CYBER SECURITY INTERNSHIP

Task-4

Firewall on Windows/Linux

Information

Name: K. Vamsi

Institution: Kalasalingam Academy of Research and Education

Internship Role: Cybersecurity Intern

Submission Date: 08/08/2025

1. Introduction

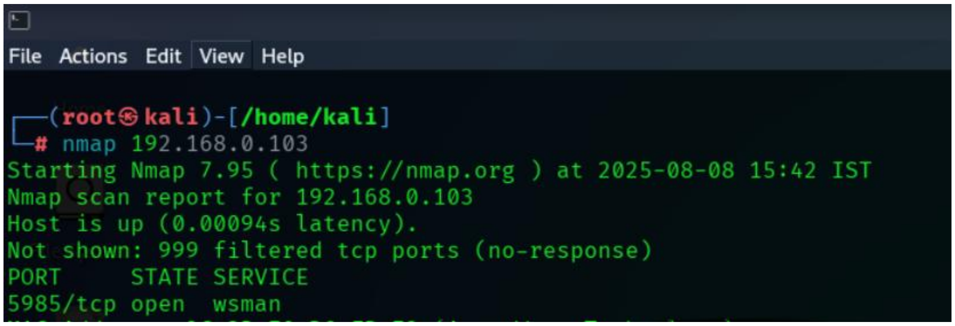
The purpose of this report is to setup and use a firewall on windows and Linux. To configure and test basic firewall rules to allow or block traffic in both windows and Linux. Actually a firewall acts as barrier between trusted network and untrusted networks, filtering inbound and outbound connection based on predefined rules. In this task we are configure the firewall settings both Windows and Linux to protect systems.

2. Tools and Environment

Tools	***Description***
Windows Firewall	*Built in windows security tool used to manage network traffic.*
Kali Linux - UFW	*Linux command line utility for managing iptables firewall rules in a simplified way.*

