Firewall Configuration Report

Eleyate Cyber Security Internship - Task 4

Prepared by: Sujay Vegi

Date: May 30, 2025

1. Introduction

This report summarizes the setup and basic usage of a firewall on a Linux system as part of Task 4 for the Eleyate Cyber Security Internship. The task involved configuring firewall rules using UFW to block and allow specific ports, enhancing the understanding of network traffic filtering and firewall management.

2. Methodology

The firewall setup process involved the following steps:

1. Tool Used: UFW (Uncomplicated Firewall) was installed and enabled.

2. Listing Rules: Existing rules were listed using `sudo ufw status verbose`.

3. Blocking Port 23: A rule was added to block inbound traffic on Telnet port using `sudo ufw deny 23`.

4. Testing: Connection to port 23 was attempted and confirmed blocked.

5. Allowing SSH: Ensured SSH access by running `sudo ufw allow 22`.

6. Cleanup: The block rule for port 23 was removed using `sudo ufw delete deny 23`.

7. Rules were documented and screenshots were captured for verification.

3. Firewall Rules

- Blocked Port: 23 (Telnet)

- Allowed Port: 22 (SSH)

- Default Policy: Deny incoming, allow outgoing

- UFW Status: Active and configured with custom rules

4. Commands Used

- sudo ufw status verbose

- sudo ufw deny 23

- sudo ufw allow 22

- sudo ufw delete deny 23

- sudo ufw enable

- sudo ufw reload

5. Recommendations

- Keep firewall enabled by default.

- Regularly review and audit firewall rules.

- Block unused and insecure ports like Telnet (23).

- Use SSH keys for secure remote access instead of passwords.

- Monitor firewall logs for unusual traffic patterns.

6. Conclusion

This exercise provided practical experience in configuring and managing a basic firewall using UFW. It emphasized the importance of filtering inbound traffic, securing services like SSH, and blocking risky ports such as Telnet to enhance overall system security.