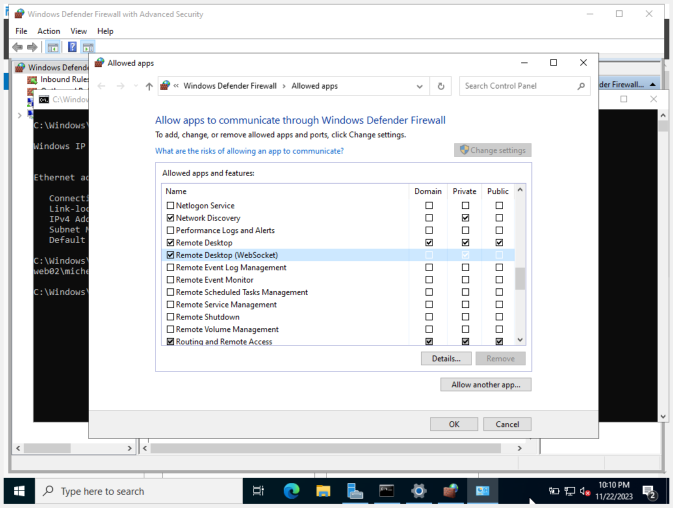
ACTIVE DIRECTORY PENTESTING

RDP CONNECTION

Windows to windows

Win+X > System > Remote desktop > enable



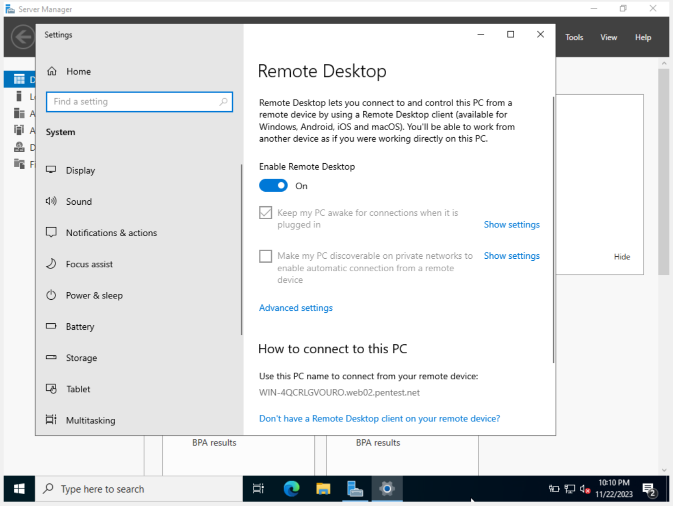
Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Domain	Private	Public
☐ Netlogon Service	☐	☐	☐
☑ Network Discovery	☐	☑	☐
☐ Performance Logs and Alerts	☐	☐	☐
☑ Remote Desktop	☑	☑	☑
☑ Remote Desktop (WebSocket)	☐	☑	☐
☐ Remote Event Log Management	☐	☐	☐
☐ Remote Event Monitor	☐	☐	☐
☐ Remote Scheduled Tasks Management	☐	☐	☐
☐ Remote Service Management	☐	☐	☐
☐ Remote Shutdown	☐	☐	☐
☐ Remote Volume Management	☐	☐	☐
☑ Routing and Remote Access	☑	☑	☑



Remote Desktop

Remote Desktop lets you connect to and control this PC from a remote device by using a Remote Desktop client (available for Windows, Android, iOS and macOS). You'll be able to work from another device as if you were working directly on this PC.

Enable Remote Desktop

● On

☑ Keep my PC awake for connections when it is plugged in — Show settings

☐ Make my PC discoverable on private networks to enable automatic connection from a remote device — Show settings

Advanced settings

How to connect to this PC

Use this PC name to connect from your remote device:

WIN-4QCRLGVOURO.web02.pentest.net

Don't have a Remote Desktop client on your remote device?

Allow outbound firewall rules too.

