**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**

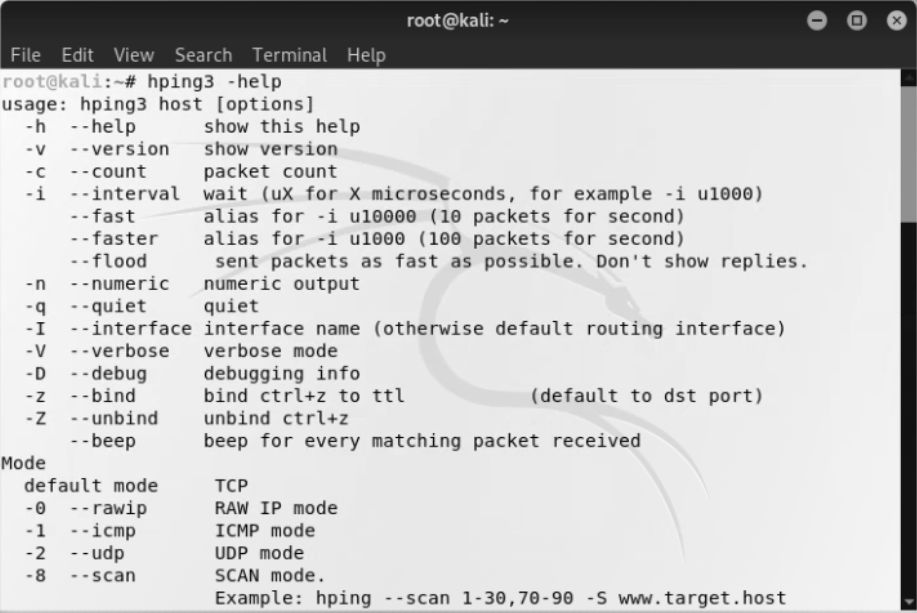
(PART B: TO BE COMPLETED BY STUDENTS)

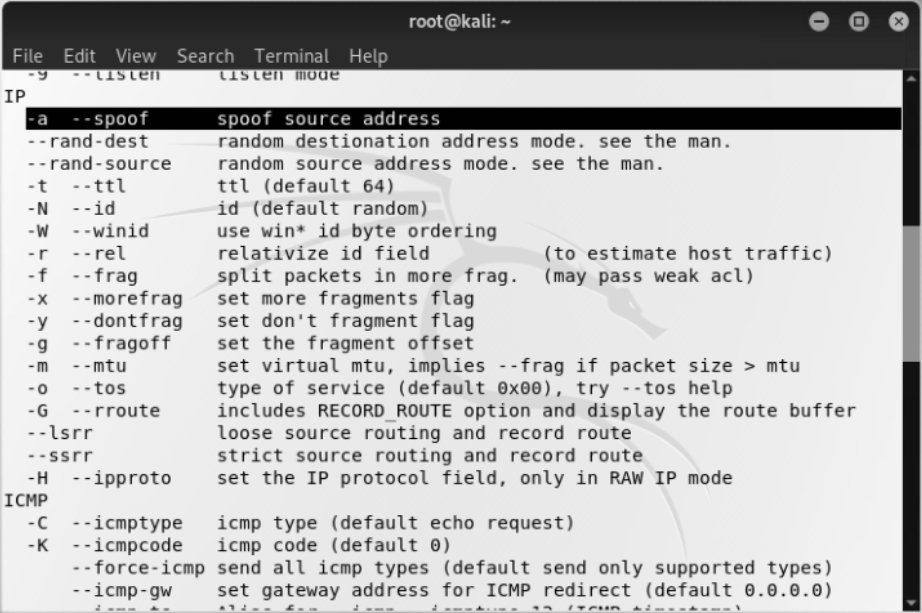
***(Students must submit the soft copy as per the following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case there is no Blackboard access available)***

