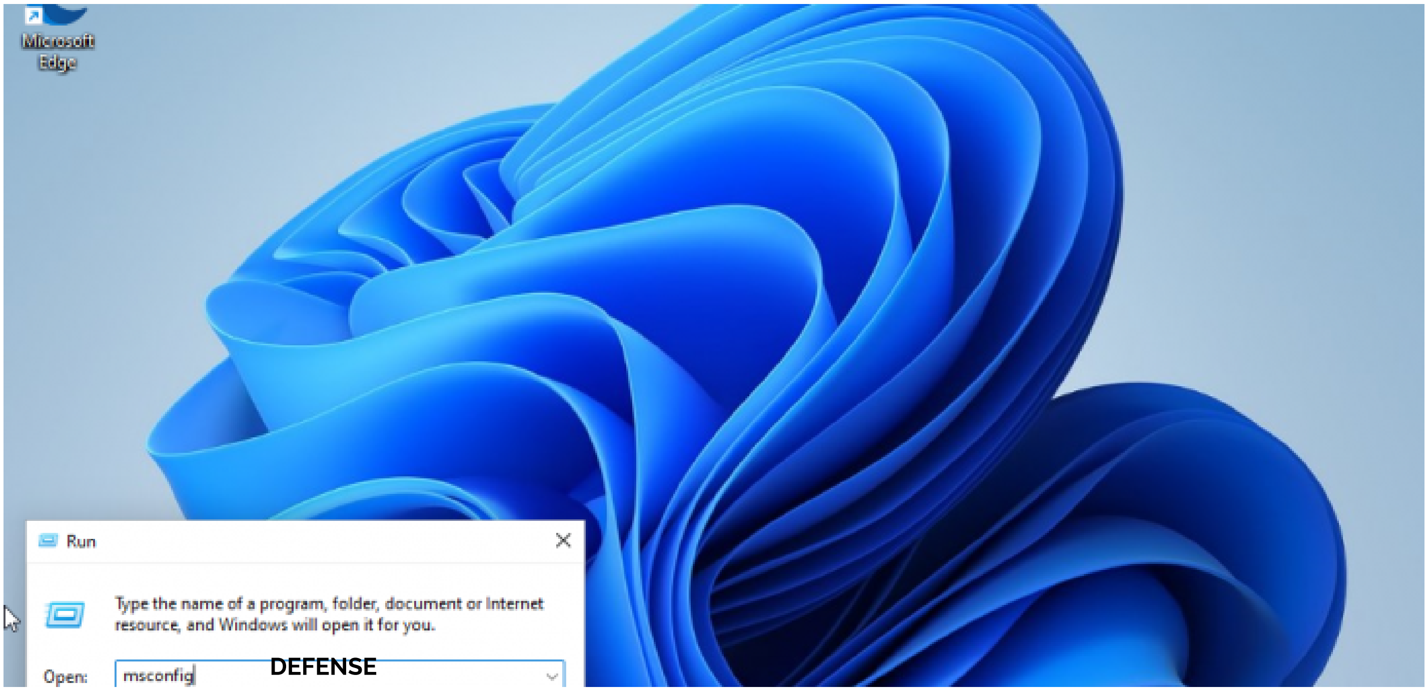
(https://www.pwndefend.com/)



Type the name of a program, folder, document or Internet resource, and Windows will open it for you.

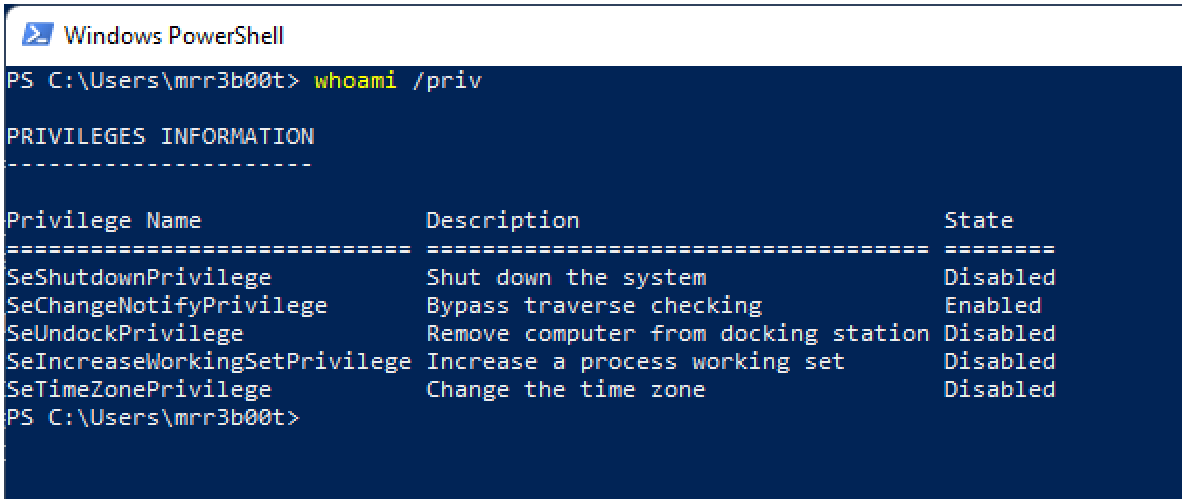
Open: msconfig

(https://www.pwndefend.com/2021/08/23/windows-11-privilege-escalation-via-uac-bypass-gui-based/)

Introduction

Ok these are a really simple UAC bypass from a userland GUI perspective. This is about increasing process integrity levels – it's not about performing LPE from low integrity to high/SYSTEM with no interaction. These clearly work in older version of Windows as well but since Windows 11 will be the current version in the near future I thought it was fun to re-visit these!

And just to be clear, a medium integrity process as an administrator user will have the following privileges:

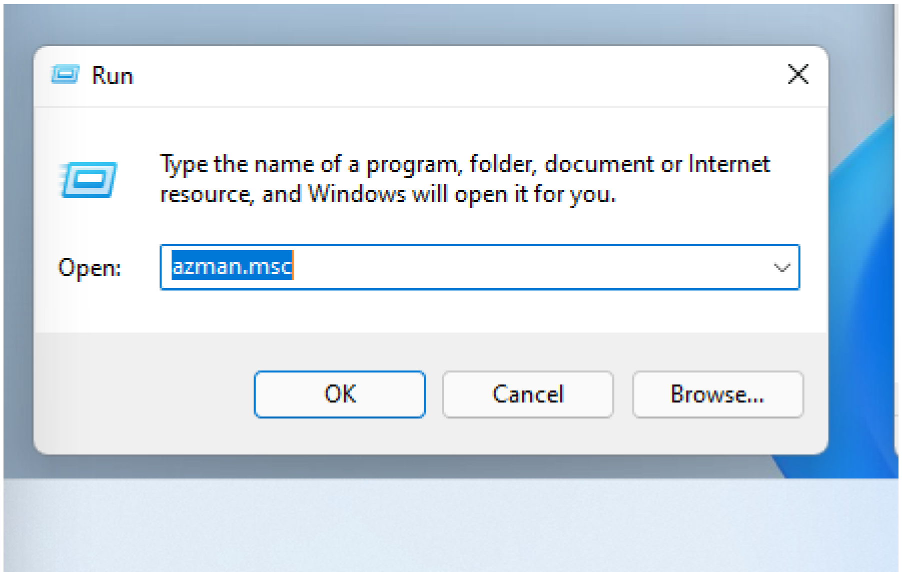


```
PS C:\Users\mrr3b00t> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
PS C:\Users\mrr3b00t>
```

