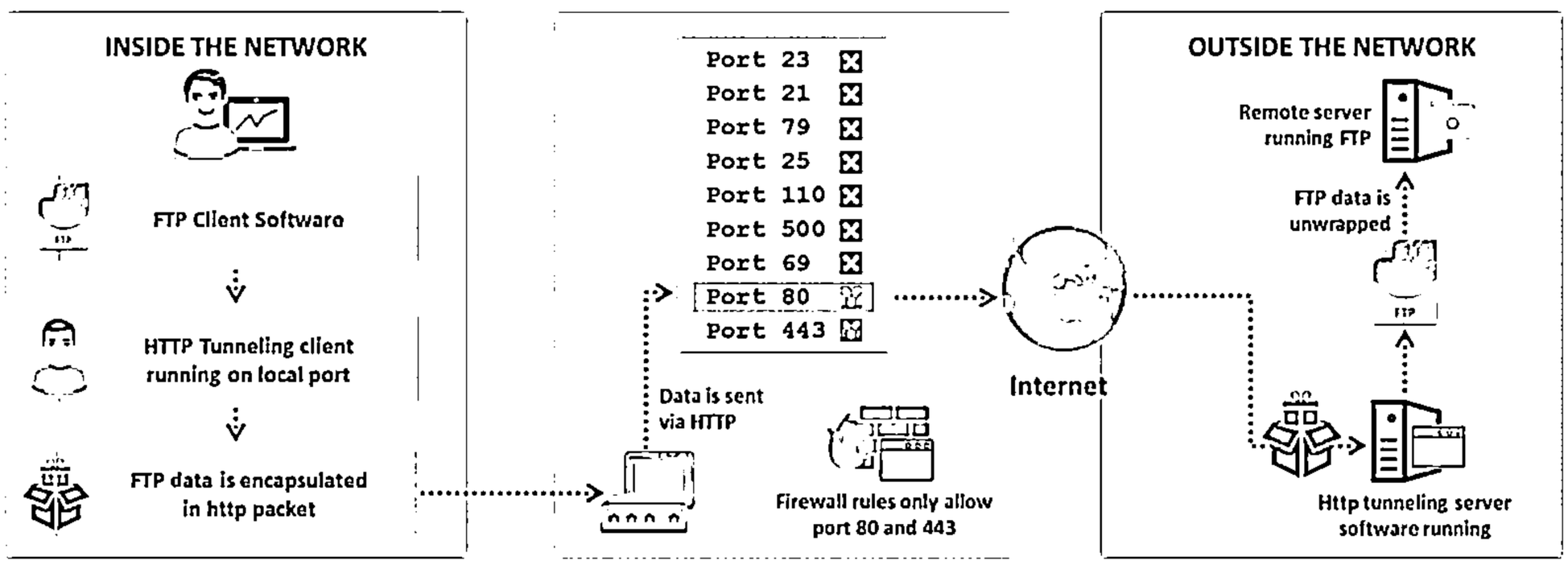


Figure 12.47: Illustration of HTTP Tunneling Method

HTTP Tunneling Tools

Some HTTP tunneling tools are as follows:

- **Super Network Tunnel**

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

  Super Network Tunnel is a two-way HTTP tunneling software that connects two computers using HTTP-Tunnel Client and HTTP-Tunnel Server. It works like VPN tunneling but uses the HTTP protocol to establish a connection for accessing the Internet without monitoring and provides an extra layer of protection against attackers, spyware, identity theft, and so on. It can bypass any firewall to surf the web, use IM

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

applications, games, and so on. Further, it integrates the SocksCap function along with bidirectional HTTP tunneling and remote control to simplify the configuration.

This tool allows HTTP, HTTPS, and SOCKS tunneling of any TCP communication between any client-server systems. The TCP traffic is sent from the client to the server via standard HTTP POST requests, which allows penetrating through firewalls, proxy servers, and so on, where HTTP traffic passes.

The client side of a tunnel is the Super Network Tunnel client app, which listens on a particular TCP port for incoming requests. Once the request comes, the program creates an HTTP/HTTPS tunnel to the server and sends data through it. The server side is a Super Network Tunnel server, which simply forwards the data to the intended recipient app running on the server computer or LAN. Both client and server sides support multiple tunnels and multiple connections through the same tunnel at the same time.

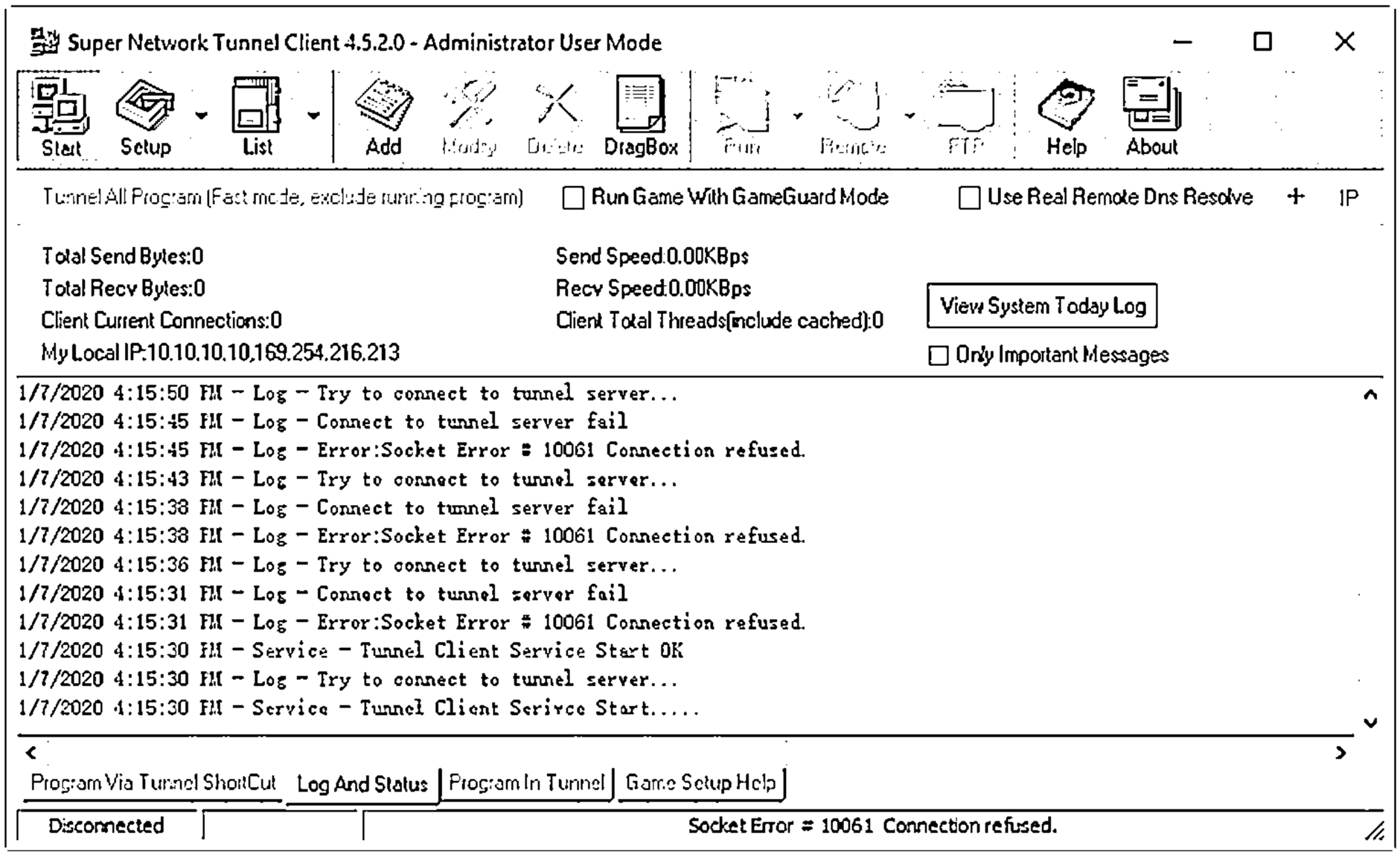


Figure 12.48: Screenshot of Super Network Tunnel

- **HTTPort and HTTHost**

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

  HTTPort allows users to bypass the HTTP proxy, which blocks Internet access to e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, and so on. Here, the Internet software is configured so that it connects to a local PC as if it is the required remote server. HTTPort then intercepts that connection and runs it through a tunnel through the proxy. HTTPort can work on devices such as proxies or firewalls that allow HTTP traffic. Thus, HTTPort provides access to websites and Internet apps. HTTPort performs tunneling using one of two modes: SSL/CONNECT mode or a remote host.

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

In the SSL/CONNECT mode, HTTPort can make a tunnel through a proxy all by itself. It requires that the proxy should support a particular HTTP feature, specifically, CONNECT HTTP. Most proxies have this method disabled by default. The SSL/CONNECT mode is much faster, but in this case, encryption cannot be used, and the proxy can track all actions.

The remote host method is capable of tunneling through any proxy. HTTPort uses a special server software called HTTHost, which is installed outside the proxy-blocked network. It is a web server; thus, when HTTPort is tunneling, it sends a series of HTTP requests to the HTTHost. The proxy responds as if the user is surfing a website and thus allows the user to do so. HTTHost, in turn, performs its half of the tunneling and communicates with the target servers. This mode is much slower but works in most cases and features strong data encryption that makes proxy logging useless.

