Task 4 Report: Firewall Configuration and Testing on Kali Linux

---

Objective:

To configure and test basic firewall rules using UFW (Uncomplicated Firewall) on Kali Linux. The goal is to learn how to manage and test firewall rules for allowing or blocking network traffic on specific ports.

Tools Used:

Kali Linux

UFW (Uncomplicated Firewall)

Terminal

Steps Performed:

1. Install UFW:

sudo apt install ufw

UFW package was successfully installed.

Screenshot: UFW installation output.

2. Enable the Firewall:

sudo ufw enable

Output confirmed: "Firewall is active and enabled on system startup."

3. Check Firewall Status and Existing Rules:

sudo ufw status numbered

Verified firewall is active and displayed any pre-existing rules.

4. Block Telnet (Port 23):

sudo ufw deny 23

This rule was added to block inbound traffic on Telnet port.

5. Test Telnet Access:

telnet localhost 23

The output showed "Connection refused", confirming the port was successfully blocked.

6. Allow SSH (Port 22):

sudo ufw allow 22

This rule allowed incoming SSH connections, essential for secure remote access.

7. Remove the Telnet Block Rule:

sudo ufw delete deny 23

This removed the block rule on port 23, cleaning up the configuration.

Screenshots Attached:

UFW installation and activation

UFW rule addition and deletion

Telnet test result

Conclusion:

This task demonstrated fundamental firewall management on a Linux system using UFW. By applying rules to block and allow specific ports and testing their behavior using tools like Telnet, we gained practical experience in controlling network access. This enhances both system security and administrative control.