Kali:

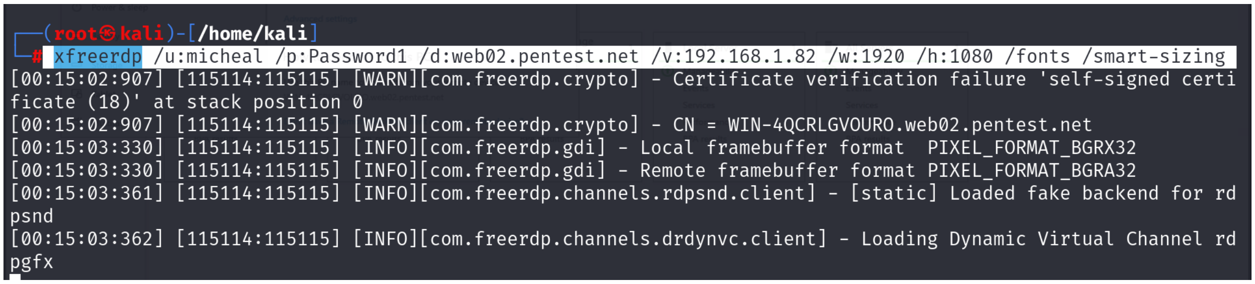
# RDP connections

```
xfreerdp /u:username /p:password /d:domain-name /v:IP-address /w:1920 /h:1080 /fonts /smart-sizing
```

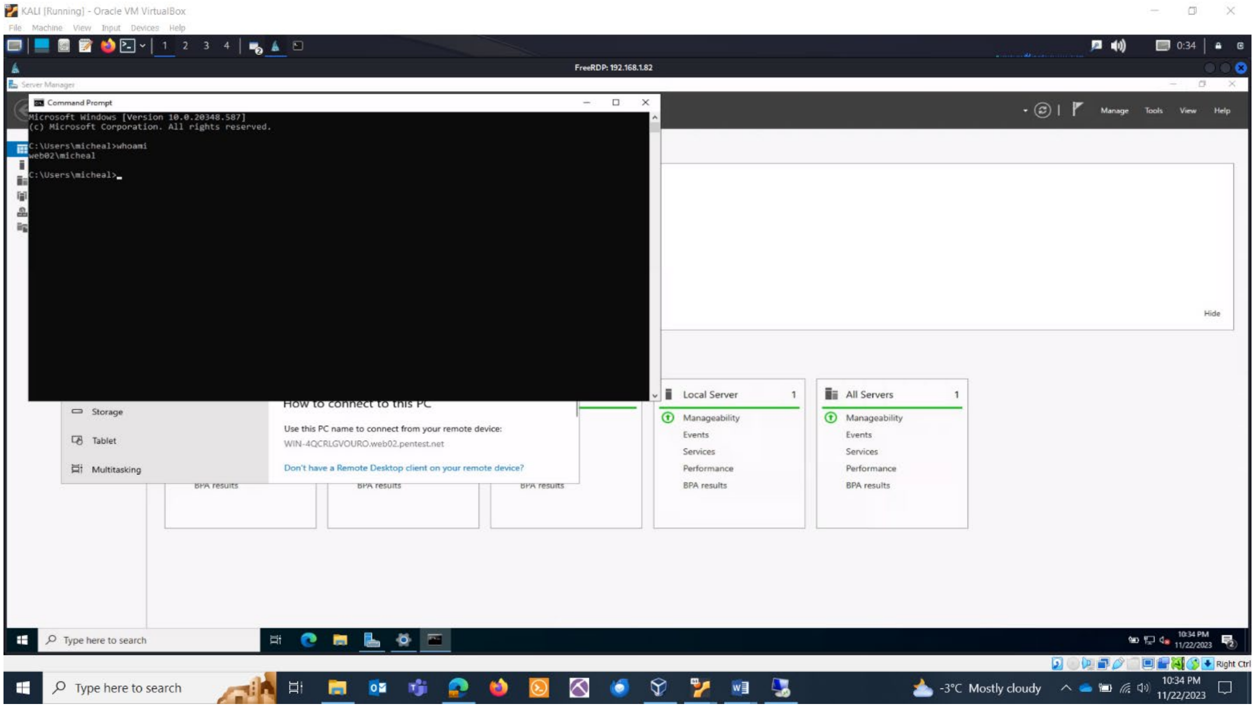
The command you provided is using xfreerdp, which is an open-source remote desktop protocol (RDP) client for Linux. It allows users to connect to a remote Windows machine using the Remote Desktop Protocol. Let's break down the command and its parameters