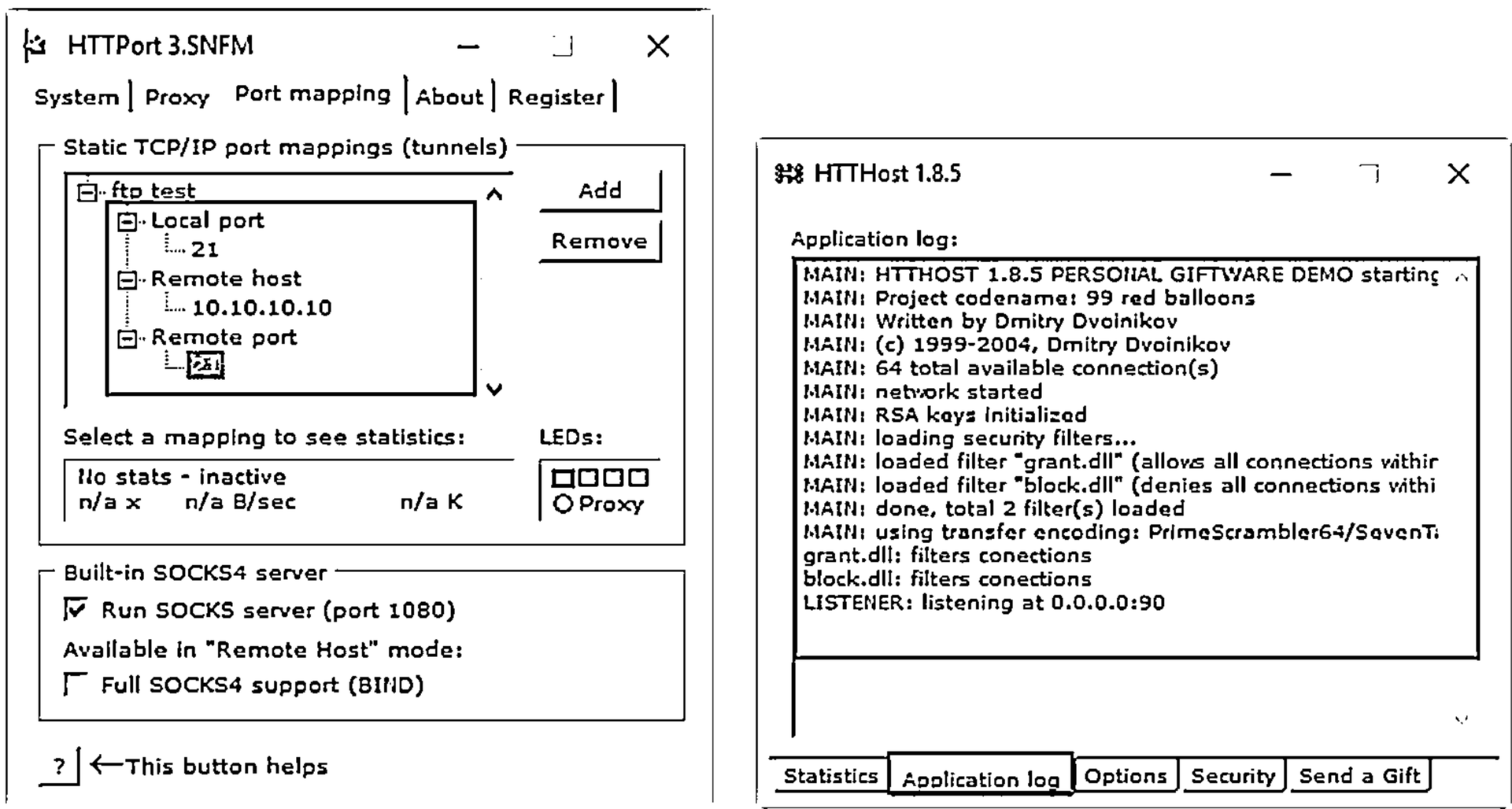


Figure 12.49: Screenshot of HTTPort and HTTHost

- **Other HTTP Tunneling Tools**
  - Tunna (*https://github.com*)
  - HTTP Tunnel (*http://http-tunnel.sourceforge.net*)

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

Bypassing Firewalls through the SSH Tunneling Method

OpenSSH

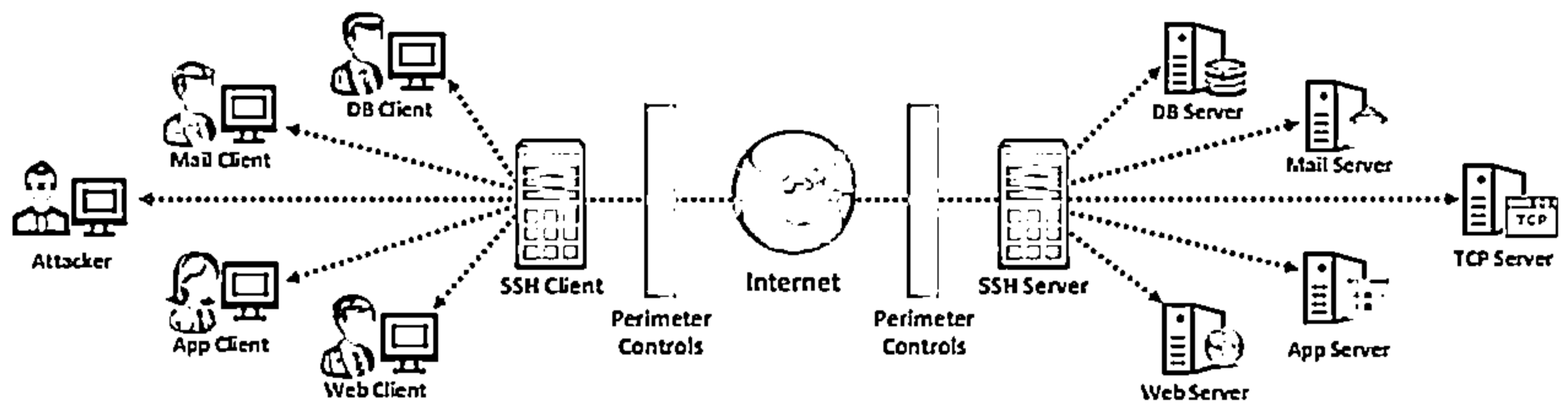
- Attackers use OpenSSH to encrypt and tunnel all the traffic from a local machine to a remote machine to avoid detection by the perimeter security controls

Example

```
ssh -f user@certifiedhacker.com -L 5000:certifiedhacker.com:25 -N
```

`-f` => background mode, `user@certifiedhacker.com` => username and server you are logging into, `-L 5000:certifiedhacker.com:25` => local-port:host:remote-port, and `-N` => Do not execute the command on the remote system

- This forwards the local port 5000 to port 25 on certifiedhacker.com encrypted
- Simply point your email client to use localhost:5000 as the SMTP server



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

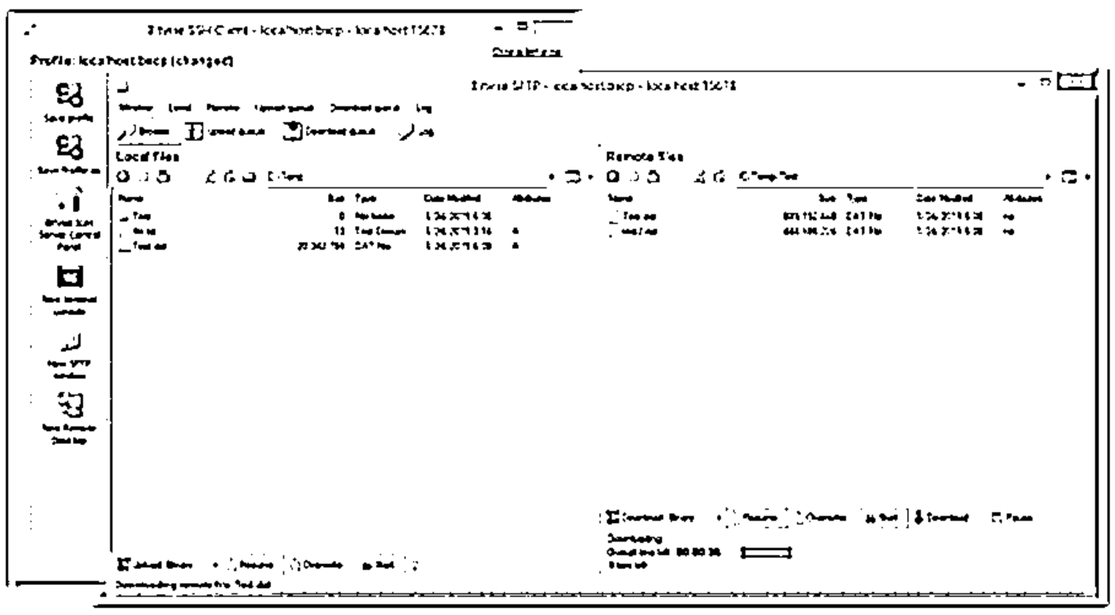
SSH Tunneling Tools: Bitvise and Secure Pipes

Bitvise

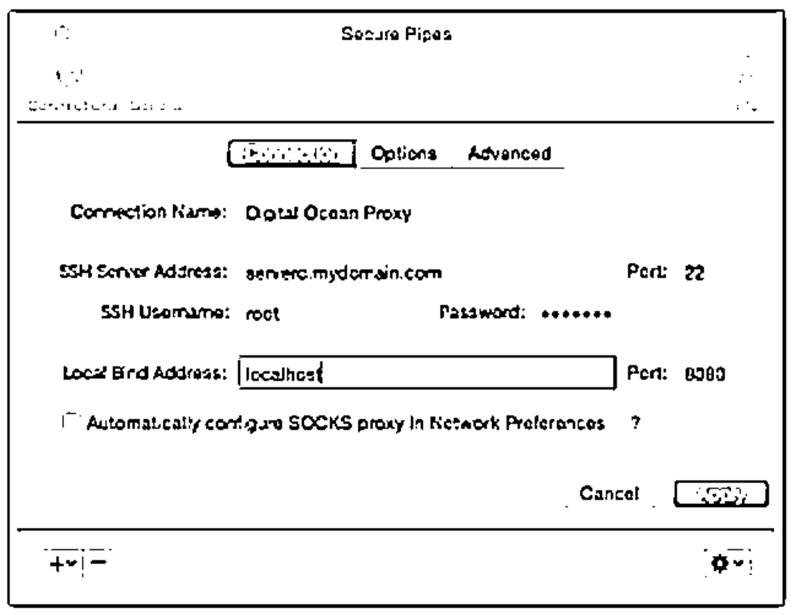
- Bitvise SSH Server provides secure remote login capabilities for Windows workstations and servers
- SSH Client includes powerful tunnelling features including dynamic port forwarding through an integrated proxy and remote administration for the SSH Server

Secure Pipes

- Secure Pipes makes managing SSH tunnels simple
- It selectively opens access to application ports normally not easily accessible due to network or service provider configuration restrictions



https://www.bitvise.com



https://www.opoet.com

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

Bypassing Firewalls through the SSH Tunneling Method

SSH protocol tunneling involves sending unencrypted network traffic through an SSH tunnel. For example, suppose you want to transfer files on an unencrypted FTP protocol, but the FTP protocol is blocked on the target firewall. The unencrypted data can be sent over the encrypted SSH protocol using SSH tunneling. Attackers use this technique to bypass firewall restrictions. They connect to external SSH servers and create SSH tunnels to port 80 on the remote server, thereby bypassing firewall restrictions.

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

Attackers use OpenSSH (OpenBSD Secure Shell) to encrypt and tunnel all traffic from a local machine to a remote machine to avoid detection by perimeter security controls. OpenSSH is a set of computer programs that provide encrypted communication sessions over a computer network using the SSH protocol.

Example:

```
ssh -f user@certifiedhacker.com -L 5000:certifiedhacker.com:25 -N
```

`-f` => background mode, `user@certifiedhacker.com` => username and server you are logging into, `-L 5000:certifiedhacker.com:25` => local-port:host:remote-port, and `-N` => Do not execute the command on the remote system.

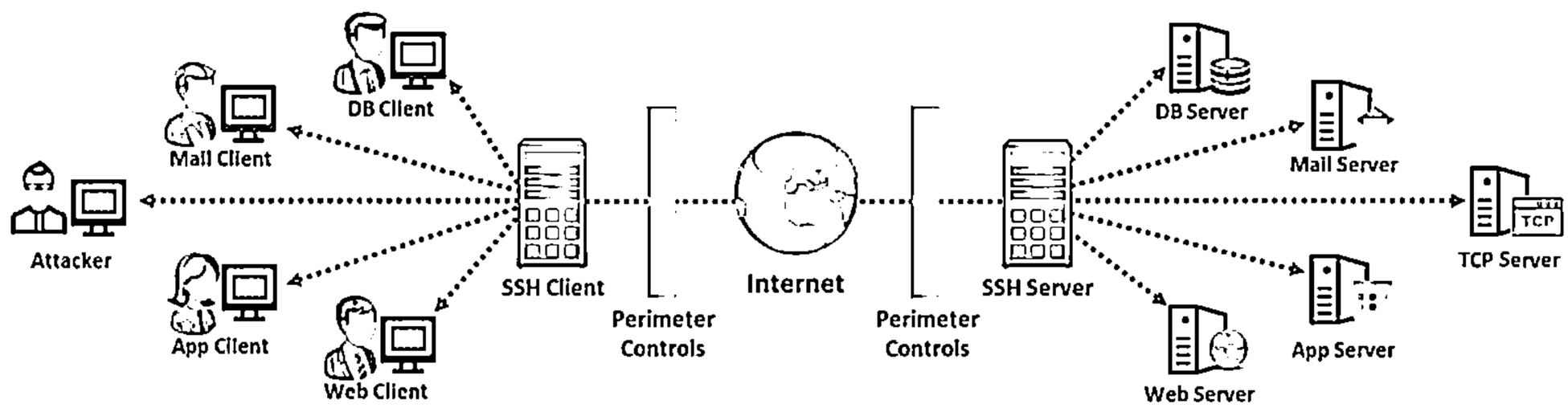


Figure 12.50: Bypassing Firewall through SSH Tunneling Method

SSH Tunneling Tools

Some SSH tunneling tools are listed below:

- **Bitvise**

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

  Bitvise SSH Server provides secure remote login capabilities to Windows workstations and servers by encrypting data during transmission. It is ideal for remote administration of Windows servers, for advanced users who wish to access their home machine from work or their work machine from home, and for a wide spectrum of advanced tasks, such as establishing a VPN using the SSH TCP/IP tunneling feature or providing a secure file depository using SFTP.

