

## **List current firewall rules**

Media Center Extenders - qWave (TCP-In)

Windows Media Player Network Sharing Service (qWave-UDP-In)

Windows Media Player Network Sharing Service (HTTP-Streaming-In)

Cast to Device streaming server (RTSP-Streaming-In)

Cast to Device streaming server (HTTP-Streaming-In)

Cast to Device streaming server (HTTP-Streaming-In)

Media Center Extenders - Media Streaming (TCP-In)

Cast to Device streaming server (RTCP-Streaming-In)

Cast to Device streaming server (RTSP-Streaming-In)

Cast to Device UPnP Events (TCP-In)

Wireless Portable Devices (SSDP-In)

Cast to Device SSDP Discovery (UDP-In)

Media Center Extenders - SSDP (UDP-In)

Cast to Device functionality (qWave-TCP-In)

Cast to Device streaming server (HTTP-Streaming-In)

Windows Media Player Network Sharing Service (HTTP-Streaming-In)

Wireless Portable Devices (UPnP-In)

Windows Media Player Network Sharing Service (SSDP-In)

Media Center Extenders - XSP (TCP-In)

Media Center Extenders - RTSP (TCP-In)

Windows Media Player Network Sharing Service (Streaming-UDP-In)

Cast to Device functionality (qWave-UDP-In)

Windows Media Player Network Sharing Service (Streaming-UDP-In)

Windows Media Player Network Sharing Service (TCP-In)

Windows Media Player Network Sharing Service (UDP-In)

Windows Media Player x86 (UDP-In)

Media Center Extenders - WMDRM-ND/RTP/RTCP (UDP-In)

Cast to Device streaming server (RTSP-Streaming-In)

Windows Media Player Network Sharing Service (qWave-TCP-In)

Windows Media Player Network Sharing Service (TCP-In)

Windows Media Player Network Sharing Service (UDP-In)

Windows Media Player Network Sharing Service (UPnP-In)

Cast to Device streaming server (RTCP-Streaming-In)

Windows Media Player Network Sharing Service (qWave-UDP-In)

Windows Media Player Network Sharing Service (qWave-TCP-In)

Media Center Extenders - qWave (UDP-In)

Media Center Extenders - HTTP Streaming (TCP-In)

Cast to Device streaming server (RTCP-Streaming-In)

Windows Media Player (UDP-In)

mDNS (UDP-In)

Core Networking Diagnostics - ICMP Echo Request (ICMPv6-In)

Distributed Transaction Coordinator (TCP-In)

Windows Remote Management - Compatibility Mode (HTTP-In)

Core Networking Diagnostics - ICMP Echo Request (ICMPv4-In)

Remote Assistance (TCP-In)

Windows Peer to Peer Collaboration Foundation (TCP-In)

mDNS (UDP-In)

Core Networking - Time Exceeded (ICMPv6-In)

Netlogon Service Authz (RPC)

Remote Volume Management - Virtual Disk Service (RPC)

Distributed Transaction Coordinator (TCP-In)

DIAL protocol server (HTTP-In)

Secure Socket Tunneling Protocol (SSTP-In)

Core Networking Diagnostics - ICMP Echo Request (ICMPv4-In)

Core Networking - Multicast Listener Report (ICMPv6-In)

Windows Peer to Peer Collaboration Foundation (SSDP-In)

Core Networking - Multicast Listener Query (ICMPv6-In)

Remote Event Log Management (RPC)

Network Discovery (WSD-In)

Remote Volume Management - Virtual Disk Service Loader (RPC)

Core Networking - Multicast Listener Report v2 (ICMPv6-In)

Windows Management Instrumentation (WMI-In)

Core Networking - Internet Group Management Protocol (IGMP-In)

Network Discovery (Pub-WSD-In)

Proximity sharing over TCP (TCP sharing-In)

Distributed Transaction Coordinator (RPC)

Remote Assistance (SSDP TCP-In)

Windows Management Instrumentation (DCOM-In)

Remote Event Log Management (RPC-EPMAP)

Performance Logs and Alerts (DCOM-In)

Network Discovery (UPnP-In)

Windows Collaboration Computer Name Registration Service (SSDP-In)

Wireless Display (TCP-In)

Wi-Fi Direct Network Discovery (In)

Network Discovery (WSD Events-In)

Windows Remote Management (HTTP-In)

Performance Logs and Alerts (TCP-In)

Performance Logs and Alerts (DCOM-In)

Remote Scheduled Tasks Management (RPC)

