

Prepared by Dr. Nermin Hamza

CYB740

Penetration test and Ethical hacking

Lecture 06



DOS Attack and Social Engineering

Lecture 06

CYB740

Penetration test and Ethical hacking

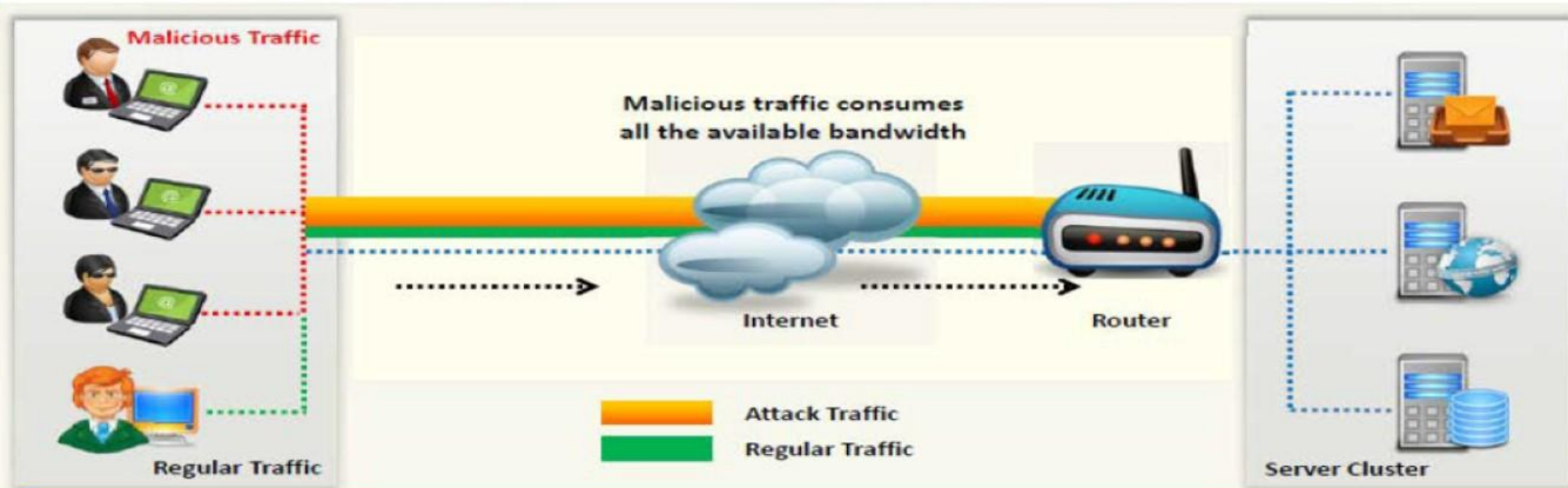
Prepared by
Dr. Nermin Hamza

- DOS Attack
 - Dos and DDos
 - DDOS attack types
 - Botnet
 - DDos Attack Tools
 - DDos prevention
- Social Engineering
 - Human-based Social Engineering
 - Computer-based Social Engineering
 - Mobile-based Social Engineering

DOS Attack

- **Denial-Of-Service Attack = DOS Attack** is a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to its customers.
- In a DoS attack, attackers flood a victim system with non-legitimate service requests or traffic to overload its resources.

When a denial of service (DoS) attack occurs, a computer or a network user is unable to access resources like e-mail and the Internet. An attack can be directed at an operating system or at the network.



