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

Name: Abinash I
Date: 08/08/2025
System Used: Kali Linux

Objective

To configure and test basic firewall rules using UFW to allow or block network traffic based on port numbers.

Tools Used

- **Linux (Kali)**
- **UFW** – Uncomplicated Firewall (frontend for iptables)
- **Telnet** – For testing blocked ports

Procedure:

Update Your Package List

```
// sudo apt update
```

Install UFW

```
// sudo apt install ufw -y
```

The `-y` just means "say yes to everything" so it installs without asking.

Verify Installation

```
// sudo ufw version
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install ufw -y

Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 457
  Download size: 169 kB
  Space needed: 880 kB / 63.8 GB available

Get:1 http://mirror.kku.ac.th/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 3s (64.3 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 412631 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' → '/usr/lib/systemd/system/ufw.service'.
Processing triggers for kali-menu (2025.2.7) ...
Processing triggers for man-db (2.13.1-1) ...

┌──(kali㉿kali)-[~]
└─$ sudo ufw version

ufw 0.36.2
Copyright 2008-2023 Canonical Ltd.
```

Start Following the Firewall Steps:

Once installed, you can go back to:

// sudo ufw enable
// sudo ufw status numbered

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
sudo ufw status numbered

Firewall is active and enabled on system startup
Status: active
```

Check current rules

// sudo ufw status numbered

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status numbered

Status: active
```

Block port 23 (Telnet)

// sudo ufw deny 23/tcp

Verify the rule is added

// sudo ufw status numbered

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw deny 23/tcp

Rule added
Rule added (v6)

┌──(kali㉿kali)-[~]
└─$ sudo ufw status numbered

Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23/tcp                     DENY IN     Anywhere
[ 2] 23/tcp (v6)                DENY IN     Anywhere (v6)
```

Test the block

```
// sudo apt install telnet -y
// telnet localhost 23
```

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install telnet -y
telnet localhost 23

Upgrading:
  inetutils-telnet

Installing:
  telnet

Summary:
  Upgrading: 1, Installing: 1, Removing: 0, Not Upgrading: 456
  Download size: 174 kB
  Space needed: 56.3 kB / 63.8 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 inetutils-telnet amd64 2:2.6-3 [130 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 telnet all 0.17+2.6-3 [43.3 kB]
Fetched 174 kB in 1s (125 kB/s)
(Reading database ... 412744 files and directories currently installed.)
Preparing to unpack .../inetutils-telnet_2%3a2.6-3_amd64.deb ...
Unpacking inetutils-telnet (2:2.6-3) over (2:2.6-1) ...
Selecting previously unselected package telnet.
Preparing to unpack .../telnet_0.17+2.6-3_all.deb ...
Unpacking telnet (0.17+2.6-3) ...
Setting up inetutils-telnet (2:2.6-3) ...
Setting up telnet (0.17+2.6-3) ...
Processing triggers for kali-menu (2025.2.7) ...
```

- **It should fail with “Connection refused”.**

Allow SSH (Port 22)

```
// sudo ufw allow 22/tcp
```

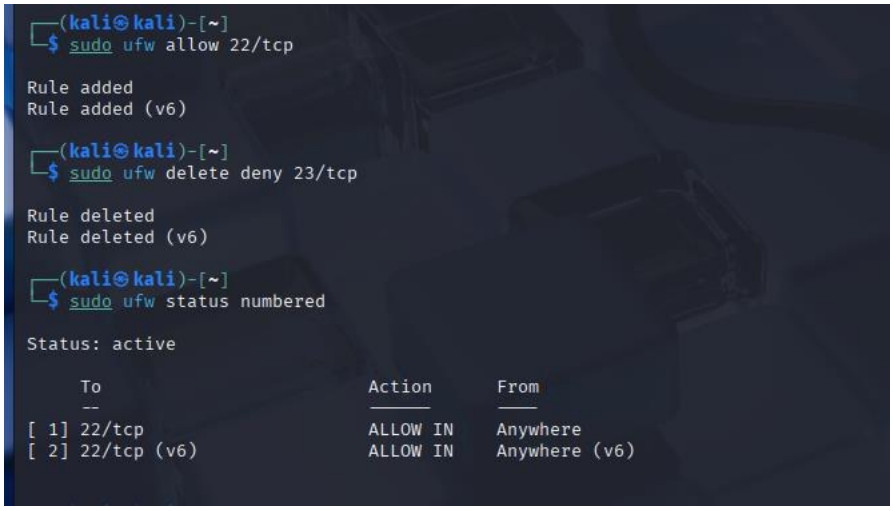
Remove the test block

```
// sudo ufw delete deny 23/tcp
```

Final check

```
// sudo ufw status numbered
```

no port 23 entry.



A firewall acts as a **security checkpoint** for network traffic.
Using UFW, we:

- Enabled the firewall.
- Blocked insecure Telnet traffic (port 23).
- Verified the block worked by testing a connection.
- Allowed secure SSH access (port 22).
- Removed the test rule to restore the system.

🔒 FIREWALL (UFW)

Internet 🌍 ⟶ [Port 22 ✓ ALLOW] ⟶ SSH Service

[Port 23 ⊘ DENY] ✕ Telnet Blocked

[Port 80 ✓ ALLOW] ⟶ Web Server