Task 4 – Basic Firewall Configuration and Testing

# Github :- https://github.com/posurabari/all-internship-tasks

# Objective

The objective of Task 4 is to understand basic firewall configuration and rule testing on both Windows and Linux systems. The task includes creating, testing, and deleting firewall rules, observing their impact, and documenting the process.

# Tools Used

- Windows Command Prompt / PowerShell  
- Windows Defender Firewall with Advanced Security  
- Linux UFW (Uncomplicated Firewall)  
- Nmap (for testing)

# Firewall Configuration on Windows

1. Open Command Prompt as Administrator.

2. Create a new firewall rule to block port 80:  
 `New-NetFirewallRule -DisplayName "Block Port 80" -Direction Inbound -LocalPort 80 -Protocol TCP -Action Block`

3. Test the rule using browser or `Test-NetConnection` (if available).

4. Delete the rule after testing:  
 `Remove-NetFirewallRule -DisplayName "Block Port 80"`

5. Observed behavior: Port 80 connection was blocked, then restored after rule deletion.

# Firewall Configuration on Linux (Kali)

1. Open terminal with sudo access.

2. Enable UFW (if not already enabled):  
 `sudo ufw enable`

3. Add rule to block port 80:  
 `sudo ufw deny 80`

4. Test with browser or Nmap scan.

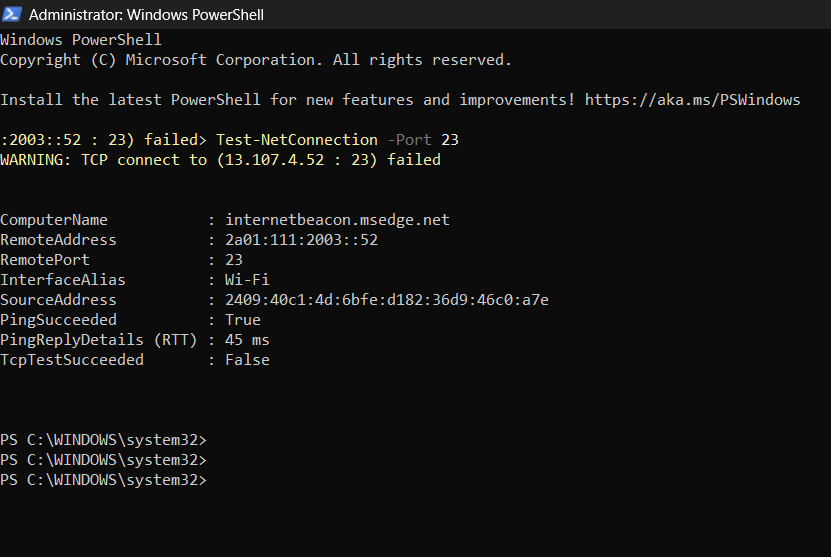
5. Remove rule:  
 `sudo ufw delete deny 80`

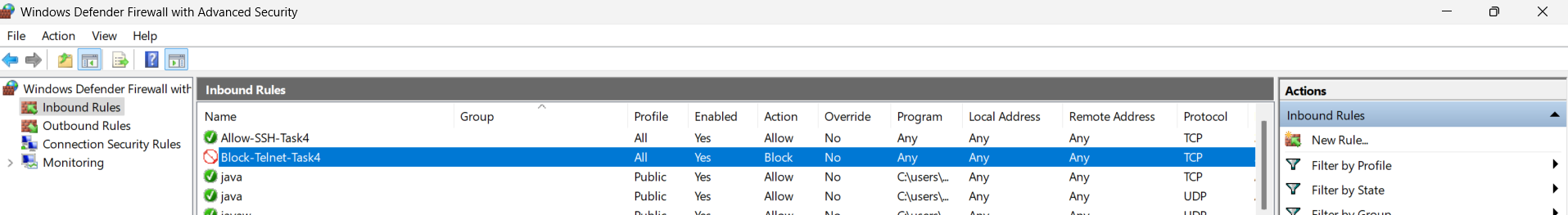
6. Observed behavior: Port 80 was blocked, then allowed after rule was removed.

