**Project Report**

**Elevate Labs Cyber-Security Internship**

**Project Title:**

**Personal Firewall using Python**

**Date:**  
**26 July 2025**

**1. Abstract**

This project focuses on building a lightweight personal firewall using Python and the Scapy library. The firewall monitors and analyzes network traffic in real-time, allowing or blocking packets based on user-defined rules. It also maintains logs of suspicious packets for auditing purposes. The project demonstrates key cybersecurity concepts such as packet sniffing, traffic filtering, and the basics of intrusion detection.

**2. Introduction**

With the rapid growth of cyber threats, a firewall plays a crucial role in protecting systems from malicious traffic. This project is a simple Python-based firewall that captures packets, applies rule-based filtering, and logs blocked packets. The primary objective is to enhance understanding of network security and firewall operations through hands-on implementation.

**3. Objectives**

* To build a Python-based firewall that monitors and filters traffic.
* To create a flexible rule system for blocking/allowing IPs, ports, and protocols.
* To log suspicious packets for later analysis.
* To gain practical knowledge of packet inspection using Scapy.

**4. Tools & Technologies**

* **Python 3.8+** – Core programming language.
* **Scapy** – For packet sniffing and packet analysis.
* **JSON** – For defining allow/block rules.
* **Command Line (Windows/Linux)** – For executing the firewall.

