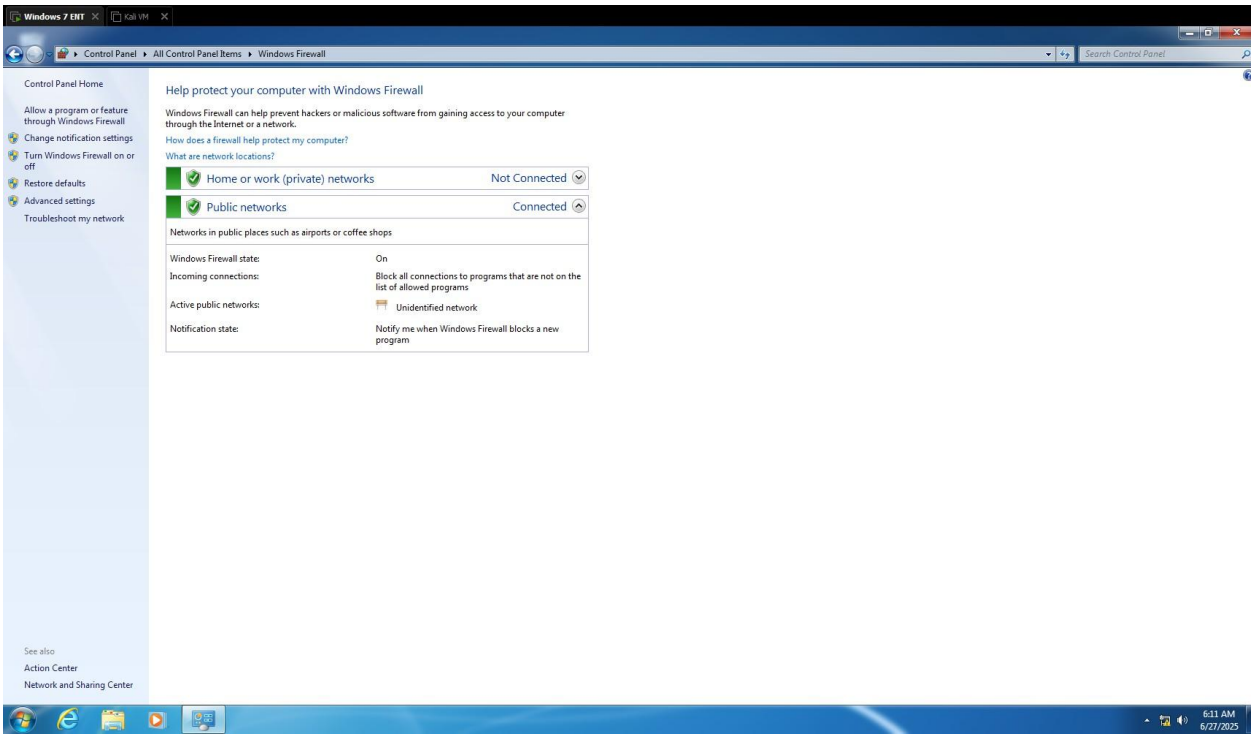
Elevate Labs Task 4

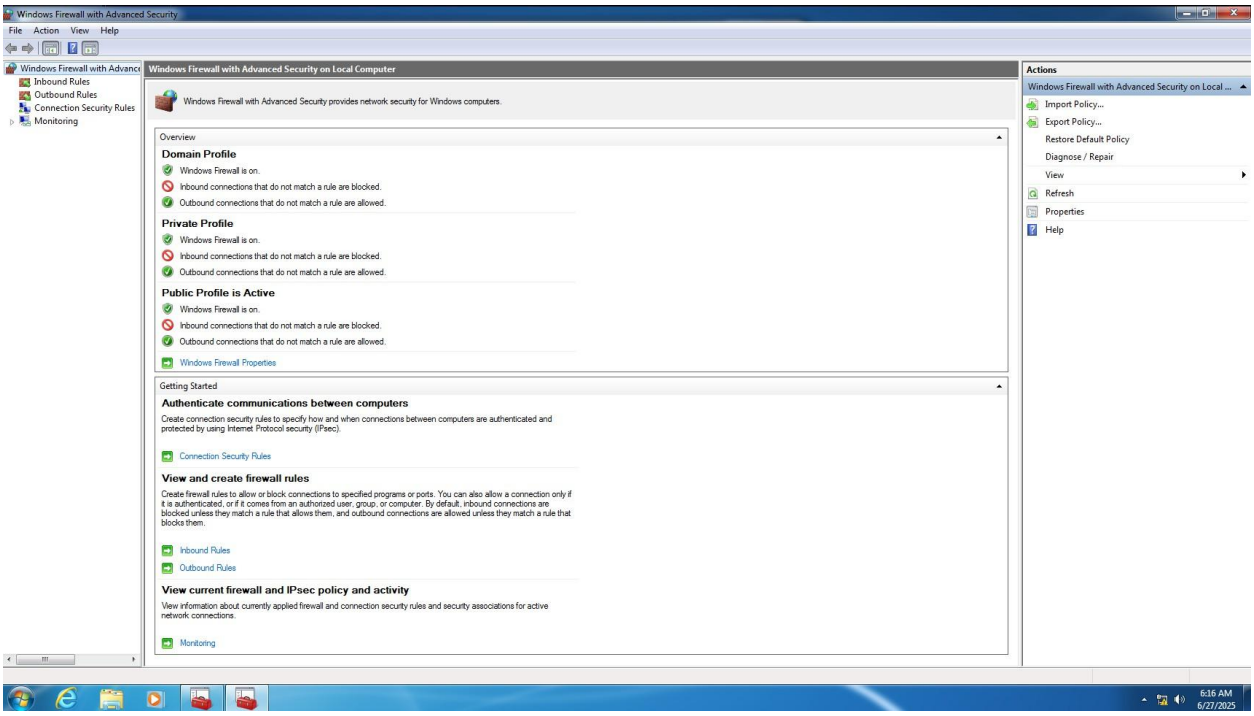
1) Open Firewall Configuration Tool

- Control Panel
