Personal Firewall Using Python - Project Report

Introduction

As cyber threats continue to evolve, protecting individual systems from malicious traffic is increasingly important. This project focuses on designing and implementing a lightweight personal firewall using Python on Kali Linux. The firewall monitors network traffic, blocks harmful connections based on customizable rules, and logs network activity for auditing and analysis. The solution is intended as a learning tool and a foundational step toward understanding host-based intrusion detection systems (HIDS).

Abstract

This project involved building a command-line-based firewall in Python that filters network packets in real time using Scapy. The firewall can block traffic based on source/destination IPs, ports, and protocol types. It also inspects DNS packets to block malicious domains and optionally logs suspicious or unauthorized traffic. The project includes an optional layer using iptables for enforcing system-level blocking rules. The tool was tested on Kali Linux and can be extended with a GUI using Tkinter for live monitoring.

Tools Used

- Python 3: Primary language for logic and packet inspection.
- Scapy: Python library for packet sniffing and analysis.
- iptables: Linux firewall utility for system-level enforcement.
- Kali Linux: Testing and development environment.
- (Optional) Tkinter: GUI interface for real-time log viewing.

Steps Involved in Building the Project

1. Environment Setup: Installed Python, pip, Scapy, and iptables on Kali Linux.

2. Packet Sniffing: Used Scapy to capture live network packets.

3. Rule Engine: Developed filters to block:

   - Inbound IPs

   - Outbound IPs

   - Blocked ports

- Non-allowed protocols
- DNS requests to malicious domains

4. Logging: Recorded blocked/allowed packets with timestamps in a log file.

5. iptables Integration: Added optional rules to block IPs/ports at OS level.

6. Testing: Verified rule behavior using tools like ping, curl, and browser requests.

Conclusion

The personal firewall developed provides visibility and control over network traffic at the host level. Using Python and open-source tools, the firewall is capable of monitoring, blocking, and logging connections in real time. This project serves as a practical foundation for cybersecurity learners and can be enhanced with features like auto-rule updates, intrusion detection, and a GUI dashboard. The use of Scapy and iptables together demonstrates a blend of scripting and system-level security enforcement.