Task-4 Document Commands:

For Windows Firewall :

Steps:

1. Open Control Panel → System and Security → Windows Defender Firewall

2. Click Advanced Settings

3. Go to Inbound Rules → Click New Rule

4. Select Port, choose TCP, specify port 23

5. Choose Block the connection

6. Apply to all profiles

7. Name the rule Block\_Telnet\_23

8. Test with telnet localhost 23

9. Delete the rule from Inbound Rules after testing.

Summary:

To block Telnet port 23 using the Windows Firewall GUI, follow these steps: Open the Control Panel and navigate to **System and Security → Windows Defender Firewall**. Click on **Advanced Settings** to open the Windows Firewall with Advanced Security window. In the left pane, select **Inbound Rules**, then click **New Rule** on the right. Choose **Port** as the rule type, select **TCP**, and specify port **23**. Next, choose **Block the connection** when prompted. Apply this rule to all profiles (Domain, Private, and Public). Name the rule **Block\_Telnet\_23** for easy identification. After applying the rule, test it by running telnet localhost 23 to confirm the port is blocked. Once testing is complete and the rule is no longer needed, go back to **Inbound Rules**, locate **Block\_Telnet\_23**, and delete it to remove the block. This process helps in temporarily or permanently blocking access to Telnet for enhanced system security.