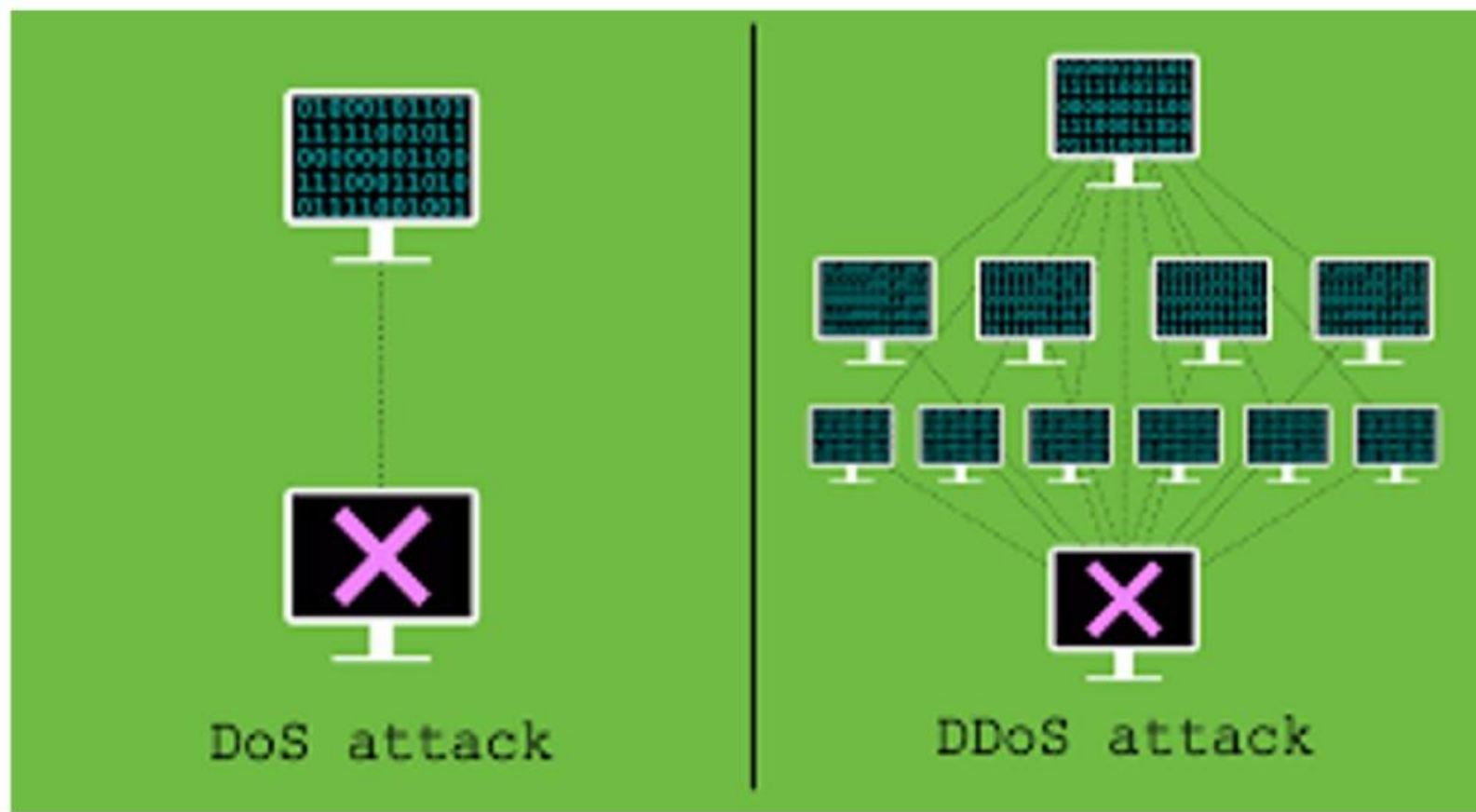
DoS = when a single host attacks

DDoS = when multiple hosts attack simultaneously

Distributed Denial of Service Attacks (DDoS)?

- A distributed denial-of-service (DDoS) attack involves a **multitude of compromised systems** attacking a single target, thereby causing denial of service for users of the targeted system.
- To launch a DDoS attack, an attacker **uses botnets** and **attacks a single system**.

DOS Attack



DOS leads to

- Unavailability of a particular web site
- Slow network performance

Why do DDoS Attacks Happen?

Some of the main reasons for DDoS attacks are:

- **Ransom:** فدية Attackers usually demand ransom after conducting DDoS attacks. However, at times, a ransom note threatening an attack can also be sent beforehand.
- **Hacktivism:** القرصنة من اجل هدف DDoS attacks are also used to voice opinion. Hacktivists can carry out a DDoS attack to show their support or opposition to a regulation, person, or company.
- **Competition:** منافسة او مسابقة Some organizations can use DDoS attacks as a method of unfair competition and try to gain an advantage by causing damage to their competitors' business flows and reputation.
- **Cyber warfare:** الحرب السيبرانية Governments can authorize DDoS attacks to damage critical online infrastructure of an enemy country or take down opposition websites.

