Cyber Security Internship

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

**Objective:** Configure and test basic firewall rules to allow or block traffic.

**Tools:** Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

**Deliverables:** Screenshot/configuration file showing firewall rules applied.

**1.Open firewall configuration tool (Windows Firewall or terminal for UFW).**

──(kali㉿kali)-[~]

└─$ sudo apt install ufw -y

ufw is installed.

┌──(kali㉿kali)-[~]

└─$ sudo ufw enable

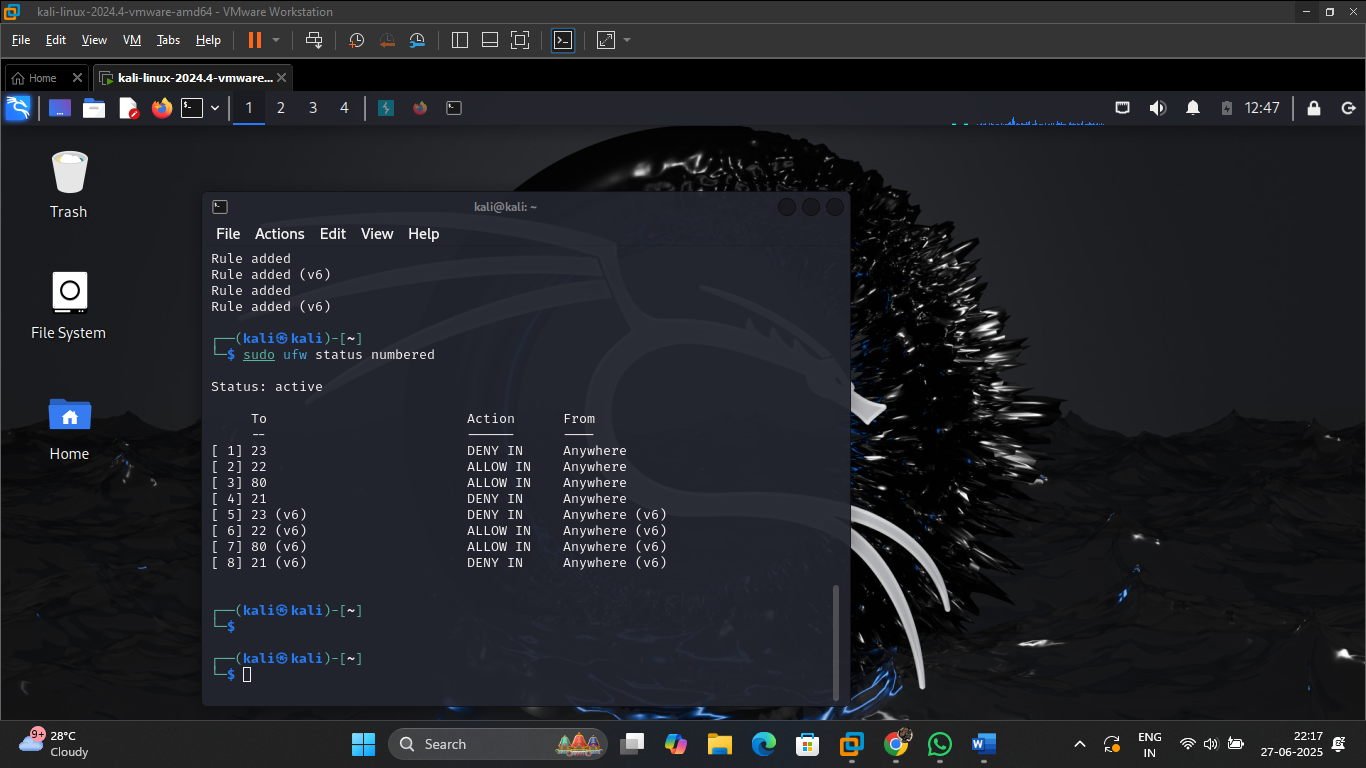
Firewall is active and enabled on system startup

┌──(kali㉿kali)-[~]

