Internship Project Report

Name: Moksh Sharma

Internship Duration: 23rd June 2025 – 28th July 2025

Organization: ***Elevate Labs***

# Project 1: Personal Firewall using Python with GUI

## Introduction

In the digital era, securing systems from network threats is essential. During my internship, I developed a **Personal Firewall using Python** with a user-friendly GUI. It monitors real-time traffic, detects threats like high packet rates and Nimda worm patterns, and supports IP blacklisting/whitelisting for customizable protection.

## Abstract

This project presents a basic but effective firewall built using Python and the Scapy library for packet sniffing. It features a graphical interface using Tkinter, enabling users to monitor network activity in real time. The firewall can:  
- Detect and block high-frequency packet sources (indicative of DDoS-like behavior).  
- Identify suspicious payloads like the Nimda worm signature.  
- Block IPs dynamically based on pre-defined rules or packet rate thresholds.  
- Maintain and display logs of all network-related events.

## Tools and Technologies Used

- Python: Core programming language  
- Scapy: Network packet sniffing and inspection  
- Tkinter: GUI development  
- iptables: System-level command-line firewall to block IPs  
- OS & Sys modules: Interaction with the system and process control  
- Threading: Background sniffing without freezing GUI  
- ScrolledText & Listbox (Tkinter widgets): Displaying real-time logs and blocked IPs

## Steps Involved

1. Setup and Requirements  
2. Designing the GUI  
3. IP Whitelist and Blacklist Management  
4. Packet Sniffing using Scapy  
5. Threat Detection and Blocking  
6. Logging Events to file and GUI

## Conclusion

This internship project gave me practical exposure to network security fundamentals and Python programming for system-level applications. The Personal Firewall showcases how simple tools can be combined to build effective cybersecurity solutions. It also reinforced my understanding of traffic monitoring, process threading, GUI development, and Linux-based IP control.

**Project 2: Linux System Security Audit Tool Using Python**

## Introduction

System administrators and security professionals must continuously assess the security posture of Linux systems to ensure they are protected against vulnerabilities, misconfigurations, and unauthorized access. To support this, I developed a Linux System Security Audit Tool using Python during my internship. This command-line utility performs automated security checks across various areas of a Linux system, offering both real-time feedback and a detailed summary report.

## Abstract

This Python-based security audit tool automates essential checks on a Linux system to help identify potential security misconfigurations and vulnerabilities. It verifies critical file permissions, insecure services, SSH configurations, firewall status, software updates, and kernel settings. It provides a comprehensive output with categorized results—PASS, FAIL, WARN, or INFO—and calculates an overall security score based on the audit results.

## Tools and Technologies Used

- Python: Programming language  
- subprocess: Executes system commands  
- os, stat, pwd, grp: File, user, and permission handling  
- sys, socket, re, datetime, json: System info, parsing, and report generation  
- Linux shell commands (awk, grep, ss, ufw, iptables): Security-related data collection

## Steps Involved

1. Initialization and system metadata collection  
2. User Account Security Audit  
3. File Permissions Audit  
4. Network Services and Port Monitoring  
5. Firewall Configuration Check (UFW or iptables)  
6. System Update Availability Check  
7. SSH Configuration Analysis  
8. Kernel Parameter Security Audit  
9. Report Generation and JSON Export

## Conclusion

This project provided practical experience in Linux system security auditing and advanced Python scripting. The tool effectively automates a wide range of important security checks and gives users immediate insight into their system’s posture. It serves as both a diagnostic utility and a learning platform for anyone interested in cybersecurity or Linux system administration.