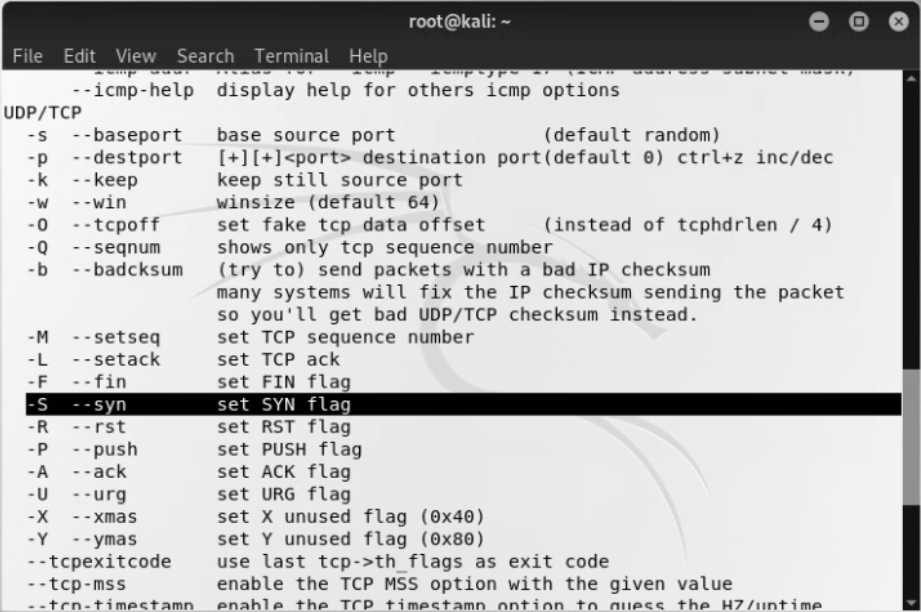
|  |  |
| --- | --- |
| **Roll No.** 50 | **Name:** AMEY THAKUR |
| **Class:** Comps TE B | **Batch:** B3 |
| **Date of Experiment:** 20/04/2021 | **Date of Submission:** 20/04/2021 |
| **Grade:** |  |

