Introduction

This project aims to **develop a lightweight personal firewall using Python**, capable of filtering network packets, applying user-defined rules, and logging suspicious activities.
The firewall is designed for educational and personal use to demonstrate how traffic filtering and packet inspection work at a basic level.

Abstract

The “Personal Firewall using Python” project is a simple yet powerful demonstration of network packet filtering.
It utilizes the **Scapy** library to capture, analyze, and filter packets based on customizable rules defined by the user. The project allows blocking or allowing packets depending on **IP address, port number, or protocol**.

The firewall runs as a **Command-Line Interface (CLI)** tool and optionally features a **Tkinter-based Graphical User Interface (GUI)** for live monitoring and rule management.

Tools Used

Tool / Library	Purpose / Description
Python 3	Core programming language used for implementation.
Scapy	Python library for packet capturing and analysis.
Tkinter	Used to build the optional graphical user interface (GUI).
iptables	Linux firewall tool used for enforcing rules at the kernel level.
JSON	Used to store user-defined rules in a simple configuration file.
Logging Module	For recording suspicious or blocked packets.

Steps Involved in Building the Project

Step 1: Setting up the Environment

```
sudo apt install python3 python3-tk -y
pip3 install scapy
```

Step 2: Packet Sniffing

Step 3: Rule Definition and Filtering

Step 4: Logging Suspicious Packets

Step 5: Optional GUI Integration

Step 6: System-Level Enforcement (Optional)

Step 7: Testing the Firewall

Conclusion

The Personal Firewall using Python project demonstrates the core functionality of network security systems in a simplified and educational manner.
By using Python's powerful libraries, it provides a clear understanding of:

- How packets flow through a network,
- How rules can be applied to manage this flow,
- How security systems can log and respond to suspicious activities.

While not intended for enterprise use, the project successfully showcases key firewall concepts such as packet inspection, rule enforcement, and logging.