Roll No: 09
Name: Shreya Bagade
Date: 08/09/2023

LAB ASSIGNMENT NO:09

Aim: Simulate DOS attack using Hping3.

Lab Outcome Attained: Use open-source tools to scan the network for vulnerabilities and simulate attacks.

Theory:

1. What is Denial of Service Atack?

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 traffic, requests, or other malicious activities. The primary goal of a DoS attack is to make a resource (such as a website or network service) temporarily or indefinitely unavailable to its intended users. Here are key characteristics and components of a DoS attack:

Volume of Traffic: A DoS attack typically involves an excessive volume of traffic or requests directed at the target system or service. This flood of traffic consumes the available resources, such as bandwidth, processing power, or memory, leading to a slowdown or complete unavailability of the target.

Intentional Malicious Action: DoS attacks are intentionally launched by malicious actors who aim to disrupt services, cause inconvenience, or damage the reputation of the targeted organization or individual.

Variants: There are various types of DoS attacks, including:

Flooding Attacks: Involving overwhelming the target with excessive traffic or requests. Examples include SYN floods and UDP floods.

Resource Depletion: Targeting specific resources, like CPU, memory, or network bandwidth, until they are exhausted.

Application Layer Attacks: Targeting vulnerabilities in application software, such as HTTP floods or Slowloris attacks.

Roll No: 09
Name: Shreya Bagade
Date: 08/09/2023

2. Explain SYN flood, ICMP flood and SMURF attack.

SYN Flood Attack:

A SYN Flood attack targets the TCP (Transmission Control Protocol) handshake process, which is used to establish a connection between a client and a server. During this handshake, the client sends a SYN (synchronize) packet to the server, and the server responds with a SYN-ACK (synchronize-acknowledgment) packet, followed by an ACK (acknowledgment) from the client to complete the connection.

Attack Process: In a SYN Flood attack, an attacker sends a large number of SYN packets to a target server without intending to complete the handshake. This consumes the server's resources as it waits for the expected ACK packets to complete the connections, eventually causing the server to become overwhelmed and unable to handle legitimate requests.

Impact: The target server becomes slow or unresponsive, denying service to legitimate users.

ICMP Flood Attack:

An ICMP (Internet Control Message Protocol) Flood attack targets network devices and routers by sending an excessive number of ICMP echo requests (ping) packets.

Attack Process: The attacker sends a flood of ICMP echo requests to the target device, often with spoofed source IP addresses to make it challenging to identify the attacker. The target device consumes resources processing and responding to these requests, leading to network congestion and potential device failure.

Impact: Network devices become overwhelmed, leading to network congestion, packet loss, and service disruption for legitimate users.

SMURF Attack:

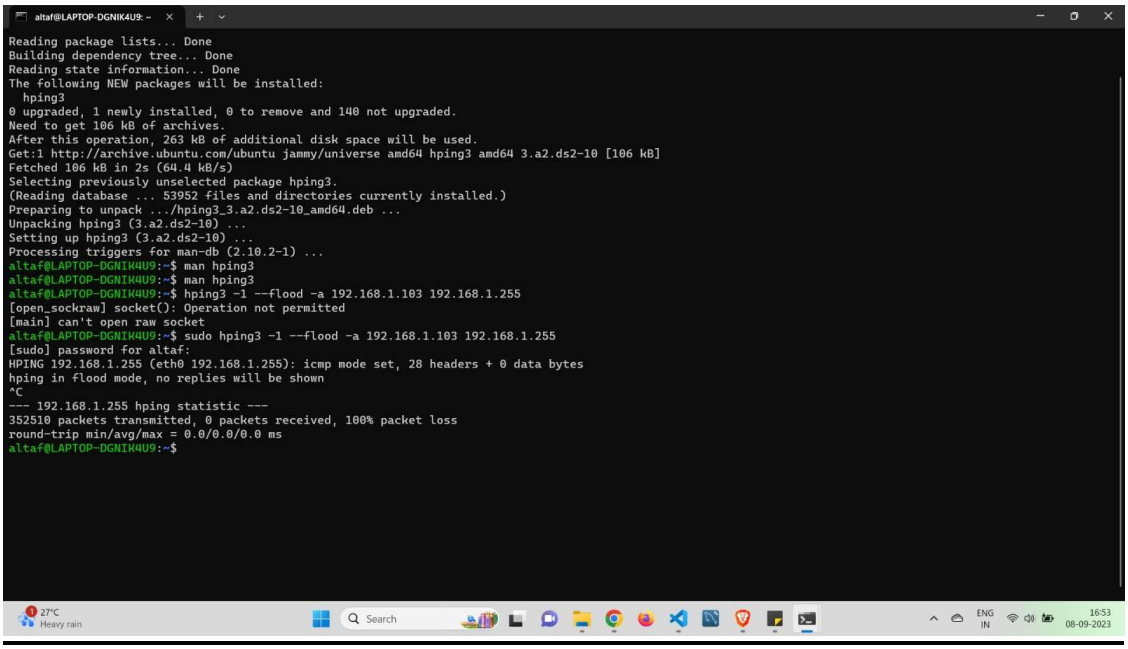
A SMURF attack is an amplification DDoS attack that exploits ICMP and broadcast networks.