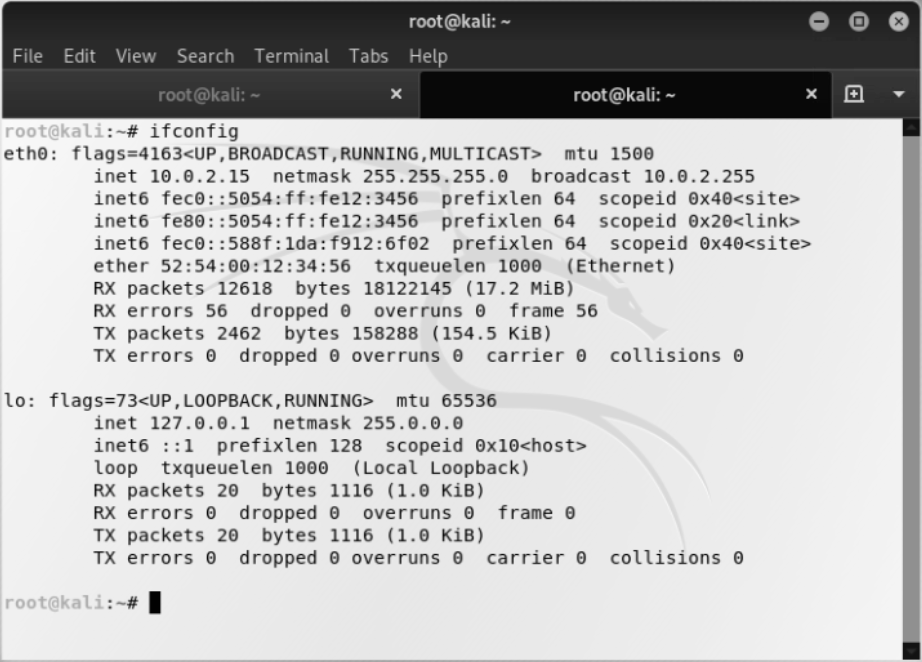
**B.1 Output**

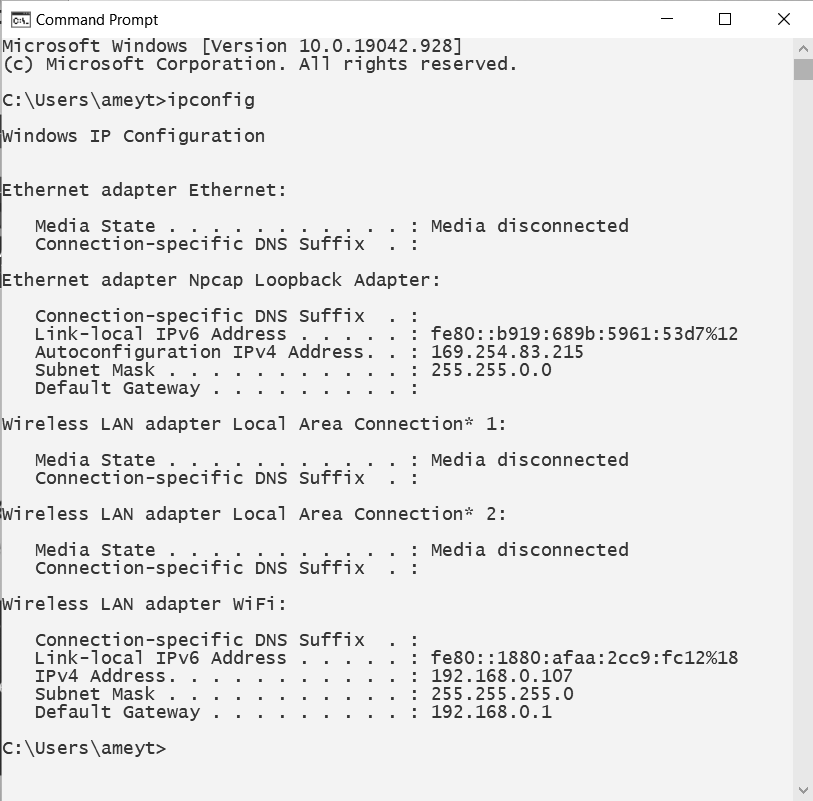
***(add a snapshot of output )***

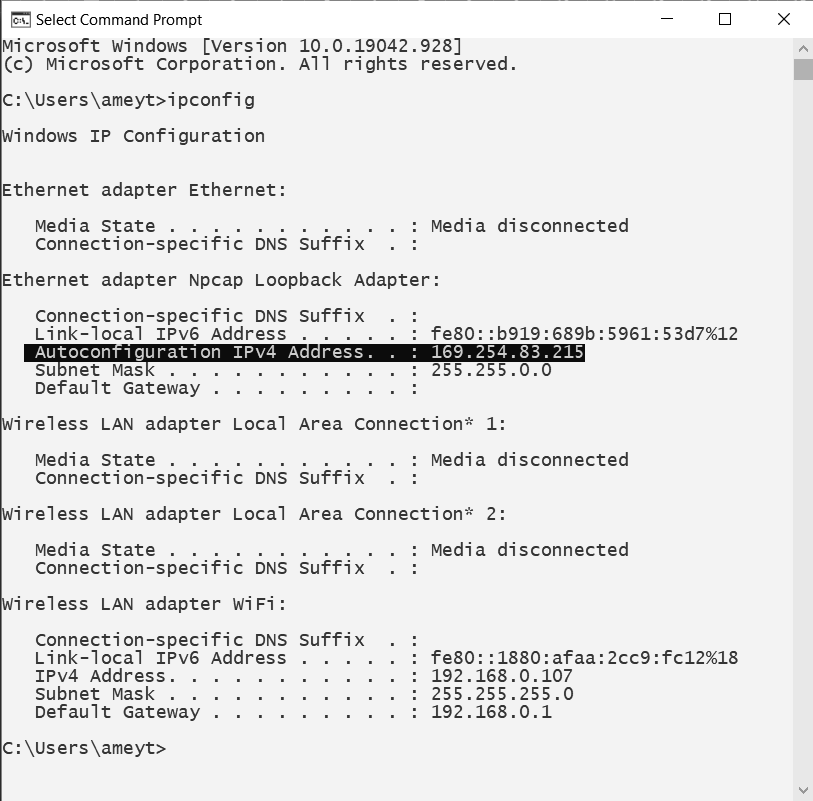
