Personal Firewall using Python

Abstract

This project focuses on building a lightweight personal firewall using Python. It enables users to monitor, filter, and block network traffic based on customizable rules. The firewall uses Scapy for packet sniffing and filtering, iptables for system-level enforcement on Linux, and PyQt5 for a graphical user interface to manage rules and monitor live traffic. The project serves as an educational tool for understanding how firewalls operate and provides a basic security layer for personal systems.

Introduction

A firewall is a critical component of network security that monitors and controls incoming and outgoing network traffic. The primary objective of this project is to develop a personal firewall in Python that can filter traffic based on rules defined by the user. In addition to providing acommand-line interface (CLI), a graphical user interface (GUI) is implemented using PyQt5 for ease of use. This project is not only practical but also helps students and cybersecurity enthusiasts gain hands-on experience in packet filtering and security mechanisms.

Tools Used

- Python: Core programming language used for building the firewall. - Scapy: Library for packet sniffing, analysis, and manipulation. - iptables: Linux firewall utility for enforcing traffic filtering at the system level. - PyQt5: GUI framework for building a user-friendly interface. - Logging Module: To record suspicious and blocked traffic for auditing.

Steps Involved in Building the Project

1. Packet Sniffing: Using Scapy to capture incoming and outgoing packets.
2. Rule Definition:Allowing users to create custom rules for blocking or allowing traffic based on IP, port, and protocol.
3. Traffic Filtering: Applying the defined rules to decide whether to block or allow packets.
4. GUI Development: Building a PyQt5 interface for live traffic monitoring and rule management.

Conclusion

The personal firewall developed in this project provides a lightweight and customizable solution for monitoring and controlling network traffic. By combining Scapy, iptables, and PyQt5, it offers both command-line and graphical interfaces to suit different user preferences. The project demonstrates the fundamentals of packet filtering, system-level rule enforcement, and security auditing. It is a practical implementation that bridges theoretical knowledge with real-world application in cybersecurity.