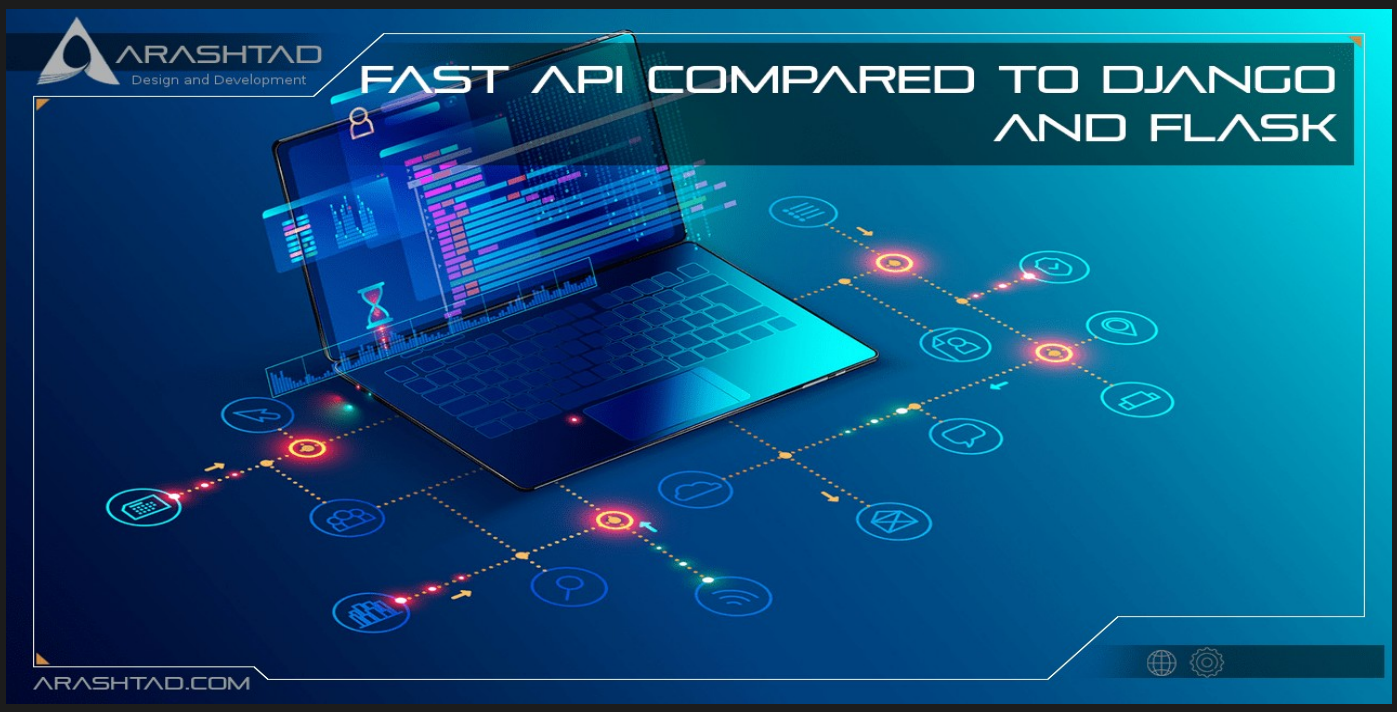
| | |
|---|---|
| Title | WHAT IS DOS ATTACK AND HOW TO PREVENT IT? |
| Description | Intro |
| Date | 2022 22 Augus |
| Author | Arashtad |
| Author URI | https://Arashtad.com |




Denial-of-Service attacks (DoS) shut down a machine or network by flooding it with traffic or sending information that triggers it to crash, preventing its users from accessing it. DoS attacks accomplish this by flooding the target with traffic. The DoS attack robs legitimate users (e.g. employees, members, or account holders) of the services or resources they expect. Often, DoS attacks target the web servers of high-profile organizations, such as banks, commerce, and media firms, as well as government agencies and trade associations. Although DoS attacks rarely result in the theft or loss of significant information or assets, they can cost the victim a lot of time and money to handle.

## HOW DOES A DOS ATTACK HAPPEN?

Often, DoS events are caused by the overloading of a service's underlying systems. In order to clarify how overload-based DoS attacks work, let's imagine an attack on a shopping website. The requests that you make when you shop online pass through your Internet Service Provider's network. Through one or more exchanges, and out to other providers' networks. Once your clicks have passed through the hosting service, they reach the shopping site's infrastructure.
Each server within a shopping site will do a small part of the work needed to create the page you see. These include database servers that provide product lists and application servers that interpret product information. And also, web servers that create the pages you are viewing. Like humans, each server can only do so much work in a given period of time. Thus, when too many users request pages from a shopping site at once, the infrastructure or servers may not be able to handle everyone's requests in a timely manner. This may result in some or all users not being able to view the shopping site. or, to put it another way, they are unable to access the service.

