Personal Firewall Using Python

1. Introduction
This project presents the development of a lightweight Personal Firewall using Python. The firewall monitors live network traffic, filters packets based on predefined rules, logs suspicious activity, and enforces blocking using Linux iptables. The objective is to understand packet-level traffic inspection and implement rule-based filtering in a practical cybersecurity environment.

2. Objectives
• Capture live network packets using Python.
• Implement IP, port, and protocol-based filtering.
• Log suspicious and blocked traffic.
• Enforce blocking using iptables.
• Test in a controlled virtual environment.

3. Technologies Used
Python 3, Scapy library, Linux iptables, VirtualBox, JSON configuration files.

4. System Architecture
1. Load rules from rules.json.
2. Apply iptables rules.
3. Capture packets using Scapy.
4. Match packets against firewall rules.
5. Log blocked traffic.
6. Allow permitted traffic.

5. Implementation Details
Rules are defined in a JSON file allowing dynamic customization. Scapy captures packets and extracts source IP, destination IP, protocol, and ports. iptables enforces actual blocking at the kernel level. All blocked packets are recorded in firewall.log with timestamps for auditing.

6. Testing Environment
The firewall was tested using a VirtualBox virtual machine in Bridged Adapter mode. The VM simulated attacks such as ICMP ping requests and port connection attempts. Blocked traffic was successfully denied and logged.

7. Results
The firewall successfully captured traffic, enforced rule-based filtering, blocked restricted protocols and ports, and logged suspicious packets.

8. Limitations
Basic filtering only, no deep packet inspection, CLI-based monitoring, performance may reduce under heavy traffic.

9. Future Enhancements
GUI dashboard, automatic IP blocking, rate limiting, intrusion detection integration, real-time statistics visualization.

10. Conclusion
This project demonstrates practical implementation of a personal firewall using Python and Linux networking tools. It provides foundational knowledge for developing advanced network security systems.