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.09

A.1 Aim:

Simulate DOS attack using Hping, hping3 and Wireshark

A.2 Prerequisite:

Basic Knowledge of DOS attacks,

A.3 Outcome:

After the successful completion of this experiment, students will 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. Besides, 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 emails 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

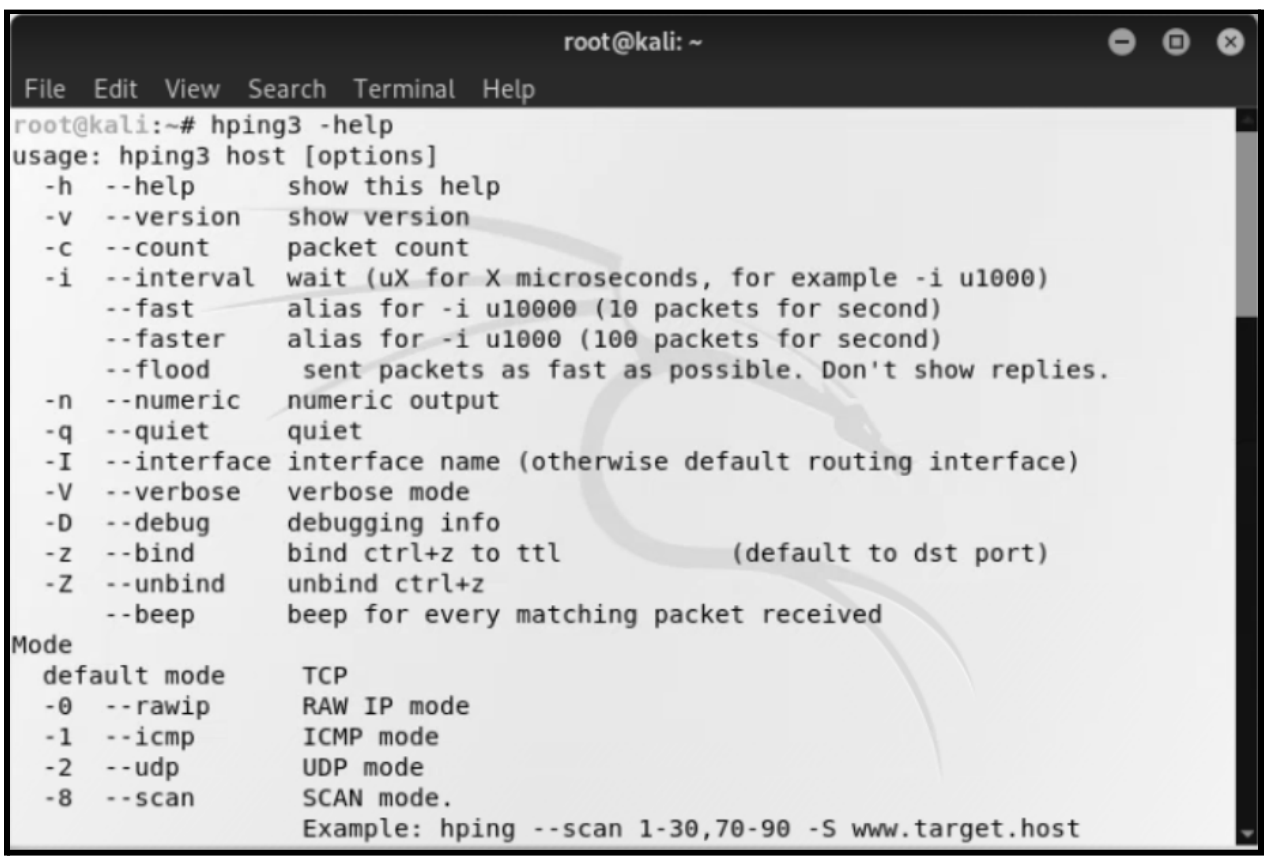
(PART B: TO BE COMPLETED BY STUDENTS)

