Project Report – Windows Firewall Configuration and Testing

Objective

The objective of this task was to configure Windows Firewall rules to: 1. Block specific inbound network traffic (Telnet – Port 23). 2. Allow specific inbound network traffic (SSH – Port 22). 3. Test and verify the effectiveness of these firewall rules. 4. Document the process with evidence and explanations.

System Used

• Operating System: Windows 10/11 • Firewall Tool: Windows Defender Firewall with Advanced Security

Procedure

1. Opening Windows Firewall with Advanced Security

• Pressed Win + R, typed wf.msc, and pressed Enter. • The Windows Defender Firewall with Advanced Security console opened, showing Inbound Rules and Outbound Rules.

2. Creating a Block Rule for Port 23 (Telnet)

1. Selected Inbound Rules from the left panel. 2. In the right panel, clicked New Rule… 3. Rule Type: Selected Port → Next. 4. Protocol and Ports: Chose TCP → Selected Specific local ports → Entered 23 → Next. 5. Action: Selected Block the connection → Next. 6. Profile: Checked all profiles (Domain, Private, Public) → Next. 7. Name: Entered Block Telnet Port 23 → Finish. Result: A new rule appeared in the inbound rules list, blocking all incoming Telnet traffic.

3. Testing the Block Rule

• Enabled Telnet Client from Control Panel → Programs → Turn Windows features on or off. • Opened Command Prompt and ran: telnet 127.0.0.1 23 • Outcome: Connection failed, confirming the firewall rule was blocking port 23.

4. Creating an Allow Rule for Port 22 (SSH)

1. Selected Inbound Rules → New Rule… 2. Rule Type: Selected Port → Next. 3. Protocol and Ports: Kept TCP → Entered 22 → Next. 4. Action: Selected Allow the connection → Next. 5. Profile: Checked all profiles (Domain, Private, Public) → Next. 6. Name: Entered Allow SSH Port 22 → Finish. Result: A new inbound rule appeared to allow SSH traffic.

5. Testing the Allow Rule

• Since Windows does not run an SSH server by default, testing requires either installing an SSH server or testing from another machine on the same network. • In this project, the rule was visually verified as enabled and configured correctly.

Conclusion

This project successfully demonstrated: - How to create inbound firewall rules in Windows Defender Firewall. - Blocking Telnet traffic on port 23 effectively prevents unauthorized remote access. - Allowing SSH traffic on port 22 prepares the system for secure remote connections. - Testing confirmed the block rule’s effectiveness, and the allow rule was set up correctly.

Key Learning Outcomes

• Understanding of inbound traffic control using Windows Firewall. • Practical experience in creating, enabling, and testing firewall rules. • Awareness of protocol-specific port usage and security implications.