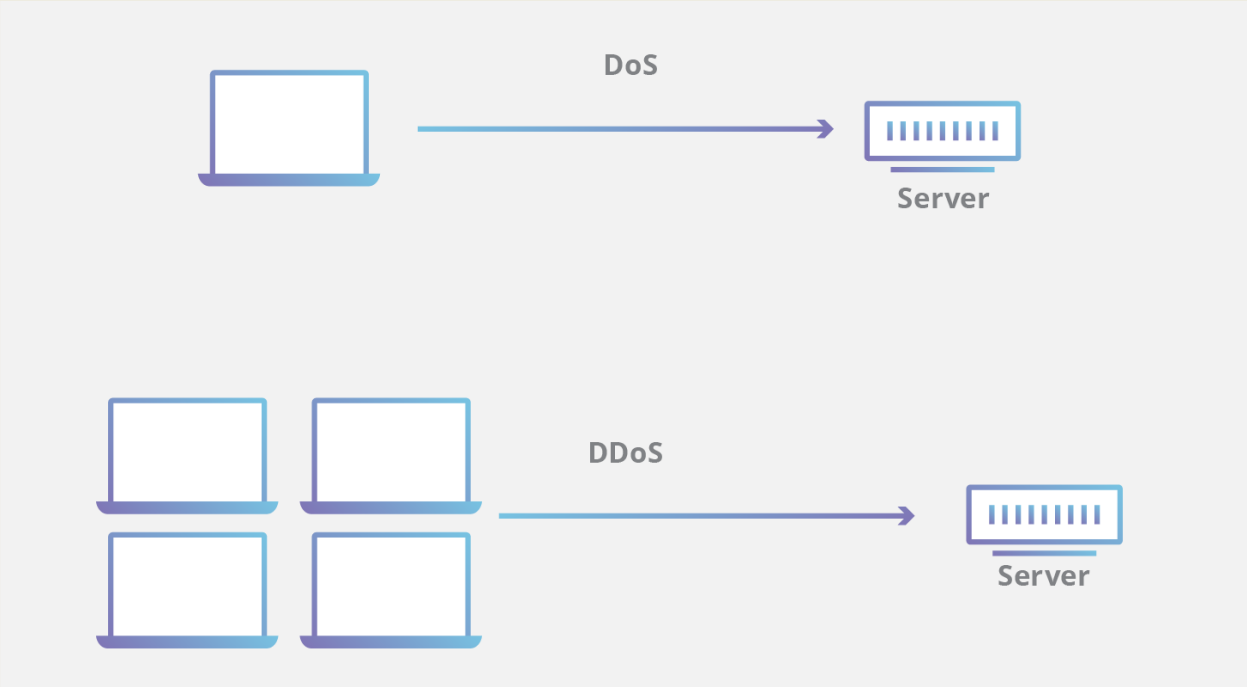
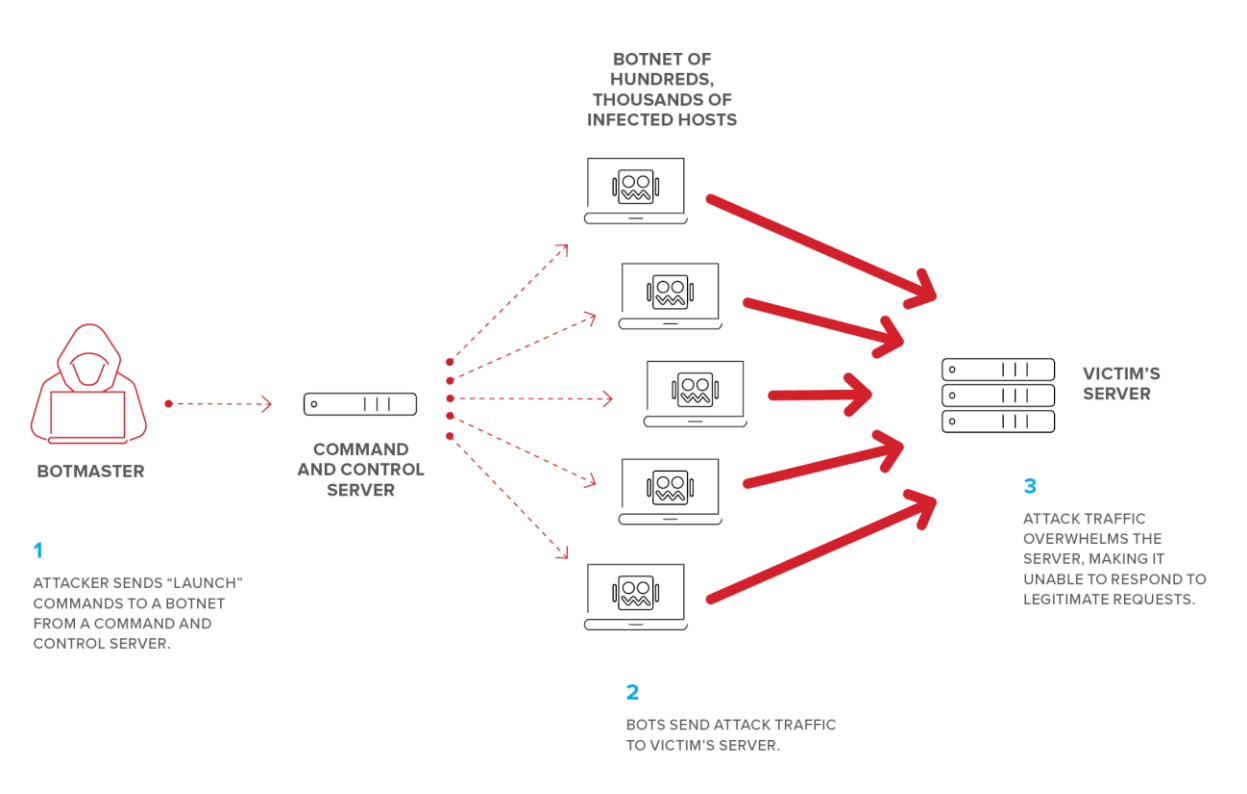
DoS/DDoS Concepts

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 targets



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.



