Terna Engineering College

Computer Engineering Department

Class: TE **Sem.: VI**

Course: System Security Lab

PART A

(PART A : TO BE REFFERED BY STUDENTS)

Experiment No.9

A.1 Aim: Simulate DOS attack using Hping, hping3 and Wireshark

A.2 Prerequisite:

1. Basic Knowledge of DOS attacks,

A.3 Outcome:

After successful completion of this experiment students will be able to

To be able to use open source technologies and explore email security and explore various attacks.

A.4 Theory:

Denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services. A distributed denial-of-service (DDoS) is where the attack source is more than one, often thousands of, unique IP addresses. It is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

A DoS attack tries to make a web resource unavailable to its users by flooding the target URL with more requests than the server can handle. That means that during the attack period, regular trafficon the website will be either slowed down or completelyinterrupted.

ADistributedDenialofService(DDoS)attackisaDoSattackthatcomesfrommorethano nesource at the same time. A DDoS attack is typically generated using thousands (potentially hundreds of thousands) of unsuspecting zombie machines. The machines used in such attacks are collectively known as “botnets” and will have previously been infected with malicious software, so they can be remotely controlled by the attacker. According to research, tens of millions of computers are likely to be infected with botnet programsworldwide.

Cybercriminals use DoS attacks to extort money from companies that rely on their websites being accessible. But there have also been examples of legitimate businesses having paid underground elementsoftheInternettohelpthemcripplerivalwebsites.Inaddition,cybercriminalsco mbineDoS attacks and phishing to target online bank customers. They use a DoS attack to take down the bank's website and then send out phishing e-mails to direct customers to a fake emergency siteinstead.

Installation Steps:

1. Install Hping3 andwireshark
2. Flood the victim with TCP/ICMP/UDP packet using Hping3 (-- floodoption)
3. Observe the Dos attack and DDos attack usingWireshark

PART B

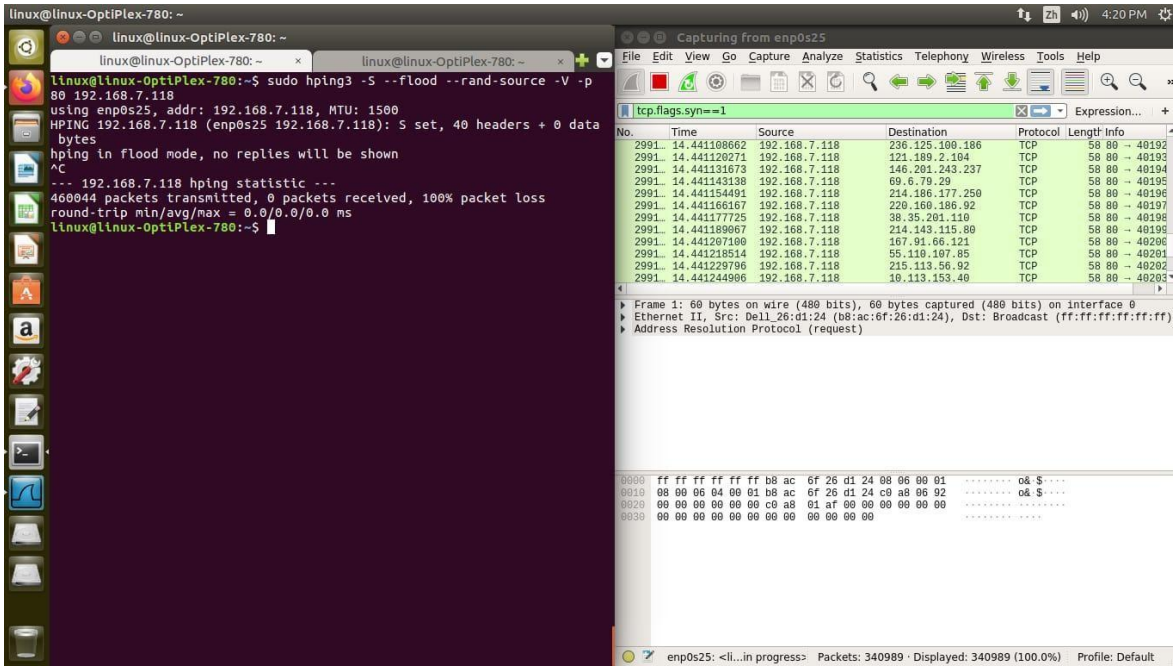
(PART B : TO BE COMPLETED BY STUDENTS)

