■ Network Intrusion Detection Project Report

This project demonstrates the development of a custom Network Intrusion Detection System (IDS) using Python. It passively sniffs network traffic, detects common reconnaissance and flooding attacks, logs events, and provides analysis with visualizations.

■ Objectives

- Capture live TCP/UDP packets from a chosen interface.
- Detect common scanning techniques (SYN, FIN, Xmas, Null, UDP).
- Identify flood attacks exceeding defined thresholds.
- Log alerts into both a file (alerts.log) and SQLite database (packets.db).
- Provide analysis of logs through CLI queries.
- Generate charts summarizing attacks and top sources.

■ Tools Used

- Python 3 - Scapy (packet sniffing) - SQLite3 (alert storage) - Matplotlib (visualization) - Linux/Kali environment (testing with Nmap & Hping3)

■■ Implementation Steps

1. Developed `sniffer.py` to sniff packets and detect scans/floods.
2. Configured thresholds (Flood >100 pkts in 10s, Scan >10 ports in 10s).
3. Created `analyze.py` to query database: top attackers, scan types, recent alerts.
4. Implemented `charts.py` to generate: Alerts by Type, Top Attackers, Alerts Timeline.
5. Tested tool using `nmap` (SYN, FIN, Xmas, Null, UDP scans) and flood attacks (hping3).
6. Logs saved in `alerts.log` and structured data in `packets.db`.
7. Visual charts exported as PNG images and added to report.

■ Results

- Successfully detected multiple scan types: SYN, FIN, Xmas, Null, UDP. - Detected flood attacks with thousands of packets in short windows. - Analysis showed **192.168.80.129** as the top attacking source with 63+ alerts. - Charts generated: - Alerts by Scan Type - Top Attacking Sources - Alerts Timeline

■ Conclusion

The project successfully demonstrates how a Python-based IDS can monitor live network traffic, detect scanning and flooding attacks, and log them for forensic analysis. It provides both command-line summaries and visual insights, making it useful for learning and real-world scenarios.

■ Future Improvements

- Add machine learning models for anomaly-based detection.
- Integrate with a web dashboard for real-time monitoring.
- Support for distributed IDS sensors across multiple networks.