



Ethical Hacking Essentials (EHE)

Master of Science in Cybersecurity

1



Dr. Kamal Alieyan

Everyone Smart University

Faculty of IT – 2022/2023

EHE

Ethical Hacking Essentials

SECURITY BREACH

INTRUSION DETECTED

HACKING DETECTED

Module 06

Network Level Attacks and Countermeasures



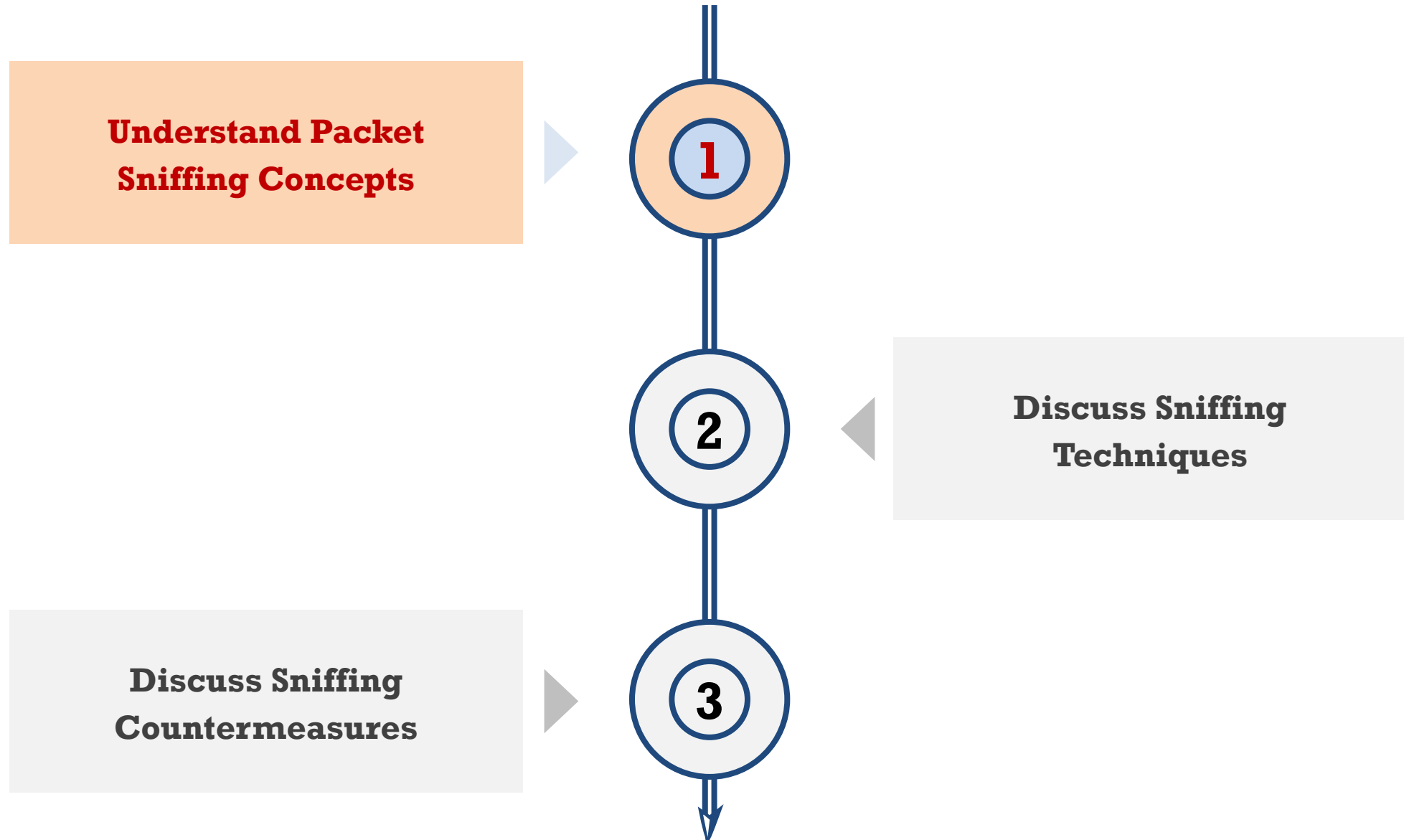
Module Objectives

- 1 Understanding Packet Sniffing and Types of Sniffing
- 2 Understanding Various Sniffing Techniques and Tools
- 3 Understanding Different Sniffing Countermeasures
- 4 Overview of Different Types of DoS and DDoS Attacks
- 5 Understanding Different DoS/DDoS Attack Tools
- 6 Understanding Different DoS/DDoS Attack Countermeasures and Protection Tools
- 7 Overview of Session Hijacking and Types of Session Hijacking
- 8 Understanding Different Session Hijacking Tools and Countermeasures



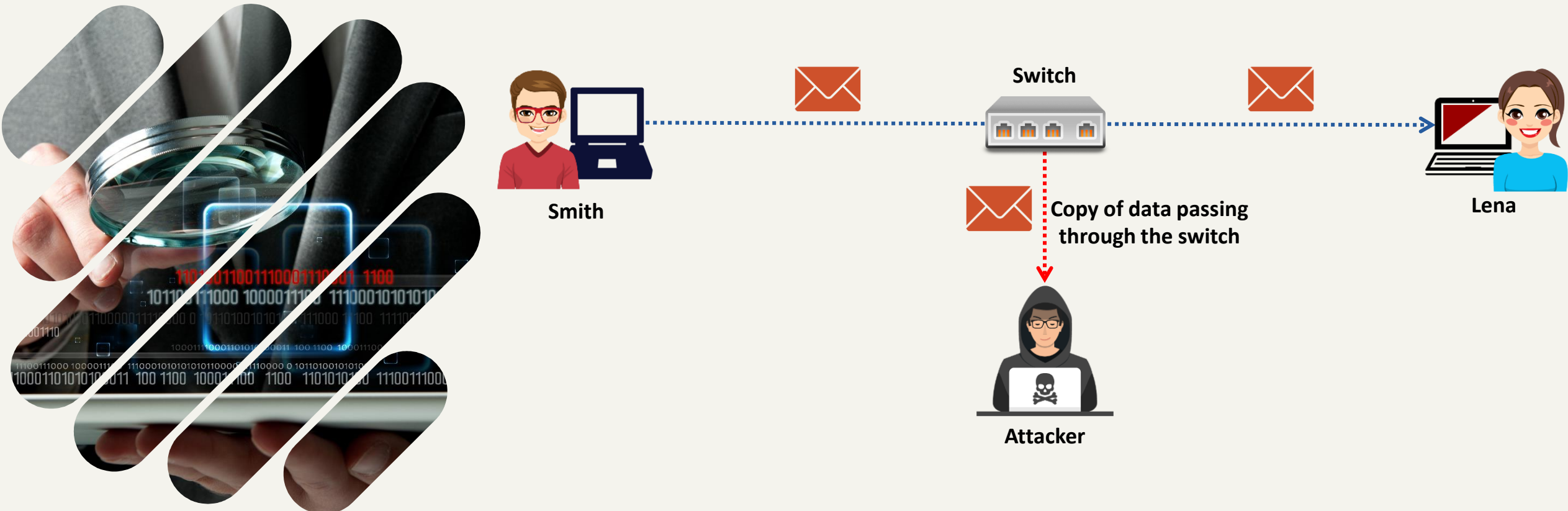
Sniffing

Module Flow



Packet Sniffing

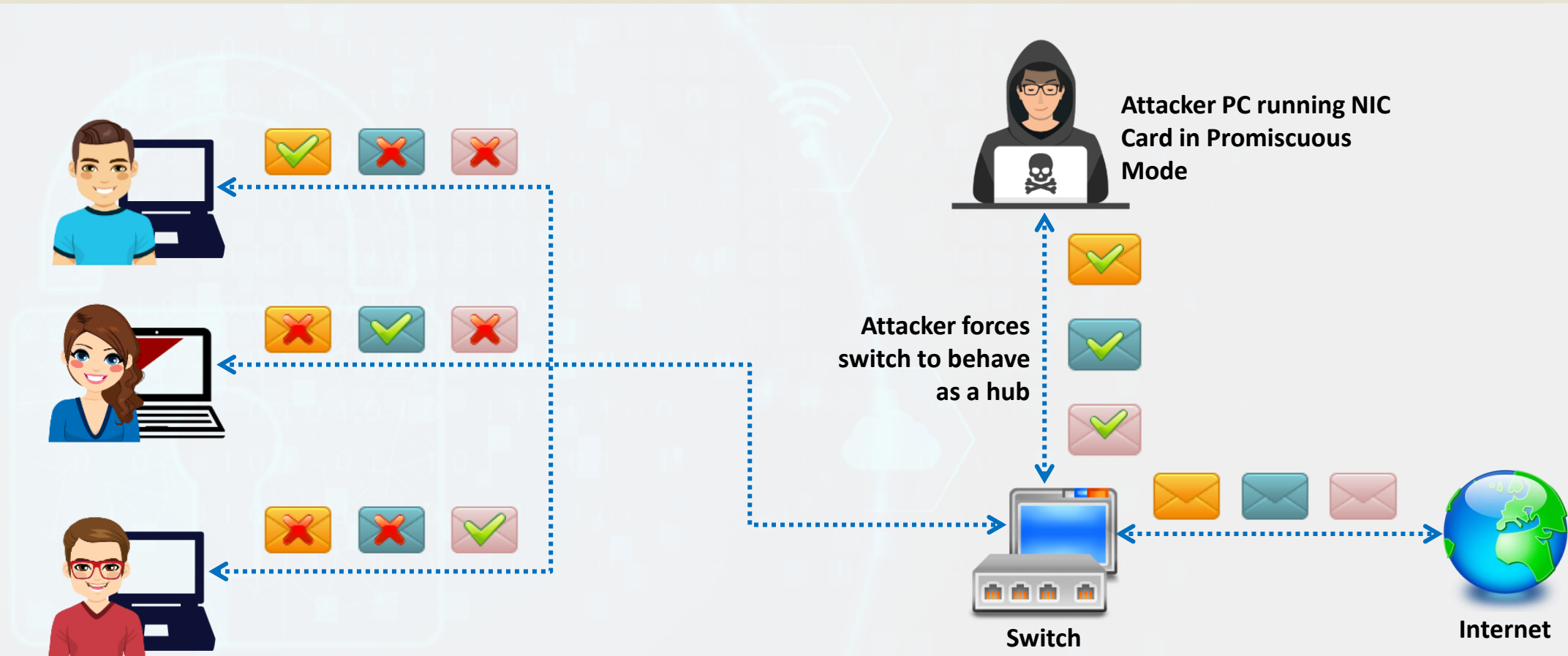
- ❑ Packet sniffing is the process of **monitoring and capturing all data packets** passing through a given network using a software application or hardware device
- ❑ It allows an attacker to observe and **access the entire network traffic** from a given point in order to **gather sensitive information**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



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



Types of Sniffing

Passive Sniffing



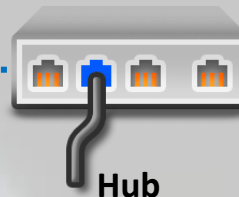
Passive sniffing refers to sniffing through a **hub**, wherein the traffic is sent to all ports



It involves monitoring packets sent by others without sending **any additional data packets** in the network traffic



Attacker



Hub



LAN



Note: Passive sniffing provides significant stealth advantages over active sniffing

Types of Sniffing (Cont'd)

Active Sniffing

- ❑ Active sniffing is used to sniff a **switch-based network**
- ❑ It 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 |



How an Attacker Hacks the Network Using Sniffers

01

An attacker connects his desktop/laptop to a switch port



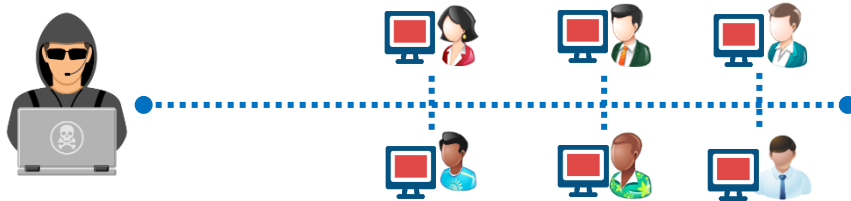
04

He/she runs discovery tools to learn about network topology



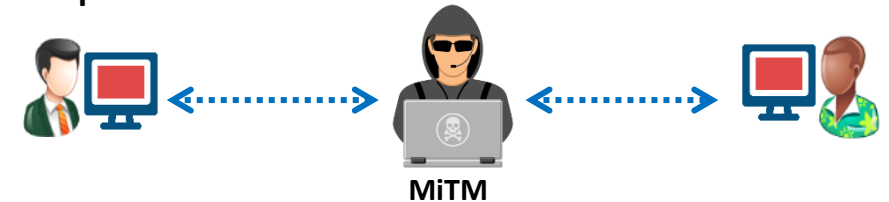
02

He/she identifies a victim's machine to target his/her attacks



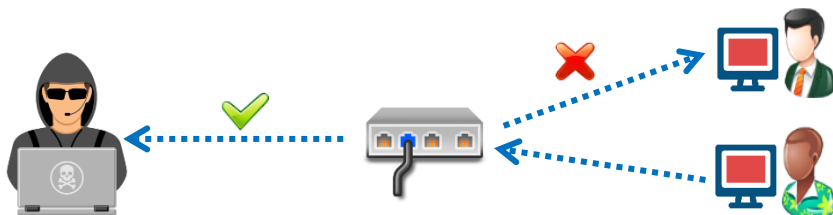
05

He/she poisons the victim's machine by using ARP spoofing techniques



03

The traffic destined for the victim's machine is redirected to the attacker



06

The hacker extracts passwords and sensitive data from the redirected traffic



Protocols Vulnerable to Sniffing



Telnet and Rlogin

- ☐ Keystrokes including usernames and passwords are sent in clear text



HTTP

- ☐ Data is sent in clear text



POP

- ☐ Passwords and data are sent in clear text



IMAP

- ☐ Passwords and data are sent in clear text



SMTP and NNTP

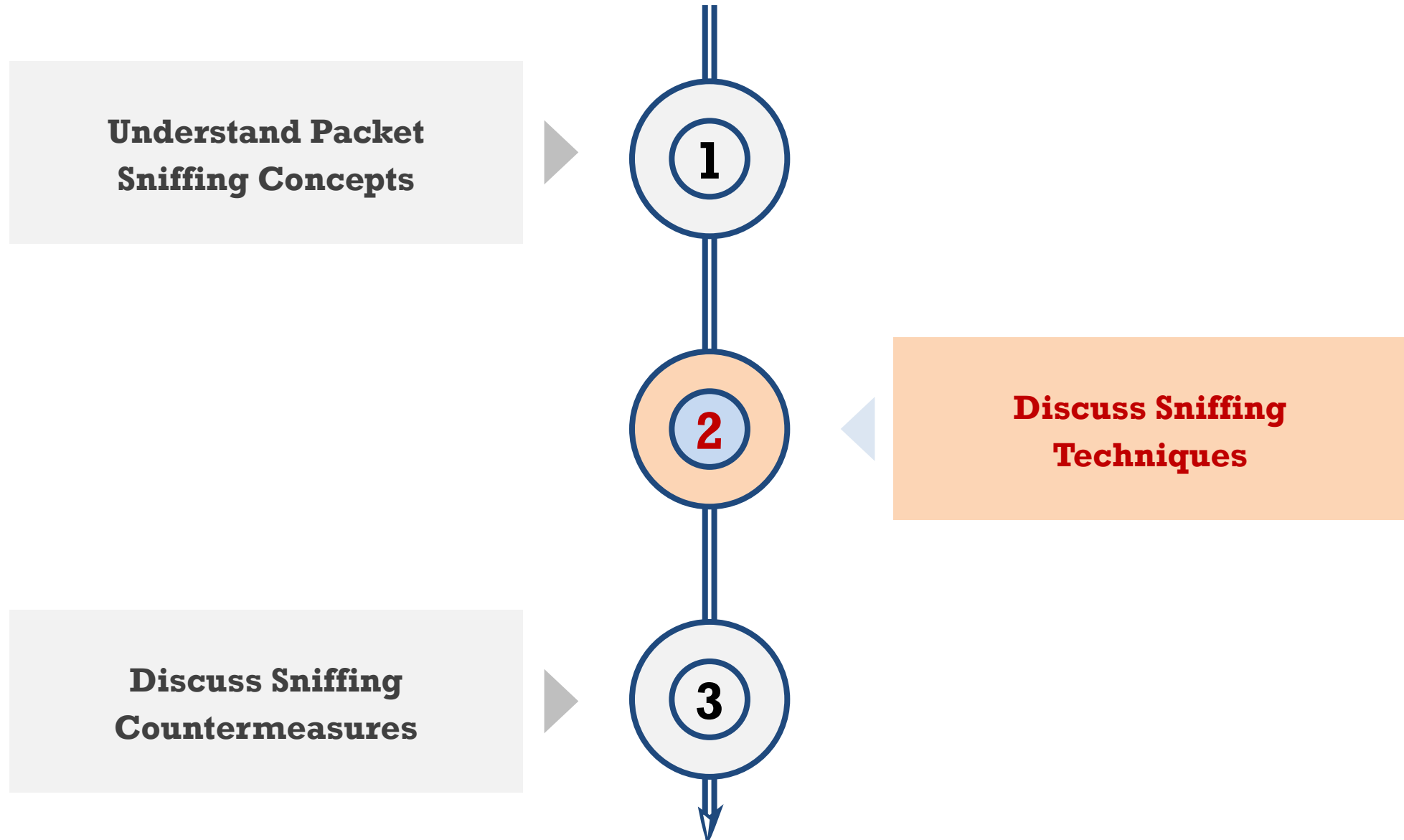
- ☐ Passwords and data are sent in clear text