****

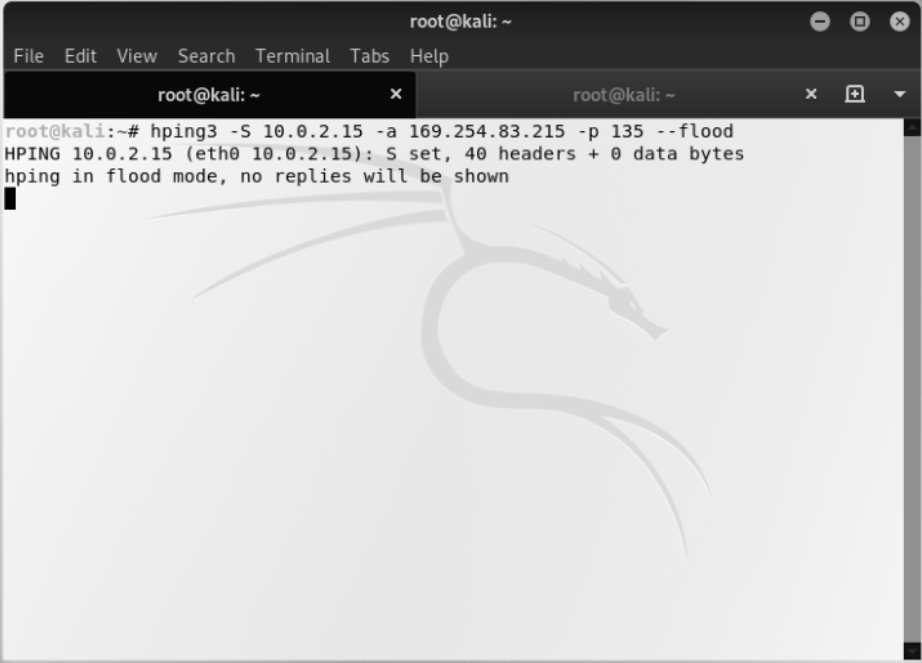
****

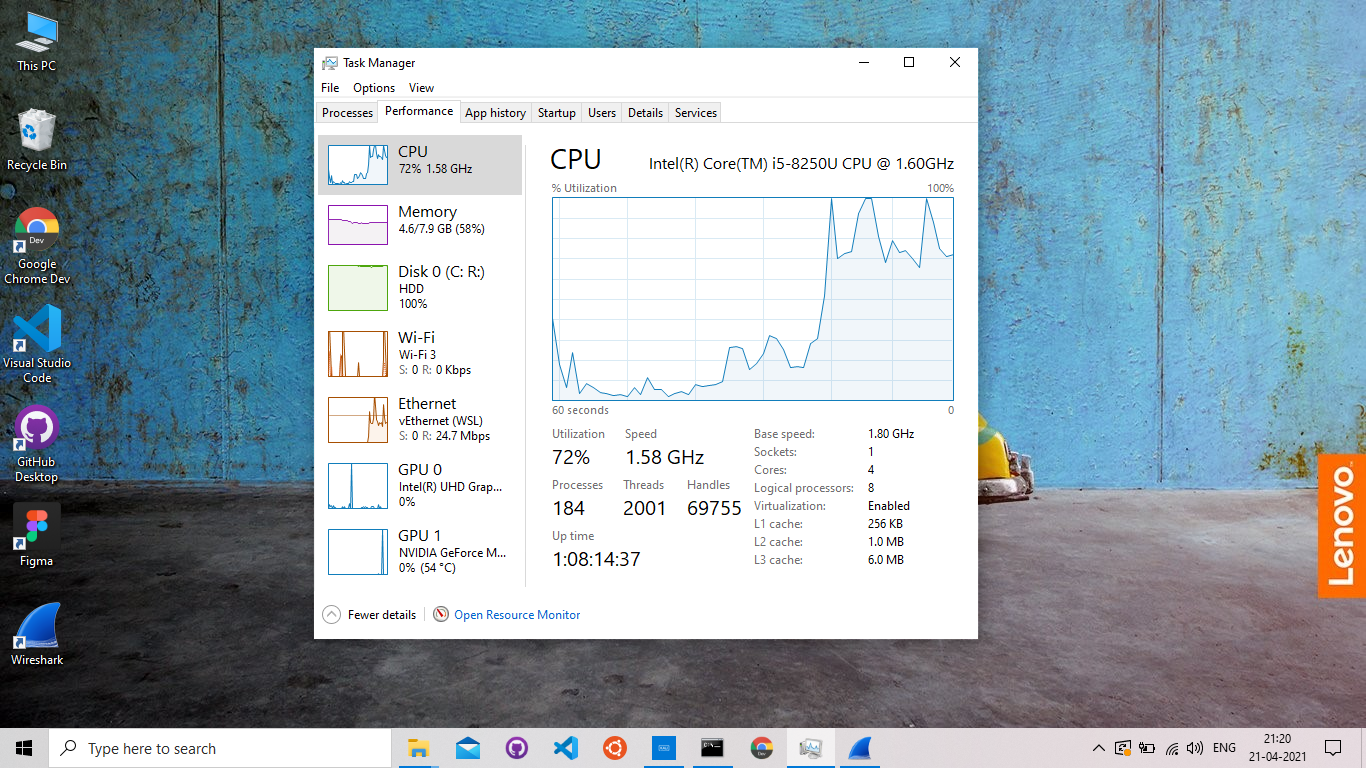
****

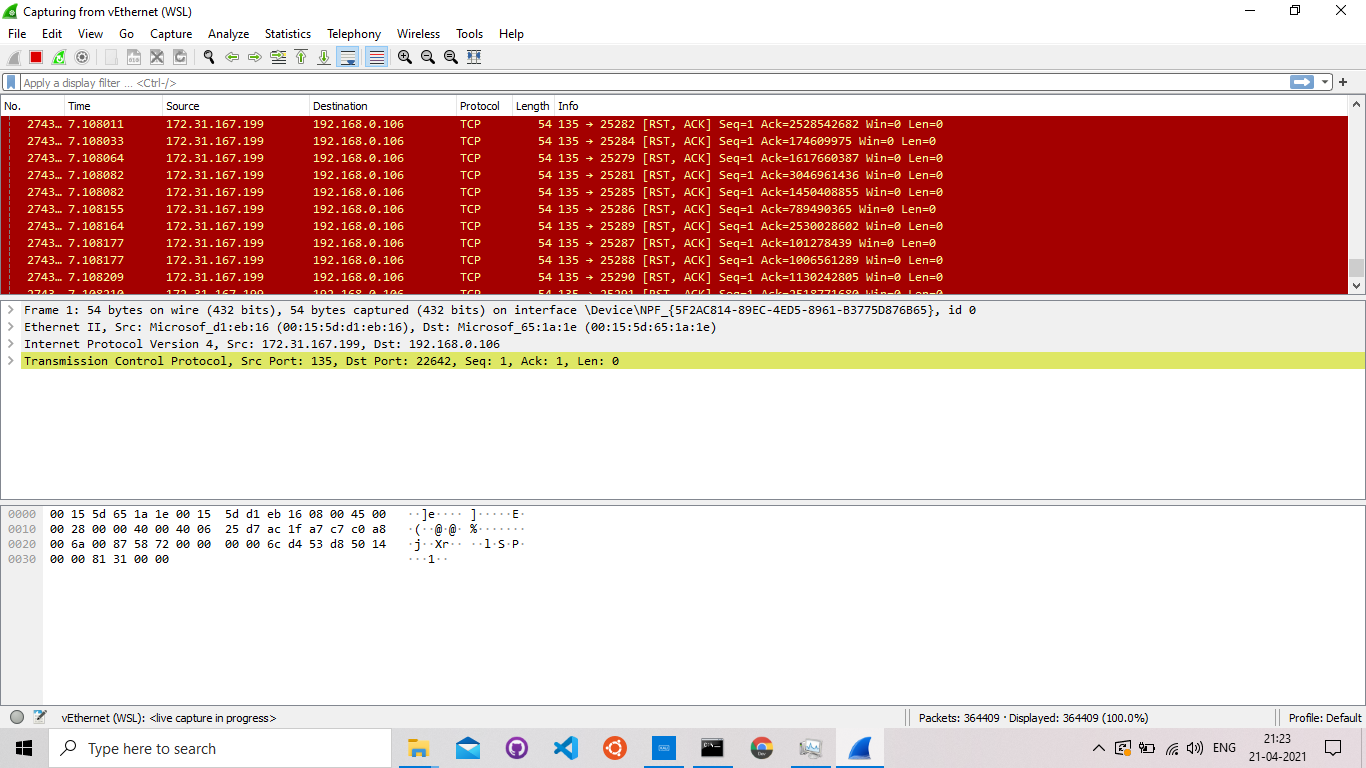
****

****

****

****



****

**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 |

1. 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.

1. 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.