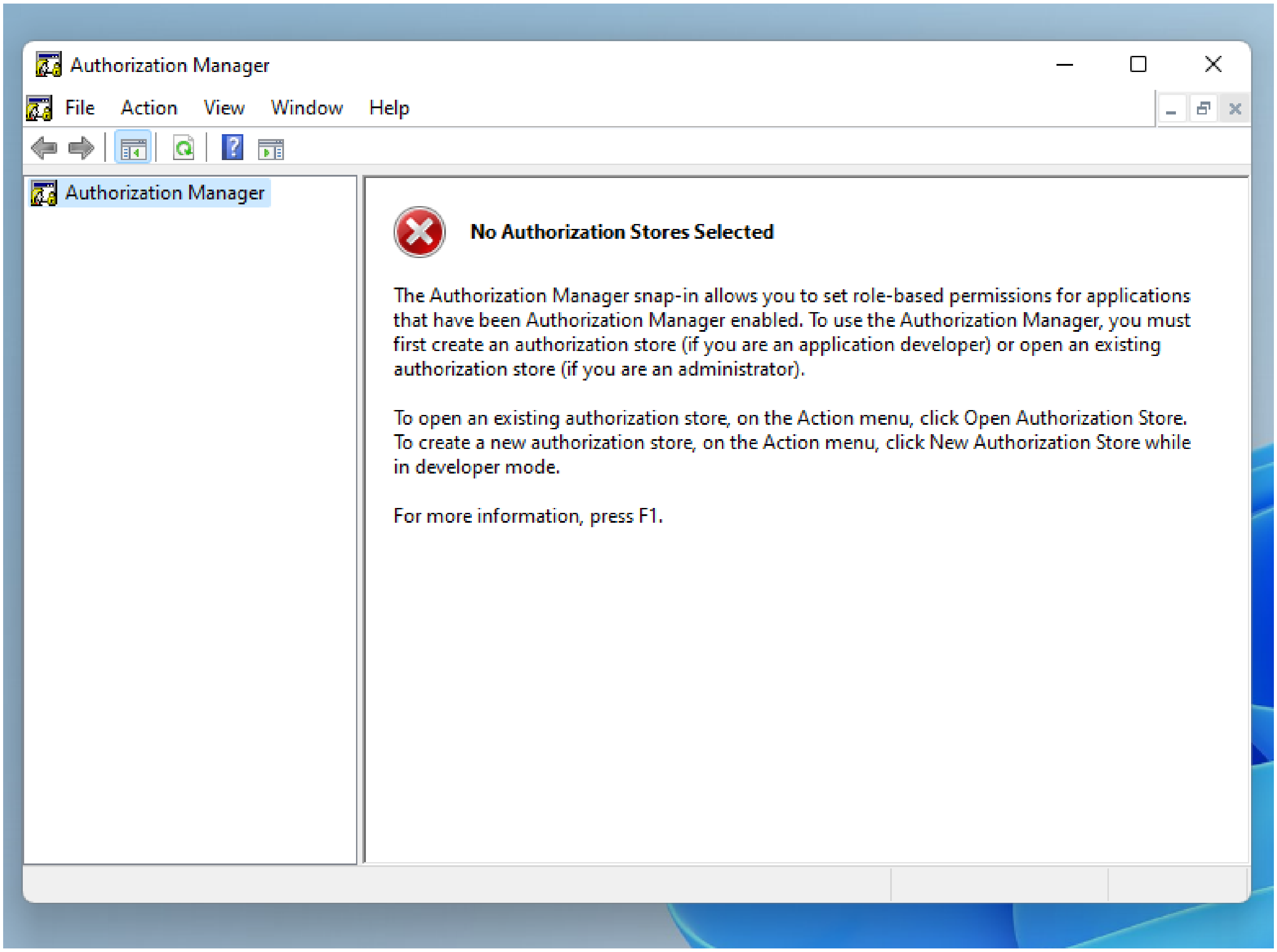
What we are talking about here is to move to a high integrity process without knowing credentials or having the secure desktop launch.

AZMAN.MSC

Run azman.msc


Run
Type the name of a program, folder, document or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

Open: azman.msc



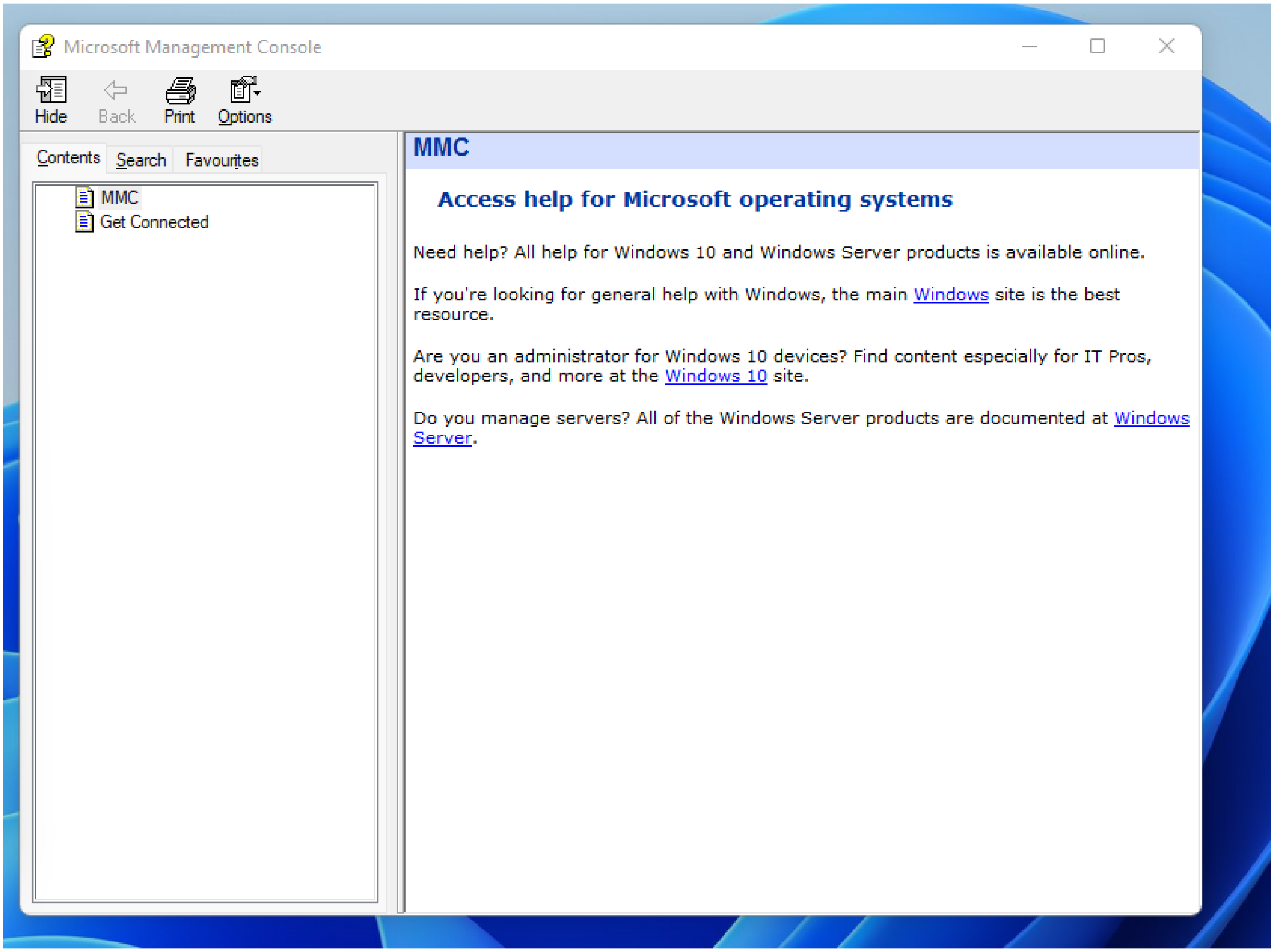
No Authorization Stores Selected

The Authorization Manager snap-in allows you to set role-based permissions for applications that have been Authorization Manager enabled. To use the Authorization Manager, you must first create an authorization store (if you are an application developer) or open an existing authorization store (if you are an administrator).

