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

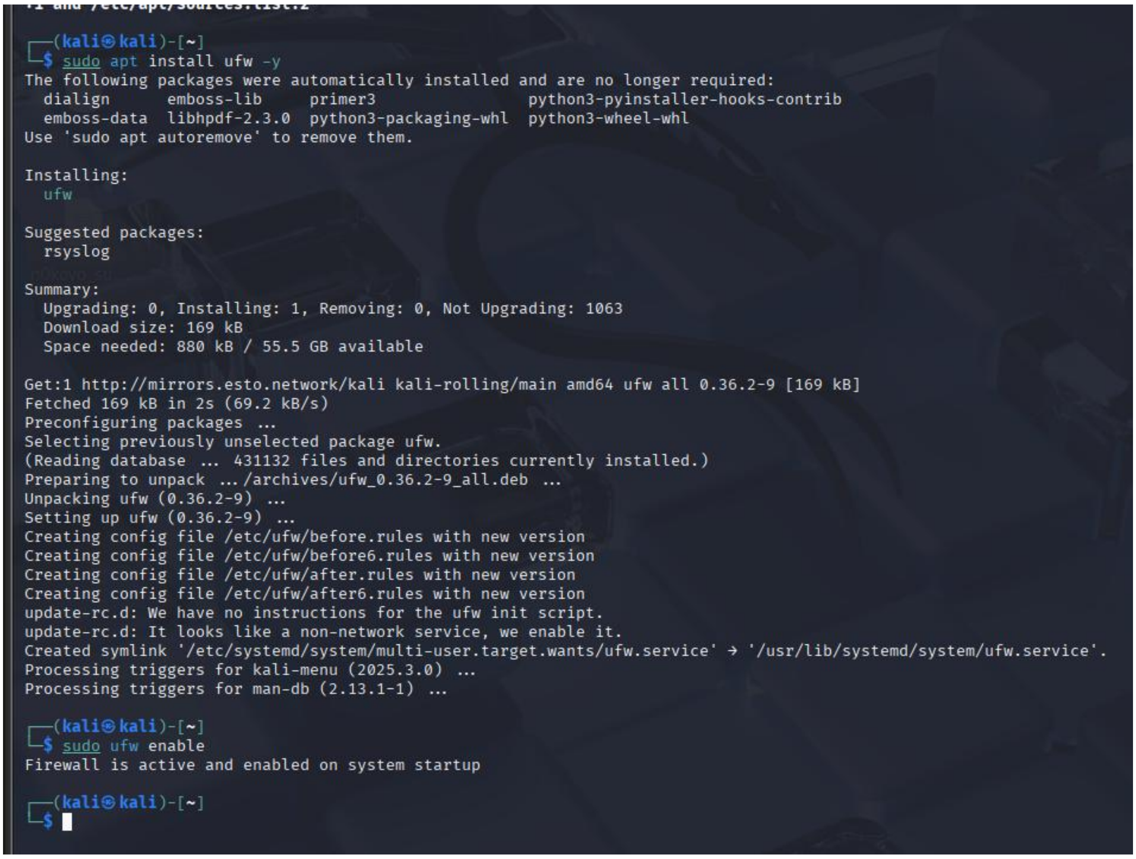
Name - Anisha Khairnar (anishakhairnar284@gmail.com)

Job – CyberSecurity intern

## Objective: Configure and test basic firewall rules to allow or block traffic:

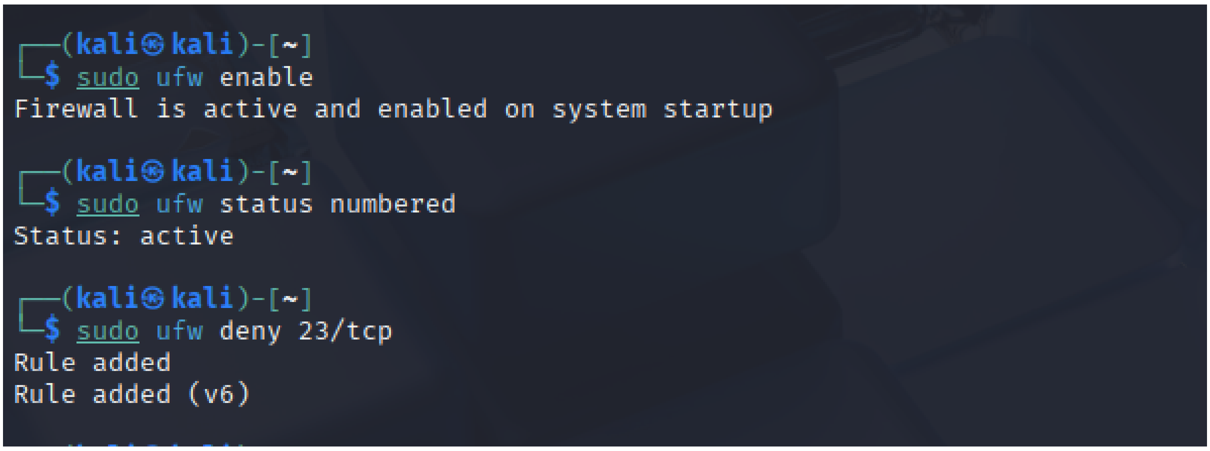
Firewalls are a critical component of system and network security, designed to control the flow of traffic based on predefined rules. They act as a barrier between trusted and untrusted networks, allowing safe communication while blocking potentially harmful connections. In this task, the objective was to configure and test basic firewall rules using **UFW (Uncomplicated Firewall)** on Kali Linux. By creating, testing, and removing rules for specific ports such as Telnet (port 23) and SSH (port 22), the exercise demonstrates how firewalls filter traffic to secure a system against unauthorized access while still permitting legitimate connections.

