

# **Terna Engineering College**

## **Computer Engineering Department**

**Class: TE**

**Sem.: VI**

**Course: System Security Lab**

### **PART A**

**(PART A : TO BE REFERRED 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 traffic on the website will be either slowed down or completely interrupted.

A Distributed Denial of Service (DDoS) attack is a DoS attack that comes from more than one source 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 programs worldwide.

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 elements of the Internet to help them cripple rival websites. In addition, cybercriminals combine DoS 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 site instead.

**Installation Steps:**

1. Install Hping3 and Wireshark
2. Flood the victim with TCP/ICMP/UDP packet using Hping3 (-- flood option)
3. Observe the DoS attack and DDoS attack using Wireshark

## 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)*

<b>Roll No: B30</b>	<b>Name: Bhatt Pranjal</b>
<b>Class : TE COMPS B</b>	<b>Batch : B2</b>
<b>Date of Experiment:</b>	<b>Date of Submission</b>
<b>Grade :</b>	

### B.1 Output:

## Command for TCP SYN Flood:

The screenshot shows a Kali Linux terminal window with the following content:

```

linux@linux-OptiPlex-780: ~
linux@linux-OptiPlex-780: ~
linux@linux-OptiPlex-780: ~
linux@linux-OptiPlex-780: ~$ sudo hping3 -S --flood --rand-source -V -p
80 192.168.7.118
using enp0s25, addr: 192.168.7.118, MTU: 1500
HPING 192.168.7.118 (enp0s25 192.168.7.118): S set, 40 headers + 0 data
bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.7.118 hping statistic ---
460044 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
linux@linux-OptiPlex-780: ~$

```

On the right side of the terminal, a packet capture window is open, showing the captured traffic. The capture is titled "Capturing from enp0s25". The filter is "tcp.flags.syn==1". The capture shows a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are all SYN packets from 192.168.7.118 to 192.168.7.118.

No.	Time	Source	Destination	Protocol	Length	Info
2991	14.441108662	192.168.7.118	236.125.100.186	TCP	58	80 → 40192
2991	14.441120271	192.168.7.118	121.189.2.104	TCP	58	80 → 40193
2991	14.441131679	192.168.7.118	146.201.243.237	TCP	58	80 → 40194
2991	14.441143138	192.168.7.118	69.6.79.29	TCP	58	80 → 40195
2991	14.441154491	192.168.7.118	214.186.177.250	TCP	58	80 → 40196
2991	14.441166167	192.168.7.118	220.168.186.92	TCP	58	80 → 40197
2991	14.441177725	192.168.7.118	38.35.201.110	TCP	58	80 → 40198
2991	14.441189667	192.168.7.118	214.143.115.80	TCP	58	80 → 40199
2991	14.441207100	192.168.7.118	167.91.66.121	TCP	58	80 → 40200
2991	14.441218514	192.168.7.118	55.110.107.85	TCP	58	80 → 40201
2991	14.441229706	192.168.7.118	215.113.56.92	TCP	58	80 → 40202
2991	14.441244986	192.168.7.118	10.113.153.40	TCP	58	80 → 40203

Below the packet list, there is a summary of the captured frame:

```

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Dell_26:d1:24 (b8:ac:6f:26:d1:24), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