  Bitvise SSH Client for Windows includes terminal emulation, graphical as well as command-line SFTP support, an FTP-to-SFTP bridge, tunneling features—including dynamic port forwarding through an integrated proxy—and remote administration for SSH Server.

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

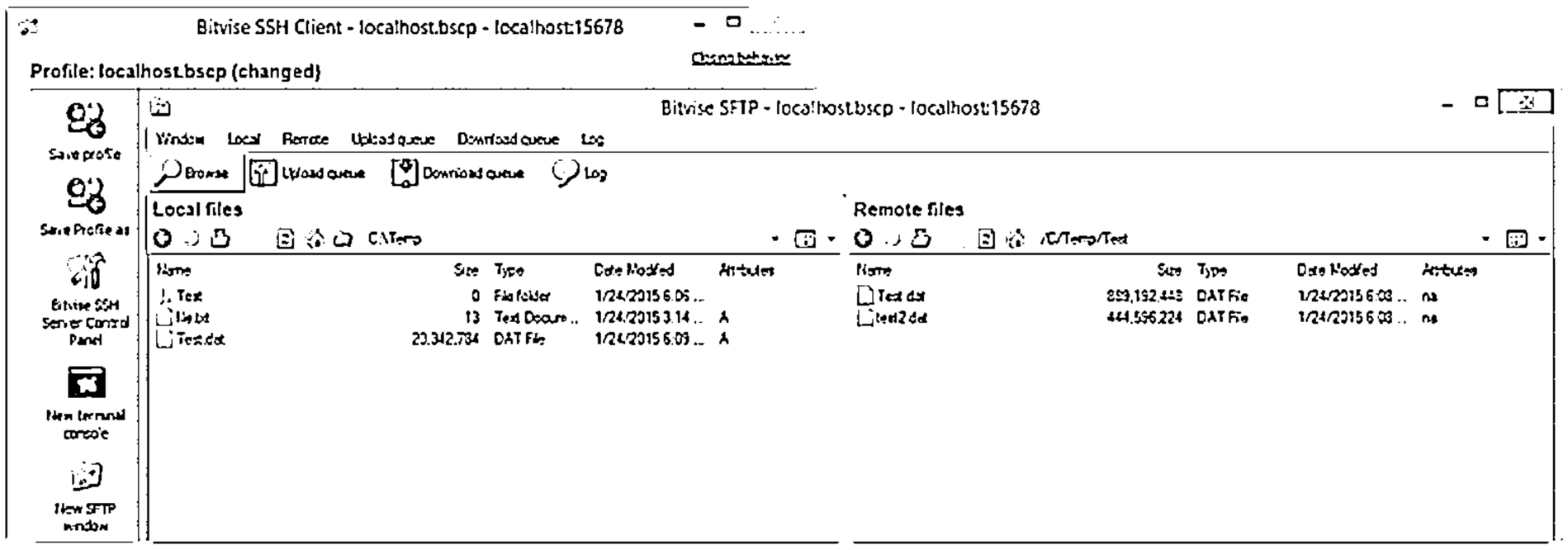


Figure 12.51: Screenshot of Bitvise

- **Secure Pipes**

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

  Secure Pipes is an OS X-based SSH tunneling software. Some of the features of Secure Pipes are as follows:

  - **Remote Forwards**: Selectively open up access to application ports that are usually not easily accessible owing to network or service provider configuration restrictions. Open the door to quickly leverage OS X Server on Internet-facing applications such as email and web hosting.
  - **Local Forwards**: Open application communication ports to remote servers without opening those ports to public networks. Bring the security of VPN communication to clients and servers on an ad hoc basis without the hassle of configuration and management.
  - **SOCKS Proxies**: Easily set up and manage a SOCKS proxy server for either a local client or a whole network to privatize communication and overcome local network restrictions. These tunnels are an indispensable and lightweight tool when traveling abroad, performing digital currency transactions, or simply securing a local network.

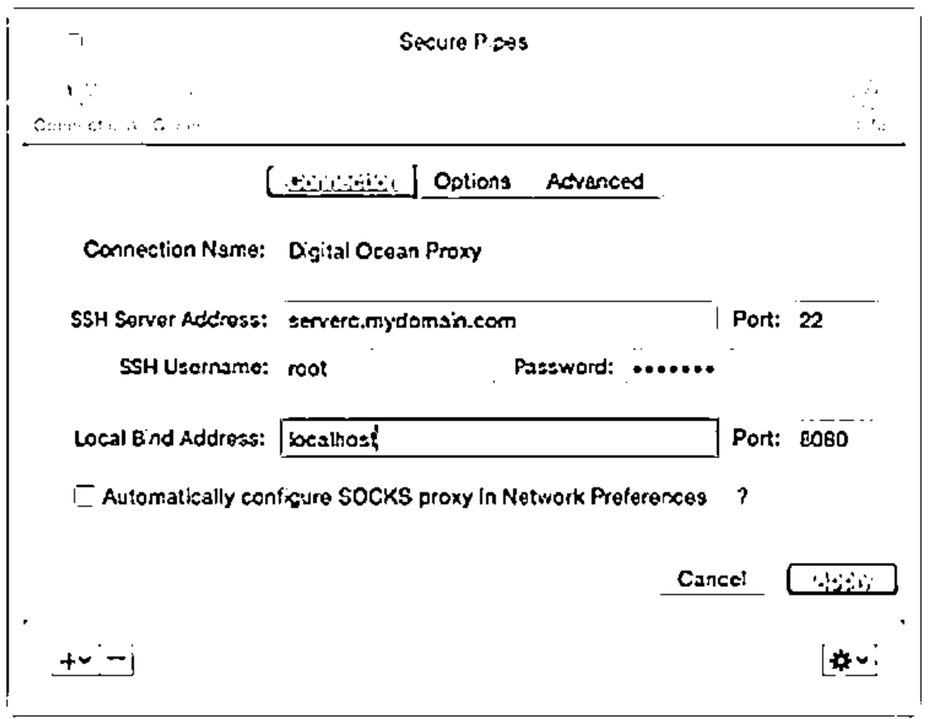


Figure 12.52: Screenshot of Secure Pipes

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

Bypassing Firewalls through the DNS Tunneling Method

- DNS operates using User Datagram Protocol (UDP) and it has a 255-byte limit on outbound queries
- This small size constraint on external queries allows the DNS to be used as an ideal choice to perform data exfiltration by various malicious entities
- Since corrupt or malicious data can be secretly embedded into the DN5 protocol packets, even DNSSEC cannot detect this abnormality in DNS tunneling
- It is effectively used by malware to bypass the firewall to maintain communication between the victim machine and the C&C server
- Tools such as NSTX (*https://sourceforge.net*), Heyoka (*http://heyoko.sourceforge.netuse*), and Iodine (*https://code.kryo.se*) use this technique of tunneling traffic across DNS port 53

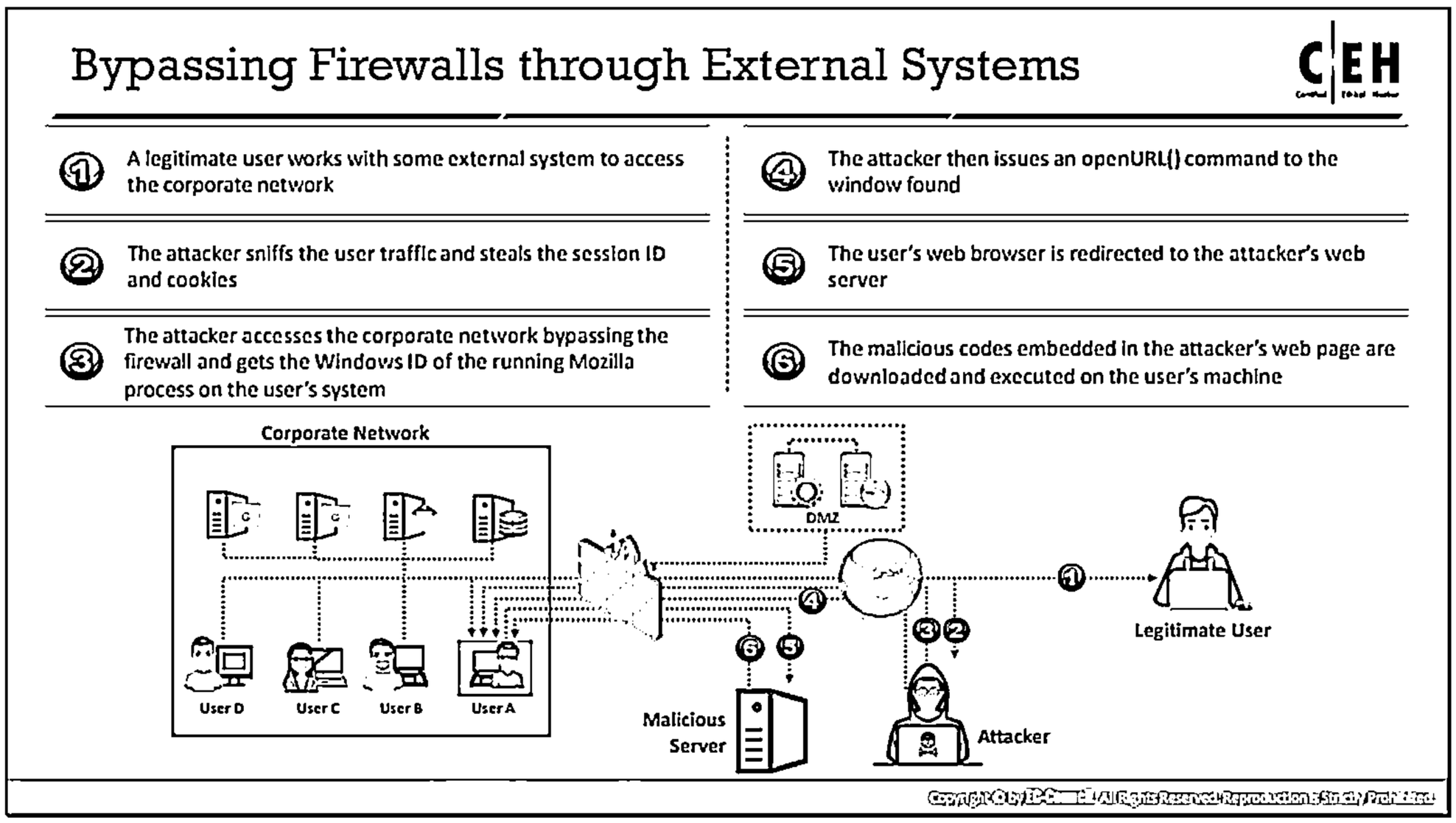
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bypassing Firewalls through the DNS Tunneling Method

DNS operates using UDP, and it has a 255-byte limit on outbound queries. Moreover, it allows only alphanumeric characters and hyphens. Such small size constraints on external queries allow DNS to be used as an ideal choice to perform data exfiltration by various malicious entities. Since corrupt or malicious data can be secretly embedded into the DNS protocol packets, even DNSSEC cannot detect the abnormality in DNS tunneling. It is effectively used by malware to bypass the firewall to maintain communication between the victim machine and the C&C server.