(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)

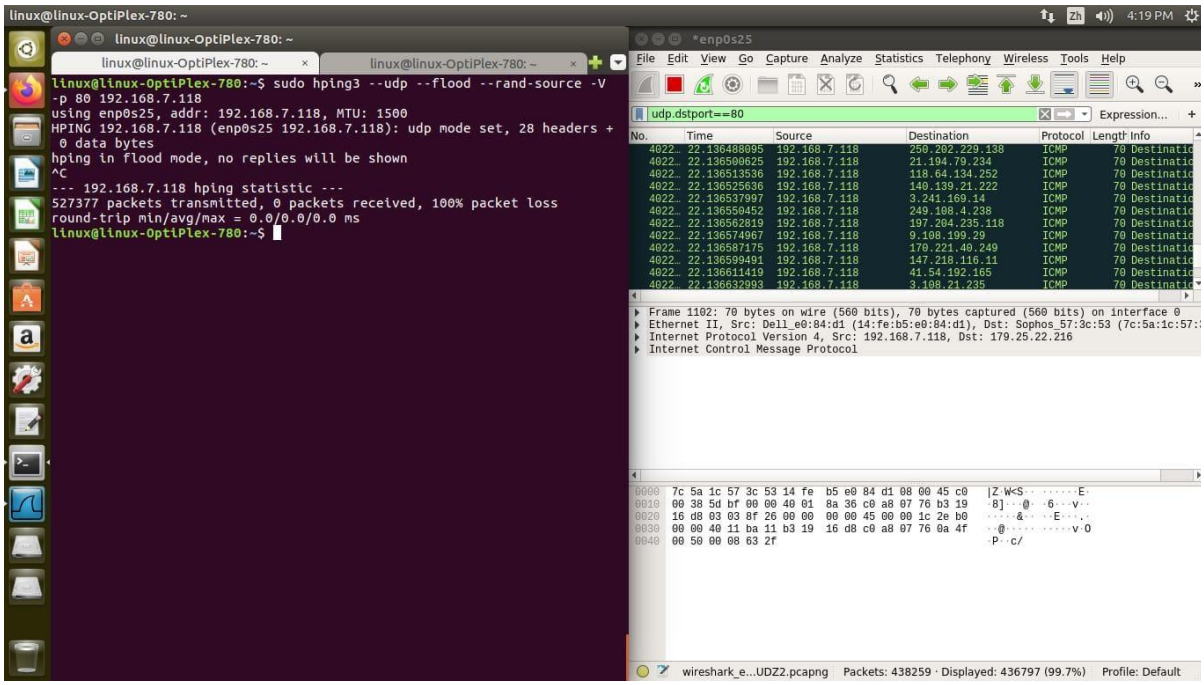
Roll No: B30	**Name: Bhatt Pranjal**
Class : TE COMPS B	**Batch : B2**
Date of Experiment:	**Date of Submission**
Grade :	

B.1 Output:

Command for TCP SYN Flood:



Command for UDP Flood:



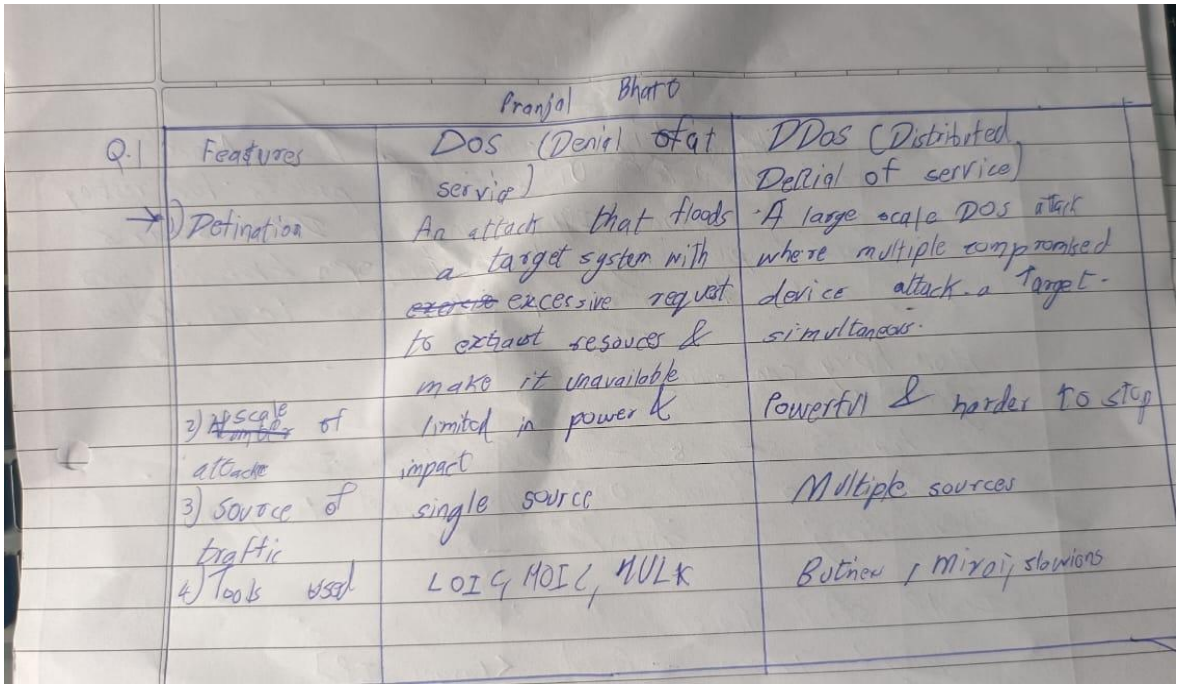
B.2 Commands / tools used with syntax:

•

Command for TCP SYN Flood: hping3 --flood --rand-source -S -p 80 <target_ip>
Command for UDP Flood: hping3 --flood --rand-source --udp -p 80 <target_ip>

B.3 Question of Curiosity: *(Attempt at least 3 questions handwritten)*

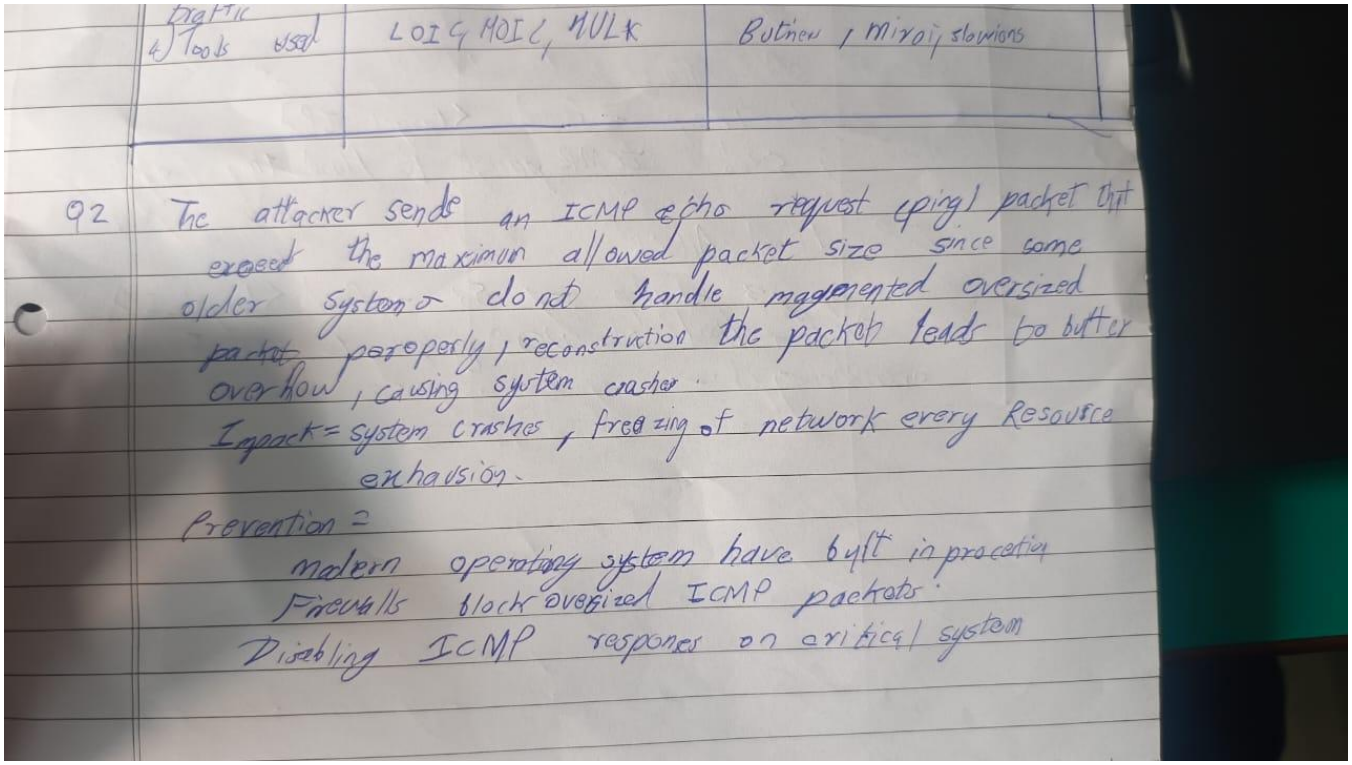
1. What is the difference between Dos and DDos?