To open an existing authorization store, on the Action menu, click Open Authorization Store. To create a new authorization store, on the Action menu, click New Authorization Store while in developer mode.

For more information, press F1.

Click Help



MMC

Access help for Microsoft operating systems

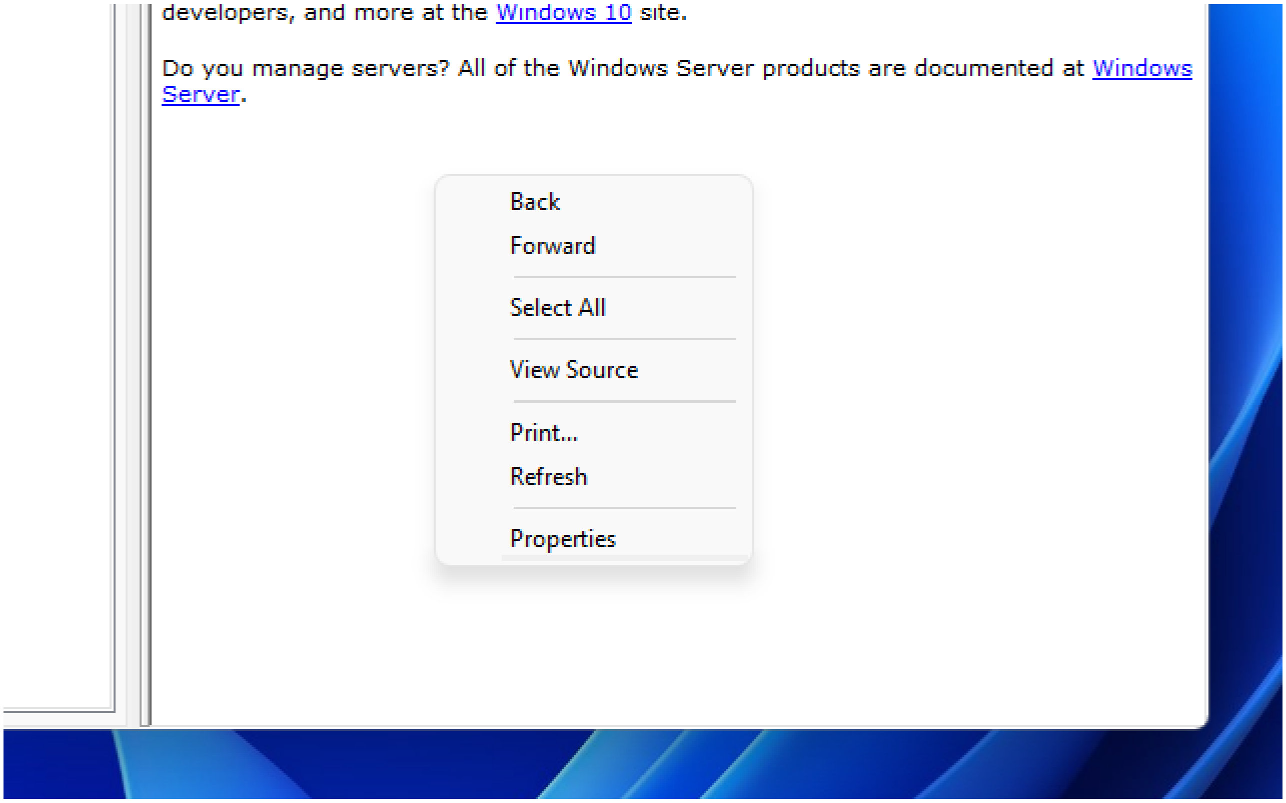
Need help? All help for Windows 10 and Windows Server products is available online.

If you're looking for general help with Windows, the main Windows site is the best resource.

Are you an administrator for Windows 10 devices? Find content especially for IT Pros, developers, and more at the Windows 10 site.

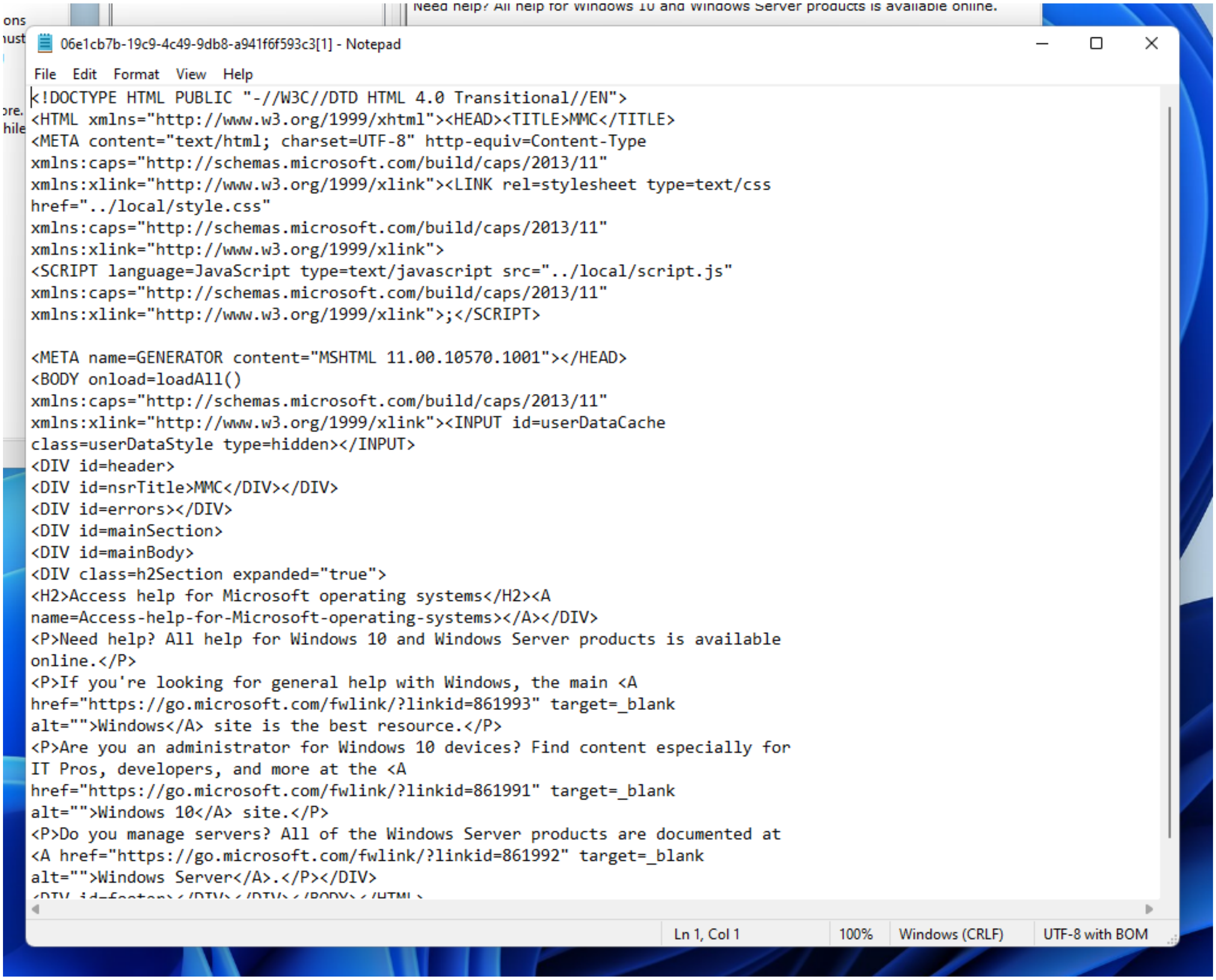
Do you manage servers? All of the Windows Server products are documented at Windows Server.

