ICMP Flood Attack

An Internet Control Message Protocol (ICMP) flood DDoS attack, also known as a Ping flood attack, is a common Denial-of-Service (DoS) attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings). Normally, ICMP echo-request and echo-reply messages are used to ping a network device in order to diagnose the health and connectivity of the device and the connection between the sender and the device. By flooding the target with request packets, the network is forced to respond with an equal number of reply packets. This causes the target to become inaccessible to normal traffic]

Others types of ICMP request attacks may involve custom tools or code, such as hping and scapy. An ICMP flood DDoS attack requires that the attacker knows the IP address of the target.

Because an ICMP flood DDoS attacks overwhelm the targeted device's network connections with bogus traffic, legitimate requests are prevented from getting through.

UDP flood attack

A UDP flood is a type of denial-of-service attack in which a large number of User Datagram Protocol (UDP) packets are sent to a targeted server with the aim of overwhelming that device's ability to process and respond. The firewall protecting the targeted server can also become exhausted as a result of UDP flooding, resulting in a denial-of-service to legitimate traffic.

A UDP flood works primarily by exploiting the steps that a server takes when it responds to a UDP packet sent to one of it's ports. Under normal conditions, when a server receives a UDP packet at a particular port, it goes through two steps in response:

1. The server first checks to see if any programs are running which are presently listening for requests at the specified port.

2. If no programs are receiving packets at that port, the server responds with a ICMP (ping) packet to inform the sender that the destination was unreachable.