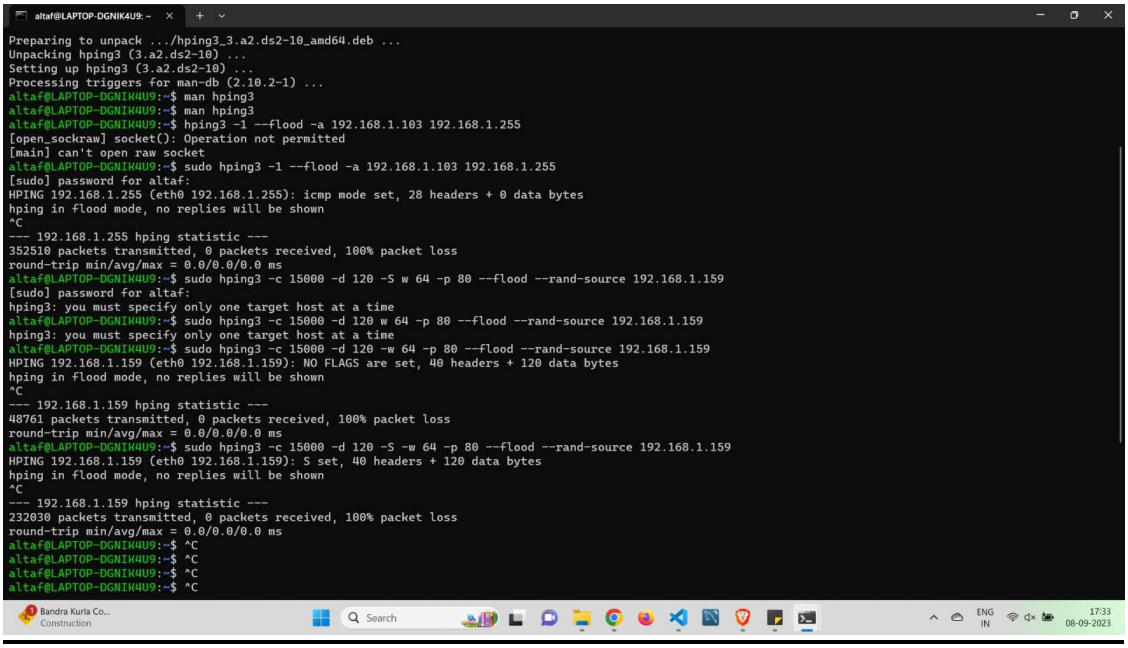
Attack Process: In a SMURF attack, the attacker sends ICMP echo requests (ping) to a network's broadcast address, which results in all devices on the network responding to the spoofed source IP address (the victim's IP). This

amplifies the traffic sent to the victim's IP address, overwhelming their network connection.

Impact: The victim's network experiences a flood of traffic from multiple sources, causing congestion and potentially rendering the network or services unavailable.

Output Screenshots:





Roll No: 09
Name: Shreya Bagade
Date: 08/09/2023

Conclusion: This experiment with the GnuPG tool for PGP (Pretty Good Privacy) has demonstrated its effectiveness in securing digital communication through encryption and digital signatures. We successfully generated key pairs, encrypted and decrypted messages, and verified digital signatures. This powerful tool provides a robust framework for ensuring the confidentiality, integrity, and authenticity of sensitive data in the realm of secure communication.