<https://www.digitalattackmap.com/>

Digital Attack Map Top daily DDoS attacks worldwide

[Map](#) · [Gallery](#) · [Understanding DDoS](#) · [FAQ](#) · [About](#) [Settings and more \(Alt\)](#)



DDOS attack types

- Application layer attacks
- Protocol attacks
- Volumetric attacks

Application layer attacks

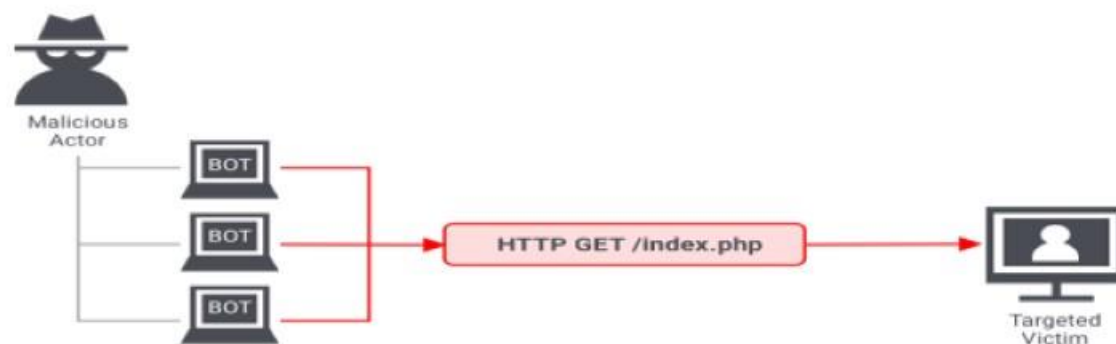
- The application layer is where the server generates the response to an incoming client request.
- For example, if a user enters `http://www.xyz.com/learning/` on their browser, an HTTP request is sent to the server, requesting the learning page. The server will fetch all the information related to the page, package it in a response, and send it back to the browser.
- This information fetching and packaging happens on the application layer. An application layer attack occurs when a hacker uses different bots/machines to repeatedly request the same resource from the server, eventually overwhelming it.

Application-layer attacks are conducted by flooding applications with maliciously crafted requests. The size of application-layer attacks is measured in requests per second (RPS).

The most common application-level attacks are:

- HTTP flood
- Slowloris

- **HTTP flood** — Using botnets, attackers flood an application or a web server with massive volumes of standard GET and POST requests. As these requests often appear as legitimate traffic, detecting an HTTP flood attack is quite a challenge.
- The most common type of application layer attacks are the HTTP flood attacks in which malicious actors just keep sending various HTTP requests to a server using different IP addresses.
- One example of this is asking a server to generate PDF documents over and over again. Since the IP address and other identifiers change in every request, the server can't detect that it's being attacked.



