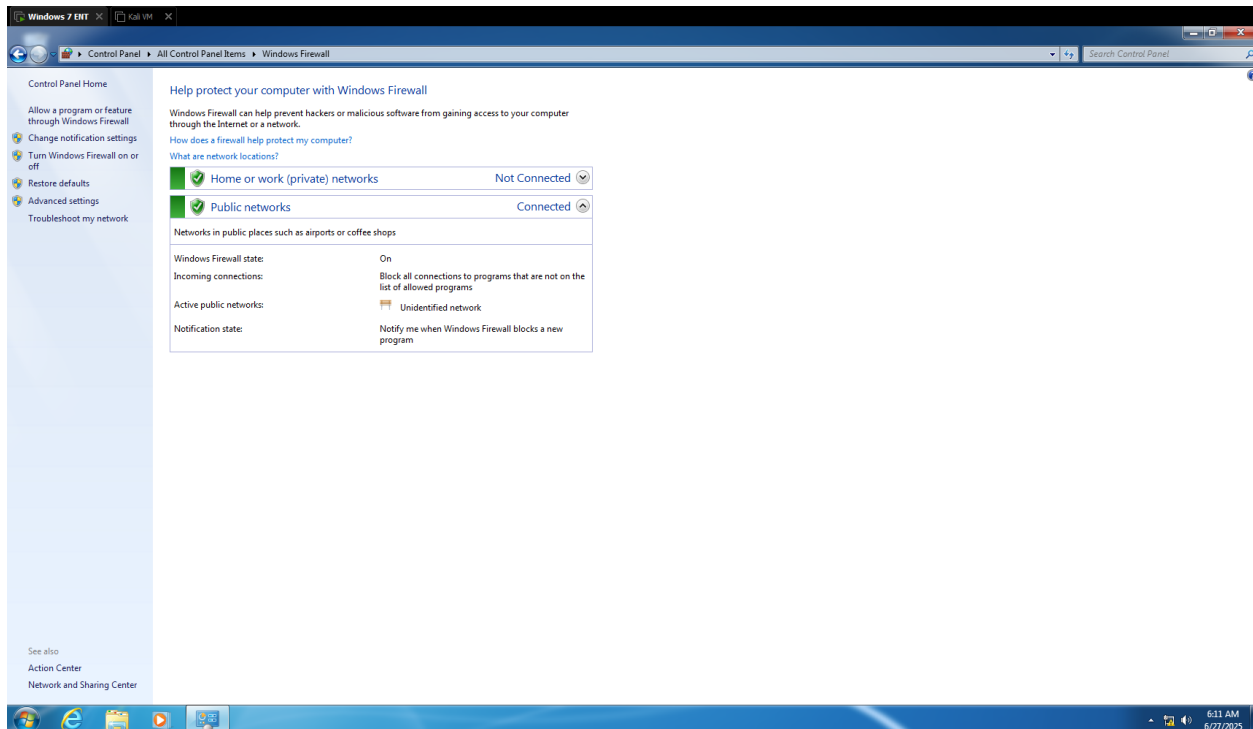


Elevate Labs Task 4

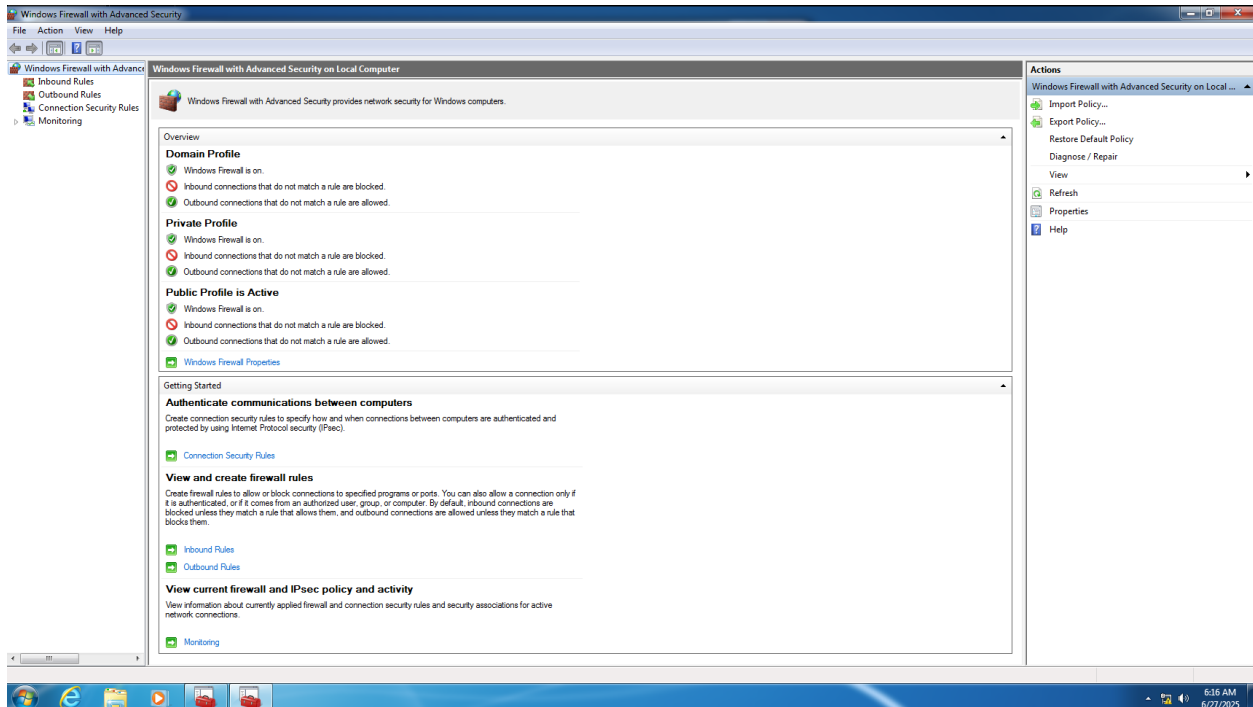
1) Open Firewall Configuration Tool

- Control Panel