3. Methodology

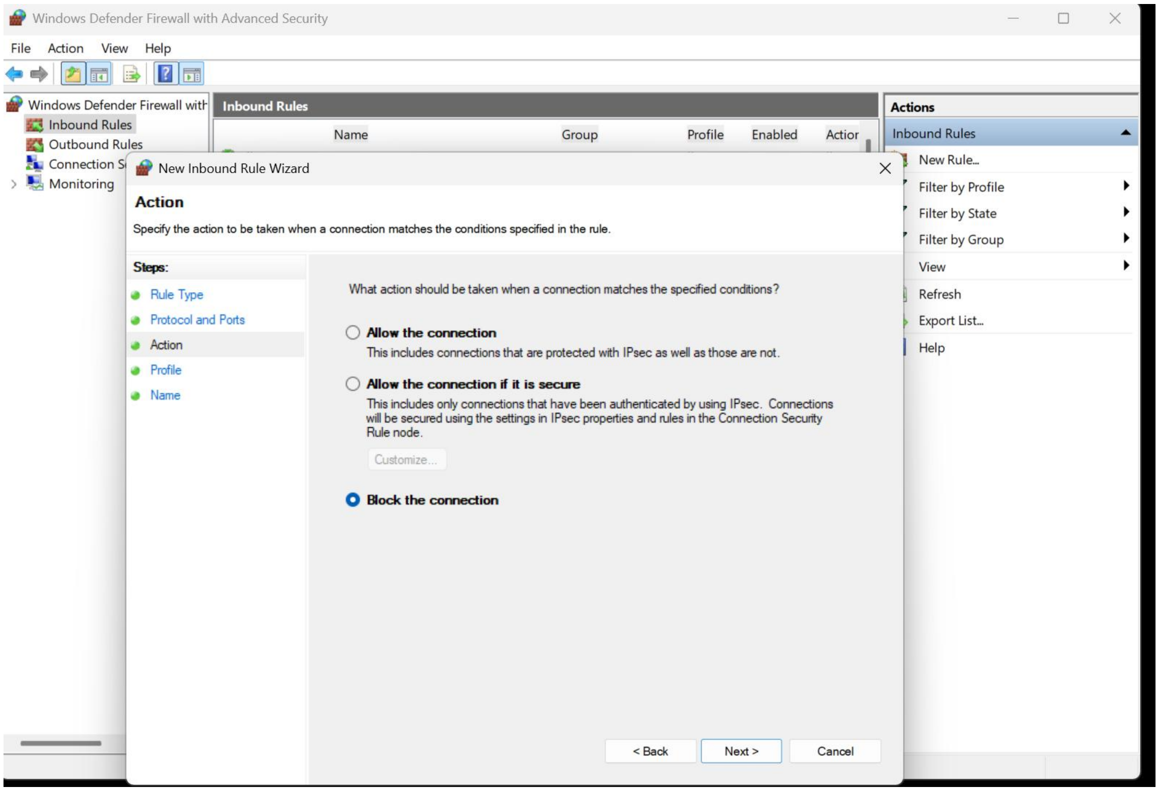
WINDOWS



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.0.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 15:42 IST
Nmap scan report for 192.168.0.103
Host is up (0.00094s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5985/tcp open  wsman
```

Fig (1): open ports(1st scan)

- Open firewall configuration tool press Win+R and type mf.msc.
- Press Enter Windows Defender Firewall with advanced security will open.
- In left panel click inbound Rules and outbound rules
- Check what ports are active in your system using Nmap I found wsman – 5985 is active.



Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

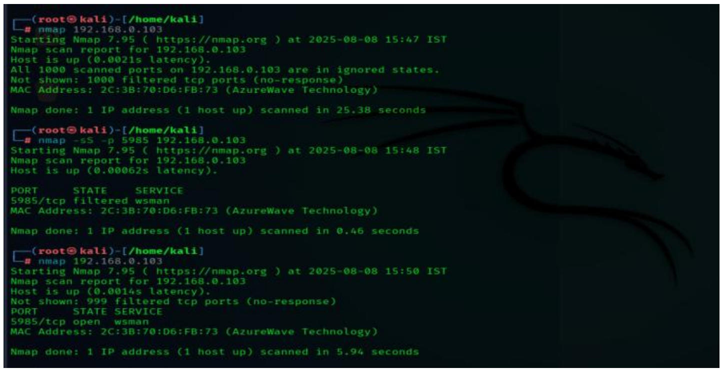
○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

Fig (2): Block the connection

- In the left panel click inbound rule and click new rule.
- Choose TCP and enter port number 5985 Specify port.
- Select Block the connection and apply to Domain, Private, Public.
- Name it as a WSMAN and test the firewall rule now.



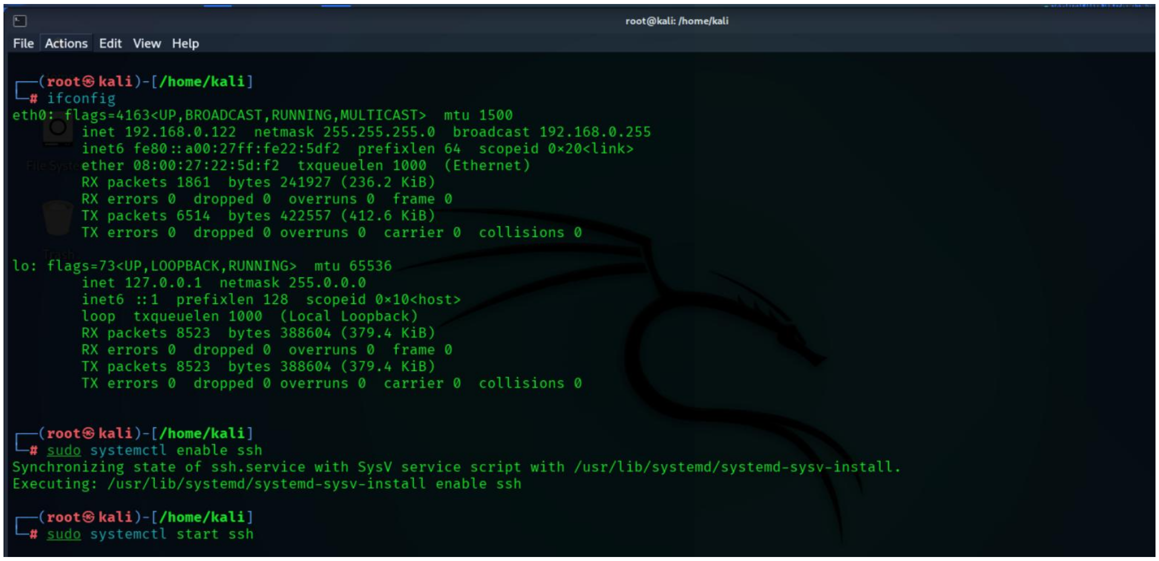
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.0.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 15:47 IST
Nmap scan report for 192.168.0.103
Host is up (0.0021s latency).
All 1000 scanned ports on 192.168.0.103 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 2C:3B:70:D6:FB:73 (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 25.38 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -p 5985 192.168.0.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 15:48 IST
Nmap scan report for 192.168.0.103
Host is up (0.00062s latency).

PORT     STATE    SERVICE
5985/tcp filtered wsman
MAC Address: 2C:3B:70:D6:FB:73 (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.0.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 15:50 IST
Nmap scan report for 192.168.0.103
Host is up (0.0014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5985/tcp open  wsman
MAC Address: 2C:3B:70:D6:FB:73 (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 5.94 seconds
```

