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

Objective: Configure and test basic firewall rules to allow or block traffic.

Tools: Windows Firewall / UFW (Uncomplicated Firewall) on Linux

Steps on Windows (Windows Defender Firewall)

1. Open Firewall Configuration Tool: Press Win + R → type wf.msc → press Enter.
2. List Current Rules: In the left pane, click Inbound Rules to view existing rules.
3. Add Rule to Block Port 23 (Telnet): Right-click Inbound Rules → New Rule → Port → 23 → Block the connection → Apply.
4. Test the Rule: Try 'telnet localhost 23' (if Telnet client installed). It should fail.
5. Add Rule to Allow SSH (Port 22): New Rule → Port → 22 → Allow connection.
6. Remove Test Block Rule: Right-click the Block Telnet rule and Delete.
7. Take Screenshot: Capture the firewall rules showing Block Telnet and Allow SSH.

Steps on Linux (UFW)

1. Check UFW Status: sudo ufw status verbose
2. Block Port 23 (Telnet): sudo ufw deny 23/tcp
3. Test Rule: telnet localhost 23 (should be blocked).
4. Allow SSH (Port 22): sudo ufw allow 22/tcp
5. List Rules: sudo ufw status numbered
6. Remove Test Rule: sudo ufw delete deny 23/tcp
7. Take Screenshot: Capture terminal showing rules (sudo ufw status).

Summary:

- Firewalls filter network traffic based on defined rules (port, protocol, IP).
- Allow rules explicitly permit traffic; Deny/Block rules reject or drop traffic.
- Blocking Telnet (23) prevents insecure access while allowing SSH (22) enables secure remote login.
- This exercise provides basic firewall management skills and traffic filtering understanding.

Outcome: Basic firewall management skills were practiced by blocking and allowing ports, verifying rules, and restoring settings.