- Windows Defender Firewall



2) List Current Firewall Rule

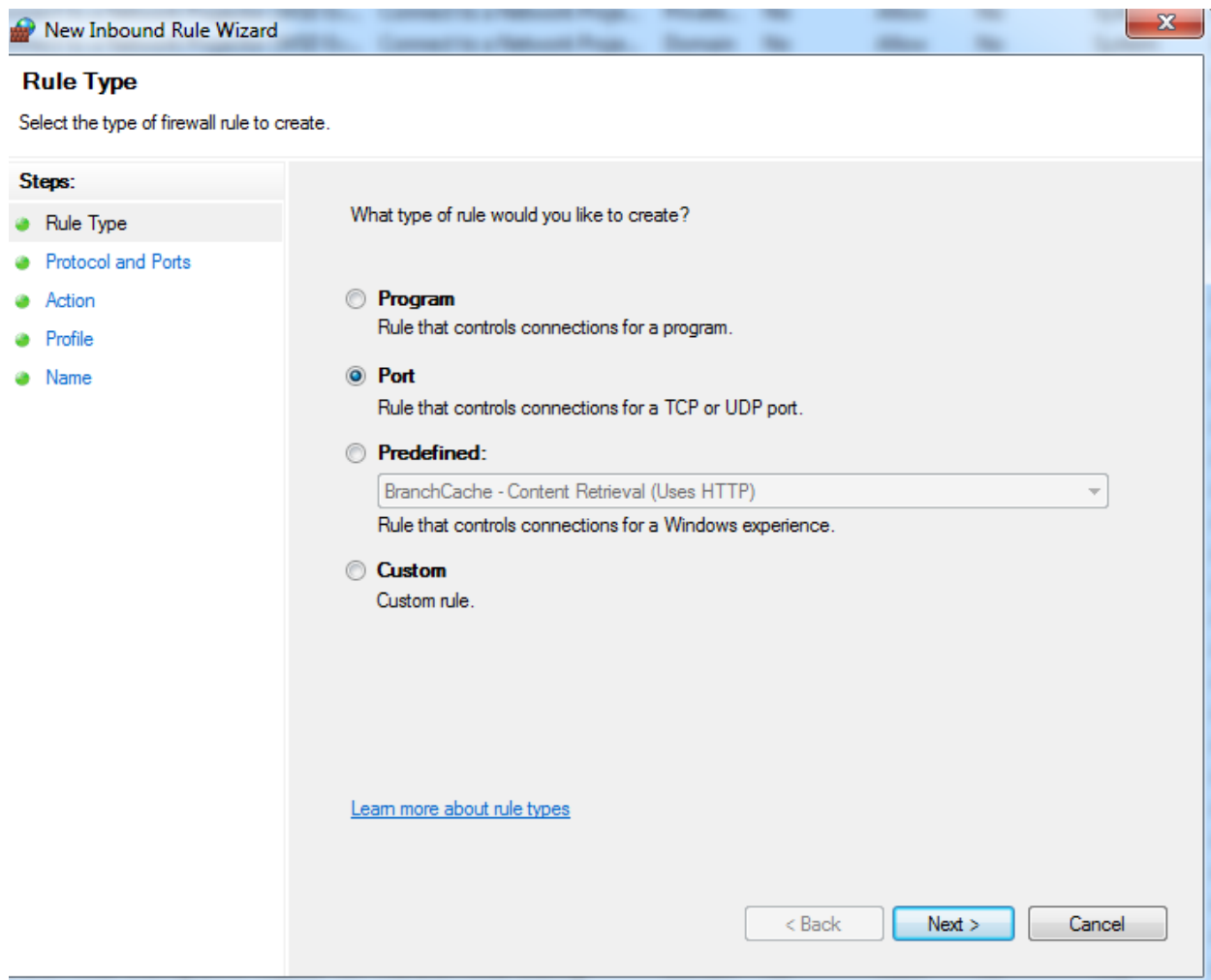
- Press Ctrl + R
- In the RUN dialogue box type wf.msc



