🔐 Firewall Configuration & Testing Report

Task 10 – Cyber Security Internship

1. Aim of the Task

The aim of this task is to understand firewall concepts and to configure, test, and analyze firewall rules using **UFW (Uncomplicated Firewall)**. The task focuses on allowing and denying network traffic, testing connectivity, blocking malicious IP addresses, observing logs, and documenting the impact of firewall rules.

2. Tools Used

- **Operating System:** Kali Linux
- **Firewall Tool:** UFW (Uncomplicated Firewall)
- **Alternative (Not Used):** iptables

3. Firewall Overview

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. It acts as a barrier between a trusted internal network and untrusted external networks.

Firewalls help in:

- Preventing unauthorized access
- Reducing attack surface
- Controlling network communication
- Monitoring suspicious activities

4. Firewall Configuration Steps

4.1 Checking Firewall Status

Initially, the firewall status was checked to verify whether UFW was active or inactive.

- Command used:
  sudo ufw status

The firewall was found to be inactive.

4.2 Enabling the Firewall

The UFW firewall was enabled to start filtering network traffic.

- Command used:
  sudo ufw enable

After enabling, the firewall status was verified.

- Command used:
  sudo ufw status verbose

The firewall was successfully activated with default policies set to deny incoming traffic and allow outgoing traffic.

4.3 Allowing Required Ports

To ensure normal system functionality, essential ports were allowed.

- SSH (Port 22) – Remote access
- HTTP (Port 80) – Web traffic
- HTTPS (Port 443) – Secure web traffic

These rules allow only trusted services while keeping other ports blocked.

4.4 Blocking Unused / Risky Ports

An unused and insecure port (Telnet – Port 23) was blocked to prevent potential attacks.

Blocking unused ports helps reduce vulnerabilities and prevents unauthorized access.

4.5 Testing Connectivity

Connectivity tests were performed to verify firewall behavior:

- Blocked ports failed to establish a connection
- Allowed ports successfully established a connection

This confirmed that the firewall rules were working as expected.

4.6 Enabling and Observing Firewall Logs

Firewall logging was enabled to monitor blocked and allowed traffic.

- Logs were checked to observe blocked connection attempts
- Suspicious activities were recorded in firewall logs

Firewall logs help in identifying attack attempts and monitoring network behavior.

