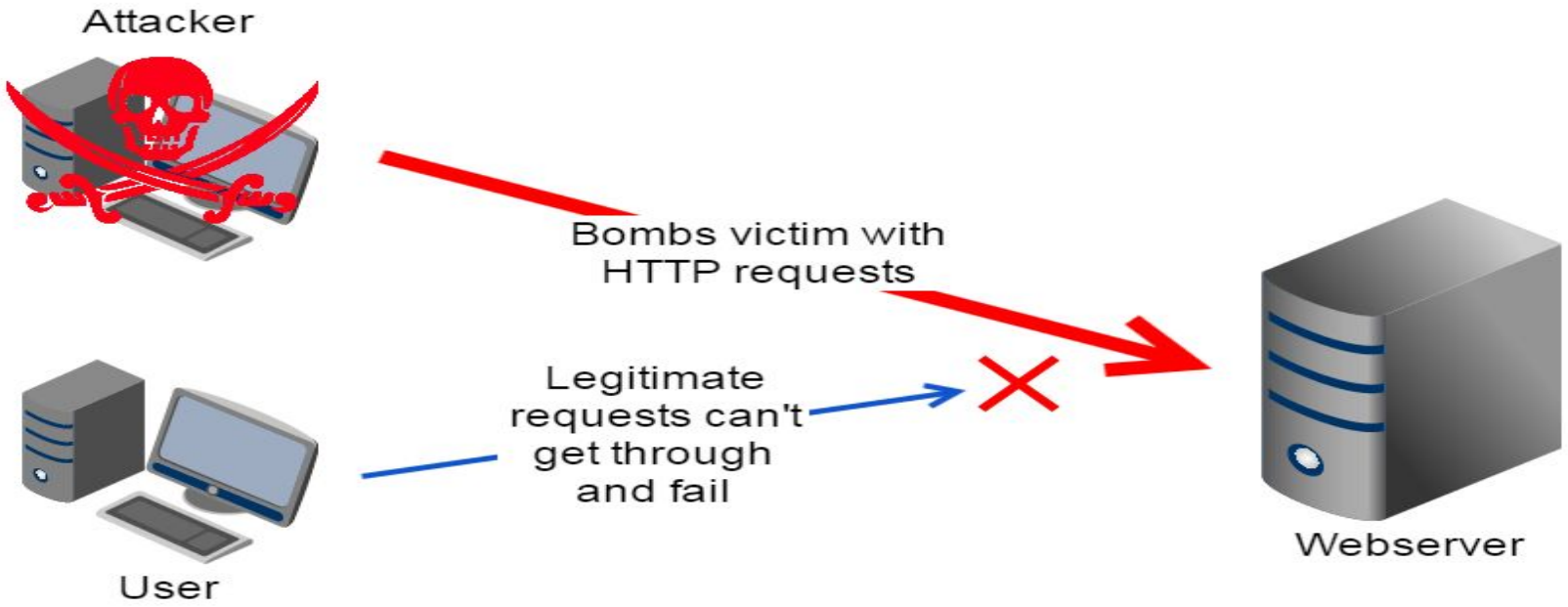
09 Denial of Service

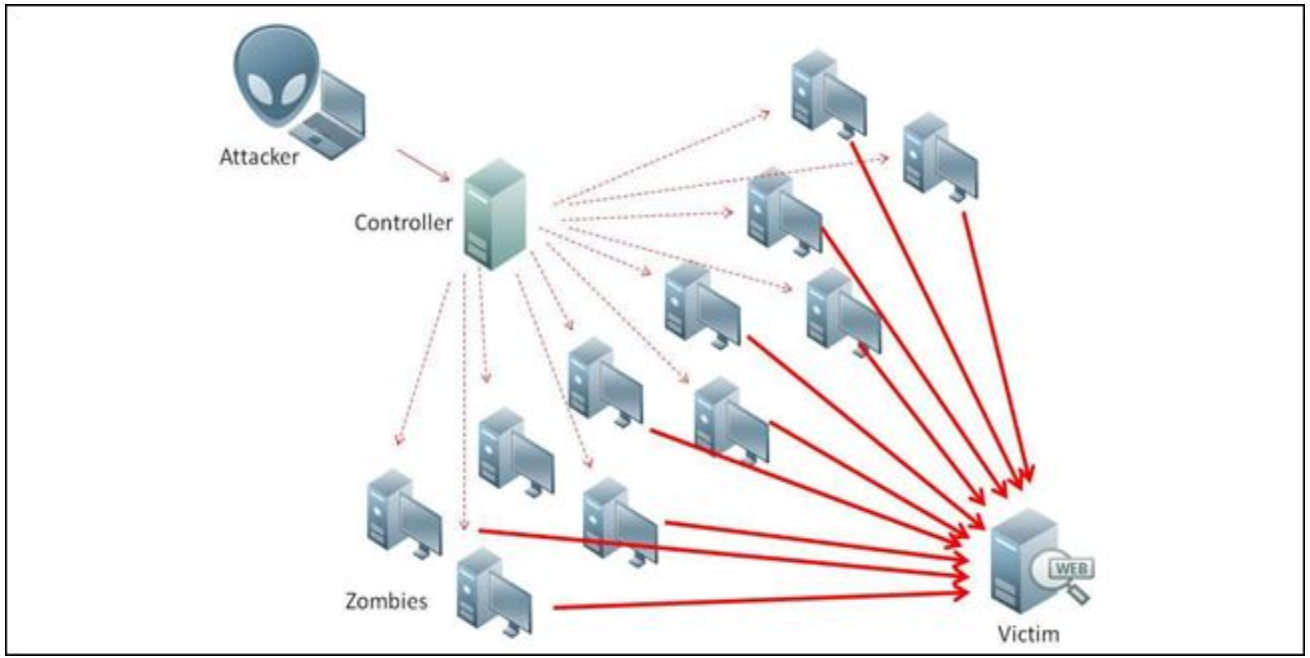
Denial of Service (DoS)

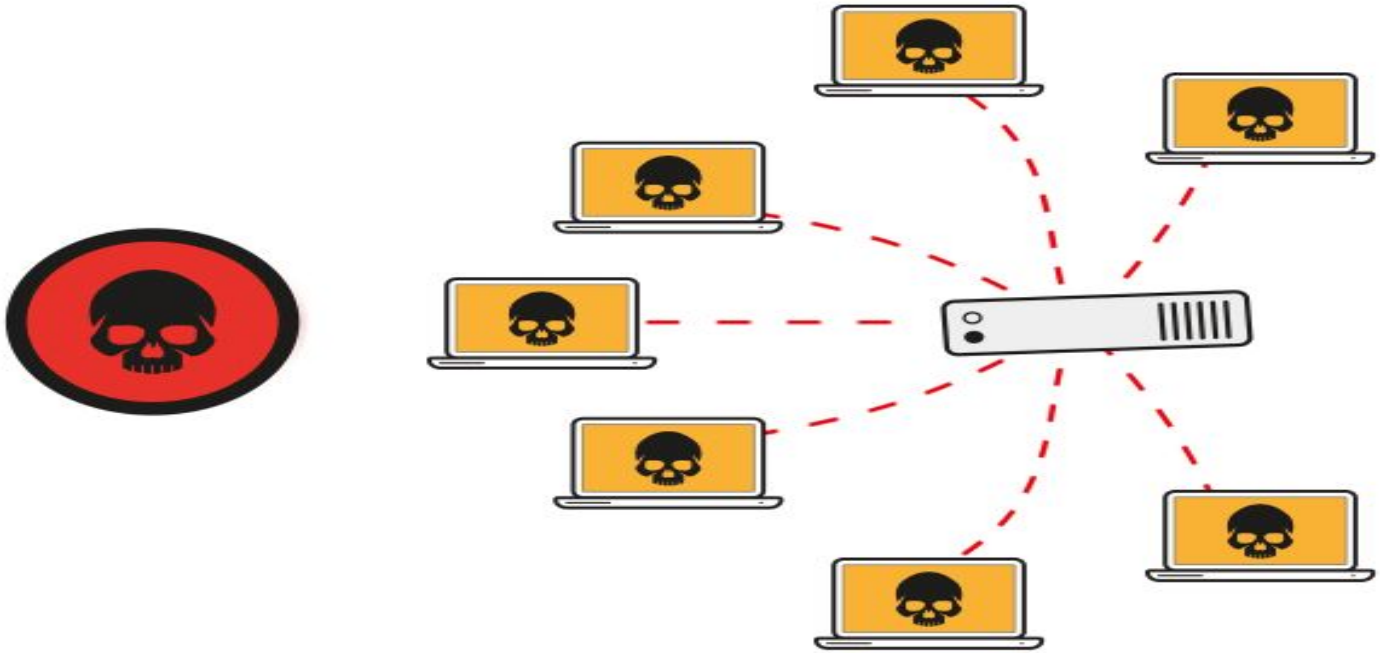
A Denial of Service (DOS) is an attempt to make a machine or network resource unavailable to its intended users, such as temporarily or indefinitely to interrupt or suspend services of a host connected to the internet.


