Project: Personal Firewall Using Python

Name: Sahil Husain Tadavi

Introduction

In the modern digital landscape, the rise in cyber threats makes personal security tools increasingly essential. This project aims to develop a lightweight personal firewall using Python. It is capable of sniffing, filtering, and logging network traffic based on customizable rules. This firewall is ideal for learning network security concepts and creating a foundational security tool.

Abstract

This project demonstrates the creation of a personal firewall that captures and filters network traffic in real-time using Python and the Scapy library. The firewall applies user-defined rules to allow or block packets based on IP addresses, ports, and protocols. Logged data provides visibility into allowed and blocked communications, while optional integrations with Linux iptables and a Tkinter GUI add enforcement and interactivity.

Tools Used:

- Python 3
- Scapy (pip install scapy)
- Linux iptables (for enforcing rules)
- Tkinter (for optional GUI interface)
- Text editor (e.g., VS Code, nano)

Features:

- Real-time packet sniffing using Scapy
- Rule-based filtering for IP, port, protocol
- Activity logging with timestamps
- Optional iptables integration for system-level enforcement
- Optional Tkinter-based GUI for live monitoring

Conclusion

This project provides hands-on experience in building a personal firewall using Python. By leveraging Scapy for packet sniffing and rule enforcement, users learn about network protocols, real-time monitoring, and packet-level filtering.

It can be expanded with anomaly detection, machine learning, or deeper OS-level integrations for advanced use cases.