- Windows Defender Firewall



2) List Current Firewall Rule

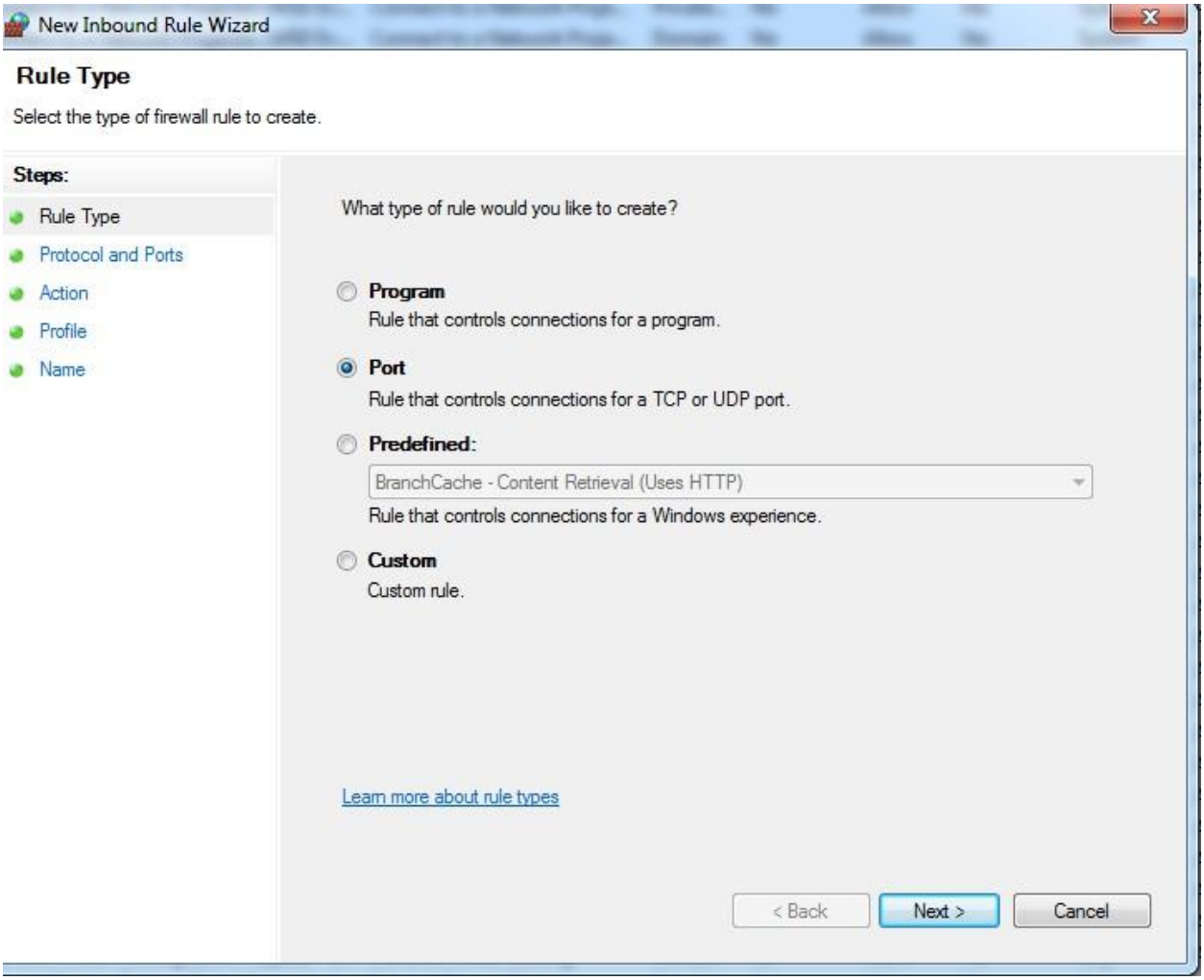
- Press Ctrl + R
- In the RUN dialogue box type *wf.msc*



