Project Title: Python-Based GUI Personal Firewall using Scapy and Tkinter

---

1. Introduction: This project involves creating a personal firewall using Python that can monitor, block, and log suspicious network packets. A simple graphical user interface (GUI) built with Tkinter allows users to easily define firewall rules. The system also integrates with Linux's iptables to apply real network rules.

---

2. Abstract: The firewall uses Scapy for packet sniffing and inspection. It monitors incoming packets in real-time, checks them against a set of custom user rules, and either logs or blocks them. Rules can include specific IP addresses, ports, or protocols to be blocked. The GUI provides options to add, remove, and view rules. The project also auto-elevates privileges on Linux and Windows platforms to ensure firewall functionality.

---

3. Tools Used: Python 3.11 - Scapy - Tkinter - iptables (Linux) - subprocess, json, logging, threading - ctypes, os, sys (for admin elevation)

---

4. Steps Involved in Building the Project: 1. Install required Python packages (Scapy). 2. Design the rule structure using JSON. 3. Build a GUI using Tkinter (entry box, buttons, listbox). 4. Create rule management functions: add, delete, and save to JSON. 5. Implement Scapy-based packet sniffing in a background thread. 6. Match packets against rules (IP, ports, protocol). 7. Log or apply iptables rules based on matches. 8. Add cross-platform privilege elevation.

---

5. Conclusion: The firewall is a simple yet powerful demonstration of using Python for cybersecurity tasks. It effectively combines real-time monitoring, GUI interaction, and system-level rule enforcement. This project can be further extended into a more comprehensive network defense tool.