FTP

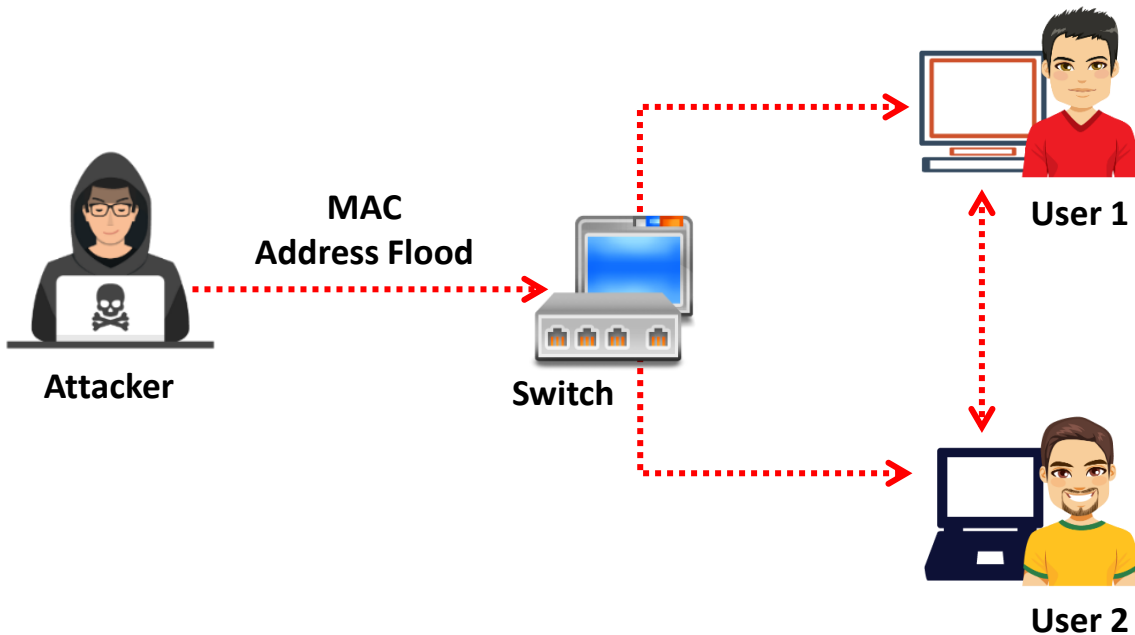
- ☐ Passwords and data are sent in clear text

Module Flow



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



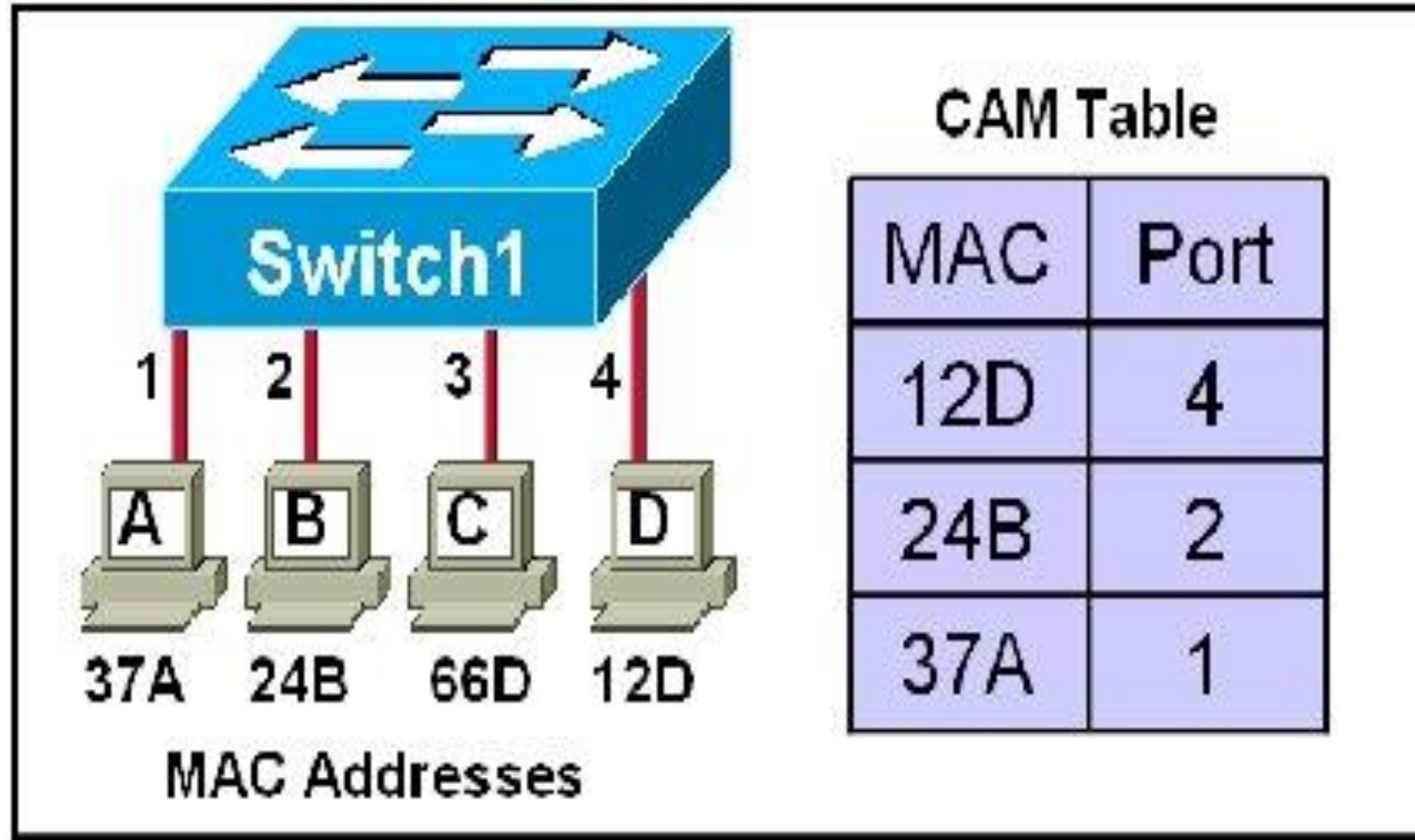
Mac Flooding Switches with macof

- macof** is a Unix/Linux tool that **floods the switch's CAM tables** (131,000 per min) by sending bogus MAC entries

```
Parrot Terminal
File Edit View Search Terminal Help
[~]-[root@parrot]-[~]
#macof -i eth0 -n 10
5d:2f:98:3c:94:6d 9a:5:5b:1f:75:13 0.0.0.0.21067 > 0.0.0.0.45855: S 746864890:74686
4890(0) win 512
7f:e8:cc:4a:51:59 74:88:e0:40:8b:3c 0.0.0.0.39850 > 0.0.0.0.49263: S 586168580:5861
68580(0) win 512
14:83:59:7f:2f:fc 4:bb:21:27:82:db 0.0.0.0.48709 > 0.0.0.0.15710: S 1044800461:1044
800461(0) win 512
3:1e:f4:12:9:e 9f:84:98:37:ec:55 0.0.0.0.9433 > 0.0.0.0.62409: S 1330659371:1330659
371(0) win 512
53:e8:38:25:c7:42 3f:4c:6a:1f:e1:d6 0.0.0.0.57830 > 0.0.0.0.6910: S 628366088:62836
6088(0) win 512
60:7c:41:4f:e9:c2 a6:94:65:25:c7:ad 0.0.0.0.58215 > 0.0.0.0.56497: S 447162501:4471
62501(0) win 512
27:d5:2e:56:23:74 cb:b9:b9:59:8d:67 0.0.0.0.17385 > 0.0.0.0.28393: S 1018850322:101
8850322(0) win 512
35:23:c:5e:59:b6 8f:6a:9d:2b:ea:ec 0.0.0.0.27895 > 0.0.0.0.61217: S 1066823910:1066
823910(0) win 512
95:a0:68:c:1d:fc b9:f1:a4:7e:9:67 0.0.0.0.60630 > 0.0.0.0.3405: S 99214739:99214739
(0) win 512
1e:e:ab:4:d3:16 af:dd:77:46:4e:26 0.0.0.0.56144 > 0.0.0.0.16970: S 1864068613:18640
68613(0) win 512
```

<https://www.monkey.org>

MAC Flooding



DHCP Starvation Attack

1

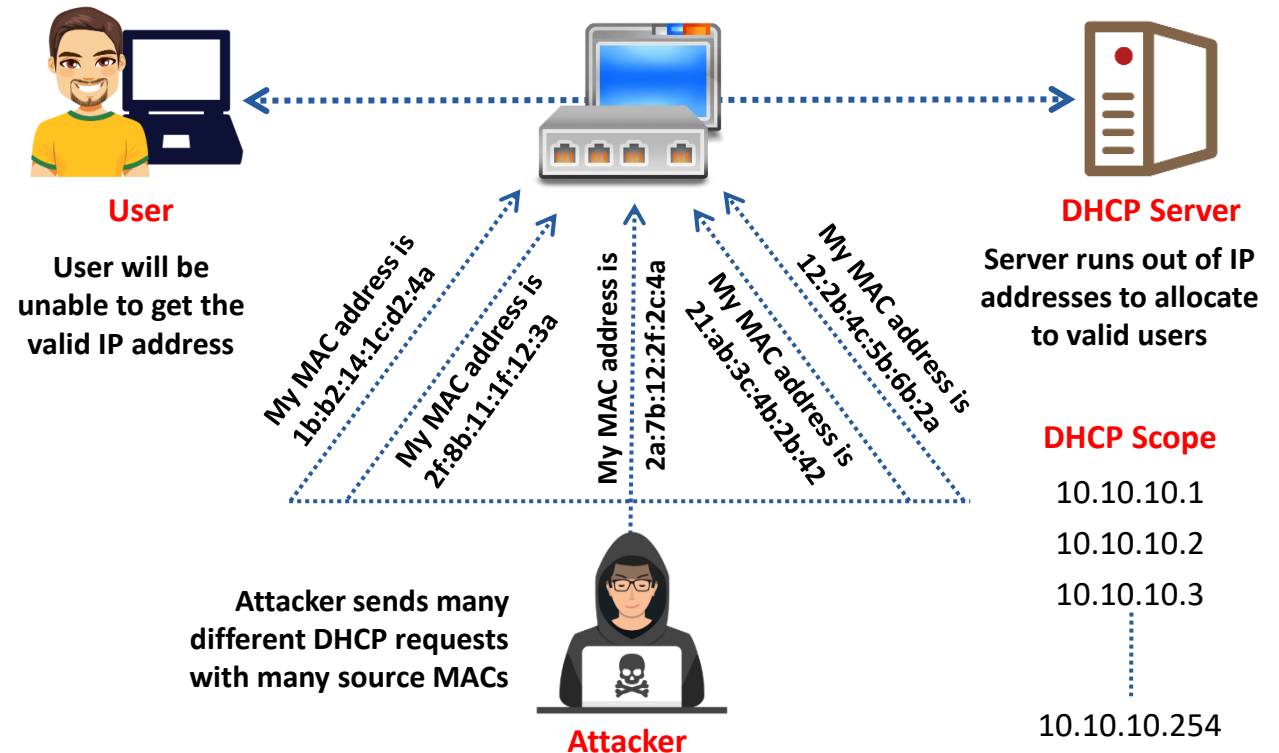
DHCP is a **configuration protocol** that assigns valid IP addresses to host systems out of a pre-assigned DHCP pool

2

DHCP starvation attack is a process of **inundating DHCP servers** with fake DHCP requests and using all the available IP addresses

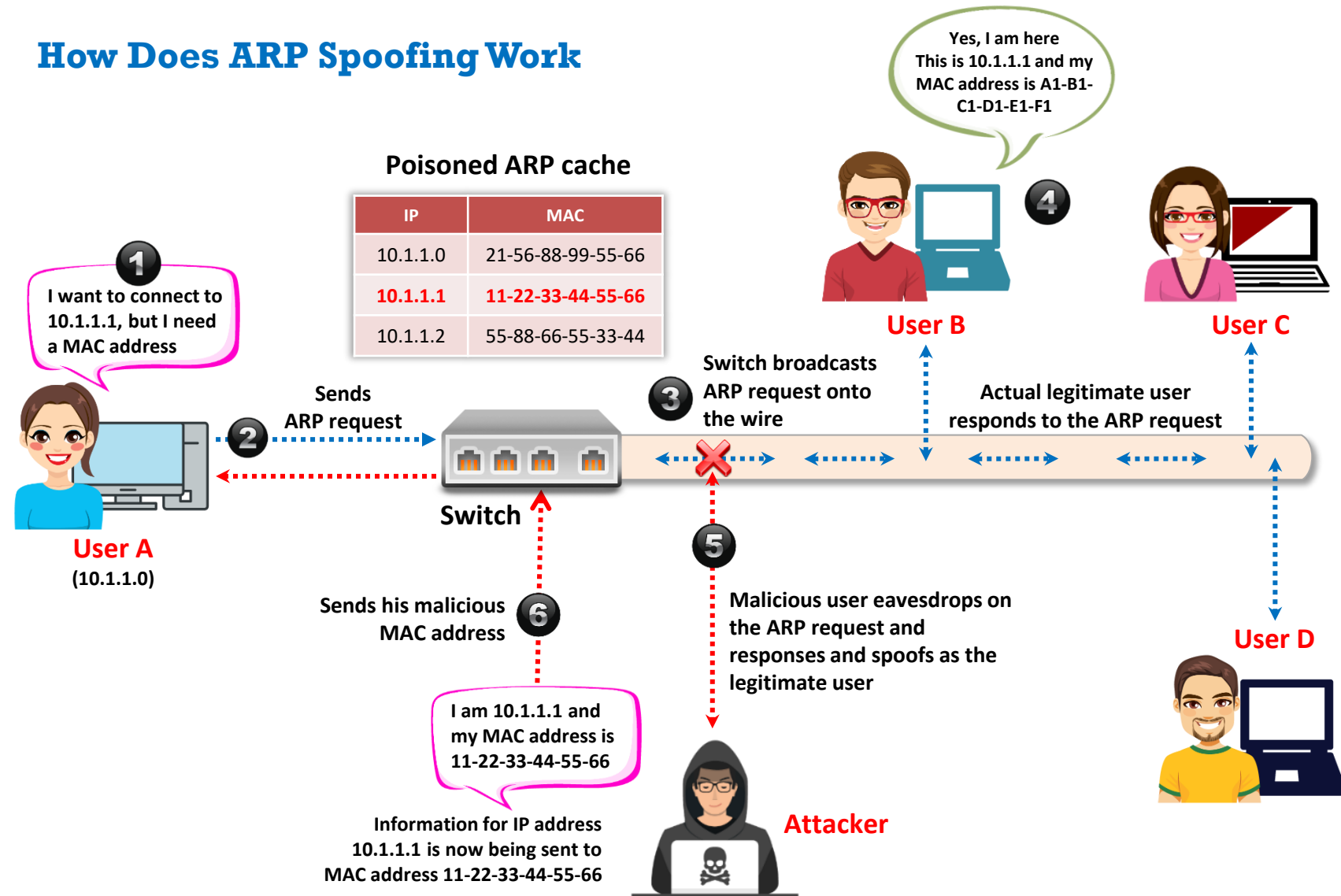
3

This results in a **denial-of-service attack**, where the DHCP server cannot issue new IP addresses to genuine host requests



