Name: Samrat Amit Sawant
Project: Enhanced Network Packet Sniffer with Security Monitoring

Project Report

Introduction

This project involved developing a comprehensive Enhanced Network Packet Sniffer - a real-time desktop application designed to capture, analyze, and monitor network traffic with advanced security threat detection capabilities. The application serves as a centralized platform for network administrators and security professionals to perform deep packet inspection, anomaly detection, and comprehensive network security analysis. The sniffer provides both IPv4 and IPv6 protocol support with intelligent threat scoring and automated alerting mechanisms.

Abstract

The Enhanced Network Packet Sniffer integrates advanced packet capture capabilities using Scapy library with sophisticated anomaly detection algorithms including port scan detection, SYN flood analysis, and DNS flood monitoring. The system utilizes SQLite for efficient data storage and implements real-time risk scoring (0-10 scale) for each captured packet. The application features a comprehensive GUI built with Tkinter, providing interactive visualizations through Matplotlib and real-time security dashboards. Advanced features include automated email alerting via SMTP, multi-protocol filtering, IPv6 support, and comprehensive data export functionality in CSV and JSON formats. The dashboard provides an intuitive interface for security operations teams to efficiently monitor, analyze, and respond to network security threats in real-time.

Tools Used

Core Technologies:

- Python 3.8+ with Tkinter framework for desktop GUI development
- Scapy library for advanced packet capture and manipulation
- SQLite3 for embedded database management and packet storage
- Matplotlib for statistical data visualization and trend analysis
- Threading module for concurrent packet processing

Security Libraries:

- smtplib for automated email alert system integration
- ipaddress for IPv4/IPv6 address validation and network analysis
- collections module for advanced data structures and traffic analysis

System Dependencies:

- Npcap/WinPcap for Windows packet capture driver support
- libpcap for Linux/macOS packet capture library integration

Communication & Analysis:

- queue module for thread-safe inter-process communication
- random and time modules for demo traffic simulation
- json module for structured data export capabilities

Steps Involved in Building the Project

1. System Architecture & Design

- Configured development environment with Python virtual environment and dependencies
- Implemented modular architecture separating packet capture, analysis, and GUI components
- Designed enhanced SQLite database schema supporting packet metadata, security events, and alert management

2. Core Packet Capture Engine Development

- Developed advanced packet sniffing functionality using Scapy with multi-interface support
- Created comprehensive protocol parsers supporting TCP, UDP, ICMP, IPv4, and IPv6
- Implemented real-time packet processing with efficient memory management and threading

3. Security Analysis Module Implementation

- Built intelligent anomaly detection algorithms with configurable thresholds:
- Port scan detection with time-based tracking and IP reputation analysis
- SYN flood detection monitoring packet rate patterns and TCP flag analysis
- DNS flood monitoring with query volume analysis and suspicious pattern recognition
- Developed comprehensive risk scoring algorithm providing quantitative threat assessment (0-10 scale)

4. Enhanced GUI Development

- Designed professional desktop interface using Tkinter with tabbed navigation layout
- Implemented real-time packet visualization with advanced filtering and search capabilities
- Created interactive security dashboard displaying threat metrics, risk scores, and attack patterns
- Built comprehensive configuration panel for detection thresholds and system parameters

5. Advanced Features Integration

- Developed automated SMTP email alerting system with customizable templates and cooldown protection
- Implemented multi-format data export functionality (CSV/JSON) with filtering options
- Created enhanced IPv6 support for modern network infrastructure monitoring
- Built comprehensive help system with troubleshooting guides and feature documentation

6. Testing & Performance Optimization

- Conducted extensive testing with simulated network traffic and real-world packet captures
- Implemented performance optimizations including memory management and efficient data structures
- Validated security detection algorithms against known attack patterns and false positive reduction
- Performed cross-platform compatibility testing on Windows, Linux, and macOS systems

Conclusion

The Enhanced Network Packet Sniffer project successfully demonstrates the integration of advanced network monitoring capabilities with sophisticated security analysis features. The application provides comprehensive network visibility through an intuitive desktop interface while offering enterprise-grade threat detection capabilities suitable for both educational and production environments.

Project Completion Date: August 23, 2025
Technologies: Python, Scapy, Tkinter, SQLite, Matplotlib, Threading, SMTP
Key Features: Real-time monitoring, Advanced threat detection, IPv6 support, Risk scoring, Email alerts