Network Packet Sniffer with Alert System

1. Introduction

The Network Packet Sniffer with Alert System is a cybersecurity tool designed to monitor and analyze real-time network traffic. Built using Python and Scapy, this tool captures packet metadata and stores it in a SQLite database for further inspection. The system also includes a basic anomaly detection engine that flags unusual traffic patterns like port scanning or DDoS attempts.

2. Abstract

This project captures live network packets, logs them to a local SQLite database, and analyzes traffic patterns to detect anomalies. It includes a visualization module that displays the top IP addresses involved in the traffic. The system provides a foundational understanding of packet-level network monitoring, useful for cybersecurity learners and professionals.

3. Tools Used

- Python 3
- Scapy (for packet sniffing)
- SQLite3 (for local packet logging)
- Matplotlib (for visualizing traffic patterns)
- Kali Linux (for execution environment)

4. Steps Involved

Step 1: Install dependencies using apt (python3-scapy, python3-matplotlib, sqlite3).

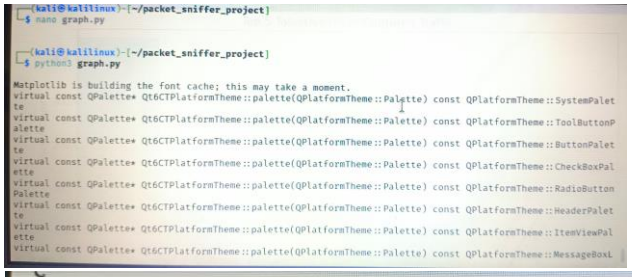
Step 2: Create sniffer.py to capture and log network packets.

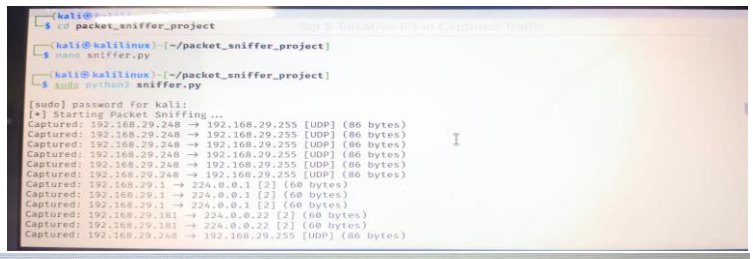
Step 3: Add anomaly detection logic for basic port scan and flood detection.

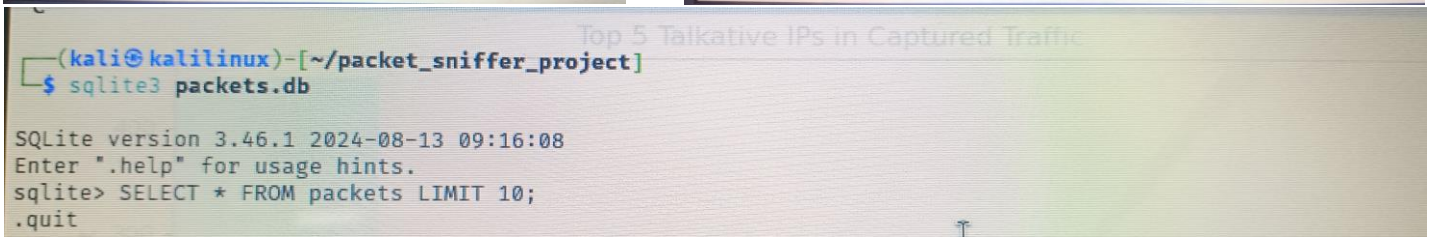
Step 4: Store all packets into packets.db using SQLite3.

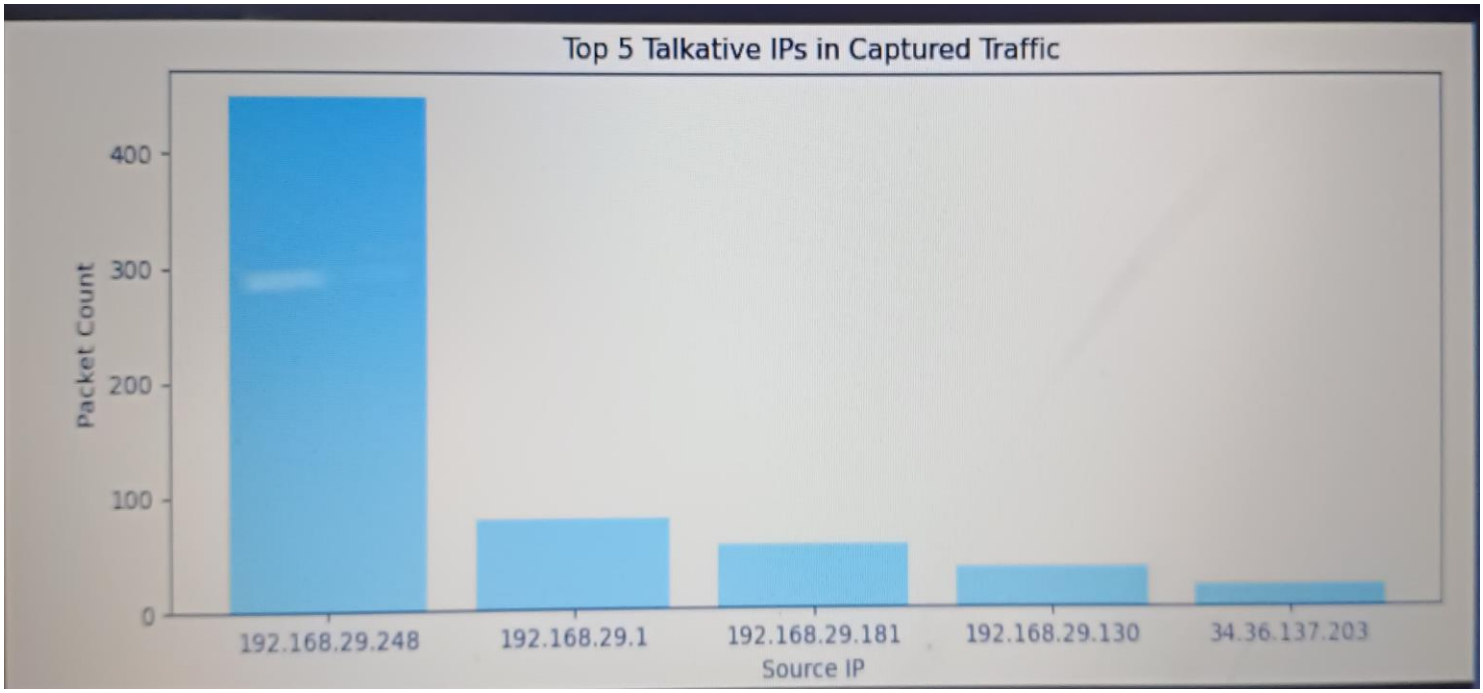
Step 5: Create graph.py to visualize packet counts per source IP using matplotlib.

OUTPUT IMAGES:









Conclusion

This project successfully demonstrates real-time packet sniffing and basic traffic analysis. It provides a foundational skillset for understanding network behavior and detecting potential intrusions.