Connected Devices Platform - Wi-Fi Direct Transport (TCP-In)

Network Discovery (NB-Datagram-In)

Core Networking - Destination Unreachable (ICMPv6-In)

Network Discovery (WSD EventsSecure-In)

Core Networking - Multicast Listener Done (ICMPv6-In)

AllJoyn Router (UDP-In)

AllJoyn Router (TCP-In)

Windows Defender Firewall Remote Management (RPC)

Core Networking - IPHTTPS (TCP-In)

Core Networking - Packet Too Big (ICMPv6-In)

Routing and Remote Access (L2TP-In)

Virtual Machine Monitoring (Echo Request - ICMPv6-In)

Network Discovery (LLMNR-UDP-In)

Remote Assistance (TCP-In)

mDNS (UDP-In)

Remote Scheduled Tasks Management (RPC-EPMAP)

Connected Devices Platform (TCP-In)

Connected Devices Platform (UDP-In)

Virtual Machine Monitoring (Echo Request - ICMPv4-In)

Network Discovery (SSDP-In)

Netlogon Service (NP-In)

Network Discovery for Teredo (UPnP-In)

Remote Assistance (SSDP UDP-In)

TPM Virtual Smart Card Management (TCP-In)

TPM Virtual Smart Card Management (DCOM-In)

Remote Volume Management - Virtual Disk Service Loader (RPC)

Remote Volume Management (RPC-EPMAP)

Core Networking Diagnostics - ICMP Echo Request (ICMPv6-In)

Network Discovery (NB-Name-In)

Remote Service Management (NP-In)

Windows Defender Firewall Remote Management (RPC-EPMAP)

Network Discovery (UPnP-In)

Distributed Transaction Coordinator (RPC-EPMAP)

Remote Service Management (RPC)

Core Networking - Teredo (UDP-In)

Remote Service Management (NP-In)

Network Discovery (NB-Datagram-In)

Core Networking - Parameter Problem (ICMPv6-In)

Network Discovery (NB-Name-In)

iSCSI Service (TCP-In)

Network Discovery (WSD-In)

Windows Remote Management - Compatibility Mode (HTTP-In)

Remote Service Management (RPC-EPMAP)

Remote Service Management (RPC)

Network Discovery (SSDP-In)

Microsoft Media Foundation Network Source IN [TCP 554]

Core Networking - Neighbor Discovery Advertisement (ICMPv6-In)

Network Discovery (WSD EventsSecure-In)

Windows Defender Firewall Remote Management (RPC)

Virtual Machine Monitoring (NB-Session-In)

Windows Management Instrumentation (ASync-In)

Remote Service Management (RPC-EPMAP)

Network Discovery (WSD Events-In)

DIAL protocol server (HTTP-In)

Windows Peer to Peer Collaboration Foundation (PNRP-In)

Remote Assistance (PNRP-In)

Remote Scheduled Tasks Management (RPC-EPMAP)

Network Discovery (Pub-WSD-In)

Wireless Display Infrastructure Back Channel (TCP-In)

Windows Management Instrumentation (DCOM-In)

Core Networking - Router Solicitation (ICMPv6-In)

Virtual Machine Monitoring (DCOM-In)

Network Discovery (NB-Datagram-In)

TPM Virtual Smart Card Management (TCP-In)

Remote Volume Management - Virtual Disk Service (RPC)

Routing and Remote Access (PPTP-In)

Remote Assistance (PNRP-In)

iSCSI Service (TCP-In)

Virtual Machine Monitoring (RPC)

Network Discovery (NB-Name-In)

Delivery Optimization (TCP-In)

Windows Remote Management (HTTP-In)

Performance Logs and Alerts (TCP-In)

Windows Defender Firewall Remote Management (RPC-EPMAP)

Windows Management Instrumentation (WMI-In)

Windows Management Instrumentation (ASync-In)

SNMP Trap Service (UDP In)

Microsoft Media Foundation Network Source IN [UDP 5004-5009]

Remote Event Monitor (RPC)

Remote Event Log Management (RPC-EPMAP)

Network Discovery (UPnP-In)

Remote Assistance (RA Server TCP-In)

Remote Volume Management (RPC-EPMAP)

Network Discovery (WSD EventsSecure-In)

Remote Assistance (DCOM-In)

Remote Event Monitor (RPC-EPMAP)

Core Networking - Neighbor Discovery Solicitation (ICMPv6-In)

Network Discovery (WSD Events-In)