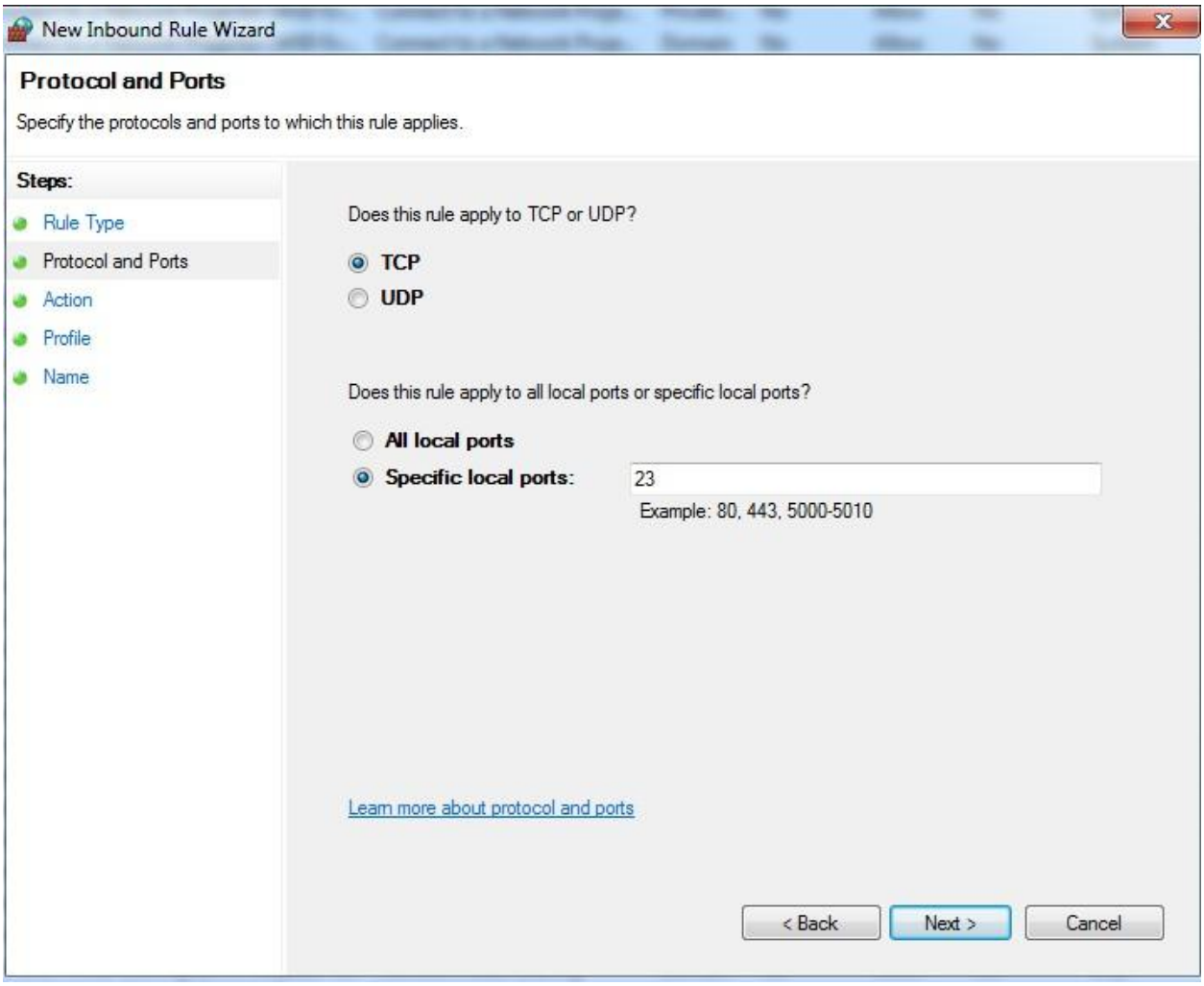
3) Adding an Telnet Rule to block Inbound Traffic

