Name : Pankaj Parihar

Roll No.: 74

Batch: T21

Assignment – 9

Aim : To simulate DOS attack using Hping3.

Theory :

Understanding Denial of Service (DoS) Attack

A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functioning and availability of a network, system, service, or resource. The primary goal of a DoS attack is to overwhelm the target with a flood of traffic or to exploit vulnerabilities in such a way that it becomes inaccessible to its legitimate users. Let's delve deeper into some common types of DoS attacks:

SYN Flood Attack

A SYN Flood Attack is a sophisticated form of DoS attack that exploits the way TCP (Transmission Control Protocol) connections are established. In a standard TCP handshake, when a client wants to establish a connection with a server, it sends a SYN (synchronize) packet to initiate the connection. The server responds with a SYN-ACK (synchronize acknowledge) packet, and the client completes the handshake with an ACK (acknowledge) packet.

In a SYN flood attack, the attacker sends an excessive number of SYN packets to the target server but does not follow up with ACK packets to complete the handshake. Instead, the attacker continually sends new SYN packets, causing the server to allocate resources for incomplete connections. Over time, these half-open connections can accumulate and exhaust the server's resources, making it unable to respond to legitimate connection requests. This effectively denies service to legitimate users.

ICMP Flood Attack (Ping Flood Attack)

An ICMP Flood Attack, commonly known as a Ping Flood Attack, targets the Internet Control Message Protocol (ICMP). ICMP is used for various network diagnostic purposes, including the famous "ping" utility, which checks the reachability of a network host. In a Ping Flood Attack,

the attacker sends an overwhelming number of ICMP echo-request packets (ping requests) to a

target device.

The target device, as per standard ICMP behavior, responds to each incoming echo-request with an echo-reply. In the case of a flood attack, the attacker's goal is to generate an excessive number of echo-requests, forcing the target to respond with an equal number of echo-replies. This massive traffic can quickly consume the target's network and computing resources, causing it to become unresponsive to legitimate network traffic.

SMURF Attack

A SMURF attack is a type of Denial of Service (DoS) attack that targets the Internet Control Message Protocol (ICMP) and leverages a technique called "amplification." In a SMURF attack, the attacker sends a large number of ICMP echo-request packets (commonly known as "pings") to an intermediate network, which then reflects these packets to a victim's IP address. This results in a flood of responses overwhelming the victim's network and causing a DoS condition.

Here's how a SMURF attack works:

1. The attacker sends a large number of ICMP echo-request packets (pings) to the broadcast address of an intermediate network.

2. The routers on the intermediate network, as per standard behavior, broadcast these ICMP requests to all hosts on the network.

3. Numerous hosts on the intermediate network respond to these ICMP requests by sending ICMP echo-reply packets to the source IP address specified in the requests. Since the source IP address in the requests is the victim's IP address, these responses flood the victim's network.

4. The victim's network becomes overwhelmed with ICMP traffic, leading to high resource utilization and unavailability of services, effectively causing a DoS condition.

Hping3 Commands for SYN Flood and ICMP Flood

SYN Flood using Hping3

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

- `-c 15000`: Specifies sending 15,000 packets.

- `-d 120`: Sets the data size to 120 bytes in each packet.

- `-S`: Sets the SYN flag in TCP packets.

- `-w 64`: Defines a window size of 64.

- `-p 80`: Targets port 80 (commonly used for HTTP).

- `--flood`: Floods the target with packets continuously.

- `--rand-source`: Utilizes random source IP addresses.

- `192.168.1.159`: Specifies the target IP address.

ICMP Flood using Hping3

```bash hping3 -1 --flood -a 192.168.103 192.168.1.255

```

- `-1`: Indicates the use of ICMP echo (ping) requests.

- `--flood`: Initiates the continuous flooding of the target.

- `-a 192.168.103`: Spoofs the source IP address as 192.168.103.

