Introduction

With the increasing number of cyber attacks and unauthorized network access attempts, firewalls play a vital role in protecting systems and networks. This project focuses on designing and implementing a Python-based Linux Firewall with a graphical user interface to monitor, control, and block malicious network traffic in real time.

Abstract

The Python Linux Firewall project is a rule-based firewall application developed using Python and the Scapy library. It inspects incoming network packets and applies predefined security rules to block malicious IP addresses, ports, and protocols. The system also detects port scanning behavior and dynamically blocks attackers using iptables, while providing real-time logs and alerts through a user-friendly GUI.

Tools Used

- Python
- Scapy – Packet sniffing and protocol analysis
- Tkinter – Graphical User Interface
- IPTables – Linux packet filtering and blocking
- Socket – Local IP detection
- Threading – Parallel packet processing
- Linux OS

Steps Involved in Building the Project

1. Requirement analysis and identification of firewall rules.
2. Designing rule sets for IP, port, and protocol blocking.
3. Implementing packet sniffing using Scapy.
4. Detecting port scanning based on SYN packet thresholds.
5. Integrating iptables commands for dynamic blocking.
6. Developing a GUI using Tkinter for rule management.
7. Implementing logging and alert mechanisms.
8. Adding dark mode and real-time status monitoring.
9. Testing firewall behavior under simulated attacks.

Conclusion

The Python Linux Firewall successfully demonstrates an effective approach to real-time network protection using packet inspection and rule-based filtering. By combining Scapy, iptables, and a graphical interface, the project provides both functionality and usability. This firewall can be further enhanced with advanced intrusion detection techniques, machine learning-based analysis, and support for outbound traffic control.