Fig (3): filtered port to open port

- I observe that when I scanned it shows port state is filtered so windows firewall rule is applied successfully.
- Now disable the rule which u created and allow all connection and do scan again observe the port status again.

LINUX

- Open Linux terminal check the ip address using command **ifconfig .**
- Start services ssh using Sudo Systemctl enable ssh.
- Check the status and start ssh services. Port number 22/tcp.



```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.122  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe22:5df2  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:5d:f2  txqueuelen 1000  (Ethernet)
        RX packets 1861  bytes 241927 (236.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6514  bytes 422557 (412.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8523  bytes 388604 (379.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8523  bytes 388604 (379.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh

┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl start ssh
```

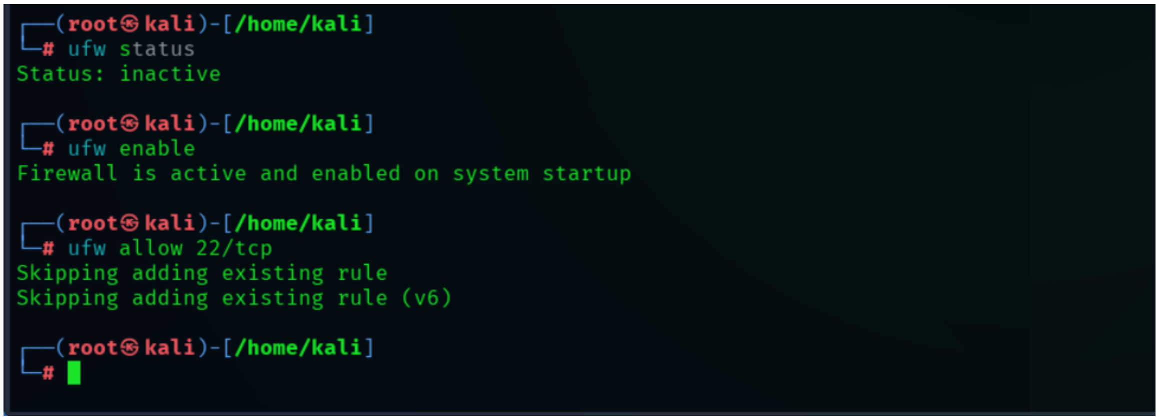
Fig (4): Start ssh services

- Check the status and scan your IP whether u found ssh port is open or not using nmap.

