**Ping flood Attack**

**Description 1**

Ping flood attack is similar to Smurf attack wherein the victim is bombarded with thousands of ping packets. [1]

**Description 2**

A ping flood is a simple denial-of-service attack where the attacker overwhelms the victim with ICMP "echo request" (ping) packets. This is most effective by using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies. Most implementations of ping require the user to be privileged in order to specify the flood option. It is most successful if the attacker has more bandwidth than the victim (for instance an attacker with a DSL line and the victim on a dial-up modem). The attacker hopes that the victim will respond with ICMP "echo reply" packets, thus consuming both outgoing bandwidth as well as incoming bandwidth. If the target system is slow enough, it is possible to consume enough of its CPU cycles for a user to notice a significant slowdown. [2]

**Description 3**

Ping flood, also known as ICMP flood, is a common Denial of Service (DoS) attack in which an attacker takes down a victim's computer by overwhelming it with ICMP echo requests, also known as pings.

The attack involves flooding the victim's network with request packets, knowing that the network will respond with an equal number of reply packets. Additional methods for bringing down a target with ICMP requests include the use of custom tools or code, such as hping and scapy.

This strains both the incoming and outgoing channels of the network, consuming significant bandwidth and resulting in a denial of service. [3]

**Reference**

**[1]** [**https://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi-33764**](https://www.sans.org/reading-room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi-33764)

**[2]** [**https://en.wikipedia.org/wiki/Ping\_flood**](https://en.wikipedia.org/wiki/Ping_flood)

**[3]** [**https://www.incapsula.com/ddos/attack-glossary/ping-icmp-flood.html**](https://www.incapsula.com/ddos/attack-glossary/ping-icmp-flood.html)