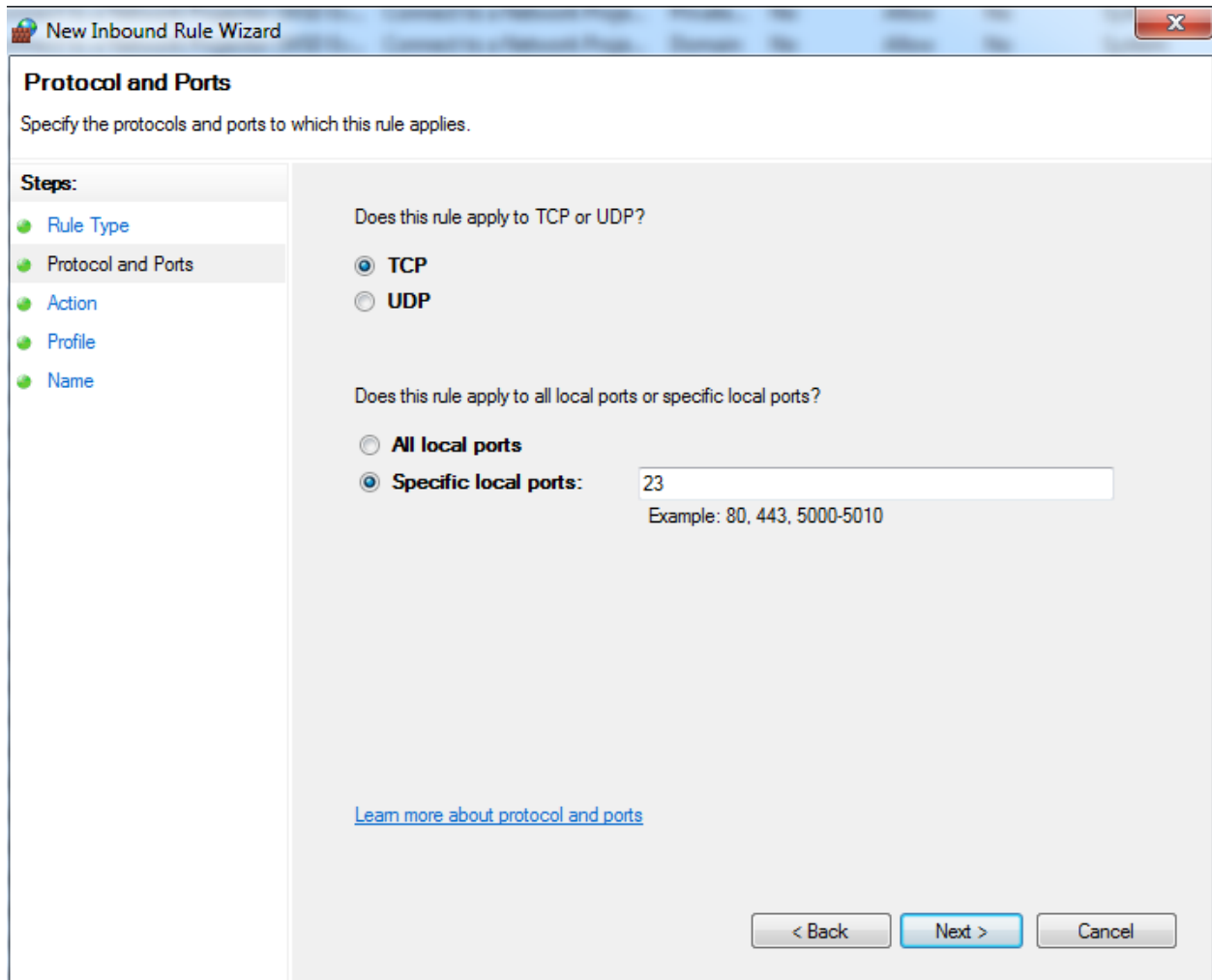
3) Adding an Telnet Rule to block Inbound Traffic

