

Roll No:138

Name: Anmol Tripathi

Batch: T23

### **Lab Assignment 9**

**AIM:** Simulate DOS attack using HPING3.

**LO5:** Use open source tools to scan the networks for vulnerabilities and simulate attacks.

#### **THEORY:**

A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a computer system, network, or online service by overwhelming it with a flood of illegitimate requests or traffic. The primary goal of a DoS attack is to make a resource, such as a website or server, unavailable to its intended users. It does so by consuming the target's resources, such as bandwidth, processing power, or memory, to the point where it cannot handle legitimate requests.

Here are explanations of three common types of DoS attacks:

#### **SYN Flood Attack:**

A SYN flood attack is a type of network-based DoS attack that targets the three-way handshake process in the Transmission Control Protocol (TCP), which is used for establishing connections between devices on the internet.

In a TCP connection, the client sends a SYN (synchronize) packet to initiate a connection with a server. The server is expected to respond with a SYN-ACK (synchronize-acknowledgment) packet, and then the client responds with an ACK (acknowledgment) packet to complete the handshake and establish the connection.

In a SYN flood attack, the attacker sends a high volume of SYN packets to the target server, but they do not complete the handshake by sending the expected ACK packets. This leaves the server waiting for the final ACKs, tying up its resources and preventing it from accepting legitimate connections.

SYN flood attacks can quickly overwhelm a server's ability to handle incoming connections, leading to service disruption.

#### **ICMP Flood Attack:**

An ICMP (Internet Control Message Protocol) flood attack, also known as a "ping flood" attack, targets the ICMP protocol, which is used for network diagnostics, particularly the "ping" command.

In this type of attack, the attacker sends a high volume of ICMP echo requests (ping requests) to the target system. Each request typically generates a response from the target, creating a flood of traffic.

ICMP flood attacks can consume the target's network bandwidth and processing resources, making it difficult for legitimate network traffic to pass through. This results in network congestion and service degradation or unavailability.

### **SMURF Attack:**

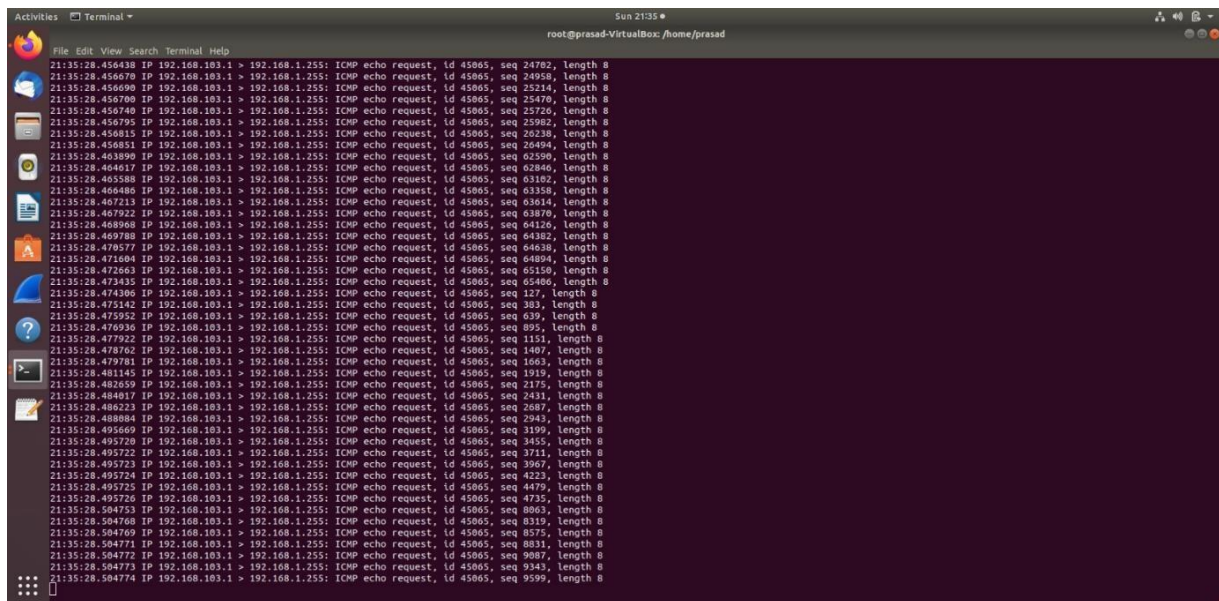
A SMURF attack is a network-based DoS attack that takes advantage of ICMP and IP addressing.

In a SMURF attack, the attacker sends a large number of ICMP echo request (ping) packets to an IP broadcast address, typically spoofing the source IP address to make it appear as if the requests are coming from the victim's IP address.

When these requests are sent to the broadcast address, all devices on the target network respond with ICMP echo replies. With a high enough volume of requests, this can flood the victim's network, overwhelming its resources and causing a DoS.

To mitigate DoS attacks, organizations use various security measures, including firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and content delivery networks (CDNs). These tools help identify and filter out malicious traffic, allowing legitimate traffic to reach its destination. Additionally, proper network design and configuration can help minimize the impact of DoS attacks.





```
21:35:28.456438 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 24702, length 8
21:35:28.456670 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 24950, length 8
21:35:28.456690 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 25214, length 8
21:35:28.456700 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 25470, length 8
21:35:28.456740 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 25726, length 8
21:35:28.456795 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 25982, length 8
21:35:28.456815 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 26238, length 8
21:35:28.456851 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 26494, length 8
21:35:28.463890 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 62590, length 8
21:35:28.464017 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 62846, length 8
21:35:28.465588 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 63102, length 8
21:35:28.466480 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 63358, length 8
21:35:28.467213 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 63614, length 8
21:35:28.467922 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 63870, length 8
21:35:28.468968 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 64126, length 8
21:35:28.469780 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 64382, length 8
21:35:28.470577 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 64638, length 8
21:35:28.471604 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 64894, length 8
21:35:28.472661 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 65150, length 8
21:35:28.473435 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 65406, length 8
21:35:28.474306 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 127, length 8
21:35:28.475142 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 303, length 8
21:35:28.475932 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 609, length 8
21:35:28.476936 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 895, length 8
21:35:28.477922 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 1151, length 8
21:35:28.478762 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 1407, length 8
21:35:28.479781 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 1663, length 8
21:35:28.481145 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 1919, length 8
21:35:28.482659 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 2175, length 8
21:35:28.484017 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 2431, length 8
21:35:28.486223 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 2687, length 8
21:35:28.488884 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 2943, length 8
21:35:28.495669 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 3199, length 8
21:35:28.495720 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 3455, length 8
21:35:28.495722 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 3711, length 8
21:35:28.495723 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 3967, length 8
21:35:28.495724 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 4223, length 8
21:35:28.495725 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 4479, length 8
21:35:28.495726 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 4735, length 8
21:35:28.504753 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 8063, length 8
21:35:28.504760 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 8319, length 8
21:35:28.504769 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 8575, length 8
21:35:28.504771 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 8831, length 8
21:35:28.504772 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 9087, length 8
21:35:28.504773 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 9343, length 8
21:35:28.504774 IP 192.168.103.1 > 192.168.1.255: ICMP echo request, id 45065, seq 9599, length 8
```

## CONCLUSION:

Hence, we gained knowledge about the network analysis and security assessment tools. Explore various network probing and testing techniques, which are valuable skills in the field of network administration and cybersecurity. We used various hping3 commands.