

**Batch: B-1 Roll No: 16010422234 Name: Chandana Ramesh Galgali**

**Experiment No.:8**

### Aim: To study analysis of network using Scapy Library

### 

**Resources needed**: Python IDE



### Theory:

Traffic analysis is the process of intercepting and analyzing network traffic in order to deduce information from communication. The size of the packets exchanged between two hosts, details of the systems communicating, time and duration of communication are some of the valuable information to an attacker. Following is required to be studied under this experiment:

* Networking basics
* Raw socket programming
* Packet sniffing with Scapy
* Packet injection with Scapy
* Parse DNS traffic with Scapy
* OS fingerprinting with Scapy

### Activities:

### Students are expected to sit in pair-neighboring PC’s and should perform the communication)

### Result: (script and output)

Code:

### from scapy.all import \*

### def packet\_handler(packet):

### if packet.haslayer(IP):

### src\_ip = packet[IP].src

### dst\_ip = packet[IP].dst

### print(f"Source IP: {src\_ip} --> Destination IP: {dst\_ip}")

### if packet.haslayer(TCP):

### src\_port = packet[TCP].sport

### dst\_port = packet[TCP].dport

### print(f"Source Port: {src\_port} --> Destination Port: {dst\_port}")

### if packet.haslayer(Raw):

### http\_data = packet[Raw].load

### print(f"HTTP Data: {http\_data}")

### # Set the network interface to monitor

### interface = "eth0"

### # Start sniffing packets

### sniff(iface=interface, prn=packet\_handler)

Output:

### 

### 

### Outcomes: Demonstrate handling database with python and to understand network

### programming with Python scapy.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Conclusion:** (Conclusion to be based on the objectives and outcomes achieved)

The study of network analysis using the Scapy library proved to be a valuable learning experience, equipping us with the necessary skills and knowledge to effectively analyze and understand network traffic, identify potential security risks, and take appropriate measures to ensure network integrity and security.



**References:**

1. [https://www.oreilly.com/library/view/effective-python penetration/9781785280696/ch02.html](https://www.oreilly.com/library/view/effective-python%20penetration/9781785280696/ch02.html)