ARP Spoofing Attack

How Does ARP Spoofing Work



ARP Poisoning Tools



arpspoof

arpspoof **redirects packets** from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies

```
Parrot Terminal
File Edit View Search Terminal Help
#arpspoof -i eth0 -t 10.10.10.2 10.10.10.10
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
```

Obtained ARP cache and MAC address is replaced with that of the attacker's system

```
Parrot Terminal
File Edit View Search Terminal Help
#arpspoof -i eth0 -t 10.10.10.10 10.10.10.2
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
```

Reverse command so that the attacker can send replies both ways

<https://linux.die.net>



BetterCAP

<https://www.bettercap.org>



Ettercap

<http://www.ettercap-project.org>



dsniff

<https://www.monkey.org>



MITMf

<https://github.com>

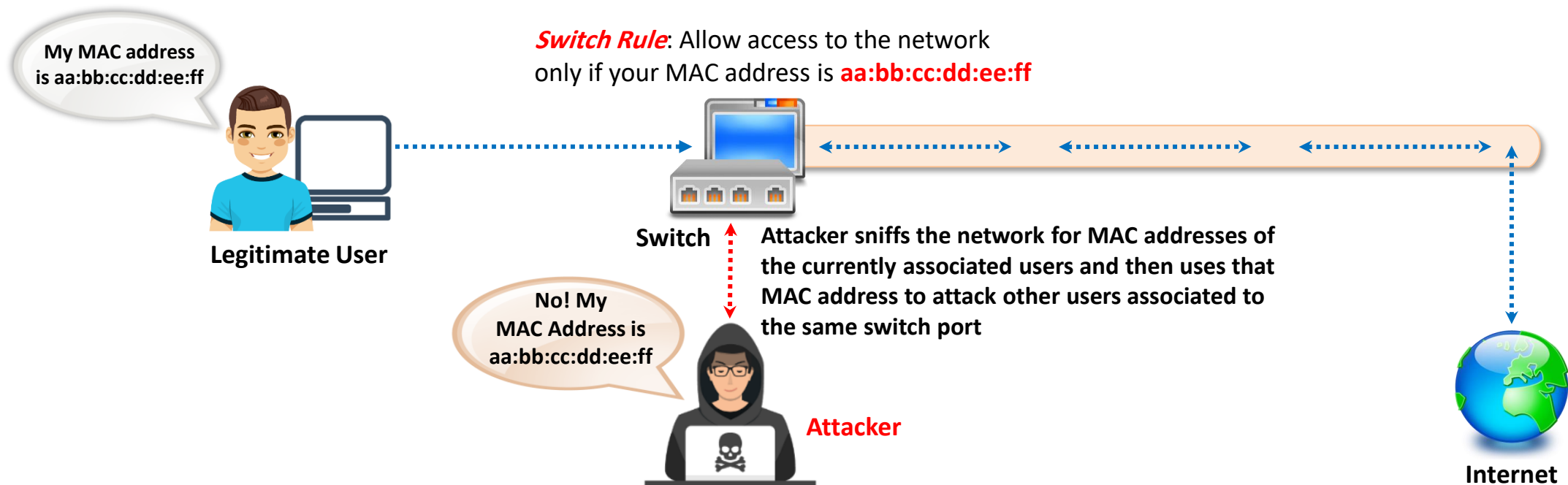


Arpoison

<https://sourceforge.net>

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

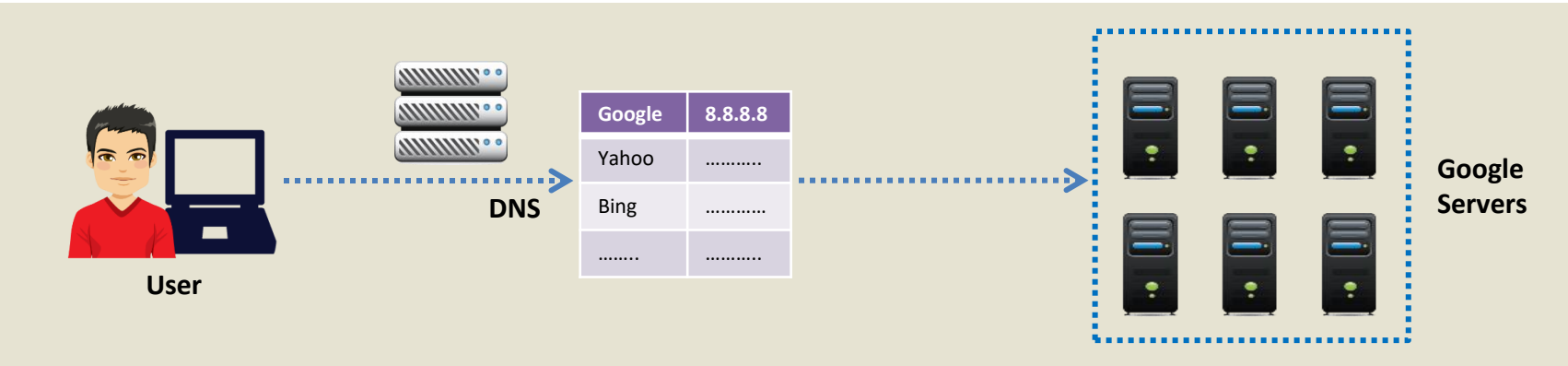




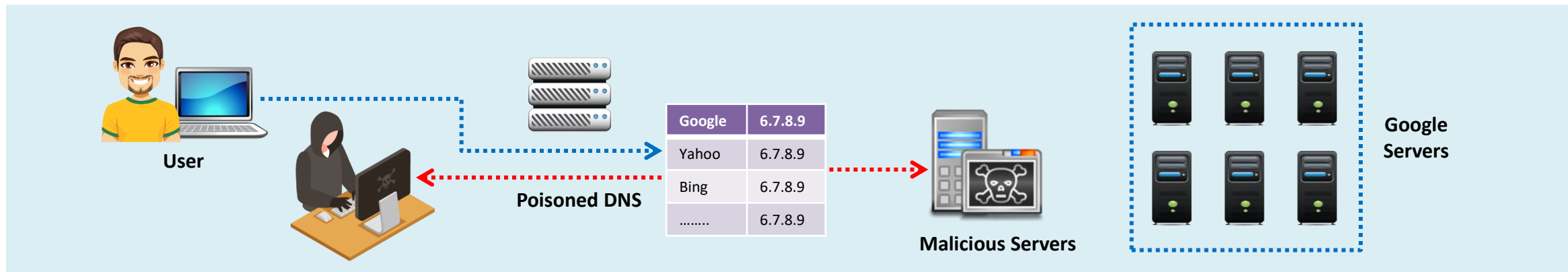
DNS Poisoning



Domain Name Server (DNS) poisoning is the **unauthorized manipulation** of IP addresses in the DNS cache



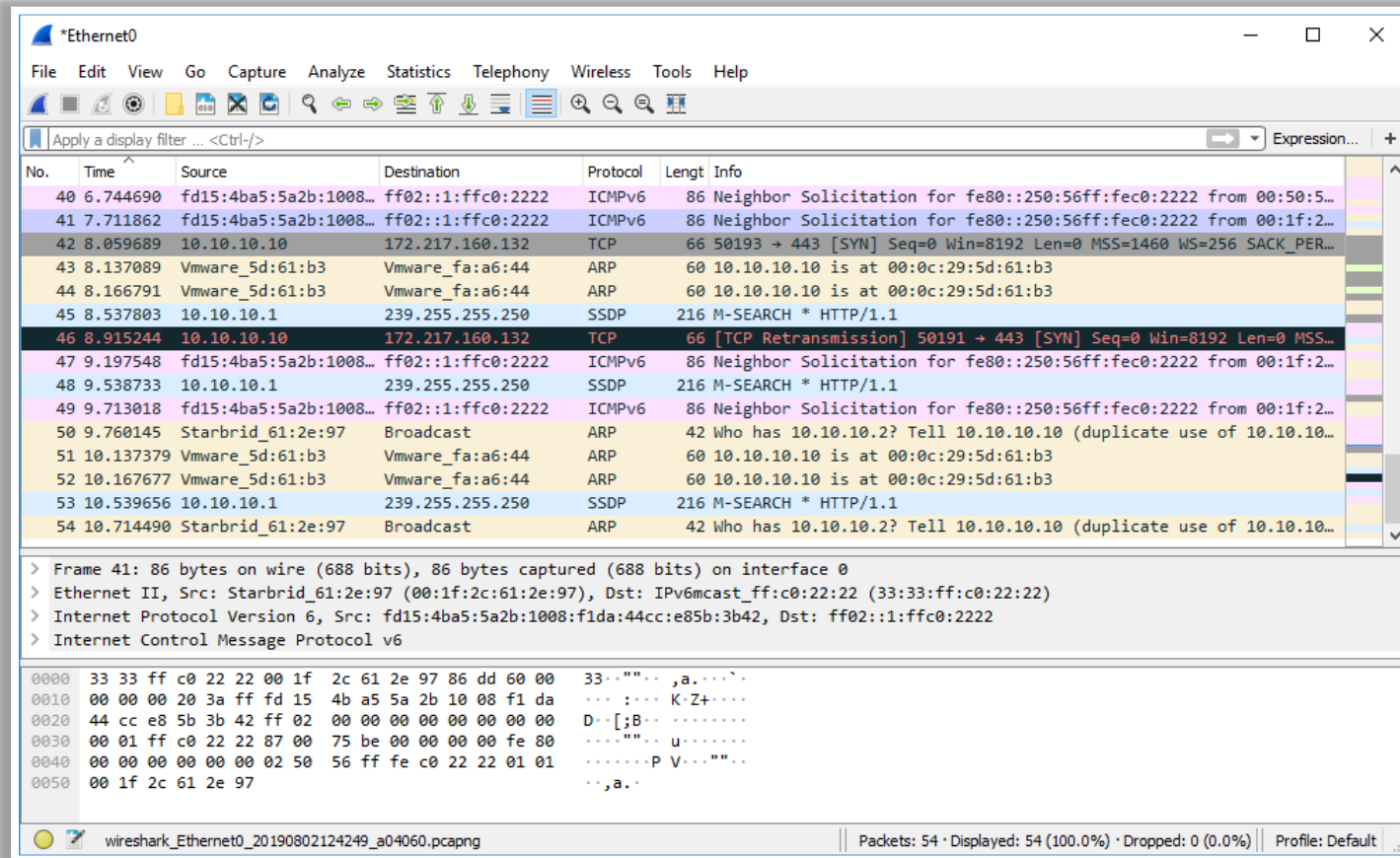
A corrupted DNS redirects a user request to a malicious website to perform **illegal activities**



Sniffing Tools: Wireshark

Wireshark

- ❑ Wireshark lets you **capture and interactively browse the traffic** running on a computer network



<https://www.wireshark.org>



SteelCentral Packet Analyzer
<https://www.riverbed.com>



Capsa Network Analyzer
<https://www.colasoft.com>



Observer Analyzer
<https://www.viavisolutions.com>

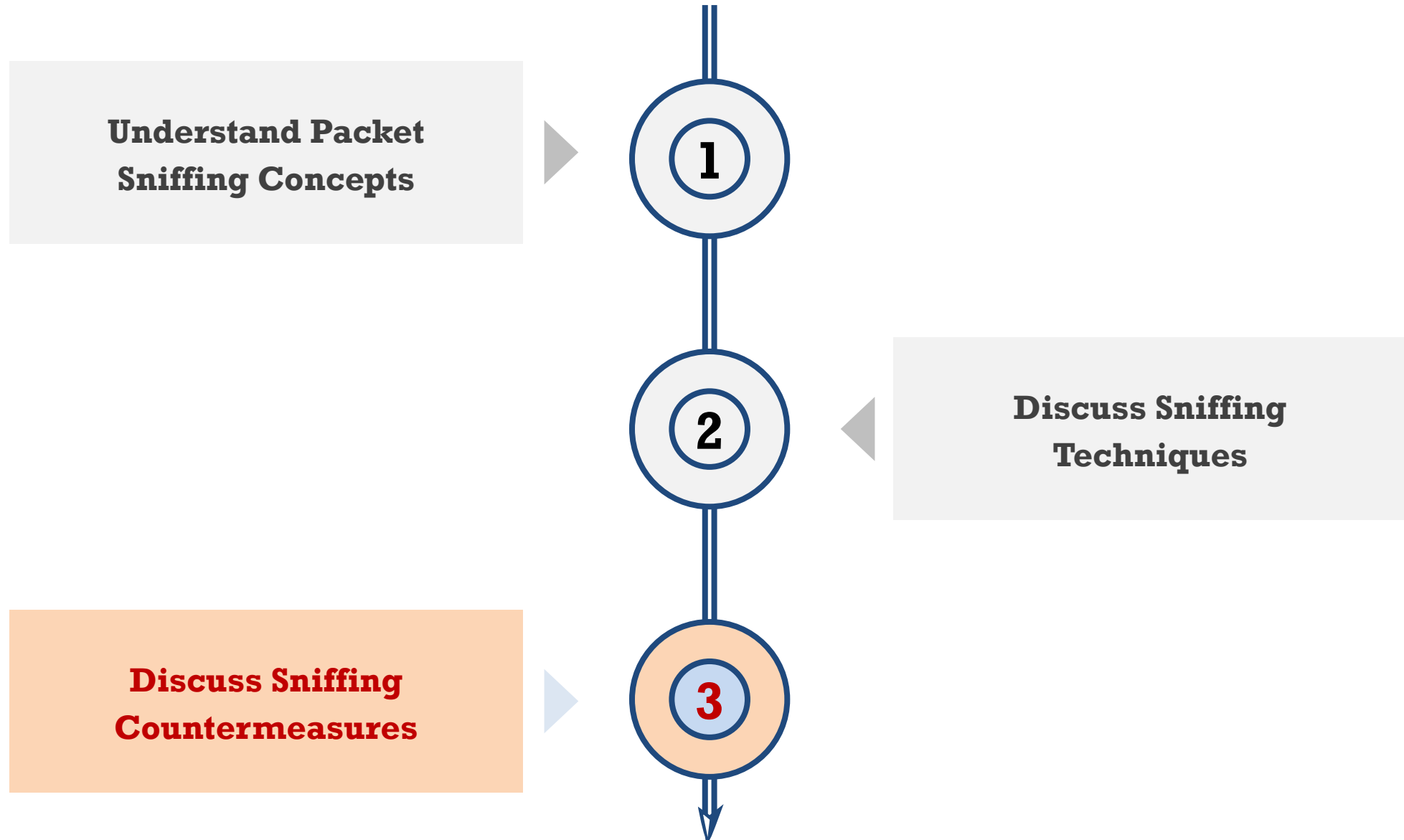


PRTG Network Monitor
<https://www.paessler.com>



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

Module Flow



Sniffing Countermeasures



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

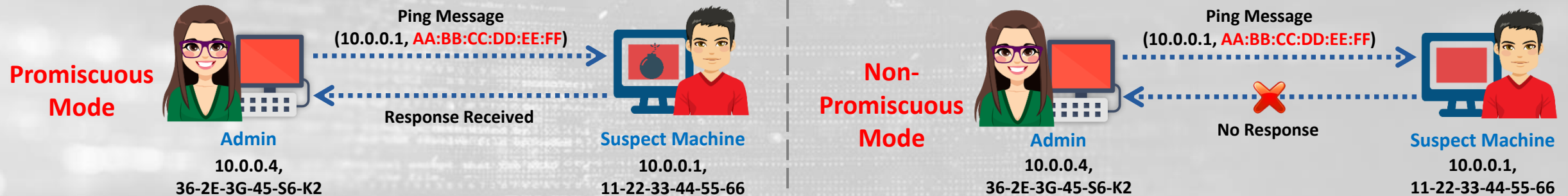


Use **static IP addresses** and **ARP tables** to prevent attackers from adding spoofed ARP entries for machines in the network



Turn off **network identification broadcasts**, and if possible, restrict the network to authorized users to protect the network from being discovered with sniffing tools