Tools such as NSTX (*https://sourceforge.net*), Heyoka (*http://heyoka.sourceforge.netuse*), and Iodine (*https://code.kryo.se*) use this technique of tunneling traffic across DNS port 53.

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



Bypassing Firewalls through External Systems

Attackers can bypass firewall restrictions of target networks from an external system that can access the internal network. This external system can be:

- A home machine of and employee
- A machine that conducts remote administration of the target network
- A machine from the company's network but located at a different place

Steps to be followed to bypass a firewall through external systems:

1. Legitimate user works with some external system to access the corporate network
2. Attacker sniffs the user traffic and steals the session ID and cookies
3. Attacker accesses the corporate network by bypassing the firewall and gets the Windows ID of the running Mozilla process on the user's system
4. Attacker then issues an OpenURL() command to the found window
5. User's web browser is redirected to the attacker's web server
6. The malicious code embedded in the attacker's web page is downloaded and executed on the user's machine

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

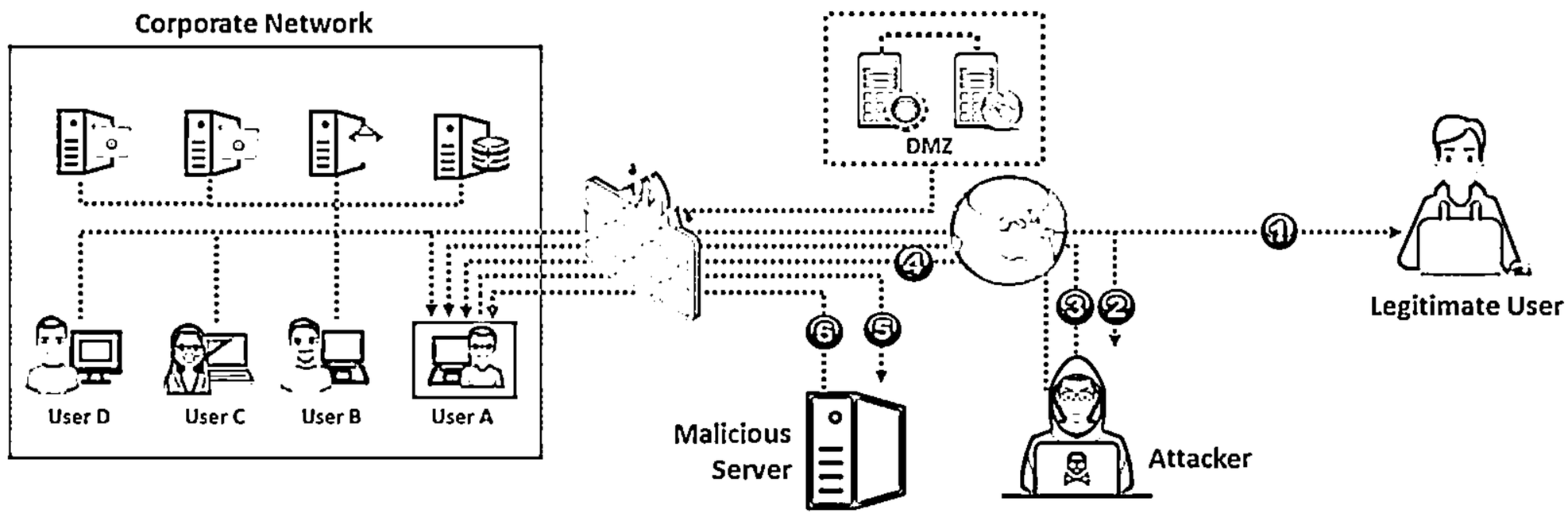
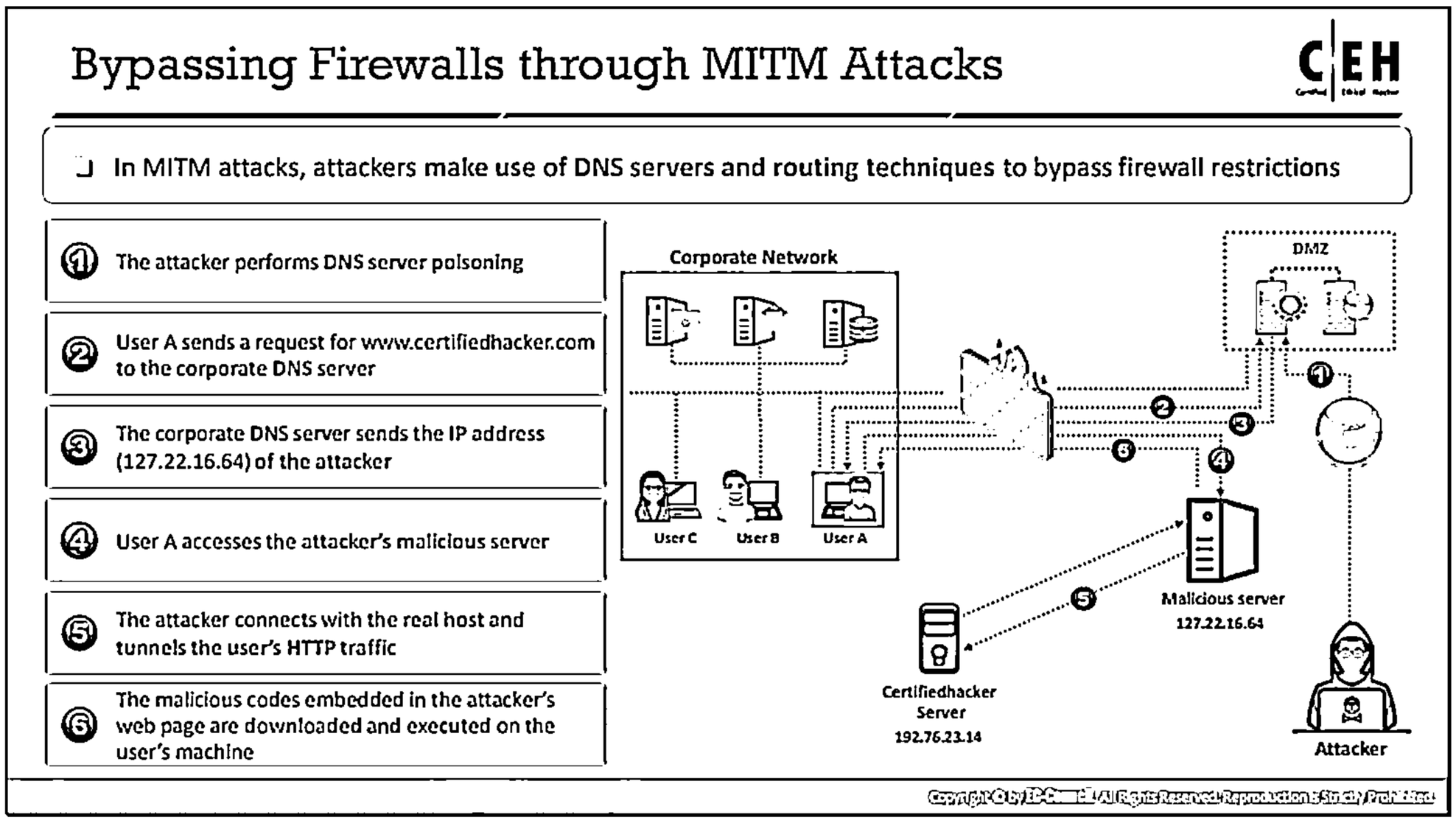


Figure 12.53: Bypassing firewall through external systems

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



Bypassing Firewalls through MITM Attacks

Most security administrators focus on the possibility of an external or internal network bypassing their firewall while ignoring the fact that firewalls can be bypassed using MITM attacks on DNS servers. In MITM attacks, attackers use DNS servers and routing techniques to bypass firewall restrictions. They may either take over the corporate DNS server or spoof DNS responses to perform the MITM firewall attack.

Steps to be followed to bypass a firewall through MITM attacks:

1. Attacker performs DNS server poisoning
2. User A requests for www.certifiedhacker.com from the corporate DNS server
3. Corporate DNS server sends the IP address (127.22.16.64) of the attacker
4. User A accesses the attacker's malicious server
5. Attacker connects to the real host and tunnels the user's HTTP traffic
6. The malicious code embedded in the attacker's web page is downloaded and executed on the user's machine

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

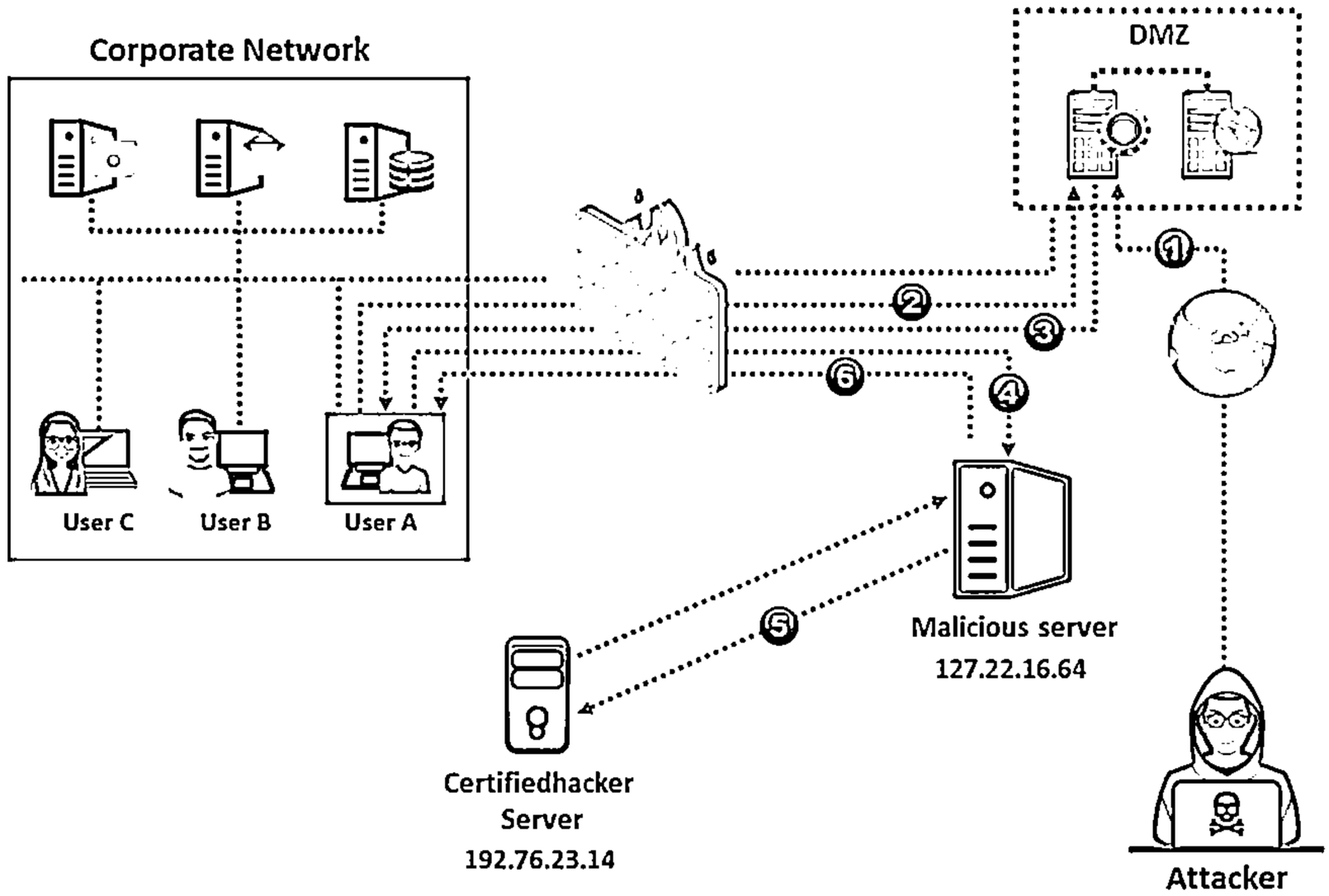


Figure 12.54: Bypassing firewall through MITM attack

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

Bypassing Firewalls through Content

- In this method, the attacker sends the content containing malicious code to the user and tricks him/her to open it so that the malicious code can be executed

- **Examples:**

  Sending an email containing a malicious executable file or Microsoft office document capable of a macro bypass exploit

- There are many file formats that can be used as a malicious content carrier

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

Bypassing Firewalls through Content

In this method, the attacker sends content containing malicious code to the user and tricks him/her into opening it so that the malicious code can be executed. For example, an attacker can send an email containing a malicious executable file or Microsoft office document capable of exploiting a macro bypass exploit. Attackers can also target WWW/FTP servers and embed Trojan horse files as software installation files, mobile phone software, and so on to lure users into accessing them. There are many file formats for text, multimedia, and graphics content that can be used to carry malicious content.

