Elevate Labs - Cybersecurity Internship: Task 4 Report

Task Objective

The objective of this task was to learn. This repository documents the completion of Task 4: Setup and Use a Firewall on Linux.

Tools Used

UFW (Uncomplicated Firewall).

2. Firewall Configuration Steps

- Provide a numbered list of the commands you used, along with a short explanation of what each one does.
    - sudo ufw status verbose: Check the firewall's status.

```
sujan-gowda@ubuntu2025:~$ sudo ufw status verbose
[sudo] password for sujan-gowda:
Status: inactive
```

    - sudo ufw allow ssh: Ensure you don't lose remote access.

```
sujan-gowda@ubuntu2025:~$ sudo ufw allow ssh
sudo ufw enable
Rules updated
Rules updated (v6)
Firewall is active and enabled on system startup
```

    - sudo ufw deny 23: Block the specified port (Telnet).

```
sujan-gowda@ubuntu2025:~$ telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```

    - sudo ufw status: Verify that the new rule is active.

```
sujan-gowda@ubuntu2025:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
23                         DENY        Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
23 (v6)                    DENY        Anywhere (v6)
```

    - sudo ufw delete deny 23: Remove the temporary rule.

```
sujan-gowda@ubuntu2025:~$ sudo ufw delete deny 23/tcp
Could not delete non-existent rule
Could not delete non-existent rule (v6)
```

3. Summary of Firewall Concepts

- **What is a Firewall?** A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet.
- **Inbound vs. Outbound Rules: Inbound rules** control traffic coming into your system from the outside. **Outbound rules** control traffic leaving your system to the outside.
- **Why Block Telnet (Port 23)?** Telnet is an old protocol that sends data, including passwords, in plain text. This makes it highly vulnerable to eavesdropping and is a significant security risk. Blocking it is a basic but essential security practice.
- **How UFW Simplifies Firewall Management:** UFW provides a simplified, user-friendly interface for managing iptables, the complex underlying firewall system in Linux. It abstracts away the complex syntax, making it easier for users to create and manage rules.