Methods of infiltration

Social engineering

**- It is the manipulation of people into performing actions of divulging confidential Information**

**- It often relys on peoples willingness to be helpful, but they also prey on their weaknesses**

- PRETEXTING

Attacker calls an individual and lies to them in attempt to gain access to privileged data

- TAILGATING

Attacker quickly follows an authorized person into a secure, physical location

- SOMETHING FOR SOMETHING

Attacker requests personal info. From a person in exchange for smt

Denial of service (DoS)

- (DoS) attacks are a **type of network attack** that is relatively simple to carry out

- **this attack results in some sort of interruption** of network service to users, devices or

Applications

There are 2 main types:  
 - overwhelming quantity of traffic  
 - **smt is sent an enormous amount of data at a rate which it cannot handle**  
 - This causes a slowdown in transmission or response, or the device or service to crash

- maliciously formatted packets

- it is a **collection of data that flows between a source and a receiver computer** or

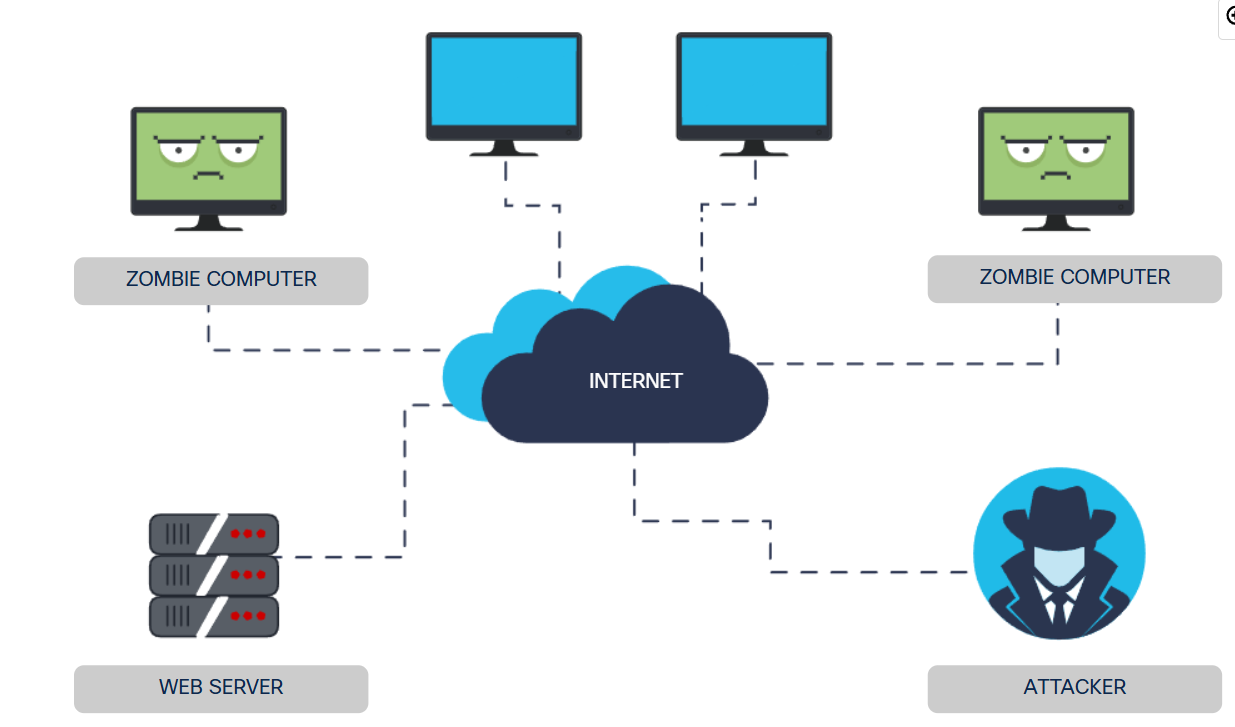
application **over a network**, (internet)

- **When it is sent, the receiver will be unable to handle it**

Distributed DoS

- A distributed DoS (DDoS) attack is **similar to a Dos attack but from multiple, coordinated**

**Sources**



Attacker builds a network of infected hosts called zombies, zombies will constantly scan and infect more hosts, when ready the hacker will instruct the handler systems to make the botnet of zombies carry out the DDoS attack

Botnet

- It’s a **group of bots, connected through the internet**, that can be controlled by a malicious

Individual/group

- **these bots can be activated to distribute malware, launch DDoS attacks, distribute spam**

**emails, or execute brute-force password attacks**

On-path attacks

- **they intercept or modify communications between two devices**, either to collect info from

or to impersonate one of the device

- it is also called man-in-the-middle or man-in-the-mobile attack

-man-in-the-middle (MitM)

- It happens when a **cybercriminal takes control of a device without the user’s knowledge**

- Basically the **attacker can intercept and capture user info before it is sent to destination**

-man-in-the-mobile(MitMo)

- **It takes control of user’s mobile device**  
 - When infected the mobile is instructed to exfiltrate user-sensitive info and send it to

attacker

SEO poisoning

- SEO = search engine optimization

- attackers **take advantage of popular search terms and use SEO to push malicious sites**

**higher up the ranks of search results**.

- the **most common goal is to increase traffic to malicious sites that may host malware or**

**attempt social engineering**

Password attacks

- some common password security attacks are:

- PASSWORD SPRAYING  
 - it attempts to gain access to a system by **‘spraying’ a few commonly used**

**passwords across a large number of accounts**

- DICTIONARY ATTACKS

- **tries every word in a dictionary or a list of commonly used words as a**

**Password**

- BRUTE-FORCE ATTACKS

- it’s the simplest and most commonly used way  
 - he **tries all possible combinations of letters, numbers and symbols until**

**it is correct**

- RAINBOW ATTACKS

- passwords are stored as hashed values  
 - a rainbow table is large dictionary of precomputed hashes and the

passwords from with they were calculate

- it **compares the hash of password with those store in the rainbow table**

- TRAFFIC INTERCEPTION

- if you store your password in clear, readable text, anyone who has access

can read it

Advanced persistent threats (APTs)

- **multi-phase, long term, stealthy and advanced operation againts a specific target**

- it is usually well-funded and typically targets organizations or nations for business/politics

- **its main purpose is to deploy malware and remain undetected**