# Task 4 : Setup and Use a Firewall on Windows/Linux

# 1. Open Firewall Configuration Tool

Command Used:  
ufw status verbose

Output:  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip

# 2. List Current Firewall Rules

Command Used:  
sudo iptables -L

Chain INPUT (policy DROP)  
target prot opt source destination   
ufw-before-logging-input all -- anywhere anywhere   
ufw-before-input all -- anywhere anywhere   
ufw-after-input all -- anywhere anywhere   
ufw-after-logging-input all -- anywhere anywhere   
ufw-reject-input all -- anywhere anywhere   
ufw-track-input all -- anywhere anywhere   
  
Chain FORWARD (policy DROP)  
target prot opt source destination   
ufw-before-logging-forward all -- anywhere anywhere   
ufw-before-forward all -- anywhere anywhere   
ufw-after-forward all -- anywhere anywhere   
ufw-after-logging-forward all -- anywhere anywhere   
ufw-reject-forward all -- anywhere anywhere   
ufw-track-forward all -- anywhere anywhere   
  
Chain OUTPUT (policy ACCEPT)  
target prot opt source destination   
ufw-before-logging-output all -- anywhere anywhere   
ufw-before-output all -- anywhere anywhere   
ufw-after-output all -- anywhere anywhere   
ufw-after-logging-output all -- anywhere anywhere   
ufw-reject-output all -- anywhere anywhere   
ufw-track-output all -- anywhere anywhere

**3.Blocking Inbound Traffic on Port 23(Telnet)**

Objective:  
Prevent unauthorized access through the Telnet protocol by blocking TCP traffic on port 23.

Using UFW:  
sudo ufw deny 23

Using iptables:  
sudo iptables -A INPUT -p tcp --dport 23 -j DROP

**4.Test the rule by attempting to connect to that port loca ly or remotely.**

1. Test Locally:  
sudo nc -l -p 23

2. Test from Another System:  
telnet <target-ip> 23

3. Local Test:  
telnet 127.0.0.1 23

Note : If the firewall rule is effective, all connection attempts on port 23 should fail.

**5.Add rule to alow SSH (port 22) if on Linux.**

Command Used:  
sudo ufw allow ssh

Verify Rule:  
sudo ufw status numbered

Status: active

To Action From

--- ---------- --------

[ 1] 23 ALLOW IN Anywhere

[ 2] 22/tcp ALLOW IN Anywhere

[ 3] 23 (v6) ALLOW IN Anywhere (v6)

[ 4] 22/tcp (v6) ALLOW IN Anywhere (v6]

# 6. Remove the Test Block Rule (Restore Original State)

Step 1: Revoke Allow Rule (if mistakenly added):  
sudo ufw deny 23

Step 2: Delete the Block Rule:  
sudo ufw delete 23

# 7. Summary: How Firewalls Filter Network Traffic

Traffic Inspection:  
Each packet is examined based on:  
- Source IP address  
- Destination IP address  
- Port number  
- Protocol

Rule Matching:  
- Packets are compared against a top-down rule set.  
- The first matching rule decides the action: ALLOW or DENY.

Decision Making:  
- If it matches an ALLOW rule -> accepted.  
- If it matches a DENY rule -> blocked.  
- If no rule matches -> default policy applied (usually deny).

Types of Firewalls:  
- Packet-filtering: Basic filtering based on headers.  
- Stateful Inspection: Tracks active connections.  
- Application-layer: Filters by application-level protocols.  
- Next-Gen Firewall (NGFW): Adds deep packet inspection, intrusion prevention, and more.