# What is DDoS Attack?

A Distributed Denial of Service (DDoS) attack attempts to make an online service or a website unavailable by overloading it with vast floods of internet traffic generated from multiple sources. Exploited machines can include computers and other networked resources such as IoT devices.

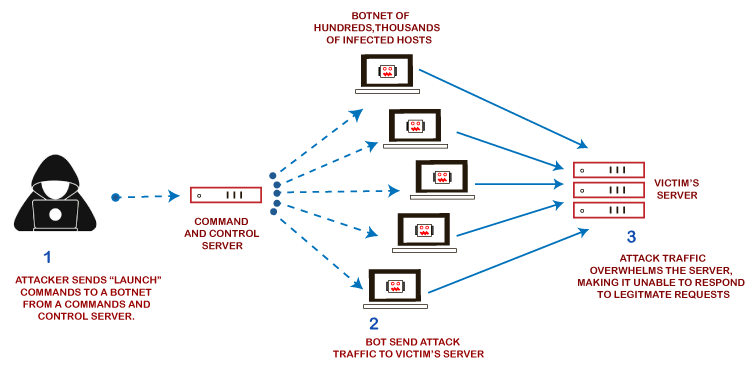
A Denial of Service (DoS) attack, in which one computer and one Internet connection are used to flood a targeted resource with packets, but a DDoS attack uses many computers and many Internet connections, often distributed globally in what is referred to as a **botnet**.

A large-scale volumetric DDoS attack can generate traffic measured in tens of Gigabits (and even hundreds of Gigabits) per second. A regular network will not be able to handle such traffic.

Attackers build a network of hacked machines known as **botnets** by spreading malicious code through emails, websites, and social media. Once these computers are infected, they can be controlled remotely, without their owners' knowledge, and used as an army to launch an attack against any target.

**How DDoS attack works?**

DDoS attacks are carried out with networks of Internet-connected machines. A DDoS attack can be generated in the following step by step way, such as:



1. These networks consist of computers and other devices such as IoT devices that have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots or zombies, and a group of bots is called a **botnet**.
2. Once a botnet has been established, the attacker can direct an attack by sending remote instructions to each bot. It can use for sending more connection requests than a server can handle at a time.
3. Attackers can have computers send a victim resource huge amounts of random data to use up the target's bandwidth.
4. When the botnet targets a victim's server or network, each bot sends requests to the target's IP address, potentially causing the server or network to become overload, resulting in a denial-of-service to regular traffic.

Due to the distributed nature of these machines, they can use to generate distributed high traffic, which may be difficult to handle. It finally results in a complete blockage of a service.

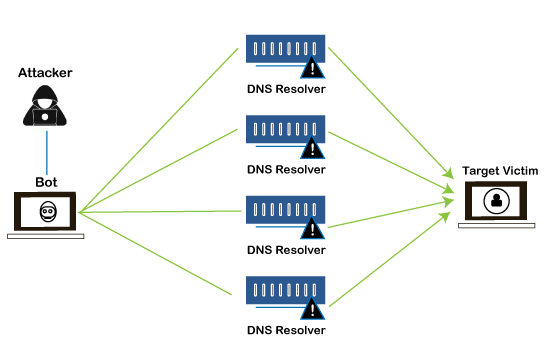
### **Types of DDoS Attacks**

Distributed Denial of Service attacks can be broadly categorized into these three categories:

**1. Volume-Based Attacks**

Volume-based attacks use massive amounts of fake traffic to overwhelm a resource such as a website or a server.

It includes TCP floods, UDP floods, ICMP floods, and other spoofed-packet floods. These are also called Layer 3 & 4 Attacks. Here, an attacker tries to saturate the bandwidth of the target site. The attack magnitude is measured in **Bits per Second** (bps).

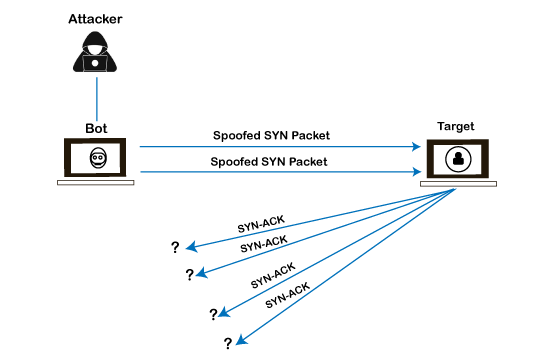


* **Amplification Attack:** The attacker makes a request that generates a significant response which includes DNS requests for large TXT records and HTTP GET requests for large files like images, PDFs, or any other data files.
* **UDP Flood:** A UDP flood is used to flood random ports on a remote host with numerous UDP packets, more specifically port number 53. Specialized firewalls are used to filter out or block malicious UDP packets.
* **ICMP Flood:** This is similar to UDP flood and flooded a remote host with numerous ICMP Echo Requests. This type of attack can consume both outgoing and incoming bandwidth, and a high volume of ping requests will result in overall system slowdown.
* **HTTP Flood:** The attacker sends HTTP GET and POST requests to a targeted web server in a large volume that the server cannot handle and leads to denial of additional connections from legitimate clients.

