💧 Task 4: Firewall Configuration and Traffic Filtering

🎯 Objective

Configure a firewall on Kali Linux using **UFW (Uncomplicated Firewall)** to allow and block specific ports, simulate filtered traffic, and document firewall behavior.

🛠 Environment

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

🧪 Steps Performed

1. **Checked Initial Firewall Status**

   sudo ufw status verbose

2. **Enabled UFW**

   sudo ufw enable

3. **Allowed SSH on Port 22**

   sudo ufw allow 22

4. **Blocked Telnet on Port 23**

   sudo ufw deny 23

5. **Verified Active Rules**

   sudo ufw status numbered

6. **Deleted Deny Rule for Port 23**

   sudo ufw delete 2

7. **Re-added Deny Rule for Port 23**

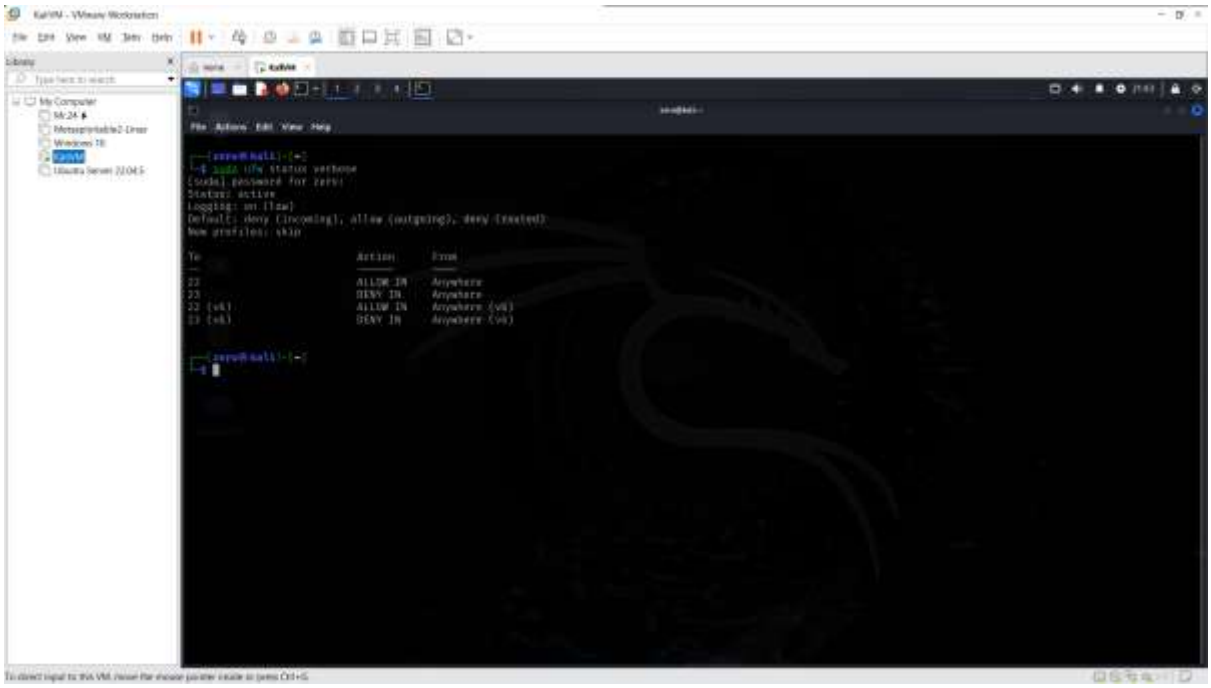
   sudo ufw deny 23

8. **Checked Final Status**

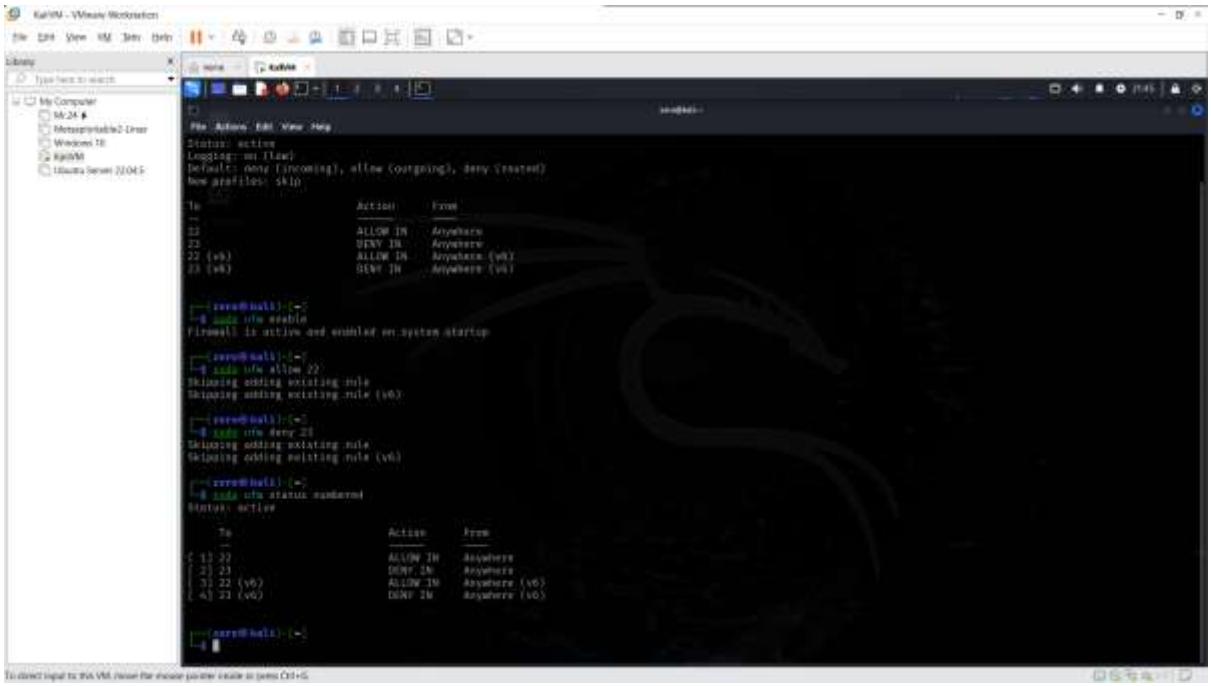
sudo ufw status numbered

📸 Screenshots Included

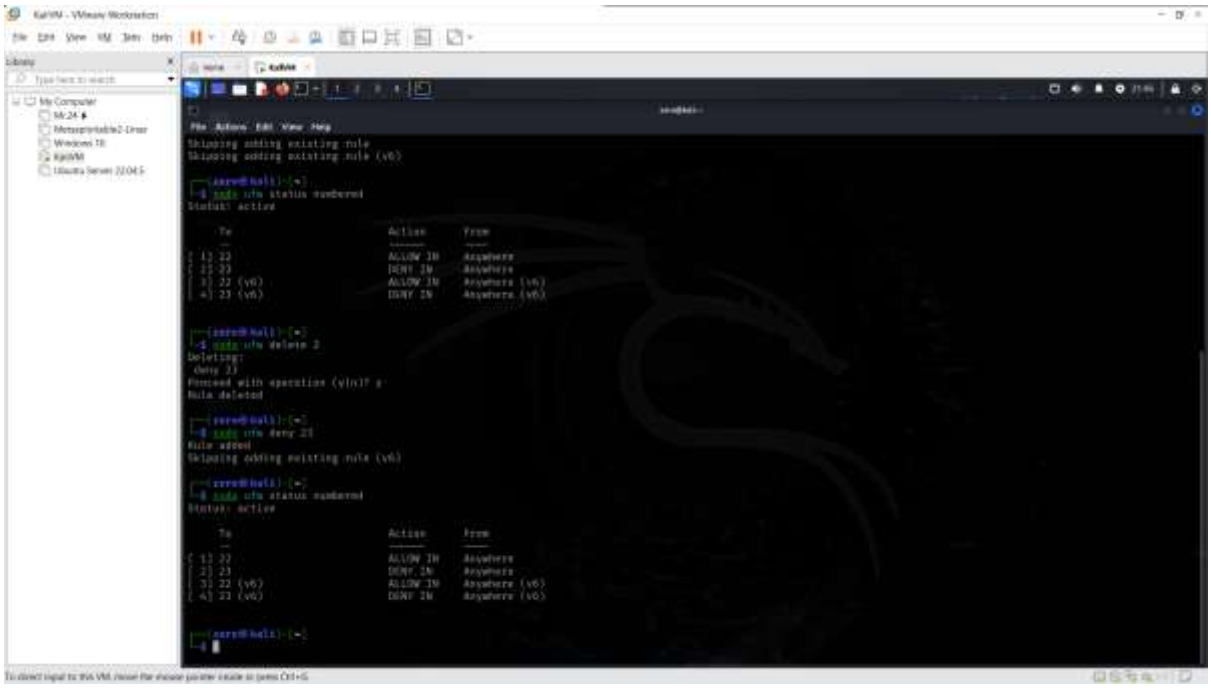
- UFW status and rule list



- Telnet block test



- Rule deletion and re-addition confirmation



✅ Outcome

- UFW successfully enabled and configured
- SSH (port 22) allowed
- Telnet (port 23) denied
- Firewall rules verified and managed interactively

📄 7. Documented Commands Used

Here's a full list of all UFW commands used in this task:

Purpose	Command
Check status	sudo ufw status verbose
Enable UFW	sudo ufw enable
Allow port 22	sudo ufw allow 22
Deny port 23	sudo ufw deny 23
View numbered rules	sudo ufw status numbered

Purpose	Command
Delete a rule (e.g., #2)	sudo ufw delete 2
Re-add deny rule	sudo ufw deny 23

No GUI steps were used, as all configurations were done via terminal.

🔎 8. How Firewall Filters Traffic

A firewall works by applying **rules** that either **allow** or **block** network traffic based on specific conditions such as:

- **Port number**
- **IP address**
- **Protocol (TCP/UDP)**

In this task, UFW filtered traffic based on **incoming port numbers**:

- It **allowed** SSH (port 22), so connections on that port were permitted.
- It **denied** Telnet (port 23), blocking all incoming attempts on that port.

These rules act as a **protective barrier**, only letting trusted traffic through and dropping or rejecting anything unauthorized — effectively reducing attack surfaces and unauthorized access risks.