- Press Ctrl + R
- In the RUN dialogue box type wf.msc
- Navigate Through Inbound Rule
- Click on New Rule

:- After Clicking On New Rule Select the Port Rule Type



Then In the next Step we will set our port number 23. We have selected TCP rule because Telnet use TCP protocols



The image shows a screenshot of the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The window has a title bar with the text 'New Inbound Rule Wizard' and a close button. The main content area is titled 'Protocol and Ports' and includes the instruction 'Specify the protocols and ports to which this rule applies.' On the left side, there is a 'Steps:' panel with a list of steps: 'Rule Type', 'Protocol and Ports' (which is highlighted), 'Action', 'Profile', and 'Name'. The main area contains two questions with radio button options. The first question is 'Does this rule apply to TCP or UDP?' with 'TCP' selected. The second question is 'Does this rule apply to all local ports or specific local ports?' with 'Specific local ports:' selected. A text input field next to 'Specific local ports:' contains the value '23', and below it is an example text 'Example: 80, 443, 5000-5010'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A link 'Learn more about protocol and ports' is located at the bottom left of the main area.

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

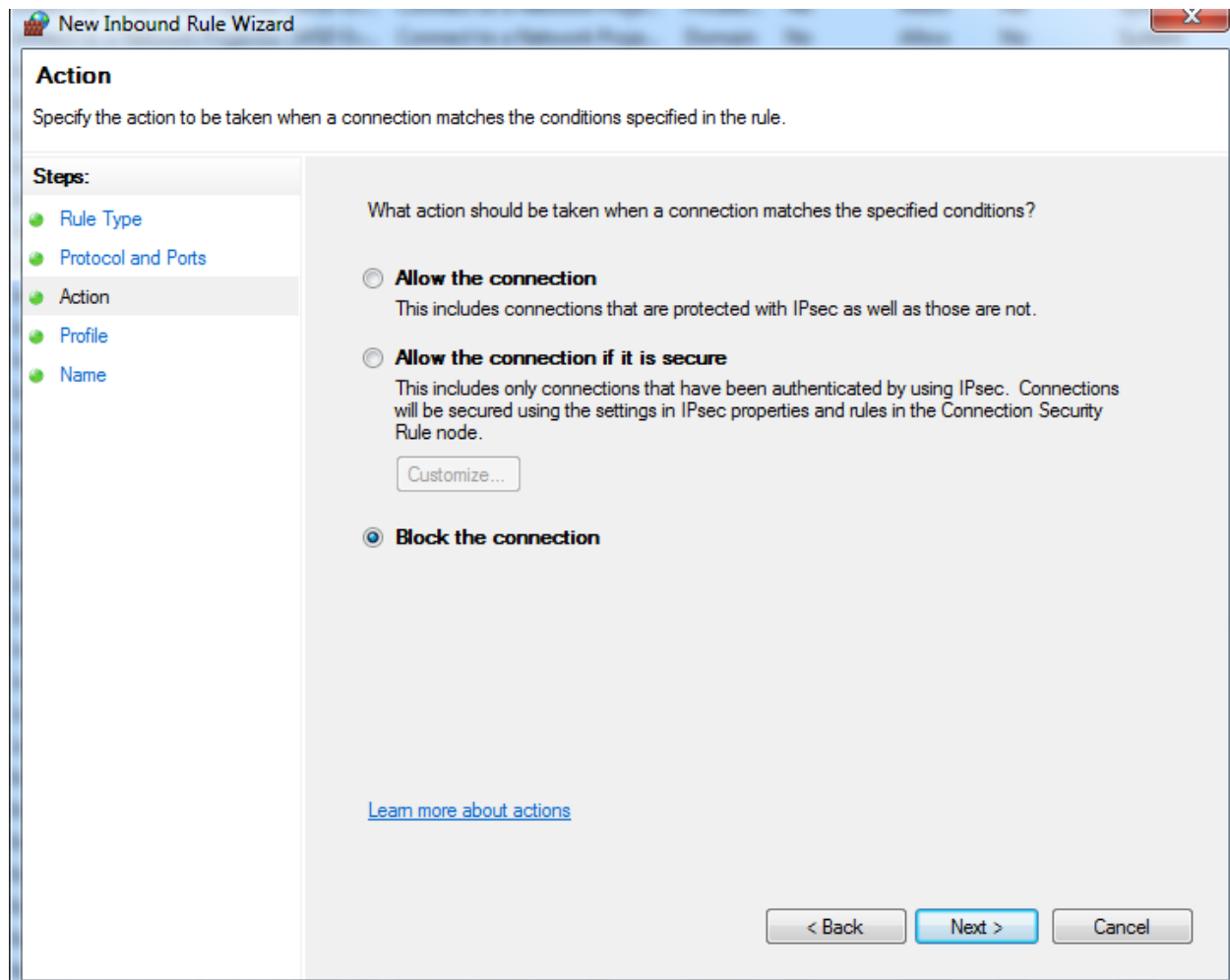
☒ Specific local ports:

Example: 80, 443, 5000-5010

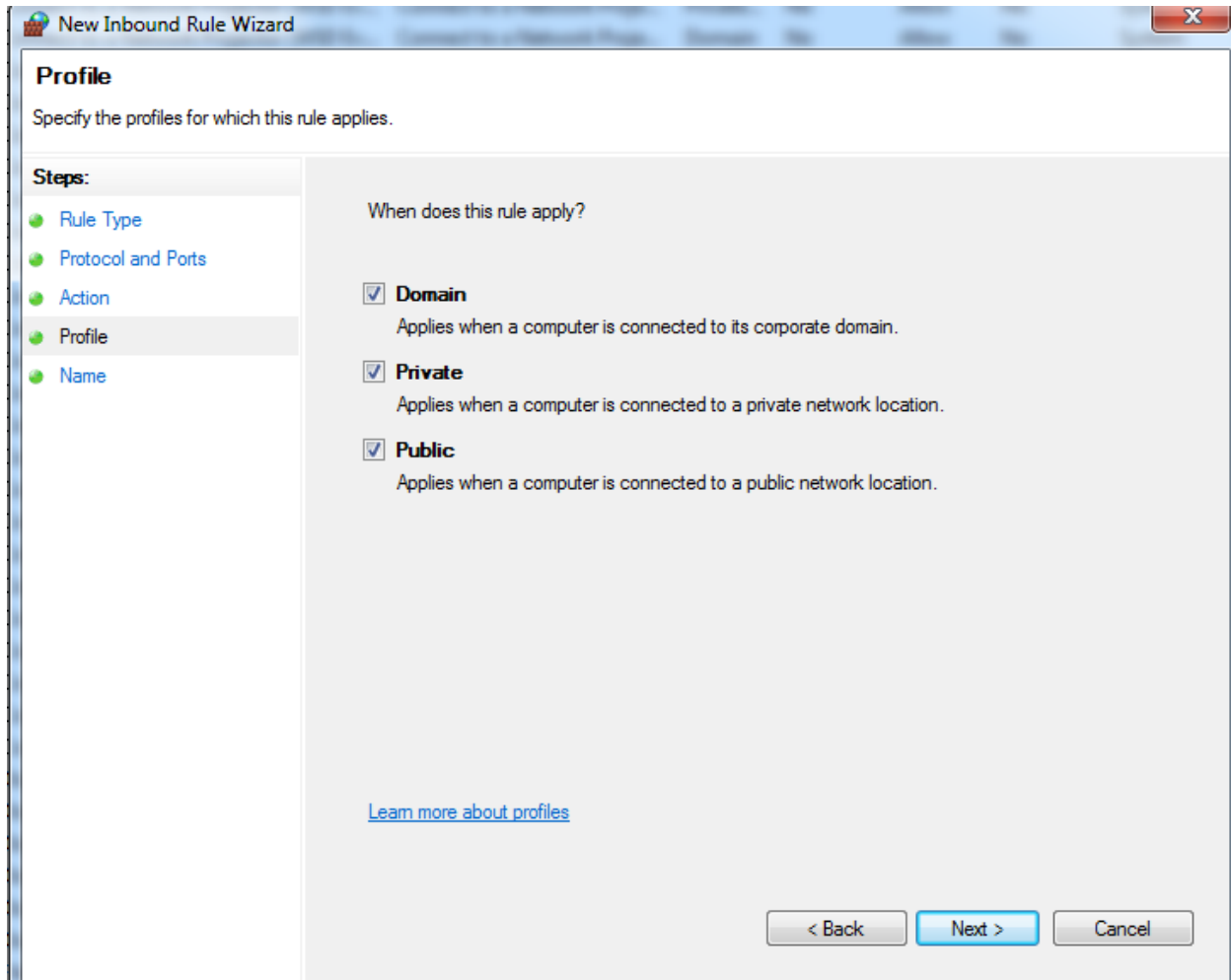
[Learn more about protocol and ports](#)