Network Discovery (WSD-In)

Wi-Fi Direct Scan Service Use (In)

Distributed Transaction Coordinator (RPC-EPMAP)

Network Discovery for Teredo (SSDP-In)

Distributed Transaction Coordinator (RPC)

Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)

TPM Virtual Smart Card Management (DCOM-In)

Routing and Remote Access (GRE-In)

Network Discovery (WSD-In)

Core Networking - Dynamic Host Configuration Protocol (DHCP-In)

Core Networking - Destination Unreachable Fragmentation Needed (ICMPv4-In)

Core Networking - Router Advertisement (ICMPv6-In)

Delivery Optimization (UDP-In)

SNMP Trap Service (UDP In)

Remote Event Log Management (NP-In)

Network Discovery (LLMNR-UDP-In)

Core Networking - IPv6 (IPv6-In)

Remote Event Log Management (RPC)

Windows Peer to Peer Collaboration Foundation (WSD-In)

Windows Collaboration Computer Name Registration Service (PNRP-In)

Wi-Fi Direct Spooler Use (In)

Remote Scheduled Tasks Management (RPC)

Remote Event Log Management (NP-In)

KillerRat v10.0.0

KillerRat v10.0.0

Visual Studio Code

Visual Studio Code

Microsoft Teams

Microsoft Teams

Spotify

Spotify

WsToastNotification

WsToastNotification

Microsoft Edge

Microsoft Edge

Java(TM) Platform SE binary

Java(TM) Platform SE binary

OpenJDK Platform binary

OpenJDK Platform binary



SpyNote V6.4

SpyNote V6.4

SpyNote V6.4

SpyNote V6.4

SpyNote V6.4

SpyNote V6.4

Firefox

Firefox

Packet Tracer Executable

Packet Tracer Executable

mdns-discovery.exe

mdns-discovery.exe

arduino ide.exe

arduino ide.exe

inaips.exe

VMware Authd Service

VMware Authd Service (private)

Work or school account

Inbound Rule for Remote Shutdown (TCP-In)

WFD ASP Coordination Protocol (UDP-In)

WFD Driver-only (TCP-In)

Inbound Rule for Remote Shutdown (RPC-EP-In)

WFD Driver-only (UDP-In)

zoom.exe

zoom.exe

File and Printer Sharing (Spooler Service - RPC-EPMAP)

File and Printer Sharing (Spooler Service - RPC)

File and Printer Sharing (NB-Session-In)

File and Printer Sharing (Spooler Service - RPC)

File and Printer Sharing (Restrictive) (SMB-In)

File and Printer Sharing (Spooler Service Worker - RPC)

File and Printer Sharing (NB-Datagram-In)

File and Printer Sharing (NB-Name-In)

File and Printer Sharing (Restrictive) (LLMNR-UDP-In)

File and Printer Sharing (Spooler Service - RPC-EPMAP)

File and Printer Sharing (NB-Name-In)

File and Printer Sharing (Restrictive) (Spooler Service - RPC)

File and Printer Sharing (NB-Session-In)

File and Printer Sharing (Echo Request - ICMPv4-In)

File and Printer Sharing (Restrictive) (Spooler Service Worker - RPC)

File and Printer Sharing (SMB-In)

File and Printer Sharing (SMB-In)

File and Printer Sharing (Spooler Service Worker - RPC)

File and Printer Sharing (Restrictive) (Echo Request - ICMPv4-In)

File and Printer Sharing (Echo Request - ICMPv6-In)

File and Printer Sharing (Restrictive) (Spooler Service - RPC-EPMAP)

File and Printer Sharing (Echo Request - ICMPv6-In)

File and Printer Sharing (NB-Datagram-In)

File and Printer Sharing (Echo Request - ICMPv4-In)

File and Printer Sharing (LLMNR-UDP-In)

File and Printer Sharing (Restrictive) (Echo Request - ICMPv6-In)

Firefox

Firefox

@{MicrosoftWindows.LKG.DesktopSpotlight\_1000.26100.3775.0\_x64\_\_cw5n1h2txyewy?ms-resource://MicrosoftWindows.LKG.Desk...

