PROJECT REPORT TASK 4

SETUP AND USE A FIREWALL ON WINDOWS/LINUX

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

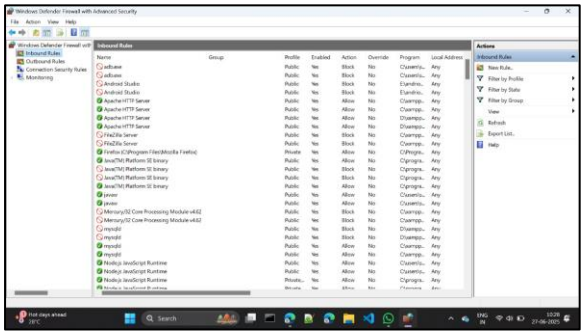
Step-by-Step:

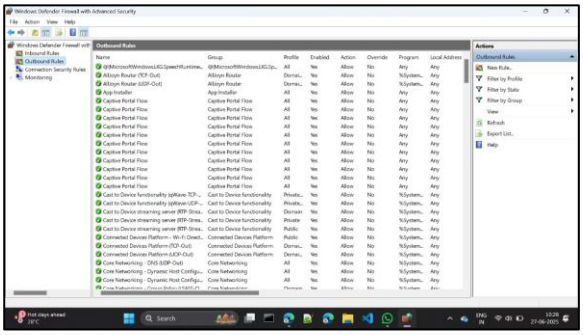
1. Open Windows Firewall

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

2. View Current Rules

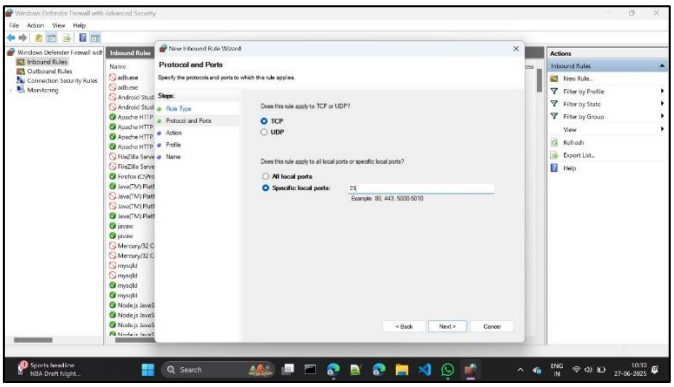
- In the left pane, click **"Inbound Rules"** and **"Outbound Rules"** to see existing rules.



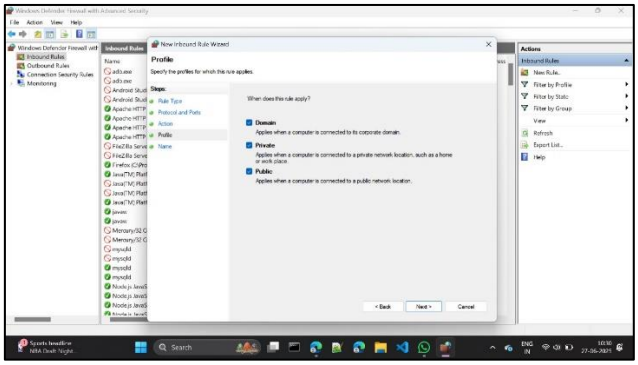


3. Block Inbound Traffic on Port 23 (Telnet)

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



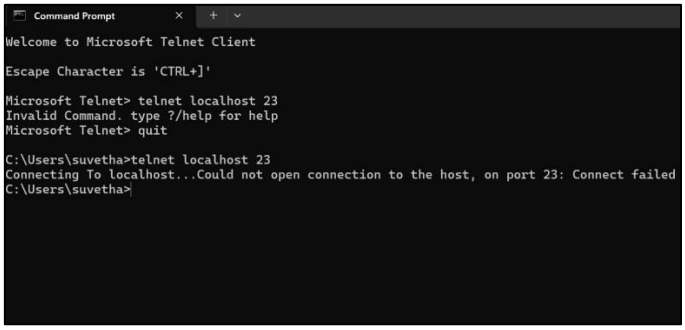
- Click **Next**, choose **Block the connection**
- Apply to **Domain, Private, Public** > Next



