🛡️ Task 4 — Setup and Use a Firewall on Linux (UFW)

Author: Yuvraj Yadav
Date: 28-10-2025
Scanner Machine: Ubuntu 22.04 LTS / Kali Linux
Tool Used: Uncomplicated Firewall (UFW)

1 Objective

The objective of this task was to **configure and test a basic firewall** on a Linux system using **UFW** (Uncomplicated Firewall).
The goal was to demonstrate how inbound and outbound network traffic can be filtered by applying simple rules — such as **blocking insecure ports (Telnet 23)** and **allowing trusted connections (SSH 22)** — and to understand how UFW implements stateful packet inspection for host protection.

2 Tools and Environment Setup

Operating System: Ubuntu 22.04 LTS / Kali Linux
Firewall Tool: UFW (v0.36 or higher)
Testing Utility: Netcat (nc)

Installation Steps:

```
sudo apt update
sudo apt install ufw -y
```

Network Setup:

- System connected to a secure LAN / Wi-Fi network
- IP Address: 127.0.0.1 (localhost for testing)
- All testing done locally to avoid remote interference

3 Steps Performed

Step 1 – Check Firewall Status

Verified UFW installation and status:

sudo ufw status

Output: `Status: inactive`

Step 2 – Enable Firewall and Set Default Policies

Configured UFW with secure default behavior:

sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw enable

Result: Firewall activated and enabled at boot.

Step 3 – Block Telnet (Port 23)

Telnet transmits credentials in plaintext and is insecure; it was blocked:

sudo ufw deny 23

Verification:

sudo ufw status numbered

Rule #1: `Deny 23/tcp`

Step 4 – Allow SSH (Port 22)

SSH is required for secure remote access:

sudo ufw allow 22

Verification: Rule #2: `Allow 22/tcp`

Step 5 – Testing Rules with Netcat

Used Netcat to simulate connections and verify behavior:

```
nc -zv 127.0.0.1 23   # should fail (blocked)
nc -zv 127.0.0.1 22   # should succeed (allowed)
```

Output:

- Port 23 → *Connection refused*
- Port 22 → *Connection succeeded*

Step 6 – View and Manage Rules

Displayed current active rules:

```
sudo ufw status verbose
```

```
Status: active
Default: deny (incoming), allow (outgoing)

To      Action   From
--      ------   ----
22/tcp  ALLOW    Anywhere
23/tcp  DENY     Anywhere
```

Step 7 – Reset Firewall After Testing

Restored UFW to default settings:

```
sudo ufw reset
```

Output: All rules removed; defaults restored.

4 Firewall Rules Summary

Rule ID	Action	Port / Service	Protocol	Purpose	Status
1	DENY	23	TCP	Block Telnet (insecure traffic)	Active
2	ALLOW	22	TCP	Allow SSH (secure access)	Active

5 Firewall Behavior Verification

Test Case	Expected Outcome	Result
Telnet connection (port 23)	Blocked by a firewall	Passed
SSH connection (port 22)	Allowed by the firewall	Passed
HTTP (port 80)	Allowed outgoing traffic	Passed

6 Analysis and Learnings

- Firewalls are essential for **restricting unauthorized access** and monitoring traffic.
- UFW simplifies `iptables` management with intuitive commands.
- The default policy (`deny incoming`, `allow outgoing`) is a secure baseline for most hosts.
- **Blocking insecure ports** like Telnet and FTP reduces the attack surface.
- The exercise demonstrated how UFW uses **stateful packet inspection** to track connection states.
- Learned to test rules using tools like `nc` (Netcat) for accurate validation.

7 Outcome

The task was successfully completed. All firewall rules worked as intended — Telnet traffic was blocked and SSH was allowed.
This ensured a secure host configuration aligned with network security best practices.

Key Skills Gained:

- Linux firewall administration
- Traffic filtering and rule management
- Understanding stateful/stateless inspection
- Testing and verification of firewall policies
- System hardening through rule optimization

8 Attachments (for GitHub Repo)

1. **Screenshots Folder** – contains:
   `01_ufw_status.png`, `02_ufw_enable.png`, `03_ufw_rules.png`, `04_telnet_block.png`, `05_ssh_allow.png`
2. **firewall_rules.txt** – export of current UFW rules
3. **report.md** – this detailed documentation
4. **README.md** – concise summary and commands overview