Attacker
Bombs victim with
HTTP requests
Legitimate
requests can't
get through
and fail
User
Webserver

Distributed Denial of Service (DDoS)

A Distributed Denial of Service attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for ex. botnets) flooding the targeted systems with traffic.


Attacker
Controller
Zombies
WEB
Victim



Motivation/ Causes? Reasons

- Ideology - Hacktivists use DoS as means of targeting websites, which they disagree with ideologically.
- Business feuds - It is used for taking down competitor websites, to keep them from participating in significant event, Ex. Flipkart Big Billion Day sale.
- Boredom - Script kiddies use pre-written scripts. The perpetrators are typically bored, would-be hackers looking for adrenaline rush.

- Extortion - Perpetrators use DoS attacks, or the threat of DoS attacks as means of extorting money from their targets.
- Cyber Warfare - Government authorized DDoS attacks can be used to both cripple opposition websites, and an enemy country's infrastructure.

Types of DoS or DDoS attacks

Broadly speaking DoS or DDoS can be divided into three types:

- Volume Based attacks
- Protocol Based attacks
- Application Layer Attacks

Volume based attacks

The goal of this attack is to saturate the bandwidth of attacked site, and magnitude is measured in bits per second (Bps)

Common examples include UDP flood, ICMP flood, and other spoofed packet flood, etc.

Protocol attacks

This type of attack consumes actual server resources or those of intermediate communication equipment such as firewalls and load balancers, and is measured in Packets per second (Pps).

Common examples include SYN flood, Ping of Death, etc.

The goal of these attacks is to crash the web server and are comprised of seemingly legitimate and innocent requests.

Common examples include attacks that target Apache, or Browsers etc

Exploiting System and Application level vulnerabilities

In this method either the application software will have bugs which will cause denial of service situation. Once attacker finds his vulnerabilities, all he has to do is find out the working exploit code for the vulnerability, if somehow attacker finds the exploit code he can use it to DoS the target without any further problems.

Flooding attacks

Attacker will try to find any kind of packets without end limits to the target so that it gets busy receiving junk packets, and thereby not responding to legitimate service requests.

Ping of death

In this method of DoS, the attacker will try to send large sized ping packets which the target cannot handle, thereby causing DoS situation on target device.

The maximum packet length of IP Header is 65535 bytes.

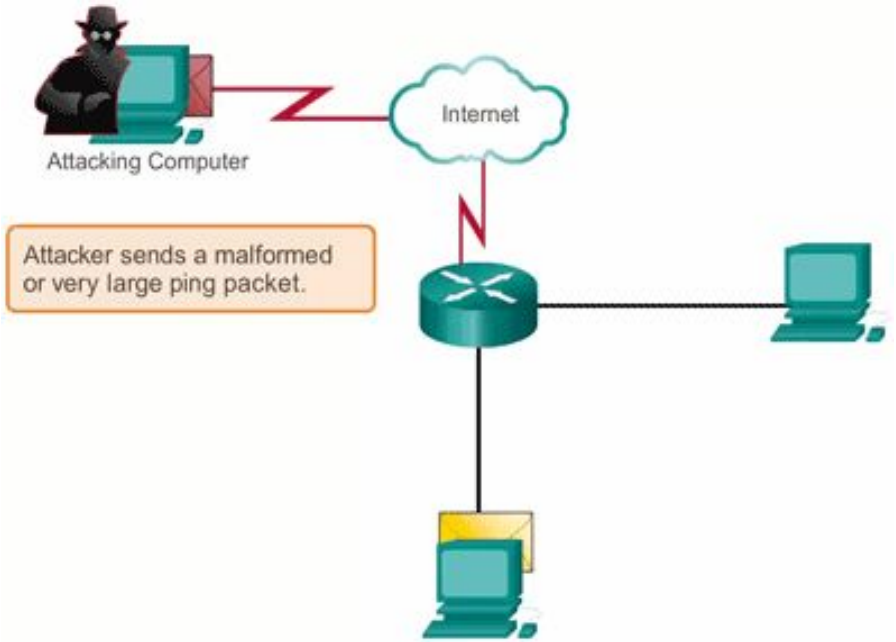
Data Link layer, poses limits to maximum frame size, for example 1500 bytes over an ethernet network.