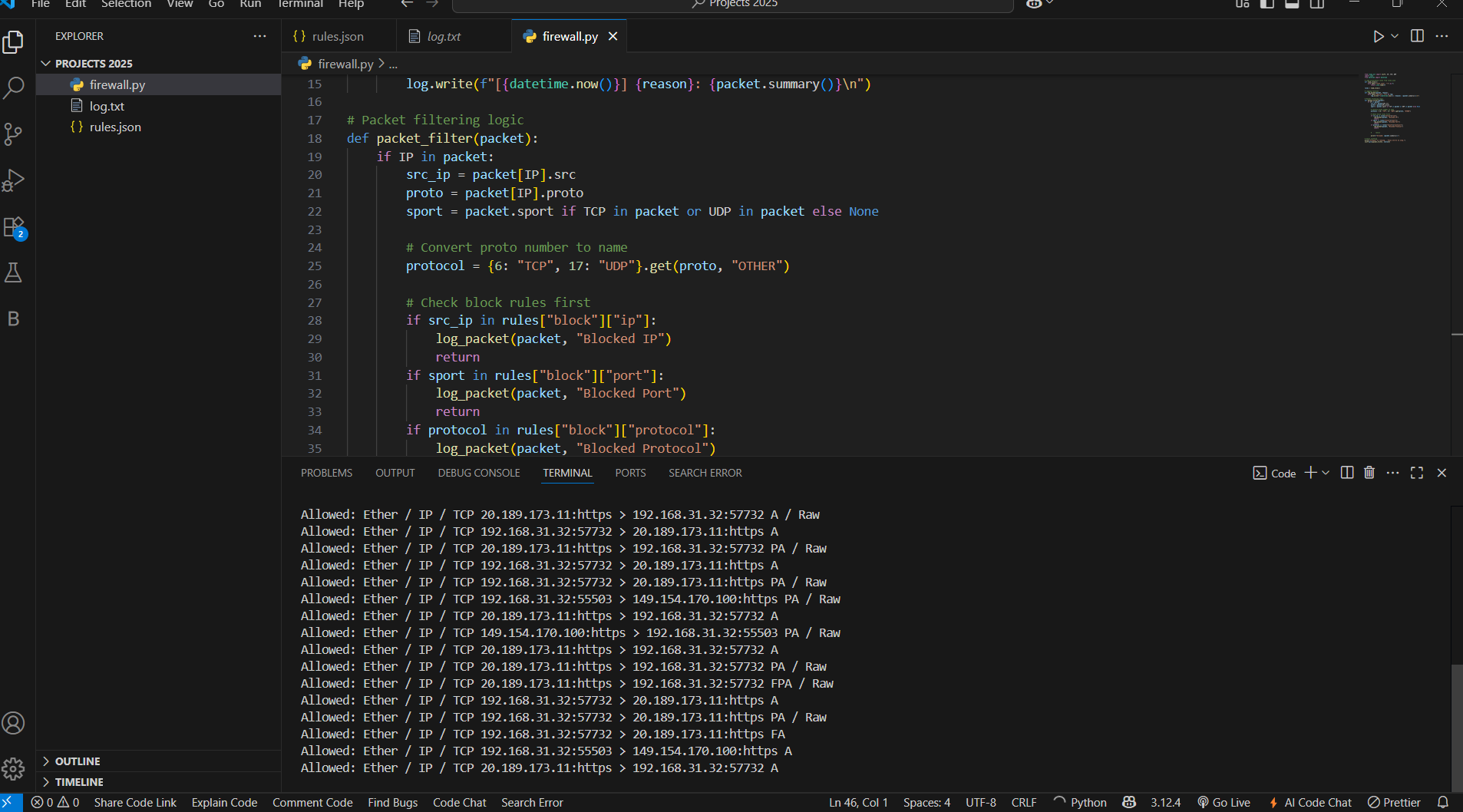
**5. Implementation Steps**

1. **Environment Setup:** Installed Python and the Scapy library.
2. **Rule Definition:** Created a rules.json file to define allow/block IPs, ports, and protocols.
3. **Packet Sniffing:** Used Scapy's sniff() function to capture real-time packets.
4. **Filtering:** Checked each packet against rules and allowed or blocked it.
5. **Logging:** Stored blocked/suspicious packets in log.txt with timestamps.
6. **Testing:** Simulated both valid and blocked traffic to verify the firewall functionality.

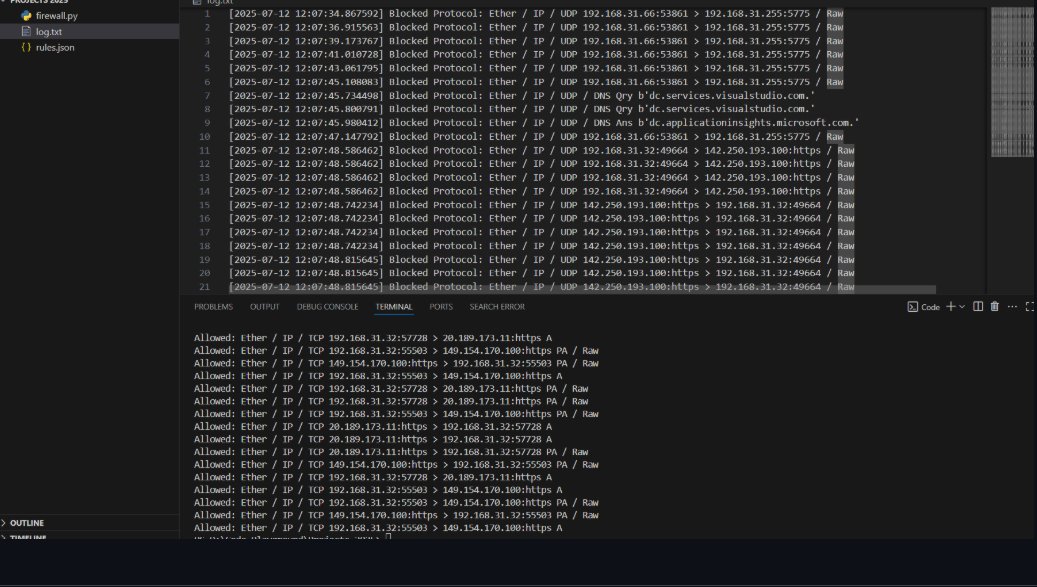
**6. Results/Features**

* Real-time packet monitoring and filtering.
* Easy customization through a rules file (rules.json).
* Detailed logs of blocked packets in log.txt.
* Cross-platform compatibility with Windows, Linux, and macOS.

**7. Screenshot**



**Log File:**



**8. Conclusion**

This project provided practical insights into the working of firewalls and network security fundamentals. By building a custom firewall using Python and Scapy, I developed skills in packet analysis, rule-based filtering, and log management. The project serves as a foundation for developing advanced security tools like Intrusion Detection Systems (IDS).

**Submitted by:**  
**Shubham Adsule**  
**Cybersecurity Intern @ Elevate Labs**