

## Task – 4 Firewall Configuration and Testing Using UFW

---

### Objective:

Configure and test basic firewall rules using UFW to allow or block network traffic.

### Tools Used:

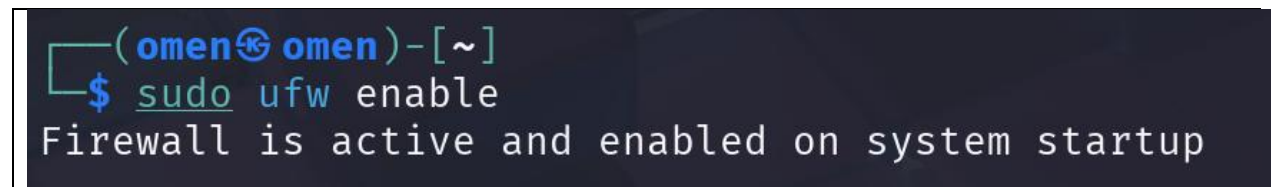
- UFW (Uncomplicated Firewall)
  - Linux Virtual Machine
- 

## Step-by-Step Procedure

### 1. Open Firewall Configuration Tool

Open the terminal and ensure UFW is installed and enabled:

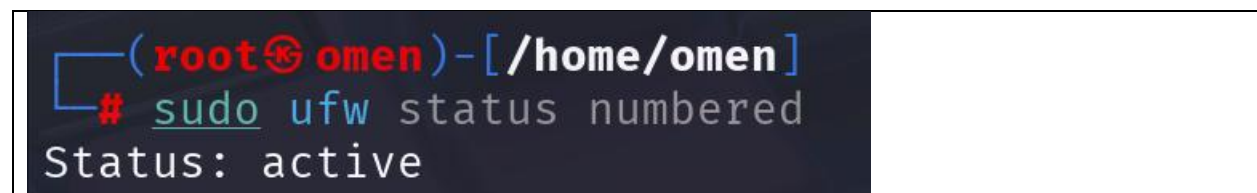
```
sudo apt update
sudo apt install ufw
sudo ufw enable
```



```
(omen@omen)-[~]
$ sudo ufw enable
Firewall is active and enabled on system startup
```

### 2. List Current Firewall Rules

```
sudo ufw status numbered
```



```
(root@omen)-[/home/omen]
# sudo ufw status numbered
Status: active
```

**Currently it is showing only status active and no rules because no rules have been implied on the firewall.**

**In upcoming steps the rules will be applied and then rules will be visible.**

For demonstration I added a rule to allow traffic from port 22.

```
(root@omen)-[/home/omen]
# sudo ufw allow 22

Rule added
Rule added (v6)
```

```
(root@omen)-[/home/omen]
# sudo ufw status numbered
Status: active
```

	To	Action	From
	--	---	---
[ 1]	22	ALLOW IN	Anywhere
[ 2]	22 (v6)	ALLOW IN	Anywhere (v6)

### 3. Block Inbound Traffic on Port 23 (Telnet)

```
sudo ufw deny 23
```

```
(root@omen)-[/home/omen]
# sudo ufw deny 23
Rule added
Rule added (v6)
```

```
(root@omen)-[/home/omen]
# 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)

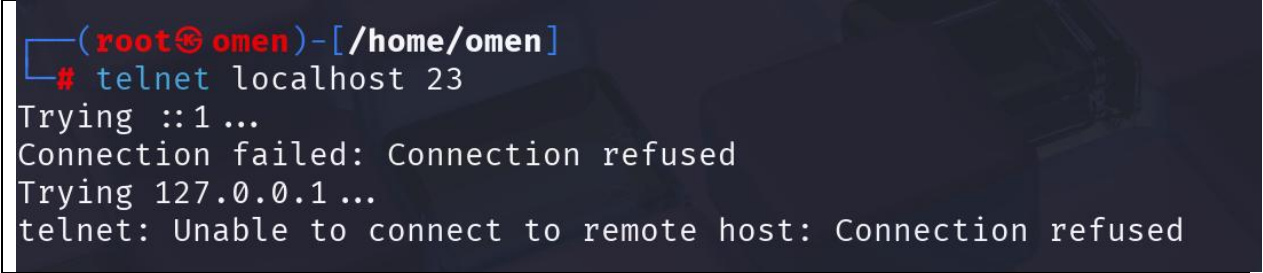
#### 4. Test the Rule by Attempting Connection

Install telnet client and test connection to port 23:

```
sudo apt install telnet
```

**#Attempt to connect to localhost on port 23**

```
telnet localhost 23
```

A terminal window with a dark background and light-colored text. The prompt is (root@omen)-[/home/omen]. The user enters # telnet localhost 23. The output shows 'Trying ::1...' followed by 'Connection failed: Connection refused'. Then it shows 'Trying 127.0.0.1...' followed by 'telnet: Unable to connect to remote host: Connection refused'.

```
(root@omen)-[/home/omen]
# telnet localhost 23
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```

#### 5. Allow SSH (Port 22)

**This can be done 2 ways:**

```
1) sudo ufw allow ssh
```

Or explicitly:

```
2) sudo ufw allow 22
```

**As I have shown in the first step itself how it can be port 22 (SSH) can be allowed.**

#### 6. Remove the Block Rule for Port 23

To remove the block rule for port 23 , first list rules with numbers:

```
sudo ufw status numbered
```

Delete the rule by its number (replace x with actual rule number):

```
sudo ufw delete X
```

```
(root@omen)~[/home/omen]
# 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@omen)~[/home/omen]
# sudo ufw delete 2
Deleting:
deny 23
Proceed with operation (y/n)? y
Rule deleted

(root@omen)~[/home/omen]
# sudo ufw status numbered
Status: active

    To      Action      From
    --      -
[ 1] 22      ALLOW IN    Anywhere
[ 2] 22 (v6)  ALLOW IN    Anywhere (v6)
[ 3] 23 (v6)  DENY IN     Anywhere (v6)
```

## Summary

### How Firewall Filters Traffic

UFW filters incoming and outgoing traffic by setting rules at the network level. By default, it blocks all unsolicited incoming traffic while allowing all outgoing traffic. Administrators can allow or deny traffic to specific ports, ensuring that only trusted services are accessible.