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

4. Test the Rule

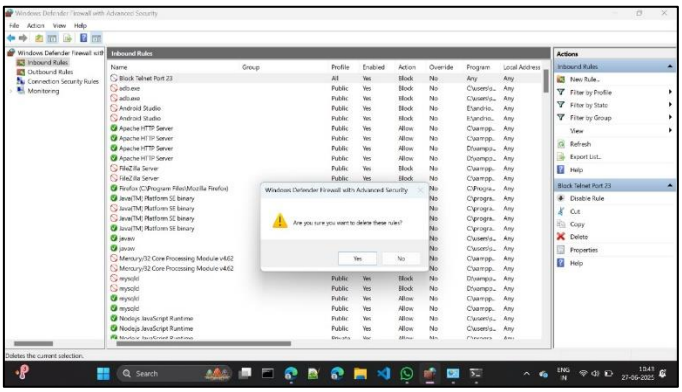
- Try using telnet localhost 23 (you may need to enable the Telnet client first).
- Connection should be **blocked**.
- Open CMD and check for connection.



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:

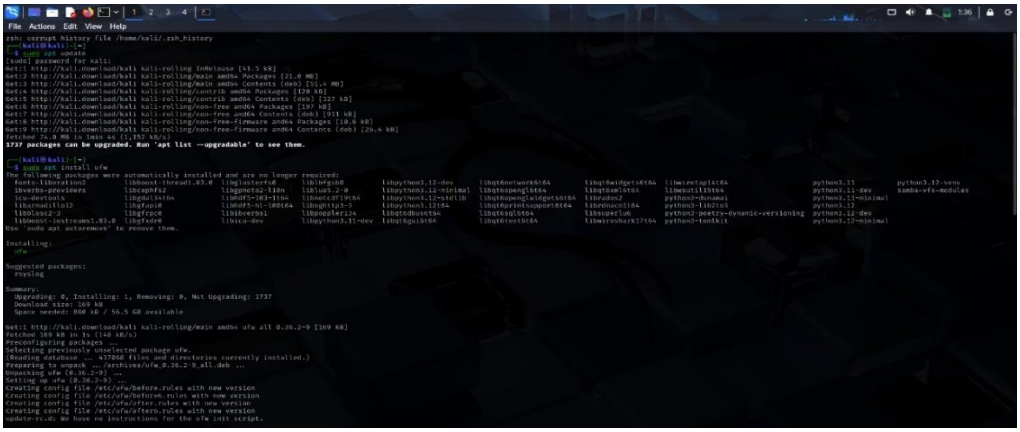
- Windows Firewall filters traffic based on port, application, protocol, and IP.
- It blocks/permits based on user-defined rules to control communication in/out of the system.

Option 2: Linux (Ubuntu/Debian) using UFW

Step-by-Step:

1. Install UFW (if not installed)

```
sudo apt update
sudo apt install ufw
```



2. Enable UFW

```
sudo ufw enable
```

3. Check Current Rules

```
sudo ufw status numbered
```

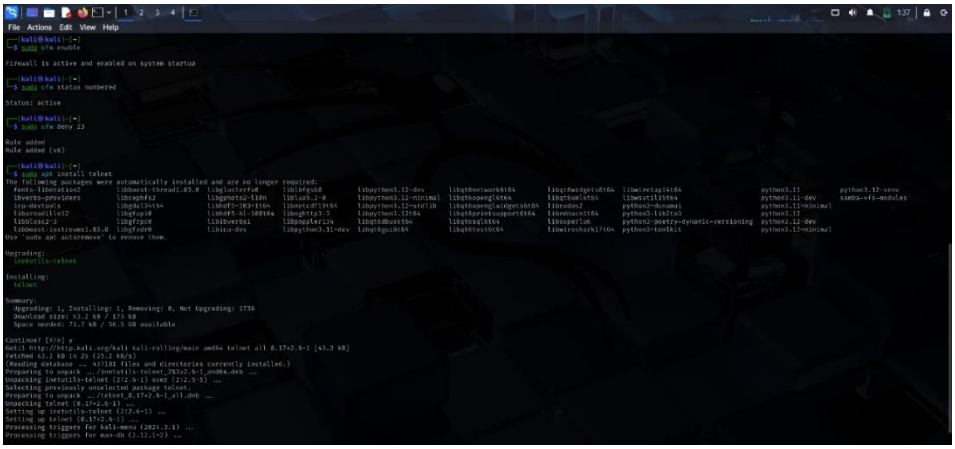
4. Block Port 23 (Telnet)

```
sudo ufw deny 23
```

5. Test the Rule

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

```
sudo apt install telnet
telnet localhost 23
```



- It should **fail to connect**.

6. Allow SSH (Port 22)

```
sudo ufw allow 22
```

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.