  Command:

  Nmap -p 22 -sS 192.168.0.122

- Check the firewall is active or not using command UFW (uncomplicated firewall).
- If not activate the Linux Firewall. It uses the netfilter firewall for easy communication we use the UFW.
- Allow the ssh on port 22/tcp. Now go to windows connect the kali through ssh.



```
┌──(root㉿kali)-[/home/kali]
└─# ufw status
Status: inactive

┌──(root㉿kali)-[/home/kali]
└─# ufw enable
Firewall is active and enabled on system startup

┌──(root㉿kali)-[/home/kali]
└─# ufw allow 22/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(root㉿kali)-[/home/kali]
└─# 
```

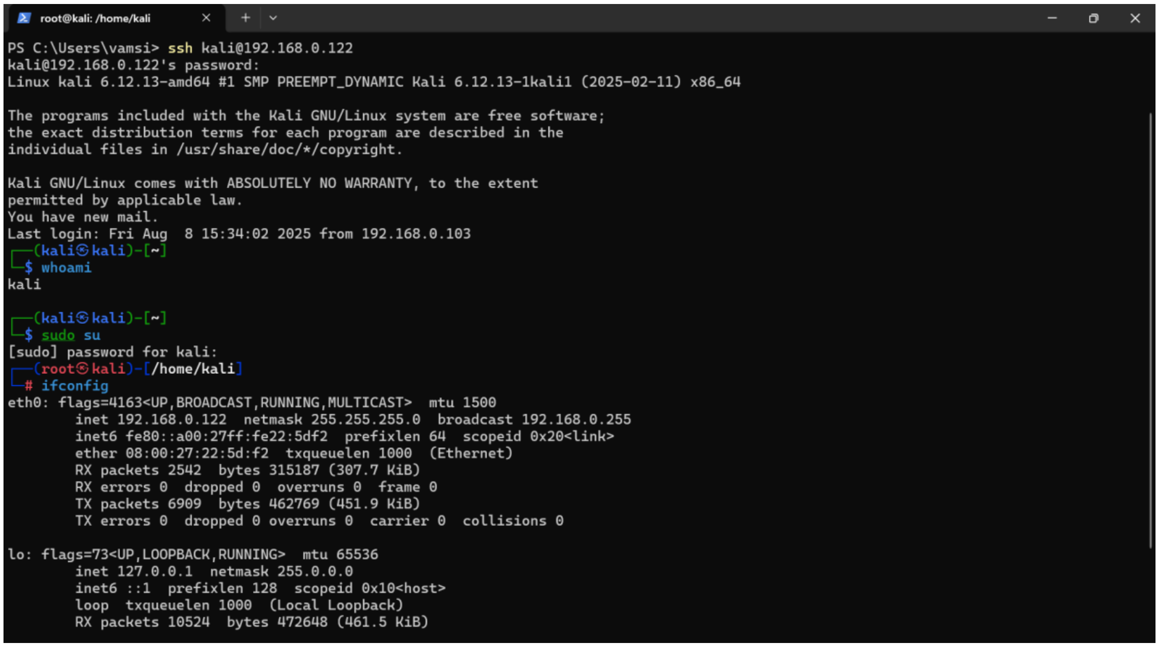
Fig (5): UFW

Command's:

Sudo ufw status

Sudo ufw enable

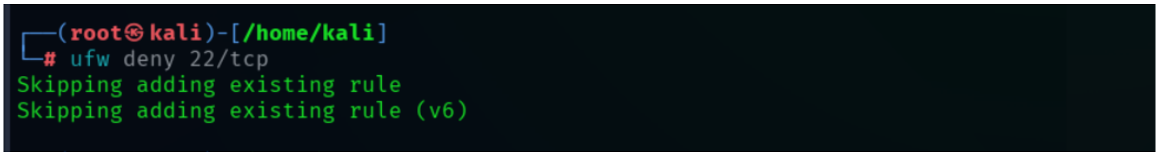
Sudo ufw allow 22/tcp



```
PS C:\Users\vamsi> ssh kali@192.168.0.122
kali@192.168.0.122's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Fri Aug  8 15:34:02 2025 from 192.168.0.103
┌──(kali㉿kali)-[~]
└─$ whoami
kali

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.122  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe22:5df2  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:5d:f2  txqueuelen 1000  (Ethernet)
        RX packets 2542  bytes 315187 (307.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6909  bytes 462769 (451.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 10524  bytes 472648 (461.5 KiB)
```