Commonly used file formats for carrying malicious content are:

- EXE, COM, BAT, PS, PDF CDR (Corel Draw)
- DVB, DWG (AutoCAD)
- SMM (AMI Pro)
- DOC, DOT, CNV, ASD (MS Word)
- XLS, XLB, XLT (MS Excel)
- ADP, MDA, MDB, MDE, MDN, MDZ (MS Access)
- VSD (Visio)
- MPP, MPT (MS Project)
- PPT, PPS, POT (MS PowerPoint)
- MSG, OTM (MS Outlook)

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

Bypassing the WAF using an XSS Attack

- An XSS attack exploits vulnerabilities that occur while processing input parameters of the end-users and the server responses in a web application
- Attackers inject malicious HTML code in the victim website to bypass the WAF
- Consider the following XSS payload

```
<script>alert("XSS")</script>
```

Using ASCII values to bypass the WAF

- After replacing the XSS payload with its equivalent ASCII values

```
<script>String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 88, 83, 83, 34, 41)</script>
```

Using Hex Encoding to bypass the WAF

- After encoding the XSS payload,

```
%3C%73%63%69%72%70%74%3E%61%6C%65%72%74%28%22%58%53%53%22%29%3C%2F%73%63%72%69%70%74%3E
```

Using Obfuscation to bypass the WAF

- After encoding the XSS payload,

```
<sCRiPt>aLeRT("XSS")</sCriPT>
```

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

Bypassing the WAF using an XSS Attack

XSS attack exploits vulnerabilities that occur while processing the input parameters of end users and the server responses in a web application. Attackers take advantage of these vulnerabilities to inject malicious HTML code into the victim website to bypass the WAF.

- **Using ASCII values to bypass the WAF**

  In this technique, attackers use ASCII characters to bypass the WAF. For example, consider the following XSS payload

  ```
  <script>alert("XSS")</script>
  ```

  When the above JavaScript code is executed, the WAF filters escape single quotes, double magic quotes, etc. Hence, the above payload is filtered by the WAF. To bypass the WAF, we need to convert the above payload into its equivalent ASCII values and then execute it. The JavaScript will automatically convert the ASCII values back into the original characters. Attackers use online websites to convert an XSS payload into its ASCII equivalent. Alternatively, the Hackbar Mozilla addon can be used to get ASCII values.

  Consider the XSS payload given below:

  ```
  XSS Payload:alert("XSS")
  ```

  The equivalent ASCII values are:

  ```
  String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 88, 83, 83, 34, 41)
  ```

  The above values are inserted into the XSS payload:

  ```
  <script>String.fromCharCode(97, 108, 101, 114, 116, 40, 34, 88, 83, 83,
  34, 41)</script>
  ```

  The above payload bypasses the WAF filters successfully.

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

- **Using Hex Encoding to bypass the WAF**

  In this technique, the entire XSS payload is replaced with Hex values to bypass WAF. Attackers use online websites such as *http://www.convertstring.com/EncodeDecode/HexEncode* to convert the XSS payload into equivalent Hex values. For example, consider the following XSS payload

  ```
  <script>alert("XSS")</script>
  ```

  The encoded value for the XSS payload is

  ```
  %3C%73%63%69%72%70%74%3E%61%6C%65%72%74%28%22%58%53%53%22%29%3C%2F%73%6
  3%72%69%70%74%3E
  ```

  The above payload bypasses the WAF filters successfully.

- **Using Obfuscation to bypass the WAF**

  Attackers use the obfuscation technique to bypass the WAF. In this technique, attackers use a combination of upper- and lower-case letters in the XSS payload. For example, consider the following XSS payload:

  ```
  <script>alert("XSS")</script>
  ```

  Using obfuscation, the above payload is replaced with

  ```
  <sCRiPt>aLeRT("XSS")</sCriPT>
  ```

  The above payload bypasses the WAF successfully

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

Module Flow

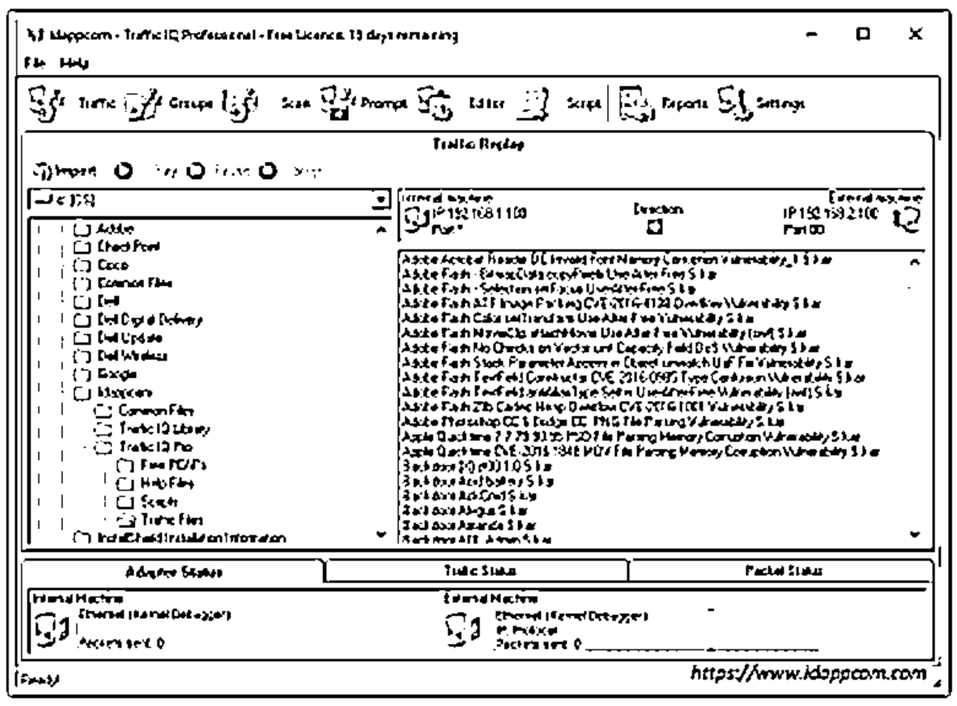
1. IDS, IPS, Firewall, and Honeypot Concepts
2. IDS, IPS, Firewall, and Honeypot Solutions
3. Evading IDS
4. Evading Firewalls
5. IDS/Firewall Evading Tools
6. Detecting Honeypots
7. IDS/Firewall Evasion Countermeasures

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

IDS/Firewall Evading Tools

Traffic IQ Professional

Traffic IQ Professional generates custom attack traffic which allows attackers to bypass the installed perimeter devices in the target network



- **Nmap** — https://nmap.org
- **Metasploit** — https://www.metasploit.com
- **Inundator** — https://sourceforge.net
- **IDS-Evasion** — https://github.com
- **Hyperion-2.0** — http://nullsecurity.net

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

IDS/Firewall Evading Tools

During firewall evasion, attackers use various security-auditing tools that assess firewall behavior. This section lists some of these tools that help attackers to bypass firewall restrictions. They automate the process of bypassing firewall rules while increasing effectiveness and consuming less time.

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

- **Traffic IQ Professional**

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

  Traffic IQ Professional is a tool that audits and validates the behavior of security devices by generating the standard application traffic or attack traffic between two virtual machines. This tool is generally used by security personnel for assessing, auditing, and testing the behavioral characteristics of any non-proxy packet-filtering device, which can include application firewalls, IDS, IPS, routers, switches, etc. However, as this tool can generate custom attack traffic, it is extensively employed by attackers to bypass the installed perimeter devices in the target network.

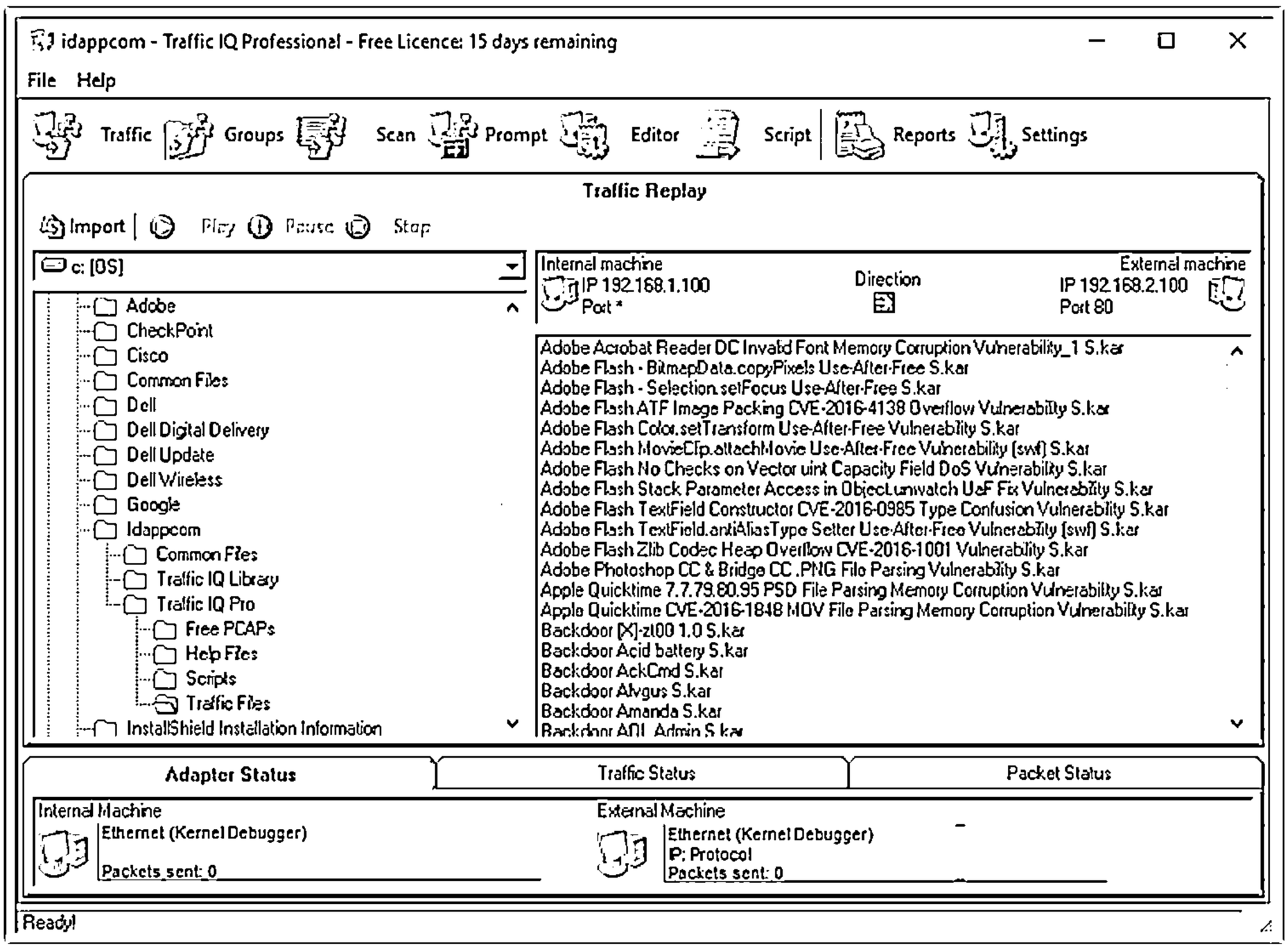


Figure 12.55: Screenshot of Traffic IQ Professional

Some additional IDS/firewall evasion tools are as follows:

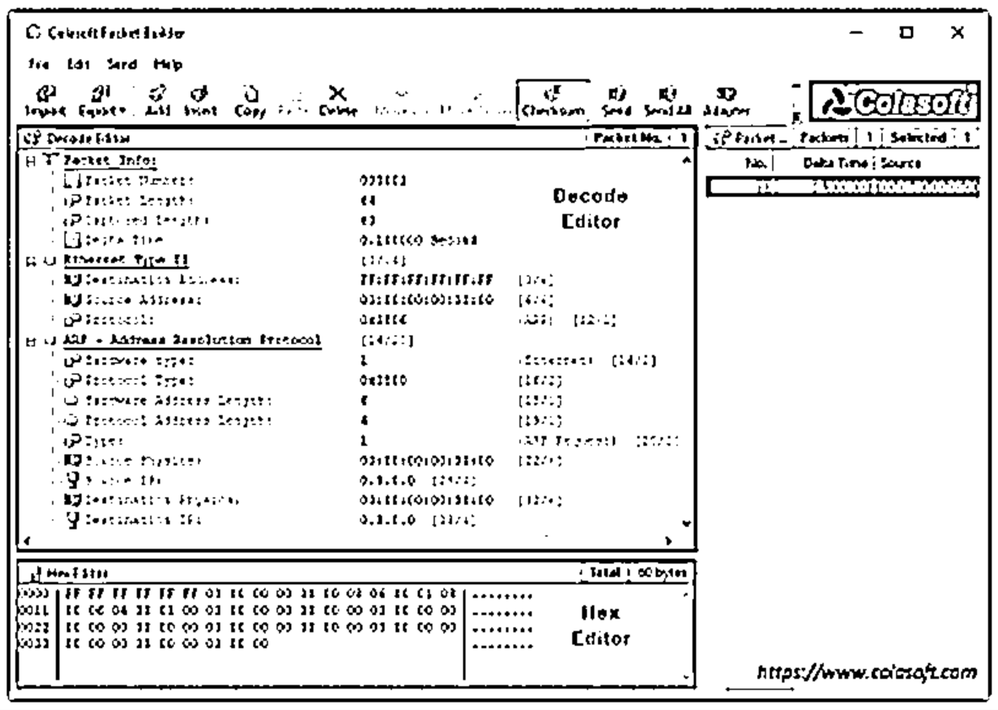
- Nmap (*https://nmap.org*)
- Metasploit (*https://www.metasploit.com*)
- Inundator (*https://sourceforge.net*)
- IDS-Evasion (*https://github.com)*
- Hyperion-2.0 (*http://nullsecurity.net)*

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

Packet Fragment Generator Tools

Colasoft Packet Builder

Colasoft Packet Builder is used to create custom network packets and fragmenting packets. Attackers use this tool to create custom malicious packets and fragment them in such a way that firewalls will not detect them



CommView
https://www.tamos.com

NetScanTools Pro
https://www.netscantools.com

Ostinato
https://ostinato.org

WAN Killer
https://www.solarwinds.com

WireEdit
https://wireedit.com

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

Packet Fragment Generator Tools

There are various packet fragment generators that attackers use to perform fragmentation attacks on firewalls to bypass them.

- **Colasoft Packet Builder**

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

  Colasoft Packet Builder is used to create custom network packets and fragmenting packets. Attackers use this tool to create custom malicious packets and fragment them such that firewalls cannot detect them. They can create custom network packets such as Ethernet Packet, ARP Packet, IP Packet, TCP Packet, and UDP Packet. Security professionals use this tool to check your network's protection against attacks and intruders.

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

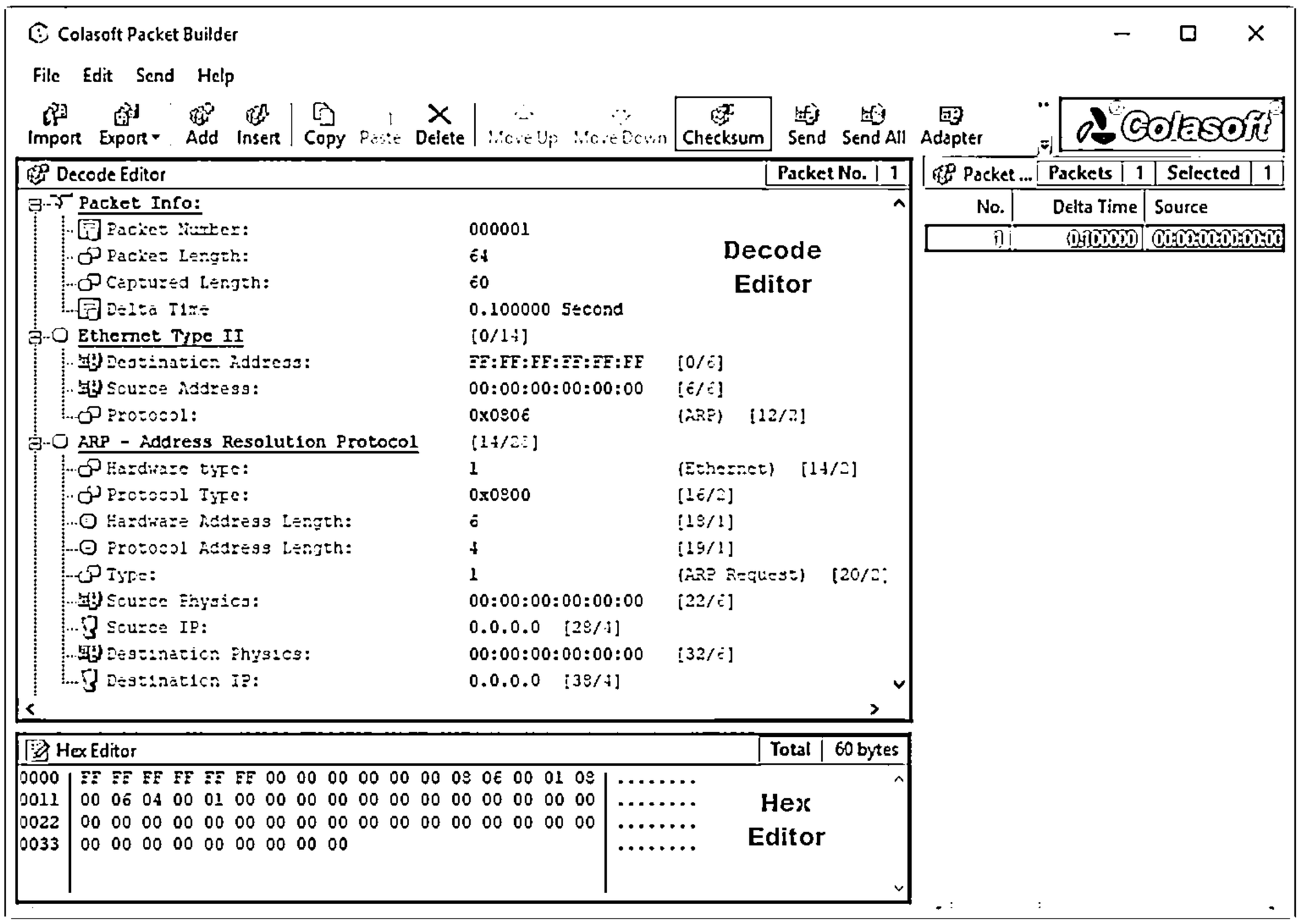


Figure 12.56: Screenshot of Colasoft Packet Builder

Some additional packet generator tools are listed below:

- CommView (*https://www.tamos.com*)
- NetScanTools Pro (*https://www.netscantools.com*)
- Ostinato (*https://ostinato.org*)
- WAN Killer (*https://www.solarwinds.com*)
- WireEdit (*https://wireedit.com*)

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

Module Flow

1. IDS, IPS, Firewall, and Honeypot Concepts
2. IDS, IPS, Firewall, and Honeypot Solutions
3. Evading IDS
4. Evading Firewalls
5. IDS/Firewall Evading Tools
6. Detecting Honeypots
7. IDS/Firewall Evasion Countermeasures

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

Detecting Honeypots

- Attackers can determine the presence of honeypots by probing the services running on the system
- Attackers craft malicious probe packets to scan for services such as HTTP over SSL (HTTPS), SMTP over SSL (SMPTS), and IMAP over SSL (IMAPS)
- Ports that show a specific service running but deny a three-way handshake connection indicate the presence of a honeypot

Tools to detect honeypots:
- Send-safe Honeypot Hunter (*http://www.send-safe.com*)
- kippo_detect (*https://github.com*)

Note: Attackers can also defeat the purpose of honeypots by using multi-proxies (TORs) and hiding their conversation using encryption and steganography techniques

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

Detecting Honeypots

Honeypots are traps set to detect, deflect, or counteract unauthorized intrusion attempts. While attempting to break into the target network, attackers perform honeypot detection using various tools and techniques. This section discusses these tools and how they are used.

A honeypot is an Internet system designed primarily for diverting attackers by tricking or attracting them during their attempts to gain unauthorized access to information systems.

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

Attackers can determine the presence of honeypots by probing the services running on the system. Attackers use honeypot detection systems or methods to identify the honeypots installed on the target network. They craft malicious probe packets to scan for services such as HTTP over SSL (HTTPS), SMTP over SSL (SMPTS), and IMAP over SSL (IMAPS). Ports that show a particular service running but deny a three-way handshake connection indicate the presence of a honeypot. Once they detect honeypots, attackers try to bypass them so that they can focus on targeting the actual network. Tools to detect honeypots include Send-safe Honeypot Hunter (*http://www.send-safe.com*) and kippo_detect (*https://github.com*).

Note: Attackers can also defeat honeypots by using multi-proxies (TORs) and hiding their conversation using encryption and steganography techniques.

