Contents

[What are DoS attack? 2](#_Toc38462506)

[General Categories of Attacks 2](#_Toc38462507)

[Volume Based Attacks 2](#_Toc38462508)

[Protocol Attacks 2](#_Toc38462509)

[Application Layer Attacks 2](#_Toc38462510)

[Common DDos Attack Types 3](#_Toc38462511)

[UDP Flood 3](#_Toc38462512)

[ICMP (Ping) Flood 3](#_Toc38462513)

[SYN Flood 3](#_Toc38462514)

[Ping of Death 3](#_Toc38462515)

[Slowloris 3](#_Toc38462516)

[NTP Amplification 4](#_Toc38462517)

[HTTP Flood 4](#_Toc38462518)

[Potential Victim Identification 4](#_Toc38462519)

[DDoS Protection Techniques 5](#_Toc38462520)

[Reduce Attack Surface Area 5](#_Toc38462521)

[Plan for Scale 5](#_Toc38462522)

[Know what is normal and abnormal traffic 5](#_Toc38462523)

[Deploy Firewalls for Sophisticated Application Attacks 5](#_Toc38462524)

[Bibliography 5](#_Toc38462525)

# What are DoS attack?

DoS is one of the oldest forms of cyber extraction attacks. The term DoS means **Denial of Service** and as it indicates, it denies its service to a legitimate user. If an airline website is brought down, for example, it fails to serve the people who want to buy tickets or get informed about their already booked flight.[1]

In general, DDoS attacks can be segregated by which layer of the Open Systems Interconnection (OSI) model they attack. They are most common at the Network (layer 3), Transport (Layer 4), Presentation (Layer 6) and Application (Layer 7) Layers.[4]

A DoS attack can happen in two ways:

1. With **specially crafted data**. If specially crafted data is sent to the victim server and if the victim server is not set up to handle the data, there are chances that it may crash. This does not involve sending too much data but includes specially crafted data packets that the victim fails to handle. This can involve manipulating fields in the network protocol packets, exploiting servers, and so on. **Ping of death** attacks are an example of such attacks.[1]
2. With **Flooding**. Sending too much data to the victim site can also slow it down. The site will spend resources on consuming the attackers’ data and fail to serve the legitimate data. This can be a DDoS attack where packets are sent to the victim by the attacker from many computers. **Slowloris** attacks are an example of such attacks.[1]

Of course, attacks can also use a combination of both. For example, **UDP flooding** attacks are an example of such attacks. There is another form of DoS attack. A DoS attack uses a single computer to carry out the attack. DDoS attack uses a series of computers to carry out the attack. sometimes the target server is flooded with so much data that it can't handle it. another way is to exploit the workings of internal protocols. DDoS attack that deals with extortion is often termed a ransom DDoS.[1]

## General Categories of Attacks

### Volume Based Attacks

These attacks include the **UDP floods**, **ICMP floods**, and other spoofed-packet floods. The attack’s goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).[2]

### Protocol Attacks

These attacks include **SYN floods**, **fragmented packet attacks**, **Ping of Death**, **Smurf DDoS** and more. 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). [2]

### Application Layer Attacks

Includes **low-and-slow** attacks, **GET/POST floods**, **attacks that target Apache, Windows or OpenBSD vulnerabilities** and more. Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server, and the magnitude is measured in Requests per second (Rps).[2]

# Common DDos Attack Types

Some of the most used DDoS attack types include:

## UDP Flood

A UDP flood, by definition, is any DDoS attack that floods a target with User Datagram Protocol (UDP) packets. The goal of the attack is to flood random ports on a remote host. This causes the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP ‘Destination Unreachable’ packet. This process saps host resources, which can ultimately lead to inaccessibility.[2]

## ICMP (Ping) Flood

Similar in principle to the UDP flood attack, an ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim’s servers will often attempt to respond with ICMP Echo Reply packets, resulting a significant overall system slowdown.[2]

## 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](https://www.imperva.com/learn/application-security/denial-of-service/).[2]

## Ping of Death

A ping of death (“POD”) attack involves the attacker sending multiple malformed or malicious pings to a computer. The maximum packet length of an IP packet (including header) is 65,535 bytes. However, the Data Link Layer usually poses limits to the maximum frame size – for example 1500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets (known as fragments), and the recipient host reassembles the IP fragments into the complete packet. In a Ping of Death scenario, following malicious manipulation of fragment content, the recipient ends up with an IP packet which is larger than 65,535 bytes when reassembled. This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets.[2]

## Slowloris

Slowloris is a highly-targeted attack, enabling one web server to take down another server, without affecting other services or ports on the target network. Slowloris does this by holding as many connections to the target web server open for as long as possible. It accomplishes this by creating connections to the target server, but sending only a partial request. Slowloris constantly sends more HTTP headers, but never completes a request. The targeted server keeps each of these false connections open. This eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.[2]