## 1] Firewall enabled :



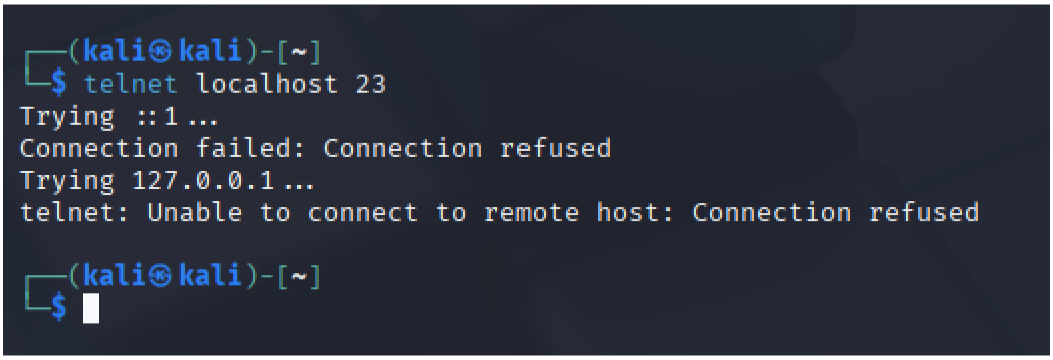
```
:1 and /etc/apt/sources.list:2

┌──(kali㉿kali)-[~]
└─$ sudo apt install ufw -y
The following packages were automatically installed and are no longer required:
  dialign      emboss-lib     primer3               python3-pyinstaller-hooks-contrib
  emboss-data  libhpdf-2.3.0  python3-packaging-whl  python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1063
  Download size: 169 kB
  Space needed: 880 kB / 55.5 GB available

Get:1 http://mirrors.esto.network/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 2s (69.2 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 431132 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 (2025.3.0) ...
Processing triggers for man-db (2.13.1-1) ...

┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

┌──(kali㉿kali)-[~]
└─$ ▮
```

2] Listed current firewall rules and added a rule to bound inbound traffic on Telnet port 23:



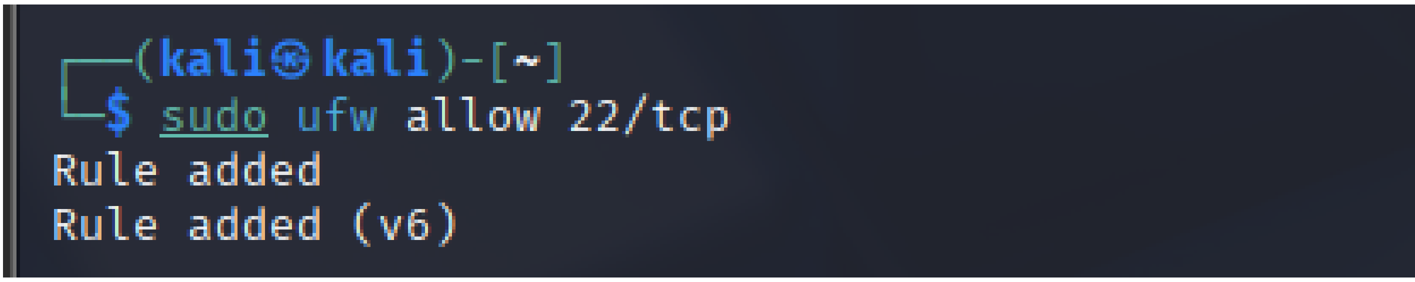
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

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

┌──(kali㉿kali)-[~]
└─$ sudo ufw deny 23/tcp
Rule added
Rule added (v6)
```

3] Trying to telnet port 23 – successfully blocked :