Right click on the right-hand pane and click VIEW SOURCE



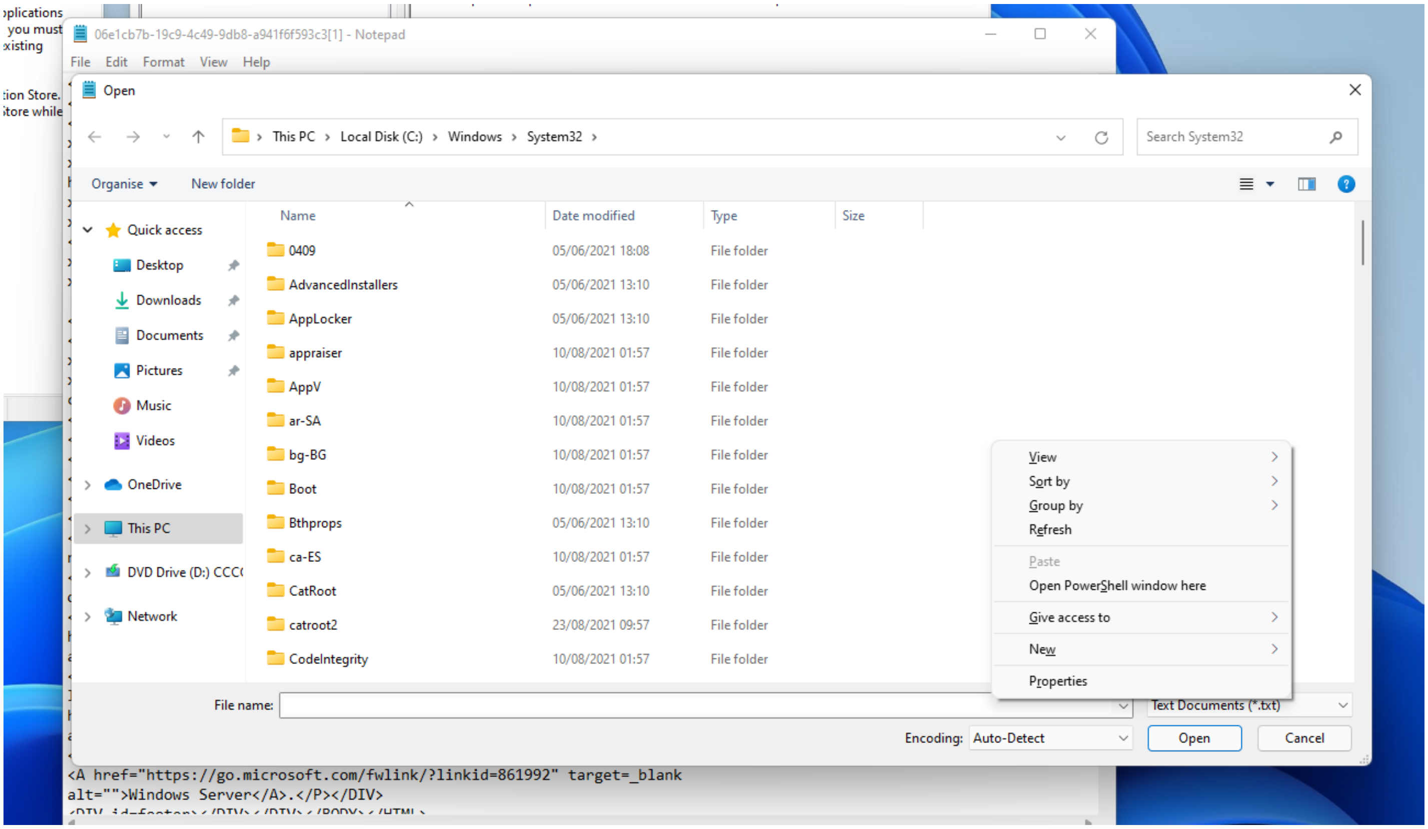
developers, and more at the Windows 10 site.

Do you manage servers? All of the Windows Server products are documented at Windows Server.


Need help? All help for Windows 10 and Windows Server products is available online.
06e1cb7b-19c9-4c49-9db8-a941f6f593c3[1] - Notepad
File
Edit
Format
View
Help
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8 with BOM

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML xmlns="http://www.w3.org/1999/xhtml"><HEAD><TITLE>MMC</TITLE>
<META content="text/html; charset=UTF-8" http-equiv=Content-Type
xmlns:caps="http://schemas.microsoft.com/build/caps/2013/11"
xmlns:xlink="http://www.w3.org/1999/xlink"><LINK rel=stylesheet type=text/css
href="../local/style.css"
xmlns:caps="http://schemas.microsoft.com/build/caps/2013/11"
xmlns:xlink="http://www.w3.org/1999/xlink">
<SCRIPT language=JavaScript type=text/javascript src="../local/script.js"
xmlns:caps="http://schemas.microsoft.com/build/caps/2013/11"
xmlns:xlink="http://www.w3.org/1999/xlink">;</SCRIPT>