- /u:username: Specifies the username for the remote desktop connection. Replace "username" with the actual username you want to use for logging in.
- /p:password: Specifies the password for the specified username. Replace "password" with the actual password for the given username. Note that storing passwords in plaintext in commands can pose security risks, and more secure methods should be considered, especially in scripts or shared environments.
- /d:domain-name: Specifies the domain name for the user account. Replace "domain-name" with the actual domain name. This parameter is optional and only needed if the user account is part of a domain.
- /v:IP-address: Specifies the IP address or hostname of the remote Windows machine you want to connect to.
- /w:1920: Sets the width of the remote desktop window to 1920 pixels.
- /h:1080: Sets the height of the remote desktop window to 1080 pixels.
- /fonts: Enables font smoothing for the remote desktop session.
- /smart-sizing: Enables smart sizing, which adjusts the remote desktop window size based on the client's window size. This can be useful for dynamically adapting to different screen resolutions.

Kali



```
┌──(root㉿kali)-[/home/kali]
└─# xfreerdp /u:micheal /p:Password1 /d:web02.pentest.net /v:192.168.1.82 /w:1920 /h:1080 /fonts /smart-sizing
[00:15:02:907] [115114:115115] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certi
ficate (18)' at stack position 0
[00:15:02:907] [115114:115115] [WARN][com.freerdp.crypto] - CN = WIN-4QCRLGVOURO.web02.pentest.net
[00:15:03:330] [115114:115115] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[00:15:03:330] [115114:115115] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[00:15:03:361] [115114:115115] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rd
psnd
[00:15:03:362] [115114:115115] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rd
pgfx
```

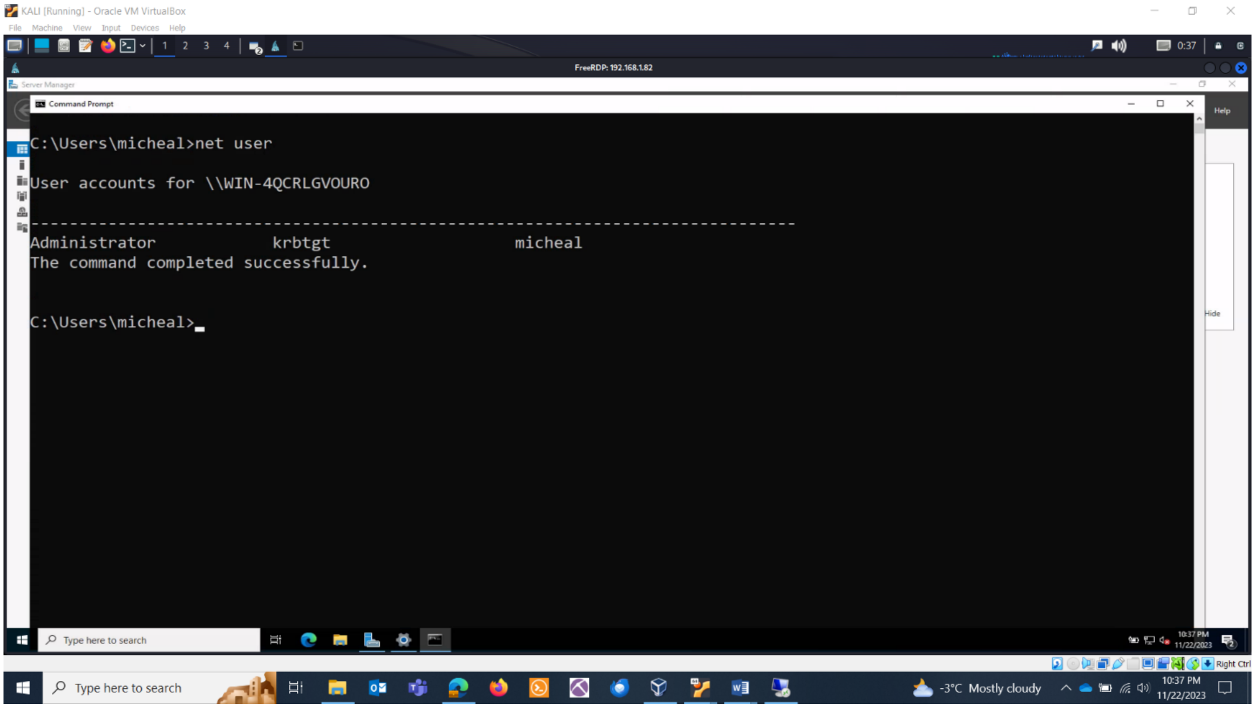


```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\micheal>whoami
web02\micheal

C:\Users\micheal>_
```