(Students must submit the soft copy as per the 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 there is no Blackboard access available)

Roll No. 50	**Name:** AMEY THAKUR
Class: Comps TE B	**Batch:** B3
Date of Experiment: 20/04/2021	**Date of Submission:** 20/04/2021
Grade:	

B.1 Output

(add a snapshot of output)



```
root@kali: ~
File  Edit  View  Search  Terminal  Help
  -9  --listen      listen mode
IP
  -a  --spoof       spoof source address
  --rand-dest       random destionation address mode. see the man.
  --rand-source     random source address mode. see the man.
  -t  --ttl         ttl (default 64)
  -N  --id          id (default random)
  -W  --winid       use win* id byte ordering
  -r  --rel         relativize id field          (to estimate host traffic)
  -f  --frag        split packets in more frag.  (may pass weak acl)
  -x  --morefrag    set more fragments flag
  -y  --dontfrag    set don't fragment flag
  -g  --fragoff     set the fragment offset
  -m  --mtu         set virtual mtu, implies --frag if packet size > mtu
  -o  --tos         type of service (default 0x00), try --tos help
  -G  --rroute      includes RECORD_ROUTE option and display the route buffer
  --lsrr            loose source routing and record route
  --ssrr            strict source routing and record route
  -H  --ipproto     set the IP protocol field, only in RAW IP mode
ICMP
  -C  --icmptype    icmp type (default echo request)
  -K  --icmpcode    icmp code (default 0)
      --force-icmp  send all icmp types (default send only supported types)
      --icmp-gw     set gateway address for ICMP redirect (default 0.0.0.0)
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
      --icmp-help   display help for others icmp options
UDP/TCP
  -s  --baseport    base source port             (default random)
  -p  --destport    [+][+]<port> destination port(default 0) ctrl+z inc/dec
  -k  --keep        keep still source port
  -w  --win         winsize (default 64)
  -O  --tcpoff      set fake tcp data offset     (instead of tcphdrlen / 4)
  -Q  --seqnum      shows only tcp sequence number
  -b  --badcksum    (try to) send packets with a bad IP checksum
                    many systems will fix the IP checksum sending the packet
                    so you'll get bad UDP/TCP checksum instead.
  -M  --setseq      set TCP sequence number
  -L  --setack      set TCP ack
  -F  --fin         set FIN flag
  -S  --syn         set SYN flag
  -R  --rst         set RST flag
  -P  --push        set PUSH flag
  -A  --ack         set ACK flag
  -U  --urg         set URG flag
  -X  --xmas        set X unused flag (0x40)
  -Y  --ymas        set Y unused flag (0x80)
  --tcpexitcode     use last tcp->th_flags as exit code
  --tcp-mss         enable the TCP MSS option with the given value
  --tcp-timestamp   enable the TCP timestamp option to guess the HZ/uptime
```

