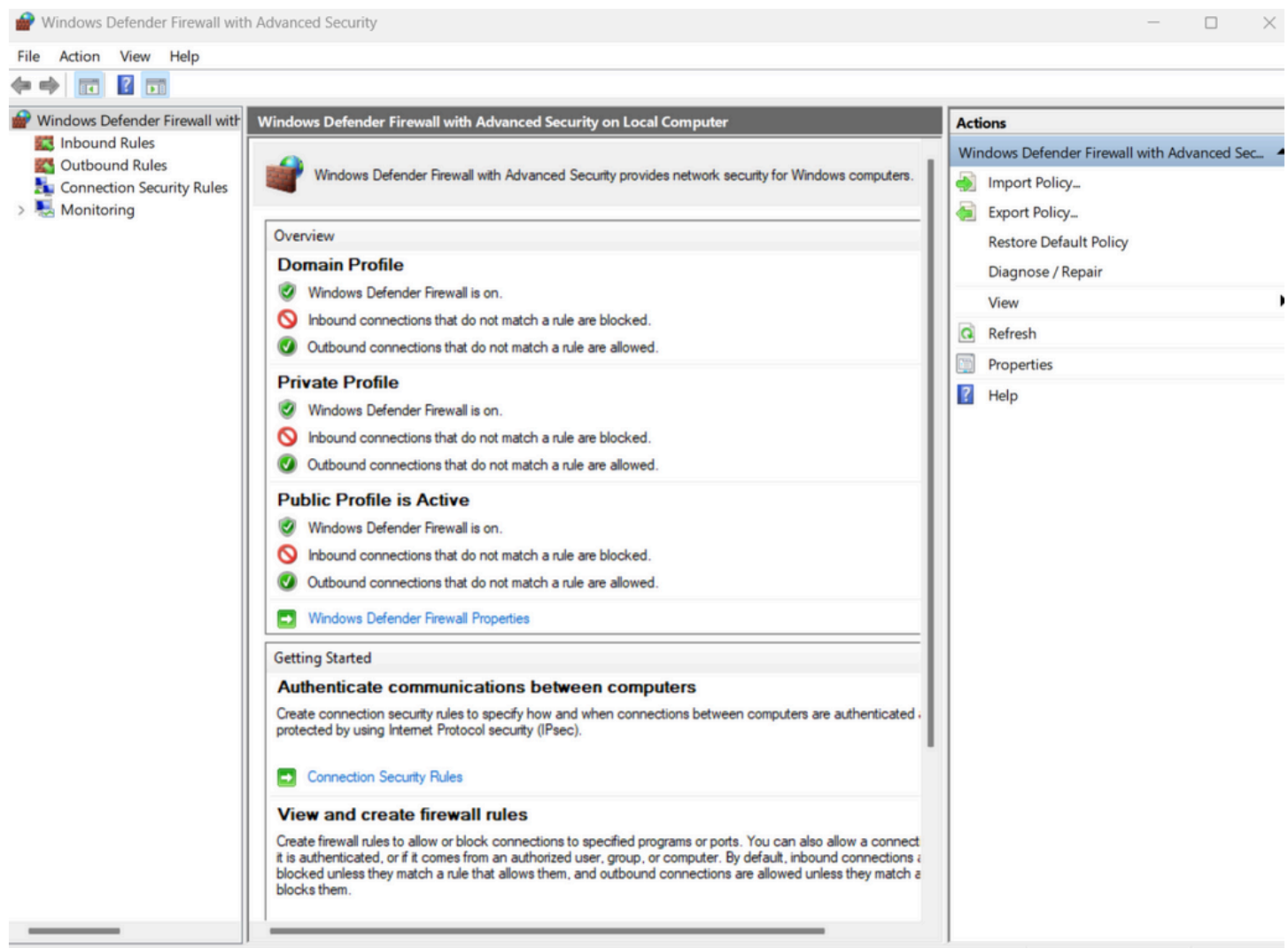


ELEVATE LABS CYBER SECURITY INTERNSHIP

Task-4:

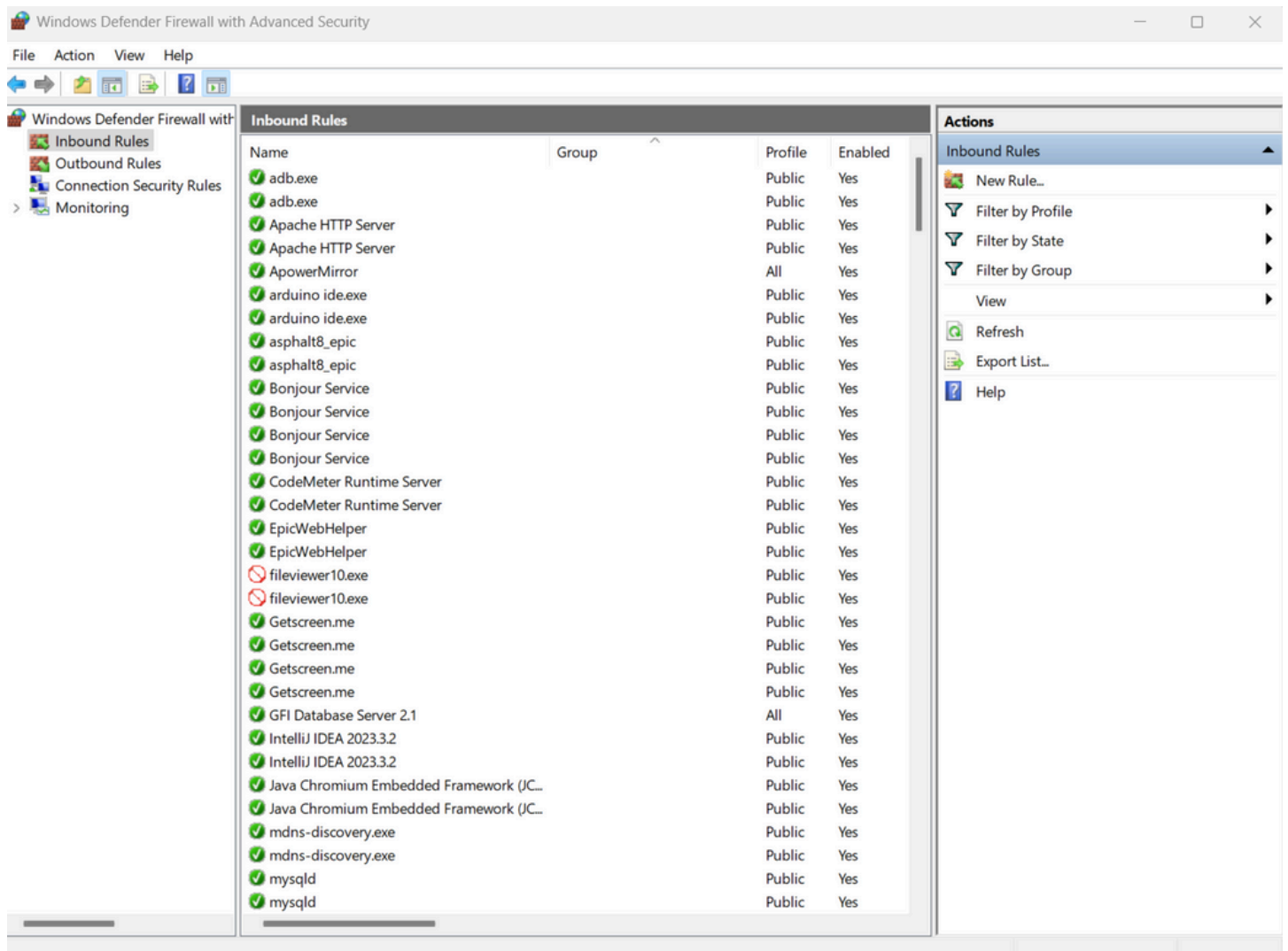
1)

using “windows+r and wf.msc



2)