Sniffer Detection Techniques: Ping Method

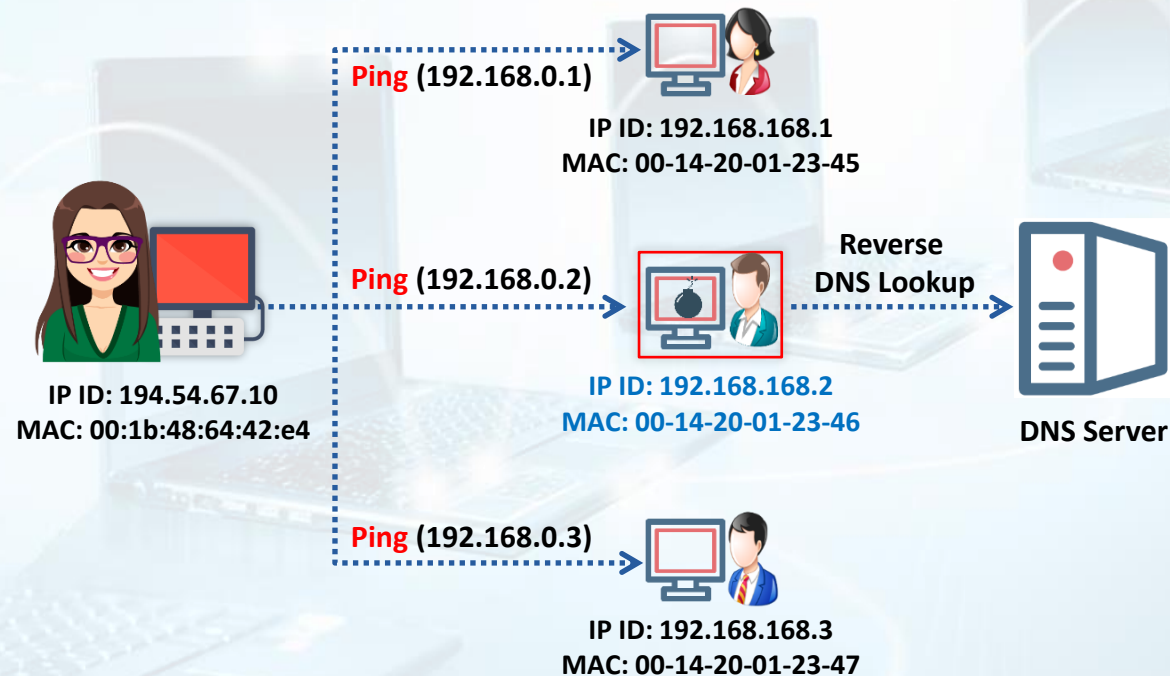


- ❑ Sends a ping request to the suspect machine with its IP address and an **incorrect MAC address**. The Ethernet adapter rejects it, as the MAC address does not match, whereas the suspect machine running the **sniffer responds** to it as it does not reject packets with a different MAC address

Sniffer Detection Techniques: 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

Sniffer Detection Techniques: ARP Method



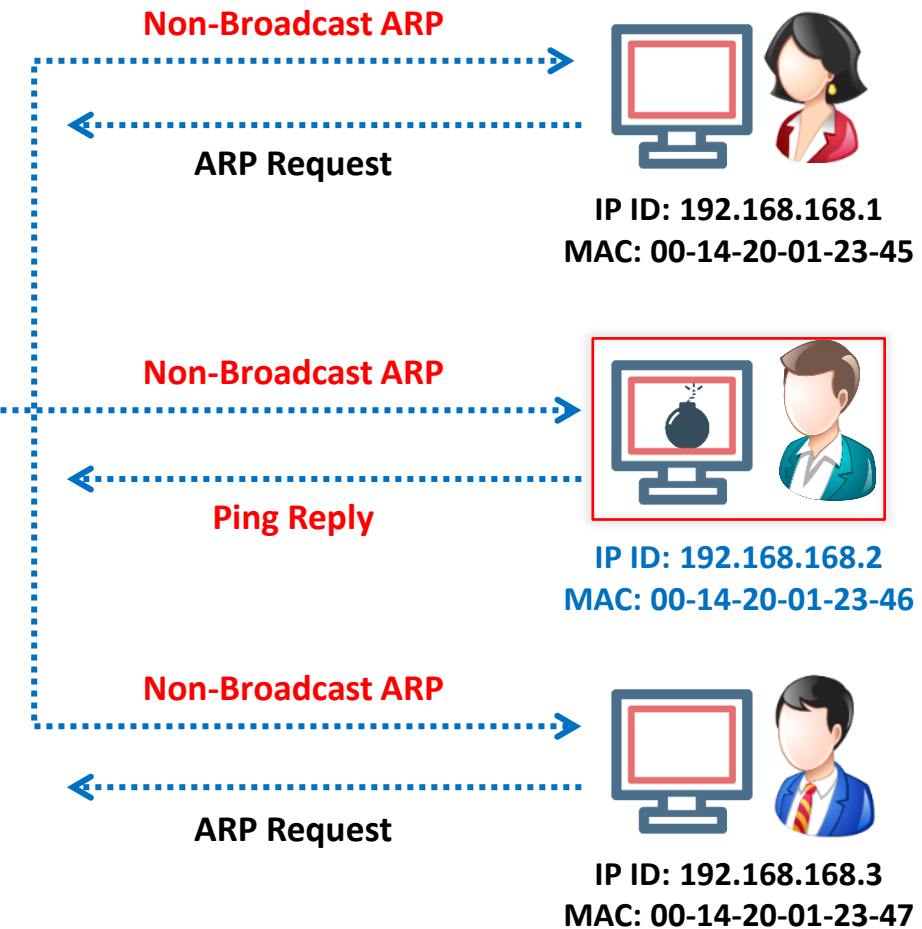
Only the machine in the promiscuous mode (machine C) **caches the ARP information** (IP and MAC address mapping)



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



IP ID: 194.54.67.10
MAC: 00:1b:48:64:42:e4





Denial-of-Service

Module Flow

1

Discuss Types of DoS and DDoS Attacks

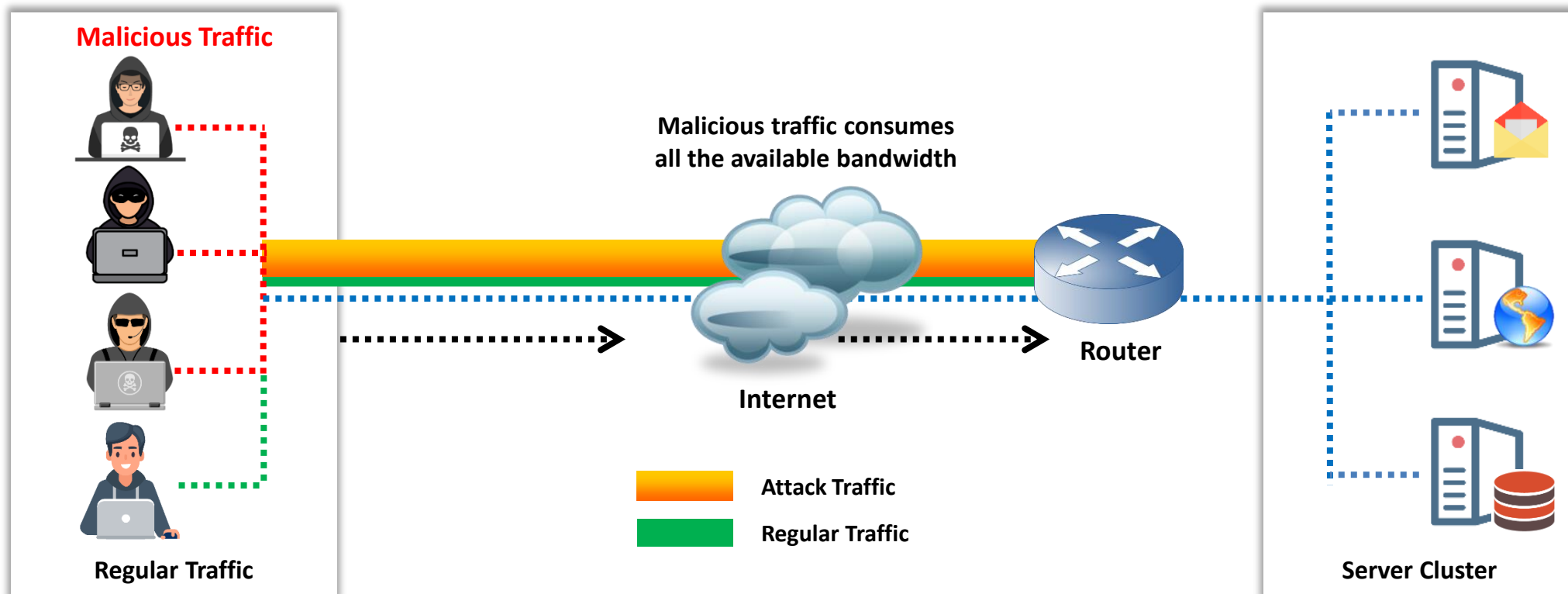
2

Discuss DoS and DDoS Attack Countermeasures



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
- ❑ Attackers flood the victim system with **non-legitimate service requests or traffic** to overload its resources

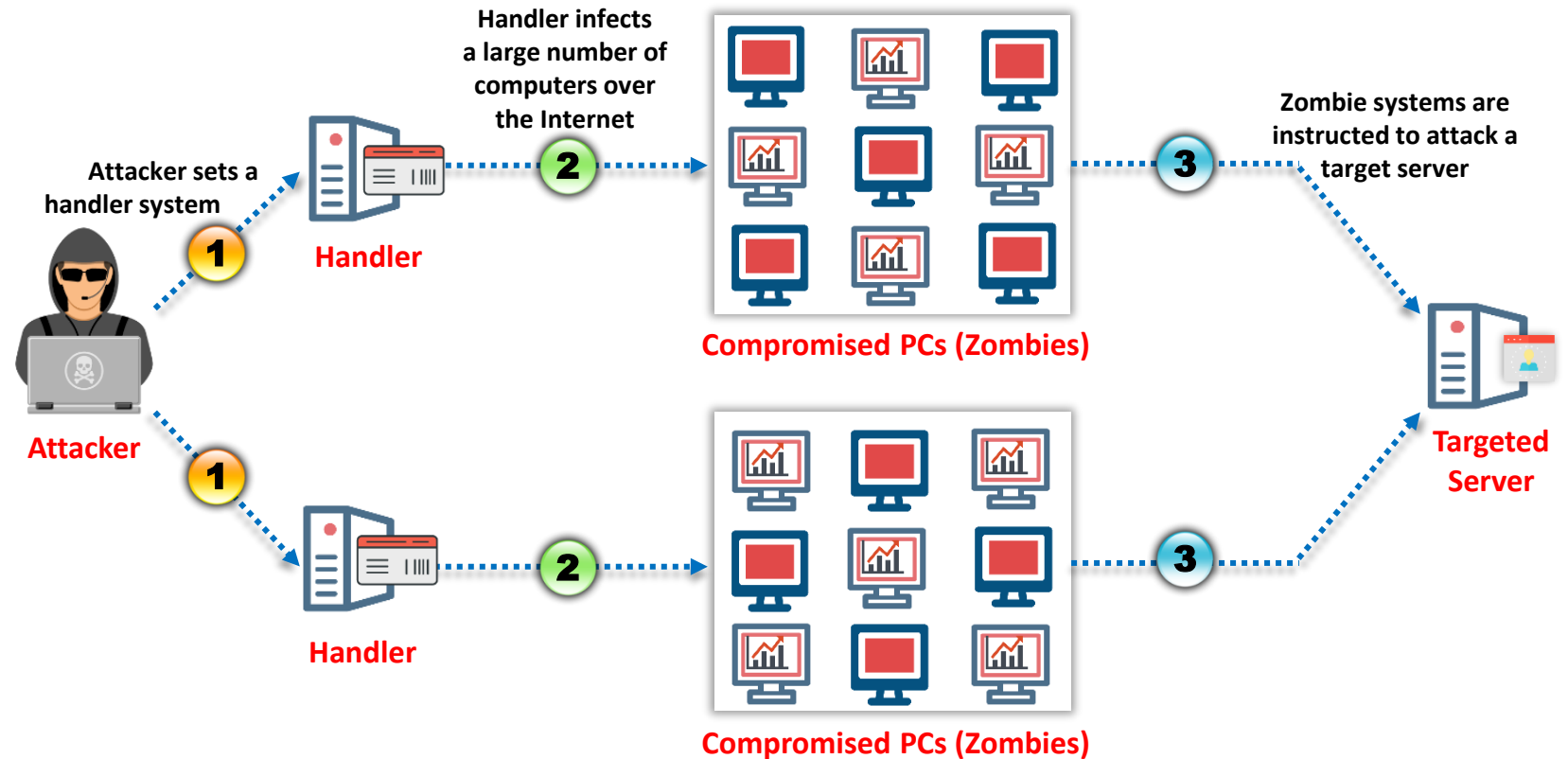


What is a DDoS Attack?

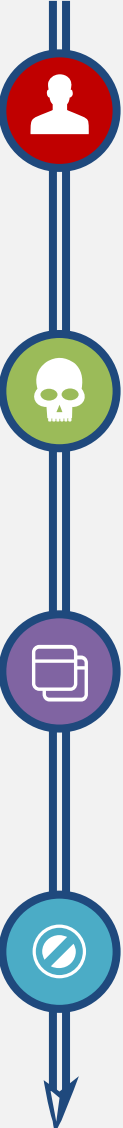


Distributed denial-of-service (DDoS) is a coordinated attack that involves a **multitude of compromised systems** (Botnet) attacking a single target, thereby denying service to users of the targeted system

How do DDoS Attacks Work?



DoS/DDoS Attack Techniques: UDP Flood Attack

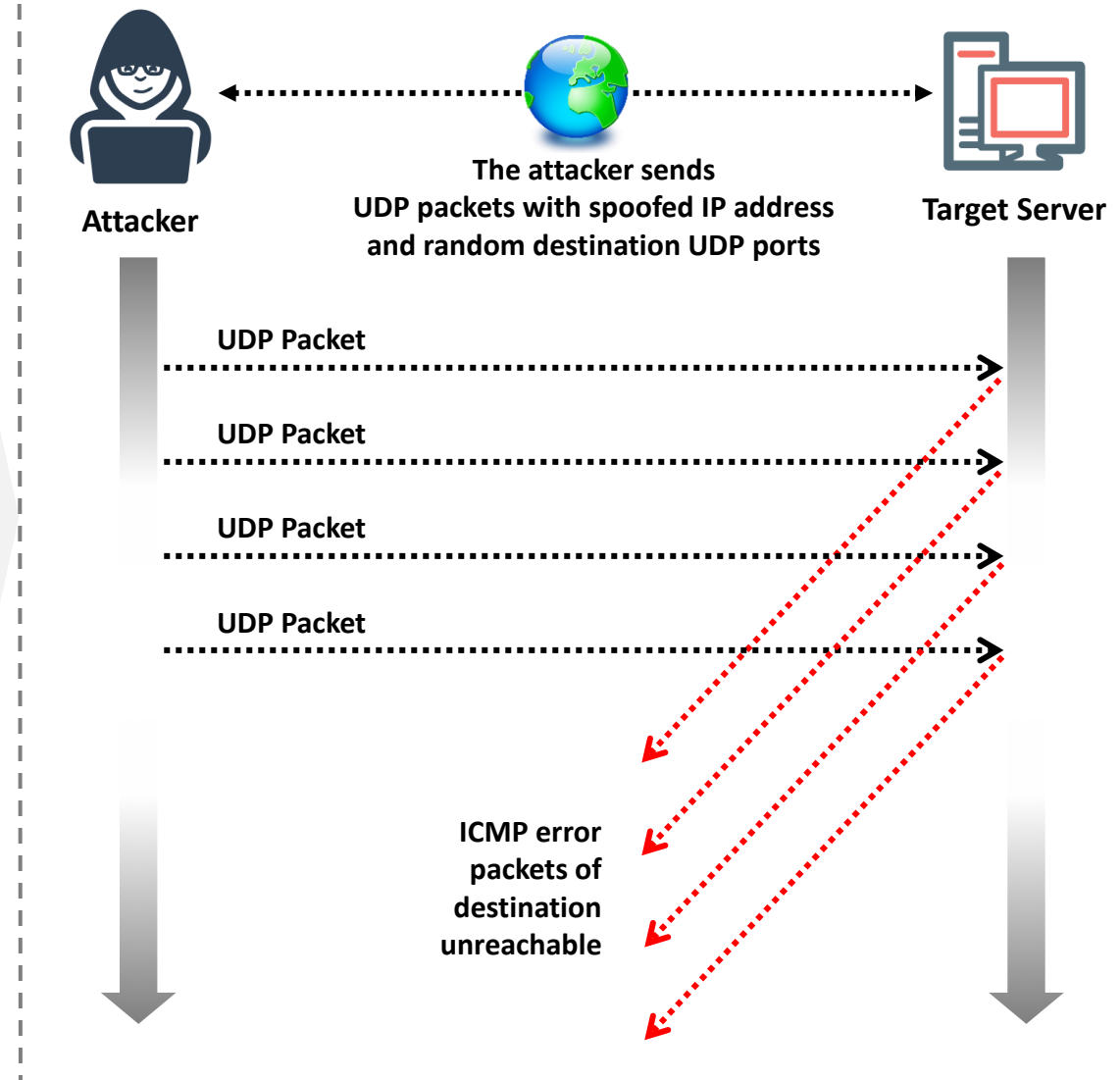


An attacker sends **spoofed UDP packets** at a very high packet rate to a remote host on random ports of a target server using a large source IP range

