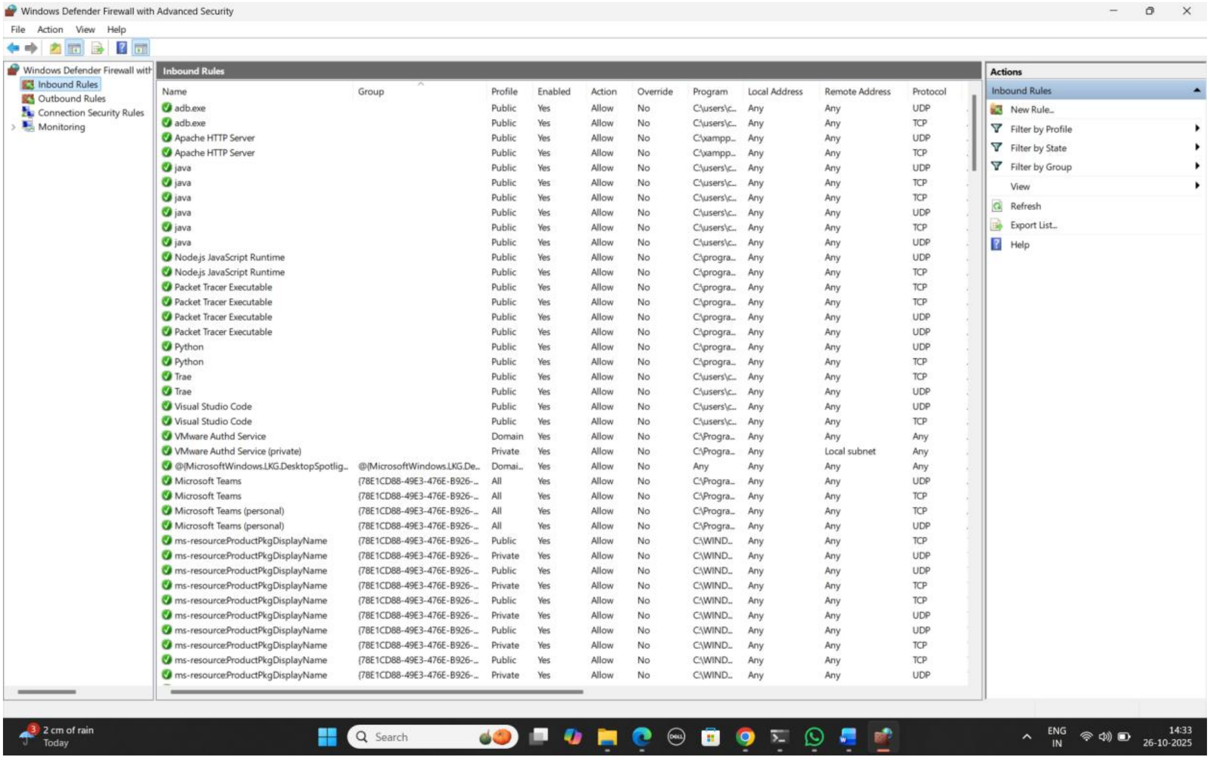
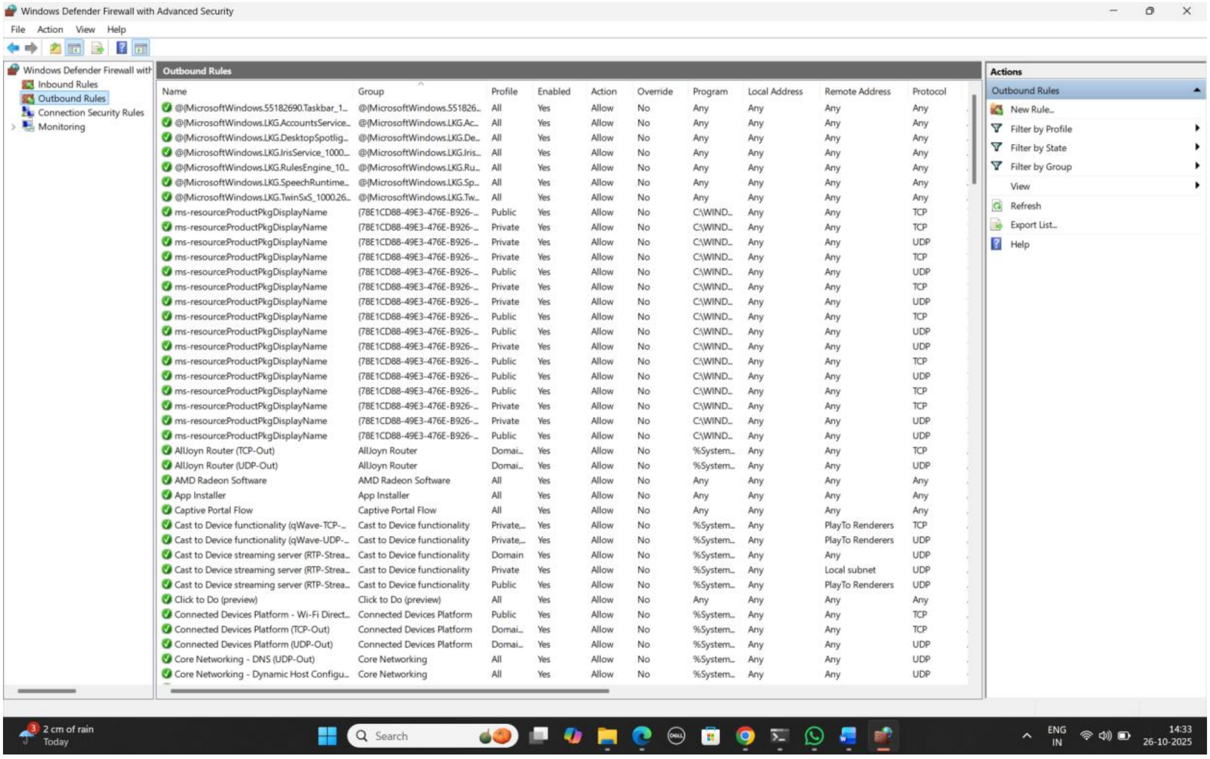
- Inbound traffic: -