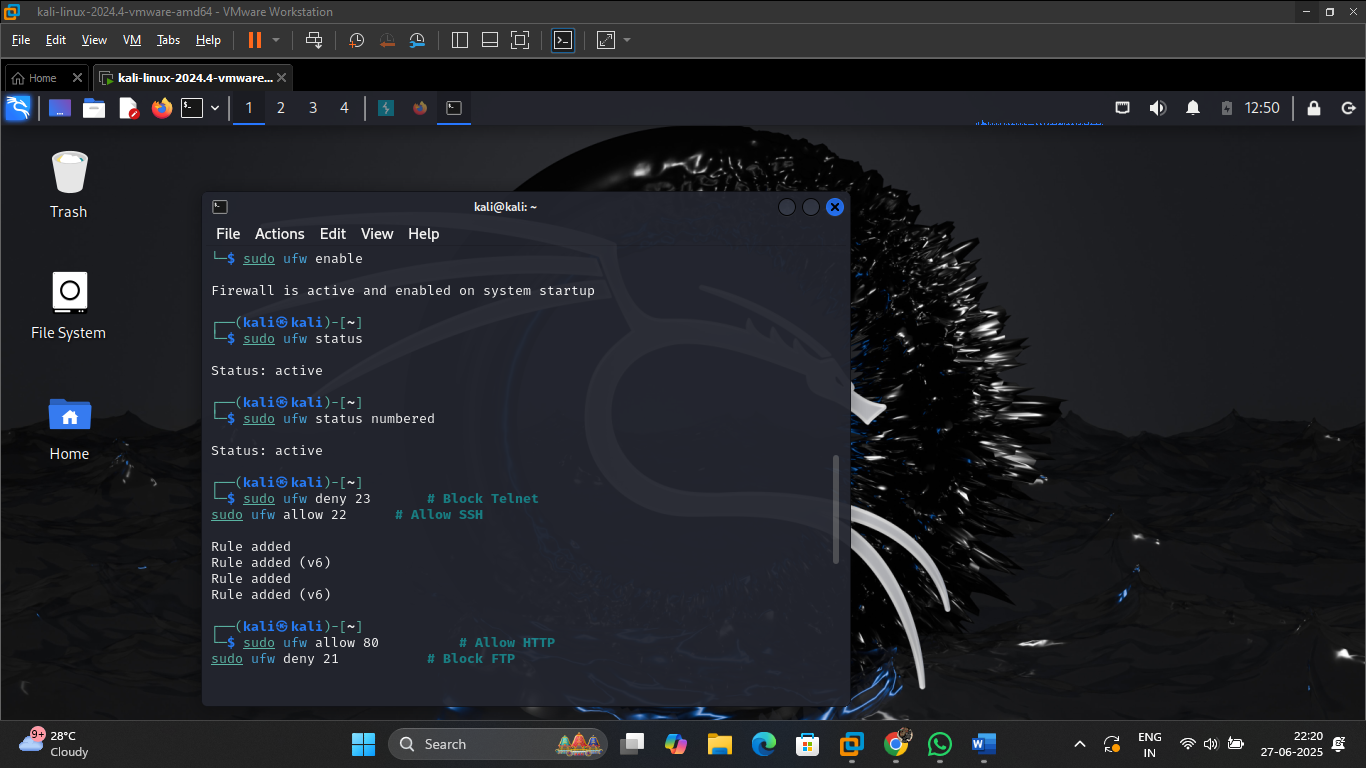
└─$ sudo ufw status

Status: active

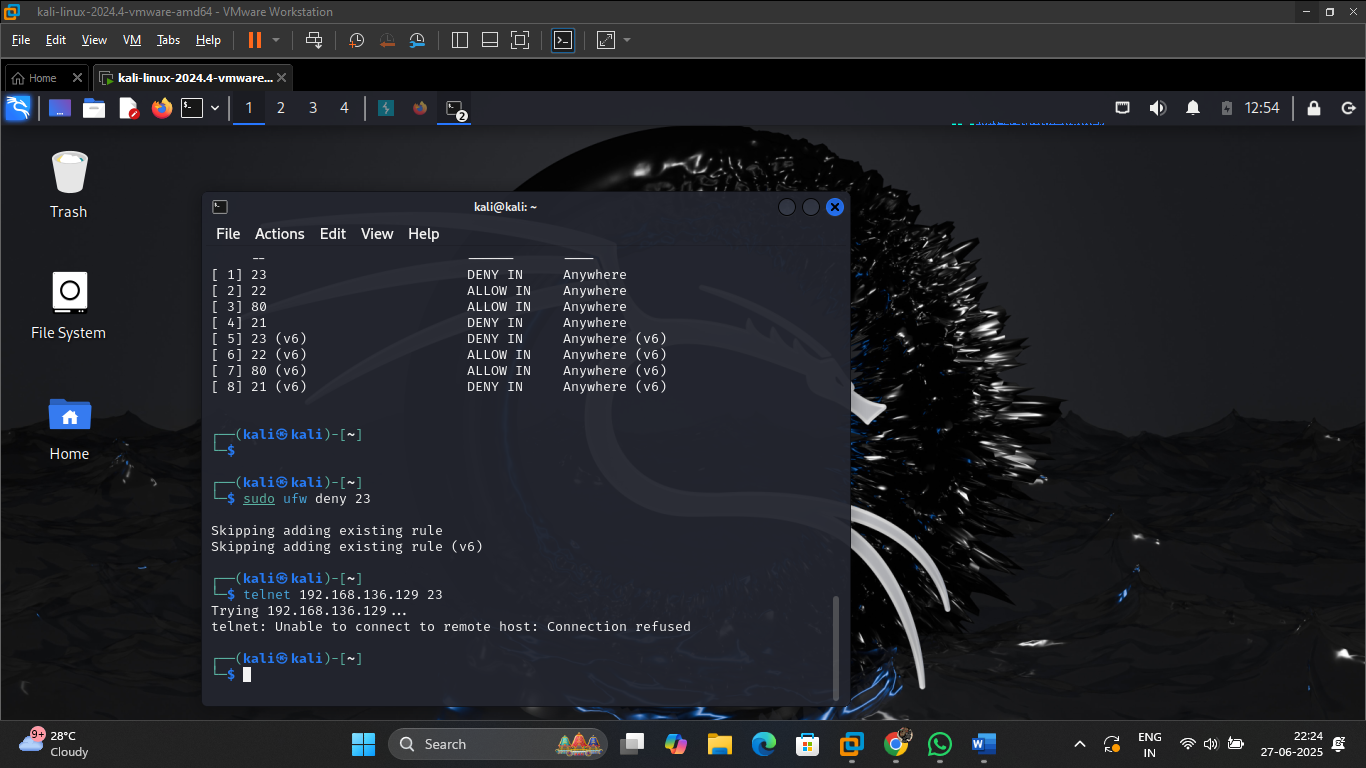