The flooding of UDP packets causes the server to repeatedly check for **non-existent applications** at the ports

Legitimate applications are inaccessible by the system and give an **error reply** with an ICMP “Destination Unreachable” packet

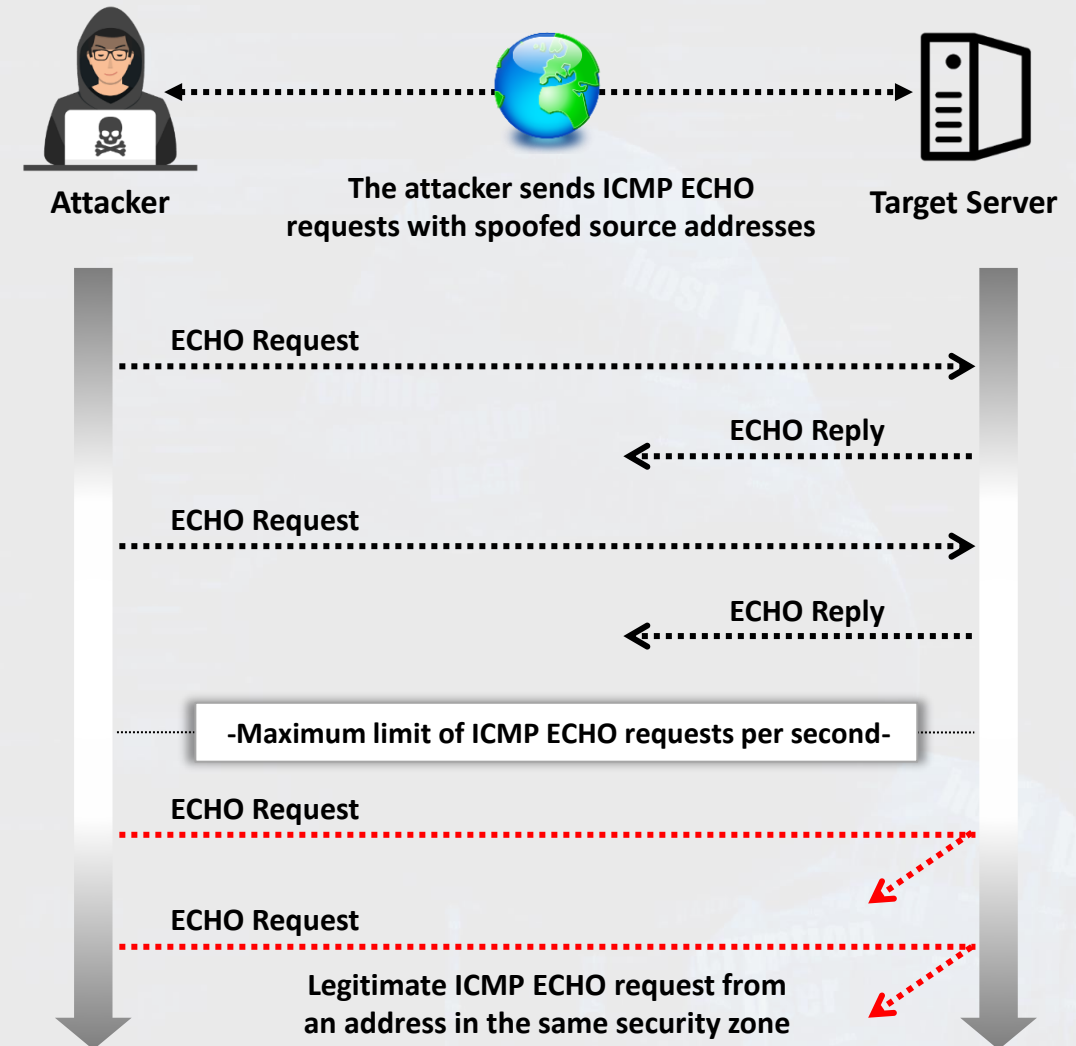
This attack consumes **network resources** and available bandwidth, exhausting the network until it goes offline



DoS/DDoS Attack Techniques: ICMP Flood Attack

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



DoS/DDoS Attack Techniques:

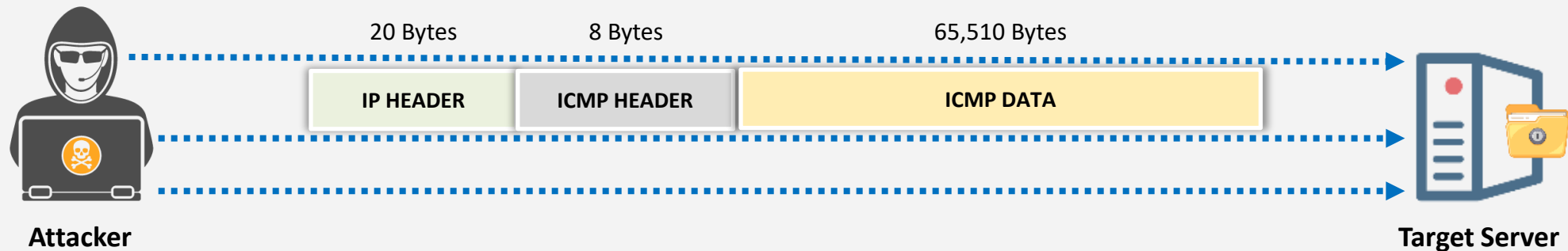
Ping of Death Attack



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



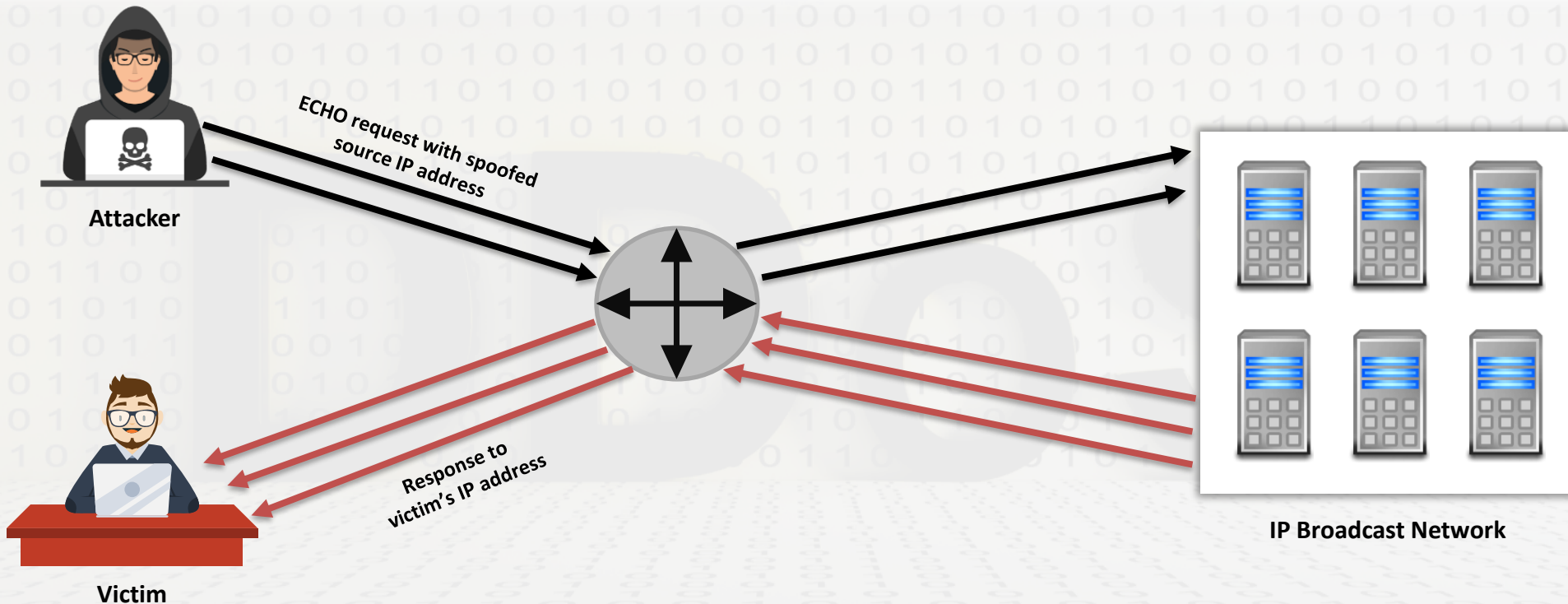
DoS/DDoS Attack Techniques: Smurf Attack



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



DoS/DDoS Attack Techniques: SYN Flood Attack



The attacker sends a large number of **SYN requests** with **fake source IP addresses** to the target server (victim)



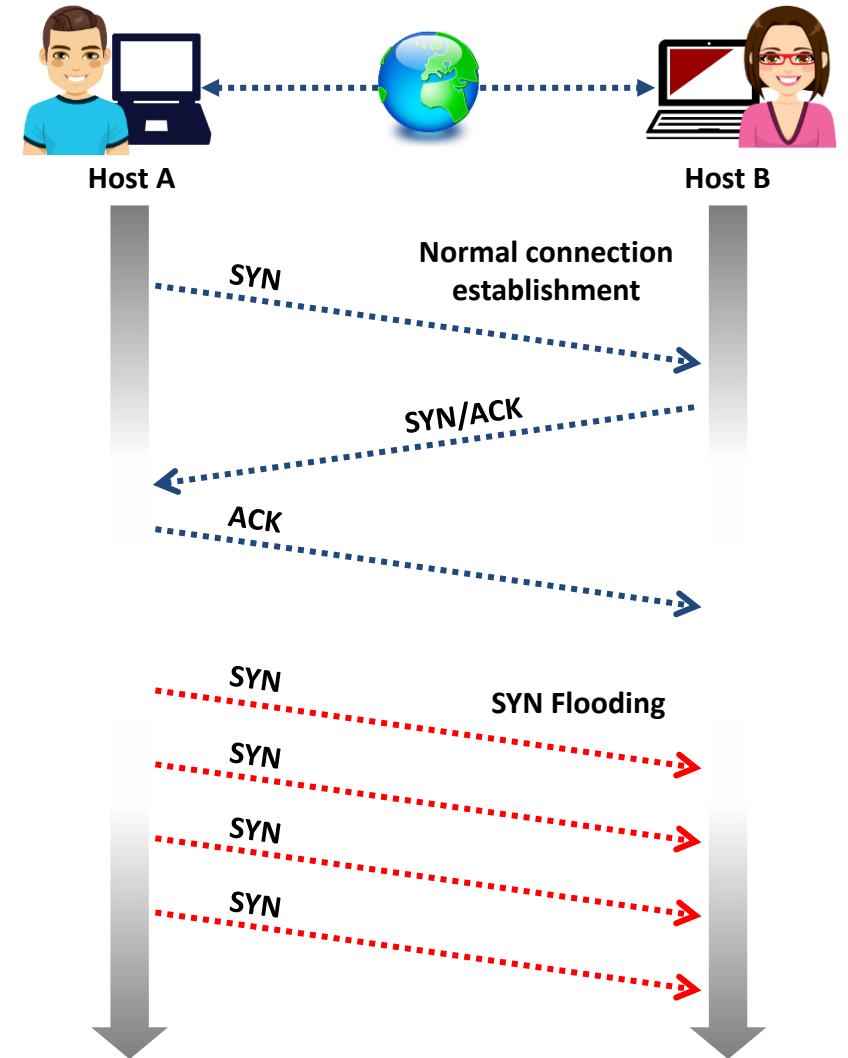
The target machine sends back a **SYN/ACK** in **response to the request** and waits for the ACK to complete the session setup



The target machine **does not get the response** because the **source address is fake**



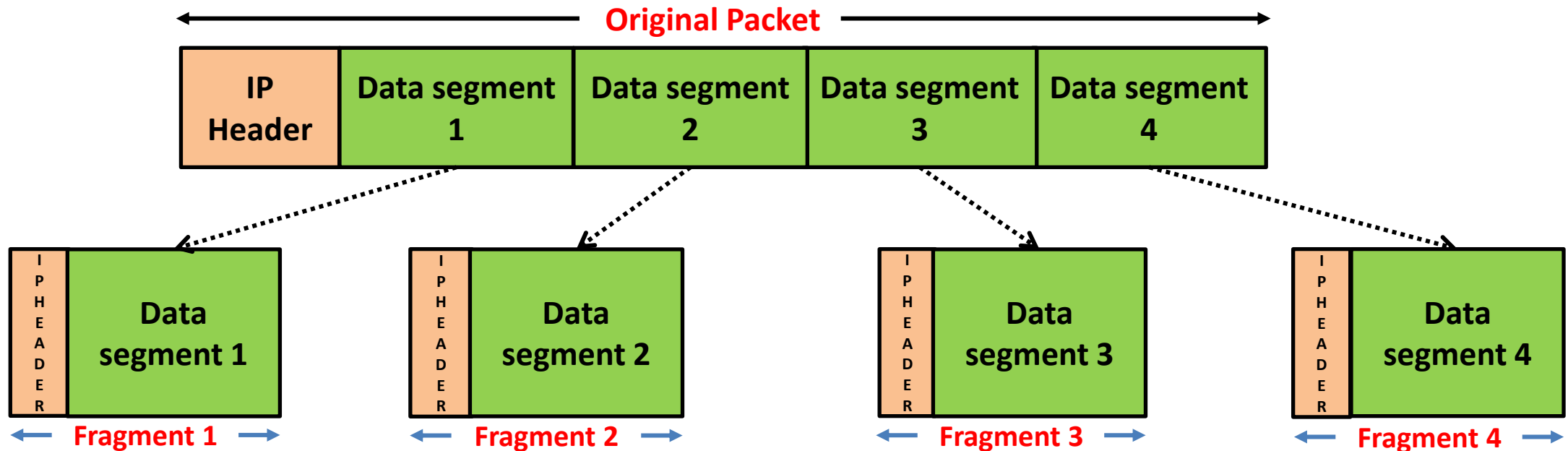
SYN flooding takes advantage of a flaw in the implementation of the **TCP three-way handshake** in most hosts



DoS/DDoS Attack Techniques: 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
- ❑ Reassembling and inspecting these large fragmented packets consumes excessive resources



DoS/DDoS Attack Techniques: Multi-Vector Attack

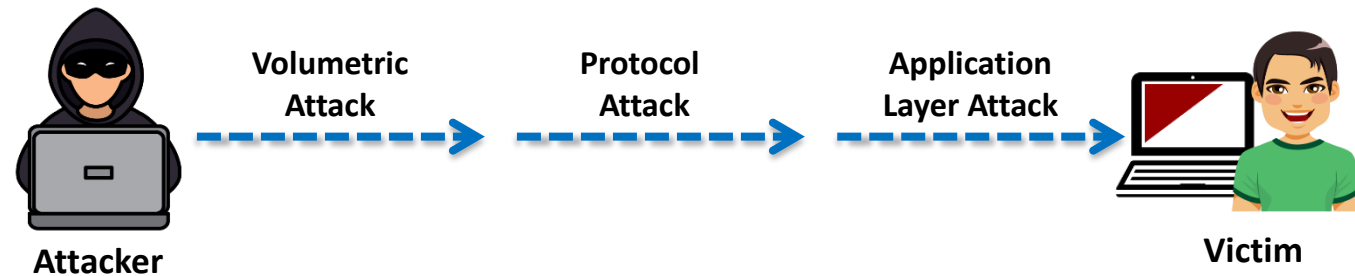


The attackers use **combinations of volumetric**, protocol, and application-layer attacks to disable the target system or service

