Task 4: Setup and use a firewall on Windows/Linux

Cybersecurity Lab Report

KANDI TEJASREE
ELEVATE LABS

Task 4:

Setup and Use a Firewall on Windows/Linux

Index:

Objective:

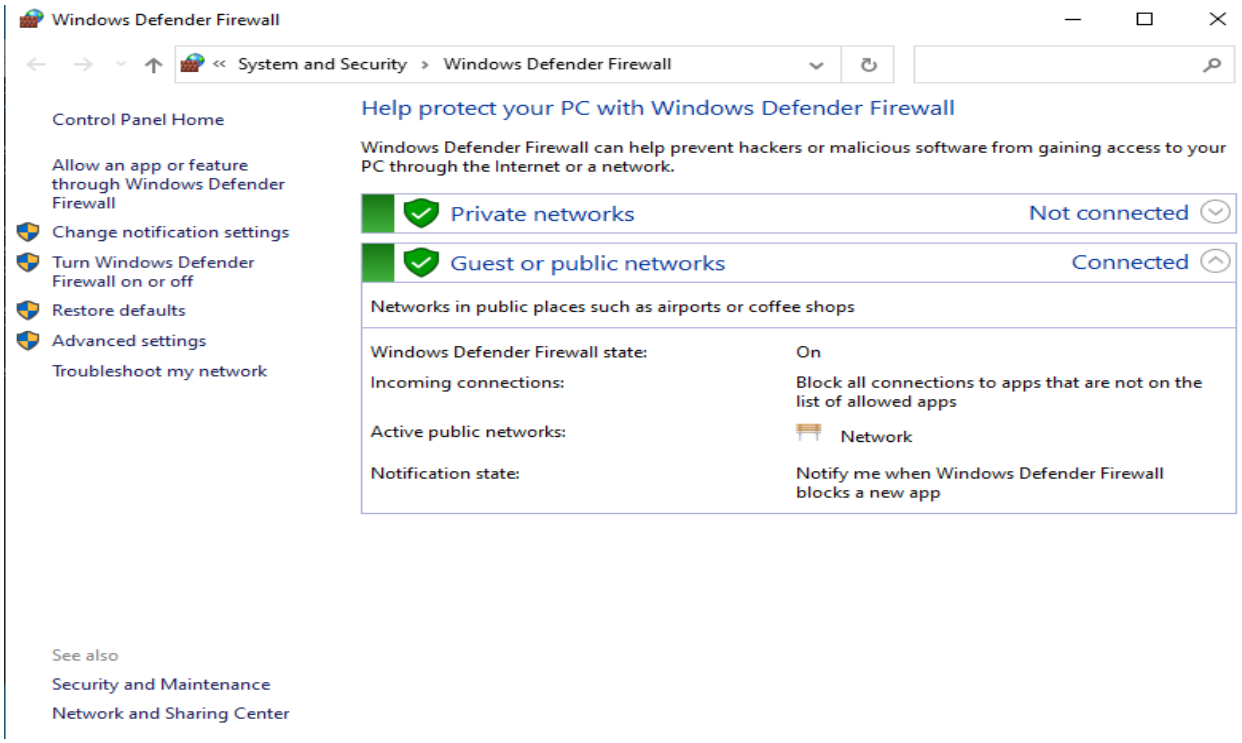
Configure and test basic firewall rules to allow or block traffic.

Tools Used:

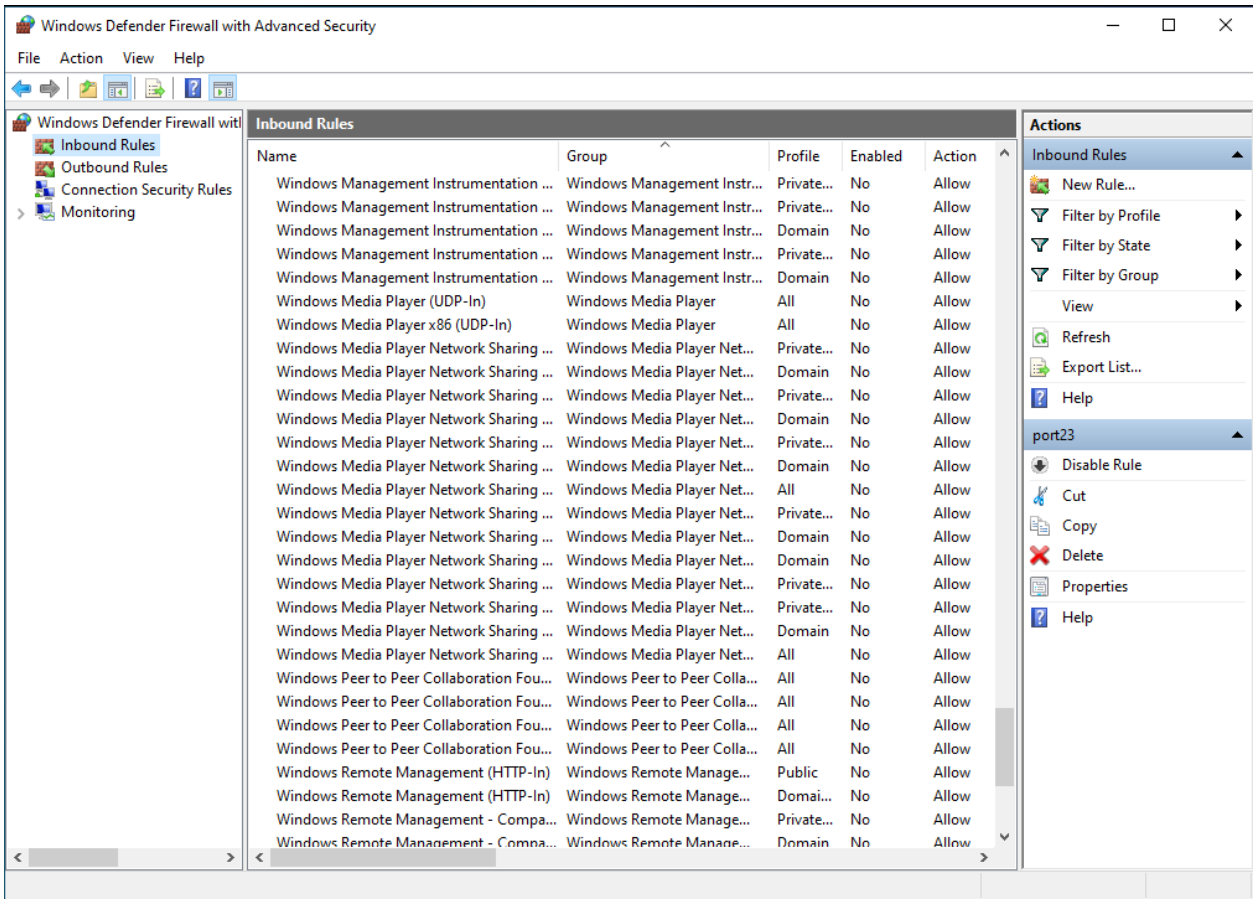
- VM Windows

Steps Performed: (on windows)

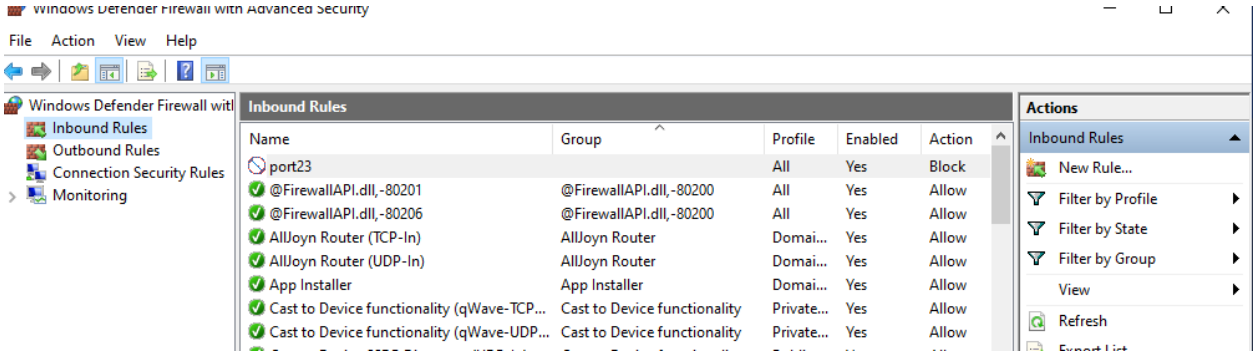
Open Firewall settings and search for **"Windows Defender Firewall" .** Click on **"Advanced Settings"**



Go to **"Inbound Rules"** and see list.