**2.List current firewall rules.**



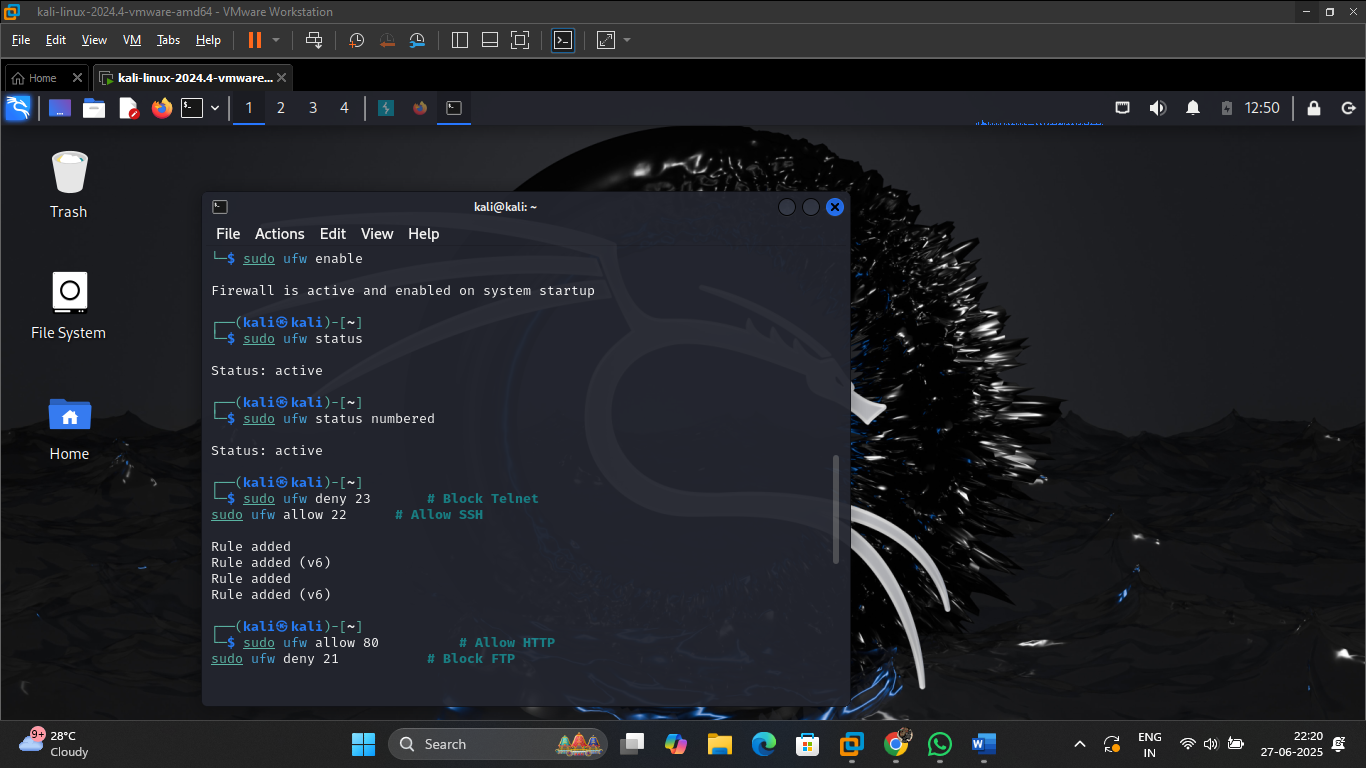
**3.Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet).**



