Denial of service attack (DOS)

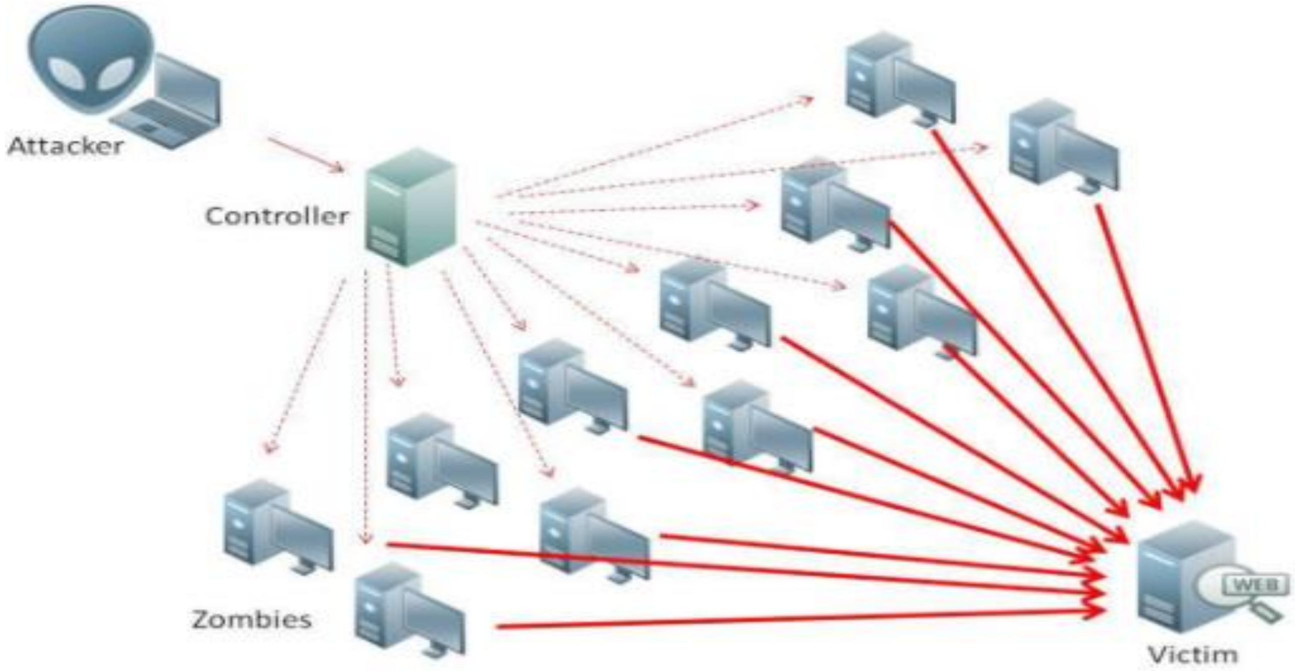
Samarendranath B

Introduction

- Denial of service attack (DOS) is an attack against computer or network which reduces, restricts or prevents accessibility of its system resources to authorized users.

- Distributed Denial of Service (DDoS) attack is an attack where multiple compromised systems simultaneously attack a single system; thereby, causing a DOS attack for the users of the target.

- An attacker can select the Zombies randomly or topologically and once compromised, he sets up a command and controller to control the zombies that attack the target. A bot is a malicious software installed on compromised machines; this gives the attacker control over the zombies. The network of Bots is called botnet.



