**Linux UFW (Uncomplicated Firewall)**

**1. Open Firewall Configuration Tool**

* Open terminal.

**2. List Current Firewall Rules**

sudo ufw status numbered

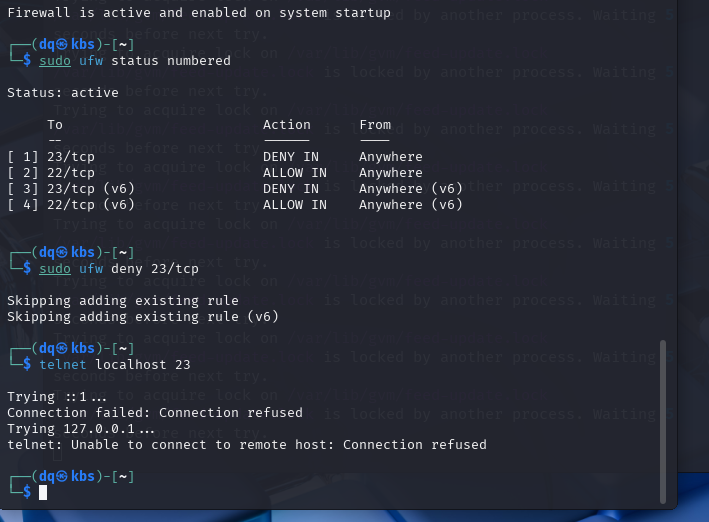
**3. Add Rule to Block Inbound Traffic on Port 23 (Telnet)**

sudo ufw deny 23/tcp

**4. Test the Rule**

telnet localhost 23

Connection should be refused.



**5. Add Rule to Allow SSH (Port 22)**

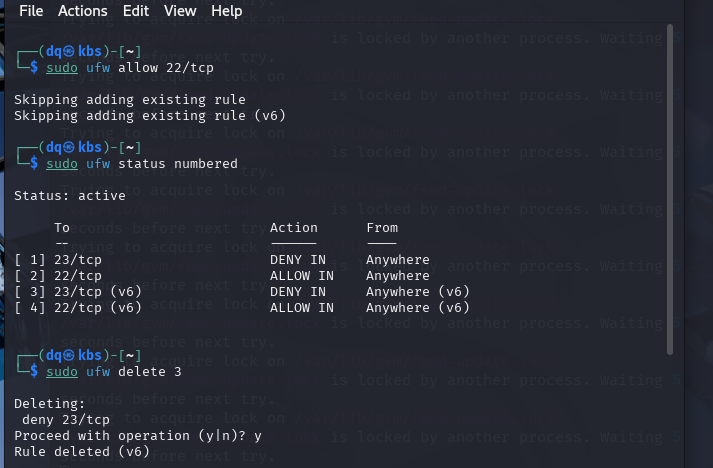
sudo ufw allow 22/tcp

**6. Remove the Test Block Rule**

* First check rule number:

sudo ufw status numbered

sudo ufw delete 3



**7. Documented Commands**

| Action | Command |
| --- | --- |
| List rules | sudo ufw status numbered |
| Block port 23 | sudo ufw deny 23/tcp |
| Test port 23 | telnet localhost 23 |
| Allow SSH (port 22) | sudo ufw allow 22/tcp |
| Remove block rule | sudo ufw delete <rule-num> |

**How Firewall Filters Traffic on Linux**

* When a network packet arrives at the Linux system, the firewall checks it first.
* The firewall has rules that say which packets to allow or block.
* Each rule looks at things like the packet’s source IP, destination IP, port number, and protocol.
* Linux firewalls organize rules in chains:
  + **INPUT** (for packets coming into the system)
  + **OUTPUT** (for packets going out)
  + **FORWARD** (for packets passing through the system)
* The firewall checks the rules one by one in the order they are written.
* If a packet matches a rule, the firewall does what the rule says (accept or block).
* If the packet doesn’t match any rule, the firewall uses a default action (usually block).
* Firewalls also track connection states, so return traffic for allowed connections is automatically accepted.
* Tools like **UFW** make managing these rules easier but work on the same principles.