**2. Protocol Attacks**

Protocol or network-layer DDoS attacks send large numbers of packets to targeted network infrastructures and infrastructure management tools.

It includes SYN floods, Ping of Death, fragmented packet attacks, Smurf DDoS, etc. This type of attack consumes existing server resources and other resources, such as firewalls and load balancers. The attack magnitude is measured in **Packets per Second** (PPS).

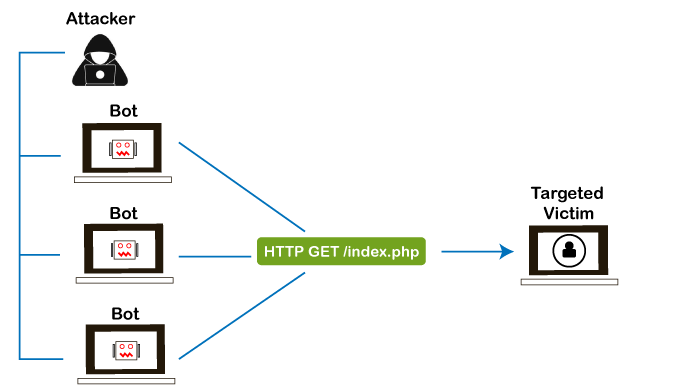


* **SYN Flood:** The attacker sends TCP connection requests faster than the targeted machine can process them, causing network saturation. Administrators can tweak TCP stacks to mitigate the effect of SYN floods. To reduce the effect of SYN floods, you can reduce the timeout until a stack frees memory allocated to a connection or selectively dropping incoming connections using a **firewall** or **iptables**.
* **DNS Flood:** DNS floods are used for attacking both the infrastructure and a DNS application to overload a target system and consume all its available network bandwidth.
* **Ping of Death:** The attacker sends malformed or oversized packets using a simple ping command. IP allows sending 65,535 bytes packets but sending a ping packet larger than 65,535 bytes violates the Internet Protocol and could cause memory overflow on the target system and finally crash the system. Many sites block ICMP ping messages altogether at their firewalls to avoid Ping of Death attacks and their variants.

**3. Application Layer Attacks**

Flooding applications with maliciously crafted requests conduct Application-layer attacks. The size of application-layer attacks is measured in requests per second (rps).

It includes Slowloris, Zero-day DDoS attacks, DDoS attacks that target Apache, Windows, or OpenBSD vulnerabilities, and more. Here the goal is to crash the webserver.



* **Application Attack:** This is also called Layer 7 Attack, where the attacker makes excessive log-in, database-lookup, or search requests to overload the application. It is tough to detect Layer 7 attacks because they resemble legitimate website traffic.
* **Slowloris:** The attacker sends many HTTP headers to a targeted web server but never completes a request. The targeted server keeps each of these false connections open and eventually overflows the maximum concurrent connection pool, leading to a denial of additional connections from legitimate clients.
* **NTP Amplification:** The attacker exploits publically accessible Network Time Protocol (NTP) servers to overwhelm the targeted server with User Datagram Protocol (UDP) traffic.
* **Zero-day DDoS Attacks:** Zero-day vulnerability is a system or application flaw previously unknown to the vendor and has not been fixed or patched. These are new types of attacks coming into existence day by day, such as exploiting vulnerabilities for which no patch has yet been released.

### **How to Fix a DDoS Attack**

You must be careful while approaching and selecting a DDoS protection service provider. Many service providers want to take advantage of your situation. If you inform them that you are under a DDoS attack, they will start offering you various services at unreasonably high costs.

If you see a low magnitude of the DDoS, you can find many firewall-based solutions that can help you filter out DDoS-based traffic. If you have a high volume of DDoS attacks like in gigabits or even more, you should take the help of a DDoS protection service provider that offers a more holistic, proactive, and genuine approach.

There are quite a few DDoS protection options that you can apply depending on the type of DDoS attack.

**1. Blocking vulnerable ports**

Your DDoS protection starts from identifying and closing all the possible OS and application-level vulnerabilities in your system, closing all the possible ports, removing unnecessary access from the system, and hiding your server behind a proxy or CDN system.

**2. Configure firewalls and routers**

Firewalls and routers should be configured to reject bogus traffic, and you should keep your routers and firewalls updated with the latest security patches. These remain your initial line of defense.

Application front-end hardware integrated into the network before traffic reaches a server analyzes and screens data packets classifying the data as a priority, regular, or dangerous as they enter a system and can be used to block threatening data.

