**Task 4 – Linux Firewall Setup & Testing (UFW)**

**# Objective**

**Configure and test basic firewall rules on Linux using UFW (Uncomplicated Firewall) to allow or block network traffic.**

**# Check if UFW is Installed**

**Bash :-**

**sudo ufw status**

**If UFW is not installed:**

**sudo apt update**

**sudo apt install ufw**

**# Screenshot → Shows if UFW is installed.**

**# Check Current Status and Rules**

**sudo ufw status verbose**

**Screenshot → Shows current rules and whether UFW is active.**

**# Enable UFW (if not enabled)**

**# Important: Allow SSH before enabling if working remotely.**

**sudo ufw allow 22/tcp**

**sudo ufw enable**

**# Screenshot → Shows UFW enabled.**

**# Block Inbound Traffic on Port 23 (Telnet)**

**sudo ufw deny 23/tcp**

**# Screenshot → Check with:**

**sudo ufw status numbered**

**# Test the Block Rule**

**Install Telnet (if not installed):**

**sudo apt install telnet**

**Try connecting to Port 23:**

**telnet localhost 23**

**Connection should fail.  
# Screenshot → Shows failed connection.**

**# Allow SSH (Port 22)**

**(If not already done)**

**sudo ufw allow 22/tcp**

**# Screenshot → Updated rules list.**

**# Remove the Test Block Rule**

**sudo ufw delete deny 23/tcp**

**# Screenshot → Confirm removal with:**

**sudo ufw status numbered**

**# Summary**

**UFW is a simple frontend for iptables, allowing administrators to manage firewall rules easily. In this task, we:**

* **Listed existing firewall rules.**
* **Added a rule to block Telnet (port 23).**
* **Verified the block with a test connection.**
* **Allowed SSH (port 22) for remote management.**
* **Removed the test block to restore the firewall to its original state.**

**# Required Screenshots:**

1. **Initial firewall status and rules.**
2. **Rule added to block port 23.**
3. **Failed Telnet connection attempt.**
4. **SSH allow rule.**
5. **Rule removal confirmation.**