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

Tools Used

- **OS**: Kali Linux

- **Firewall Tool**: UFW (Uncomplicated Firewall)

Steps Performed

1. Install and Enable UFW

sudo apt update

sudo apt install ufw -y

sudo ufw enable

2. Check Current Firewall Status

sudo ufw status verbose

3. Block Inbound Traffic on Port 23 (Telnet)

sudo ufw deny 23

This blocks Telnet, which is insecure and transmits data in plaintext.

4. Test Rule

- Start a listener:

sudo nc -lvp 23

- From another terminal:

telnet 127.0.0.1 23

Expected result: **Connection should be blocked or refused.**

5. Allow SSH (Port 22)

sudo ufw allow 22

Ensures SSH access is not blocked, especially important for remote systems.

6. Remove Test Block Rule

- First, list numbered rules:

sudo ufw status numbered

- Then delete the specific rule:

sudo ufw delete [22]

7. Final Status Check

sudo ufw status verbose

Confirm only essential rules remain.

Outputs:

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

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

Rule added
Rule added (v6)

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

Status: active

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


┌──(kali㉿kali)-[~]
└─$ sudo nc -lvp 23

listening on [any] 23 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 51748
```

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

┌──(kali㉿kali)-[~]
└─$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

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

Rule added
Rule added (v6)

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

Status: active

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


┌──(kali㉿kali)-[~]
└─$
```

```
connect to [127.0.0.1] from localhost [127.0.0.1] 51748
^C

┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22

Rule added
Rule added (v6)

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

Status: active

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


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

┌──(kali㉿kali)-[~]
└─$
```

File   Actions   Edit   View   Help

┌──(kali㉿kali)-[~]
└─$ telnet 127.0.0.1 23

Trying 127.0.0.1 ...
Connected to 127.0.0.1.
Escape character is '^]'.