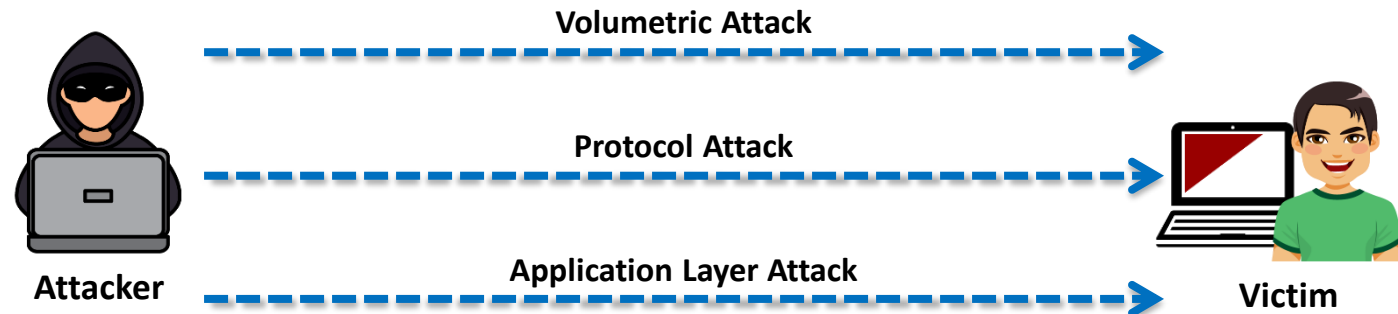


Attackers rapidly and repeatedly change the form of their DDoS attack (e.g., SYN packets, Layer 7)

Multi-Vector attack in sequence



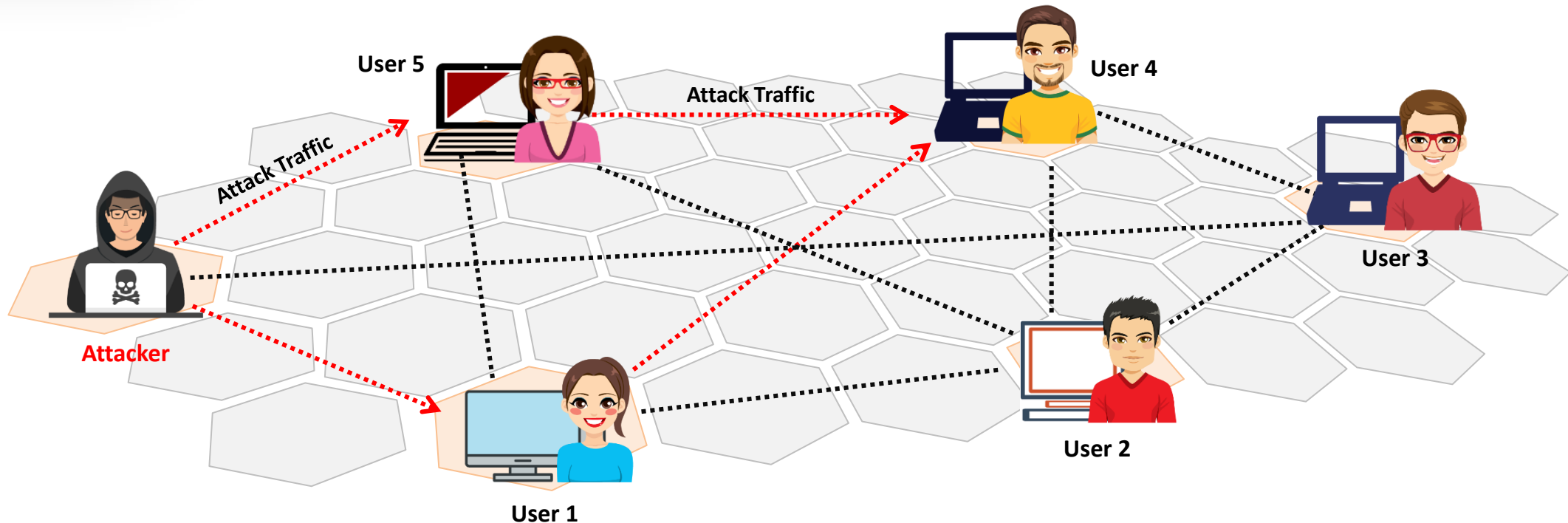
Multi-Vector attack in parallel



DoS/DDoS Attack Techniques: Peer-to-Peer Attack



- ❑ 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



DoS/DDoS Attack Techniques: Permanent Denial- of-Service Attack



Permanent DoS, also known as **phishing**, refers to attacks that cause irreversible damage to system hardware



Unlike other DoS attacks, it **sabotages the system hardware**, requiring the victim to replace or reinstall the hardware



This attack is carried out using a method known as **"bricking a system"**



Using this method, attackers send **fraudulent hardware updates** to the victims



Attacker

Sends email, IRC chats, tweets, posts, videos with fraudulent content for hardware updates

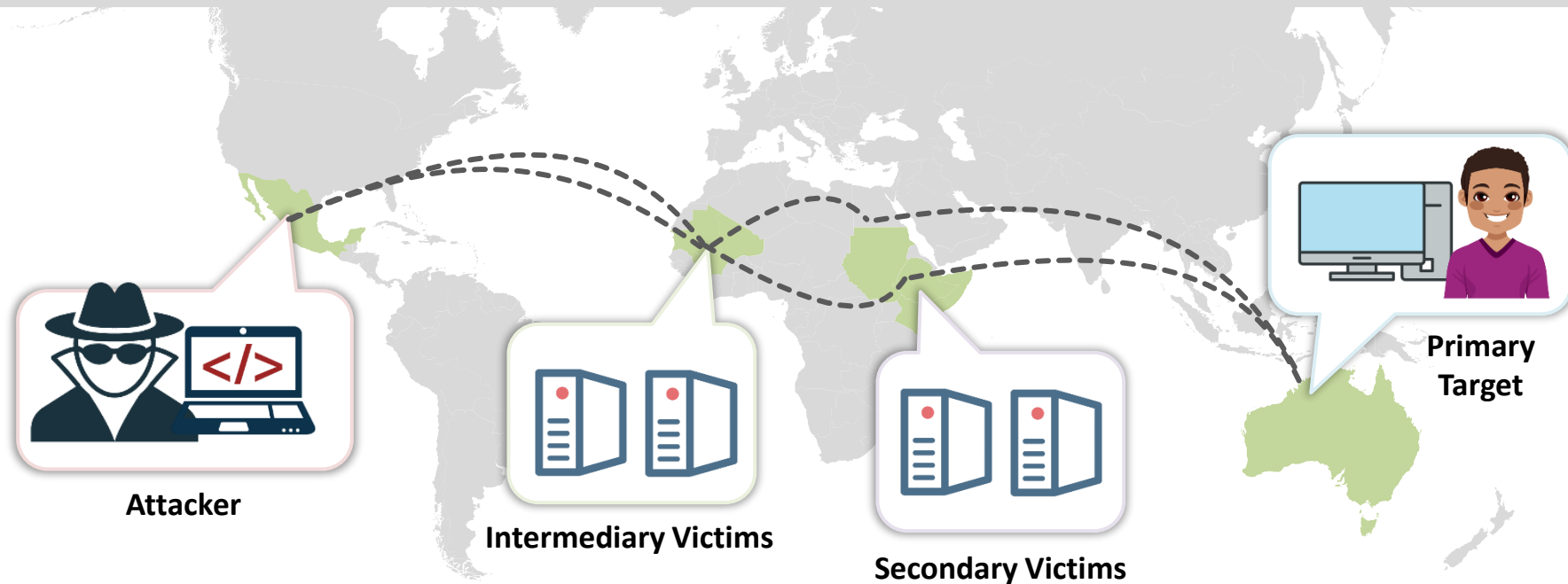
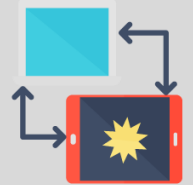


Victim
(Malicious code is executed)

Attacker gets access to victim's computer

DoS/DDoS Attack Techniques: Distributed Reflection Denial-of-Service (DRDoS) Attack

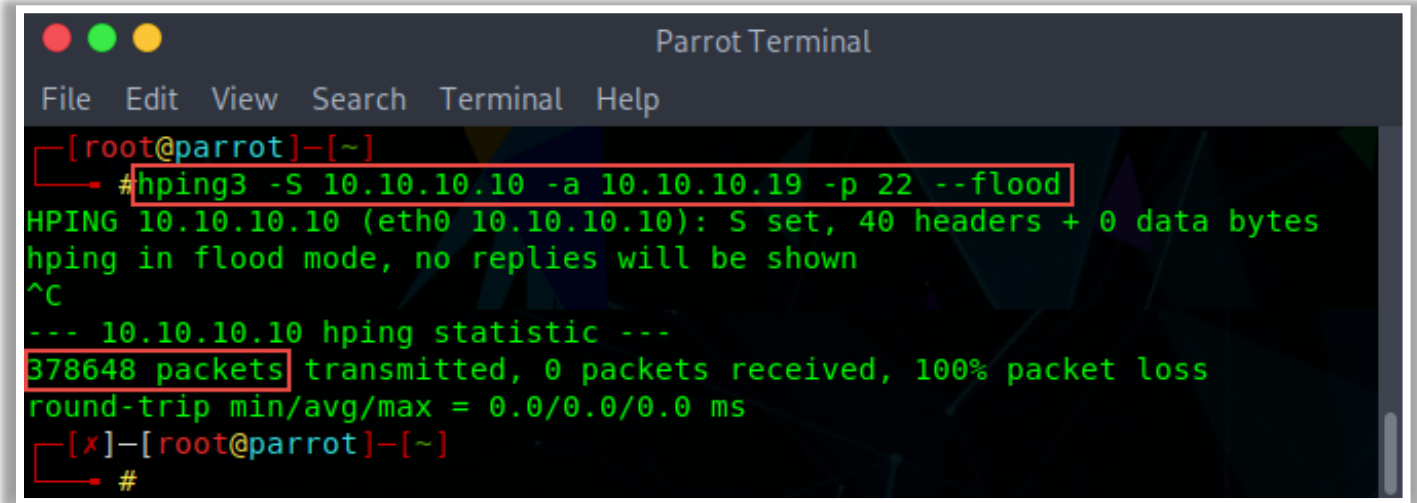
- ❑ DRDoS, also known as a spoofed attack, involves the **use of multiple intermediary and secondary machines** that contribute to the actual DDoS attack against the target machine or application
- ❑ Attackers launch this attack by sending requests to the intermediary hosts, which then redirect the requests to the secondary machines, which in turn **reflect the attack traffic to the target**



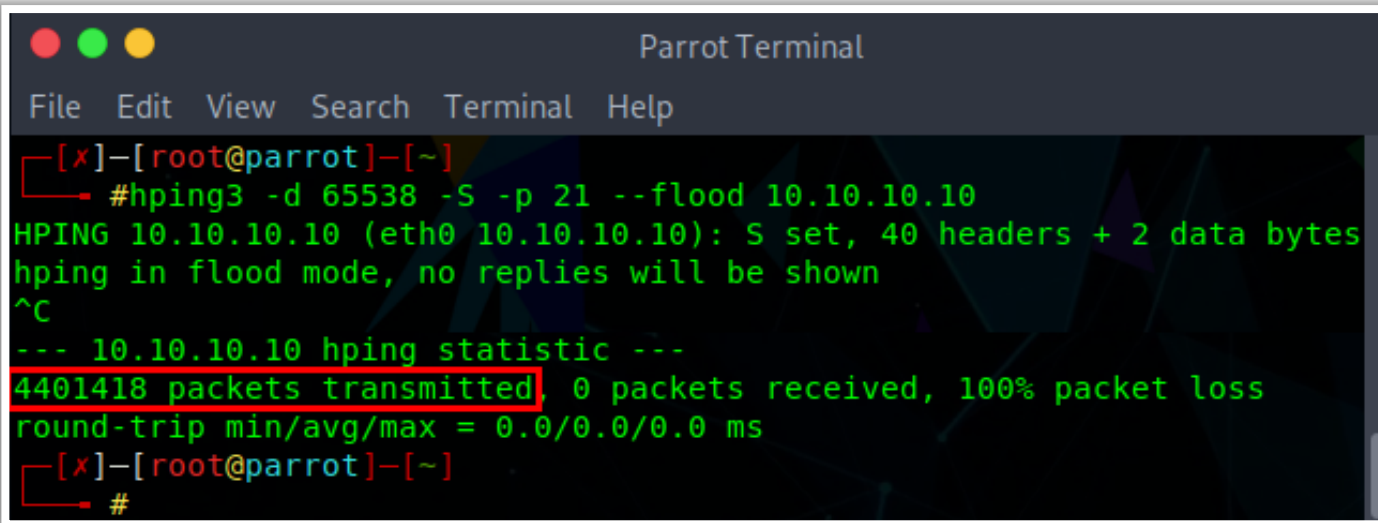
DoS/DDoS Attack Tools

hping3

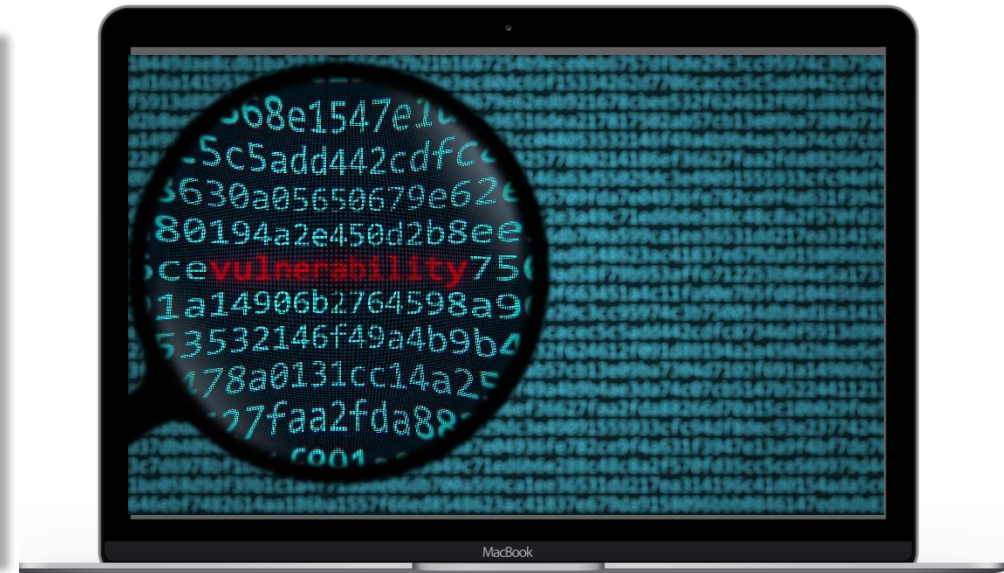
A command-line-oriented network **scanning** and **packet crafting tool** for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols

A screenshot of a Parrot Terminal window. The terminal shows a root user at the parrot prompt. A red box highlights the command: `#hping3 -S 10.10.10.10 -a 10.10.10.19 -p 22 --flood`. The output shows the tool is configured for a flood attack on 10.10.10.10, port 22, using the SYN flag. It indicates that 378648 packets were transmitted with 100% packet loss.

```
[root@parrot]-[~]
#hping3 -S 10.10.10.10 -a 10.10.10.19 -p 22 --flood
HPING 10.10.10.10 (eth0 10.10.10.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.10.10 hping statistic ---
378648 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot]-[~]
#
```

A screenshot of a Parrot Terminal window. The terminal shows a root user at the parrot prompt. A red box highlights the command: `#hping3 -d 65538 -S -p 21 --flood 10.10.10.10`. The output shows the tool is configured for a flood attack on 10.10.10.10, port 21, using the SYN flag with 65538 data bytes. It indicates that 4401418 packets were transmitted with 100% packet loss.