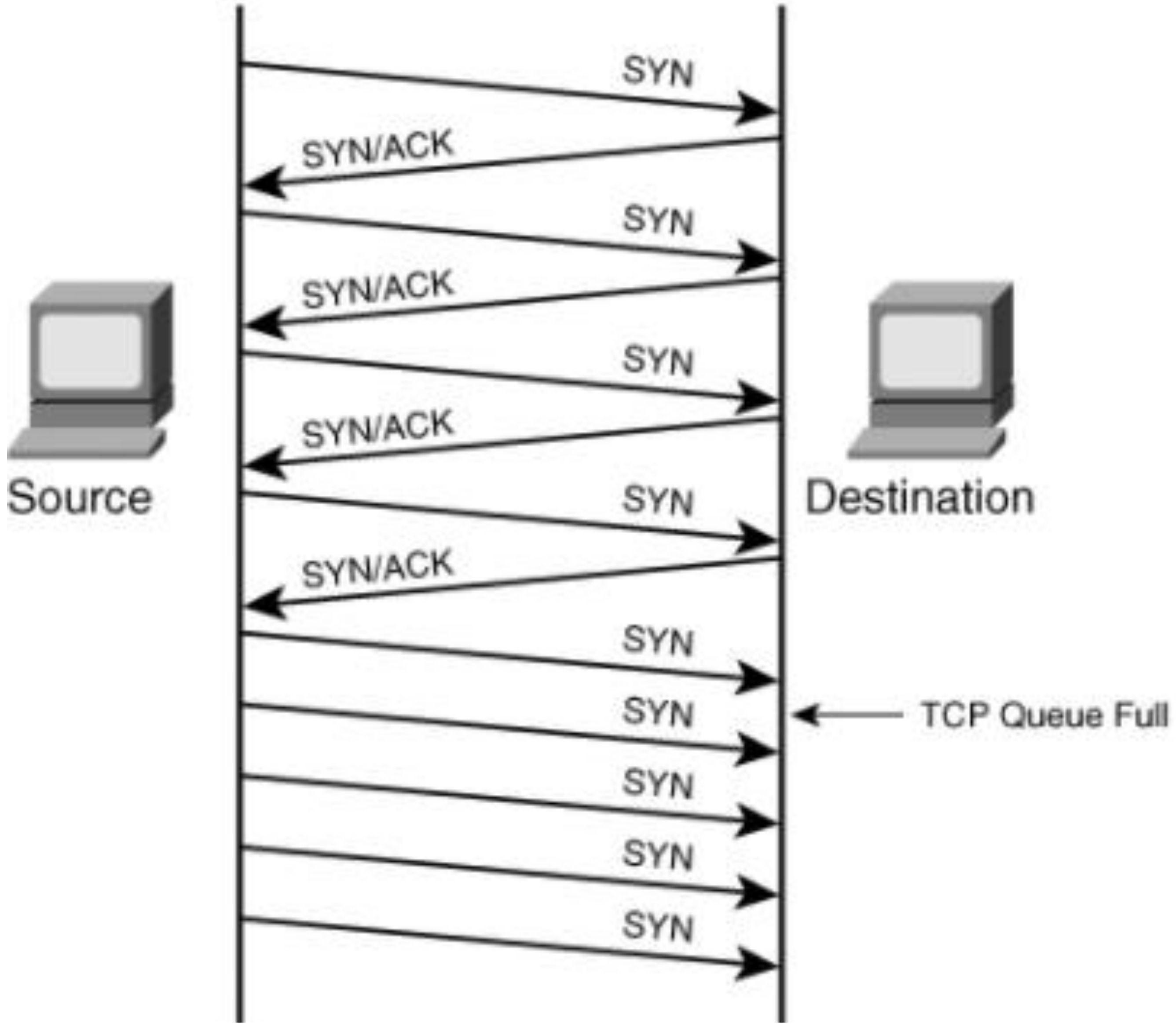
Types of DOS

- Volumetric attacks:

- This is an Attack where the entire bandwidth of a network is consumed so the authorized clients will not be able to get the resources. This is achieved BY flooding the network devices like hubs or switches with numerous ICMP echo request/reply packets, so the entire bandwidth is consumed, and no other clients are able to connect with the target network.

Types of DOS

- Syn flooding:
- Is another attack where an attacker compromises multiple zombies and simultaneously floods the target with multiple SYN packets. The target will be overwhelmed by the SYN requests, either it goes down or its performance is reduced drastically.