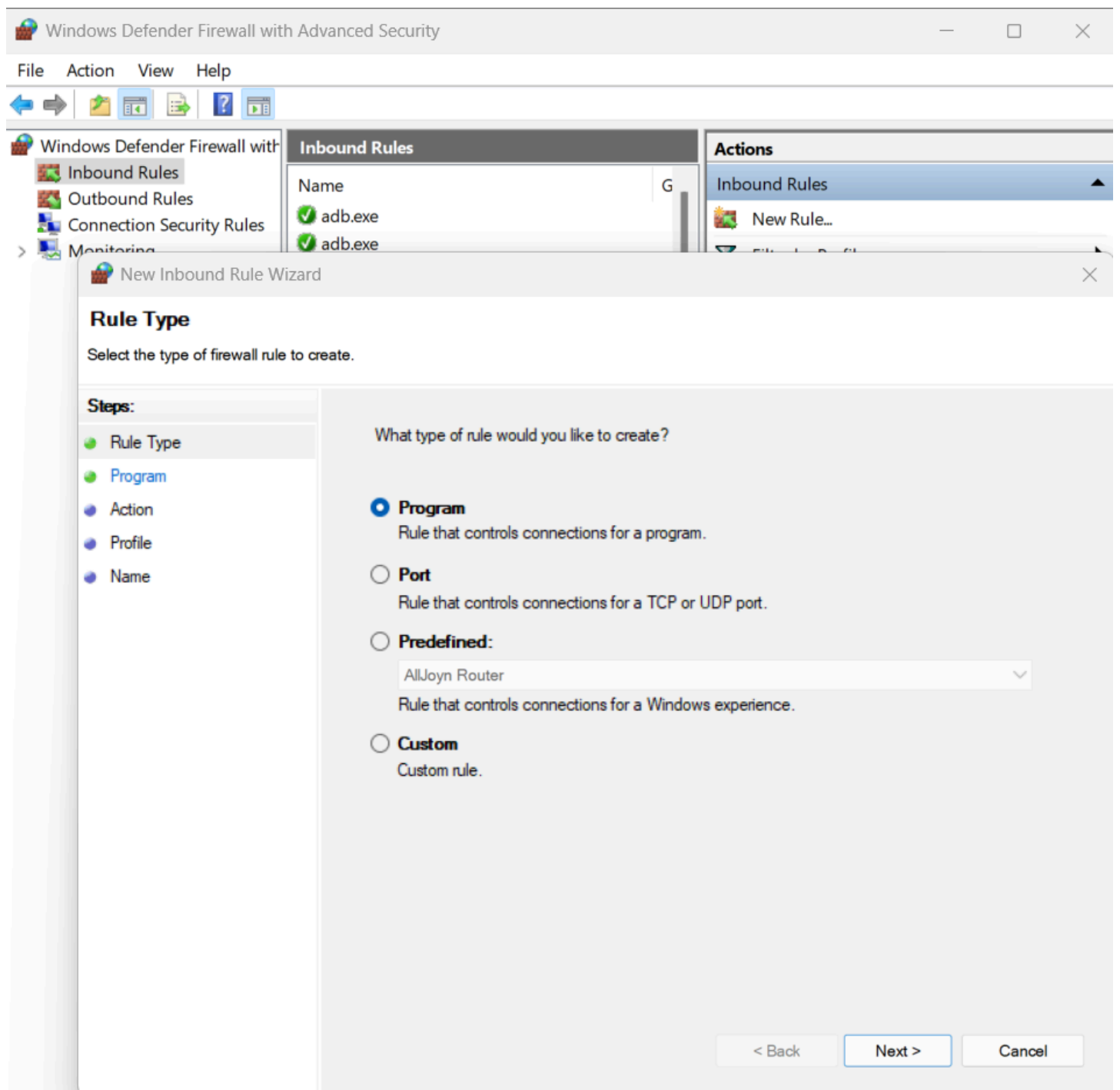
these are inbound rules of my firewall



as also can be seen outbound rules on left side of the panel

3)

Adding a new inbound rule using new rule button on right



I'll add a rule that port 22 (telnet) should be blocked

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:

23

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

Profile

Specify the profiles for which this rule applies.

