

# 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:

```
(kali@kali:~/packet_sniffer_project)
$ nano graph.py

(kali@kali:~/packet_sniffer_project)
$ python3 graph.py

Metplotlib is building the font cache; this may take a moment.
virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalet
te
virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolButtonP
alette
virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ButtonPalet
te
virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::CheckBoxPal
ette
virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::RadioButton
Palette
virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::HeaderPalet
te
virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ItemViewPal
ette
virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::MessageBoxL

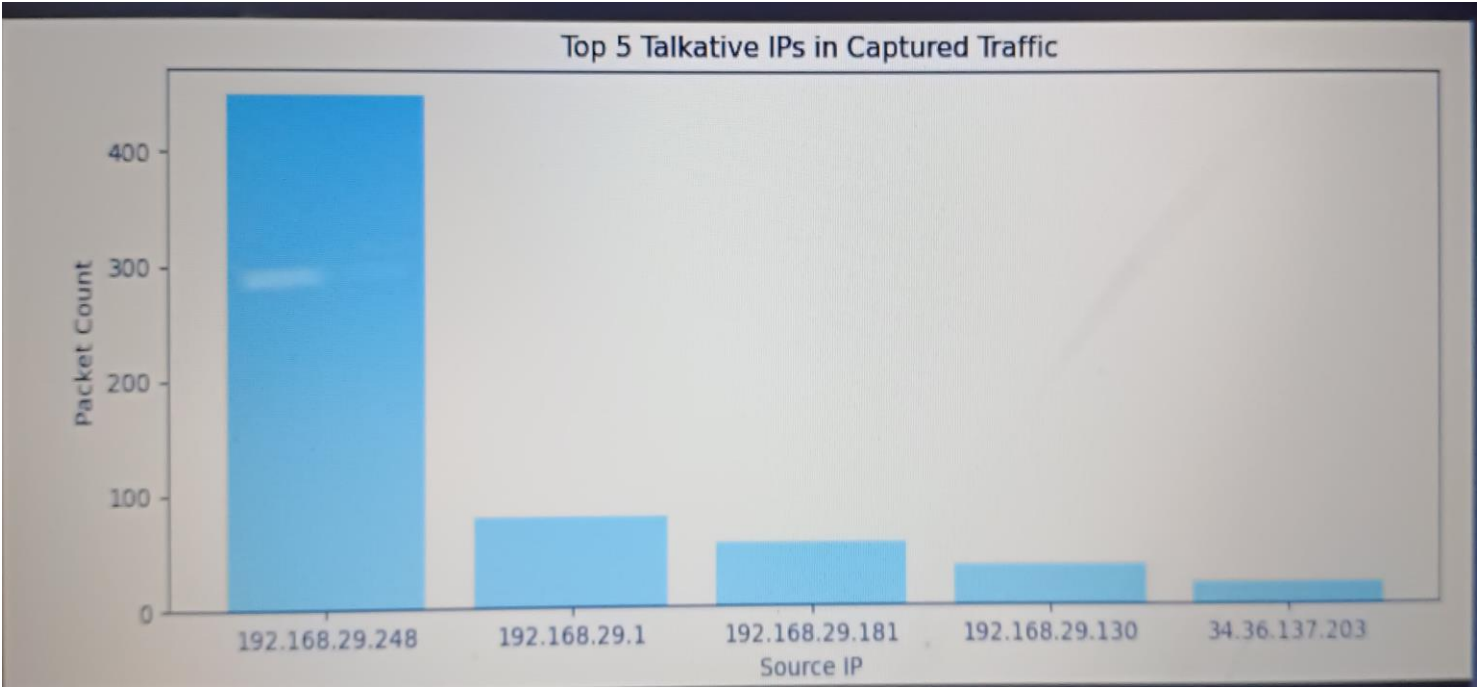
(kali@kali:~/packet_sniffer_project)
$ cd packet_sniffer_project
$ nano sniffer.py
$ sudo python3 sniffer.py

[sudo] password for kali:
[*] Starting Packet Sniffing ...
Captured: 192.168.29.248 -> 192.168.29.255 [UDP] (86 bytes)
Captured: 192.168.29.248 -> 192.168.29.255 [UDP] (86 bytes)
Captured: 192.168.29.248 -> 192.168.29.255 [UDP] (86 bytes)
Captured: 192.168.29.248 -> 192.168.29.255 [UDP] (86 bytes)
Captured: 192.168.29.248 -> 192.168.29.255 [UDP] (86 bytes)
Captured: 192.168.29.248 -> 192.168.29.255 [UDP] (86 bytes)
Captured: 192.168.29.1 -> 224.0.0.1 [2] (60 bytes)
Captured: 192.168.29.1 -> 224.0.0.1 [2] (60 bytes)
Captured: 192.168.29.1 -> 224.0.0.1 [2] (60 bytes)
Captured: 192.168.29.181 -> 224.0.0.22 [2] (60 bytes)
Captured: 192.168.29.181 -> 224.0.0.22 [2] (60 bytes)
Captured: 192.168.29.248 -> 192.168.29.255 [UDP] (86 bytes)

Top 5 Talkative IPs in Captured Traffic

(kali@kali:~/packet_sniffer_project)
$ sqlite3 packets.db

SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> SELECT * FROM packets LIMIT 10;
.quit
```



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.