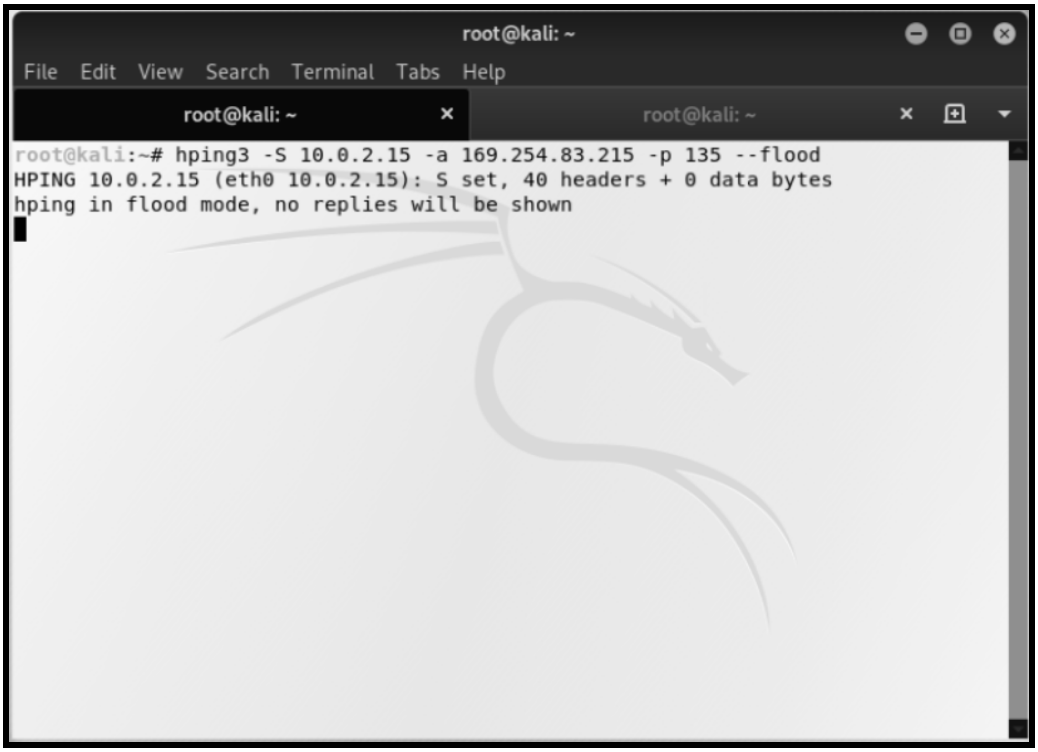
```
root@kali: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@kali: ~                    root@kali: ~

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fec0::5054:ff:fe12:3456  prefixlen 64  scopeid 0x40<site>
        inet6 fe80::5054:ff:fe12:3456  prefixlen 64  scopeid 0x20<link>
        inet6 fec0::588f:1da:f912:6f02  prefixlen 64  scopeid 0x40<site>
        ether 52:54:00:12:34:56  txqueuelen 1000  (Ethernet)
        RX packets 12618  bytes 18122145 (17.2 MiB)
        RX errors 56  dropped 0  overruns 0  frame 56
