Denial of Service (Dos)

A Denial-of-Service attack (DoS) is when someone attempts to stop someone else from viewing portions of the internet.

There are different types of Dos attacks:

- Flood attack – a very common method of attack involves flooding the target machine with external communications requests, so that it cannot respond to legitimate traffic, or responds so slowly as to be made unavailable. These attacks usually cause a server overload. DoS attacks are employed by either making the targeted computer(s) to reset, or overwhelming its resources so that it can no longer deliver its intended service or blocking the communication media between the intended users and the victim so that they can no longer communicate effectively.

- Logic and software attacks - Internet packets (packets of data) are sent that should use bugs in the software or system. These attacks are easier to protect against because firewall or software patches usually correct the problem.

- Distributed Denial-of-Service attack - This type of attack uses either flood attacks or logic attacks, but it uses many people, different computers, or bots (Botnet) under the attacker's control. This type of attack is one of the most often used, and usually against business and company websites. Perpetrators of DDoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. This type of attack is often the hardest to prevent, track, and stop.

Denial-of-service attacks are considered violations of the acceptable use policies of practically all Internet service providers. They also commonly are violations of the laws of individual nations.

The United States Computer Emergency Readiness Team (US-CERT) defines symptoms of denial-of-service attacks to include:

- Unusually slow network performance (opening files or accessing web sites)
- Unavailability of a particular web site
- Inability to access any web site
- Dramatic increase in the number of spam emails received—(this type of DoS attack is considered an e-mail bomb)
- Disconnection of a wireless or wired internet connection
- Long term denial of access to the web or any internet services

If the attack is conducted on a sufficiently large scale, entire geographical sections of Internet connectivity can be compromised without the attacker's knowledge or intent by inaccurately designed or flimsy network infrastructure equipment.

Popular Types of Attacks

Smurf attack and Ping flood

A smurf attack is one specific variation of a flooding DDoS attack on the public Internet. It relies on misconfigured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine. The network then serves as a smurf amplifier. The perpetrators will send large numbers of IP packets with the source address forged to appear to be the address of the victim. The network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination

Ping flood is centered on sending the victim an overpowering number of ping packets, usually using the "ping" command from Unix-like hosts. It is very simple to launch, the primary requirement being access to greater bandwidth than the victim.

How to prevent dos attacks?

To alleviate DDOS attacks then you must first check if your server mainly your Domain Name System server is safe and under lockdown

In order to prevent a DDOS attack you must:

- Set up simple commands for your firewall to permit or reject IP address, ports or protocols.
- Check your switch and limit your server’s bandwidth and set a limit to prevent it from being hit by a considerable amount of traffic.
- Get application front end hardware to examine your data packets as they go through the system
- Add filters to your router and get it to eliminate packets from apparent resources of attack.
- Set effective and aggressive time-outs for half-open connections.
- Set a lesser Synchronous, Internet Control Message Protocol and User Datagram Protocol flood drop entry points.

Doing these simple steps can help answer your questions about how to protect server from DDOS. This isn’t all though you should always keep a watchful eye out for these kinds of acts as no system or server is foolproof. If you get too complacent then your server might be more vulnerable to an attack.