- `192.168.1.255`: Targets the broadcast address, causing multiple devices on the network to

respond.

Example Hping3 Command for a SMURF Attack

In a SMURF attack, Hping3 can be used to generate ICMP echo-request packets and send them to the broadcast address of an intermediate network, causing amplification and flooding. Below is an example command:

```bash hping3 -1 --flood -a <spoofed_source_ip> <broadcast_address>

```

- `-1`: Indicates the use of ICMP echo (ping) requests.

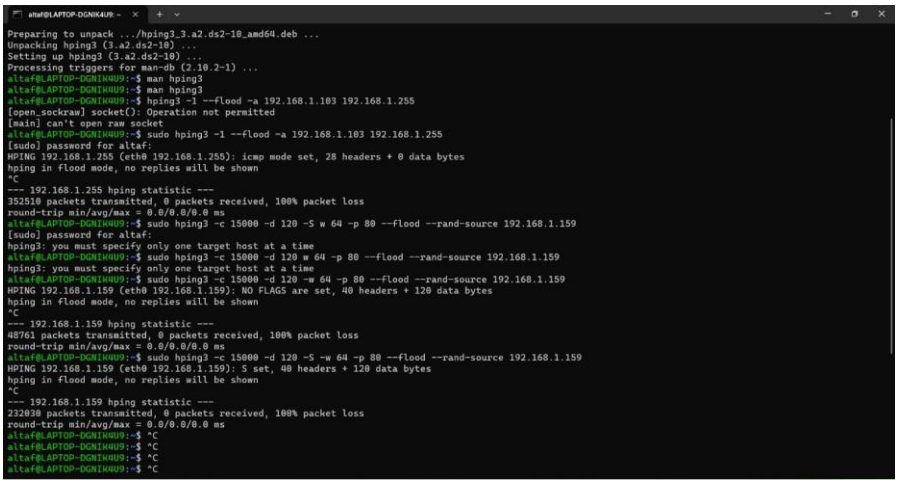
- `--flood`: Initiates the continuous flooding of the target.

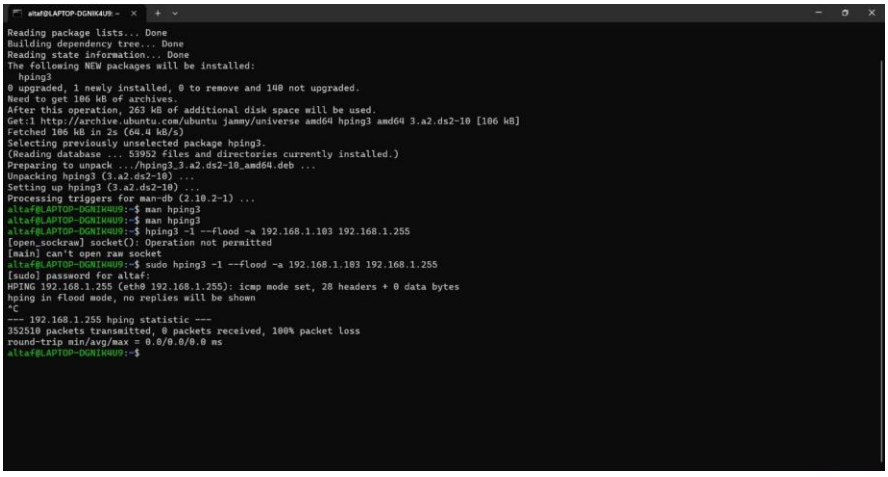
- `-a <spoofed_source_ip>`: Spoofs the source IP address as `<spoofed_source_ip>`. The

attacker often uses a spoofed IP address to hide their identity.

- `<broadcast_address>`: Specifies the broadcast address of the intermediate network. This is where the ICMP requests are sent.

Output:





Conclusion: Used open-source tools to scan the network for vulnerabilities and simulate attacks(LO4 is achieved).