Personal Firewall using Python - Project Report

Name: Chandana V

Date: 12-07-2025

Introduction

This project involves developing a personal firewall using Python. It enables real-time monitoring of network traffic and provides rule-based filtering capabilities. It also includes GUI functionality for log viewing and rule enforcement.

Abstract

The personal firewall is designed to sniff packets using Scapy, block traffic based on user-defined rules, and log suspicious activity. A Tkinter-based GUI allows real-time log viewing, exporting, and applying iptables rules. This project blends cybersecurity principles with Python development.

Tools Used

- Python 3
- Scapy
- iptables
- Tkinter
- JSON
- FPDF

Steps Involved in Building the Project

1. Built packet sniffer using Scapy.
2. Defined filtering rules for IPs, ports, and protocols.
3. Created logging system for suspicious packets.
4. Integrated iptables for system-level enforcement.
5. Developed GUI for live log viewing and rule management.
6. Added export to CSV feature.

Conclusion

This project showcases a functional personal firewall created using Python. It demonstrates network-level filtering, GUI development, and system integration using iptables. It serves as an excellent foundation for understanding cybersecurity fundamentals.

Screenshot (Firewall Logs):

```
2025-07-12 05:55:14.718056] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:14.925591] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:15.719520] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:15.759485] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:16.719905] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:16.818119] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:17.722712] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:17.825950] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:18.722035] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:18.786512] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:19.730098] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:19.834624] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:20.728865] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:20.744641] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:21.730558] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:21.745047] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:22.732077] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:22.830421] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:23.733561] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:23.789759] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:24.735859] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:24.743868] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:25.738002] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:25.747701] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:26.737483] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:26.747731] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:27.736247] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:27.741924] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:28.734405] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:28.741771] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:29.740987] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:29.753857] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:30.738622] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:30.757470] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:31.742099] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:31.755276] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:32.743030] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:32.765028] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:33.745616] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:33.758754] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:34.744238] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:34.777346] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:35.745842] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:35.764809] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:36.749510] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:36.758230] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:37.748703] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:37.755098] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
2025-07-12 05:55:38.751905] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.201.152 > 192.168.1.10 echo-request 0 / Raw
2025-07-12 05:55:38.761623] BLOCKED: ICMP Ping -> Ether / IP / ICMP 192.168.100.1 > 192.168.201.152 time-exceeded ttl-zero-during-transit / IPerror / ICMPerror
```