Task – 4 Firewall Configuration and Testing Using UFW

Objective:

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

Tools Used:

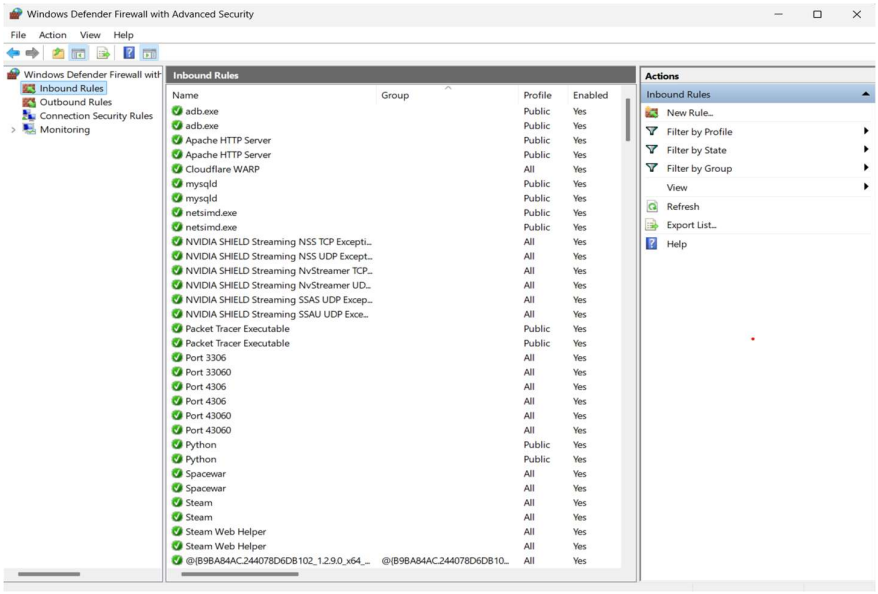
- Window

Open Firewall:

- Go to **Control Panel → System and Security → Windows Defender Firewall**
- Click **Advanced settings** (left panel)

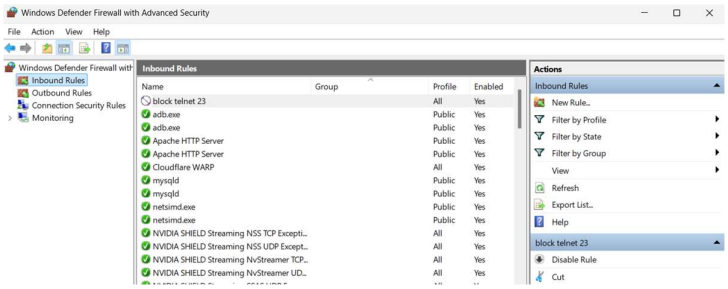
2. View current rules:

- In **Inbound Rules** panel



3. Block Port 23 (Telnet):

- Click **Inbound Rules → New Rule**
- Select **Port → TCP → Specific port: 23 → Block the connection**
- Name: "Block Telnet 23"



Tools:

- For Linux

Enable UFW:

bash
CopyEdit
sudo ufw enable

2. List current rules:

bash
CopyEdit
sudo ufw status numbered

3. Block inbound traffic on port 23 (Telnet):

bash
CopyEdit
sudo ufw deny 23

4. Test the rule:

- Use telnet localhost 23 (you may need to install telnet)

bash
CopyEdit
sudo apt install telnet
telnet localhost 23

Final rules check:

bash
CopyEdit
sudo ufw status verbose

Summary

How Firewall Filters Traffic?

UFW filters incoming and outgoing traffic by setting rules at the network level. By default, it blocks all unsolicited incoming traffic while allowing all outgoing traffic. Administrators can allow or deny traffic to specific ports, ensuring that only trusted services are accessible.