

Task 4 - Firewall Configuration (UFW)

Objective:

Configure a basic firewall on Linux using UFW to block and allow traffic, understand port management and test firewall rules.

Task SS:

```
kali@kali:~$ sudo ufw status verbose
Status: inactive
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
Rule added
Rule added (v6)
kali@kali:~$ sudo ufw allow 22
Rule added
Rule added (v6)
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)
kali@kali:~$ sudo ufw status numbered
Status: active
```

```

kali@kali:~$ sudo ufw status numbered
Firewall is active and enabled on system startup

Status: active

Rule added
Rule added (v6)
$ sudo ufw allow 22
Rule added
Rule added (v6)
$ sudo ufw deny 23
Rule added
Rule added (v6)
$ sudo ufw delete deny 23
Rule deleted
Rule deleted (v6)
$ sudo ufw status numbered
Status: active

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

```

Commands Used:

```
sudo ufw status verbose      # View current firewall status
sudo ufw enable              # Enable the firewall
sudo ufw deny 23             # Block Telnet port
sudo ufw allow 22            # Allow SSH
telnet localhost 23          # Test blocked port
sudo ufw delete deny 23      # Remove Telnet block
sudo ufw status numbered     # Confirm removal
```

Firewall Concepts:

- **Firewall:** A system designed to prevent unauthorized access to or from a private network.
- **Stateful Firewall:** Tracks the state of active connections and makes decisions based on the context of traffic.
- **Inbound Rule:** Controls traffic *into* your device.
- **Outbound Rule:** Controls traffic *out* from your device.
- **UFW:** Uncomplicated Firewall – a simple tool for managing firewall rules on Ubuntu-based systems.
- **Blocking Port 23:** Telnet is outdated and insecure. Blocking reduces risk of remote code execution.

Outcome:

- Successfully configured a firewall using UFW.
- Blocked and tested port-specific traffic (Telnet).
- Learned to manage and clean up firewall rules.
- Gained understanding of how a firewall filters traffic.