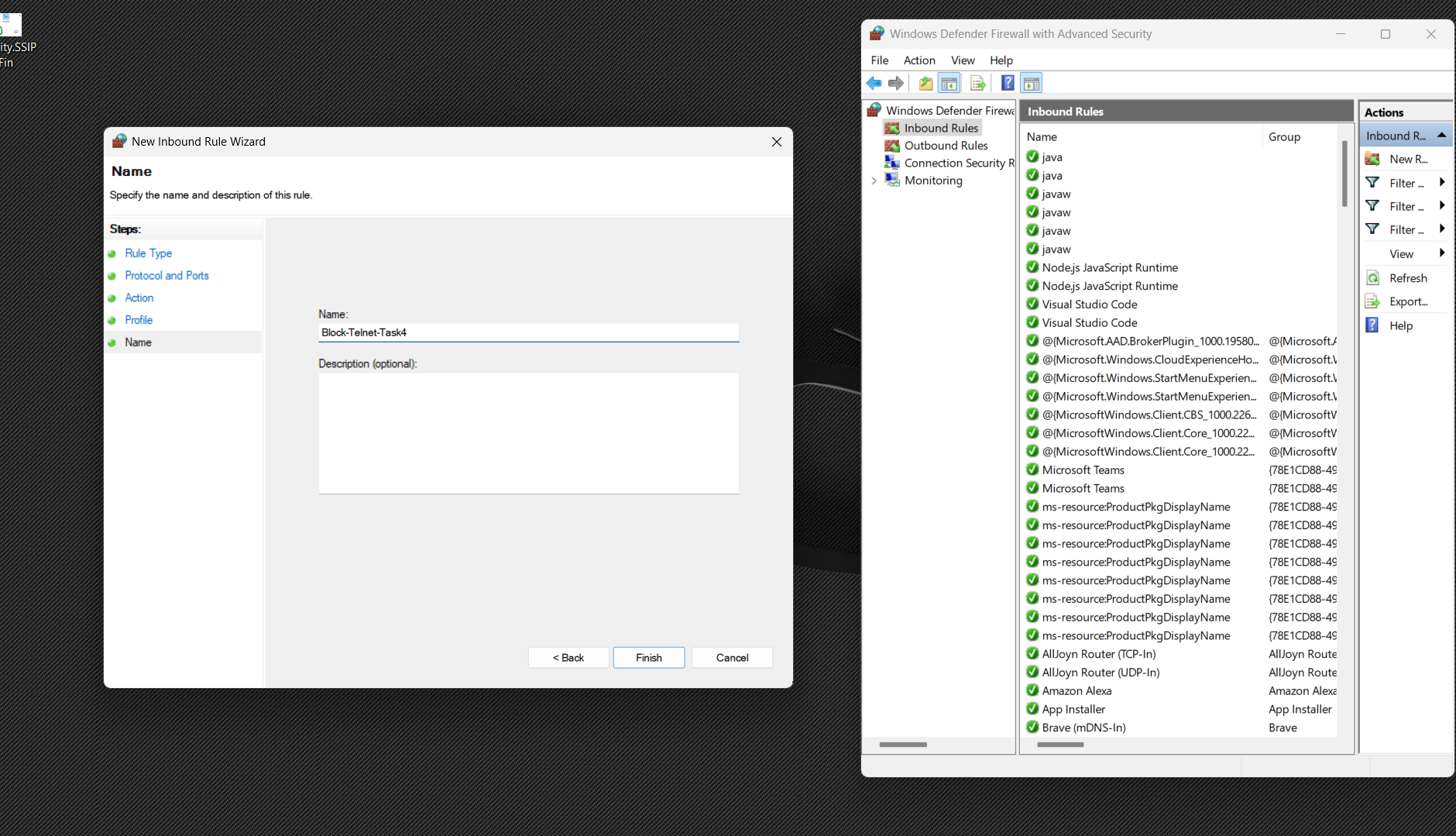
# Screenshots

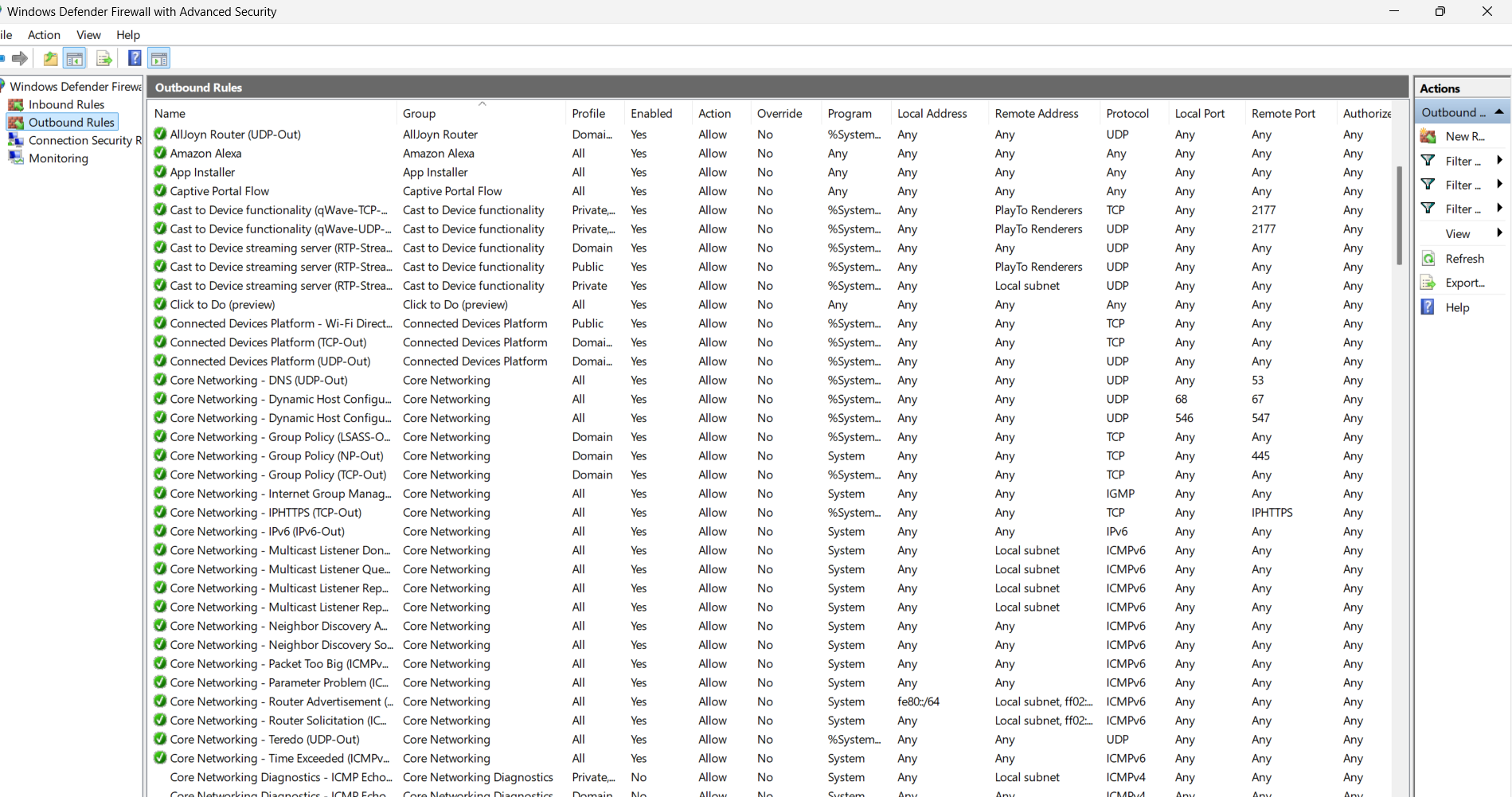
Below are the screenshots taken during the task on Windows and Linux.

