Objective

The purpose of this exercise is to demonstrate the configuration and verification of firewall rules using **UFW (Uncomplicated Firewall)** on a Kali Linux system. The tasks include installing UFW, managing inbound traffic rules, testing rule enforcement, and understanding how firewalls filter network traffic.

Environment

* **Operating System**: Kali Linux (APT-based)
* **Firewall Tool**: UFW (Uncomplicated Firewall)
* **Terminal Access**: Root privileges

Procedure

1.Installing the Firewall Tool

UFW was not pre-installed on the system. The following command was executed to install it along with necessary dependencies:

sudo apt install ufw

Dependencies such as iptables and libip6tc2 were automatically installed. Post-installation, UFW was successfully configured.

2. Enabling the Firewall

To activate UFW and ensure it starts on system boot:

sudo ufw enable

Output confirmed:  
Firewall is active and enabled on system startup

3. Listing Current Firewall Rules

To view existing rules in a numbered format:

sudo ufw status numbered

This format facilitates rule management (e.g., deletion by index).

4. Blocking Inbound Traffic on Port 23 (Telnet)

To deny incoming Telnet traffic:

sudo ufw deny in 23/tcp

This added rules for both IPv4 and IPv6. Verification:

sudo ufw status verbose

Confirmed that port 23 was blocked.

5. Testing the Telnet Block

Telnet was not initially available. It was installed using:

sudo apt install telnet

Connection attempt:

telnet 127.0.0.1 23

Result:  
Unable to connect to remote host: Connection refused  
This confirmed that the firewall rule was effective.

6. Allowing SSH Access (Port 22)

To permit secure remote access via SSH:

sudo ufw allow 22/tcp

This ensured that port 22 was open for both IPv4 and IPv6.

7. Removing Test Rules

To restore the firewall to its original state, rules were deleted using their respective indices:

sudo ufw delete

Example:

sudo ufw delete 2 sudo ufw delete 4

Note: Rule indices shift after each deletion. It is recommended to re-run ufw status numbered before each delete operation.

8. Summary of Commands Used

sudo apt install ufw sudo ufw enable sudo ufw status sudo ufw status numbered sudo ufw deny in 23/tcp sudo apt install telnet telnet 127.0.0.1 23 sudo ufw allow 22/tcp sudo ufw delete

Conceptual Summary: How Firewalls Filter Traffic

A **firewall** is a security mechanism that monitors and controls incoming and outgoing network traffic based on predefined rules. It acts as a barrier between a trusted internal network and untrusted external networks.

* **Inbound Rules**: Control external traffic attempting to access the system.
* **Outbound Rules**: Control traffic leaving the system.
* **Filtering Criteria**:
* Port numbers (e.g., 22 for SSH, 23 for Telnet)
* Protocols (TCP/UDP)
* IP addresses (source/destination)

In this exercise:

* Port 23 was blocked to prevent insecure Telnet access.
* Port 22 was allowed to maintain secure SSH connectivity.
* Rules were tested and removed to validate firewall behavior.

If you'd like, I can help format this into a PDF or markdown document for submission. Let me know how you'd like to proceed.