|  |
| --- |
| Network Sniffier |
|  |

Name: Muhammad Faisal Rahman

Email: [fmfaisalrahman@gmail.com](mailto:fmfaisalrahman@gmail.com)

Reg id: CA/MA1/9298

Submitted To: CodeAlpha

Domain: Cyber Security

**Task 1: Basic Network Sniffer**

**Introduction**

A network sniffer is a tool used to capture and analyze network traffic. It helps in understanding how data flows through a network and how packets are structured. This project involves creating a simple network sniffer in Python using the **Scapy** library, which allows us to capture and inspect network packets in real-time.

**Objectives**

* Capture live network packets.
* Analyze packet headers such as source IP, destination IP, and protocol.
* Display packet details in real-time.
* Understand network traffic flow.

**Python Code for Network Sniffer**

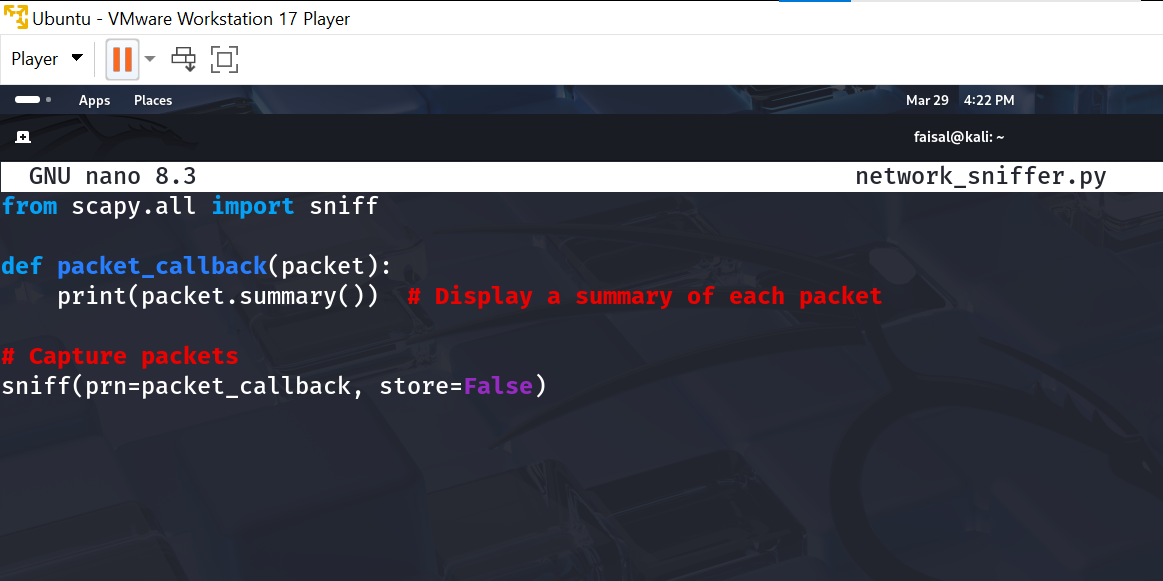
**from scapy.all import sniff**

**def packet\_callback(packet):**

**print(packet.summary()) # Display a summary of each packet**

**# Capture packets**

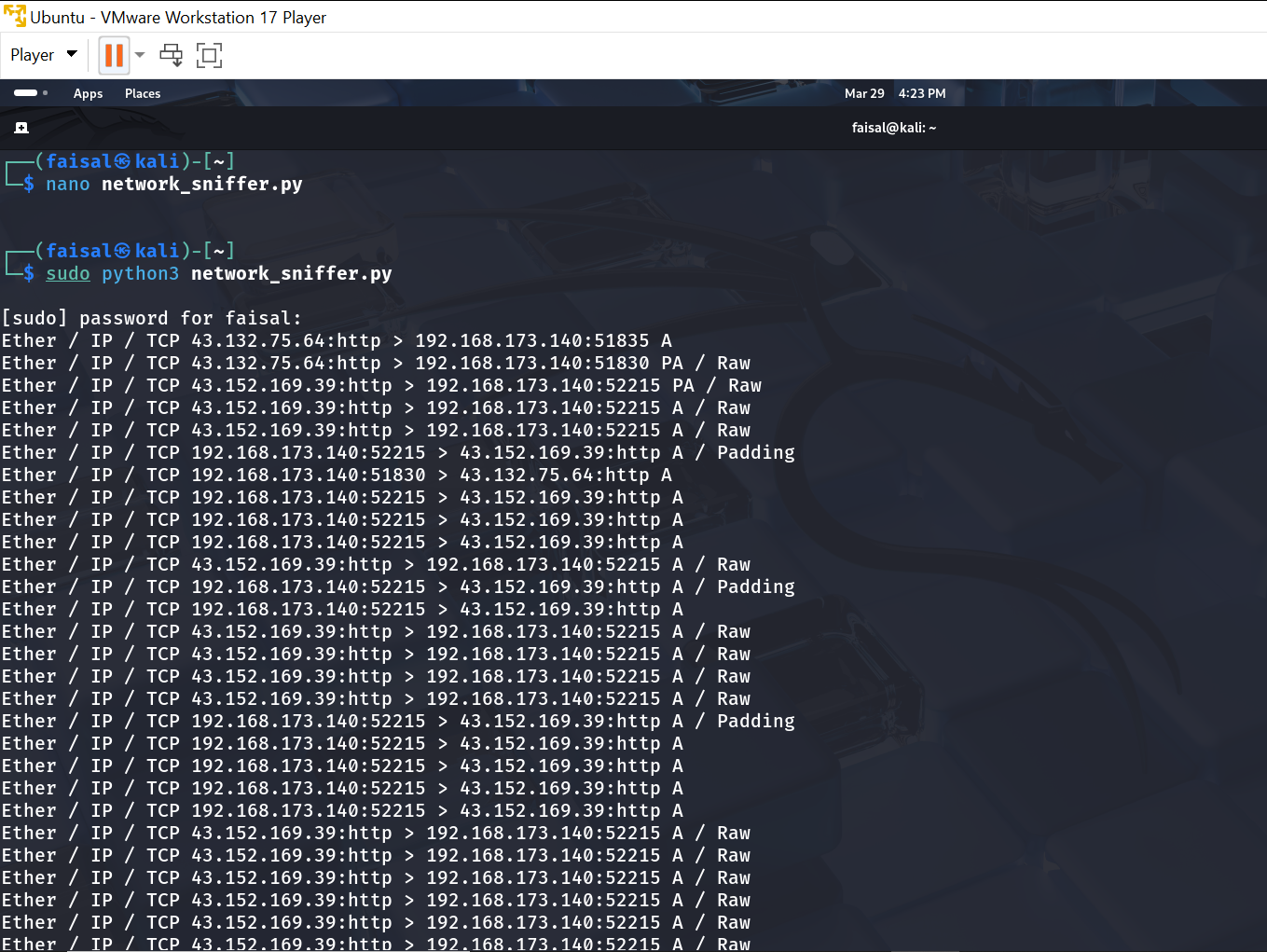
**sniff(prn=packet\_callback, store=False)**



**How to Run the Script**

1. Open a terminal in Kali Linux.
2. Navigate to the directory where the script is saved.
3. Run the following command:
4. sudo python3 network\_sniffer.py
5. The script will start capturing network packets and display them in real-time.

**Example Output**



**Conclusion**

This project provided insights into how network sniffers work and how they can be used for **network monitoring and security analysis**. By analyzing packets, we can identify potential network threats and understand data transmission patterns. This knowledge is useful for cybersecurity professionals, ethical hackers, and network administrators.