Personal Firewall using Python

Introduction

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predefined rules. In today's world of increasing cyberattacks, having a firewall is essential to protect systems from unauthorized access, malware, and network intrusions. This project aims to build a personal firewall using Python that can block IPs, ports, prefixes, and detect suspicious traffic patterns like ping floods.

Abstract

The Personal Firewall project demonstrates how Python can be used to create a basic yet effective firewall system. By integrating NetfilterQueue and Scapy, the firewall monitors packets in real-time and applies filtering rules defined by the user in a JSON configuration file.

The firewall can block:

- Specific IP addresses
- Network prefixes
- Ports (both TCP and UDP)
- Ping flood attacks (ICMP requests exceeding a threshold)

This project helps in understanding packet filtering, network security, and intrusion prevention at a practical level.

Tools Used

1. Python 3 – Programming language for implementation.
2. Scapy – For analyzing and handling packets.
3. NetfilterQueue – To interface Python with Linux's iptables for packet filtering.
4. iptables – For redirecting packets to the firewall queue.
5. JSON – To store and manage firewall rules (IP, port, thresholds).

Steps Involved in Building the Project

1. Define Rules in JSON File
- The user specifies banned IPs, ports, and prefixes in firewallrules.json.
- Example: Block IPs 192.168.43.181, Ports 80, 81, Prefix 172.

2. Packet Capturing and Filtering
- Using NetfilterQueue, packets are redirected from iptables to Python.
- Scapy parses each packet for source IP, ports, or ICMP requests.

3. Apply Filtering Logic
- If packet source matches a banned IP/port/prefix, it is dropped.
- ICMP flood detection: If too many ping requests are received in a short time, packets are blocked.

4. Integration with iptables
- Rule: iptables -I INPUT -j NFQUEUE --queue-num 1
- This ensures all incoming packets go to the Python firewall for filtering.

5. Execution
- Run the script: python3 fw.py
- Firewall runs continuously, monitoring and dropping packets based on rules.

Conclusion

The Personal Firewall using Python is a lightweight yet effective solution for learning and practicing network security concepts. It successfully demonstrates how to block malicious traffic, prevent flood attacks, and enforce custom firewall rules. Though not as advanced as enterprise firewalls, this project provides a strong foundation in packet filtering, intrusion detection, and system defense mechanisms.