Advanced Network Security Monitoring System with Automated Threat Detection

G. Tharun Reddy, M. Sai Yeswanth

Motivation:

- The landscape of cyber threats is constantly evolving, demanding continuous network monitoring.
- Adequate security requires visibility into network traffic to identify malicious activities, policy violations, and anomalies

PROBLEM STATEMENT:

- Effective network security demands real-time monitoring and the ability to correlate diverse threat indicators like suspicious payloads, protocol anomalies, scanning patterns, and malicious IP reputations.

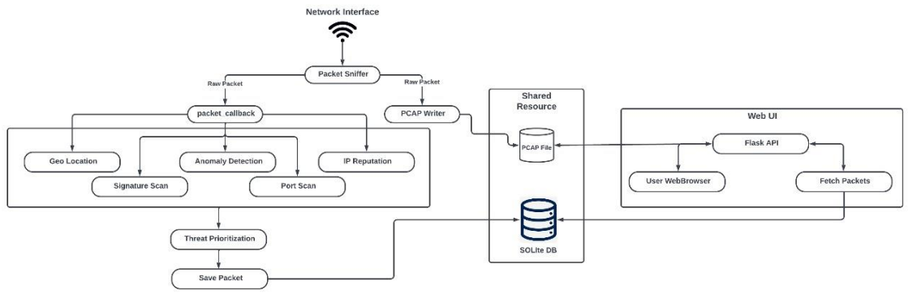
- However, analysts and students often face challenges due to the lack of accessible tools that integrate these multiple detection techniques simultaneously.

OBJECTIVE:

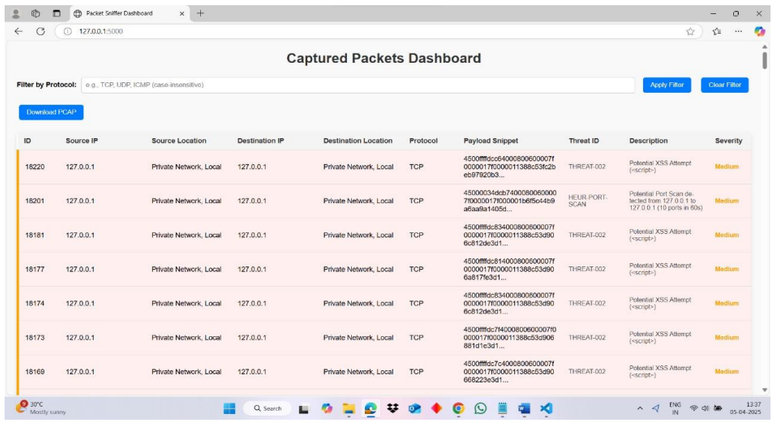
Develop: A system capable of capturing network packets from a specified interface using Scapy.

Implement: Multiple threat analysis techniques: Signature-based detection (matching known malicious patterns). Protocol anomaly detection (identifying invalid protocol usage, e.g., Xmas/Null scans).
Integrate: Geolocation lookup to provide context for source and destination IP addresses.
Visualize: Create a dynamic web-based dashboard (using Flask) to display captured packets, highlight potential threats clearly,

DESIGN:



WEB RESULTS:



TECHNOLOGY USED:

Python: The primary programming language.

Scapy: Powerful Python library for packet capture, manipulation, and analysis.

Flask: Micro web framework used to build the web dashboard API and UI.

SQLite: Lightweight, file-based database used for storing packet data.

HTML, CSS, JavaScript: Standard web technologies for the front-end dashboard.

GeoIP2 (MaxMind): Python library and database format for IP geolocation lookup.

External Services/APIs Integrated:

AbuseIPDB API: External threat intelligence service used for IP reputation checking.

CONCLUSION:

- This project successfully delivers a functional prototype of an integrated network threat detection system.

- It showcases the practical application of multiple analysis techniques and provides a valuable tool for visualizing network activity and potential threats in real-time.

- It meets the objectives of building a capture, analysis, storage, and visualization system, demonstrating key cybersecurity principles and practical software development skills.

AMRITA VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY UNDER SECTION 3 OF UGC ACT, 1956
SCHOOL OF COMPUTING CHENNAI