**3. Consider artificial intelligence**

While present defenses of advanced firewalls and intrusion detection systems are common, AI is being used to develop new systems.

The systems that can quickly route Internet traffic to the cloud, where it's analyzed, and malicious web traffic blocked before it reaches a company's computers. Such AI programs could identify and defend against known DDoS indicative patterns. Plus, the self-learning capabilities of AI would help predict and identify future DDoS patterns.

Researchers are exploring the use of blockchain, the same technology behind Bitcoin and other cryptocurrencies, to permit people to share their unused bandwidth to absorb the malicious traffic created in a DDoS attack and render it ineffective.

**4. Secure IoT devices**

If you have IoT devices, you should make sure your devices are formatted for maximum protection. Secure passwords should be used for all devices. IoT devices have been vulnerable to weak passwords, with many devices operating with easily discovered default passwords.

A strong firewall is also important. Protecting your devices is an essential part of Cyber Safety.

**5. Application front end hardware**

Application front-end hardware is intelligent hardware placed on the network before traffic reaches the servers. It can be used on networks in conjunction with routers and switches. Application front-end hardware analyzes data packets as they enter the system and then identifies them as a priority, regular, or dangerous. There are more than 25 bandwidth management vendors.

**6. Blackhole and sinkhole**

With **blackhole** routing, all the traffic to the attacked DNS or IP address is sent to a "black hole" (null interface or a non-existent server). It is managed by the ISP to be more efficient and avoid affecting network connectivity.

A DNS **sinkhole** routes traffic to a valid IP address which analyzes traffic and rejects bad packets. Sinkholing is not efficient for most severe attacks.

**7. IPS based prevention**

Intrusion prevention systems (IPS) are effective if the attacks have signatures associated with them. However, the trend among the attacks is to have legitimate content but bad intent. Intrusion-prevention systems which work on content recognition cannot block behavior-based DoS attacks.

An ASIC-based IPS may detect and block denial-of-service attacks because they have the processing power and the granularity to analyze the attacks and act like a circuit breaker in an automated way.

A rate-based IPS (RBIPS) must analyze traffic granularly and continuously monitor the traffic pattern and determine if there is a traffic anomaly. It must let the legitimate traffic flow while blocking the DoS attack traffic.

**8. DDS based defense**

More focused on the problem than IPS, a DoS defense system (DDS) can block connection-based DoS attacks and those with legitimate content but bad intent. A DDS can also address both protocol attacks (such as teardrop and ping of death) and rate-based attacks (such as ICMP floods and SYN floods). DDS has a purpose-built system that can quickly identify and obstruct denial of service attacks at a more incredible speed than software that is based system.

**9. Switches**

Most switches have some rate-limiting and ACL capability. Some switches provide automatic or system-wide rate limiting, traffic shaping, delayed binding (TCP splicing), deep packet inspection, and Bogon filtering (bogus IP filtering) to detect and remediate DoS attacks through automatic rate filtering and WAN Link failover and balancing.

These schemes will work as long as the DoS attacks can be prevented by using them. For example, SYN flood can be prevented using delayed binding or TCP splicing. Similarly, content-based DoS may be prevented using deep packet inspection. Attacks originating from dark addresses or going to dark addresses can be prevented using bogon filtering. Automatic rate filtering can work as long as set rate thresholds have been set correctly. Wan-link failover will work as long as both links have DoS/DDoS prevention mechanism.

# Difference between DOS and DDOS attack

**1. DOS Attack**is a denial of service attack, in this attack a computer sends a massive amount of traffic to a victim’s computer and shuts it down. Dos attack is an online attack that is used to make the website unavailable for its users when done on a website. This attack makes the server of a website that is connected to the internet by sending a large number of traffic to it.

**2. DDOS Attack**means distributed denial of service in this attack dos attacks are done from many different locations using many systems.

**Difference between DOS and DDOS attacks:**

| **DOS** | **DDOS** |
| --- | --- |
| 1.DOS Stands for Denial of service attack. | DDOS Stands for Distributed Denial of service attack. |
| 2. In Dos attack single system targets the victim system. | In DDoS multiple systems attacks the victims system.. |
| 3. Victim PC is loaded from the packet of data sent from a single location. | Victim PC is loaded from the packet of data sent from Multiple location. |
| 4.Dos attack is slower as compared to DDoS. | DDoS attack is faster than Dos Attack. |
| 5.Can be blocked easily as only one system is used. | It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations. |
| 6.In DOS Attack only single device is used with DOS Attack tools. | In DDoS attack,The volumeBots are used to attack at the same time. |
| 7.DOS Attacks are Easy to trace. | DDOS Attacks are Difficult to trace. |
| 8.Volume of traffic in the Dos attack is less as compared to DDos. | DDoS attacks allow the attacker to send massive volumes of traffic to the victim network. |
| 9.Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack 4. Flooding Attack | Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks 4. Protocol Attack. |