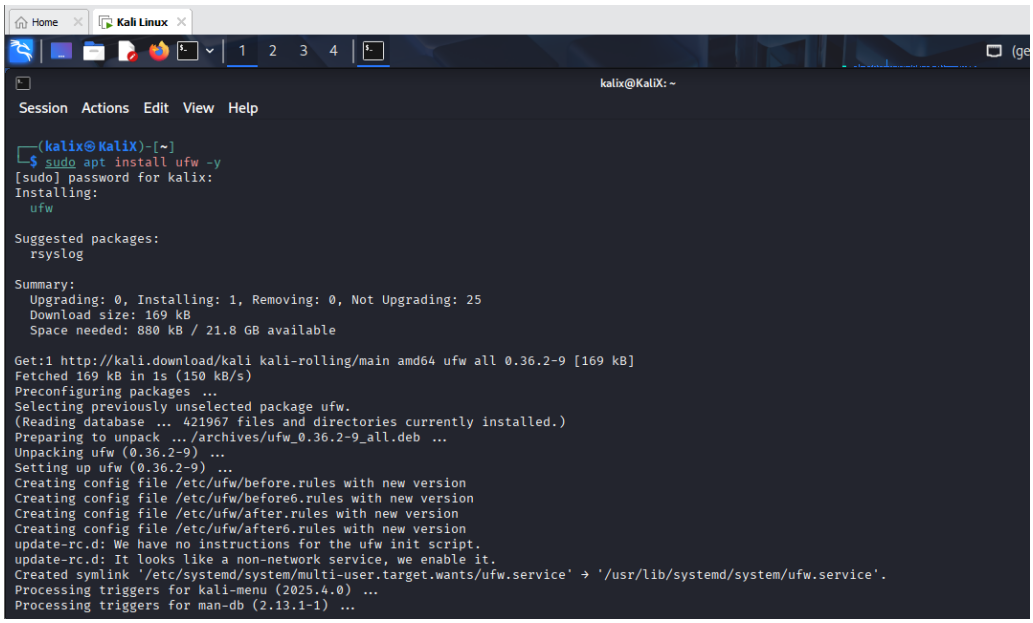
Task 4: Setup and Use a Firewall on Kali Linux with UFW

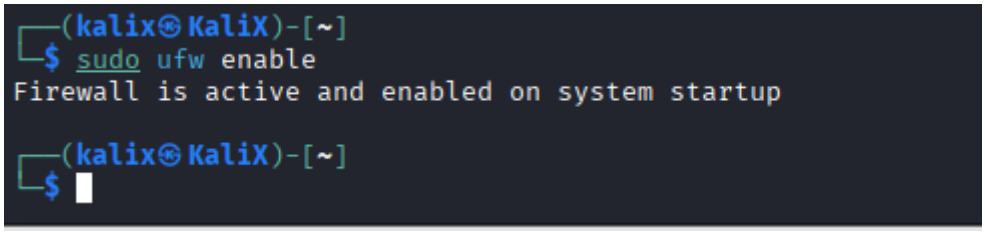
✅ Step-by-Step Process

1. Install and Enable UFW

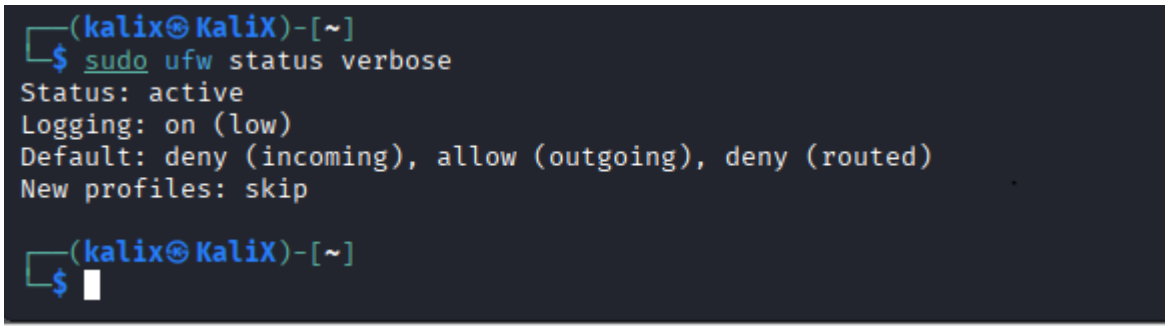
- $sudo apt update
- $sudo apt install ufw -y # Install UFW if not already installed



- $sudo ufw enable # Enable firewall



- $sudo ufw status verbose # Show current firewall status and rules



2. **Check Default Policies**

   Use if Default Policies not set

   - $sudo ufw default deny incoming
   - $sudo ufw default allow outgoing

3. **List current firewall rules**

   - $sudo ufw status numbered

```
┌──(kalix㉿KaliX)-[~]
└─$ sudo ufw status numbered
[sudo] password for kalix:
Status: active

┌──(kalix㉿KaliX)-[~]
└─$
```

   - Output shows all rules in effect (numbered for easy deletion later).

4. **Block Inbound Traffic on Port 23 (Telnet)**

   - $sudo ufw deny 23/tcp
   - $sudo ufw status numbered

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

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

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

   - Now port **23/TCP** is blocked.

5. **Test the Rule**

   - $nc -vz localhost 23

```
┌──(kalix㉿KaliX)-[~]
└─$ nc -vz localhost 23
localhost [127.0.0.1] 23 (telnet) : Connection refused

┌──(kalix㉿KaliX)-[~]
└─$
```

   - Result: **connection refused or blocked**.

6. **Allow SSH (Port 22)**

   To avoid locking yourself out:

   - $sudo ufw allow 22/tcp
   - $sudo ufw status numbered

```
┌──(kalix㉿KaliX)-[~]
└─$ sudo ufw allow 22/tcp
[sudo] password for kalix:
Rule added
Rule added (v6)

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

     To                         Action      From
     --                         ------      ----
[ 1] 23/tcp                     DENY IN     Anywhere
[ 2] 22/tcp                     ALLOW IN    Anywhere
[ 3] 23/tcp (v6)                DENY IN     Anywhere (v6)
[ 4] 22/tcp (v6)                ALLOW IN    Anywhere (v6)


┌──(kalix㉿KaliX)-[~]
└─$
```

   - This ensures remote SSH is still accessible.

7. **Remove the Test Rule**

   When finished, remove the Telnet block rule:

   - $sudo ufw delete deny 23/tcp

```
┌──(kalix㉿KaliX)-[~]
└─$ sudo ufw delete deny 23/tcp
Rule deleted
Rule deleted (v6)

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

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


┌──(kalix㉿KaliX)-[~]
└─$
```

   Or delete by rule number:

   - $sudo ufw status numbered