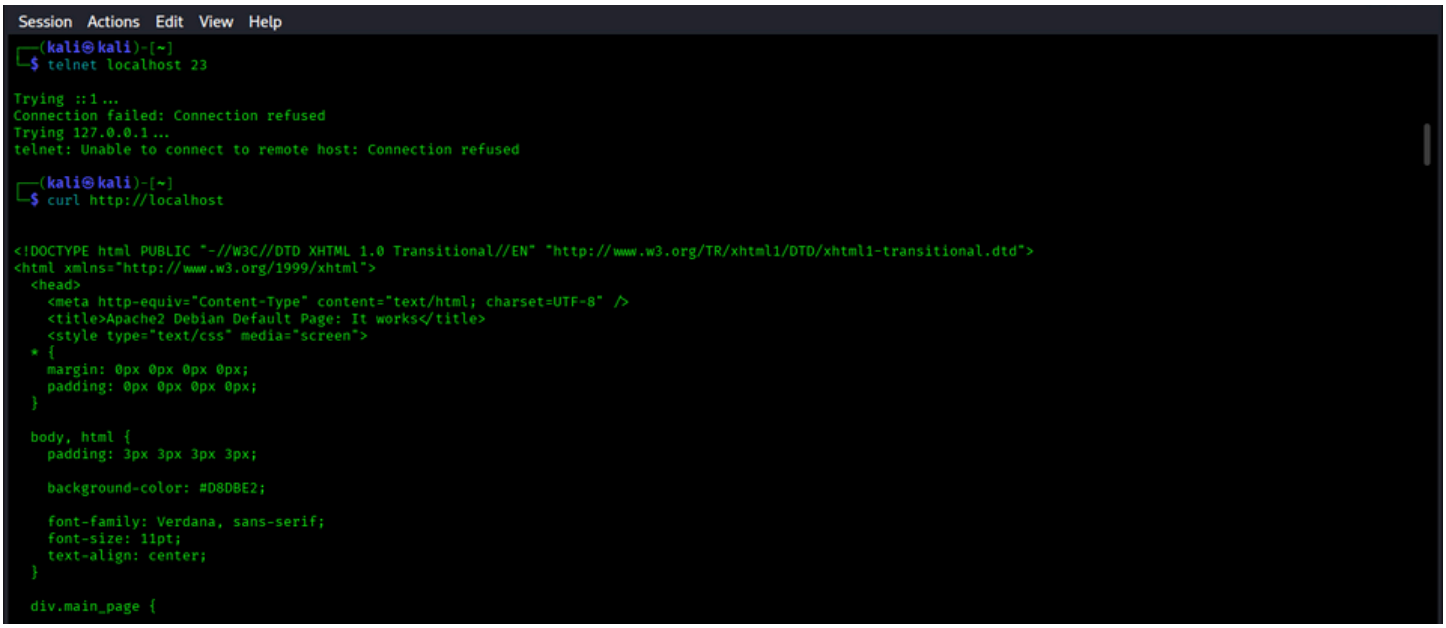
4.7 Blocking a Malicious IP Address

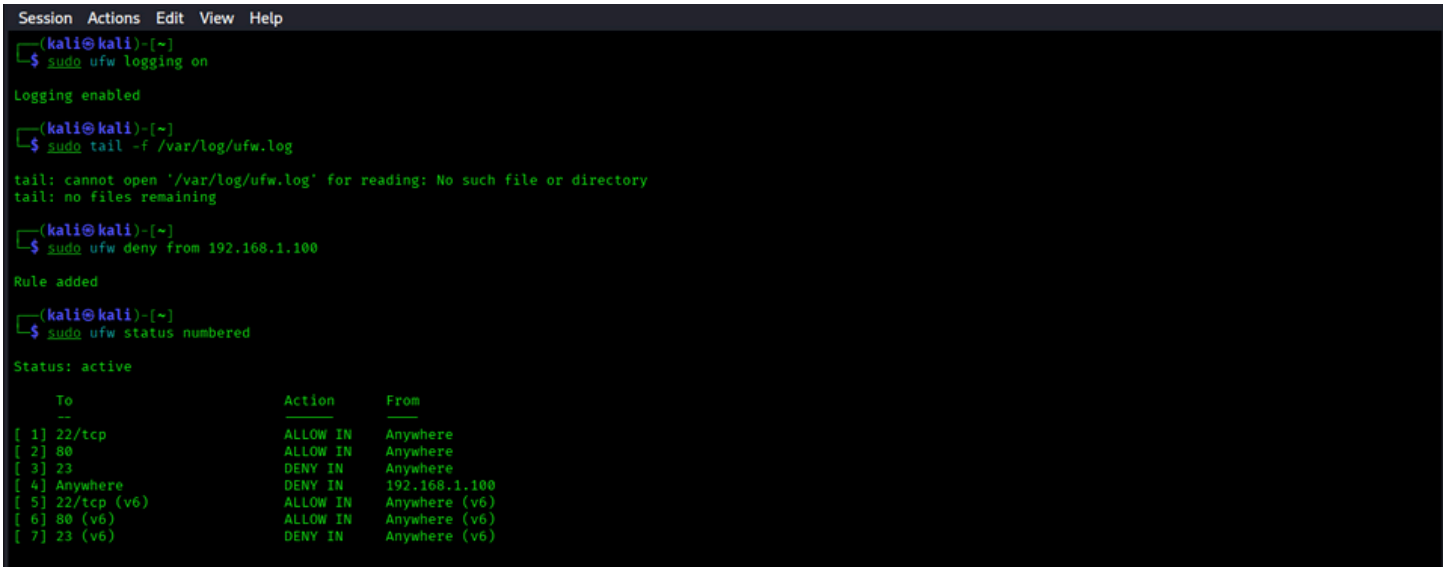
A suspicious IP address was manually blocked using firewall rules.

Blocking malicious IP addresses helps prevent attacks such as brute force attempts, scanning, and unauthorized access.

5. Firewall Rules Summary

Rule Type	Description
Allowed Ports	22 (SSH), 80 (HTTP), 443 (HTTPS)
Blocked Ports	23 (Telnet)
Blocked IP	192.168.1.100
Logging	Enabled
Default Policy	Deny incoming, Allow outgoing





6. Impact of Firewall Configuration

- Unauthorized network access was blocked
- Only essential services were allowed
- Attack surface was reduced
- Malicious traffic was denied
- Network activity could be monitored through logs
- Overall system security was improved

7. Conclusion

This task provided hands-on experience in configuring and managing firewall rules using UFW. It improved understanding of network security, traffic filtering, logging, and real-world firewall management practices.