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

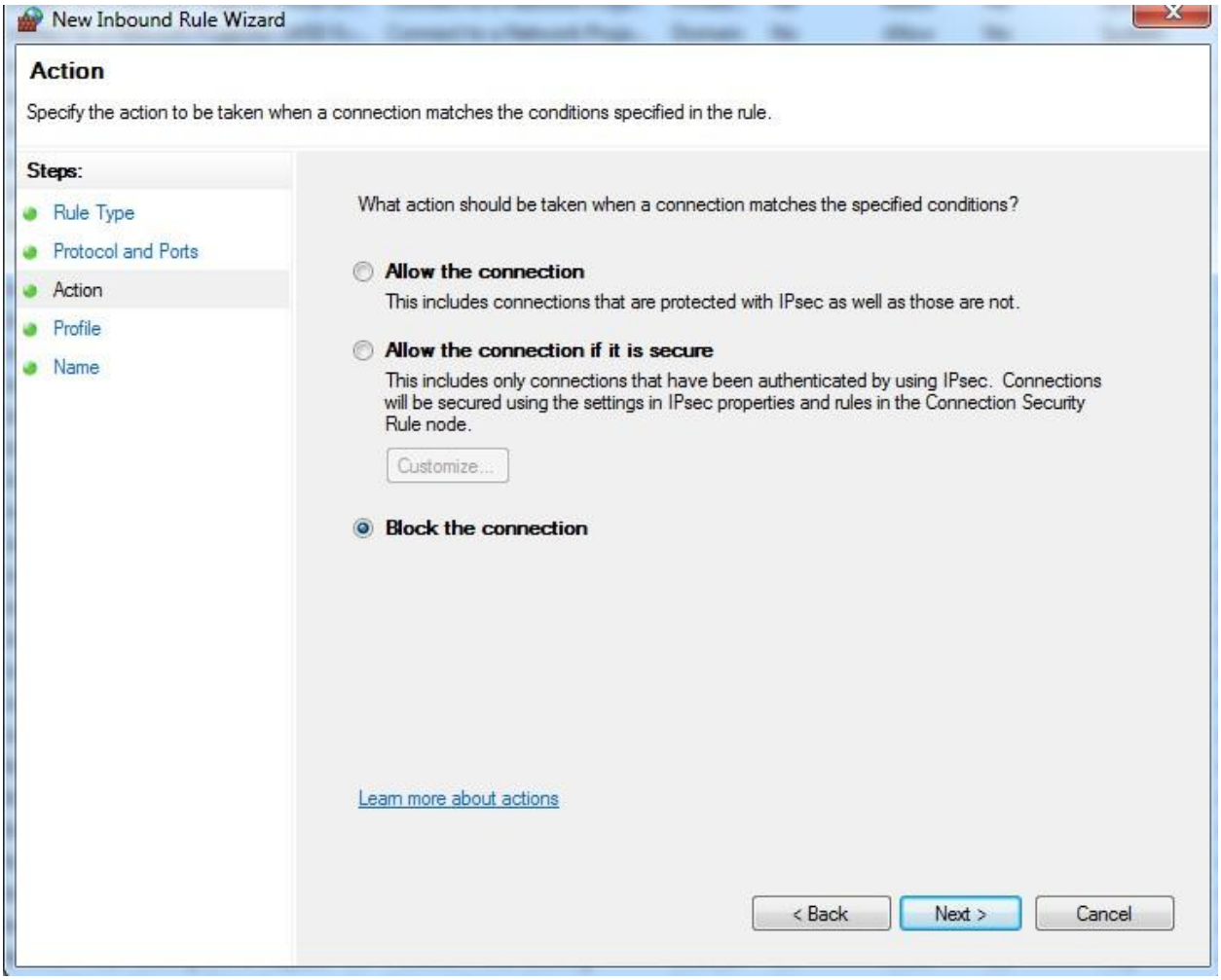
:- After Clicking On New Rule Select the Port Rule Type



