Configuring Firewall Rules in Kali Linux using UFW

Steps Performed

1. Install UFW

sudo apt update
sudo apt install ufw -y

2. Enable UFW

sudo ufw enable

3. Allow SSH (port 22)

sudo ufw allow 22/tcp

4. Block Telnet (port 23)

sudo ufw deny 23/tcp

5. Verify Current Rules

sudo ufw status verbose

Example Output:

Status: active

```
To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
23/tcp                     DENY        Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
23/tcp (v6)                DENY        Anywhere (v6)
```

Summary: How Firewall Filters Traffic

A firewall acts as a security barrier between a system and the network. It works by checking network packets against predefined rules. Rules are usually based on protocol (TCP, UDP, ICMP), port number (e.g., 22 for SSH, 23 for Telnet), and source/destination IP address.

In this task:

- The rule ALLOW 22/tcp permits incoming SSH traffic, so secure remote login works.
- The rule DENY 23/tcp blocks Telnet traffic, preventing insecure remote connections.

In short: firewalls decide whether to allow or block traffic based on rules, thus controlling access and enhancing security.