Mail and Calendar

chrome.exe

chrome.exe

Microsoft To Do

Windows Security

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

Windows Camera

Windows Media Player

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

Microsoft Journal

Packet Tracer Executable

Packet Tracer Executable

Xbox

Lenovo Companion

Films & TV

Game Bar

Feedback Hub

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

ms-resource:ProductPkgDisplayName

Start

Windows Feature Experience Pack

Windows Feature Experience Pack

Windows Feature Experience Pack

Windows Feature Experience Pack

innetcut\_windows.exe

Microsoft Store

App Installer

ms-resource:AppTitle

ms-resource:AppTitle

ms-resource:AppTitle

ms-resource:AppTitle

ms-resource:AppTitle

ms-resource:AppTitle

ms-resource:AppTitle

ms-resource:AppTitle

Firefox

Firefox

MSN Weather

Microsoft Edge (mDNS-In)

Microsoft Edge (mDNS-In)

Store Experience Host

Microsoft Teams

Microsoft Teams

WhatsApp

Microsoft Teams

arduino ide.exe

## Add a rule to block inbound traffic on a specific port

```
PS C:\Users\ROHIT KUMAR> Get-NetFirewallRule -DisplayName "Block Telnet Inbound" | Format-List *
```

```
Name           : {EFFCD51C-545D-4222-AC24-159A220B38C8}
ID              : {EFFCD51C-545D-4222-AC24-159A220B38C8}
DisplayName     : Block Telnet Inbound
Group           :
Enabled         : True
Profile        : Any
Platform       : {}
Direction      : Inbound
Action         : Block
EdgeTraversalPolicy : Block
LSM            : False
PrimaryStatus   : OK
Status         : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSourceType : Local
Caption        :
Description     :
ElementName     : Block Telnet Inbound
InstanceID     : {EFFCD51C-545D-4222-AC24-159A220B38C8}
CommonName     :
```

PolicyKeywords :  
PolicyDecisionStrategy : 2  
PolicyRoles :  
ConditionListType : 3  
CreationClassName : MSFT|FW|FirewallRule|{EFFCD51C-545D-4222-AC24-159A220B38C8}  
ExecutionStrategy : 2  
Mandatory :  
PolicyRuleName :  
Priority :  
RuleUsage :  
SequencedActions : 3  
SystemCreationClassName :  
SystemName :  
DisplayGroup :  
LocalOnlyMapping : False  
LooseSourceMapping : False  
Owner :  
PackageFamilyName :  
Platforms : {}  
PolicyAppId :  
PolicyStoreSource : PersistentStore  
Profiles : 0  
RemoteDynamicKeywordAddresses : {}  
RuleGroup :  
StatusCode : 65536  
PSComputerName :

CimClass : root/standardcimv2:MSFT\_NetFirewallRule

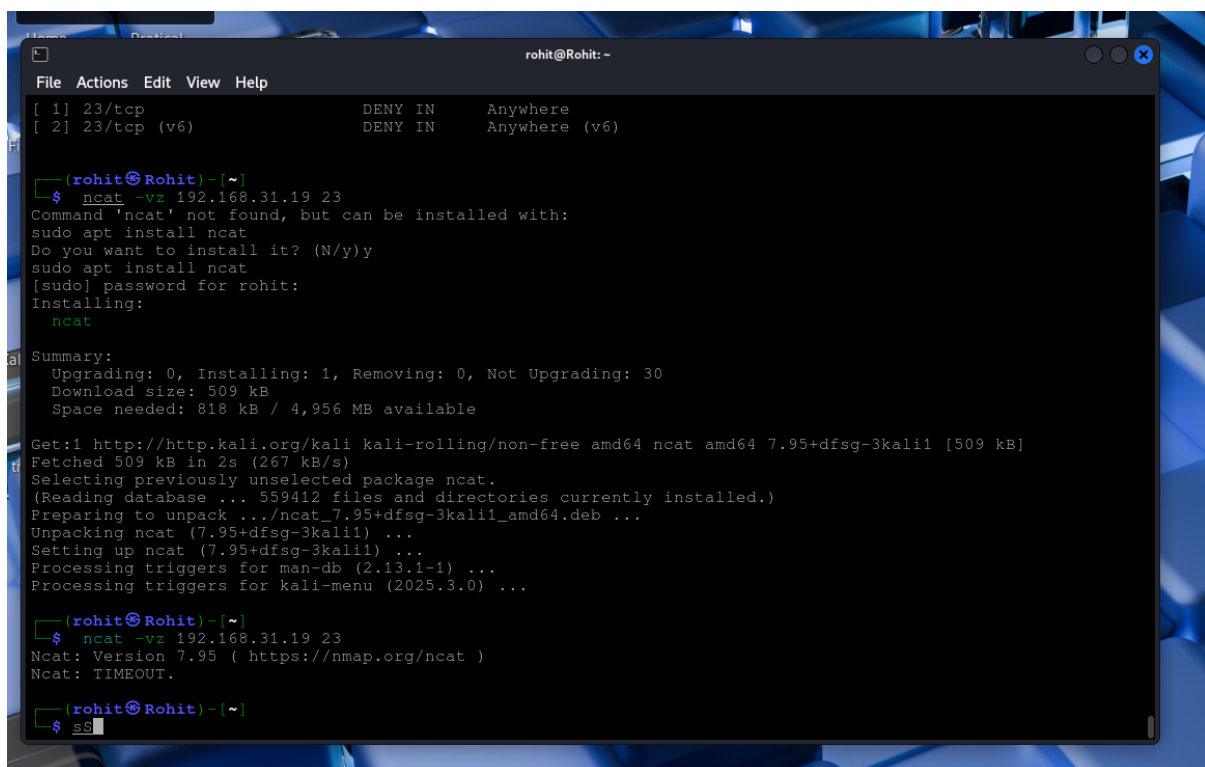
CimInstanceProperties : {Caption, Description, ElementName, InstanceID...}