        TX packets 2462  bytes 158288 (154.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

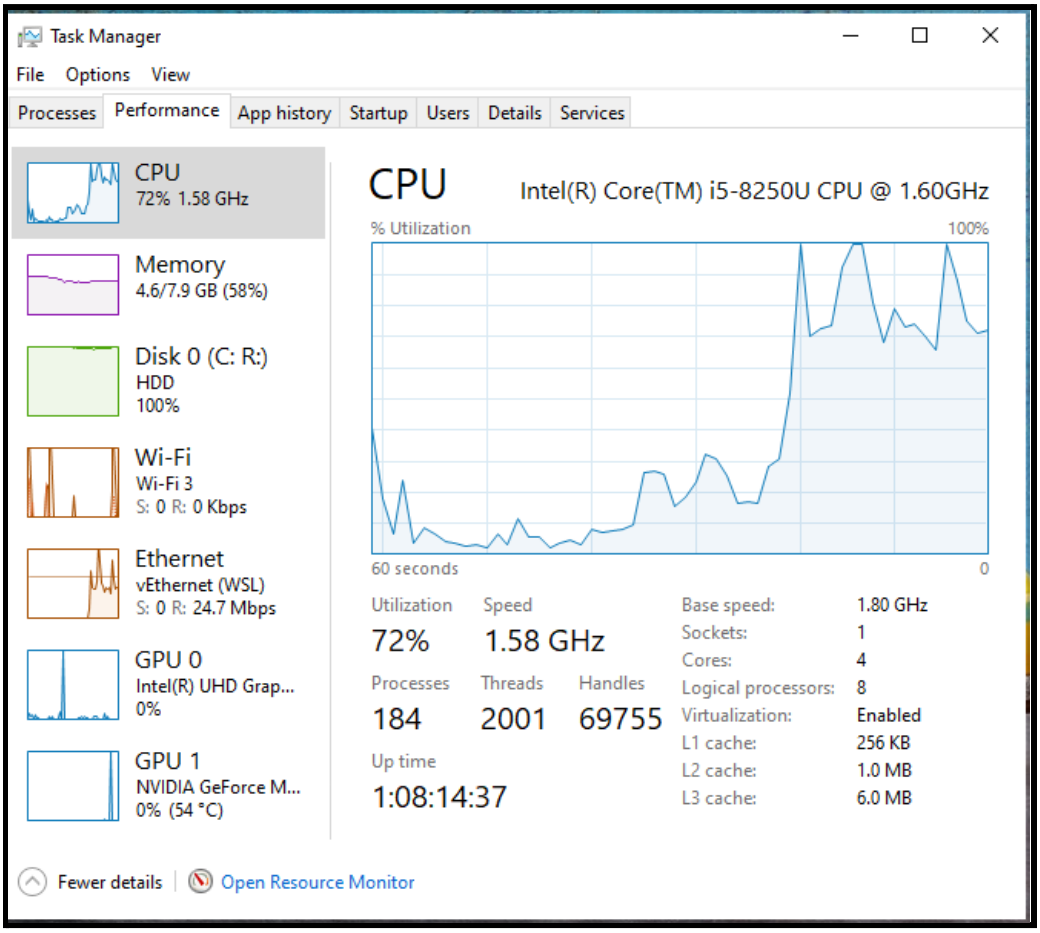
Command Prompt

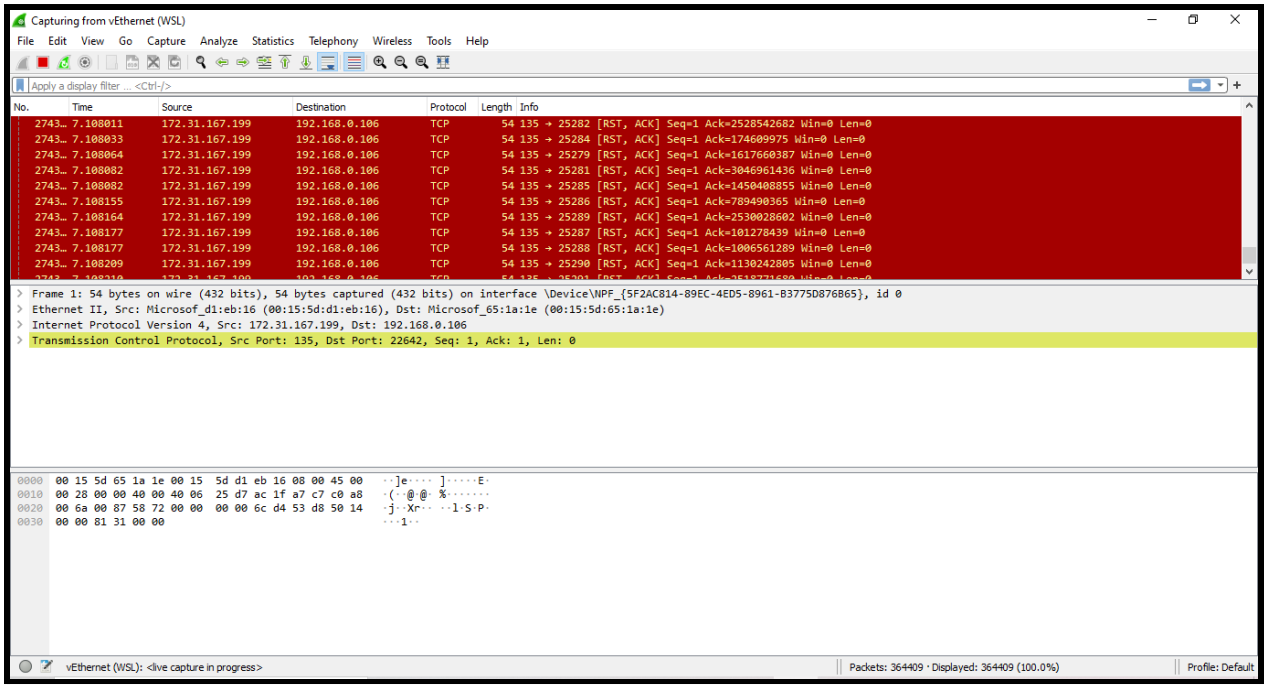
```
Microsoft Windows [Version 10.0.19042.928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ameyt>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b919:689b:5961:53d7%12
   Autoconfiguration IPv4 Address. . : 169.254.83.215
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1880:afaa:2cc9:fc12%18
   IPv4 Address. . . . . . . . . . . : 192.168.0.107
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Users\ameyt>
```

Select Command Prompt