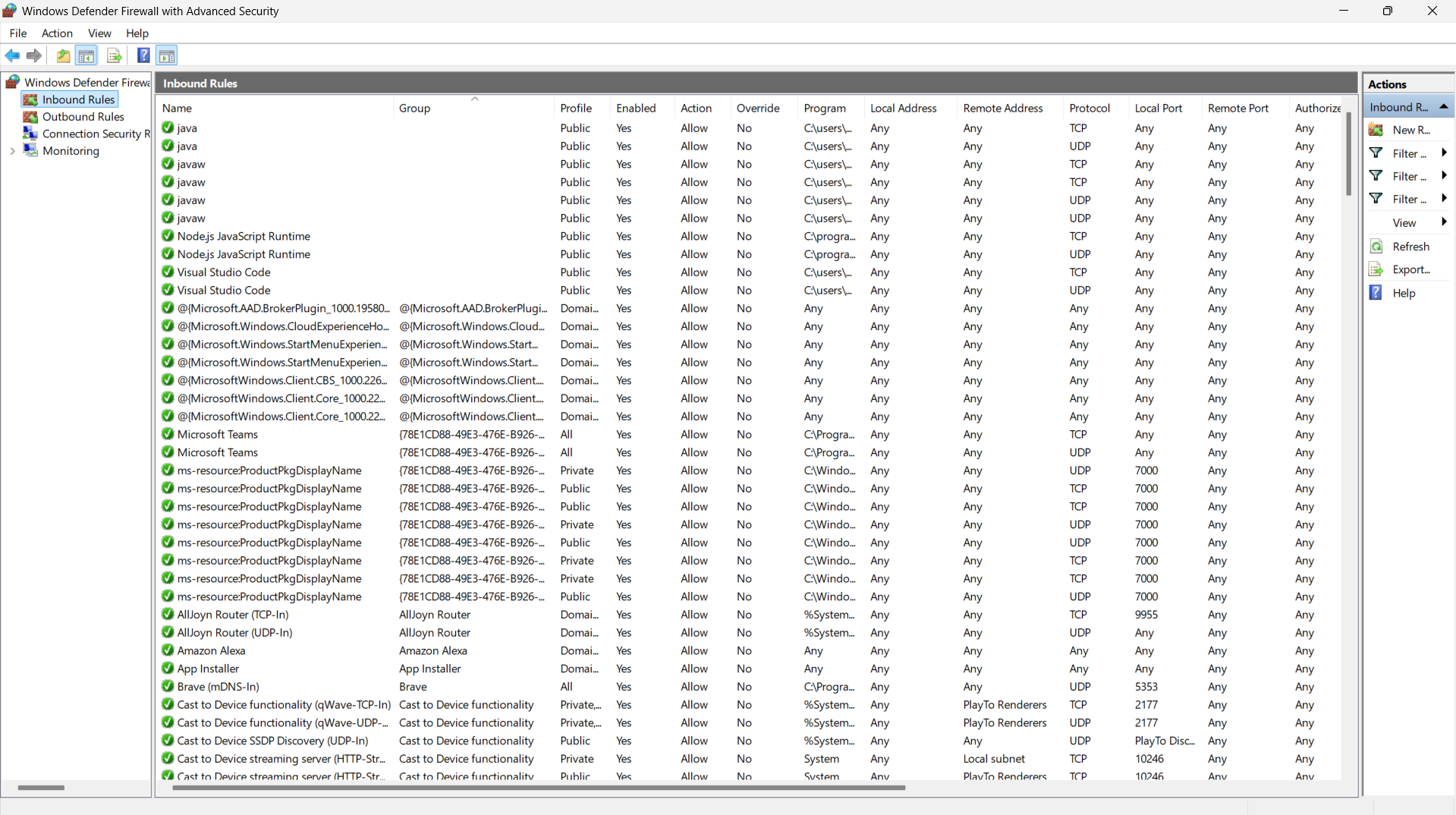
Screenshot 1: Windows Firewall Rule Added