## NTP Amplification

In NTP amplification attacks, the perpetrator exploits publicly accessible Network Time Protocol (NTP) servers to overwhelm a targeted server with UDP traffic. The attack is defined as an amplification assault because the query-to-response ratio in such scenarios is anywhere between 1:20 and 1:200 or more. This means that any attacker that obtains a list of open NTP servers (e.g., by a using tool like Metasploit or data from the Open NTP Project) can easily generate a devastating high-bandwidth, high-volume DDoS attack.[2]

## HTTP Flood

In an HTTP flood DDoS attack, the attacker exploits seemingly legitimate HTTP GET or POST requests to attack a web server or application. HTTP floods do not use malformed packets, spoofing or reflection techniques, and require less bandwidth than other attacks to bring down the targeted site or server. The attack is most effective when it forces the server or application to allocate the maximum resources possible in response to every single request.[2]

# Potential Victim Identification

Often the first and easy step in DDoS target acquisition is to review the target website looking for high-risk components. Of particular interest to an attacker is any content that is dynamically generated or pulled from a database. By targeting dynamic content, an attack is more likely to pass through a CDN provider to impact the backend servers. Similarly, requests of resources that are likely to be CPU intensive are frequently targeted because it is more efficient for the attacker.[3]

Common HTTP(S) application layer attack targets often include:

* Login functionality
* Search functionality
* Any web form
* Large image or document objects not hosted on a CDN

An attacker will also use port scanners to automatically look for target networks that run susceptible services. A port scanner is simply a tool that lets someone probe a network and get a list of what services are accessible from the internet. Of particular note is the speed with which a port scanner can probe a network. A modest server can scan a host in under a second, and an entire /16 network in 12 hours. [3]

To expand the list of potential targets an attacker invariably investigates ancillary services that are critical to the operation of the target. Although the target may be heavily defending their web server, they may be leaving other less obvious components exposed. In the webinar, the target hostname was hosted on a less heavily fortified DNS server, and it was this weak point that the attacker targeted. When reviewing DDoS defenses it’s always important to be aware of all components of the environment, and take note of any unprotected areas. It’s these weak links that will fail during a DDoS attack.[3]

# DDoS Protection Techniques

## Reduce Attack Surface Area

One of the first techniques to mitigate DDoS attacks is to minimize the surface area that can be attacked thereby limiting the options for attackers and allowing the creation of protections in a single place. We want to ensure that we do not expose our application or resources to ports, protocols or applications from where they do not expect any communication. Thus, minimizing the possible points of attack and allowing the concentration on mitigating efforts. In some cases, it can be done by placing the computation resources behind [Content Distribution Networks (CDNs)](https://aws.amazon.com/cloudfront/) or [Load Balancers](https://aws.amazon.com/elasticloadbalancing/) and restricting direct Internet traffic to certain parts of the infrastructure like the database servers. In other cases, firewalls or [Access Control Lists (ACLs)](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html) can be used to control what traffic reaches the applications.[4]

## Plan for Scale

The two key considerations for mitigating large scale volumetric DDoS attacks are bandwidth (or transit) capacity and server capacity to absorb and mitigate attacks. Transit capacity is defined as the redundancy of Internet connectivity, allowing the target server to handle large volume of traffic. Server capacity is defined as the amount of computation resources and the ability to scale them up or down depending on demand.[4]

## Know what is normal and abnormal traffic

Whenever elevated levels of traffics are detected hitting a host, the very baseline is to be able only to accept as much traffic as our host can handle without affecting availability. This concept is called rate limiting. More advanced protection techniques can go one step further and intelligently only accept traffic that is legitimate by analyzing the individual packets themselves. To do this, we need to understand the characteristics of good traffic that the target usually receives and be able to compare each packet against this baseline.[4]

## Deploy Firewalls for Sophisticated Application Attacks

A good practice is to use a Web Application Firewall (WAF) against attacks, such as SQL injection or cross-site request forgery, that attempt to exploit a vulnerability in the application itself. Additionally, due to the unique nature of these attacks, we should be able to easily create customized mitigations against illegitimate requests which could have characteristics like disguising as good traffic or coming from bad IPs, unexpected geographies, etc. At times it might also be helpful in mitigating attacks as they happen to get experienced support to study traffic patterns and create customized protections.[4]

# Bibliography

1. Mohanta, A., Hahad, M., & Velmurugan, K. (2018). *Preventing ransomware*.
2. DDoS Attack Types & Mitigation Methods | Imperva. Retrieved 22 April 2020, from <https://www.imperva.com/learn/application-security/ddos-attacks/>
3. How Attackers Find Security Gaps to Exploit Them for DDoS Attacks. (2016). Retrieved 22 April 2020, from <https://www.imperva.com/blog/attackers-identify-ddos-targets/>
4. What is a DDOS Attack & How to Protect Your Site Against One. Retrieved 22 April 2020, from https://aws.amazon.com/shield/ddos-attack-protection/