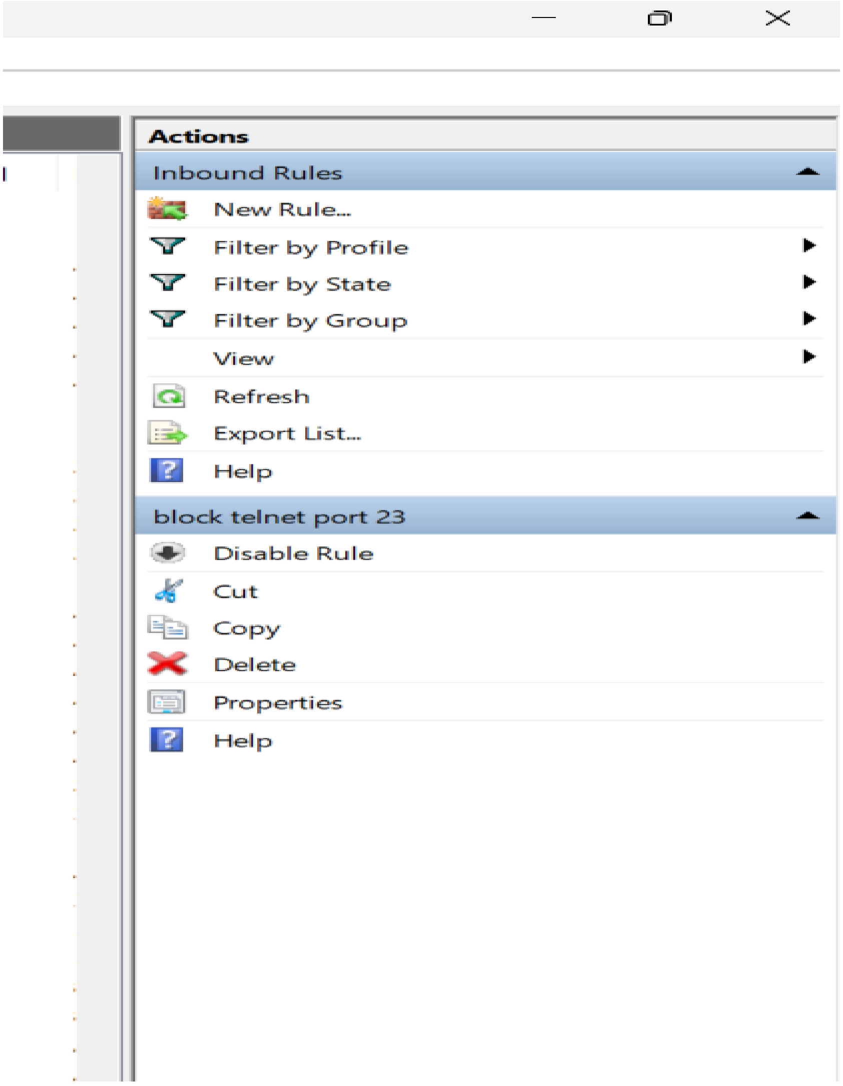
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
adb.exe		Public	Yes	Allow	No	C:\users\c...	Any	Any	UDP
adb.exe		Public	Yes	Allow	No	C:\users\c...	Any	Any	TCP
Apache HTTP Server		Public	Yes	Allow	No	C:\xampp...	Any	Any	UDP
Apache HTTP Server		Public	Yes	Allow	No	C:\xampp...	Any	Any	TCP
java		Public	Yes	Allow	No	C:\users\c...	Any	Any	UDP
java		Public	Yes	Allow	No	C:\users\c...	Any	Any	TCP
java		Public	Yes	Allow	No	C:\users\c...	Any	Any	TCP
java		Public	Yes	Allow	No	C:\users\c...	Any	Any	UDP
java		Public	Yes	Allow	No	C:\users\c...	Any	Any	TCP
java		Public	Yes	Allow	No	C:\users\c...	Any	Any	UDP
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
Node.js JavaScript Runtime		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
Packet Tracer Executable		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
Packet Tracer Executable		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
Packet Tracer Executable		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
Packet Tracer Executable		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
Python		Public	Yes	Allow	No	C:\progra...	Any	Any	UDP
Python		Public	Yes	Allow	No	C:\progra...	Any	Any	TCP
Trae		Public	Yes	Allow	No	C:\users\c...	Any	Any	TCP
Trae		Public	Yes	Allow	No	C:\users\c...	Any	Any	UDP
Visual Studio Code		Public	Yes	Allow	No	C:\users\c...	Any	Any	UDP
Visual Studio Code		Public	Yes	Allow	No	C:\users\c...	Any	Any	TCP
VMware Authd Service		Domain	Yes	Allow	No	C:\Progra...	Any	Any	Any
VMware Authd Service (private)		Private	Yes	Allow	No	C:\Progra...	Any	Local subnet	Any
@{MicrosoftWindows.LKG.DesktopSpotlig...	@{MicrosoftWindows.LKG.De...	Domai...	Yes	Allow	No	Any	Any	Any	Any
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
Microsoft Teams	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
Microsoft Teams (personal)	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	TCP
Microsoft Teams (personal)	{78E1CD88-49E3-476E-B926-...	All	Yes	Allow	No	C:\Progra...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	UDP

