Setup and Use a Firewall on Windows/Linux

Objective

To configure and test basic firewall rules to allow or block network traffic using **Windows Firewall** or **UFW (Uncomplicated Firewall)** on Linux.

Tools Used

• Operating System: Kali Linux

• Firewall Tool: UFW

Terminal

Steps Performed

1. Checked Firewall Status

Command used (for Linux): sudo ufw status

```
__(root@ kali)-[~]

# ufw status verbose

Status: inactive
```

2. Enabled the Firewall

Command: sudo ufw enable

```
root⊗ kali)-[~]
# ufw enable
Firewall is active and enabled on system startup
```

3. Listed Current Firewall Rules

Command: sudo ufw status numbered

```
(root@kali)-[~]
# ufw status numbered
Status: active
```

4. Added Rule to Block a Specific Port (e.g., 23 - Telnet)

Command:

sudo ufw deny 23

```
(root@ kali)-[~]
# ufw deny 23/tcp
Rule added
Rule added (v6)
```

Test Performed:

Attempted to connect to port 23 using telnet localhost 23 (or any similar method)

Connection was blocked as expected.

5. Allowed SSH (Port 22)

Command: sudo ufw allow 22

```
(root@ kali)-[~]
# ufw allow 22/tcp
Rule added
Rule added (v6)
```

Test: Verified SSH connection — it worked successfully.

6. Verified Final Firewall Configuration

Command: sudo ufw status

```
ufw status
Status: active
То
                            Action
                                         From
23/tcp
                            DENY
                                         Anywhere
22/tcp
                             ALLOW
                                         Anywhere
23/tcp (v6)
                            DENY
                                         Anywhere (v6)
                            ALLOW
22/tcp (v6)
                                         Anywhere (v6)
```

Summary / Explanation

• Firewall Function:

A firewall filters incoming and outgoing network traffic based on defined security rules. It helps block unauthorized access while permitting legitimate communication.

• In this task:

- o I learned how to enable and manage firewall rules.
- Verified blocking/allowing specific ports.
- o Observed how firewall rules directly control network connections.

Conclusion

The firewall was successfully configured and tested.

Blocking and allowing specific ports demonstrated how traffic filtering works effectively. The system's security posture improved by restricting unnecessary open ports.