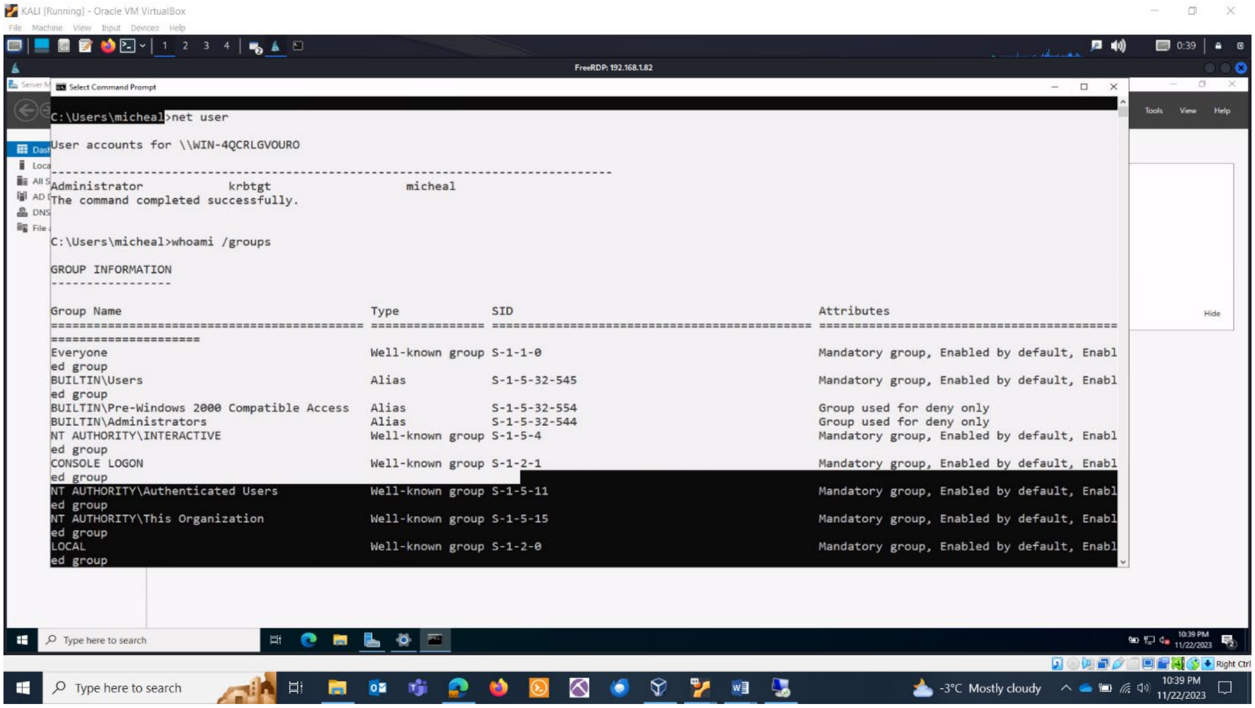
How to connect to this PC

Use this PC name to connect from your remote device:
WIN-4QCRLGVOURO.web02.pentest.net