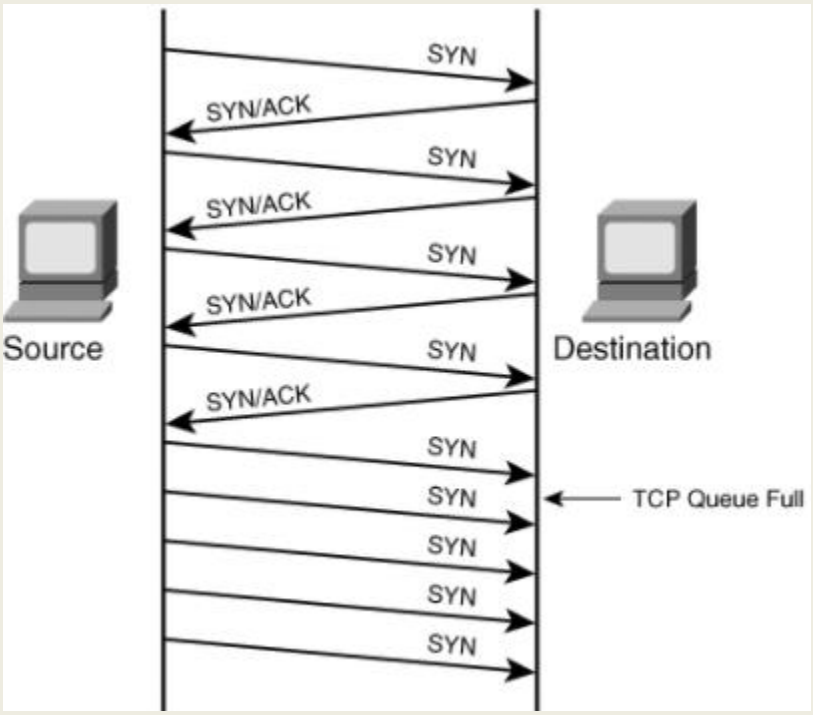
Types of DOS:

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.

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.



Source: https://swordfish.wordpress.com/2006/03/16/denial-of-service-attacks-dos/

Fragmentation attacks:

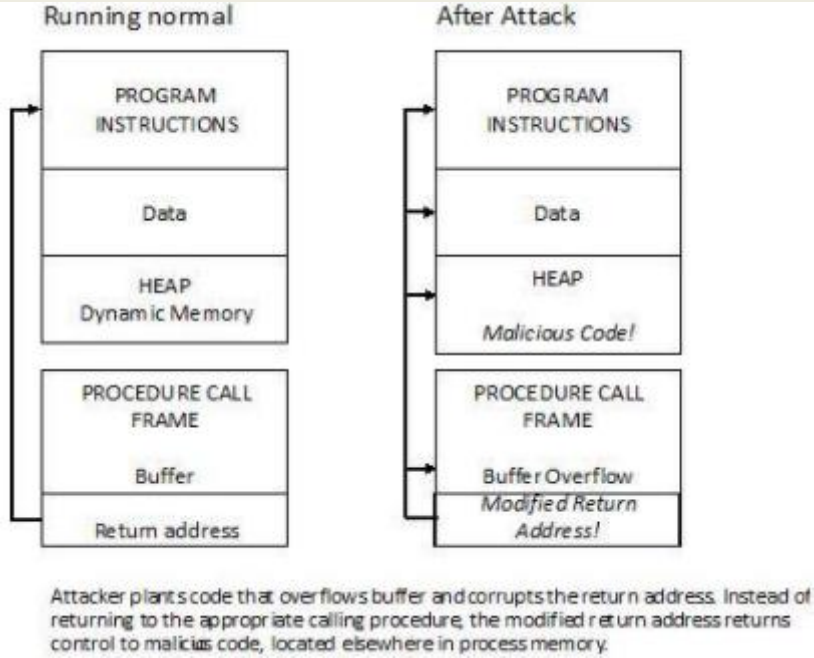
This is an attack that fights against the reassembling ability of the target. Numerous fragmented packets are sent to the target, making it difficult for the target to reassemble them; thereby, denying access to the valid clients.

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.



E.g., Buffer overflow attack, Account lockout, Request flooding, etc.

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.

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.
- 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.

DoS tool list

- LOIC (Low Orbit ION cannon) Open source DDoS tool which can easily perform TCP, UDP and HTTP DoS attacks. ...
- HOIC (High Orbit ION cannon) ...
- RUDY. ...
- Slowloris. ...
- HTTP Unbearable Load King (HULK) ...
- XOIC. ...
- DDoSIM (DDoS Simulator) ...
- PyLoris.
- Hulk.py