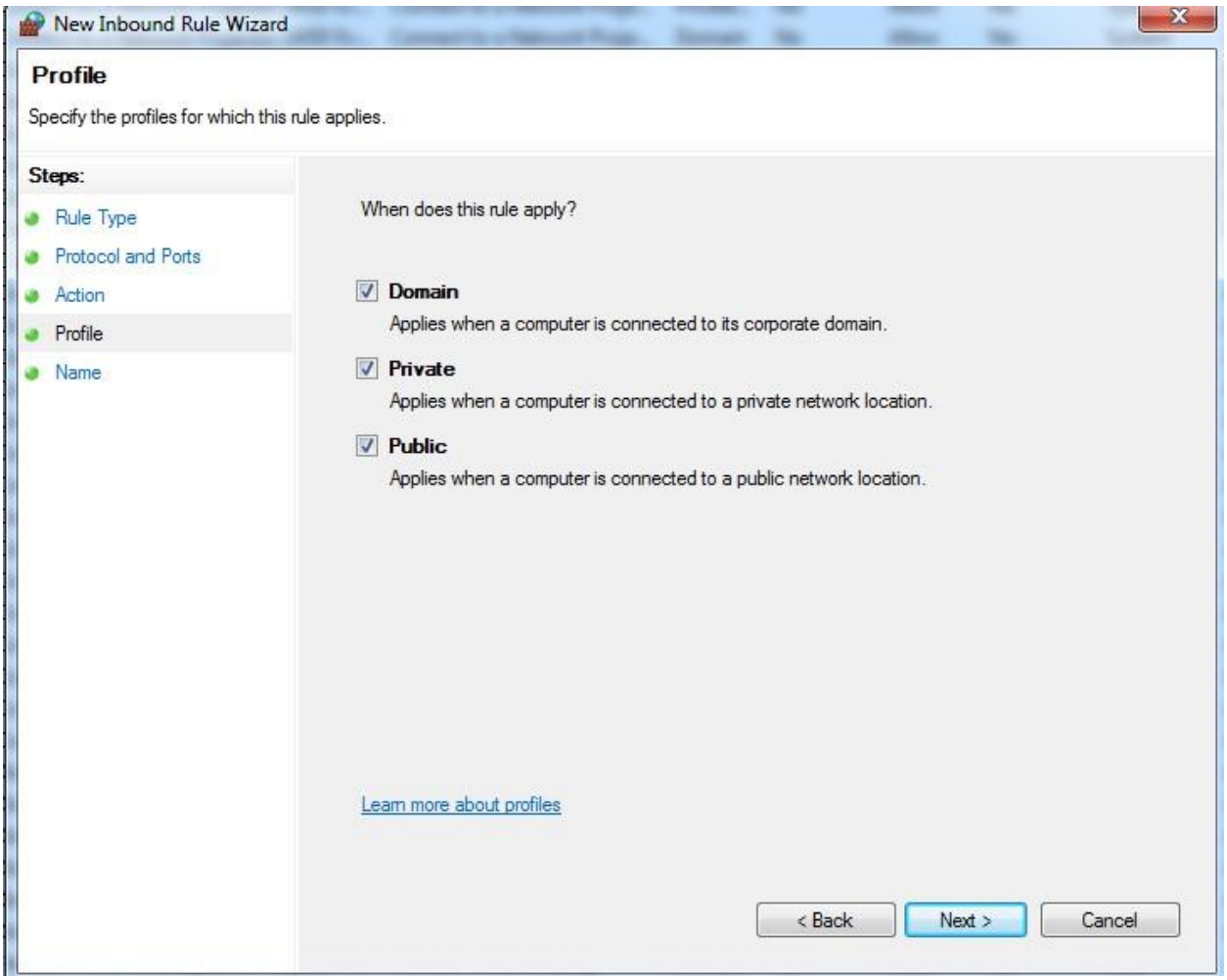
Then In the next Step we will set our port number 23. We have selected TCP rule because Telnet use TCP protocols