<META name=GENERATOR content="MSHTML 11.00.10570.1001"></HEAD>
<BODY onload=loadAll()
xmlns:caps="http://schemas.microsoft.com/build/caps/2013/11"
xmlns:xlink="http://www.w3.org/1999/xlink"><INPUT id=userDataCache
class=userDataStyle type=hidden></INPUT>
<DIV id=header>
<DIV id=nsrTitle>MMC</DIV></DIV>
<DIV id=errors></DIV>
<DIV id=mainSection>
<DIV id=mainBody>
<DIV class=h2Section expanded="true">
<H2>Access help for Microsoft operating systems</H2><A
name=Access-help-for-Microsoft-operating-systems></A></DIV>
<P>Need help? All help for Windows 10 and Windows Server products is available
online.</P>
<P>If you're looking for general help with Windows, the main <A
href="https://go.microsoft.com/fwlink/?linkid=861993" target=_blank
alt="">Windows</A> site is the best resource.</P>
<P>Are you an administrator for Windows 10 devices? Find content especially for
IT Pros, developers, and more at the <A
href="https://go.microsoft.com/fwlink/?linkid=861991" target=_blank
alt="">Windows 10</A> site.</P>
<P>Do you manage servers? All of the Windows Server products are documented at
<A href="https://go.microsoft.com/fwlink/?linkid=861992" target=_blank
alt="">Windows Server</A>.</P></DIV>
<DIV id=footer></DIV></DIV></BODY></HTML>
```

From notepad click FILE OPEN

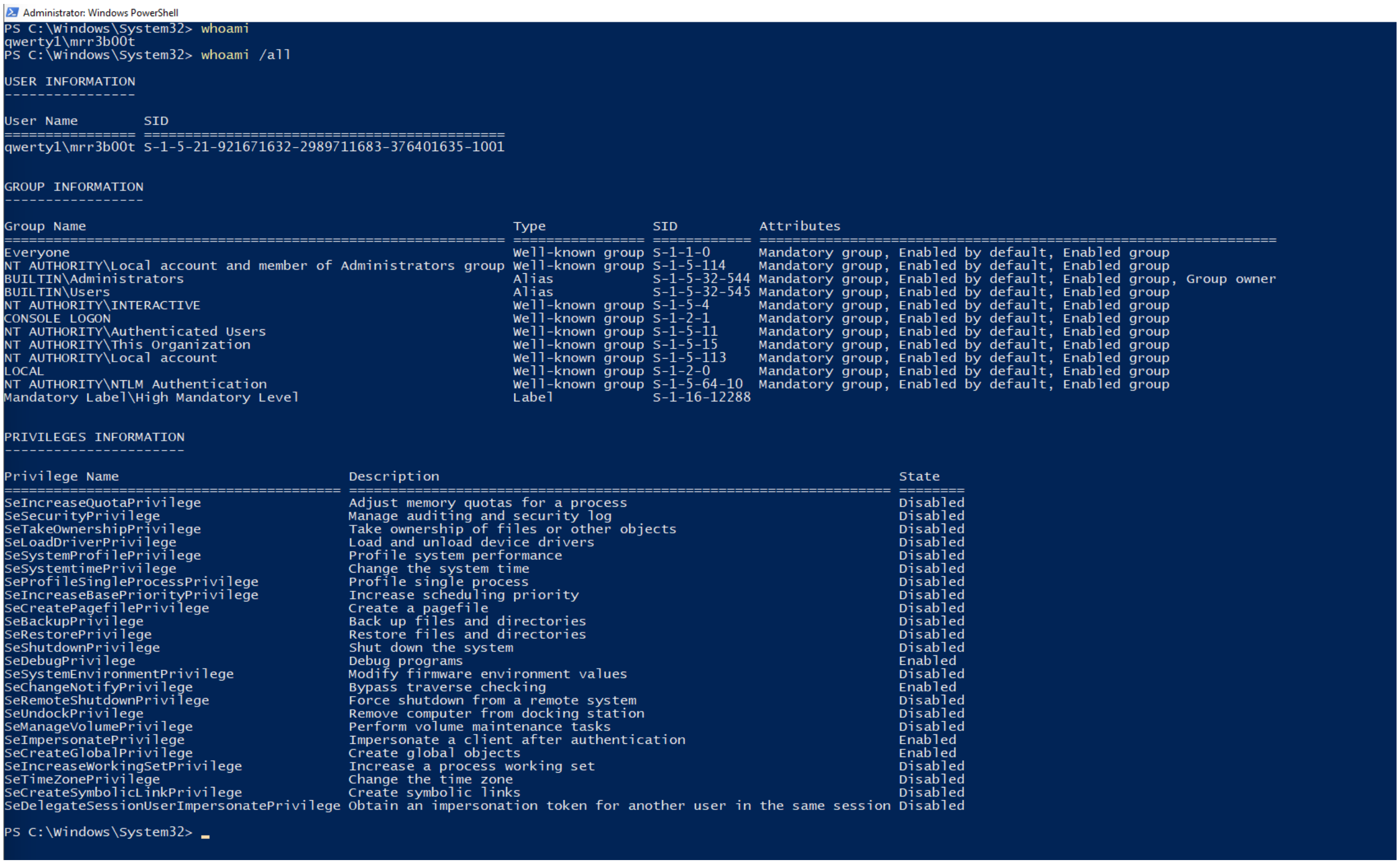


```
Name                 Date modified      Type         Size
0409                 05/06/2021 18:08   File folder
AdvancedInstallers   05/06/2021 13:10   File folder
AppLocker            05/06/2021 13:10   File folder
appraiser            10/08/2021 01:57   File folder
AppV                 10/08/2021 01:57   File folder
ar-SA                10/08/2021 01:57   File folder
bg-BG                10/08/2021 01:57   File folder
Boot                 10/08/2021 01:57   File folder
Bthprops             05/06/2021 13:10   File folder
ca-ES                10/08/2021 01:57   File folder
CatRoot              05/06/2021 13:10   File folder
catroot2             23/08/2021 09:57   File folder
CodeIntegrity        10/08/2021 01:57   File folder
```

```
<A href="https://go.microsoft.com/fwlink/?linkid=861992" target=_blank
alt="">Windows Server</A>.</P></DIV>
<DIV id=footer></DIV></DIV></BODY></HTML>
```

Right click + shift and click open powershell window here

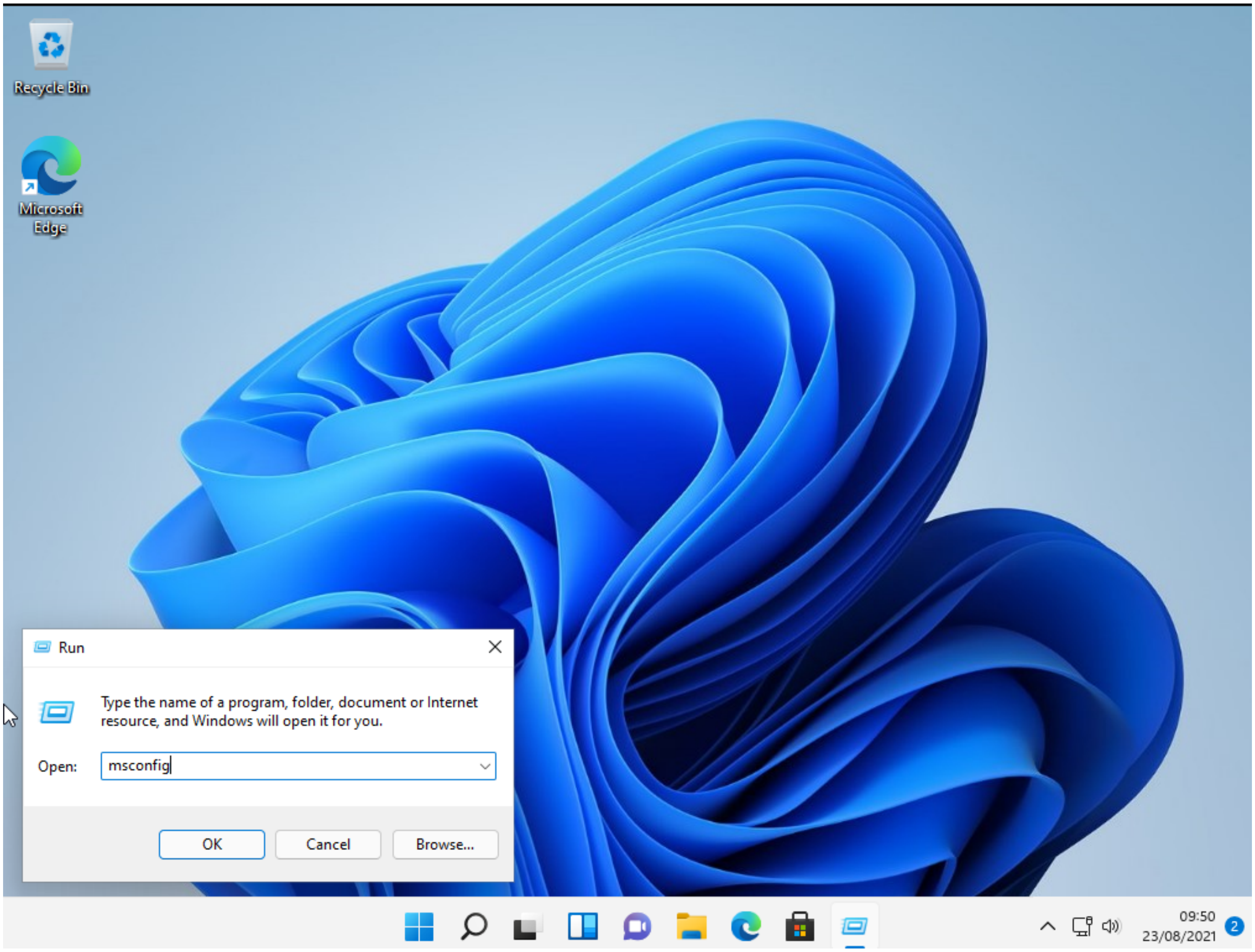
And now you have a process with high integrity