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

Detecting and Defeating Honeypots

Detecting the presence of Layer 7 Tar Pits	Observe the latency of the response from the service
Detecting the presence of Layer 4 Tar Pits	Analyze the TCP window size, where tar pits continuously acknowledge incoming packets even though the TCP window size is reduced to zero
Detecting the presence of Layer 2 Tar Pits	If an attacker is present on the same network as the Layer 2 tar pits, then the attacker can detect the presence of this daemon by looking at the responses with unique MAC address 0:0:f:ff:ff:ff which act as a kind of black hole
Detecting Honeypots running on VMware	Observe the IEEE standards for the current range of MAC addresses assigned to VMWare Inc.
Detecting the presence of Honeyd Honeypot	Perform time-based TCP Finger printing methods (SYN Proxy behavior)

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

Detecting and Defeating Honeypots (Cont'd)

Detecting the presence of User-Mode Linux (UML) Honeypot	Analyze the files such as /proc/mounts, /proc/interrupts, and /proc/cmdline, which contain UML-specific information
Detecting the presence of Sebek-based Honeypots	Sebek logs everything that is accessed via read() before transferring it to the network, causing the congestion effect. Analyze the congestion in the network layer
Detecting the presence of Snort_inline Honeypot	Analyze the outgoing packets by capturing the Snort_inline modified packets through another host system and identifying the packet modification
Detecting the presence of Fake AP	Fake access points only send beacon frames and do not generate any fake traffic on the access points and an attacker can monitor the network traffic and easily notice the presence of a fake AP
Detecting the presence of Bait and Switch Honeypots	Observe specific TCP/IP parameters such as Round-Trip Time (RTT), the Time To Live (TTL), and the TCP timestamp

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

Detecting and Defeating Honeypots

A honeypot is a security mechanism that is deployed to counterattack and trap attackers. Honeypots lure attackers into performing malicious activities, and this attack information provides insights into the level and type of threats a network infrastructure can face. As an attacker, determining whether the target system is a legitimate one or a honeypot is essential to compromise the network without being detected. Identifying and defeating these honeypot establishments stealthily is the fundamental task of a professional hacker.

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

Some techniques used to identify, detect, and defeat various honeypot infrastructures are discussed below:

- **Detecting the presence of Layer 7 Tar Pits**: Tar pits are security entities that are similar to honeypots, which are designed to respond slowly to incoming requests. They slow down unauthorized attempts of hackers. Layer 7 tar pits react slowly to incoming SMTP commands by attackers/spammers. Attackers can identify the presence of Layer 7 tar pits by looking at the latency of the response from the service.
- **Detecting the presence of Layer 4 Tar Pits**: Layer 4 tar pits manipulate the TCP/IP stack and are effectively employed to slow down the spreading of worms, backdoors, etc. In these tar pits, the iptables accept the incoming TCP/IP connection and spontaneously switch to a zero-window size, blocking the attacker from sending further data. This connection cannot be terminated by the attacker, as no data is transferred to the target machine. Layer 4 tar pits such as Labrea can be identified by the attacker by analyzing the TCP window size, where the tar pit continuously acknowledges incoming packets even though the TCP window size is reduced to zero.
- **Detecting the presence of Layer 2 Tar Pits**: If an attacker launches an attack from the same network, the issue of Layer 2 arises. Layer 2 tar pits are used to block the network penetration of the attacker who gains access to the network as well as to prevent internal threats. The attacker can detect the presence of this daemon by looking at the responses with the unique MAC address 0:0:f:ff:ff:ff, which acts as a kind of black hole. An attacker can also identify the presence of these tar pits by analyzing the ARP responses.
- **Detecting Honeypots running on VMware**: VMWare is a commercially available virtual machine that is used to launch multiple instances of an OS simultaneously. These virtual machines can be configured with various virtual machine resources such as CPU, memory, disks, I/O devices, etc. Owing to its numerous advantages, VMWare is widely used to launch honeypots. Attackers can identify instances that are running on the VMWare virtual machine by analyzing the MAC address. By looking at the IEEE standards for the current range of MAC addresses assigned to VMWare Inc., an attacker can identify the presence of VMWare-based honeypots.
- **Detecting the presence of Honeyd Honeypot**: Honeyd is a widely used honeypot daemon. It is used to create thousands of honeypots easily. It is a network-simulated and service-simulated honeypot deployment engine. This honeyd honeypot can respond to a remote attacker who tries to contact the SMTP service with fake responses.

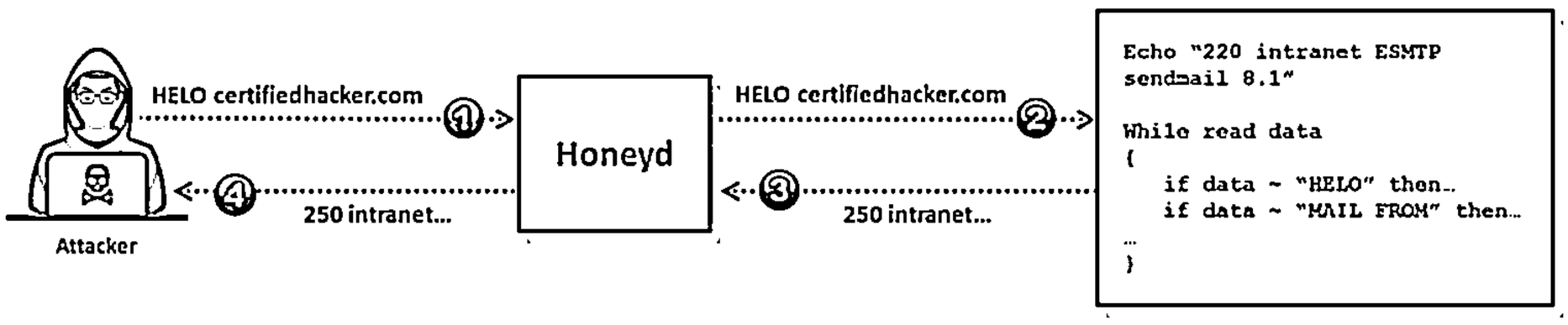


Figure 12.57: Honeyd fake response

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

An attacker can identify the presence of honeyd honeypot by performing time-based TCP fingerprinting methods (SYN proxy behavior). The following figure shows the difference between a response to a normal computer and the response of honeyd honeypot to a manual SYN request sent by an attacker.

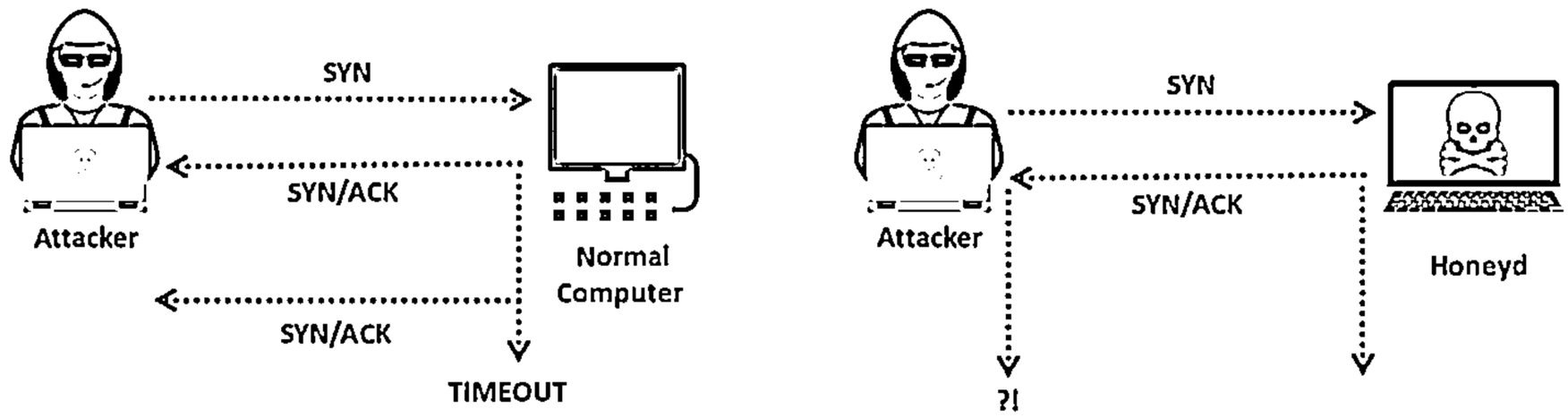


Figure 12.58: Response to SYN request by normal computer vs. Honeyd Honeypot

- **Detecting the presence of User-Mode Linux (UML) Honeypot**: User-Mode Linux is an open-source software under GNU, which is used to create virtual machines and is efficient in deploying honeypots. Attackers can identify the presence of UML honeypots by analyzing files such as /proc/mounts, /proc/interrupts, and /proc/cmdline, which contain UML-specific information.
- **Detecting the presence of Sebek-based Honeypots**: Sebek is a server/client-based honeypot application that captures the rootkits and other malicious malware that hijacks the read() system call. Such honeypots record all the data accessed via reading () call. Attackers can detect the existence of Sebek-based honeypots by analyzing the congestion in the network layer, as Sebek data communication is usually unencrypted. Since Sebek logs everything that is accessed via reading () call before transferring to the network, it causes the congestion effect.
- **Detecting the presence of Snort_inline Honeypot**: Snort_inline is a modified version of Snort IDS that is capable of packet manipulation. It can rewrite rules in the iptables and is mainly used in GenII (2nd generation) honeynets to block known attacks and avoid attacker bouncing. Attackers can identify these honeypots by analyzing the outgoing packets. If an outgoing packet is dropped, it might look like a black hole to an attacker, and when the snort_inline modifies an outgoing packet, the attacker can capture the modified packet through another host system and identify the packet modification.
- **Detecting the presence of Fake AP**: Fake access points are those that create fake 802.11b beacon frames with randomly generated ESSID and BSSID (MAC address) assignments. Fake access points only send beacon frames but do not produce any fake traffic on the access points, and an attacker can monitor the network traffic and quickly note the presence of fake AP.
- **Detecting the presence of Bait and Switch Honeypots**: Bait and switch honeypots actively participate in security mechanisms that are employed to respond quickly to incoming threats and malicious attempts. They redirect all malicious network traffic to a honeypot after any intrusion attempt is detected. An attacker can identify the presence of such honeypots by looking at specific TCP/IP parameters such as the Round-Trip Time (RTT), the Time To Live (TTL), and the TCP timestamp.