```

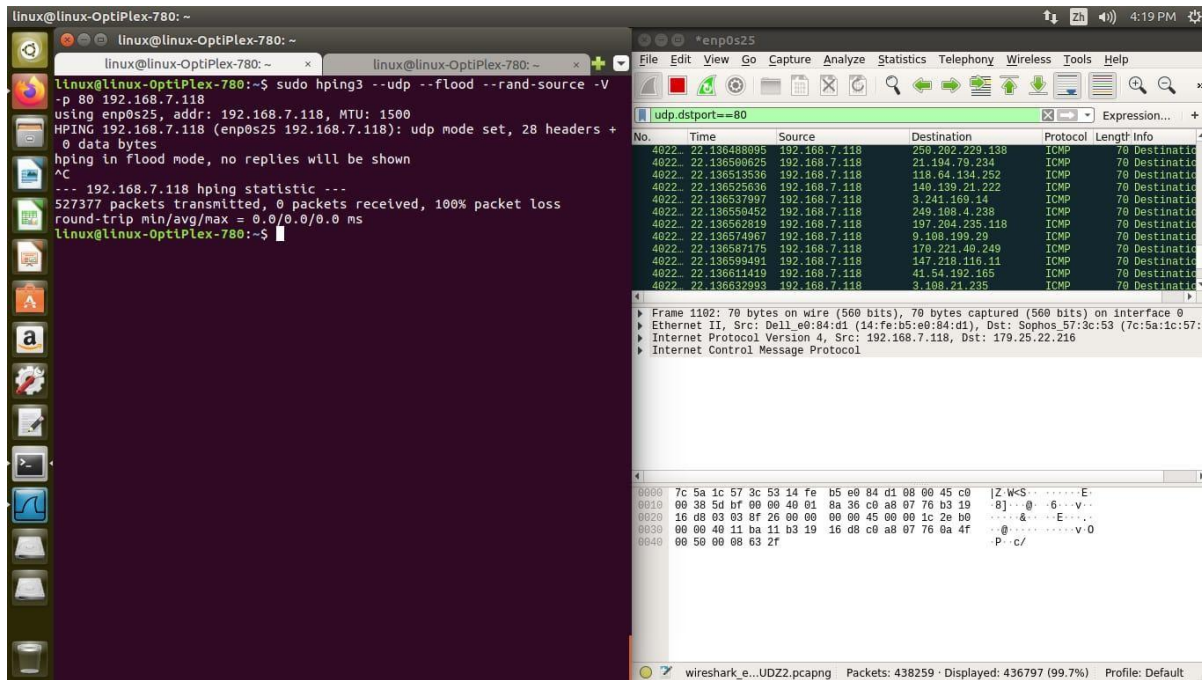
At the bottom, there is a hex dump of the captured data:

```

0000  ff ff ff ff ff ff ff ff 6f 26 d1 24 08 06 00 01  .....o6$...
0010  00 00 00 04 00 00 01 b8 ac 6f 26 d1 24 c0 a8 06 92  .....o6$...
0020  00 00 00 00 00 00 00 c0 a8 61 af 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

### 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>`

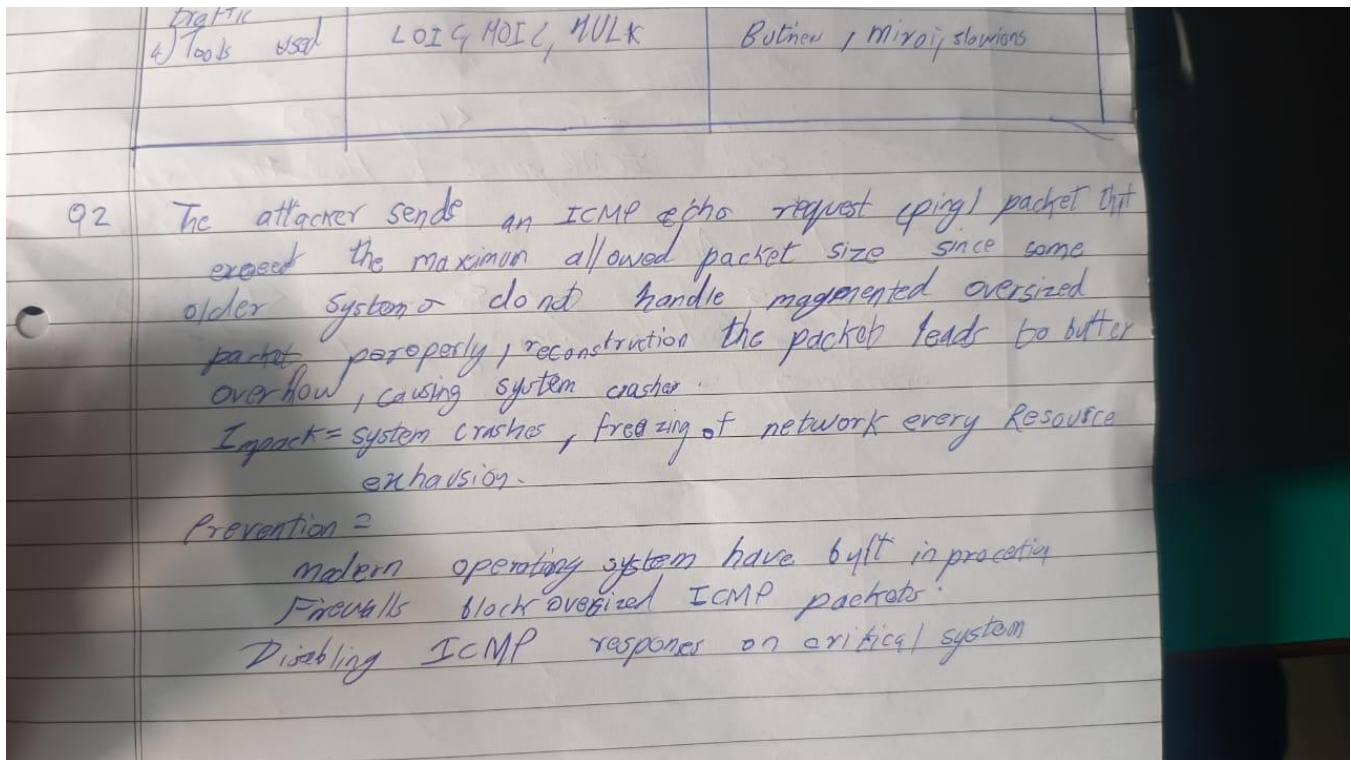
### B.3 Question of Curiosity: (Attempt at least 3 questions handwritten)

1. What is the difference between Dos and DDos?

Pranjal Bhatia

Q.1	Features	Dos (Denial of service)	DDos (Distributed Denial of service)
→ 1)	Definition	An attack that floods a target system with <del>excessive</del> excessive request to exhaust resources & make it unavailable	A large scale Dos attack where multiple compromised device attack a target simultaneously.
2)	Scale of impact	Limited in power & impact	Powerful & harder to stop
3)	Source of traffic	single source	Multiple sources
4)	Tools used	LOIC, HOIC, NULK	Botnet, mirror, slowloris

## 2. What is ping of death attack?



## 3. What is land attack?

### 1) How it Works:

- The attacker sends a TCP SYN packet where the source IP and destination IP are the same (the victim's own IP).
- The system replies to itself, leading to a loop, consuming CPU and memory resources.

### 2) Impact:

- Causes network congestion.
- Drains system resources, making it unresponsive.

### 3) Prevention:

- Firewalls should drop packets where source IP == destination IP.
- Modern operating systems are patched against such attacks.



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

- 4) How does hping help in simulating a DoS Attack?
- ① can send custom TCP, UDP & ICMP packets for testing
  - ② Allows spoofing source IPs, stimulating DDoS scenarios
  - ③ can perform port scanning checking for open & vulnerable ports
  - ④ supports packet transmission to test known target hosts.

How hping can simulate 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.