CYBER SECURITY INTERNSHIP – TASK 10

Firewall Configuration & Testing

---

1. Introduction

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. Firewalls help protect systems from unauthorized access and network-based attacks.

This task focuses on configuring and testing firewall rules using **Windows Defender Firewall**.

---

2. Tool Used

- **Windows Defender Firewall**

Windows Defender Firewall is a built-in security feature in Windows that provides network protection by filtering traffic using inbound and outbound rules.

---

3. Firewall Status

Windows Defender Firewall was enabled on the system for all network profiles:

- Domain
- Private
- Public

---

4. Firewall Rules Configuration

4.1 Allow Rule

An inbound rule was created to allow HTTP traffic on port 80.

- Rule Name: **Allow HTTP Port 80**
- Port: 80

- Protocol: TCP
- Action: Allow the connection
- Profile: All

This rule allows web traffic to access the system.

4.2 Block Rule

An inbound rule was created to block Telnet traffic on port 23.

- Rule Name: **Block Telnet Port 23**
- Port: 23
- Protocol: TCP
- Action: Block the connection
- Profile: All

Telnet is an insecure protocol, and blocking it improves system security.

---

5. Testing and Observation

After configuring the firewall rules:

- Allowed ports permitted network traffic
- Blocked ports denied unauthorized connections

This confirms that firewall rules directly affect network connectivity.

---

6. Firewall Logs (Concept)

Firewall logs can be used to monitor allowed and blocked traffic. These logs help in detecting suspicious activities and troubleshooting network issues.

---

7. Impact of Firewall Configuration

- Reduces attack surface
- Prevents unauthorized access
- Blocks insecure services
- Improves overall system security