```
PS C:\Windows\System32> whoami
qwerty1\mrr3b00t
PS C:\Windows\System32> whoami /all

USER INFORMATION
----------------

User Name        SID
================ ============================================
qwerty1\mrr3b00t S-1-5-21-921671632-2989711683-376401635-1001


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

Group Name                                                    Type             SID          Attributes
============================================================= ================ ============ ==============================================================
Everyone                                                      Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114    Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                                        Alias            S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Users                                                 Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                                      Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                                                 Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users                              Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization                                Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account                                    Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                                         Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication                              Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level                          Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled

PS C:\Windows\System32> _
```

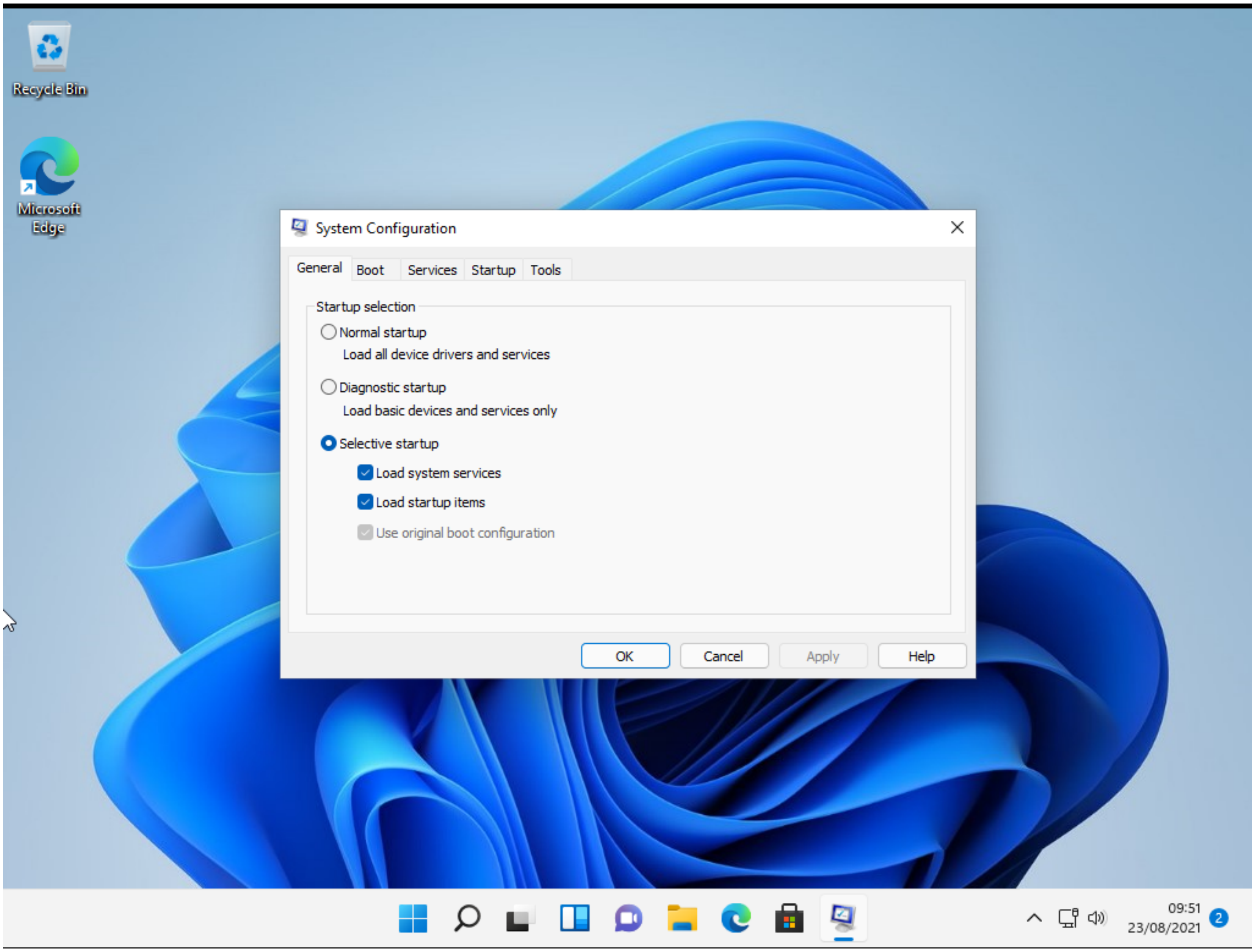
Msconfig UAC Bypass

The use case for this bypass is when you have access to the session but DO NOT have the credentials.



Type the name of a program, folder, document or Internet resource, and Windows will open it for you.

Open: msconfig



System Configuration

General | Boot | Services | Startup | Tools

Startup selection

○ Normal startup
Load all device drivers and services

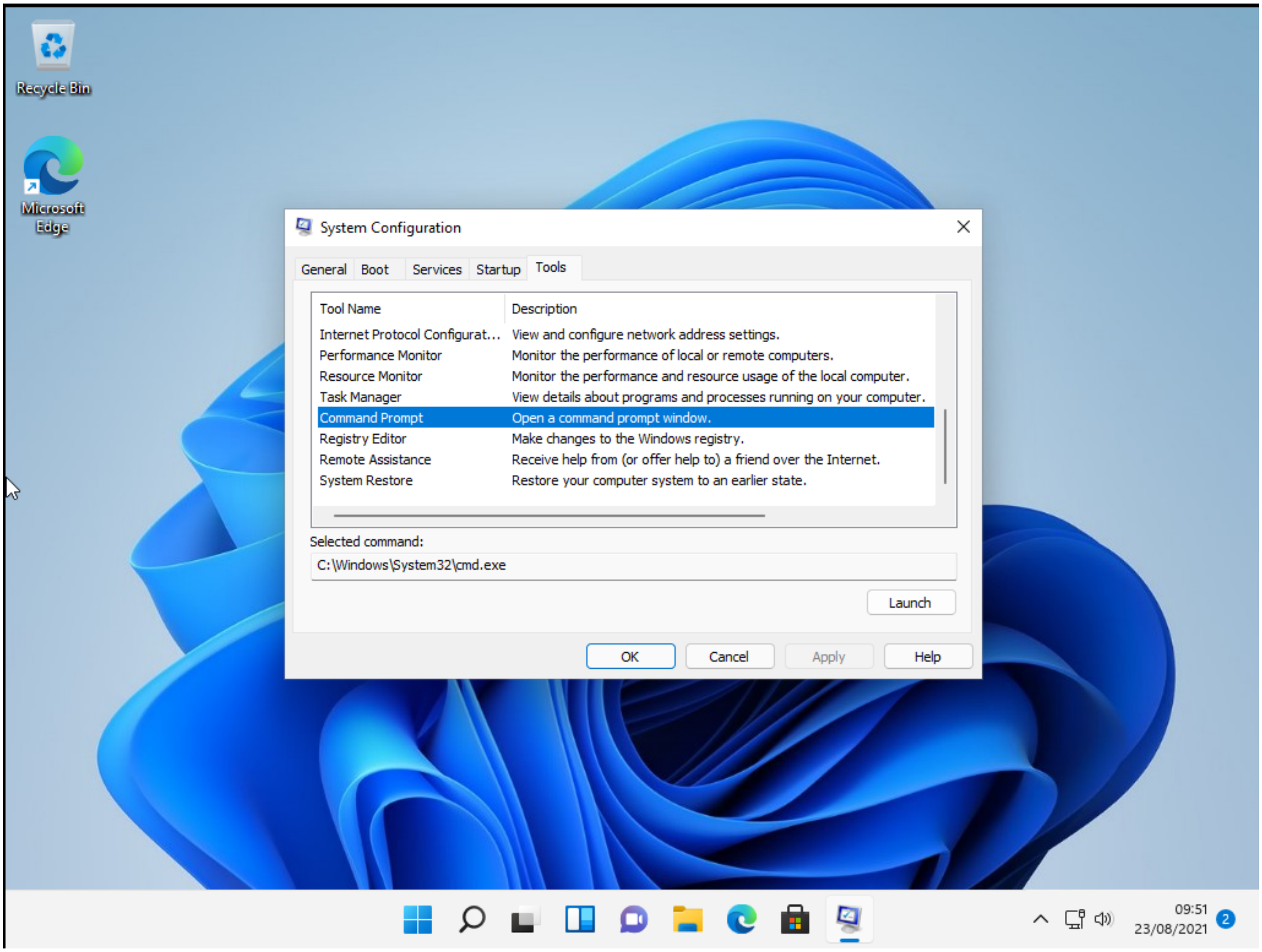
○ Diagnostic startup
Load basic devices and services only

● Selective startup

☑ Load system services

☑ Load startup items

☑ Use original boot configuration

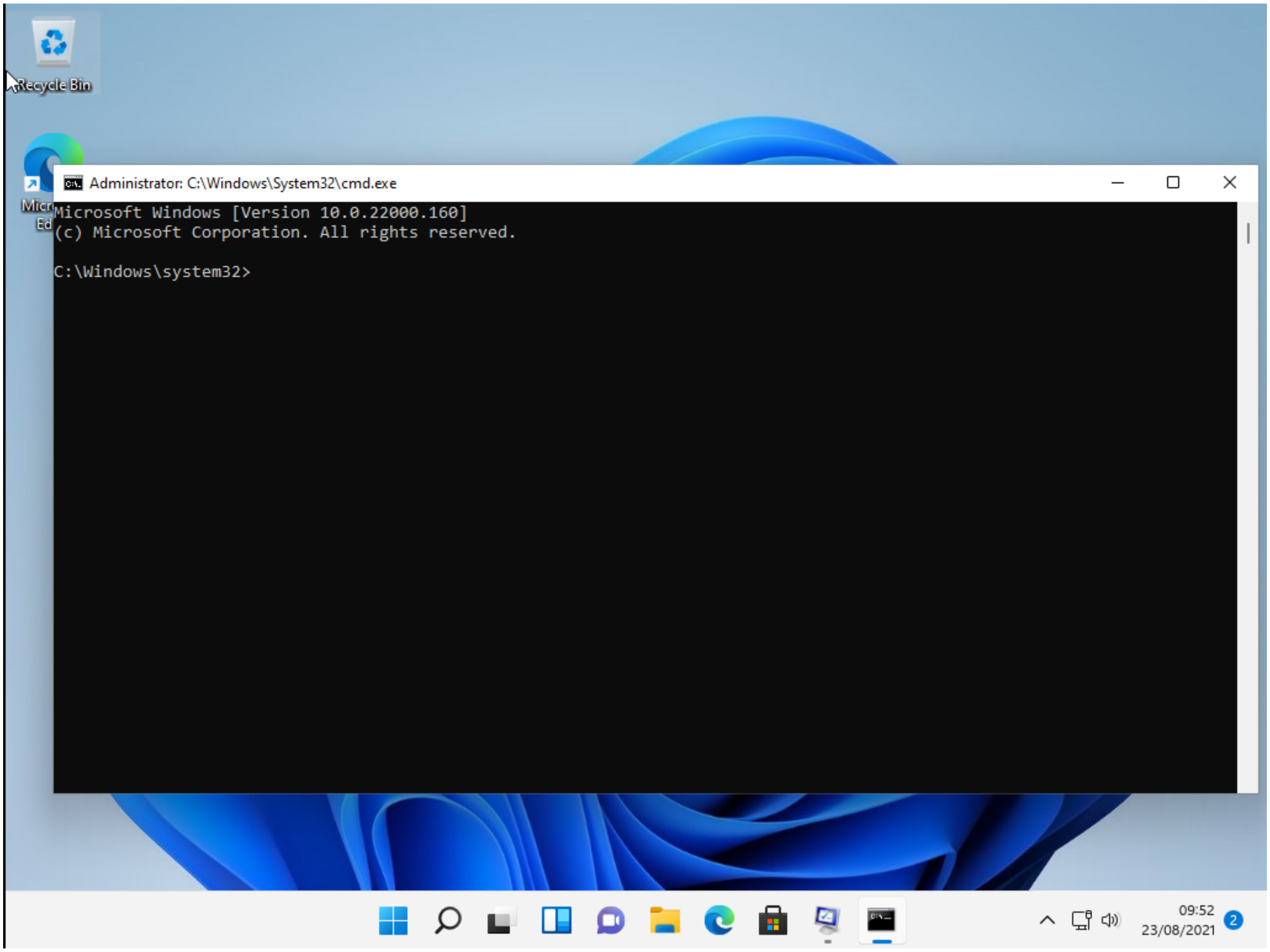


System Configuration

Tool Name	Description
Internet Protocol Configurat...	View and configure network address settings.
Performance Monitor	Monitor the performance of local or remote computers.
Resource Monitor	Monitor the performance and resource usage of the local computer.
Task Manager	View details about programs and processes running on your computer.
Command Prompt	Open a command prompt window.
Registry Editor	Make changes to the Windows registry.
Remote Assistance	Receive help from (or offer help to) a friend over the Internet.
System Restore	Restore your computer system to an earlier state.

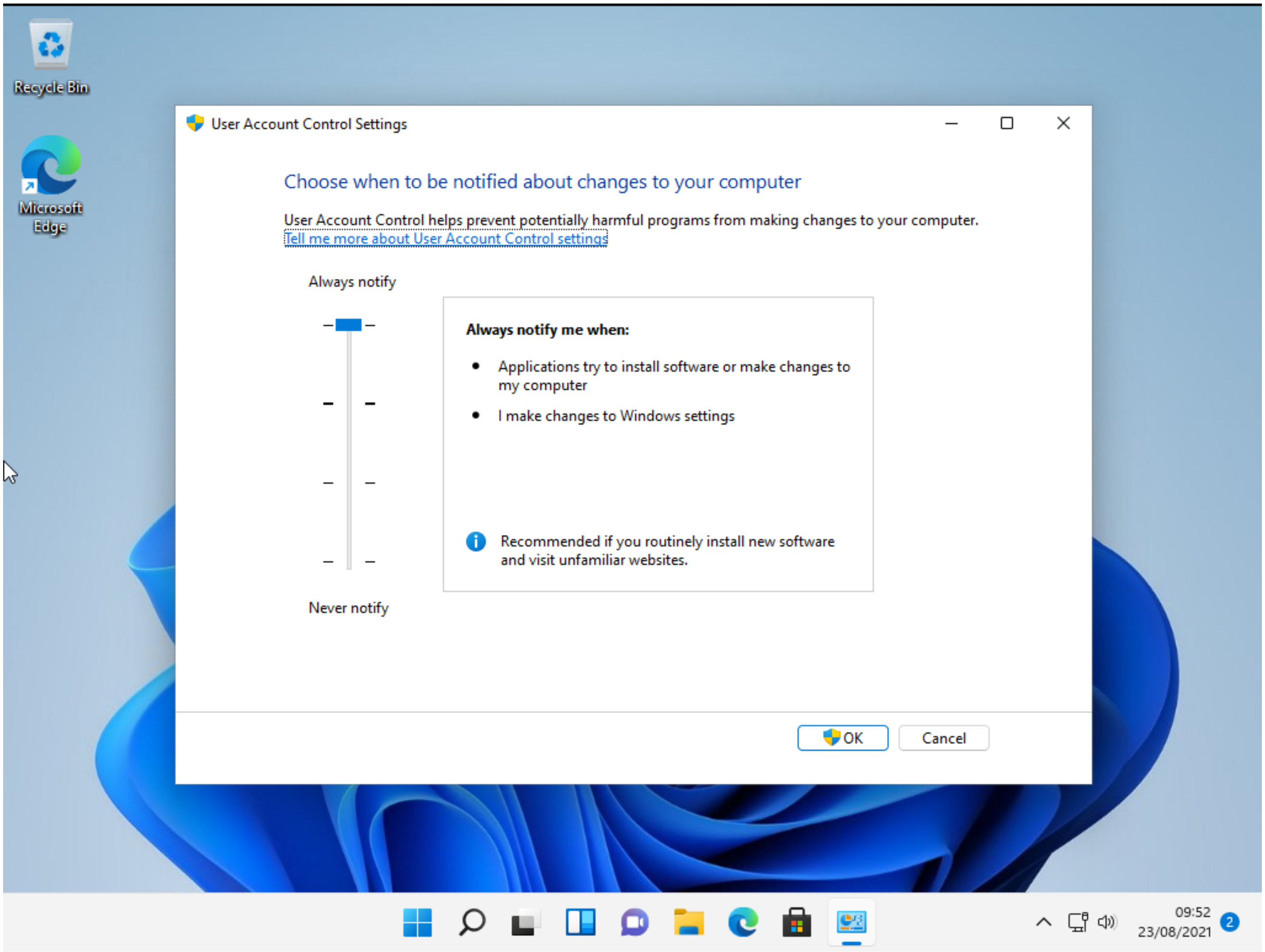
Selected command:

C:\Windows\System32\cmd.exe



