Cyber Security Internship Report

Task 4: Setup and Use a Firewall on Windows/Linux

1. Introduction

This report documents the configuration and testing of basic firewall rules on a Linux system using UFW (Uncomplicated Firewall). The objective is to understand and apply traffic filtering rules to enhance system security.

2. Objective

Configure and test basic firewall rules to allow or block traffic on a Linux system using UFW.

3. Tools Used

- Operating System: Ubuntu 22.04 LTS
- Firewall: UFW (Uncomplicated Firewall)
- Terminal Shell

4. Procedure and Commands

- Step 1: Open Terminal and check if UFW is installed:
  ```
  $ sudo ufw status
  ```
  Output: Status: inactive
- Step 2: Enable the firewall:
  ```
  $ sudo ufw enable
  ```
  Output: Firewall is active and enabled on system startup
- Step 3: List current firewall rules:
  ```
  $ sudo ufw status numbered
  ```
  Output: (No rules yet if fresh installation)
- Step 4: Add rule to block inbound traffic on port 23 (Telnet):
  ```
  $ sudo ufw deny 23
  ```
  Output: Rule added
- Step 5: Attempt to connect to port 23 (simulated)
  ```
  $ telnet localhost 23
  ```
  Output: Connection refused (indicates rule is working)
- Step 6: Add rule to allow SSH (port 22):
  ```
  $ sudo ufw allow 22
  ```
  Output: Rule added
- Step 7: Remove the test block rule on port 23:
  ```
  $ sudo ufw delete deny 23
  ```
  Output: Rule deleted
- Step 8: List current rules again:
  ```
  $ sudo ufw status
  ```

Output:

```
22 ALLOW Anywhere
22 (v6) ALLOW Anywhere (v6)
```

5. Documentation of Results

The firewall rules were successfully configured and tested. Port 23 traffic was blocked as expected, and SSH access (port 22) was allowed. All commands were executed via the Linux terminal. A simulated connection attempt to the blocked port verified that the rule worked as intended.

6. Summary

This task demonstrated basic skills in managing firewall rules using UFW on a Linux system. The ability to control network traffic through specific port access is a fundamental component of cybersecurity and network defense strategies.

7. Outcome

Successfully configured UFW to block and allow specific ports, validated the effectiveness of rules, and restored firewall state after testing.