Fig (6): Ssh kali@192.168.0.122(enter these in windows prompt)

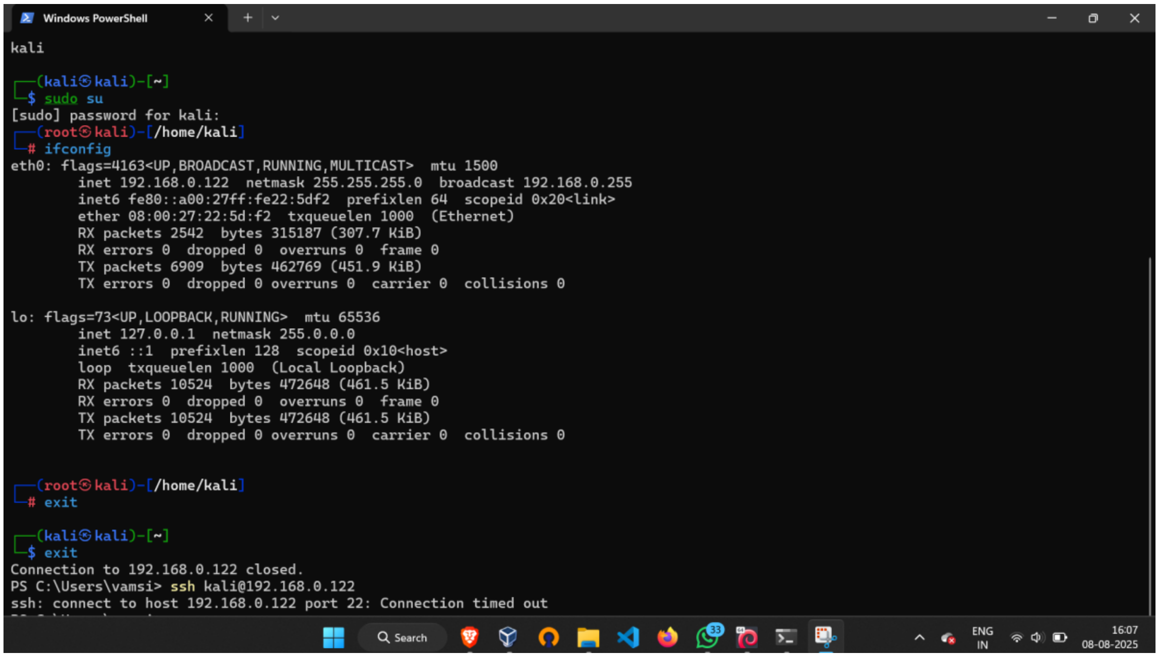
- Successfully we login through the ssh in windows so the firewall rule is applied effectively.



```
┌──(root㉿kali)-[/home/kali]
└─# ufw deny 22/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
```

- Now disable and try again
  Command

Sudo ufw deny 22/tcp



```
kali

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.122  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe22:5df2  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:5d:f2  txqueuelen 1000  (Ethernet)
        RX packets 2542  bytes 315187 (307.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6909  bytes 462769 (451.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 10524  bytes 472648 (461.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10524  bytes 472648 (461.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# exit

┌──(kali㉿kali)-[~]
└─$ exit
Connection to 192.168.0.122 closed.
PS C:\Users\vamsi> ssh kali@192.168.0.122
ssh: connect to host 192.168.0.122 port 22: Connection timed out
```

Fig (7): Connection timed out

Result – Windows & Linux:

-

  On Windows, inbound WSMAN traffic (port 5985) was blocked using Windows Defender Firewall, and the port shows filtered, confirming the rule worked.

- On Linux, inbound ssh 22 traffic was blocked using UFW (interacting with Netfilter), and remote connection attempts from Windows were denied, verifying the firewall's effectiveness.