

PROJECT REPORT TASK 4

Objective:

To configure and test basic firewall rules using Windows Firewall or UFW on Linux. This includes adding rules to block or allow specific ports, verifying rule effectiveness, and understanding how firewalls filter network traffic to enhance system security.

Option 1: Windows Firewall

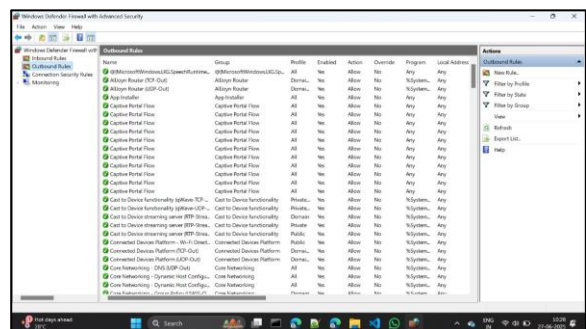
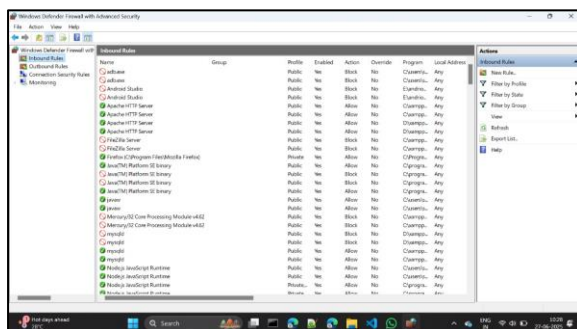
Step-by-Step:

1. Open Windows Firewall

- Search for “**Windows Defender Firewall with Advanced Security**” from the Start menu and open it.

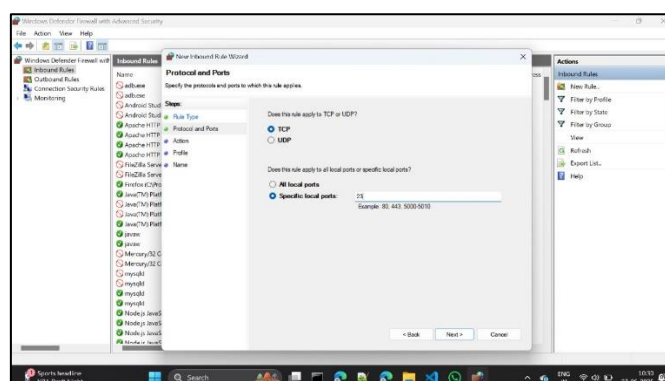
2. View Current Rules

- In the left pane, click **"Inbound Rules"** and **"Outbound Rules"** to see existing rules.

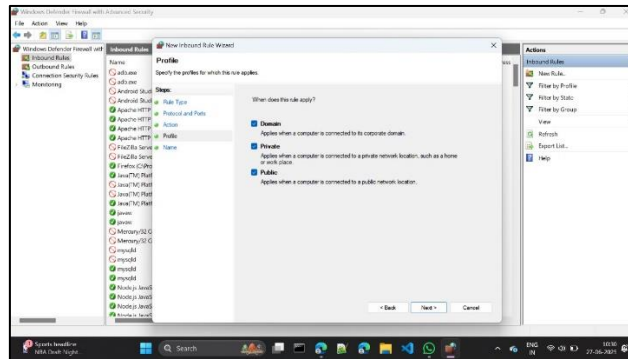


3. Block Inbound Traffic on Port 23 (Telnet)

- Click on **"Inbound Rules" > New Rule...**
- Select **Port**, click **Next**
- Select **TCP**, and enter **23** in "Specific local ports"



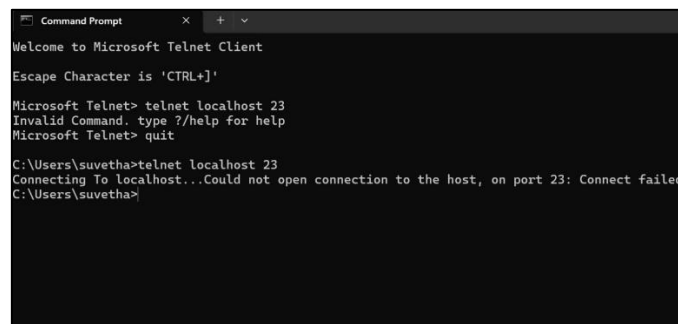
- Click **Next**, choose **Block the connection**
- Apply to **Domain, Private, Public** > Next