```
┌──(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)-[~]
└─$ 
```

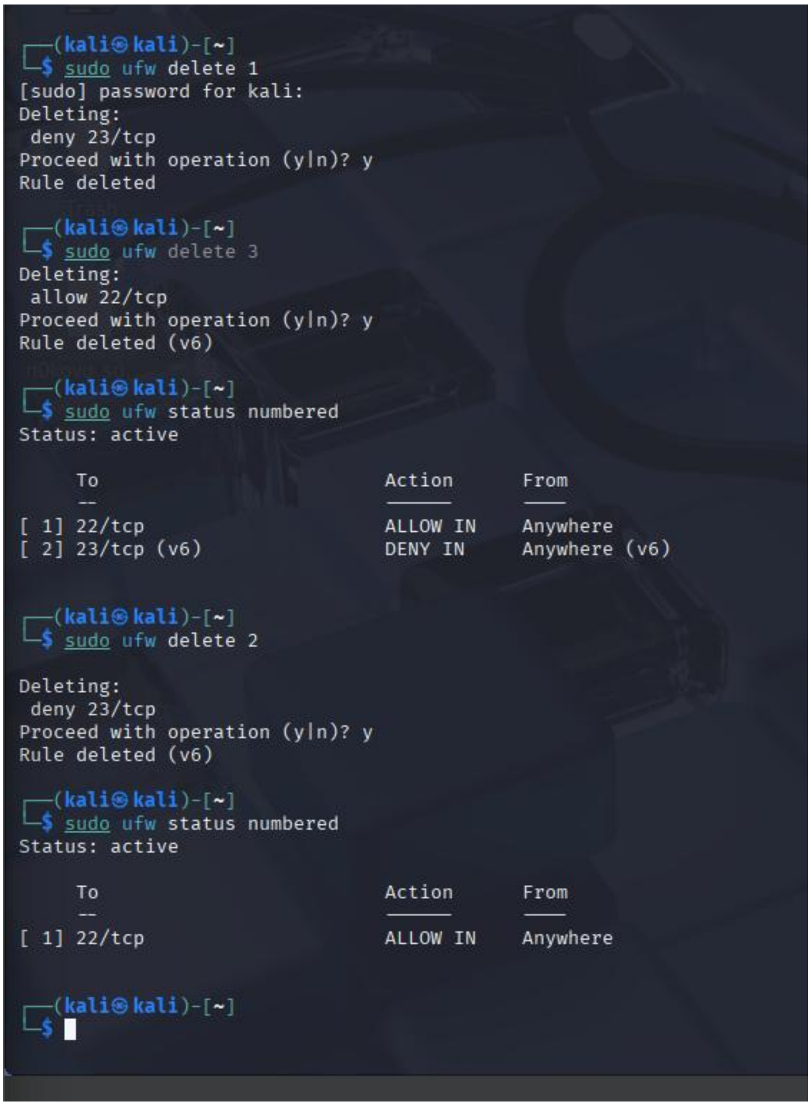
4] Allowed SSH port on 22 :



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22/tcp
Rule added
Rule added (v6)
```

5] Removed the telnet block rule – restored the original state :

Deleted port 23 and allowed port 22 successfully



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw delete 1
[sudo] password for kali:
Deleting:
 deny 23/tcp
Proceed with operation (y|n)? y
Rule deleted

┌──(kali㉿kali)-[~]
└─$ sudo ufw delete 3
Deleting:
 allow 22/tcp
Proceed with operation (y|n)? y
Rule deleted (v6)

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

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


┌──(kali㉿kali)-[~]
└─$ sudo ufw delete 2

Deleting:
 deny 23/tcp
Proceed with operation (y|n)? y
Rule deleted (v6)

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

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere


┌──(kali㉿kali)-[~]
└─$ 
```

So these are the list of commands I used:

1. ufw status numbered
2. ufw deny 23/tcp
3. telnet localhost 23
4. ufw allow 22/tcp
5. ufw delete N

**Firewall Traffic Filtering Summary**

The Uncomplicated Firewall (UFW) acts as a user-friendly front-end for **iptables**, simplifying the process of managing network traffic rules. It filters traffic based on defined **allow** or **deny** rules, which can be applied to specific ports, IP addresses, or protocols. By default, UFW blocks all inbound connections unless explicitly permitted, ensuring a secure baseline configuration. For instance, blocking port 23 prevents insecure Telnet access, while allowing port 22 enables secure SSH communication. This rule-based approach ensures that only authorized traffic is allowed, while potentially harmful or unnecessary connections are restricted, thereby enhancing system security.

Conclusion:

This task demonstrated the practical use of a firewall in controlling network traffic. By configuring rules in UFW, I was able to block insecure Telnet access on port 23, allow secure SSH connections on port 22, and then restore the firewall to its original state. This hands-on exercise highlights the importance of firewalls in protecting systems from unauthorized access while ensuring that essential communication channels remain open.