Steps:

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

When does this rule apply?

- ☒ **Domain**
Applies when a computer is connected to its corporate domain.
- ☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.
- ☒ **Public**
Applies when a computer is connected to a public network location.

< Back Next > Cancel

Windows Defender Firewall with Advanced Security

File Action View Help

Windows Defender Firewall with Advanced Security

- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Name	Group	Profile	Enabled
Block Telnet		All	Yes
adb.exe		Public	Yes
adb.exe		Public	Yes
Apache HTTP Server		Public	Yes
Apache HTTP Server		Public	Yes
ApowerMirror		All	Yes
...		Public	Yes

Block telnet is the rule i added

4)

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

5)
allowing SSH port 22

New Inbound Rule Wizard

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

New Inbound Rule Wizard

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

Rule added

Firewall with Advanced Security

help

?

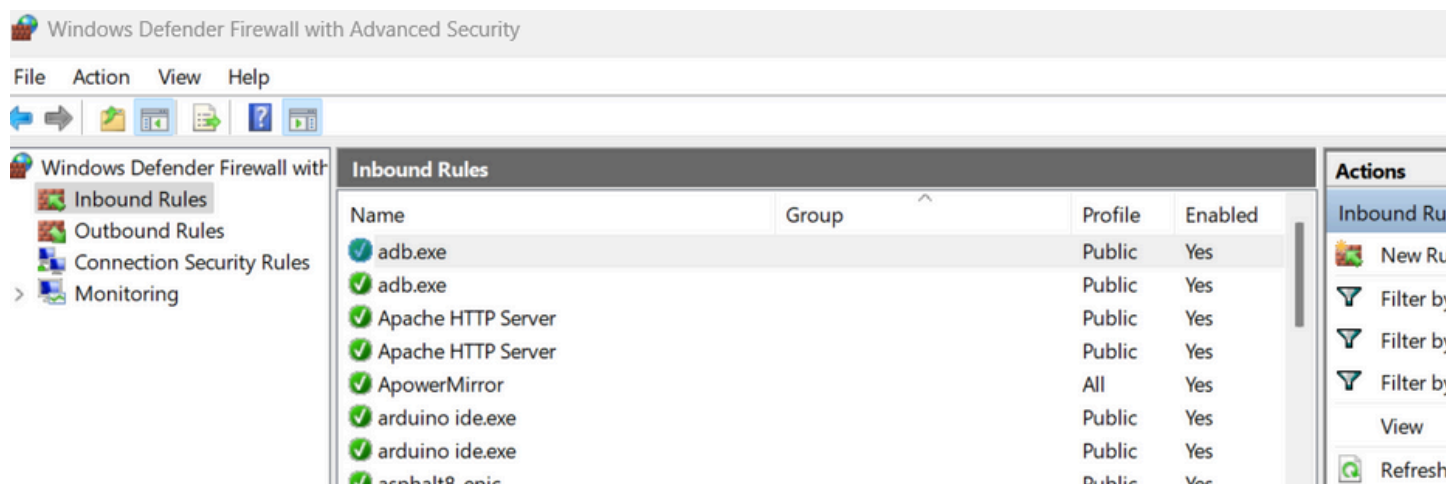
Firewall with

Advanced Security Rules

Inbound Rules				Action
Name	Group	Profile	Enabled	Inbound
Allow SSH		All	Yes	
Block Telnet		All	Yes	
adb.exe		Public	Yes	
adb.exe		Public	Yes	
Apache HTTP Server		Public	Yes	
Apache HTTP Server		Public	Yes	
ApowerMirror		All	Yes	

7)

Removed Telnet after using



8)

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