- Name the rule (e.g., "**Block Telnet Port 23**") > Finish

4. Test the Rule

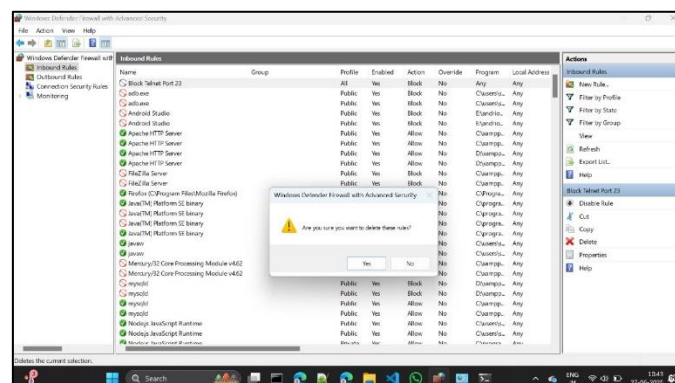
- Try using telnet localhost 23 (you may need to enable the Telnet client first).
- Connection should be **blocked**.
- Open CMD and check for connection.



5. Allow SSH (Optional for Linux, not relevant on Windows)

6. Remove the Test Rule

- Go to **Inbound Rules**, find "**Block Telnet Port 23**", right-click and choose **Delete**



7. Summary:

- Windows Firewall filters traffic based on port, application, protocol, and IP.
- It blocks/permits based on user-defined rules to control communication in/out of the system.

Option 2: Linux (Ubuntu/Debian) using UFW

Step-by-Step:

1. Install UFW (if not installed)

```
sudo apt update
```

```
sudo apt install ufw
```

[illegible]

2. Enable UFW

```
sudo ufw enable
```

3. Check Current Rules

```
sudo ufw status numbered
```

4. Block Port 23 (Telnet)

```
sudo ufw deny 23
```

5. Test the Rule

- Use telnet localhost 23 (install Telnet client if needed)

```
sudo apt install telnet
```

```
telnet localhost 23
```

```

File Actions Edit View Help
--kali@kali:~$
kali@kali:~$ sudo apt update
Get:1 http://deb.debian.org/debian bullseye InRelease [128 kB]
Get:2 http://kali.mirrors.pair.com bullseye InRelease [128 kB]
Get:3 http://kali.mirrors.pair.com bullseye/main amd64 Packages [60.9 kB]
Get:4 http://kali.mirrors.pair.com bullseye/main i386 Packages [55.1 kB]
Fetched 272 kB in 1s (250 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
10 packages can be upgraded. Run 'apt list --upgradable' to see them.

kali@kali:~$ sudo apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libpython3.9-minimal python3.9-minimal
Use 'apt autoremove' to remove them.
The following packages will be installed:
  net-tools
The following packages have security updates:
  libpython3.9-minimal python3.9-minimal
The following packages will be upgraded:
  net-tools
1 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 119 kB of archives.
After this operation, 119 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.mirrors.pair.com bullseye/main amd64 net-tools all 2:2.0.0-2 [119 kB]
Fetched 119 kB in 0s (11.9 MB/s)
debconf: delaying package configuration, since apt-utils is not installed
Selecting previously unselected package net-tools.
(Reading database ... 123456789 files and directories currently installed.)
Preparing to unpack .../net-tools_2:2.0.0-2_all.deb ...
Unpacking net-tools (2:2.0.0-2) ...
Setting up net-tools (2:2.0.0-2) ...
Processing triggers for libc-bin (2.31-0ubuntu1) ...

```

- It should **fail to connect**.

6. Allow SSH (Port 22)

```
sudo ufw allow 22
```

[illegible]

7. Remove Block Rule

```
sudo ufw delete deny 23
```

8. Example UFW Output:

Status: active

To	Action	From
--	-----	----
[1] 22	ALLOW IN	Anywhere
[2] 23	DENY IN	Anywhere
[3] 22 (v6)	ALLOW IN	Anywhere (v6)
[4] 23 (v6)	DENY IN	Anywhere (v6)

9. Summary:

- UFW (Uncomplicated Firewall) is a user-friendly interface to iptables.
- It allows/blocks traffic based on port, direction, and protocol.
- Helps in minimizing attack surface by controlling which ports/services are exposed.