Task4 Report

Overall Status: **Complete**

Project Name: **Setup and Use a Firewall on Windows/Linux**

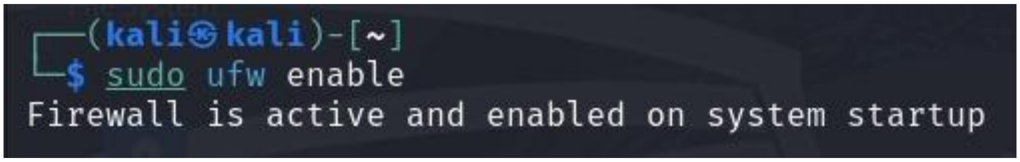
Date: 30/05/25

- **Objective: Configure and test basic firewall rules to allow or block traffic.**
- **Tools: Windows Firewall / UFW (Uncomplicated Firewall) on Linux.**
- **Deliverables: Screenshot/configuration file showing firewall rules applied.**

Steps:

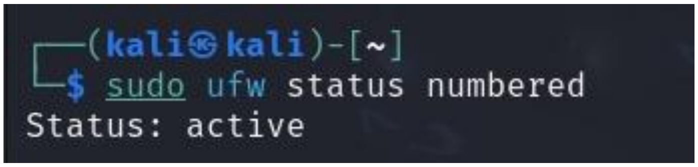
1)Open terminal and ensure ufw is installed and enabled.

install it and after that enable it



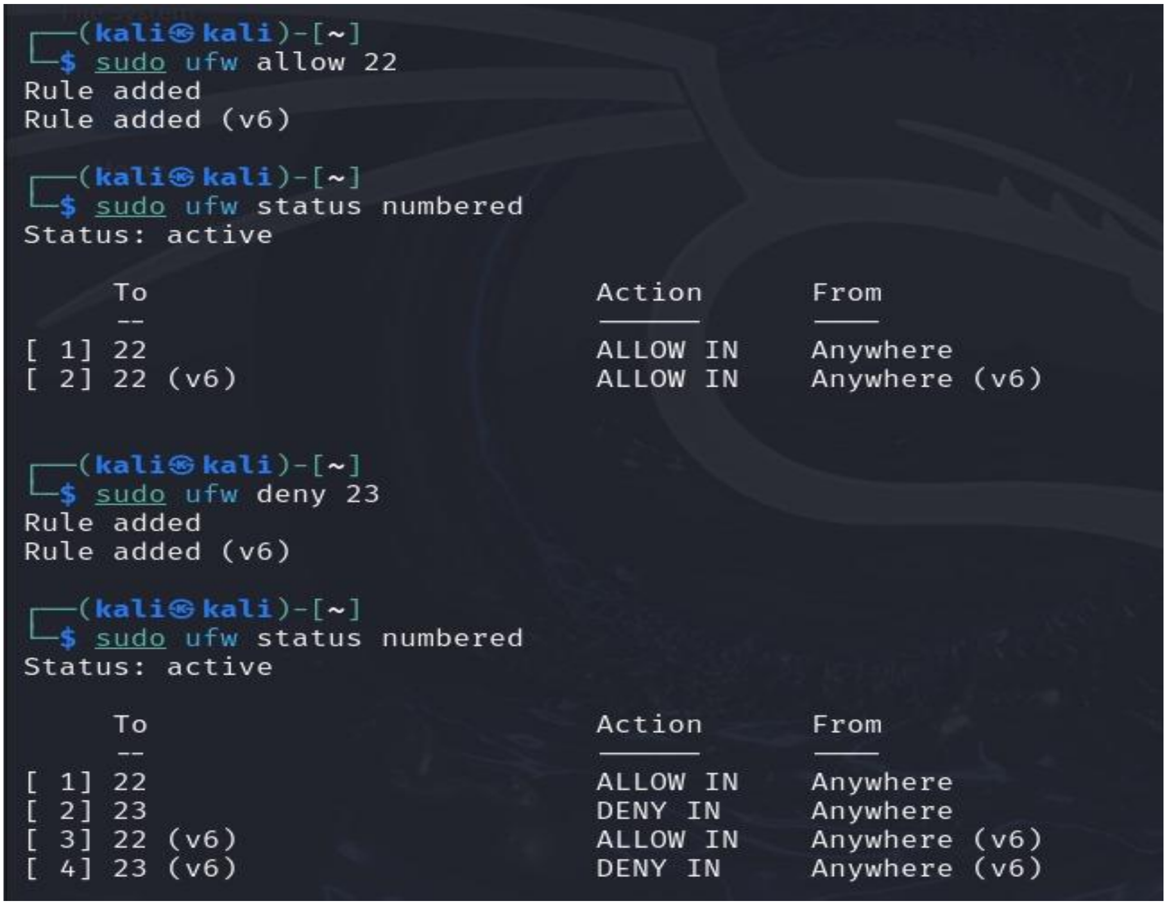
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup
```

2)Show current firewall status



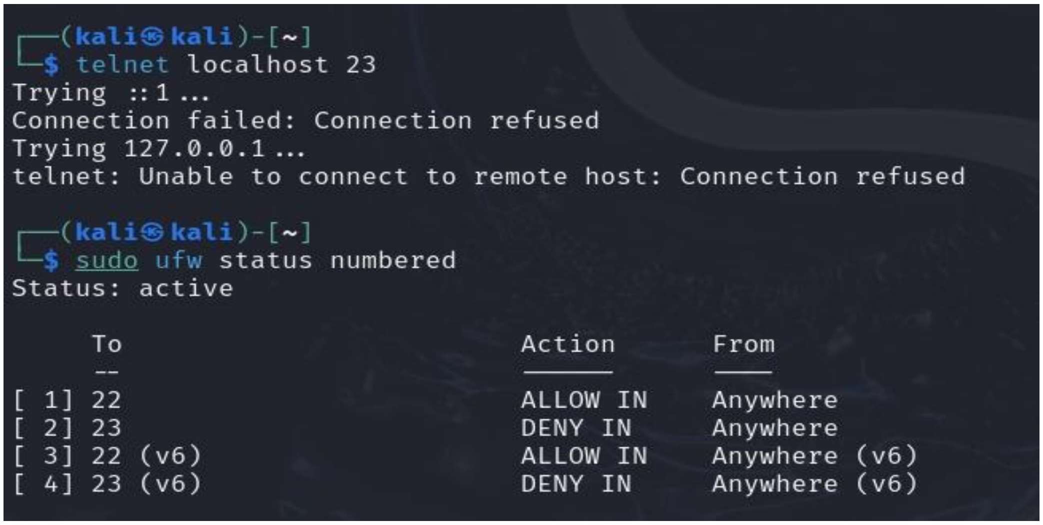
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status numbered
Status: active
```

3)Add rule to port 22 for allowing traffic and block traffic from port 23



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22
Rule added
Rule added (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)-[~]
└─$ sudo ufw deny 23
Rule added
Rule added (v6)

┌──(kali㉿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)
```

4)Test it out



```
┌──(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 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)
```

5)Remove rules from it

Summary of how firewalls filter traffic:

Firewalls filter traffic by examining data packets based on predefined rules that control network access. They can operate at different layers of the network stack, starting with basic packet filtering, which checks source and destination IP addresses, ports, and protocols. More advanced firewalls use stateful inspection to track ongoing connections and allow only legitimate, session-related traffic. At a deeper level, application-level firewalls analyze the actual content of traffic, such as HTTP requests, to detect malicious behavior. Modern next-generation firewalls (NGFWs) combine these methods with additional features like intrusion prevention, user identity tracking, and encrypted traffic inspection to provide comprehensive security.\