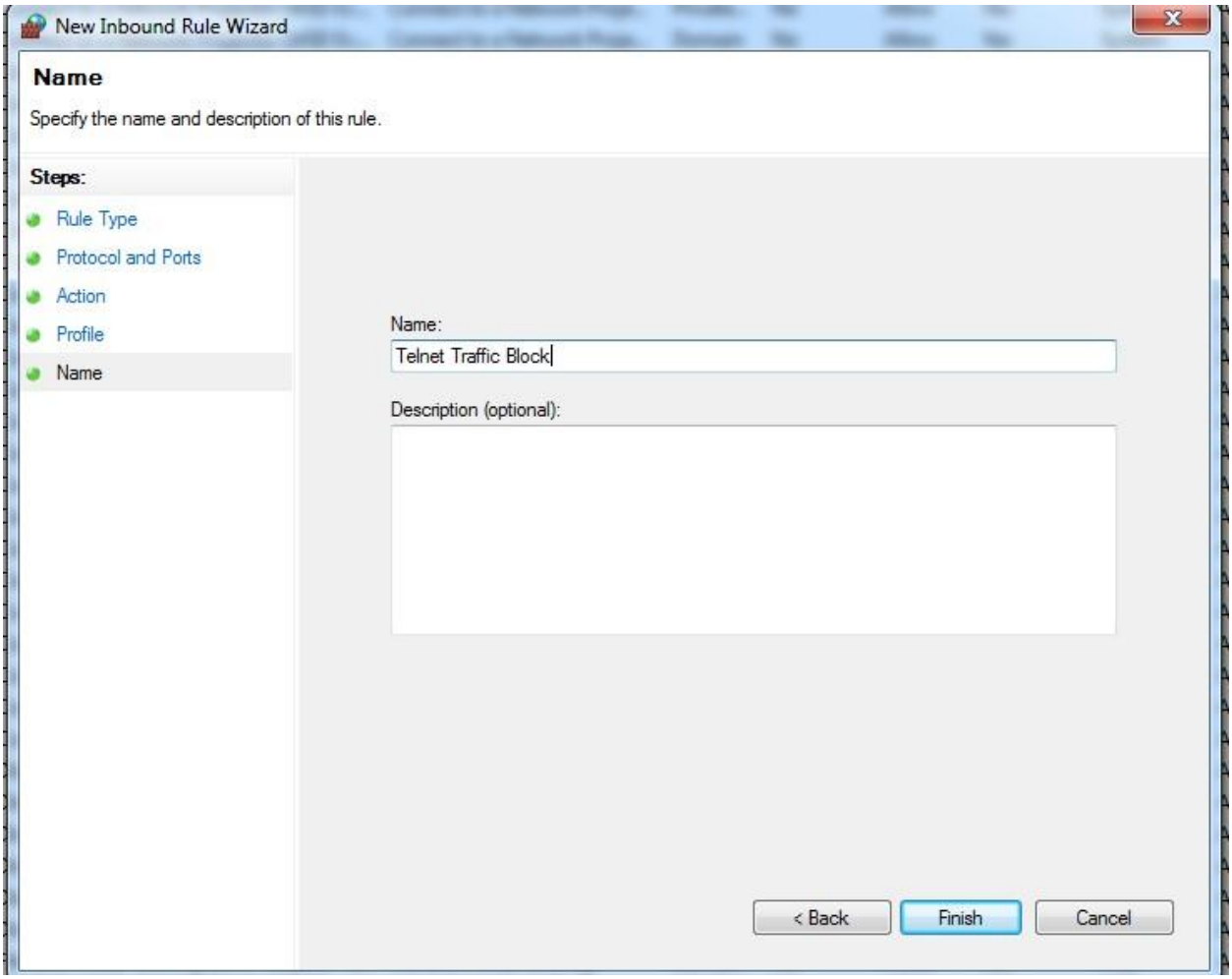
In the next step we will select block the connection option so that all services connecting to our Telnet client locally or remotely will be blocked