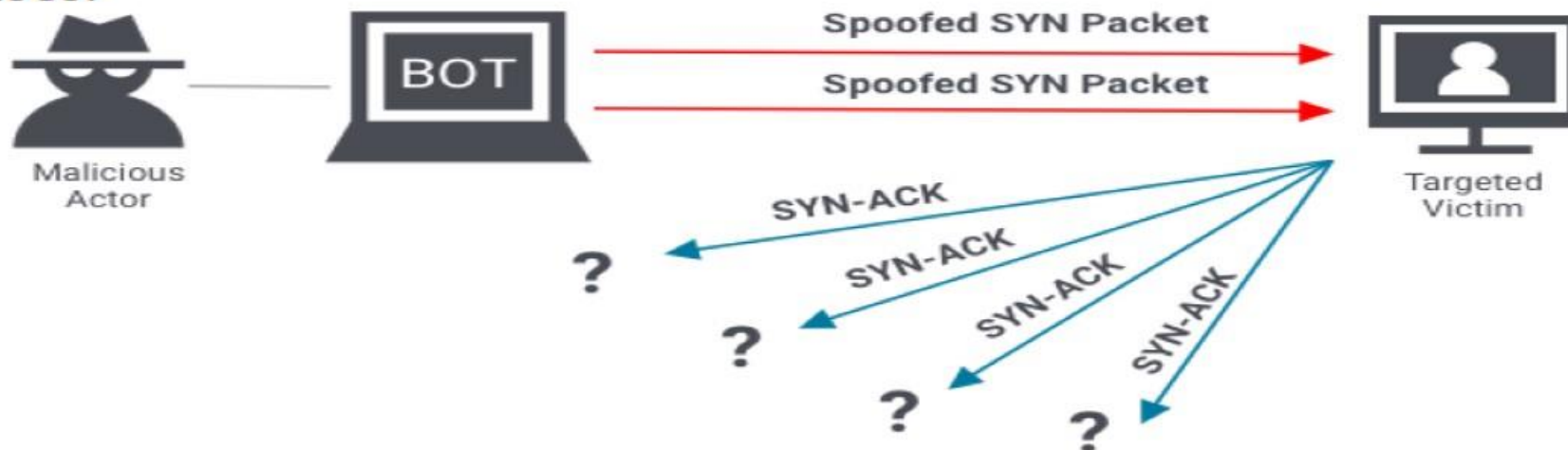
Protocol attacks

- Protocol attacks look to exhaust resources of a server or those of its networking systems like firewalls, routing engines, or load-balancers. An example of a protocol attack is the **SYN flood attack**.
- Before two computers can initiate a secure communication channel – they must perform a TCP handshake.
- A TCP handshake is a means for two parties to exchange preliminary information. A SYN packet is typically the first step of the TCP handshake, indicating to the server that the client wants to start a new channel.

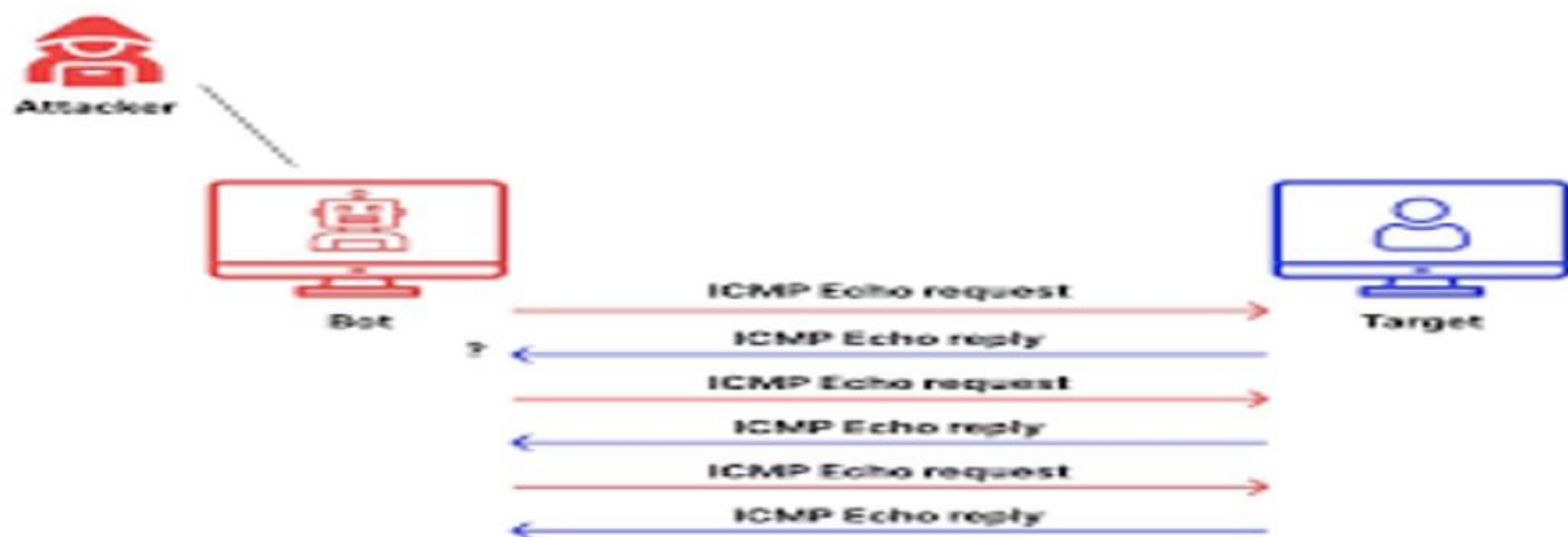
Protocol or network-layer DDoS attacks send large numbers of packets to targeted network. Protocol attacks target weaknesses in the way different internet communication protocols work. Usually, the magnitude of this type of DDoS attack is measured with the number of network packets per second (pps).

