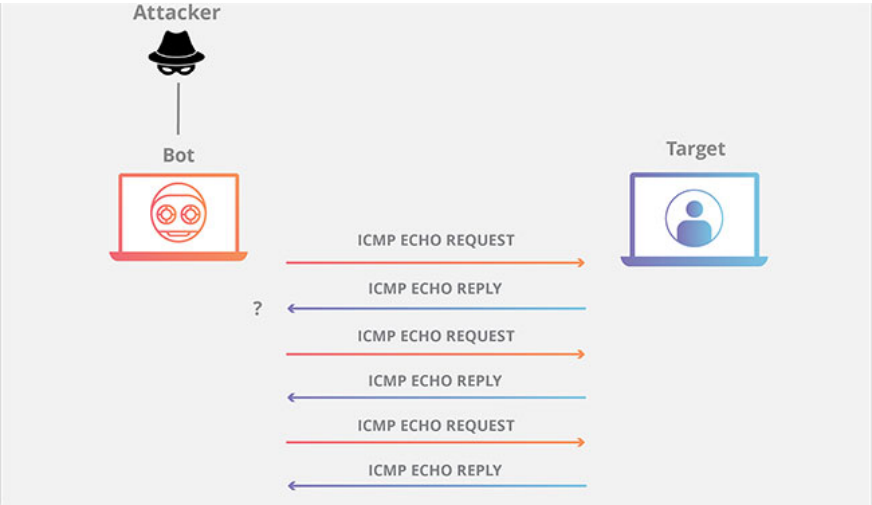
What is DDoS ICMP Flood?

An ICMP (Internet Control Message Protocol) Flood attack, also known as a Ping Flood attack, is a common denial of service (DoS) attack in which an attacker tries to overwhelm a device target with ICMP echo-request (ping).

Typically, ICMP echo-request and echo-reply messages are used to ping a network device to diagnose the device's health and connectivity, and the connection between the sender and the device. By flooding the target with the request packets, the network is forced to respond with an equal number of reply packets. This makes the target inaccessible for normal traffic.

Other types of ICMP request attacks may involve custom tools or code, such as hping and scapy. Attack traffic emitted by multiple devices is considered a distributed denial of service (DDoS) attack. In this type of DDoS attack, both the incoming and outgoing channels of the network are overwhelming, consuming significant bandwidth and leading to denial of service.



What are the signs of an ICMP Flood attack?

An ICMP Flood DDoS attack requires an attacker to know the target's IP address. Attacks can be divided into 3 categories, determined by the target and how the IP address is resolved:

Revealed local target - In this type of DDoS attack, the Ping Flood attack targets a specific computer on the local network. In this case, the attacker must obtain the destination IP address in advance.

Router revealed - Here, the Ping Flood attack targets routers with the aim of interrupting communication between computers on the network. In this type of DDoS attack, the attacker must have the internal IP address of the local router.

Blind ping - This involves using an external program to reveal the IP address of the target computer or router before launching a DDoS attack.

Why are ICMP Flood attacks dangerous?

Because the ICMP Flood DDoS attacks overwhelm the targeted device's network connections with bogus traffic, legitimate requests are blocked. This scenario constitutes a critical level of a DoS or DDoS attack (in the case of multiple coordinated attacks).

What makes this attack vector even more dangerous is that in the past, attackers would forge a false IP address to conceal the sending device. But with today's sophisticated botnet attacks (especially IoT-based bots), the attackers don't even bother to conceal the bot's IP. Instead, they use an extensive network of bots that have not been tampered with to overwhelm the target server.

You finished reading the article "**What is DDoS ICMP Flood?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com