Introduction

Network security is a critical aspect of modern computing environments. With the rise in cyber threats such as port scanning and denial-of-service attacks, real-time monitoring of network traffic has become essential. This project focuses on developing a Network Packet Sniffer with an Alert System to detect suspicious activities and notify users immediately.

Abstract

This project implements a Python-based network packet sniffer using the Scapy library. It captures TCP packets in real time and analyzes SYN traffic patterns to detect potential port scanning and SYN flood attacks. A graphical interface displays alerts, while detected threats are logged into a database and log files for future analysis.

Tools Used

• Python
• Scapy – Packet capturing and analysis
• Tkinter – Graphical User Interface
• SQLite – Alert data storage
• Winsound – Audio alerts
• Socket, Threading – Networking and concurrency

Steps Involved in Building the Project

1. Requirement analysis and threat identification.
2. Designing detection logic for port scanning and SYN flood attacks.
3. Implementing packet sniffing using Scapy.
4. Filtering and analyzing TCP SYN packets.
5. Creating an alert mechanism with severity levels.
6. Designing a dark-mode GUI using Tkinter.
7. Logging alerts into SQLite database and log files.
8. Testing the system under simulated attack conditions.

Conclusion

The Network Packet Sniffer with Alert System successfully detects suspicious network activities such as port scanning and SYN flooding in real time. By combining packet analysis, logging, and a user-friendly interface, this project demonstrates an effective approach to intrusion detection. It serves as a strong foundation for advanced IDS/IPS systems and future enhancements.