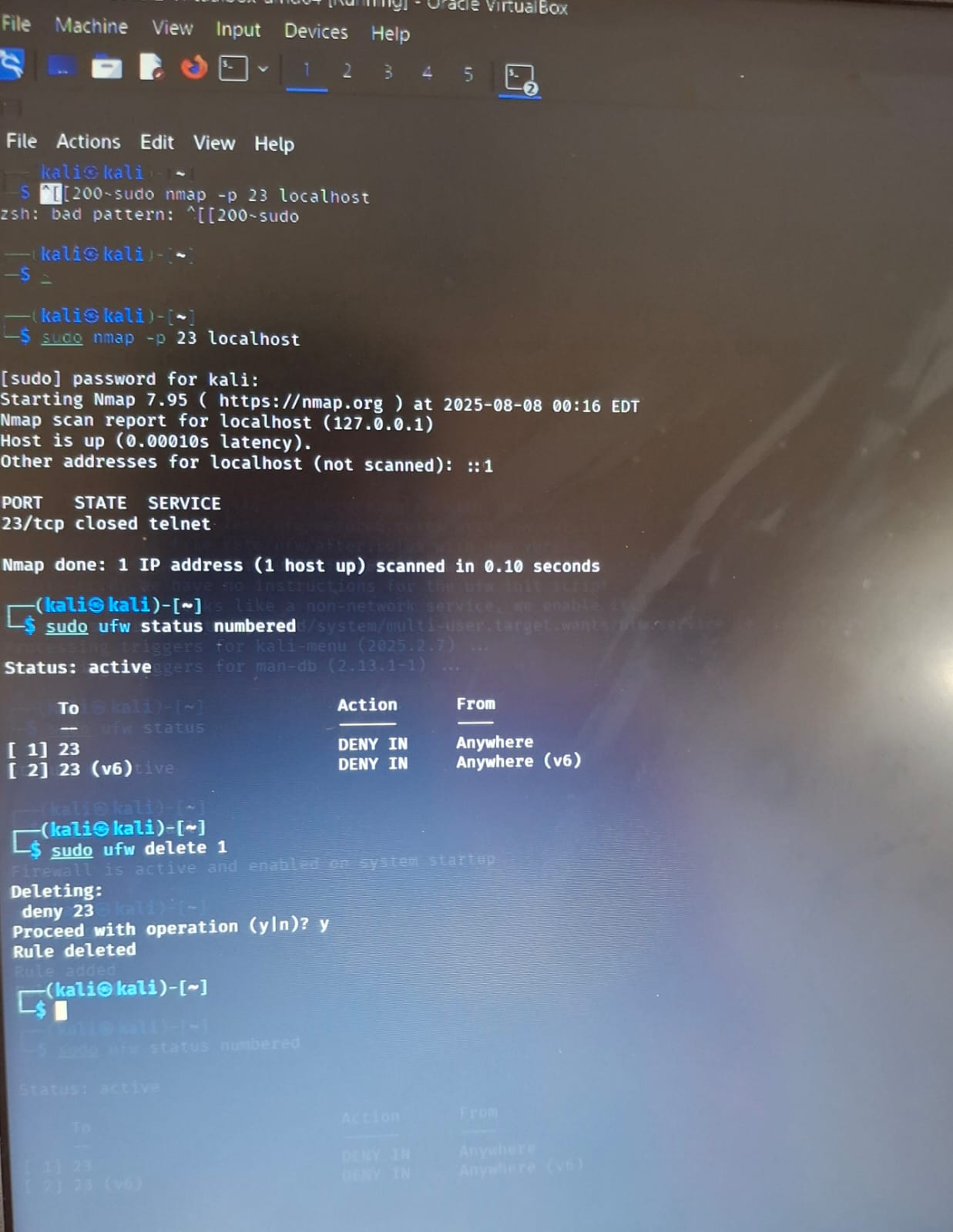


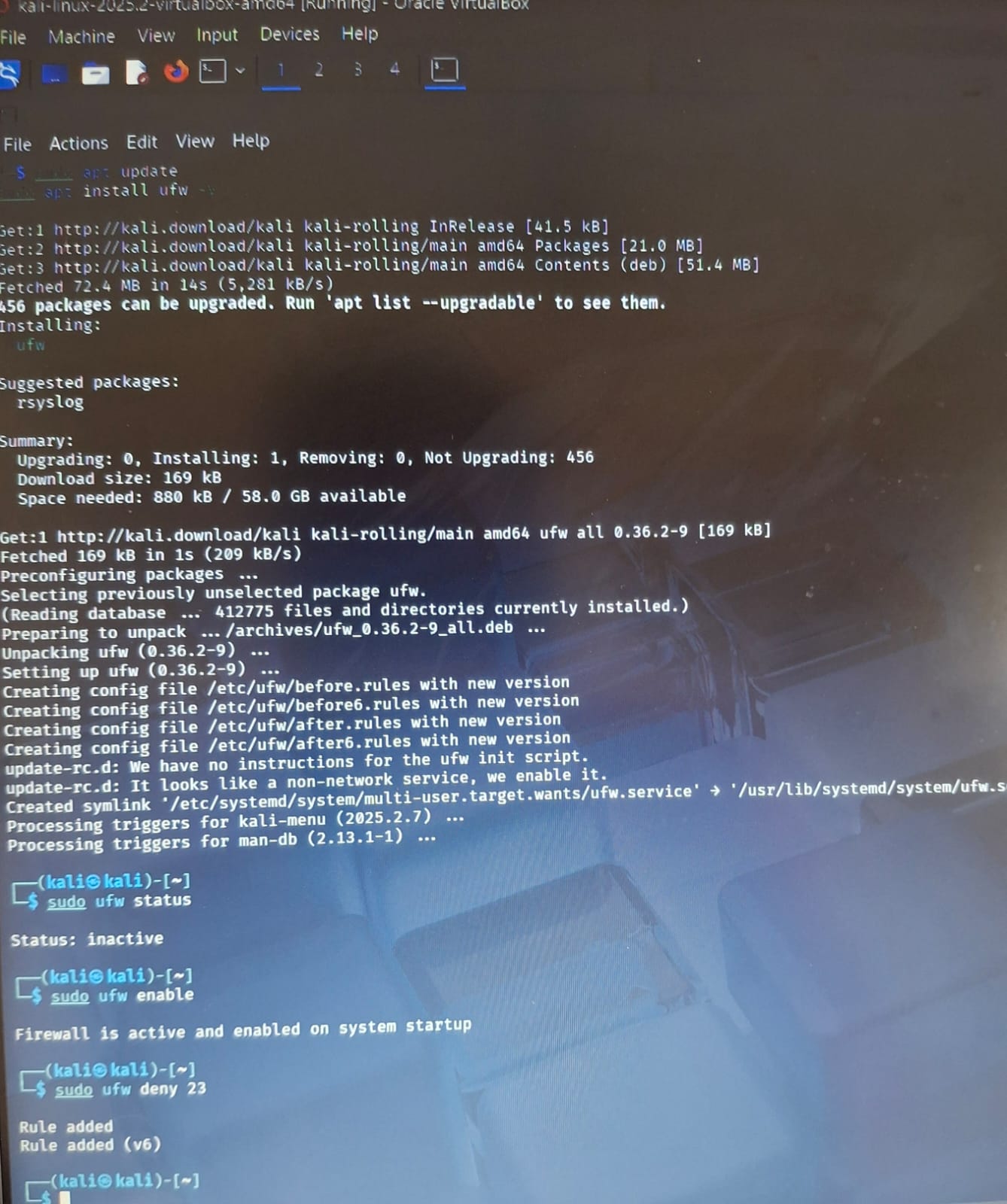






Screenshot 2: Linux UFW Block Port 23



Screenshot 3: Testing with Nmap:- 

# Conclusion

The task demonstrated the practical application of firewall rules on both Windows and Linux systems. It showed how to block specific ports, test the effects, and safely remove the rules afterward. This hands-on activity strengthens understanding of host-based firewalls in real-world scenarios.