Task 4: Setup and Use a Firewall on Kali Linux

# Objective:

Configure and test basic firewall rules to allow or block traffic using UFW (Uncomplicated Firewall) on Kali Linux.

# Tools Used:

• Kali Linux  
• UFW (Uncomplicated Firewall)  
• Terminal

# Steps and Terminal Commands:

## Check current firewall status

ufw status  
Status: inactive

## Enable the firewall

ufw enable  
Firewall is active and enabled on system startup

## Check numbered status after enabling

ufw status numbered  
Status: active

## Block inbound traffic on port 23 (Telnet)

ufw deny 23  
Rule added  
Rule added (v6)

## Check current rules

## ufw status Status: active To Action From -- ------ ---- 23 DENY Anywhere 23 (v6) DENY Anywhere (v6)

## Test blocked port 23 using Telnet

## telnet localhost 23 Trying ::1... Connection failed: Connection refused Trying 127.0.0.1... telnet: Unable to connect to remote host: Connection refused

## Allow SSH traffic on port 22

ufw allow 22  
Rule added  
Rule added (v6)

## Check current rules

ufw status  
  
Status: active  
  
To Action From  
-- ------ ----  
23 DENY Anywhere   
22 ALLOW Anywhere   
23 (v6) DENY Anywhere (v6)   
22 (v6) ALLOW Anywhere (v6)

## Remove deny rule for port 23

ufw delete deny 23  
Rule deleted  
Rule deleted (v6)

## Verify only SSH is allowed

ufw status  
  
Status: active  
  
To Action From  
-- ------ ----  
22 ALLOW Anywhere   
22 (v6) ALLOW Anywhere (v6)

# Summary:

Using UFW on Kali Linux, firewall rules were applied to block Telnet (port 23) and allow SSH (port 22). Rules were verified using status checks and a telnet connection test confirmed the port was blocked. This exercise demonstrates basic traffic filtering using firewall rules.