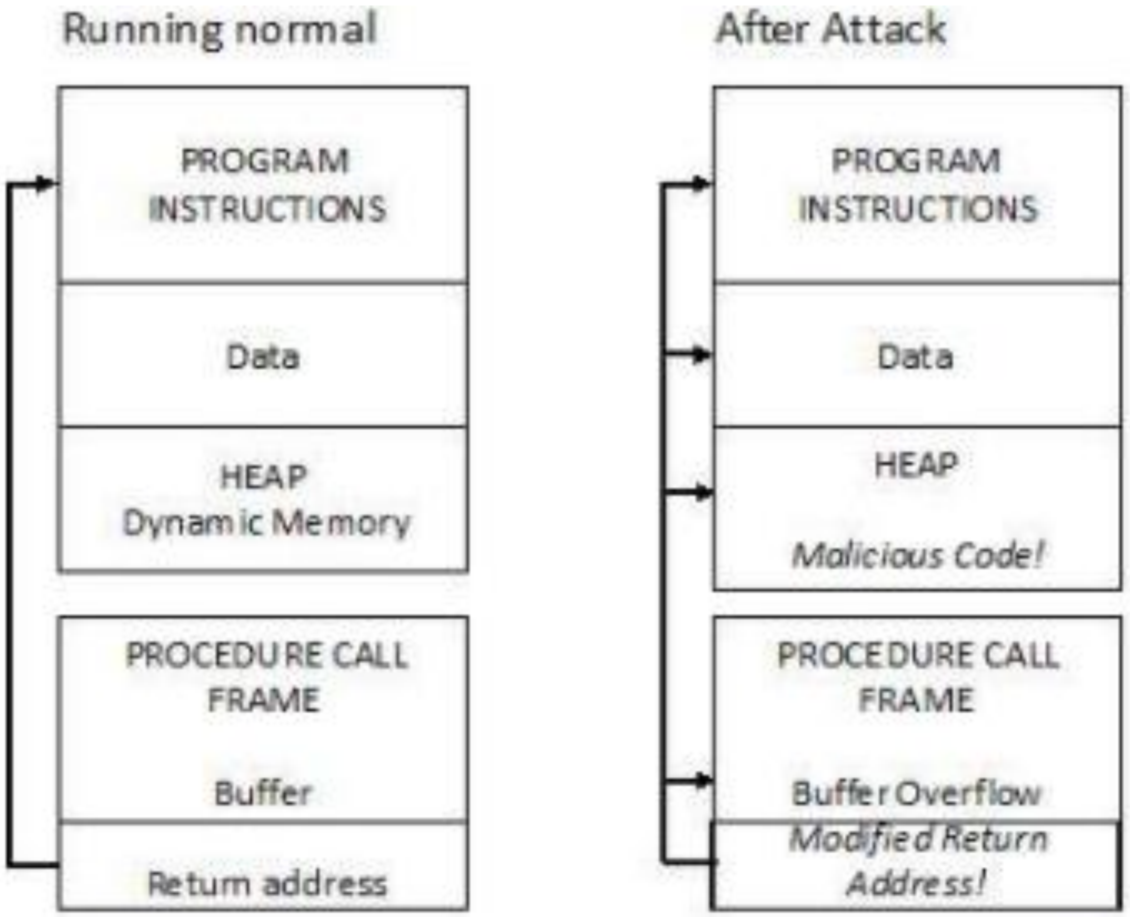


- Fragmentation attacks:
- This is an attack that fights against the reassembling ability of the target. Numerous fragmented packets are sent to the target, making it difficult for the target to reassemble them; thereby, denying access to the valid clients.

- TCP-State exhaustion attack:
- The attacker sets up and tears down TCP connections and overwhelms the stable tables; thereby, causing a DOS attack.