## DOS AND DDOS:

In a Dos attack, the attacker employs a small number of attacking systems (possibly just one) to overload the target. This was the most common approach to attacking the Internet during the early days when services were small and security technology was developing rapidly. Nevertheless, nowadays, a simple DoS attack is usually easy to ward off since the attacker is easily identifiable and blocked. Industrial control systems may be notable exceptions to this, as equipment may not tolerate bogus traffic well, or may be connected via low bandwidth connections that are easily saturated.

On the other hand, in DDos (stands for Distributed Denial of Service) attacks, an attacker recruits (many) thousands of Internet users to send a small number of requests each, which, when combined, overload the target. These participants may be willing accomplices (for example, attacks initiated by loosely organized illegal "hacktivist" groups) or unwitting victims whose machines have been infected with malware.

## DIFFERENT TYPES OF DOS ATTACKS:

## VOLUME BASED ATTACKS

Flooding attacks include UDP floods, ICMP floods, and other spoofed packet floods. The attack aims to overload the attacked site's bandwidth and is measured in bits per second (Bps).

## PROTOCOL ATTACKS

Among them are SYN floods, fragmented packet attacks, Pings of Death, and Smurf DDoS attacks. These attacks consume the actual server resources or those of intermediate communication equipment, such as firewalls and load balancers, and are measured in packets per second (Pps).

## APPLICATION LAYER ATTACKS

There are many types of attacks in this class. These attacks include low-speed attacks, GET/POST floods, attacks on Apache, Windows, or OpenBSD vulnerabilities, and more. Usually composed of seemingly innocent and legitimate requests, these attacks aim to crash the web server. The magnitude of these requests is measured in Requests per second (Rps).

## DIFFERENT TYPES OF DDOS ATTACKS:

UDP Flood
User Datagram Protocol (UDP) floods, by definition, are DDoS attacks that flood a target with UDP packets. Their goal is to flood random ports on a remote server. It causes the host to keep checking for applications listening on that port, and (when none are found) reply with an ICMP 'Destination Unreachable' packet. This consumes host resources, resulting in unavailability.

ICMP (Ping) Flood
This attack is similar to the UDP flood attack in that the target resource is the subject of the attack with ICMP Echo Request (ping) packets. Due to ICMP Echo Reply packets that the victim's server sends, this type of attack consumes both outgoing and incoming bandwidth.

SYN Flood
As a result of a weakness in TCP connection sequence (the "three-way handshake"), an SYN flood DDoS attack exploits a feature of an SYN request. This feature consists of the fact that in order to initiate a TCP connection with a host, an SYN request must be followed by an SYN-ACK reply from that host. And also an ACK response from the requester must come in the following. SYN floods occur when the requester sends multiple SYN requests without acknowledging the host's SYN-ACK response or sends the SYN requests from a spoofed IP address. In either case, the host system keeps waiting for acknowledgments to each request, binding resources until new connections are not possible, resulting in a denial of service.

Ping of Death
In a POD attack, the attacker sends multiple malformed or malicious pings to a computer. the maximum IP packet length is 65,535 bytes (including headers). Nevertheless, the Data Link Layer usually limits the maximum frame size – for example, 1500 bytes over an Ethernet network. In this case, a large IP packet consists of multiple IP packets, and the recipient host reassembles the IP fragments into a complete packet. The recipient ends up with an IP packet with more than 65,535 bytes when reassembled as a result of malicious manipulation of fragment content in a Ping of Death scenario. The packet overflows the memory buffer, causing legitimate packets to underperform.

HTTP Flood
A DDoS attack involving HTTP floods exploits a web server or application using seemingly legitimate HTTP GET or POST requests. HTTP floods don't use sub-standard packets, spoofing, or reflection techniques, and take less bandwidth than other attacks to bring down a site or server. When a server or application has to allocate maximum resources to every request, the attack is most effective.

NTP Amplification
In NTP amplification attacks, the perpetrator exploits publicly-accessible Network Time Protocol (NTP) servers to overwhelm a victim server with UDP traffic. the name of the attack is amplification assault because the query-to-response ratio is anywhere from 1:20 to 1:200. In other words, if an attacker obtains a list of open NTP servers (e.g., by using Metasploit or Open NTP Project data), he or she can easily launch a devastating DDoS attack that is high-bandwidth and high-volume.

Slowris
With Slowloris, one web server can take down another without affecting other services or ports on the target network. Slowloris does this by keeping as many connections as possible open to the target web server. Using Slowloris, the target server has a connection, but only a partial request is sent to the server. Slowloris constantly sends more HTTP headers, but never completes a request. the target server keeps each of these false connections open until the maximum concurrent connection pool reaches the overflow level, which prevents legitimate clients from connecting.

## CONCLUSION:

In this article, you learned about DoS and DDoS attacks and their different types. Most of the attacks occur by creating an overload of requests to the target server by the attacker. The attacker may have different motivations such as a political reason, boredom, money extortion, etc. The Overload DoS attacks may happen on the application layer or the network layer.