In such cases large IP packets is split across multiple packets(known as fragments)

The recipient host reassembles fragments to complete packet.

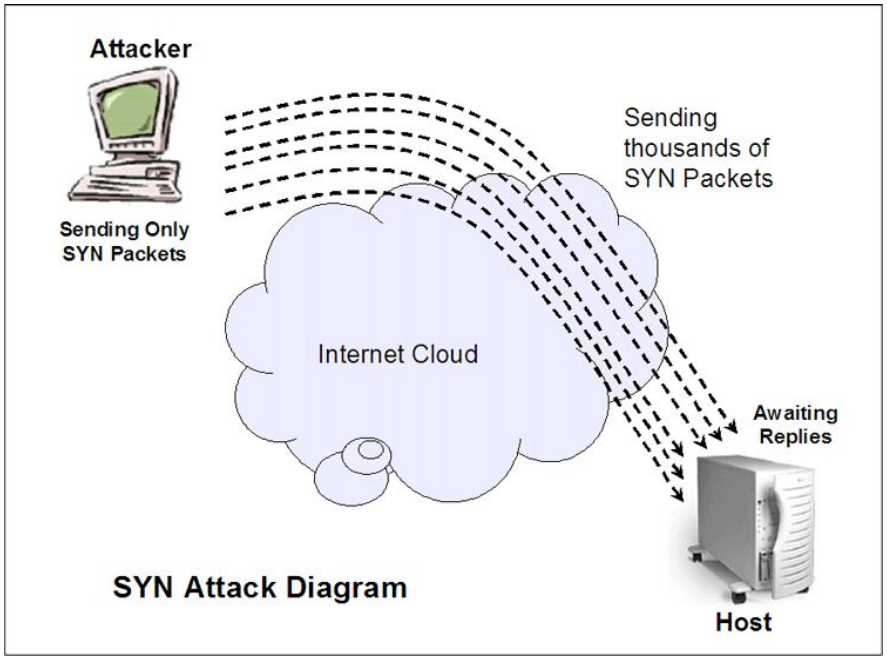
In Ping of death, following malicious manipulation of fragment content, the recipient ends up with IP packet larger than 65535 bytes when reassembled.

This overflows the memory buffer allocated for packet, causing denial of service for legitimate packets


Internet
Attacking Computer
Attacker sends a malformed or very large ping packet.

SYN Flood

A SYN flood DDoS attack exploits a known weakness in the TCP connection sequence (the “three-way handshake”), wherein a SYN request to initiate a TCP connection with a host must be answered by a SYN-ACK response from that host, and then confirmed by an ACK response from the requester. In a SYN flood scenario, the requester sends multiple SYN requests, but either does not respond to the host’s SYN-ACK response, or sends the SYN requests from a spoofed IP address. Either way, the host system continues to wait for acknowledgement for each of the requests, binding resources until no new connections can be made, and ultimately resulting in denial of service.


Attacker
Sending Only
SYN Packets
Sending
thousands of
SYN Packets
Internet Cloud
Awaiting
Replies
Host
SYN Attack Diagram

MAC Flooding

The intelligent device which maintains a table called CAM (Content Addressable Memory) to prevent MitM attacks, but it contains only limited number of entries, so when an attacker tries to overload this CAM table with more number of MAC addresses than its capability, the switch may not be responding to the legitimate requests.

Other Flooding attacks

Attackers can use any other protocol vulnerabilities to flood packets to target devices so that the target device will be busy with handling flood packets and may not respond to the original request made by legitimate user. For ex. IPv6 flood etc.