- **SYN flood** — Hackers exploit a weakness in the three-way handshake TCP mechanism.
- **ICMP flood** — Malicious actors use an extensive series of Internet Control Message Protocol (ICMP) requests, or pings, in an attempt to exhaust the victim's server bandwidth.

- In a SYN flood attack, the attacker floods the server with numerous SYN packets, each containing spoofed IP addresses.
- The server responds to each packet (via SYN-ACKs), requesting the client to complete the handshake. However, the client(s) never respond, and the server keeps waiting. Eventually, it crashes after waiting too long for too many responses.

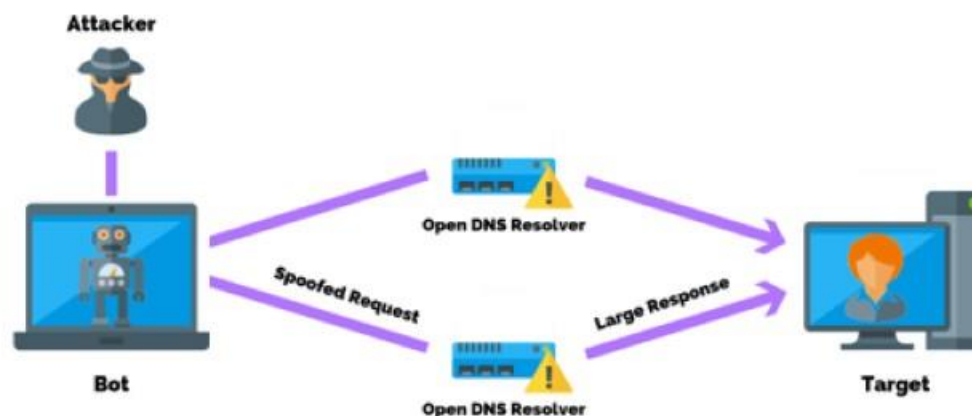


- **ICMP flood attack occurs** when zombies send large volumes of ICMP echo request packet to the victim system
- These packets signal the victim's system to reply, and the combination of the traffic saturates the bandwidth of the victim's network connection.



- **Volumetric attacks**
- Volumetric DDoS attacks are designed to disrupt normal traffic by overwhelming the target of the attack with a flood of traffic from multiple sources.
- The size of a volume-based attack is measured in bits per second (bps).

- **The most common types of volumetric attacks are:**
- **UDP flood** : Attackers send User Datagram Protocol (UDP) packets forged with the victim's source address to random ports
- **DNS amplification** : Cyber criminals compromise domain name systems (DNS) to flood the victim's system with DNS response traffic.



DIVERSITY OF DDoS ATTACKS

Type

Volume-based

Protocol-based

Application layer

Magnitude measurement

Bits per second (bps)

Packets per second
(pps)

Requests per second
(rps)