- Application Layer Attacks:

- The attacker takes advantage of the programming errors in the application to cause the denial-of-service attack. It is achieved by sending numerous application requests to the target to exhaust the target’s resources so it will not be able to service any valid clients. A programming error in the case of buffer overflow attack- if the memory allocated to a variable is smaller than the requested, then it may lead to memory leakage or crashing the entire application.



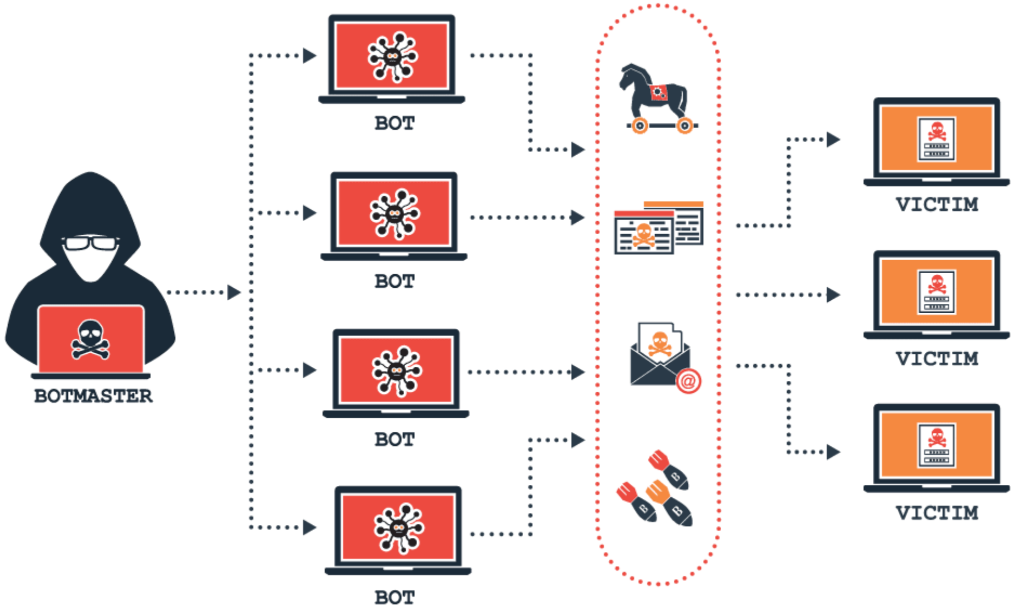
Attacker plants code that overflows buffer and corrupts the return address. Instead of returning to the appropriate calling procedure, the modified return address returns control to malicious code, located elsewhere in process memory.

- Plashing:

- This is done by causing a permanent damage to the system hardware by sending fraudulent updates to the hardware thereby making them completely unusable. The only solution is to re-install the hardware.

How Do Denial of Service Attacks Work?

- A denial of Service attack is often achieved using TCP and UDP packets. In a DoS attack, the perpetrators flood the user's system with illegal traffic or service requests to inundate its resources and stop it from executing intended tasks.



