****

**ELEVATE LABS  
Cyber Security Internship**

**Task 4  
Documentation Report  
Submitted by Suhaila P.S**

**Lab Report: Firewall Configuration with UFW on Linux**

**Name:** Suhaila P.S  
**Date:** 30-05-2025  
**Objective:** Configure and test basic firewall rules using UFW to allow/block network traffic.

**1. Introduction**

A firewall filters network traffic based on predefined rules. This lab uses **UFW (Uncomplicated Firewall)** on Linux to:

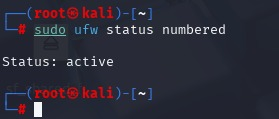
* Block inbound traffic on port 23 (Telnet).
* Allow inbound traffic on port 22 (SSH).
* Test and document the rules.

**2. Steps & Screenshots**

**Step 1: Check UFW Status**

**Command:**

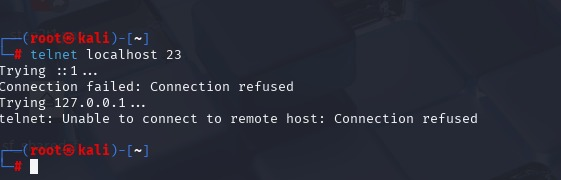
sudo ufw status

**Purpose:** Verify if UFW is active.  
**Screenshot:**  


**Step 2: Block Telnet (Port 23)**

**Command:**

sudo ufw deny 23/tcp

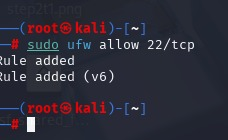
**Purpose:** Block inbound Telnet traffic.  
**Screenshot:**  


**Step 3: Allow SSH (Port 22)**

**Command:**

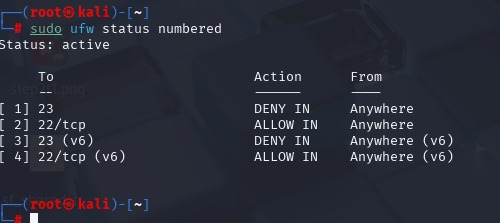
sudo ufw allow 22/tcp

**Purpose:** Ensure SSH remains accessible.  
**Screenshot:**



**Step 4: Verify Rules**

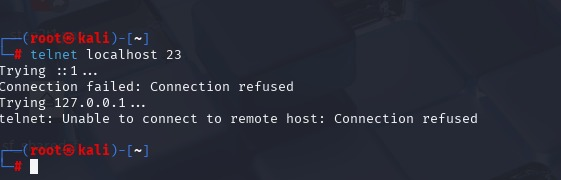
**Command:**

sudo ufw status numbered  
  
**Screenshot:**

**Step 5: Test Telnet Block**

**Command:**

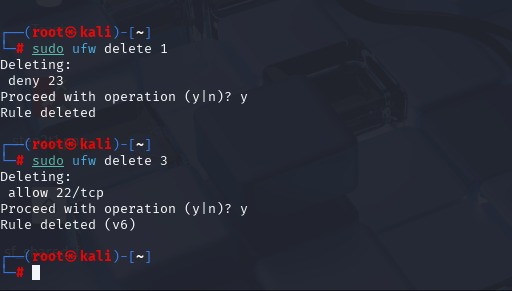
telnet localhost 23

**Screenshot:**  


**Step 6: Remove Telnet Block Rule**

**Command:**

sudo ufw delete [rule-number]  
**Purpose:** Clean up test rules.  
**Screenshot:**

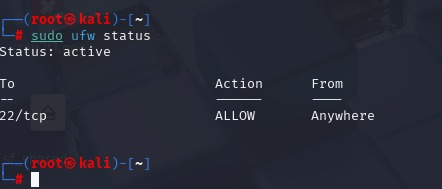


**Step 7: Final Rules**

**Command:**

sudo ufw status

**Screenshot:**



**3. Conclusion**

Successfully configured UFW to block unwanted traffic (Telnet) while permitting critical services (SSH). Documented all steps with commands and screenshots.

**Submitted by:** Suhaila P.S  
**Lab Completed on:** 30-05-2025