**Task 4 : Setup and Use a Firewall on Linux**

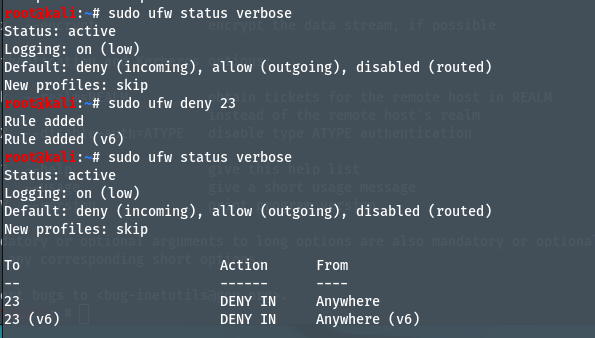
We will configure and test basic firewall rules to allow or block traffic using **UFW** on Linux.

**Steps Performed:**

1. **Open firewall configuration tool**

**UFW was active with default policies:**

* Incoming: Deny
* Outgoing: Allow
* No custom rules initially.

****

1. **List current firewall rules:**

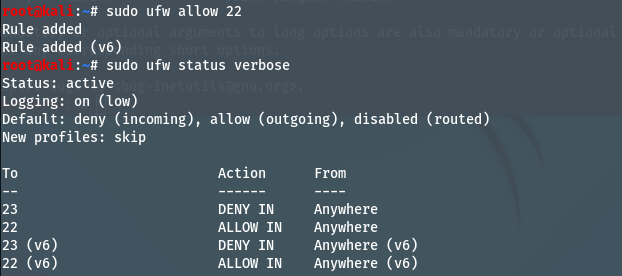
* sudo ufw status numbered

1. **Block inbound traffic on port 23 (Telnet)**

****

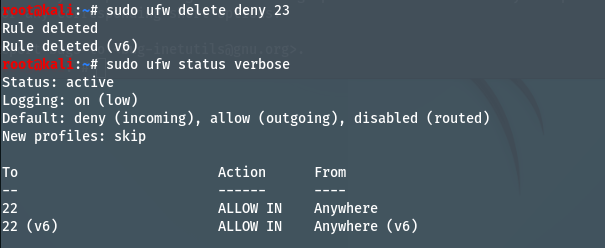
1. **Allow SSH (port 22):**

* sudo ufw allow 22

****

1. **Remove the test block rule:**

* sudo ufw delete deny 23

****

How Firewall Filters Traffic

* A firewall inspects network traffic and applies rules to allow or block based on ports, protocols, or IPs.
* In this task:
  + deny 23 → Blocked Telnet traffic.
  + allow 22 → Allowed SSH traffic.
* Traffic not explicitly matched by rules follows the default policy:
  + Deny incoming, allow outgoing.