- Outbound traffic: -

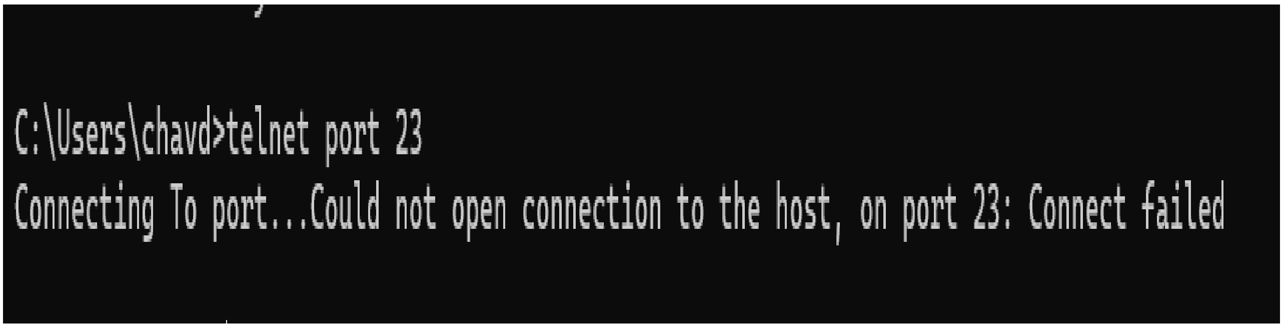


Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
@{MicrosoftWindows.55182690.Taskbar_1...	@{MicrosoftWindows.551826...	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LKG.AccountsService...	@{MicrosoftWindows.LKG.Ac...	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LKG.DesktopSpotlig...	@{MicrosoftWindows.LKG.De...	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LKG.IrisService_1000...	@{MicrosoftWindows.LKG.Iris...	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LKG.RulesEngine_10...	@{MicrosoftWindows.LKG.Ru...	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LKG.SpeechRuntime...	@{MicrosoftWindows.LKG.Sp...	All	Yes	Allow	No	Any	Any	Any	Any
@{MicrosoftWindows.LKG.TwinSxS_1000.26...	@{MicrosoftWindows.LKG.Tw...	All	Yes	Allow	No	Any	Any	Any	Any
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	TCP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow	No	C:\WIND...	Any	Any	UDP
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow	No	C:\WIND...	Any	Any	UDP
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP
AMD Radeon Software	AMD Radeon Software	All	Yes	Allow	No	Any	Any	Any	Any
App Installer	App Installer	All	Yes	Allow	No	Any	Any	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any
Cast to Device functionality (qWave-TCP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP
Cast to Device functionality (qWave-UDP-...	Cast to Device functionality	Private,...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP
Cast to Device streaming server (RTP-Strea...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP
Click to Do (preview)	Click to Do (preview)	All	Yes	Allow	No	Any	Any	Any	Any
Connected Devices Platform - Wi-Fi Direct...	Connected Devices Platform	Public	Yes	Allow	No	%System...	Any	Any	TCP
Connected Devices Platform (TCP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	TCP
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP
Core Networking - Dynamic Host Configu...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP

- Block the telnet port 23: -

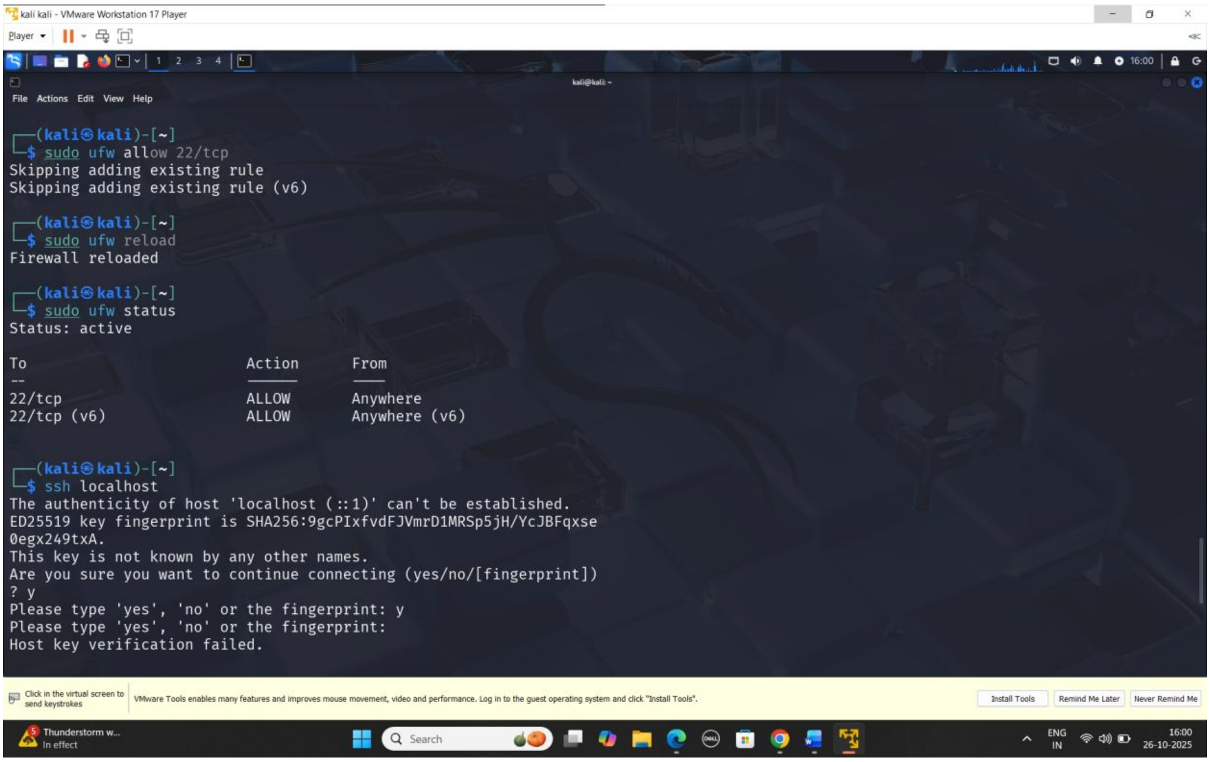


- The result of the entered rule.



```
C:\Users\chavd>telnet port 23
Connecting To port...Could not open connection to the host, on port 23: Connect failed
```

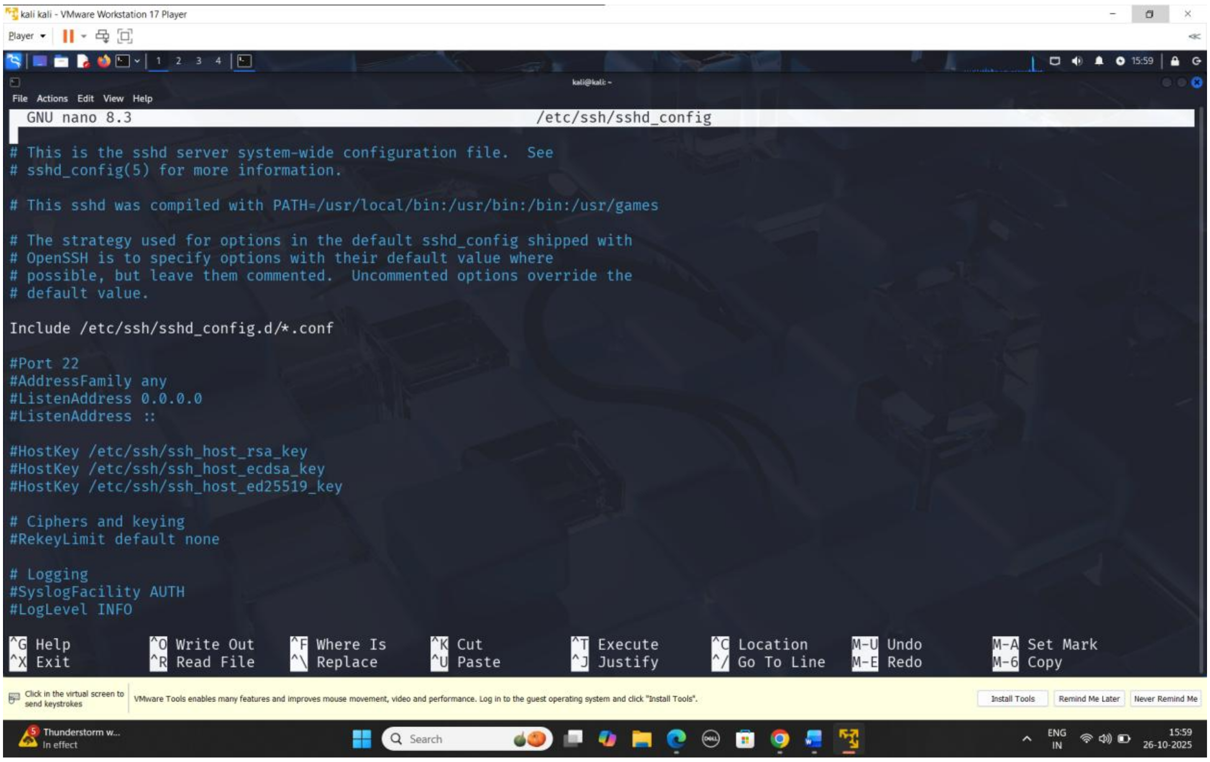
- Allow the SSH 22 port traffic (in Linux).



```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 22/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(kali㉿kali)-[~]
└─$ sudo ufw reload
Firewall reloaded

┌──(kali㉿kali)-[~]
└─$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)


┌──(kali㉿kali)-[~]
└─$ ssh localhost
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:9gcPIxfvdFJVmrD1MRSp5jH/YcJBFqxse
0egx249txA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])
? y
Please type 'yes', 'no' or the fingerprint: y
Please type 'yes', 'no' or the fingerprint:
Host key verification failed.
```