Pranjal Bhatt

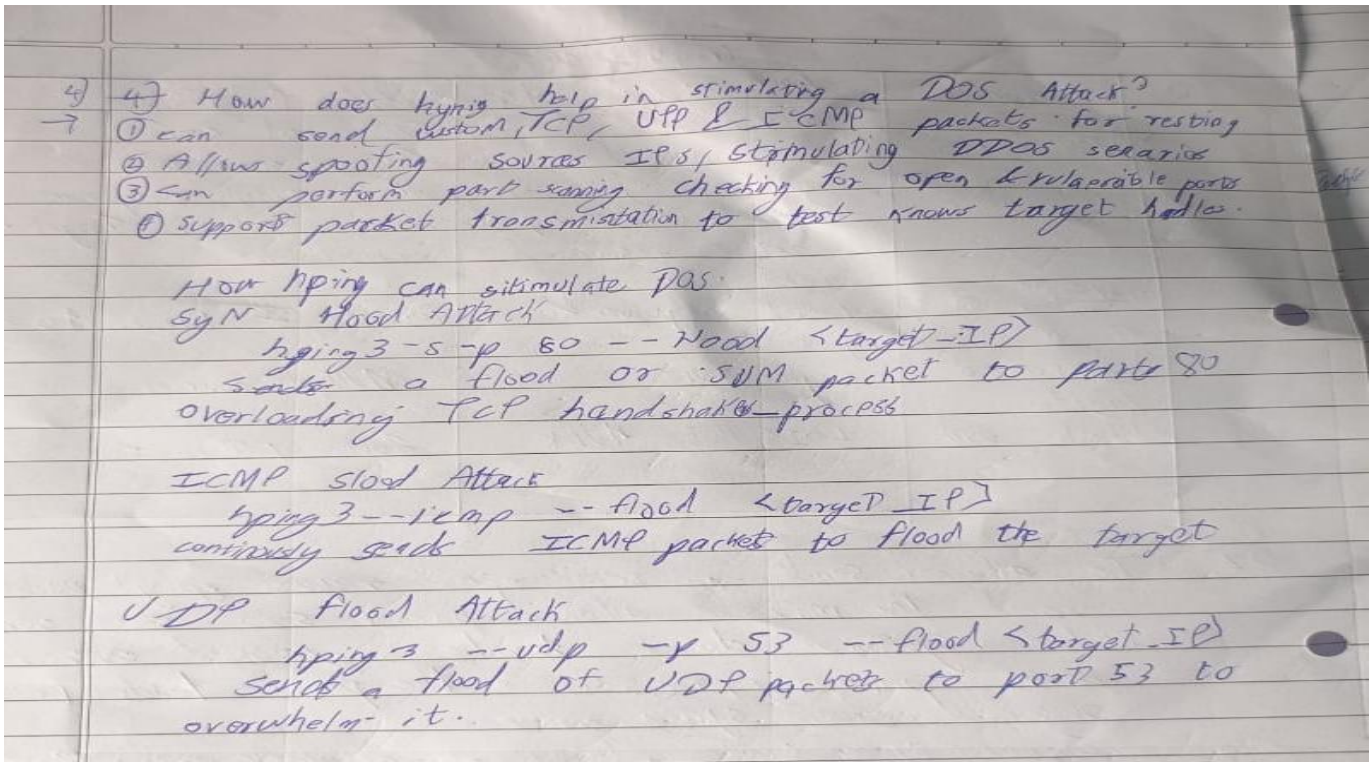
Q.1	Features	DOS (Denial of service)	DDOS (Distributed Denial of service)
→	1) Defination	An attack that floods a target system with excessive request to exhaust resources & make it unavailable	A large scale DOS attack where multiple compromised device attack a target simultaneously.
	2) Attack scale	limited in power & impact	Powerful & harder to stop
	3) Source of traffic	single source	Multiple sources
	4) Tools used	LOIC, HOIC, HULK	Butnet / Mirai, slowloris

