**Objective**

To configure and test basic firewall rules on Kali Linux using UFW to allow or block specific network traffic.

**Tools**

* **Operating System:** Kali Linux
* **Firewall Tool:** UFW (Uncomplicated Firewall)

**Steps Performed**

**1. Check UFW Status**

sudo ufw status verbose

**2. Enable UFW**

sudo ufw enable

**3. Block Inbound Traffic on Port 23 (Telnet)**

sudo ufw deny 23*.*

**4. Test the Rule**

Try connecting with:

telnet localhost 23

Result: Connection should fail.

**5. Allow SSH on Port 22**

sudo ufw allow 22

**6. Remove the Test Block Rule**

sudo ufw delete deny 23

**7. Final Rule Listing**

sudo ufw status numbered

**Commands Used (Summary)**

sudo ufw status verbose

sudo ufw enable

sudo ufw deny 23

telnet localhost 23

sudo ufw allow 22

sudo ufw delete deny 23

sudo ufw status numbered

**Summary: How UFW Filters Traffic**

The firewall works as a traffic filter by applying rules to control network connections:

* **Allow Rules:** Let trusted traffic pass (e.g., SSH on port 22).
* **Deny Rules:** Block unwanted/unsafe services (e.g., Telnet on port 23).
* **Default Policy:** Deny all incoming, allow outgoing (can be changed).
* **Rule Priority:** Processed in the order defined.

Thus, UFW provides a simple but powerful way to secure the system against unauthorized access.

**Result:** Successfully configured UFW to block Telnet (port 23), tested blocking, allowed SSH (port 22), and restored firewall to its original state.