

## 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

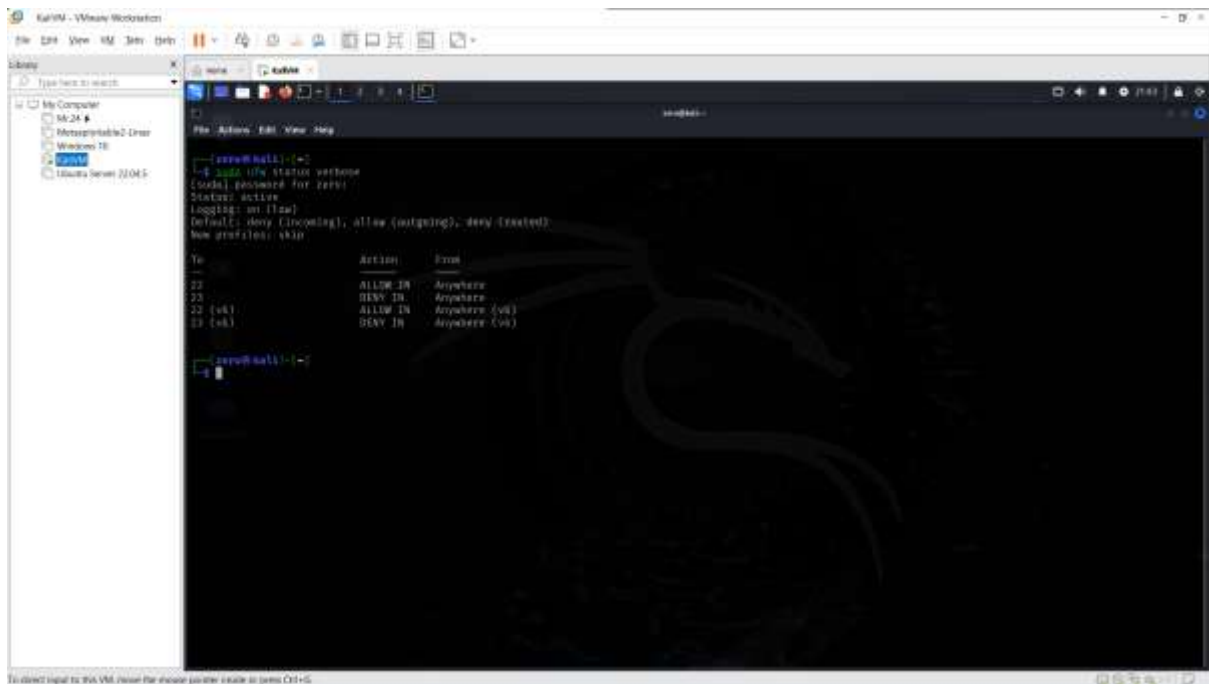
```
sudo ufw deny 23
```

## 8. Checked Final Status

sudo ufw status numbered

### Screenshots Included

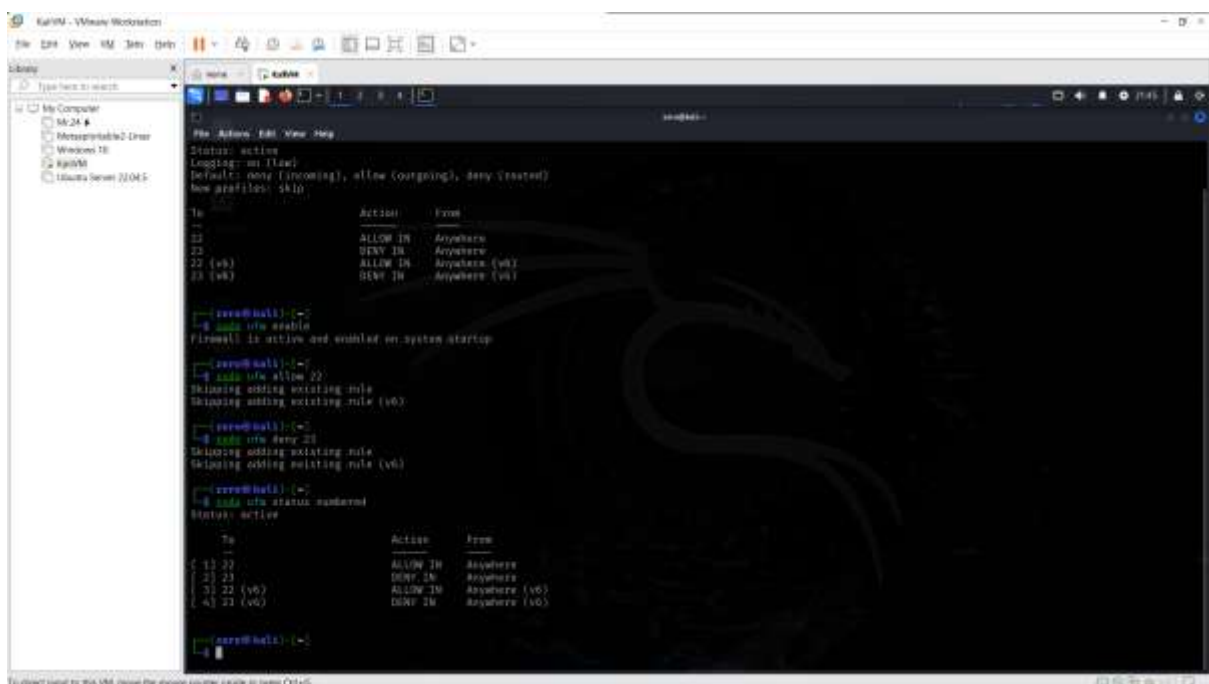
- UFW status and rule list



```
root@kali:~# sudo ufw status
Status: active
Logging: on (off)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

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

- Telnet block test



```
root@kali:~# sudo ufw enable
Firewall is active and enabled on system startup

root@kali:~# sudo ufw allow 22
Skipping adding existing rule
Skipping adding existing rule (v6)

root@kali:~# sudo ufw deny 22
Skipping adding existing rule
Skipping adding existing rule (v6)

root@kali:~# sudo ufw status numbered
Status: active

To Action From
--
11 22 ALLOW IN Anywhere
21 23 DENY IN Anywhere
31 22 ALLOW IN Anywhere (v6)
41 23 DENY IN Anywhere (v6)
```

- Rule deletion and re-addition confirmation

```

root@kali:~# sudo ufw status verbose
Status: active

To:      Action      From
--      -
1) 22    ALLOW IN    Anywhere
2) 23    DENY IN     Anywhere
3) 22 (v6) ALLOW IN    Anywhere (v6)
4) 23 (v6) DENY IN     Anywhere (v6)

root@kali:~# sudo ufw delete 2
Deleting:
Only 23
Removed with expiration (v6): 2
Rule deleted

root@kali:~# sudo ufw deny 23
Rule added
Deleting existing rule (v6)

root@kali:~# sudo ufw status numbered
Status: active

To:      Action      From
--      -
1) 22    ALLOW IN    Anywhere
2) 23    DENY IN     Anywhere
3) 22 (v6) ALLOW IN    Anywhere (v6)
4) 23 (v6) DENY IN     Anywhere (v6)

root@kali:~#

```

## ✓ 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	<code>sudo ufw status verbose</code>
Enable UFW	<code>sudo ufw enable</code>
Allow port 22	<code>sudo ufw allow 22</code>
Deny port 23	<code>sudo ufw deny 23</code>
View numbered rules	<code>sudo ufw status numbered</code>

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

*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.