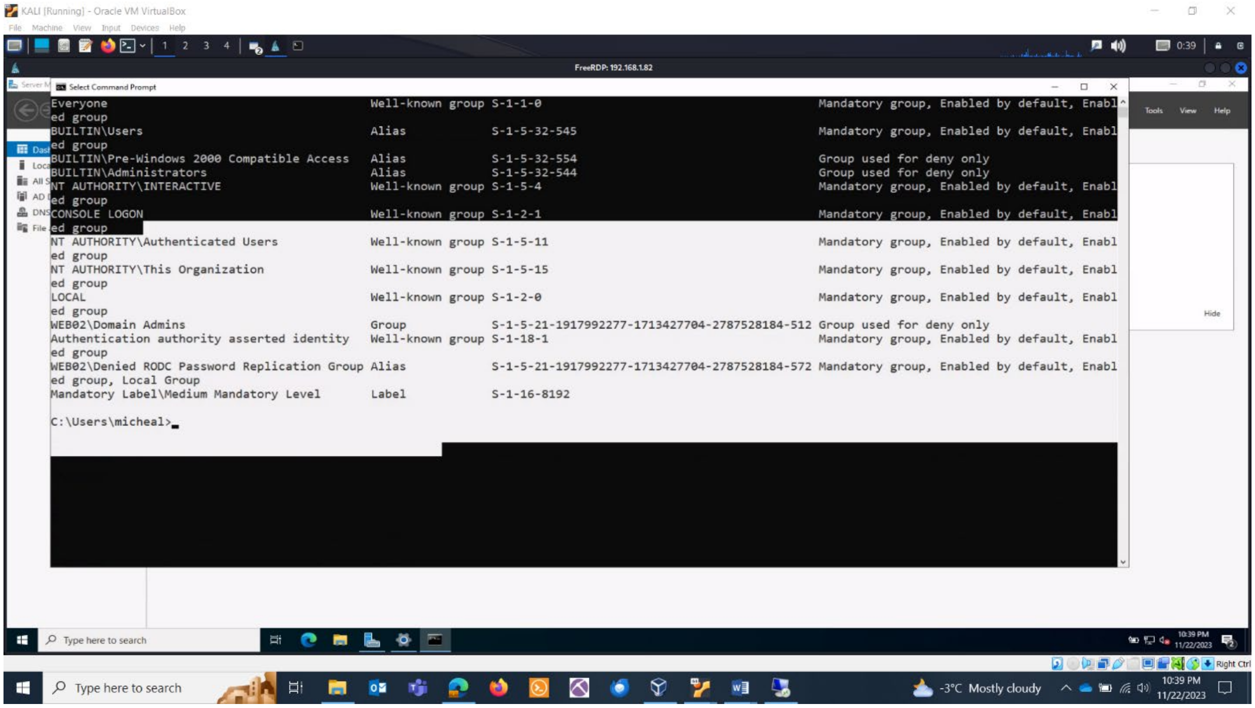
Don't have a Remote Desktop client on your remote device?



```
C:\Users\micheal>net user

User accounts for \\WIN-4QCRLGVOURO

-------------------------------------------------------------------------------
Administrator            krbtgt                   micheal
The command completed successfully.


C:\Users\micheal>_
```



```
C:\Users\micheal>net user

User accounts for \\WIN-4QCRLGVOURO

-------------------------------------------------------------------------------
Administrator            krbtgt                   micheal
The command completed successfully.


C:\Users\micheal>whoami /groups

GROUP INFORMATION
-----------------

Group Name                                   Type             SID                                           Attributes
============================================ ================ ============================================= ==========================================
====================
Everyone                                     Well-known group S-1-1-0                                       Mandatory group, Enabled by default, Enabl
ed group
BUILTIN\Users                                Alias            S-1-5-32-545                                  Mandatory group, Enabled by default, Enabl
ed group
BUILTIN\Pre-Windows 2000 Compatible Access   Alias            S-1-5-32-554                                  Group used for deny only
BUILTIN\Administrators                       Alias            S-1-5-32-544                                  Group used for deny only
NT AUTHORITY\INTERACTIVE                     Well-known group S-1-5-4                                       Mandatory group, Enabled by default, Enabl
ed group
CONSOLE LOGON                                Well-known group S-1-2-1                                       Mandatory group, Enabled by default, Enabl
ed group
NT AUTHORITY\Authenticated Users             Well-known group S-1-5-11                                      Mandatory group, Enabled by default, Enabl
ed group
NT AUTHORITY\This Organization               Well-known group S-1-5-15                                      Mandatory group, Enabled by default, Enabl
ed group
LOCAL                                        Well-known group S-1-2-0                                       Mandatory group, Enabled by default, Enabl
ed group
```



```
Everyone                                     Well-known group S-1-1-0                                       Mandatory group, Enabled by default, Enabl
ed group
BUILTIN\Users                                Alias            S-1-5-32-545                                  Mandatory group, Enabled by default, Enabl
ed group
BUILTIN\Pre-Windows 2000 Compatible Access   Alias            S-1-5-32-554                                  Group used for deny only
BUILTIN\Administrators                       Alias            S-1-5-32-544                                  Group used for deny only
NT AUTHORITY\INTERACTIVE                     Well-known group S-1-5-4                                       Mandatory group, Enabled by default, Enabl
ed group
CONSOLE LOGON                                Well-known group S-1-2-1                                       Mandatory group, Enabled by default, Enabl
ed group
NT AUTHORITY\Authenticated Users             Well-known group S-1-5-11                                      Mandatory group, Enabled by default, Enabl
ed group
NT AUTHORITY\This Organization               Well-known group S-1-5-15                                      Mandatory group, Enabled by default, Enabl
ed group
LOCAL                                        Well-known group S-1-2-0                                       Mandatory group, Enabled by default, Enabl
ed group
WEB02\Domain Admins                          Group            S-1-5-21-1917992277-1713427704-2787528184-512 Group used for deny only
Authentication authority asserted identity   Well-known group S-1-18-1                                      Mandatory group, Enabled by default, Enabl
ed group
WEB02\Denied RODC Password Replication Group Alias            S-1-5-21-1917992277-1713427704-2787528184-572 Mandatory group, Enabled by default, Enabl
ed group, Local Group
Mandatory Label\Medium Mandatory Level       Label            S-1-16-8192

C:\Users\micheal>_
```

