MODULE-5: Network Security

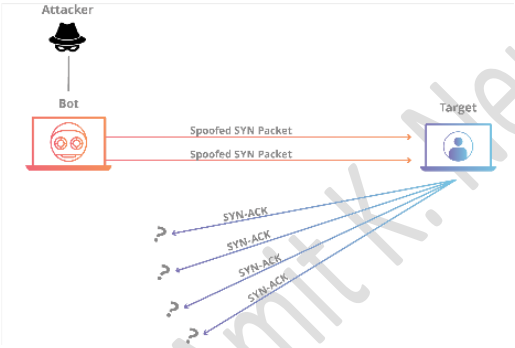
VIT | Vidyalankar Institute of Technology
Accredited A+ by NAAC

Prepared by Prof. Amit K. Nerurkar

Classic DOS attacks

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.

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.

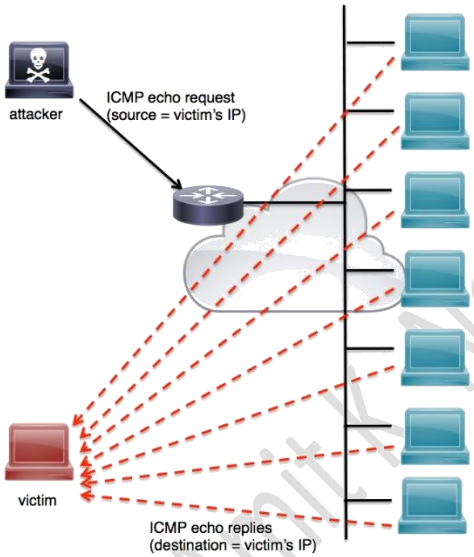


By saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service. In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

A few common historic DoS attacks include:

Ping flood - this simple denial-of-service attack is based on overwhelming a target with ICMP (ping) packets. By inundating a target with more pings than it is able to respond to efficiently, denial-of-service can occur. This attack can also be used as a DDoS attack.

Ping of Death - often conflated with a ping flood attack, a ping of death attack involves sending a malformed packet to a targeted machine, resulting in deleterious behavior such as system crashes.



Smurf attack - a previously exploited DoS attack in which a malicious actor utilizes the broadcast address of vulnerable network by sending spoofed packets, resulting in the flooding of a targeted IP address.

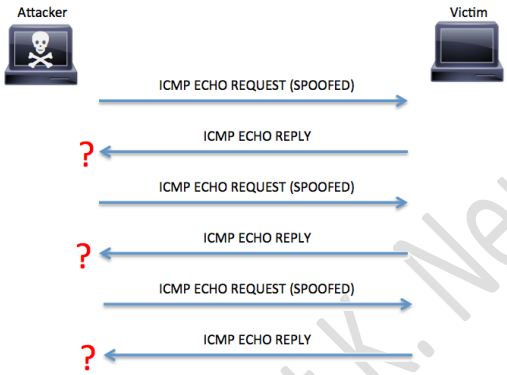
Source Address spoofing (Same as explained in 5.1)

SYN flood (Same as explained in 5.1)

CSS Notes by Amit K. Nerurkar

ICMP flood

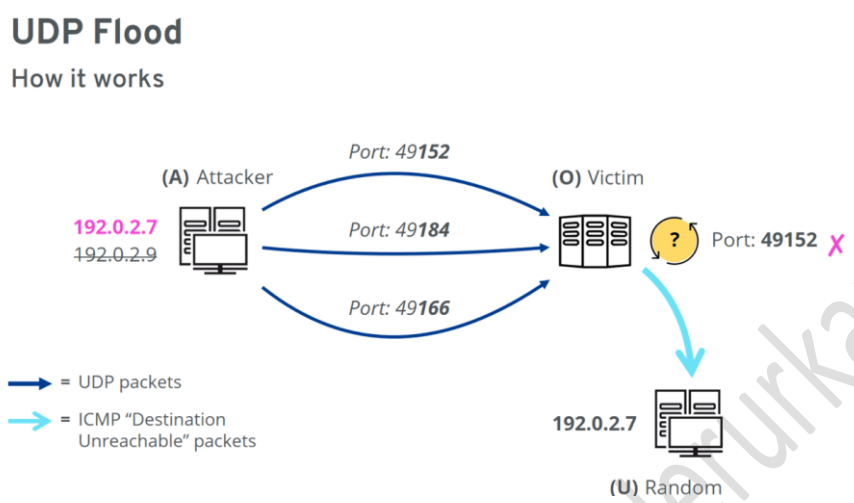
Internet Control Message Protocol (ICMP) flood attacks have existed for many years. They are among the oldest types of DoS attacks. In ICMP flood attacks, the attacker overwhelms the targeted resource with ICMP echo request (ping) packets, large ICMP packets, and other ICMP types to significantly saturate and slow down the victim's network infrastructure.



UDP flood

A UDP flood attack is a type of denial-of-service attack. Similar to other common flood attacks, e.g. ping flood, HTTP flood and SYN flood, the attacker sends a large number of spoofed data packets to the target system. The goal is to overwhelm the target to the point that it can no longer respond to legitimate requests. Once this point is reached, the service comes to a halt.

CSS Notes by Prof. Amit K. Nerurkar



In the event of a UDP flood attack, the following process occurs:

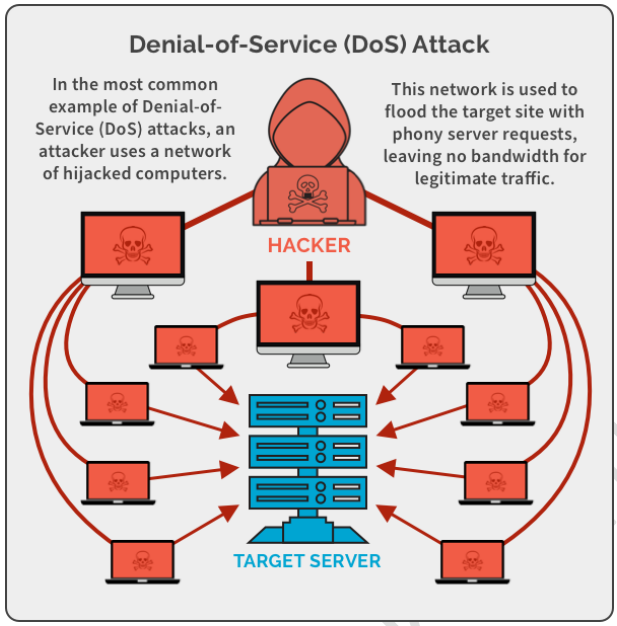
An attacker sends UDP packets with a spoofed IP sender address to random ports on the target system.

On the system side, the following procedure must be repeated for eachincoming packet.
Check the port specified in the UDP packet for a listening application; since it is a randomly selected port, this is generally not the case.
Send an ICMP "destination unreachable" packet to the supposed sender; since the IP address has been spoofed, these packets are usually received by some random bystander.

Distributed Denial of Service

A distributed denial of service (DDoS) attack is when an attacker, or attackers, attempt to make it impossible for a service to be delivered. This can be achieved by thwarting access to virtually anything: servers, devices, services, networks, applications, and even specific transactions within applications. In a DoS attack, it's one system that is sending the malicious data or requests; a DDoS attack comes from multiple systems.

CS Notes by Amit K. Nerurkar



References

1. https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/
2. https://securityboulevard.com/2020/06/denial-of-service-dos-attacks-web-based-application-security-part-7/
3. https://tools.cisco.com/security/center/resources/guide_ddos_defense
4. https://www.ionos.com/digitalguide/server/security/udp-flood/