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



Then we'll name our rule and apply it



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

- To test it we have used Kali Linux

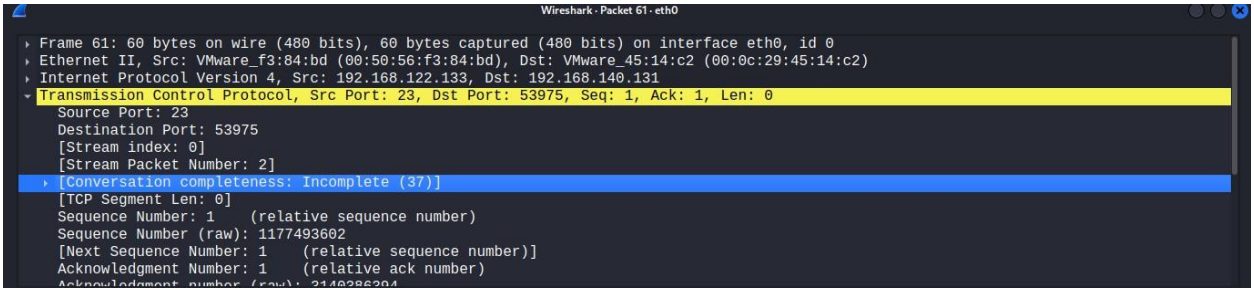
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -p23 -sV 192.168.122.133
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-27 18:12 IST
Nmap scan report for 192.168.122.133
Host is up.

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

5) Summary of how Firewall Filter Traffic

1. Packet Filtering (Stateless)

- Inspects each packet individually.
- Filters traffic based on IP address, port number, and protocol (TCP/UDP).
- Rules might look like:
    - Allow: 192.168.1.10:80 TCP
    - Block: Any:23 TCP (blocks Telnet)

Pros: Simple, fast

Cons: No context of packet state (e.g., if part of a conversation)

2. Stateful Inspection

- Tracks the state of active connections.
- Allows only packets that are part of an established session.
- Example:
    - If a device initiates a request to a website, the firewall will allow the response packets back, but will block unsolicited responses.

Pros: More secure

Cons: Requires more resources to track sessions

3. Proxy Firewall (Application Layer)

- Acts as an intermediary between two endpoints.
- Inspects application-level data (like HTTP, FTP).
- Can block specific content or keywords in traffic.

Pros: Deep inspection

Cons: Slower, more resource-intensive

4. Next-Generation Firewall (NGFW)

- Combines stateful inspection with deep packet inspection (DPI), intrusion prevention, malware filtering, and application awareness.
- Can identify and control applications (e.g., block Facebook or BitTorrent).
- Uses threat intelligence to update rules dynamically.

Pros: Very secure and intelligent

Cons: Expensive, complex to configure

Typical Filtering Criteria

- Source & Destination IP addresses
- Source & Destination ports
- Protocol (TCP/UDP/ICMP, etc.)
- Application (e.g., HTTP, DNS, Skype)
- Content (e.g., keywords in payloads)
- Time & Schedule