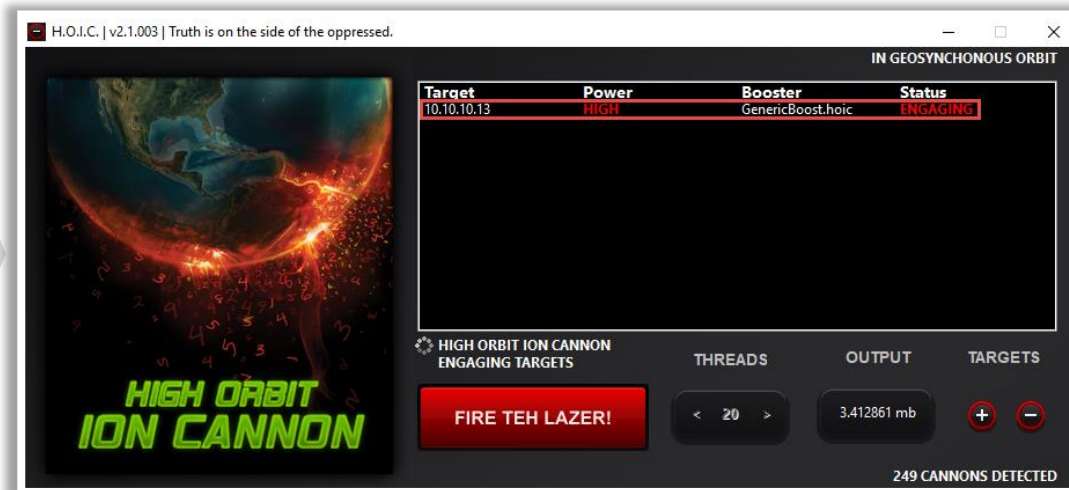
```
[x]-[root@parrot]-[~]
#hping3 -d 65538 -S -p 21 --flood 10.10.10.10
HPING 10.10.10.10 (eth0 10.10.10.10): S set, 40 headers + 2 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.10.10 hping statistic ---
4401418 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot]-[~]
#
```



DoS/DDoS Attack Tools (Cont'd)

High Orbit Ion Cannon (HOIC)

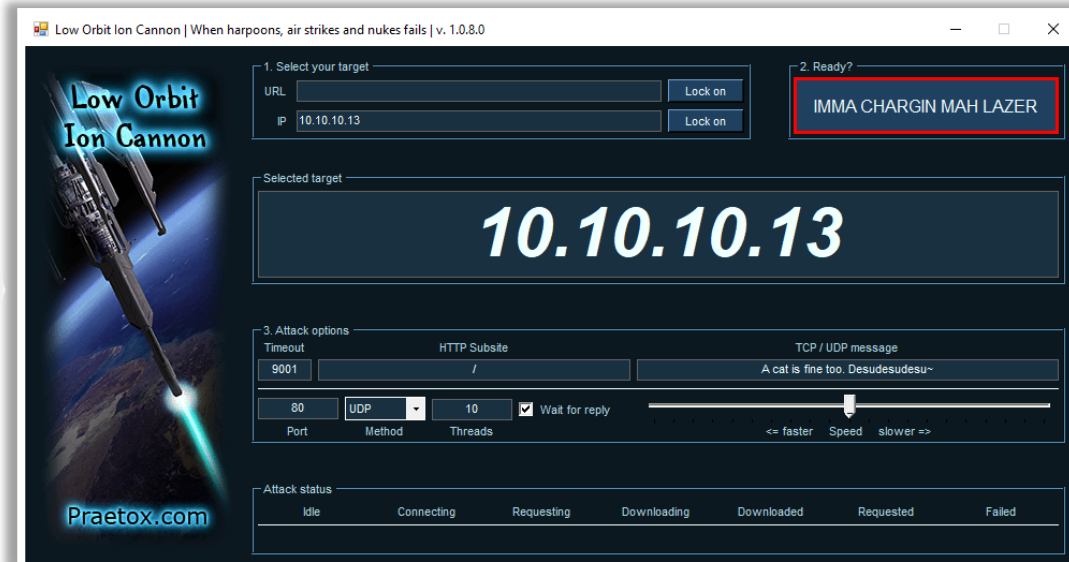
- HOIC carries out a DDoS to attack **any IP address** with a user selected port and a user selected protocol



<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>

Module Flow

1

Discuss Types of DoS and DDoS Attacks

2

Discuss DoS and DDoS Attack Countermeasures



DoS/DDoS Attack Countermeasures



Use **strong encryption mechanisms** such as WPA2 or AES 256 for broadband networks to protect against eavesdropping



Block all **inbound packets** originating from service ports to block the traffic from reflection servers



Ensure that the software and protocols are **up-to-date**, and scan the machines thoroughly to detect any anomalous behavior



Update each kernel to its latest release



Disable unused and **unsecure services**

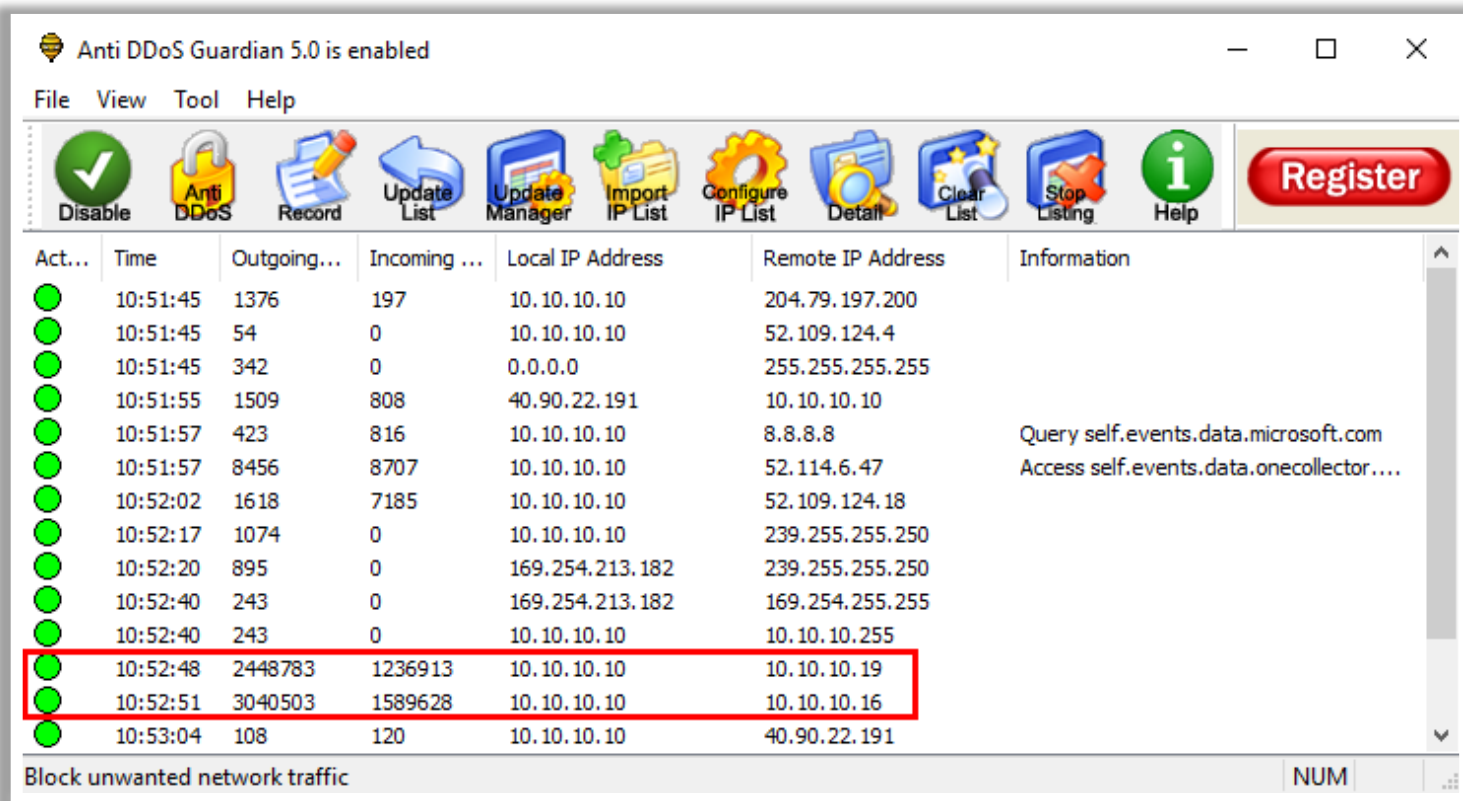


Prevent the transmission of **fraudulently addressed packets** at the ISP level

DoS/DDoS Protection Tools

Anti DDoS Guardian

A DDoS attack protection tool that protects IIS servers, **Apache serves**, game servers, Camfrog servers, mail servers, etc.



<http://www.beethink.com>



Imperva DDoS Protection
<https://www.imperva.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>

Session Hijacking



PASSWORD

Module Flow



01

Discuss Types of Session Hijacking Attacks



02

Discuss Session Hijacking Attack Countermeasures

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



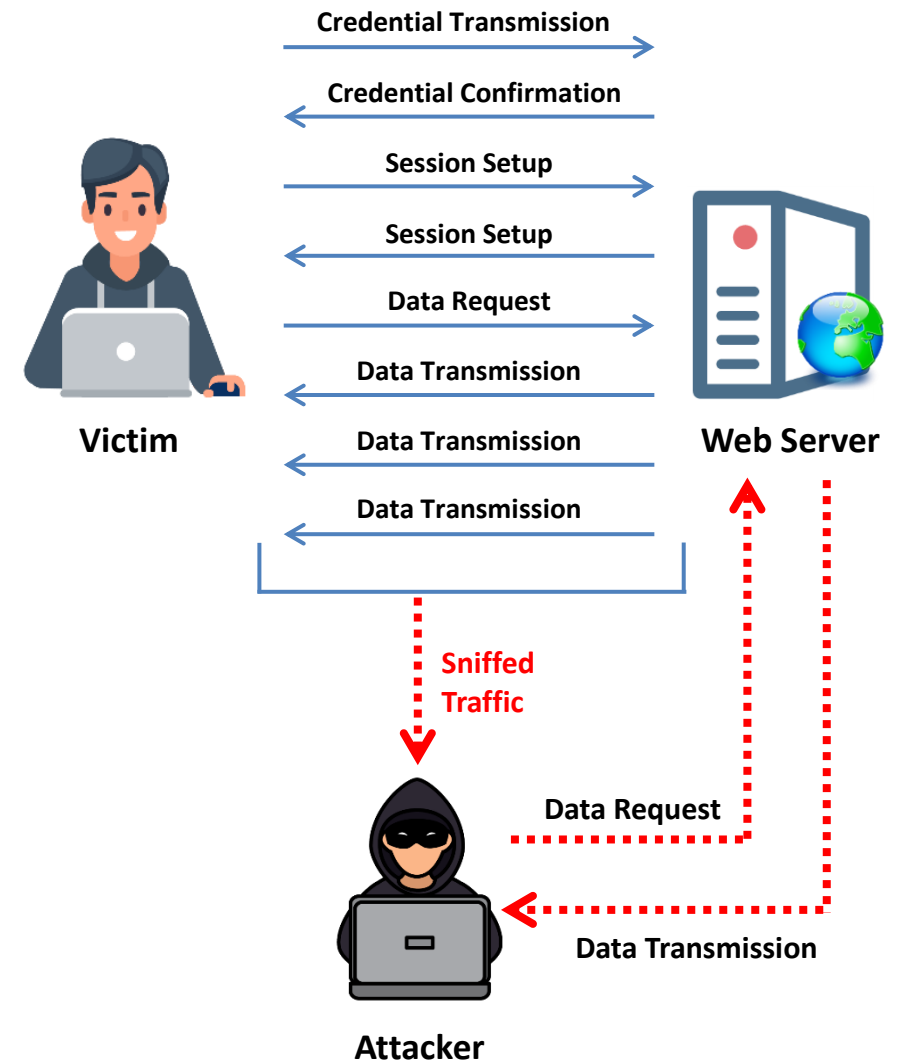
As most **authentications only occur at the start of a TCP session**, this allows the attacker to gain access to a machine



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**



Why is Session Hijacking Successful?



Absence of account lockout for **invalid session IDs**



Weak **session-ID generation algorithm** or small session IDs



Insecure handling of session IDs



Indefinite **session timeout**



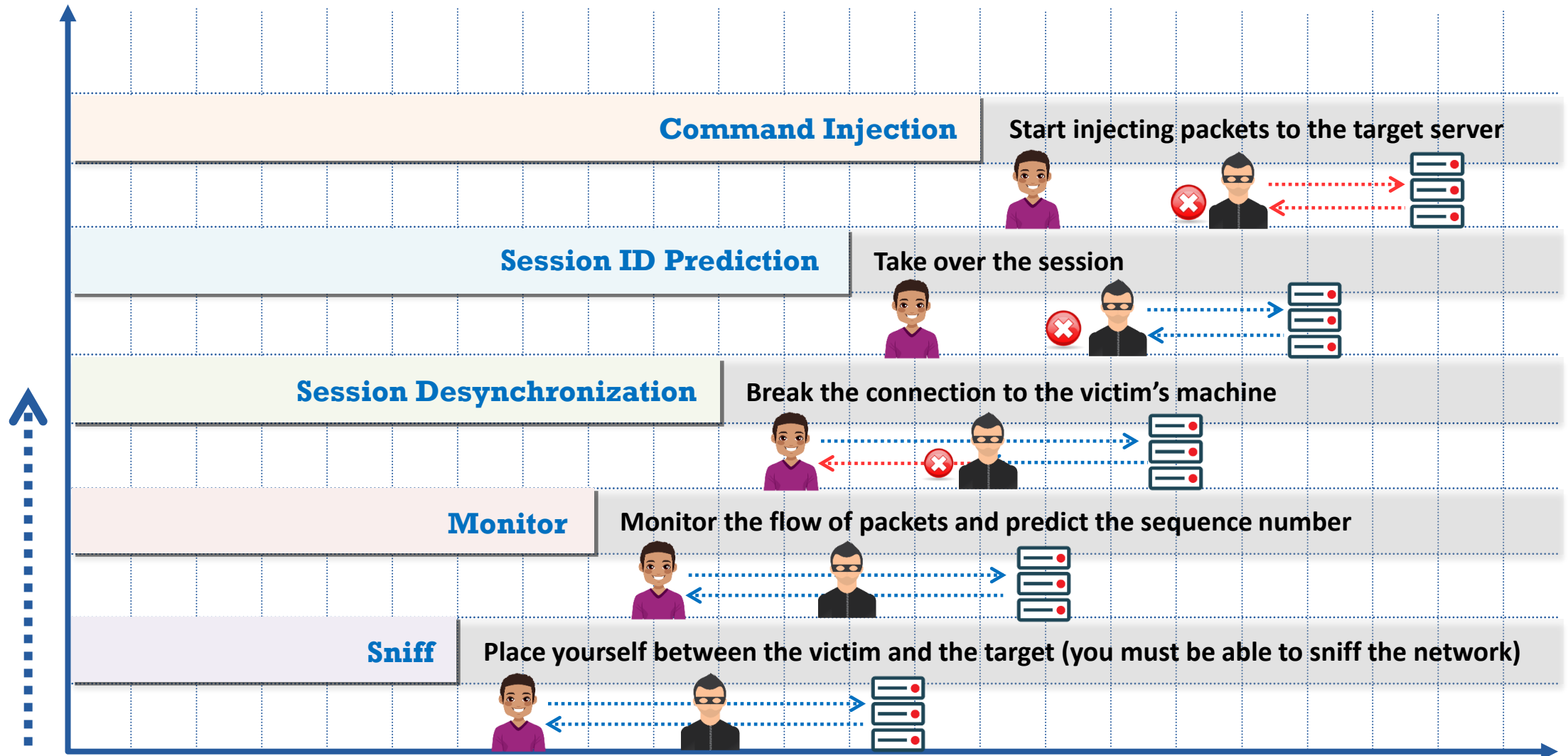
Most computers using **TCP/IP are vulnerable**



Most countermeasures **do not work without encryption**

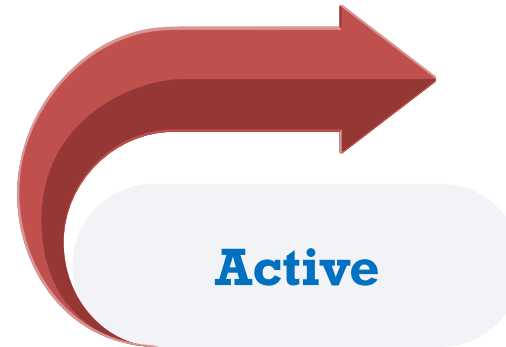
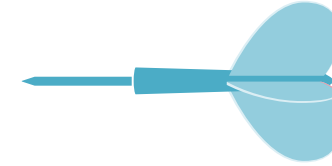
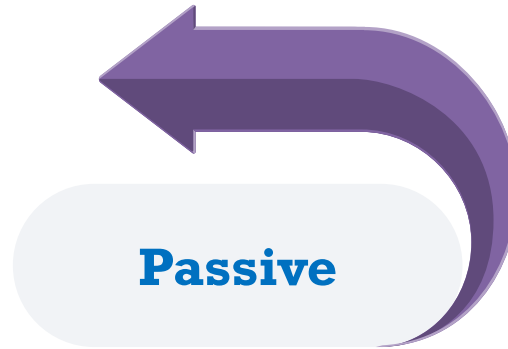


Session Hijacking Process



Types of Session Hijacking

- ❑ In a passive attack, an attacker **hijacks a session** but sits back, watches, and records all the traffic in that session



- ❑ In an active attack, an attacker finds an **active session** and seizes control of it



Attacker



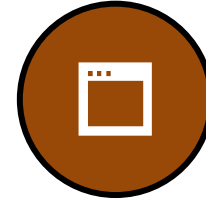
Victim

Session Hijacking in OSI Model



Network Level Hijacking

- ❑ Defined as the **interception of packets** during the transmission between a client and the server in a TCP or UDP session