CimSystemProperties :

Microsoft.Management.Infrastructure.CimSystemProperties

## Testing the Firewall Block

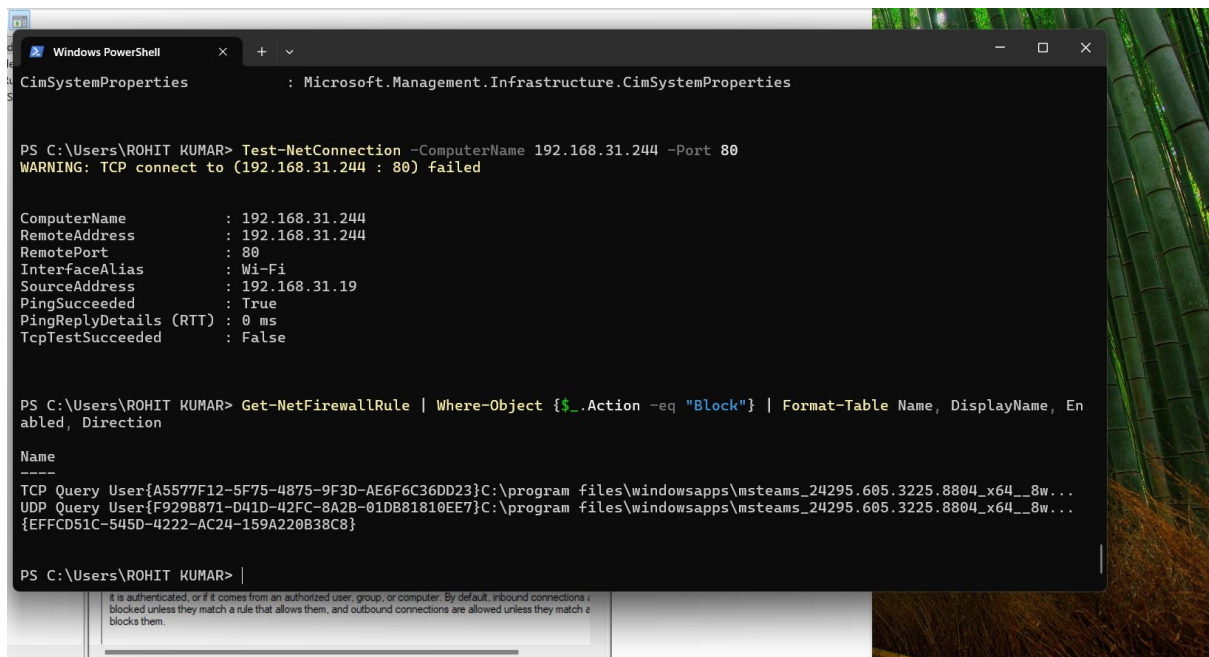
### Tool Used: Ncat (Netcat)



```
rohit@Rohit: ~  
[ 1] 23/tcp DENY IN Anywhere  
[ 2] 23/tcp (v6) DENY IN Anywhere (v6)  
  
(rohit@Rohit)~  
$ ncat -vz 192.168.31.19 23  
Command 'ncat' not found, but can be installed with:  
sudo apt install ncat  
Do you want to install it? (N/y)y  
sudo apt install ncat  
[sudo] password for rohit:  
Installing:  
ncat  
  
Summary:  
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 30  
Download size: 509 kB  
Space needed: 818 kB / 4,956 MB available  
  
Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 ncat amd64 7.95+dfsg-3kali1 [509 kB]  
Fetched 509 kB in 2s (267 kB/s)  
Selecting previously unselected package ncat.  
(Reading database ... 559412 files and directories currently installed.)  
Preparing to unpack .../ncat_7.95+dfsg-3kali1_amd64.deb ...  
Unpacking ncat (7.95+dfsg-3kali1) ...  
Setting up ncat (7.95+dfsg-3kali1) ...  
Processing triggers for man-db (2.13.1-1) ...  
Processing triggers for kali-menu (2025.3.0) ...  
  
(rohit@Rohit)~  
$ ncat -vz 192.168.31.19 23  
Ncat: Version 7.95 ( https://nmap.org/ncat )  
Ncat: TIMEOUT.  
  
(rohit@Rohit)~  
$ ss
```



