Task 10: Firewall Configuration & Testing

By : Nroupsinh gohil

Tool Used: Windows Defender Firewall
Operating System: Windows

📘 Introduction

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

In this task, Windows Defender Firewall was used to configure inbound and outbound rules, test connectivity, block suspicious traffic, and document the security impact.

🔹 Firewall Concepts

- **Inbound Rules:** Control traffic coming into the system.
- **Outbound Rules:** Control traffic leaving the system.
- **Stateful Firewall:** Tracks the state of active connections and allows or blocks traffic accordingly.
- **Purpose of Firewall:** Prevent unauthorized access, reduce attack surface, and protect system resources.

🔹 Firewall Configuration Performed

1️⃣ Inbound Rule – Blocking Telnet Port

- **Rule Name:** Block Telnet Port 23
- **Direction:** Inbound
- **Protocol:** TCP
- **Port:** 23
- **Action:** Block
- **Profiles:** Domain, Private, Public

Reason:
Telnet is an insecure protocol that transmits data in plain text. Blocking port 23 prevents potential unauthorized access and reduces security risks.

2️⃣ Outbound Rule – Blocking Application Internet Access

- **Rule Name:** Block Notepad Internet Access
- **Direction:** Outbound
- **Program:** notepad.exe
- **Action:** Block
- **Profiles:** Domain, Private, Public

Reason:
Blocking outbound access for applications helps prevent unauthorized data transmission and improves control over system communications.

3️⃣ Blocking a Malicious IP Address

- **Rule Name:** Block Malicious IP
- **Direction:** Inbound
- **Remote IP Address:** 203.0.113.45
- **Action:** Block

Reason:
Suspicious or malicious IP addresses can be blocked to prevent potential attacks or unauthorized communication.

🔹 Test Connectivity

Connectivity testing was performed by verifying firewall rule enforcement.

- Inbound connections on port **23 (Telnet)** are blocked.
- Outbound internet access for **Notepad** is blocked.
  This confirms that firewall rules are applied and functioning correctly.

🔹 Observe Logs

Windows Defender Firewall monitors and logs all firewall activities internally.
The configured rules were verified as **enabled and active**, confirming successful enforcement of security policies.

🔹 **Firewall Rules Summary**

Rule Name	Direction	Action	Purpose
Block Telnet Port 23	Inbound	Block	Prevent insecure Telnet access
Block Notepad Internet Access	Outbound	Block	Control outbound application traffic
Block Malicious IP	Inbound	Block	Prevent suspicious IP communication

---

🔹 **Impact of Firewall Configuration**

- Reduced system attack surface
- Prevented unauthorized inbound connections
- Controlled outbound application traffic
- Improved overall system security

✅ **Conclusion**

This task demonstrated the importance of firewall configuration in securing a system. By creating inbound and outbound rules, blocking insecure ports, controlling application access, and preventing malicious IP communication, Windows Defender Firewall effectively enhanced system security.