Common examples

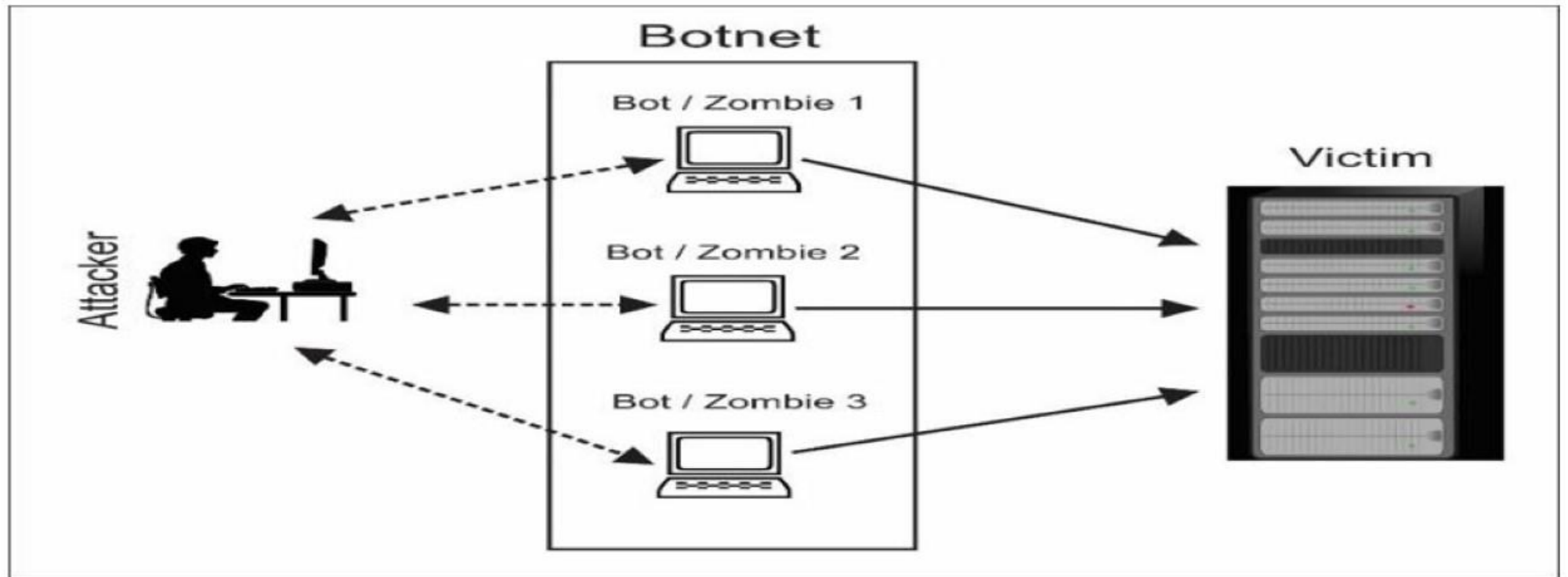
- UDP flood
- DNS amplification
- Misused application

- SYN flood
- ICMP flood
- Ping of death

- HTTP flood
- Slowloris

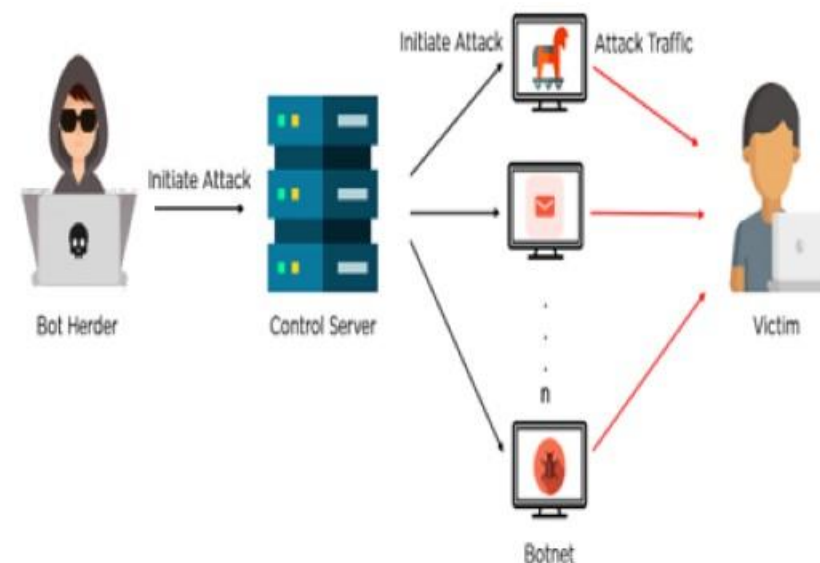
- The words "robot" and "network" together give rise to the term Botnet.
- Bots are software applications that run automated tasks over the internet.
- **Botnet** refers to a network of hijacked internet-connected devices (a group of computers) that are installed with malicious codes known as malware.
- Each of these infected devices is known as Bots, and a hacker/cybercriminal known as the "Bot herder" remotely controls them.

A bot is also called a zombie, and a botnet is referred to as a zombie army.



How Does a Botnet Work?