< Back Next > Cancel

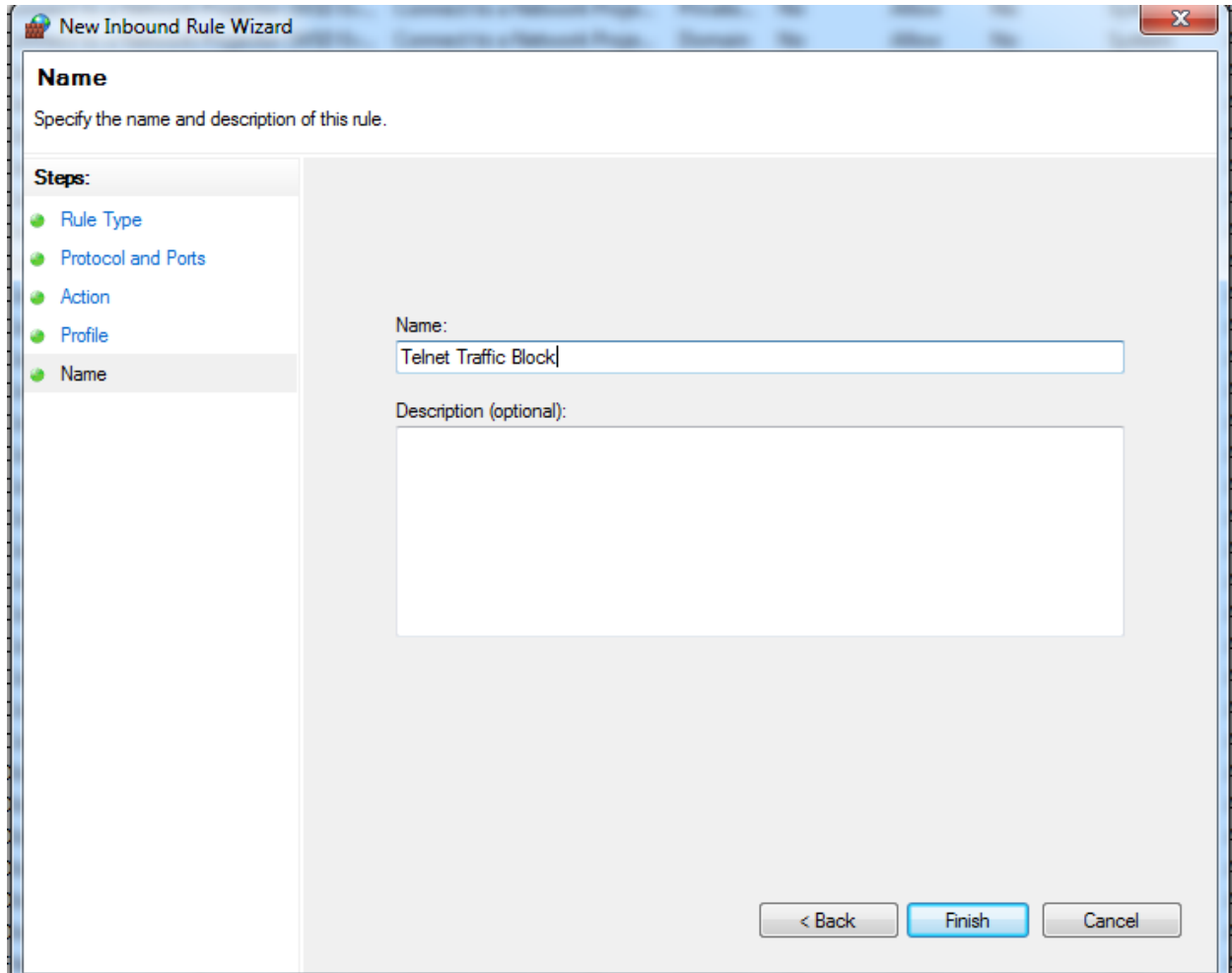
In the next step we will select block the connection option so that all services connecting to our Telnet client locally or remotely will be blocked