Application Level Hijacking

- ❑ Refers to **gaining control** over the **HTTP's user session** by obtaining the session IDs

Spoofing vs. Hijacking

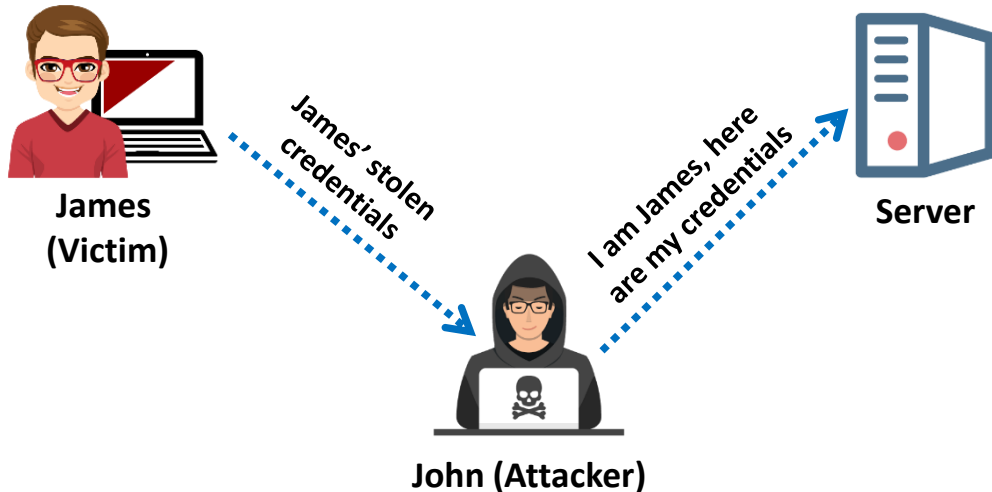
Spoofing Attack



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**



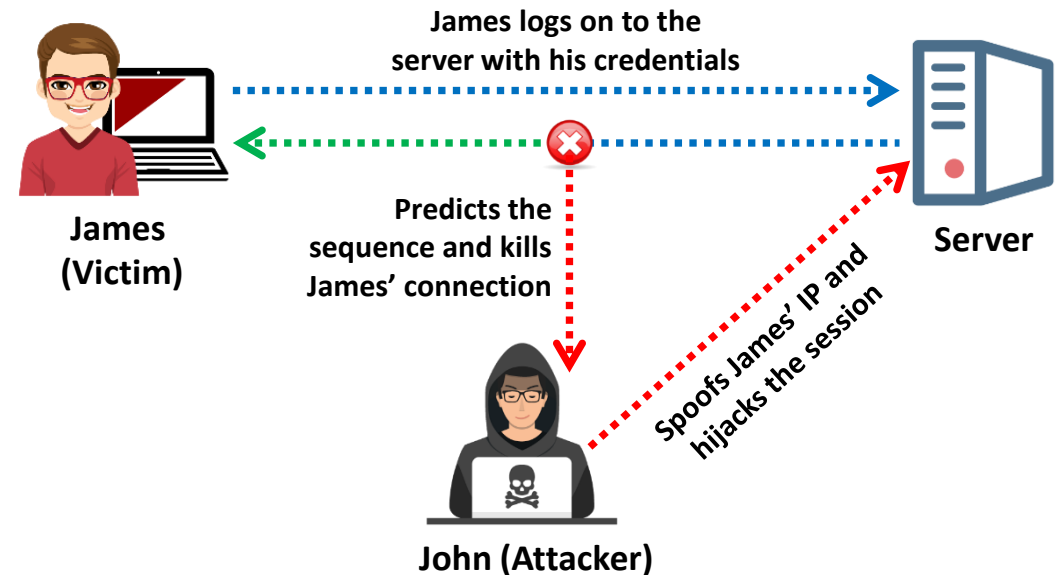
Hijacking



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



Session Hijacking Tools

**OWASP
ZAP**

An integrated penetration testing tool for finding
vulnerabilities in web applications



Burp Suite

<https://portswigger.net>



bettercap

<https://www.bettercap.org>



netool toolkit

<https://sourceforge.net>



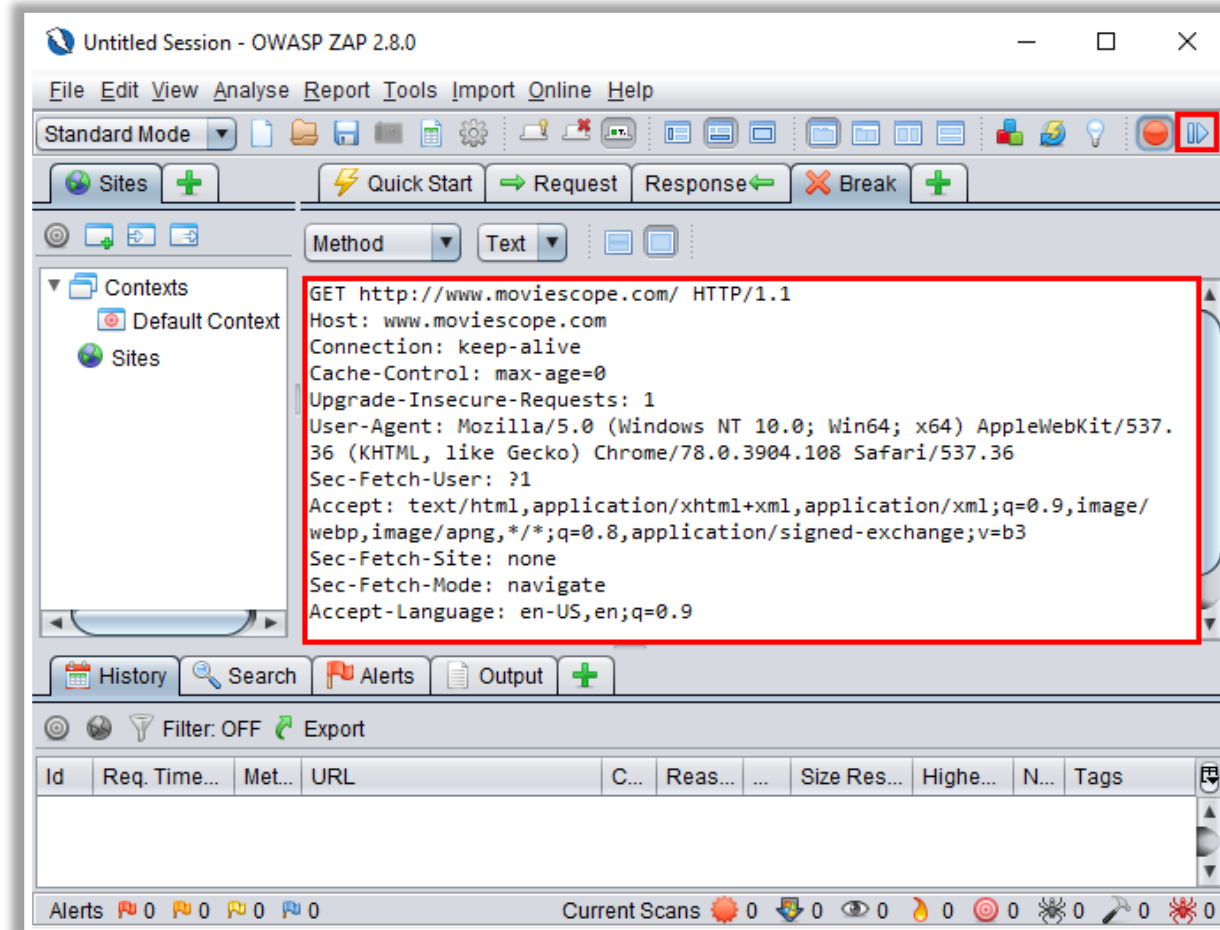
WebSploit Framework

<https://sourceforge.net>



sslstrip

<https://pypi.org>



<https://owasp.org>

Module Flow



01

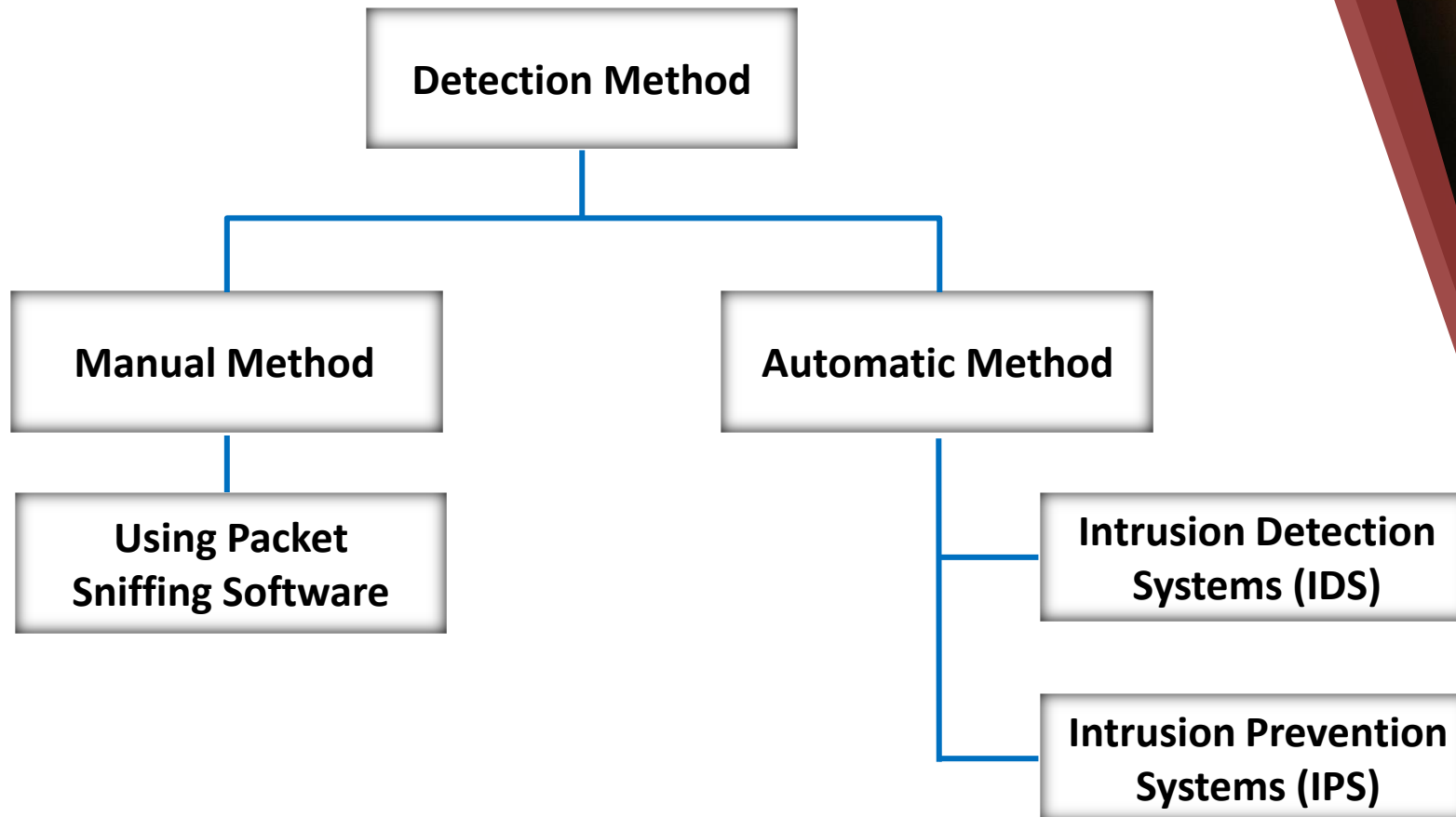
Discuss Types of Session Hijacking Attacks



02

Discuss Session Hijacking Attack Countermeasures

Session Hijacking Detection Methods



Session Hijacking Countermeasures



Use **Secure Shell (SSH)** to create a secure communication channel

Implement the **log-out functionality** for the user to end the session

Generate the **session ID** after a successful login and accept session IDs generated by the server only

Ensure that data in transit is **encrypted** and implement the **defense-in-depth** mechanism

Use **string** or a **long random number** as a session key

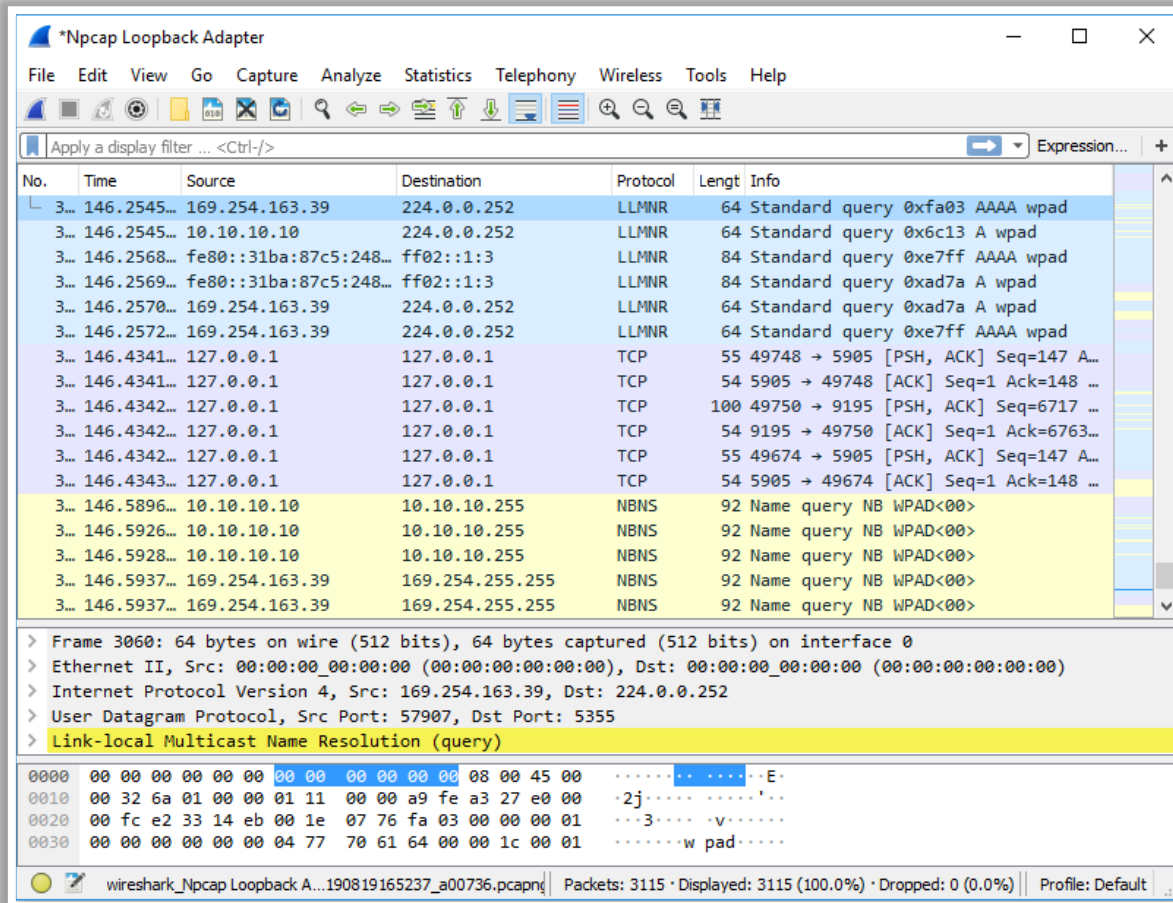
Use different **usernames** and **passwords** for different accounts

Session Hijacking Detection Tools



Wireshark

- ❑ Wireshark allows you to **capture and interactively browse the traffic** running on a computer network



<https://www.wireshark.org>



USM Anywhere

<https://cybersecurity.att.com>



Check Point IPS

<https://www.checkpoint.com>



LogRhythm

<https://logrhythm.com>



SolarWinds Security Event Manager (SEM)

<https://www.solarwinds.com>



IBM Security Network Intrusion Prevention System

<https://www.ibm.com>

Module Summary



- ➡ This module has discussed packet sniffing and types of sniffing
- ➡ It has covered various sniffing techniques and sniffing tools
- ➡ It also discussed different sniffing countermeasures
- ➡ It has covered different types of DoS and DDoS attacks and attack tools
- ➡ It also discussed different DoS/DDoS attack countermeasures and protection tools
- ➡ It has covered session hijacking and types of session hijacking attacks and tools
- ➡ Finally, this module ended with a detailed discussion on various countermeasures to defend session hijacking attempts
- ➡ In the next module, we will discuss in detail on various web application attacks and countermeasures