## Viewing the Rule



```
Windows PowerShell
CimSystemProperties : Microsoft.Management.Infrastructure.CimSystemProperties

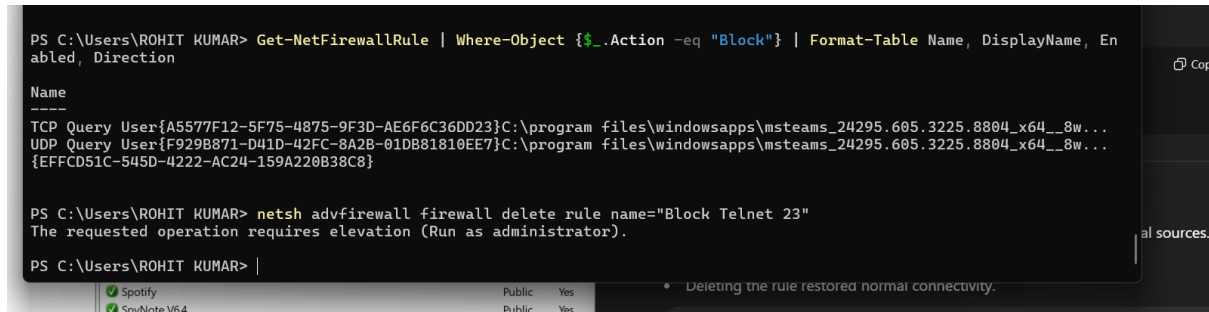
PS C:\Users\ROHIT KUMAR> Test-NetConnection -ComputerName 192.168.31.244 -Port 80
WARNING: TCP connect to (192.168.31.244 : 80) failed

ComputerName       : 192.168.31.244
RemoteAddress      : 192.168.31.244
RemotePort         : 80
InterfaceAlias     : Wi-Fi
SourceAddress      : 192.168.31.19
PingSucceeded      : True
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded   : False

PS C:\Users\ROHIT KUMAR> Get-NetFirewallRule | Where-Object {$_.Action -eq "Block"} | Format-Table Name, DisplayName, Enabled, Direction

Name
----
TCP Query User{A5577F12-5F75-4875-9F3D-AE6F6C36DD23}C:\program files\windowsapps\msteams_24295.605.3225.8804_x64__8w...
UDP Query User{F929B871-D41D-42FC-8A2B-01DB81810EE7}C:\program files\windowsapps\msteams_24295.605.3225.8804_x64__8w...
{EFFCD51C-545D-4222-AC24-159A220B38C8}
```

## Deleting the Firewall Rule



```
PS C:\Users\ROHIT KUMAR> Get-NetFirewallRule | Where-Object {$_.Action -eq "Block"} | Format-Table Name, DisplayName, Enabled, Direction

Name
----
TCP Query User{A5577F12-5F75-4875-9F3D-AE6F6C36DD23}C:\program files\windowsapps\msteams_24295.605.3225.8804_x64__8w...
UDP Query User{F929B871-D41D-42FC-8A2B-01DB81810EE7}C:\program files\windowsapps\msteams_24295.605.3225.8804_x64__8w...
{EFFCD51C-545D-4222-AC24-159A220B38C8}

PS C:\Users\ROHIT KUMAR> netsh advfirewall firewall delete rule name="Block Telnet 23"
The requested operation requires elevation (Run as administrator).

PS C:\Users\ROHIT KUMAR>
```

## Result

- The firewall successfully blocked connections on port 23 from external sources.
- Ncat confirmed the block by failing to connect.
- Deleting the rule restored normal connectivity.