Click in the virtual screen to send keystrokes

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".



```
  GNU nano 8.3                          /etc/ssh/sshd_config

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

^G Help        ^O Write Out   ^F Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
```

Click in the virtual screen to send keystrokes

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

- Steps and commands: -

1. Open the Windows Firewall Configuration
   - Press Windows + R, type wf.msc, and press Enter.
   - This opens the Windows Defender Firewall with Advanced Security window.
2. View Current Firewall Rules
   - Click on Inbound Rules and Outbound Rules in the left panel.
   - Scroll to see the existing rules and their status (Allowed/Blocked).
3. Add a Rule to Block Traffic on a Specific Port (e.g., Port 23 for Telnet)
   - In the right panel, click New Rule…
   - Choose Port, then click Next.
   - Select TCP and enter the port number (e.g., 23).
   - Choose Block the connection, click Next, and select all profiles (Domain, Private, Public).
   - Name it (e.g., *Block Telnet Port 23*) and click Finish.
4. Test the Block Rule
   - Try connecting to port 23 (e.g., using telnet localhost 23).
   - The connection should fail, showing the rule works.
5. Add a Rule to Allow Traffic (e.g., Port 22 for SSH) (Linux)
   - Again, create a New Rule, choose Port, enter 22, and select Allow the connection.
   - Name it (e.g., *Allow SSH Port 22*).
   - Check if SSH Server is Installed - sudo apt install openssh-server -y
   - Start the SSH Service - sudo systemctl start ssh / sudo systemctl start ssh
   - Verify SSH Service Status - sudo systemctl status ssh
   - Check if Port 22 is Listening - sudo netstat -tuln | grep 22 / sudo ss -tuln | grep 22
   - Allow SSH Through UFW (Firewall) - sudo ufw allow 22/tcp, sudo ufw reload, sudo ufw status
   - Test the Connection - ssh localhost

6. Remove or Disable the Test Rule
    - Right-click on *Block Telnet Port 23* and select Disable Rule or Delete.
    - This restores the original firewall configuration.

- Summary – How Firewall Filters Traffic
    - A firewall acts as a protective barrier between a trusted internal network and untrusted external networks. It filters network traffic based on defined rules — such as port numbers, IP addresses, and protocols.
    - The firewall examines each incoming and outgoing data packet and decides whether to allow or block it according to these rules. For example, it can block unwanted or insecure ports (like port 23 for Telnet) and allow secure connections (like port 22 for SSH).
    - By doing this, the firewall ensures that only authorized and safe communication passes through while preventing unauthorized access or attacks, thereby maintaining the security and integrity of the system.