



ELEVATE LABS CYBER SECURITY INTERNSHIP

Task-4:

1.Open firewall configuration tool:

 Run ✕

 Type the name of a program, folder, document or Internet resource, and Windows will open it for you.

Open: ▼

OK

Cancel

Browse...

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

- ☐ **Program**
Rule that controls connections for a program.
- ☒ **Port**
Rule that controls connections for a TCP or UDP port.
- ☐ **Predefined:**

AllJoyn Router

Rule that controls connections for a Windows experience.
- ☐ **Custom**
Custom rule.

< Back

Next >

Cancel

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

- ☒ TCP
- ☐ UDP

Does this rule apply to all local ports or specific local ports?

☐ All local ports

☒ Specific local ports:

Example: 80, 443, 5000-5010

< Back

Next >

Cancel

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☐ **Allow the connection**

This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

[Customize...](#)

☒ **Block the connection**

< Back

Next >

Cancel

New Inbound Rule Wizard
✕

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

Name:

Description (optional):

< Back
Finish
Cancel

4.Test the rule by attempting to connect to that port locally or remotely.

```

C:\Users\Chakr>telnet localhost 23
Connecting To localhost...Could not open connection to the host, on port 23: Connect failed
C:\Users\Chakr>

```

5.Add rule to allow SSH (port 22).

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Authc
✓ Allow SSH		All	Yes	Allow	No	Any	Any	Any	TCP	22	Any	Any	Any
✓ Apache HTTP Server		Public	Yes	Allow	No	C:\xampp...	Any	Any	TCP	Any	Any	Any	Any
✓ Apache HTTP Server		Public	Yes	Allow	No	C:\xampp...	Any	Any	UDP	Any	Any	Any	Any
✓ Apache HTTP Server		Public	Yes	Allow	No	E:\xampp...	Any	Any	UDP	Any	Any	Any	Any
✓ Apache HTTP Server		Public	Yes	Allow	No	E:\xampp...	Any	Any	TCP	Any	Any	Any	Any
✓ Arduino IDE		Public	Yes	Allow	No	D:\sem-6...	Any	Any	UDP	Any	Any	Any	Any

6.Remove the test block rule to restore original state.

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Users	Authc
Block the telnet		Public	Yes	Block	No	Any	Any	Any	TCP	23	Any	Any	Any
Apache HTTP Server		Public	Yes	Allow	No	C:\xampp...	Any	Any	TCP	Any	Any	Any	Any
Apache HTTP Server		Public	Yes	Allow	No	C:\xampp...	Any	Any	UDP	Any	Any	Any	Any
Apache HTTP Server		Public	Yes	Allow	No	E:\xampp...	Any	Any	UDP	Any	Any	Any	Any
Apache HTTP Server		Public	Yes	Allow	No	E:\xampp...	Any	Any	TCP	Any	Any	Any	Any
Arduino IDE		Public	Yes	Allow	No	D:\sem-6...	Any	Any	UDP	Any	Any	Any	Any
Arduino IDE		Public	Yes	Allow	No	D:\sem-6...	Any	Any	TCP	Any	Any	Any	Any
AsusSwitchNet_56ACDA9B		Public	Yes	Allow	No	C:\WIND...	Any	Any	Any	Any	Any	Any	Any
AsusSwitchNetMDNS_269A2EB3		Public	Yes	Allow	No	C:\WIND...	Any	Any	Any	Any	Any	Any	Any
autopsy64		Public	Yes	Allow	No	C:\progr...	Any	Any	UDP	Any	Any	Any	Any

7. Document Commands or GUI Steps Used

- Opened wf.msc
- Added inbound rule to block TCP port 23
- Verified using Telnet
- Allowed port 22 (SSH)
- Removed Telnet rule after testing

8. Summarize how firewall filters traffic.

Windows Firewall filters traffic by applying rules to incoming and outgoing connections. Each rule can allow or block traffic based on protocol, port, IP address, and profile (Domain, Private, Public). We tested this by blocking Telnet (port 23) and verifying it with a connection attempt, then allowed SSH (port 22). The firewall enforces these rules in real time to protect the system.