**Setup and Use a Firewall on Windows**

Step 1 – Open Firewall Configuration Tool

Windows:

1. Press Windows + R
2. Type wf.msc and press Enter.
3. Windows Defender Firewall with Advanced Security opens.

Step 2 – List Current Firewall Rules

Windows:

* In the left panel, click Inbound Rules to see all inbound traffic rules.
* Click Outbound Rules to see outbound traffic rules.

Step 3 – Add Rule to Block Port 23 (Telnet)

Windows:

1. Go to Inbound Rules → New Rule.
2. Select Port → TCP → Port 23.
3. Choose Block the connection.
4. Select profiles (Domain, Private, Public).
5. Name it: Block Telnet Port 23 → Finish.

Step 4 – Test the Rule

* Verify the blocking rule exists and is enabled.
* Do a local test (on the machine with the rule).
* Do a remote test (from another machine on the network or Internet).
* Scan the port with nmap to classify its state.
* Check firewall logs for blocked entries.

Step 5 – Remove Test Block Rule

Windows:

* In Inbound Rules, locate Block Telnet Port 23 → Right-click → Delete.

Commands & GUI Steps Used

Windows:

* Opened firewall via wf.msc
* Checked inbound/outbound rules
* Created inbound block rule for TCP port 23
* Tested using Telnet
* Removed rule to restore state

Conclusion

* Accessed firewall settings.
* Viewed current firewall rules.
* Created a custom inbound block rule for port 23.
* Tested firewall effectiveness.
* Restored firewall to original state