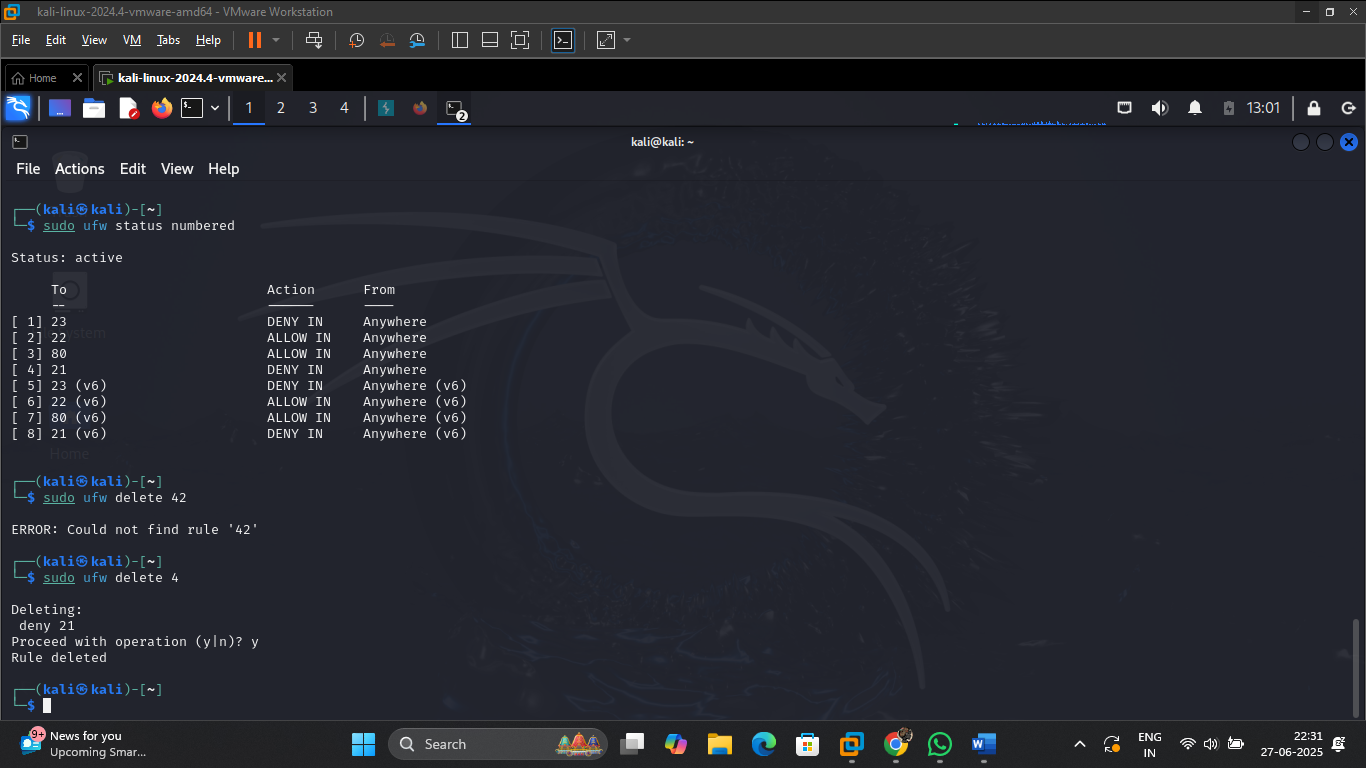
**4.Test the rule by attempting to connect to that port locally or remotely.**



**5.Add rule to allow SSH (port 22) if on Linux.**



**6.Remove the test block rule to restore original state.**



**7.Document commands or GUI steps used.**

| **Step** | **Command** |
| --- | --- |
| Enable firewall | sudo ufw enable |
| View rules | sudo ufw status numbered |
| Block port 23 | sudo ufw deny 23 |
| Allow SSH | sudo ufw allow 22 |
| Remove rule | sudo ufw delete <rule-number> |

**8.Summarize how firewall filters traffic.**

* A **firewall** monitors **incoming and outgoing traffic**.
* Based on **rules**, it **allows or blocks** data packets.
* It uses:
  + **Port numbers** (e.g., 22 for SSH, 80 for HTTP)
  + **IP addresses**
  + **Protocols (TCP/UDP)**

Firewalls protect systems from:

* **Unauthorized access**
* **Port scanning**
* **Unwanted services (e.g., Telnet, FTP)**