Elevate Labs Project Final Report

Title: Personal Firewall using Python and Scapy

Name : Y KISHANSAI
Date : 29 - 07 - 2025

1. Introduction

In today's internet-driven world, every device connected to a network is exposed to various forms of unwanted or malicious traffic. A firewall is an essential layer of defense that filters incoming and outgoing network packets to protect systems from attacks. In this project, a simple personal firewall was developed using Python and the Scapy library to block ICMP and HTTP packets. The goal was to understand the fundamentals of packet inspection and filtering at the user level without relying on existing firewall applications.

2. Abstract

This project implements a basic yet functional personal firewall using Python and Scapy to monitor live network traffic and block specific packet types such as ICMP and HTTP. The firewall inspects each packet in real-time using a custom filtering function and blocks any packet that matches predefined rules. Blocked packets are logged with timestamps for later analysis. The firewall was built without using pip or any external dependencies, making it lightweight and system-compatible. The simplicity of the design allows for easy understanding and sets a strong foundation for future enhancements such as protocol extension, rule customization, and GUI support.

3. Tools Used

The main tools used in this project include:

- Python 3.11.2 – Used for writing the packet filtering logic.
- Scapy (installed via apt) – A Python library used to sniff and manipulate network packets.
- Parrot OS – Linux-based operating system used for development and testing.
- Nano – A terminal-based text editor used to create and modify the script.
- Logging module – To capture and store log messages related to blocked packets.

All tools were installed using the system's built-in package manager, and no pip installations were required, which aligns with the minimal dependency requirement of the project.

4. Steps Involved in Building the Project

Step 1: Environment Setup
The development was done on Parrot OS. Python and Scapy were installed using sudo apt install python3 python3-scapy.

Step 2: Project Folder Creation
A folder named Final_proj was created to hold the Python script, the log file, and images for documentation. All work was organized within this directory.

Step 3: Writing the Firewall Script
A Python file named firewall.py was created using Nano. Inside the script, Scapy's sniff() function was used to capture live packets. A custom function checked each packet to determine whether it was an ICMP or HTTP request. If matched, it was blocked, and an entry was written to a log file named firewall.log.

Step 4: Running the Firewall
The script was executed using sudo python3 firewall.py to ensure root-level permissions for packet sniffing. Once started, the script printed summaries of allowed packets and blocked the defined ones silently.

Step 5: Testing
ICMP traffic was generated using the ping command, and HTTP traffic was generated using the curl command. Both were successfully detected and blocked by the script, and appropriate logs were written.

Step 6: Verifying Logs
The contents of firewall.log were reviewed to verify the blocked entries. Screenshots were captured to show the script in action and the logged results.

5. Conclusion

The personal firewall project demonstrated how low-level packet filtering can be implemented in Python without relying on external or built-in OS firewall tools. It gave hands-on experience in working with Scapy for packet sniffing and filtering, and enhanced understanding of protocols like ICMP and TCP. The firewall was able to identify and block network packets based on protocol type and port, logging all blocked attempts for future review.

While this project is basic in nature, it successfully meets its goal of introducing network packet filtering to beginners. Future improvements can include rule configuration files, GUI support, extended protocol blocking (e.g., DNS or FTP), and email alerts. The experience gained through this project will serve as a foundation for more advanced cybersecurity work in both academic and professional settings.