- **Prepping the Botnet Army:** The first step in creating a botnet is to infect as many connected devices as possible, to ensure that there are enough bots to carry out the attack.
 - This way, it creates bots either by exploiting security gaps in software or websites or phishing emails. They often deploy botnets through a trojan horse virus.
- **Establishing the connection:** Once it hacks the device, it infects with a specific malware that connects the device back to the central botnet server.



- This way, it connects all the devices within the botnet network, and they are ready to execute the attack. A bot herder uses command programming to drive the bot's actions.
- **Launching the attack:** Once infected, a bot allows access to admin-level operations like gathering and stealing user data, reading and writing system data, monitoring user activities, performing DDoS attacks, sending spam, launching brute force attacks, crypto mining, and so on.
- The fraction of bandwidth taken from a single machine isn't sufficient, and hence the Botnet combines millions of devices to carry out large-scale attacks.

Hoic

- Hoic makes a DDos attack to any IP address with a user selected port and a user selected protocol



Derell

- Derell professional (DDos) Tool with modern patterns for attack via TCP,UDP, and HTTP protocols



DDos Attack Tools

- **How to respond to a DDoS attack**
 - When your server is under attack, you have plenty of choices. But know that most of them will impact legitimate traffic too.

Mitigation options can involve:

- **Blackhole filtering:** تصفية الثقب الأسود Develop restriction criteria, and drop off any traffic that doesn't meet those requirements.
- **Scrubbers:** أجهزة التنقية: Your IT team or hosting company examines how your traffic changed right before the attack, and that could identify the malignant addresses. A scrubber keeps them from connecting.
- **Casting:** الإرسال You distribute your traffic among a network of servers. Increasing your capacity can stop traffic from overwhelming your ability to respond to requests.

Your company may benefit from:

- Application front-end hardware: Examine packets as they enter your system, and manage them based on threat level.
- Application-level key completion indicators: determine whether large amounts of incoming traffic are legitimate or part of a coordinated attack. Make capacity decisions accordingly.
- Firewalls: Place a layer of protection between the internet and your server. Filter requests with custom rules, or use a simple rule to block all incoming traffic from an attacker.
- Rate limiting: Define how many times a user can connect your server within a specific timeframe. Some users feel these services are "unfair" to heavy site users. But they can be effective in case of an attack.

**Before the
Attack –
Preparation Plan**

**After the Attack
– Preparation
Plan**

Risk Assessment	Identify systems/services most likely to be targeted (e.g., login APIs, DNS, web servers).
Deploy DDoS Protection	Use cloud-based services like Cloudflare , AWS Shield , Azure DDoS Protection , or Google Cloud Armor .
Configure Firewalls and Rate Limits	Use firewall rules , rate limiting , SYN cookies , and geo-blocking to limit exposure.

DNS Protection

Use services like Google DNS or Cloudflare DNS to protect DNS servers from being overwhelmed

Use a Web Application Firewall (WAF)

Block malicious patterns in HTTP/S traffic. Tools: **ModSecurity, Fortinet WAF**, etc.

Activate Incident Response Plan	Notify team and activate predefined roles and protocols.
Identify Attack Type	Determine if it's a volumetric, protocol, or application layer attack. Tools: tcpdump, Wireshark, NetFlow.
Communicate Internally & Externally	Inform stakeholders, customers, and possibly law enforcement if the attack is severe.

Log All Data

Collect logs from firewalls, WAF, application servers for forensic analysis.

Isolate Critical Systems

Temporarily move or isolate important services to maintain business continuity

What is Social Engineering?

What is Social Engineering?

- Social Engineering is a cyber-attack technique where manipulation is the key weapon used by hackers. It exploits any human error to gain access to sensitive information, confidential and private files, etc.
- In Social Engineering attacks, the hackers are usually someone who is known to the victim or lure the victim into exposing data, allowing system access and other malicious activities. Social Engineering takes advantage of how users think, act and react to a particular situation.

- Social Engineering is used in the majority of cases or situations where manipulation of human behavior is easy to hack into systems. The hackers use this technique to read the behavior of the user. Once he gets an idea of what triggers or motivates the user to initiate a specific action, the hacker tries to manipulate and deceive the user.

How Does Social Engineering Work?

- Most social engineering attacks rely on actual communication between attackers and victims. The attacker tends to motivate the user into compromising themselves, rather than using brute force methods to breach your data.