2. What is ping of death attack?



3. What is land attack?
    1) How it Works:
        a) The attacker sends a TCP SYN packet where the source IP and destination IP are the same (the victim's own IP).
        b) The system replies to itself, leading to a loop, consuming CPU and memory resources.
    2) Impact:
        a) Causes network congestion.
        b) Drains system resources, making it unresponsive.
    3) Prevention:
        a) Firewalls should drop packets where source IP == destination IP.
        b) Modern operating systems are patched against such attacks.

4. How does Hping help in simulating a DoS attack?



4) 4) How does hping help in stimulating a DOS Attack?
→ ① can send custom TCP, UDP & ICMP packets for testing
② Allows spoofing sources IPs, stimulating DDOS scenarios
③ Can perform port scanning checking for open & vulnerable ports
④ Supports packet transmission to test knows target hosts.

How hping can stimulate DOS.
SyN Flood Attack
hping3 -S -p 80 --flood <target_IP>
Sends a flood of SYN packet to port 80
overloading TCP handshake process

ICMP Flood Attack
hping3 --icmp --flood <target_IP>
continuously sends ICMP packets to flood the target

UDP Flood Attack
hping3 --udp -p 53 --flood <target_IP>
Sends a flood of UDP packets to port 53 to
overwhelm it.

5. What is the role of Wireshark in analyzing DoS attacks?
    1) How Wireshark Helps in Detection:
        a) Captures and analyzes network traffic in real time.
        b) Detects large volumes of SYN requests (SYN flood).
        c) Identifies high rates of ICMP requests (ping flood).
        d) Finds repeated requests from a single IP, indicating an attack source.
        e) Shows anomalous packet sizes that may suggest malformed packet attacks.
    2) Example Wireshark Filters for DoS Analysis:
        a. Show only SYN flood traffic:tcp.flags.syn == 1 && tcp.flags.ack == 0
        b. Show only ICMP flood traffic:icmp
        c. Show packets larger than 1000 bytes:frame.len > 1000

6. How can DoS attacks be mitigated using firewall rules and rate limiting?
    1) Firewall Rules to Prevent DoS
        a) Block ICMP (Ping of Death) Attacks:iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
        b) Limit SYN Floods (TCP SYN Attack):iptables -A INPUT -p tcp --syn -m limit --limit 10/s --limit-burst 20 -j ACCEPT
        c) Drop Packets from Known Malicious IPs:iptables -A INPUT -s <malicious_IP> -j DROP
    2) Rate Limiting to Prevent DoS

    Limit HTTP Requests Per IP:

        a) In NGINX:

```
limit_req_zone $binary_remote_addr zone=one:10m rate=5r/s;
server {
location / {
        limit_req zone=one burst=10;


}
```

        b) In Apache (mod_evasive):

```
sudo apt install libapache2-mod-evasive
```

Add to apache2.conf:

DOSHashTableSize 2048

DOSPageCount 10

DOSSiteCount 50

DOSBlockingPeriod 60

B.4 Conclusion:

A DoS attack can be simulated using hping3 by flooding a target with UDP, TCP SYN, or ICMP packets, overwhelming system resources. Commands like hping3 --flood --rand-source -S -p 80 <target_ip> generate massive traffic, while Wireshark helps analyze attack patterns by filtering packets such as tcp.flags.syn == 1 && tcp.flags.ack == 0. The captured data in Wireshark shows excessive incoming packets, indicating a potential attack. DoS attacks exploit system vulnerabilities, and mitigation requires firewall rules, rate limiting, and intrusion detection systems (IDS) to filter malicious traffic.