POWERSHELL:

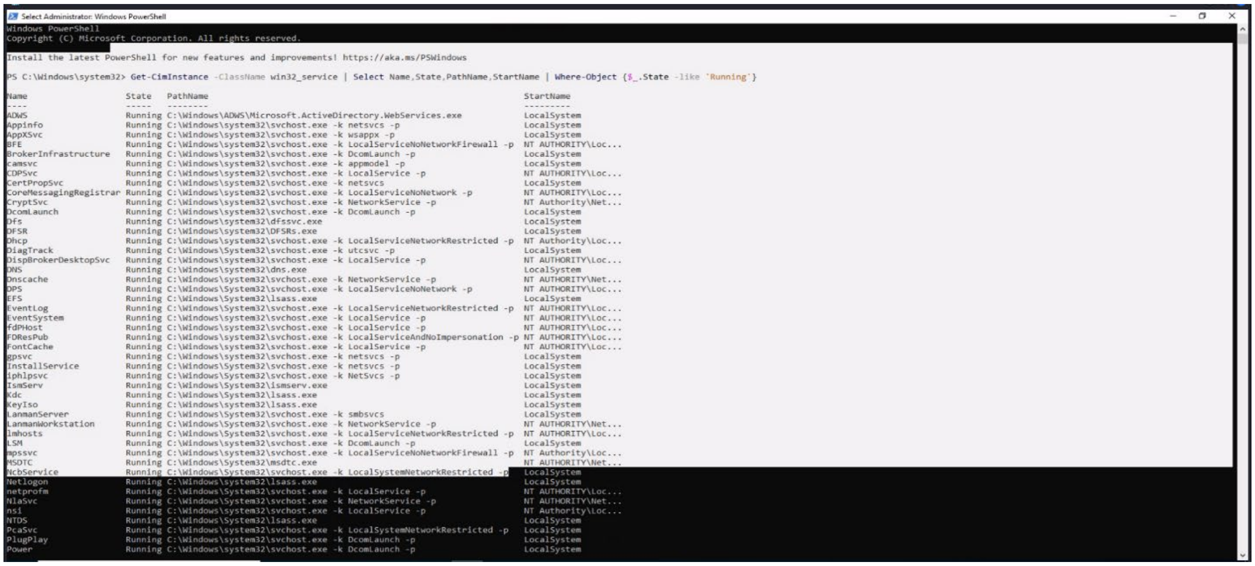
PRIV ESC: **Get-CimInstance -ClassName win32_service | Select Name,State,PathName,StartName | Where-Object {$_.State -like 'Running'}**

