CYBER SECURITY INTERNSHIP

Task 4: Firewall Configuration using UFW on Kali Linux

Prepared By: Oleti Chandini

Date: 08-08-2025

Objective

The objective of this task is to configure and manage basic firewall rules on a Linux-based system using the Uncomplicated Firewall (UFW). The task helps build practical knowledge of network traffic filtering, port management, and Linux-based system hardening.

Introduction

Firewalls play a crucial role in securing systems by filtering network traffic based on rules. In this task, the Uncomplicated Firewall (UFW), a user-friendly command-line interface for managing iptables in Linux, was used to configure basic allow and deny rules on Kali Linux. The goal was to block a vulnerable port (Telnet) and ensure secure ports like SSH are allowed.

Tools and Environment

Tool Used: UFW (Uncomplicated Firewall)
OS: Kali Linux
Port Blocked: 23 (Telnet)
Port Allowed: 22 (SSH)
Test Tool: Telnet

Steps Followed (Clear and Detailed)

Step 1: Update System Repositories.

```
sudo apt update
```

Step 2: Install UFW (Uncomplicated Firewall)
   sudo apt install ufw -y

Step 3: Enable UFW
   sudo ufw enable

Firewall is active and enabled on system startup
Step 4: Check Firewall Status
   sudo ufw status numbered

Step 5: Block Inbound Traffic on Port 23 (Telnet)
   sudo ufw deny 23

Step 6: Allow Inbound SSH (Port 22)

sudo ufw allow 22


```
┌──(root㉿kali)-[~]
└─# sudo ufw allow 22

Rule added
Rule added (v6)
```

Step 7: Install Telnet for Testing

sudo apt install telnet -y


```
┌──(root㉿kali)-[~]
└─# sudo apt install telnet -y
telnet localhost 23

Upgrading:
  inetutils-telnet

Installing:
  telnet

Summary:
  Upgrading: 1, Installing: 1, Removing: 0, Not Upgrading: 2158
  Download size: 174 kB
  Space needed: 73.7 kB / 59.9 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 inetutils-telnet amd64 2:2.6-3 [130 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 telnet all 0.17+2.6-3 [43.3 kB]
Fetched 174 kB in 2s (89.1 kB/s)
(Reading database ... 395936 files and directories currently installed.)
Preparing to unpack .../inetutils-telnet_2%3a2.6-3_amd64.deb ...
Unpacking inetutils-telnet (2:2.6-3) over (2:2.5-5) ...
Selecting previously unselected package telnet.
Preparing to unpack .../telnet_0.17+2.6-3_all.deb ...
Unpacking telnet (0.17+2.6-3) ...
Setting up inetutils-telnet (2:2.6-3) ...
Setting up telnet (0.17+2.6-3) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for man-db (2.12.1-2) ...
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```

Step 8: Remove the Test Rule (Cleanup)

sudo ufw delete deny 23


```
┌──(root㉿kali)-[~]
└─# sudo ufw delete deny 23

Rule deleted
Rule deleted (v6)
```

Rule deleted and Rule deleted (v6)

Step 9: Final Status Check

sudo ufw status numbered


```
┌──(root㉿kali)-[~]
└─# sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    Anywhere
[ 2] 22 (v6)                    ALLOW IN    Anywhere (v6)

┌──(root㉿kali)-[~]
```

Test Output Summary

After blocking port 23, the system was tested using telnet. The result showed 'connection refused', confirming that the firewall rule was working. The SSH port (22) remained accessible, ensuring remote management was still possible.

Learning Outcomes

- Learned to install and use UFW on a Linux system.
- Understood how to apply, list, and delete firewall rules.
- Identified the importance of blocking insecure ports like Telnet.
- Gained confidence in using command-line tools for system hardening.

Conclusion

This task provided practical experience with Linux-based firewall management. By configuring and testing rules using UFW, I gained a deeper understanding of how network ports can be controlled to protect systems from unauthorized access. This skill is essential for cybersecurity professionals in both offensive and defensive roles.