

Task 4 – Firewall Configuration using UFW (Kali Linux)

Objective:

Configure and test a basic firewall using UFW on Kali Linux. Block Telnet (port 23), allow

Tools Used:

- Kali Linux
- UFW (Uncomplicated Firewall)

Steps Performed:

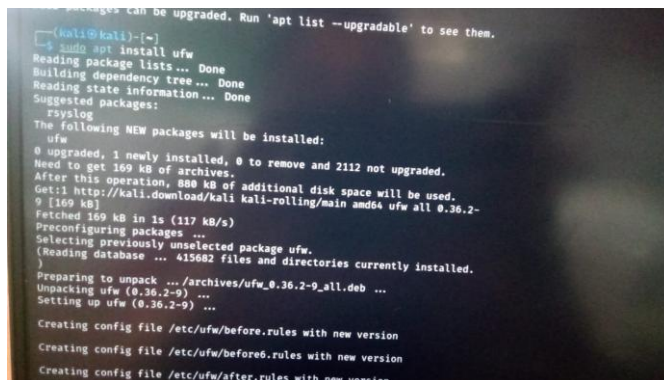
1. Installed UFW

```
''' bash

sudo apt update

sudo apt install ufw

'''
```

A screenshot of a terminal window showing the installation of UFW. The prompt is (kali@kali)-[~]. The command 'sudo apt install ufw' is entered. The output shows the package lists being read, the dependency tree being built, and the state information being read. It then lists suggested packages: rsyslog. The following NEW packages will be installed: ufw. It shows that 0 packages are upgraded, 1 is newly installed, and 0 are to be removed. The total size of the download is 169 kB. The terminal output continues with the fetching of the package, preconfiguration, and the creation of UFW configuration files: /etc/ufw/before.rules, /etc/ufw/before6.rules, and /etc/ufw/after.rules.

```
(kali@kali)-[~]
$ sudo apt install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  rsyslog
The following NEW packages will be installed:
  ufw
0 upgraded, 1 newly installed, 0 to remove and 2112 not upgraded.
Need to get 169 kB of archives.
After this operation, 888 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-
9 [169 kB]
Fetched 169 kB in 1s (117 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 415682 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
```

2.Enabled the Firewall

```
''' bash

sudo ufw enable

'''
```

3.Checked Current Firewall Rules

```
'''bash

sudo ufw status verbose

'''
```

4. Blocked Inbound Traffic on Port 23 (Telnet)

```
'''bash

sudo ufw deny 23

'''
```

```

Connection failed: Connection refused
Trying 127.0.0.1 ...
telnet: Unable to connect to remote host: Connection refused

(kali@kali)-[~]
$ sudo nano /etc/xinetd.d/telnet

(kali@kali)-[~]
$ telnet localhost 23
Trying ::1 ...
Connection failed: Connection refused
Trying 127.0.0.1 ...
telnet: Unable to connect to remote host: Connection refused

(kali@kali)-[~]
$ sudo ufw delete deny 23
Rule deleted
Rule deleted (v6)

```

5.Allowed SSH Port (22)

```bash

sudo ufw allow 22

```

6.Verified Rules Applied

```bash

sudo ufw status numbered

```

```

(kali@kali)-[~]
$ sudo ufw delete deny 23
Rule deleted
Rule deleted (v6)

(kali@kali)-[~]
$ sudo ufw status numbered
Status: active

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

(kali@kali)-[~]
$

```

Expected Output:

To Action From

-- ----- ---

22 ALLOW Anywhere

23 DENY Anywhere

7.Tested Blocked Port with Telnet

```bash

telnet localhost 23

```

Result:

Connection refused

⚠ If telnet is not installed:

```
```bash
 sudo apt install telnet
```
```

Removed the Block Rule

```
```bash
 sudo ufw delete deny 23
```
```

Summary: How Firewall Filters Traffic

A firewall acts like a gatekeeper, inspecting incoming and outgoing traffic based on predefined rules. It filters traffic by:

- Allowing traffic on trusted ports (like **SSH on port 22**)
- Blocking insecure or unwanted traffic (like **Telnet on port 23**)
- Preventing unauthorized access to sensitive services
- Ensuring only permitted connections are allowed

In this task, UFW (Uncomplicated Firewall) was used to apply and verify rules that control which traffic is allowed or blocked, thus improving system security.