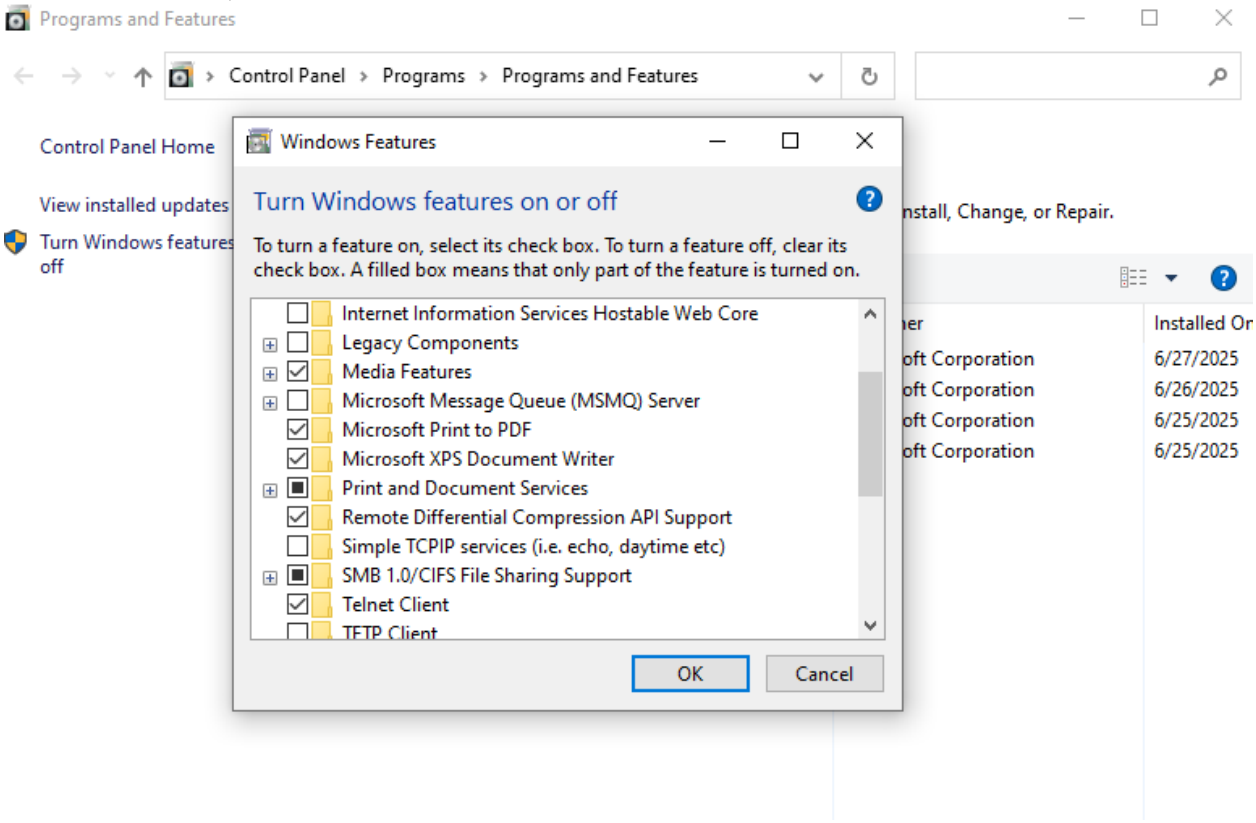


Right click Inbound Rules > New Rule > Port > TCP > Port 23 > Block.



Now install **"Telnet".**

- Press **Win + R**, type **appwiz.cpl,** and **press Enter.**
- Click on "Turn Windows features on or off" (left sidebar).
- In the list, scroll down and check **"Telnet Client".** Then click ok.



Open cmd prompt and run as administrator. And give command **"telnet localhost 23".**

```
C:\Windows\system32>telnet localhost23
Connecting To localhost23...Could not open connection to the host, on port 23: Connect failed

C:\Windows\system32>
```

Now it confirms that port 23(telnet) is being blocked. Firewall successfully blocked telnet traffic on port 23.

Conclusion:
In this task, we successfully configured firewall rules to control network traffic. By blocking inbound connections on port 23 (Telnet), and demonstrated how firewalls can effectively prevent access to insecure services and also tested and verified the rule using the Telnet command, which confirmed the firewall was functioning as expected. This task improved my understanding of basic firewall management and highlighted the importance of filtering network traffic to protect systems from unauthorized access.