How to Tell if You are Experiencing a DoS Attack

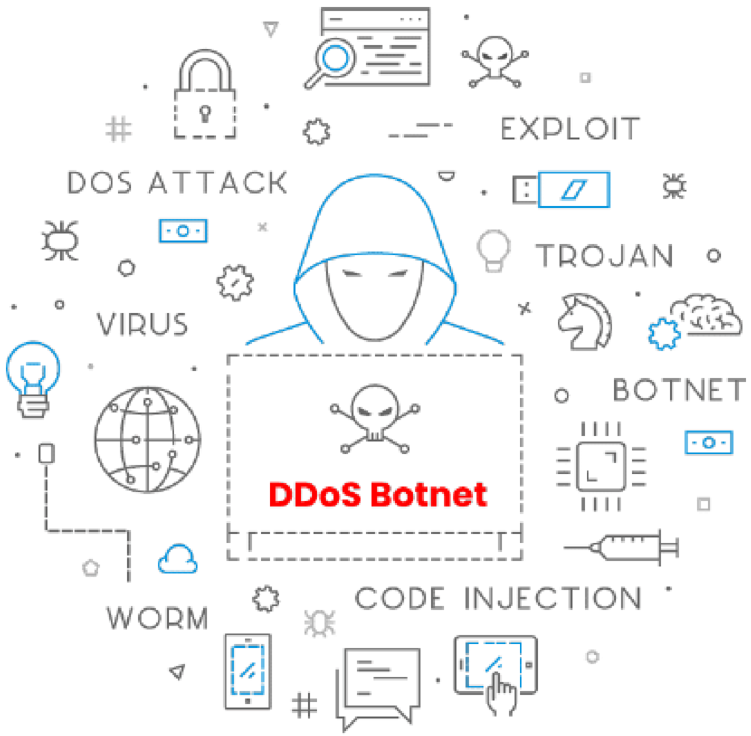
- The incapability to load certain websites
- The extreme volume of spam emails
- Uncharacteristically slow network performance, including extended load times for files or websites
- Prolonged failure to access specific websites
- A sudden loss of connectivity across devices on the same network

What Is Distributed denial of service (DDoS) Attack With Example?

- Distributed denial of service (DDoS) attack is a malicious effort to render an online service or website inaccessible to users, typically by momentarily disrupting or appending the services of the host server.
- A Distributed denial of service attack naturally comprises of above 3 to 5 nodes on diverse networks, anything lesser may serve as a denial of service attack.
- The traffic can involve fake packets, incoming mails, or requests for connections. Sometimes the target is compromised at a low level or threatened with a DDoS attack. This may be joined with blackmail and threats of more overwhelming attacks except the organization meets the set ransom. DDoS typically uses botnets to execute these malicious tasks.

What is a DDoS Botnet?

- The term “botnet” refers to a group of hijacked internet-connected devices that are operated remotely from a Command & Control Center (C&C) by a malicious attacker. A botnet is a combination of the word network and robot and each compromised computer is referred to as a bot. These attacks characteristically comprise of unsecured IoT devices, PCs, smartphones, and sometimes resources from public cloud services.



What Is the Difference Between DoS and DDoS Attack?

- DDoS and DoS differ in that the latter uses a single internet connection (that is one internet-connected device or network) to flood the victim's computer or other networks with malicious traffic, while the former uses multiple internet connections to render the victim's network or device inaccessible to them. Hence, a DoS attack can be obstructed by blocking the single IP address.
- DDoS attacks are the most powerful internet attacks and also the most difficult to detect. The reason being that they are introduced from several locations to hide their identities and prevent the victim from easily identifying the main source of the attack. As a result, it is unfeasible to distinguish between genuine and counterfeit network traffic.

- Another difference between DDoS and DoS attacks lies in the volume of the attack being launched. While DDoS attacks give room for the cyber-attacker to introduce enormous volumes of traffic to the user’s computer or network, DoS cannot afford the attacker with such excesses. Additionally, you should also note that their mode of execution varies as well. While DoS attacks are executed using a script or DoS tool, such as Low Orbit Ion Cannon, DDoS attacks are usually launched using botnets or through the networks of the devices infiltrated by the attacker.

Counter Measures

- Use up-to-date anti-virus and IDS tools.
- Perform network analysis to find out the possibility of DOS attack.
- Shut down unnecessary services in the target network.
- Find and neutralize handlers. Protect secondary victims.
- Perform proper activity profiling and ingress/egress filtering to filter out unwanted traffic.
- Enforce in-depth packet Analysis.

Counter Measures

- Use Defense-in–depth approach.
- Add additional load balancers to absorb traffic and set up a throttle logic to control traffic.
- Correct program errors.
- Use Strong encryption mechanisms.
- Use high quality rated dedicated servers and bare metal servers for your software and website to keep it safe from DDOS attack.