After that we will set the Profile type like Domain, Private, Public



Then we'll name our rule and apply it



The image shows a Windows-style dialog box titled "New Inbound Rule Wizard". It has a standard Windows window border with a close button (X) in the top right corner. The dialog is divided into two main sections. On the left is a "Steps:" sidebar with a list of five steps, each preceded by a green circular icon: "Rule Type", "Protocol and Ports", "Action", "Profile", and "Name". The "Name" step is currently selected and highlighted. The main area of the dialog is titled "Name" and contains the instruction "Specify the name and description of this rule." Below this instruction, there are two input fields. The first is labeled "Name:" and contains the text "Telnet Traffic Block". The second is labeled "Description (optional):" and is an empty text area. At the bottom right of the dialog, there are three buttons: "< Back", "Finish", and "Cancel". The "Finish" button is highlighted with a blue border.

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

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

Name:
Telnet Traffic Block

Description (optional):

< Back Finish Cancel

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

- To test it we have used Kali Linux

```
(kali@kali)-[~]
$ sudo nmap -Pn -p23 -sV 192.168.122.133
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-27 18:12 IST
Nmap scan report for 192.168.122.133
Host is up.

PORT      STATE      SERVICE VERSION
23/tcp    filtered  telnet

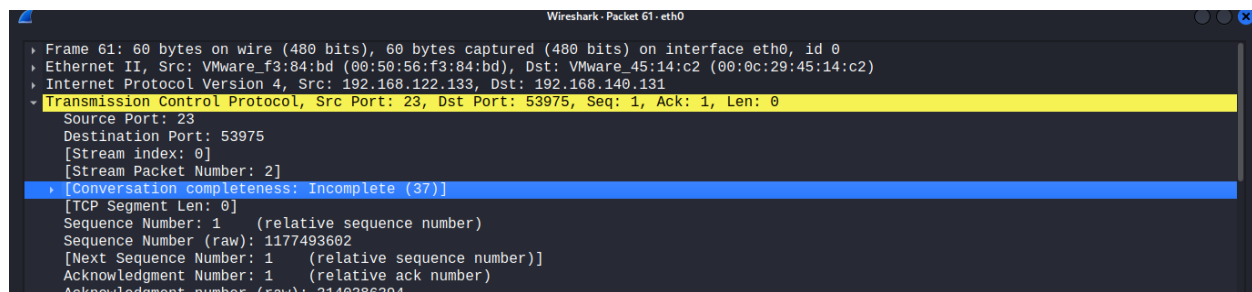
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.33 seconds
```

Here, 192.168.122.133 is the IP-Address of my Windows 7 VM machine on which, I have performed NMAP scan on specific port 23

➤ Here are the result in Wireshark

60	0.936049613	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.140.2? Tell 192.168.140.1
61	0.421907237	192.168.122.133	192.168.140.131	TCP	60	23 → 53975 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
62	0.436767783	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.140.2? Tell 192.168.140.1
63	0.279328662	192.168.140.1	224.0.0.251	MDNS	77	Standard query 0x0000 PTR _dosvc._tcp.local, "QU" question
64	0.000337133	fe80::5f1a:cd91:470b:4214	ff02::fb	MDNS	97	Standard query 0x0000 PTR _dosvc._tcp.local, "QU" question
65	0.268303239	192.168.122.133	192.168.140.131	TCP	60	23 → 53977 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

You can see that the Telnet port is continuously Resetting the request



We can see that conversation is incomplete between the HOST and the Target