The PowerShell command you provided is using the Get-CimInstance cmdlet to retrieve information about Windows services, and then it filters and selects specific properties. Let's break down the command step by step:

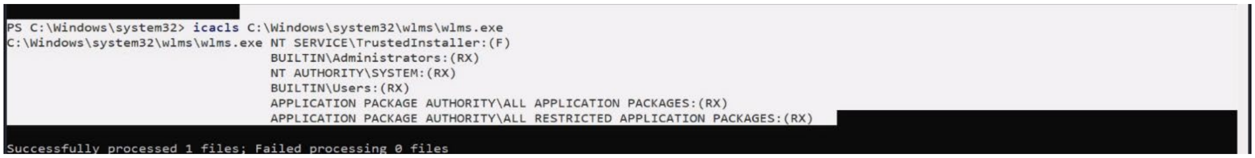
- Get-CimInstance -ClassName Win32_Service: Get-CimInstance is a cmdlet in PowerShell used for querying management information on local and remote computers.
- -ClassName Win32_Service specifies that we want to retrieve instances of the Win32_Service CIM class, which represents information about Windows services.
- | Select-Object Name, State, PathName, StartName: The pipe (|) takes the output from the previous command and passes it to the Select-Object cmdlet.
- Select-Object is used to choose specific properties of the retrieved objects. In this case, it selects the Name, State, PathName, and StartName properties of the Win32_Service instances.
- | Where-Object {$_.State -eq 'Running'}: Another pipe is used to pass the selected properties to the Where-Object cmdlet.Where-Object is used for filtering objects based on a specified condition.
- {$_} represents the current object in the pipeline. $_.State refers to the State property of the current object.The condition -eq 'Running' filters the objects, selecting only those where the state of the service is equal to 'Running'.

So, the overall purpose of this command is to retrieve information about Windows services, specifically selecting the Name, State, PathName, and StartName properties, and then filtering to include only those services where the state is 'Running'. The result is a list of running services with the specified properties.

Run in powershell:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> Get-CimInstance -ClassName win32_service | Select Name,State,PathName,StartName | Where-Object {$_.State -like 'Running'}