```
Microsoft Windows [Version 10.0.19042.928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ameyt>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b919:689b:5961:53d7%12
   Autoconfiguration IPv4 Address. . : 169.254.83.215
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1880:afaa:2cc9:fc12%18
   IPv4 Address. . . . . . . . . . . : 192.168.0.107
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Users\ameyt>
```


root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: ~
root@kali:~# hping3 -S 10.0.2.15 -a 169.254.83.215 -p 135 --flood
HPING 10.0.2.15 (eth0 10.0.2.15): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
CPU
72% 1.58 GHz
Memory
4.6/7.9 GB (58%)
Disk 0 (C: R:)
HDD
100%
Wi-Fi
Wi-Fi 3
S: 0 R: 0 Kbps
Ethernet
vEthernet (WSL)
S: 0 R: 24.7 Mbps
GPU 0
Intel(R) UHD Grap...
0%
GPU 1
NVIDIA GeForce M...
0% (54 °C)
CPU
Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz
% Utilization
100%
60 seconds
0
Utilization
72%
Speed
1.58 GHz
Processes
184
Threads
2001
Handles
69755
Up time
1:08:14:37
Base speed: 1.80 GHz
Sockets: 1
Cores: 4
Logical processors: 8
Virtualization: Enabled
L1 cache: 256 KB
L2 cache: 1.0 MB
L3 cache: 6.0 MB
Fewer details
Open Resource Monitor



B.2 Commands/tools used with the syntax:

Commands:

- ➔ ifconfig
- ➔ ipconfig
- ➔ apt install hping3
- ➔ hping3 -S <attacking IP address> -a <target IP address. -p 135 --flood

Tools Used:

- ➔ Kali Linux and Terminal

B.3 Question of Curiosity:

1. What is the difference between Dos and DDos?

Ans:

DOS	DDOS
DOS Stands for Denial of service attack.	DDOS Stands for Distributed Denial of service attack.
In Dos attacks, a single system targets the victim's system.	In DDoS multiple systems attack the victim's system.
Victim PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from multiple locations.
Dos attack is slower as compared to DDoS.	The DDoS attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
In DOS Attack only a single device is used with DOS Attack tools.	In a DDoS attack, Bots are used to attack at the same time.
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace.
The volume of traffic in Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.
Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack	Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks

2. What is the ping of death attack?

Ans:

- ➔ Ping of Death (a.k.a. PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.
- ➔ While PoD attacks exploit legacy weaknesses that may have been patched in target systems. However, in an unpatched system, the attack is still relevant and dangerous. Recently, a new type of PoD attack has become popular. In this attack, commonly known as a Ping flood, the targeted system is hit with ICMP packets sent rapidly via ping without waiting for replies.

3. What is a land attack?

Ans:

- ➔ A LAND Attack is a Layer 4 Denial of Service (DoS) attack in which, the attacker sets the source and destination information of a TCP segment to be the same. A vulnerable machine will crash or freeze due to the packet being repeatedly processed by the TCP stack.

B.4 Conclusion:

(Write an appropriate conclusion.)

We have studied to perform a DOS attack on a system using Hping3 and track it using Wireshark.