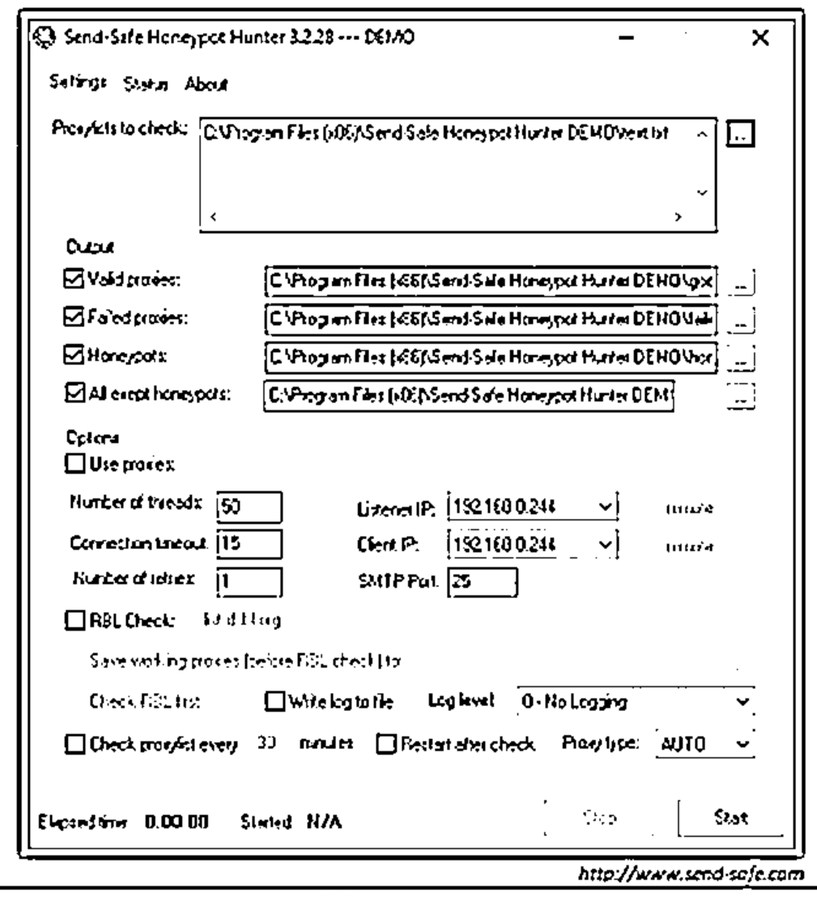
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Honeypot Detection Tools: Send-Safe Honeypot Hunter

- Send-Safe Honeypot Hunter is a tool designed for checking lists of HTTPS and SOCKS proxies for "honey pots"

Features:

1. Checks lists of HTTPS, SOCKS4, and SOCKS5 proxies with any ports
2. Checks several remote or local proxylists at once
3. Can upload "Valid proxies" and "All except honeypots" files to FTP
4. Can process proxylists automatically every specified time interval
5. May be used for usual proxylist validating as well



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

Honeypot Detection Tools

Attackers user honeypot detection tools such as Send-Safe Honeypot Hunter (*http://www.send-safe.com*) and kippo_detect (*https://github.com*) to detect honeypots in the target organizational networks.

- **Send-Safe Honeypot Hunter**

  Source: *http://www.send-safe.com*

  Send-Safe Honeypot Hunter is a tool designed for checking lists of HTTPS and SOCKS proxies for "honey pots."

  Features:

  - Checks lists of HTTPS, SOCKS4, and SOCKS5 proxies with any ports
  - Checks several remote or local proxylists at once
  - Can upload "Valid proxies" and "All except honeypots" files to FTP
  - Can process proxylists automatically in every specified period
  - May be used for usual proxylist validating as well

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

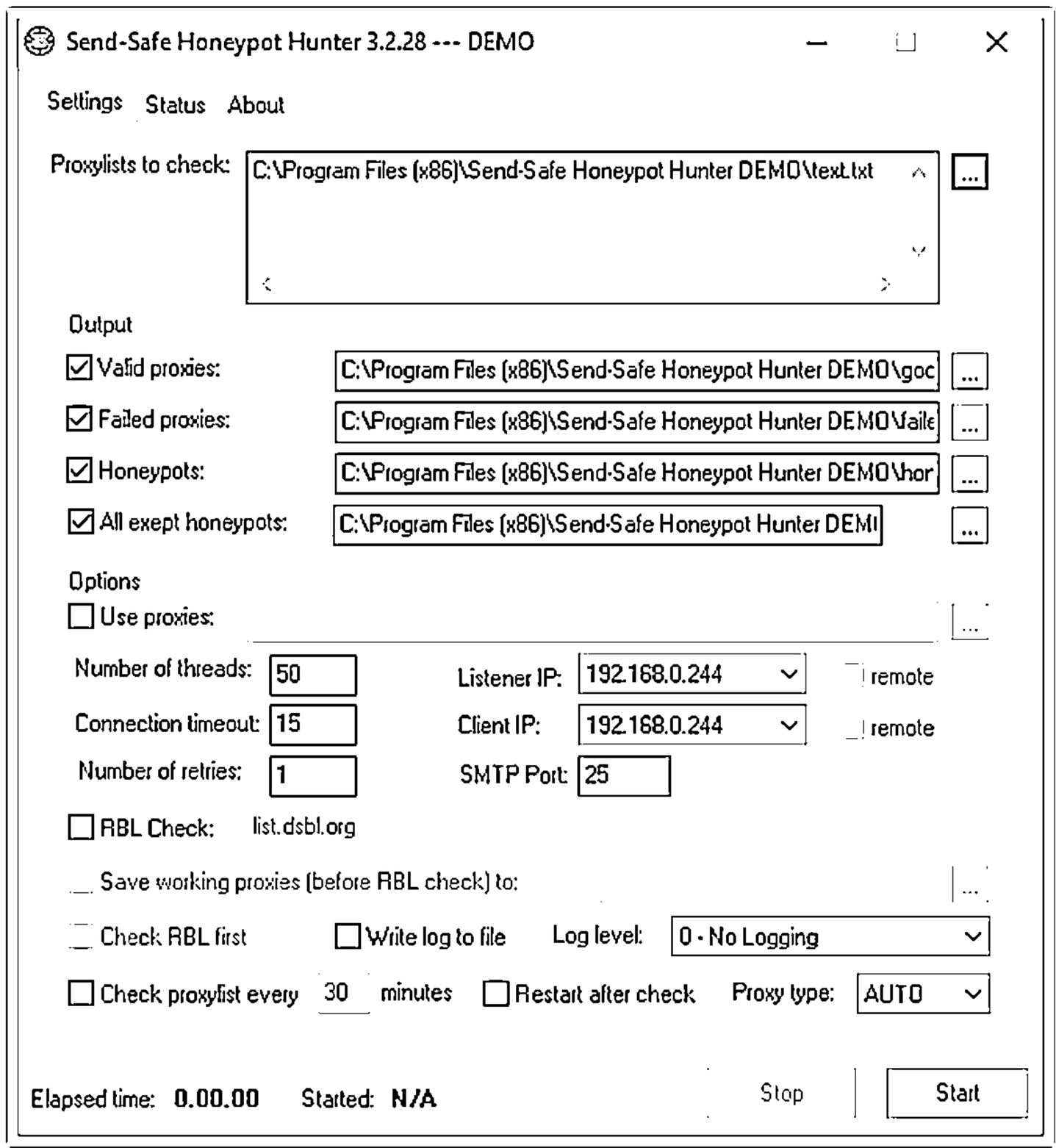


Figure 12.59: Screenshot of Send-Safe Honeypot Hunter

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

Module Flow

1. IDS, IPS, Firewall, and Honeypot Concepts
2. IDS, IPS, Firewall, and Honeypot Solutions
3. Evading IDS
4. Evading Firewalls
5. IDS/Firewall Evading Tools
6. Detecting Honeypots
7. IDS/Firewall Evasion Countermeasures

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

IDS/Firewall Evasion Countermeasures

The previous sections discussed various tools and techniques used by attackers to bypass network security perimeters such as IDS, firewalls, and honeypots to enter target networks. It is necessary to deploy and configure these security mechanisms securely to avoid attacks. This section discusses various countermeasures and best practices for hardening such network security perimeters.

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

How to Defend Against IDS Evasion

1. Shut down switch ports associated with known attack hosts
2. Perform an in-depth analysis of ambiguous network traffic for all possible threats
3. Use a TCP FIN or a reset (RST) packet to terminate malicious TCP sessions
4. Look for the a nop opcode other than 0x90 to defend against the polymorphic shellcode problem
5. Train users to identify attack patterns and regularly update/patch all the systems and network devices
6. Deploy an IDS after a thorough analysis of the network topology, the nature of network traffic, and the number of hosts to monitor
7. Use a traffic normalizer to remove potential ambiguity from the packet stream before it reaches the IDS
8. Ensure that IDSs normalize fragmented packets and allow those packets to be reassembled in the proper order
9. Define the DNS server with a client resolver for the routers and similar network devices
10. Tighten the security of all communication devices such as modems, routers, and switches
11. If possible, block ICMP TTL expired packets at the external interface level and change the TTL field to a large value
12. Regularly update the antivirus signature database
13. Use a traffic normalization solution at the IDS to protect the system against evasions
14. Store the attack information (attacker IP, victim IP, timestamp) for future analysis

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

How to Defend Against IDS Evasion

- Shut down switch ports associated with known attack hosts.
- Perform an in-depth analysis of ambiguous network traffic for all possible threats.
- Use TCP FIN or Reset (RST) packet to terminate malicious TCP sessions.
- Look for the nop opcode other than 0x90 to defend against the polymorphic shellcode problem.
- Train users to identify attack patterns and regularly update/patch all the systems and network devices.
- Deploy IDS after a thorough analysis of the network topology, nature of network traffic, and number of hosts to monitor.
- Use a traffic normalizer to remove potential ambiguity from the packet stream before it reaches the IDS.
- Ensure that IDS normalize fragmented packets and allow those packets to be reassembled in the proper order.
- Define DNS server for client resolver in routers or similar network devices.
- Harden the security of all communication devices such as modems, routers, etc.
- If possible, block ICMP TTL expired packets at the external interface level and change the TTL field to a considerable value, ensuring that the end host always receives the packets.
- Regularly update the antivirus signature database.
- Use a traffic normalization solution at the IDS to protect the system from evasions.
- Store the attack information (attacker IP, victim IP, timestamp) for future analysis.

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

How to Defend Against Firewall Evasion

1. The configuration of the firewall should be done in such a way that the IP addresses of intruders should be filtered out
2. Set the firewall ruleset to deny all traffic and enable only the services required
3. If possible, create a unique user ID to run the firewall services, rather than running the services using the administrator or root IDs
4. Configure a remote syslog server and apply strict measures to protect it from malicious users
5. Monitor the firewall logs at regular intervals and investigate all suspicious log entries found
6. By default, disable all FTP connections to or from the network
7. Catalog and review all inbound and outbound traffic allowed through the firewall
8. Run regular risk queries to identify vulnerable firewall rules
9. Monitor user access to the firewalls and restrict who can modify the firewall configuration
10. Specify the source and destination IP addresses as well as the ports
11. Notify the security policy administrator on firewall changes and document them
12. Control physical access to the firewall
13. Take regular backups of the firewall ruleset and configuration files
14. Schedule regular firewall security audits

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

How to Defend Against Firewall Evasion

- The firewall should be configured such that the IP address of an intruder should be filtered out.
- Set the firewall rule set to deny all traffic and enable only the services required.
- If possible, create a unique user ID to run the firewall services instead of running the services using the administrator or root ID.
- Configure a remote syslog server and adopt strict measures to protect it from malicious users.
- Monitor firewall logs at regular intervals and investigate all suspicious log entries found.
- By default, disable all FTP connections to or from the network.
- Catalog and review all inbound and outbound traffic allowed through the firewall.
- Run regular risk queries to identify vulnerable firewall rules.
- Monitor user access to firewalls and control who can modify the firewall configuration.
- Specify the source and destination IP addresses as well as the ports.
- Notify the security policy administrator about firewall changes and document them.
- Control physical access to the firewall.
- Take regular backups of the firewall rule set and configuration files.
- Schedule regular firewall security audits.

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:
  - IDS, IPS, firewall, and honeypot concepts and solutions
  - Various techniques to bypass IDSs and firewalls
  - Various IDS/Firewall evasion tools
  - How to detect and defeat honeypots
  - We concluded with a detailed discussion on various countermeasures that should be employed in order to prevent IDS/Firewall evasion attempts by threat actors
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform web server hacking to get valuable information such as credit card numbers and passwords

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

Module Summary

This module discussed different IDS, IPS, firewall, and honeypot concepts and solutions. It also described various techniques for bypassing IDS and firewalls. In addition, it illustrated various IDS/firewall evasion tools. Further, it explained how to detect and defeat honeypots. Finally, it ended with a detailed discussion of various countermeasures to be adopted to prevent IDS/Firewall evasion attempts by threat actors.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen-testers perform web server hacking to gain valuable information such as credit card numbers and passwords.

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