Name                     State   PathName                                                         StartName
----                     -----   --------                                                         ---------
ADWS                     Running C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe        LocalSystem
Appinfo                  Running C:\Windows\system32\svchost.exe -k netsvcs -p                    LocalSystem
AppXSvc                  Running C:\Windows\system32\svchost.exe -k wsappx -p                     LocalSystem
BFE                      Running C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p NT AUTHORITY\Loc...
BrokerInfrastructure     Running C:\Windows\system32\svchost.exe -k DcomLaunch -p                 LocalSystem
camsvc                   Running C:\Windows\system32\svchost.exe -k appmodel -p                   LocalSystem
CDPSvc                   Running C:\Windows\system32\svchost.exe -k LocalService -p               NT AUTHORITY\Loc...
CertPropSvc              Running C:\Windows\system32\svchost.exe -k netsvcs                       LocalSystem
CoreMessagingRegistrar   Running C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p      NT AUTHORITY\Loc...
CryptSvc                 Running C:\Windows\system32\svchost.exe -k NetworkService -p             NT Authority\Net...
DcomLaunch               Running C:\Windows\system32\svchost.exe -k DcomLaunch -p                 LocalSystem
Dfs                      Running C:\Windows\system32\dfssvc.exe                                   LocalSystem
DFSR                     Running C:\Windows\system32\DFSRs.exe                                    LocalSystem
Dhcp                     Running C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p NT Authority\Loc...
DiagTrack                Running C:\Windows\System32\svchost.exe -k utcsvc -p                     LocalSystem
DispBrokerDesktopSvc     Running C:\Windows\system32\svchost.exe -k LocalService -p               NT AUTHORITY\Loc...
DNS                      Running C:\Windows\system32\dns.exe                                      LocalSystem
Dnscache                 Running C:\Windows\system32\svchost.exe -k NetworkService -p             NT AUTHORITY\Net...
DPS                      Running C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork -p      NT AUTHORITY\Loc...
EFS                      Running C:\Windows\System32\lsass.exe                                    LocalSystem
EventLog                 Running C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p NT AUTHORITY\Loc...
EventSystem              Running C:\Windows\system32\svchost.exe -k LocalService -p               NT AUTHORITY\Loc...
fdPHost                  Running C:\Windows\system32\svchost.exe -k LocalService -p               NT AUTHORITY\Loc...
FDResPub                 Running C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p NT AUTHORITY\Loc...
FontCache                Running C:\Windows\system32\svchost.exe -k LocalService -p               NT AUTHORITY\Loc...
gpsvc                    Running C:\Windows\system32\svchost.exe -k netsvcs -p                    LocalSystem
InstallService           Running C:\Windows\System32\svchost.exe -k netsvcs -p                    LocalSystem
iphlpsvc                 Running C:\Windows\System32\svchost.exe -k NetSvcs -p                    LocalSystem
IsmServ                  Running C:\Windows\System32\ismserv.exe                                  LocalSystem
Kdc                      Running C:\Windows\System32\lsass.exe                                    LocalSystem
KeyIso                   Running C:\Windows\system32\lsass.exe                                    LocalSystem
LanmanServer             Running C:\Windows\System32\svchost.exe -k smbsvcs                       LocalSystem
LanmanWorkstation        Running C:\Windows\System32\svchost.exe -k NetworkService -p             NT AUTHORITY\Net...
lmhosts                  Running C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p NT AUTHORITY\Loc...
LSM                      Running C:\Windows\system32\svchost.exe -k DcomLaunch -p                 LocalSystem
mpssvc                   Running C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p NT Authority\Loc...
MSDTC                    Running C:\Windows\System32\msdtc.exe                                    NT AUTHORITY\Net...
NcbService               Running C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p LocalSystem
Netlogon                 Running C:\Windows\system32\lsass.exe                                    LocalSystem
netprofm                 Running C:\Windows\System32\svchost.exe -k LocalService -p               NT AUTHORITY\Loc...
NlaSvc                   Running C:\Windows\System32\svchost.exe -k NetworkService -p             NT AUTHORITY\Net...
nsi                      Running C:\Windows\system32\svchost.exe -k LocalService -p               NT Authority\Loc...
NTDS                     Running C:\Windows\System32\lsass.exe                                    LocalSystem
PcaSvc                   Running C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p LocalSystem
PlugPlay                 Running C:\Windows\system32\svchost.exe -k DcomLaunch -p                 LocalSystem
Power                    Running C:\Windows\system32\svchost.exe -k DcomLaunch -p                 LocalSystem
```



```
PS C:\Windows\system32> icacls C:\Windows\system32\wlms\wlms.exe
C:\Windows\system32\wlms\wlms.exe NT SERVICE\TrustedInstaller:(F)
                                  BUILTIN\Administrators:(RX)
                                  NT AUTHORITY\SYSTEM:(RX)
                                  BUILTIN\Users:(RX)
                                  APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
                                  APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)

Successfully processed 1 files; Failed processing 0 files
```