- Steps for the social engineering attack cycle are usually as follows:
 1. **Prepare** by gathering background information about the victim.
 2. **Infiltrate** by establishing a relationship or initiating an interaction, started by building trust.
 3. **Exploit** the victim once trust and a weakness are established to advance the attack.
 4. **Disengage** once the user has taken the desired action.

Categories of Social Engineering

- ***Human-based Social Engineering:*** Gathers sensitive information by interaction.
- ***Computer-based Social Engineering:*** Social engineering is carried out with the help of computers.
- ***Mobile-based Social Engineering:*** It is carried out with the help of mobile applications.

Impersonation

- It is most common human-based social engineering technique where attacker pretends to be someone legitimate or 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 in tricking a target to reveal sensitive information.
- Posing as a legitimate end user: Give identity and ask for the sensitive information.
- Posing as an important user: Posing as a VIP of a target company, valuable customer, etc.
- Posing as technical support: Call as technical support staff and request IDs and passwords to retrieve data.

Eavesdropping:

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

Shoulder Surfing:

- Shoulder surfing uses direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.
- Shoulder surfing can also be done from a longer distance with the aid of vision enhancing devices such as binoculars to obtain sensitive information.



Tailgating:

- An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access.

<https://www.youtube.com/watch?v=xGuOanYTQ9o>

Computer-based Social Engineering

- **Pop-up Windows:** Windows that suddenly pop up while surfing the Internet and ask for **users' information** to login or sign-in.
- **Hoax Letters:** Hoax letters are emails that issue **warnings** to the user on new viruses, Trojans, or worms that may harm the user's system.
- **Chain Letters:** Chain letters are emails that offer **free gifts** such as money and software on the condition that the user has to **forward the mail to the said number of persons**.

Computer-based Social Engineering

- **Instant Chat Messenger:** Gathering personal information by chatting with a selected online user to get information such as birth dates.
- **Spam Email:** Irrelevant, unwanted, and unsolicited email to collect the financial information, social security numbers, and network information.

Phishing

- An illegitimate email falsely claiming to be from a legitimate site attempts to acquire the user's personal or account information.
- Phishing emails or pop-ups redirect users to fake webpages of mimicking trustworthy sites that ask them to submit their personal information.

Spear Phishing

- Spear phishing is a direct, targeted phishing attack aimed at specific individuals within an organization.
- In contrast to normal phishing attack where attackers send out hundreds of generic messages to random email addresses, attackers use spear phishing to send a message with social engineering content directed at a specific person or a small group of people.
- Spear phishing generates higher response rate when compared to normal phishing attack.

Mobile-based Social Engineering:

Publishing Malicious Apps

- Attackers create malicious apps with attractive features and similar names to that of popular apps, and publish them on major app stores.
- Unaware users download these apps and get infected by malware that sends credentials to attackers.

Fake Security Applications

1. Attacker infects the victim's device.
2. The victim logs onto his/her bank account.
3. Malware in device pop-ups a message telling the victim to download an application onto his/her phone in order to receive security messages.
4. Victim downloads the malicious application on his/her phone.
5. Attacker can now access second authentication factor sent to the victim from the bank via SMS.

Fake Antivirus Warning Signs



Using SMS (story)

1. Tracy received an SMS text message, ostensibly from the security department at XIM Bank.
2. It claimed to be urgent and that Tracy should call the phone number in the SMS immediately. Worried, she called to check on her account.
3. She called thinking it was a XIM Bank customer service number, and it was a recording asking to provide her credit card or debit card number.
4. Predictably, Tracy revealed the sensitive information due to the fraudulent texts.

Social Engineering

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone
Perimeter security	Impersonation, fake IDs, piggy backing, etc.	Implement strict badge, token or biometric authentication, employee training, and security guards
Office	Shoulder surfing, eavesdropping, Ingratiation, etc.	Employee training, best practices and checklists for using passwords Escort all guests
Phone (help desk)	Impersonation, Intimidation, and persuasion on help desk calls	Employee training, enforce policies for the help desk
Mail room	Theft, damage or forging of mails	Lock and monitor mail room, employee training
Machine room/Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment

<https://www.onelogin.com/learn/ddos-attack>

<https://www.youtube.com/watch?v=bc120b-L4SU>

Thank You