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 using UFW.

2. Methodology

Steps included enabling UFW, blocking port 23, allowing port 22, and testing rules.

3. Interview Questions and Answers

1. What is a firewall?

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

2. Difference between stateful and stateless firewall?

Stateful firewalls track the state of active connections and make decisions based on context, while stateless firewalls make decisions based solely on predefined rules.

3. What are inbound and outbound rules?

Inbound rules control traffic coming into the device, while outbound rules control traffic going out from the device.

4. How does UFW simplify firewall management?

UFW provides a user-friendly command-line interface for managing iptables, making it easier to configure basic firewall rules without deep networking knowledge.

5. Why block port 23 (Telnet)?

Port 23 is used by Telnet, which transmits data in plaintext and is considered insecure. Blocking it reduces the attack surface.

6. What are common firewall mistakes?

Common mistakes include leaving unnecessary ports open, using weak rules, forgetting to save changes, and not monitoring traffic.

7. How does a firewall improve network security?

Firewalls prevent unauthorized access, reduce the risk of attacks, and help enforce security policies by controlling traffic flow.

8. What is NAT in firewalls?

NAT (Network Address Translation) allows multiple devices on a local network to share a single public IP address, improving security by masking internal IPs.