```
Microsoft Windows [Version 10.0.22000.160]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

The mitigation for this is to set UAC to the maximum level


User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

Always notify me when:

- Applications try to install software or make changes to my computer
- I make changes to Windows settings

Recommended if you routinely install new software and visit unfamiliar websites.

Never notify

iscsicpl.exe

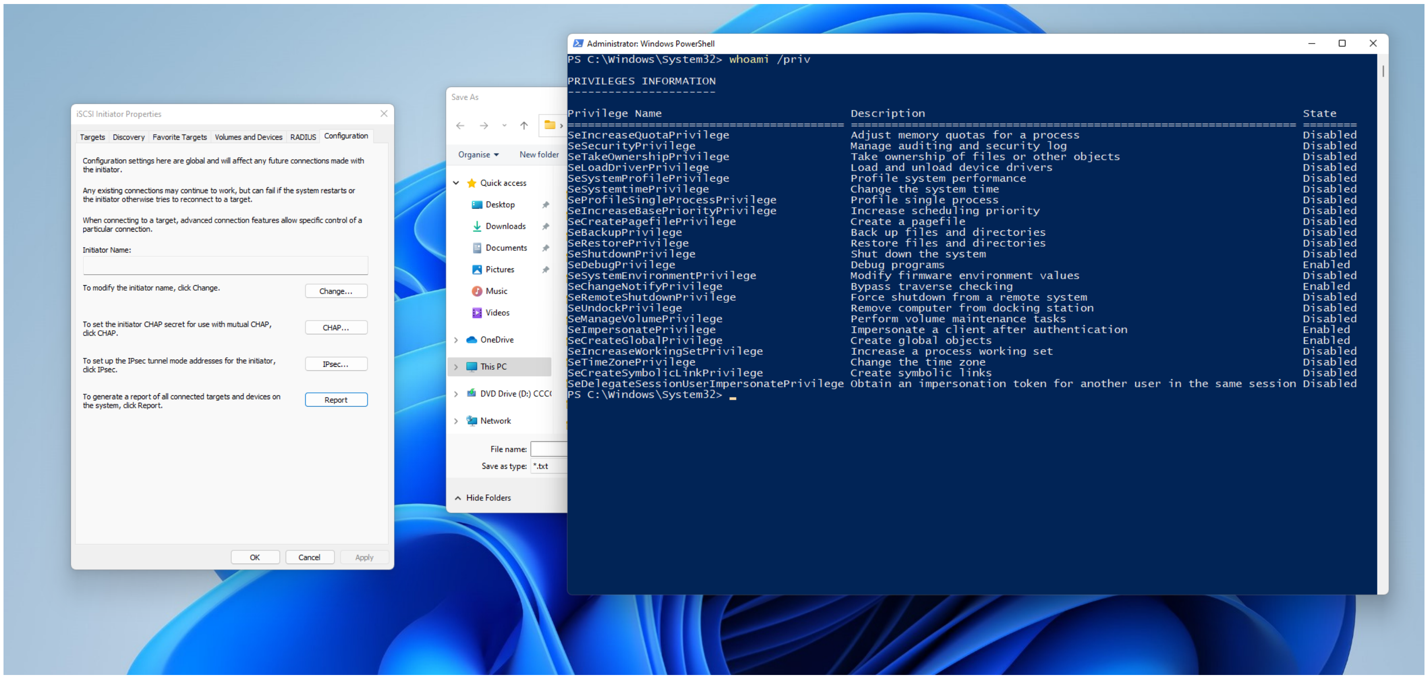
Another method comes from running c:\windows\system32\iscsicpl.exe

Click No

Click CONFIGURATION

Click REPORT

Right Click + SHIFT and Open Powershell



Configuration settings here are global and will affect any future connections made with the initiator.

Any existing connections may continue to work, but can fail if the system restarts or the initiator otherwise tries to reconnect to a target.

When connecting to a target, advanced connection features allow specific control of a particular connection.

Initiator Name:

To modify the initiator name, click Change.

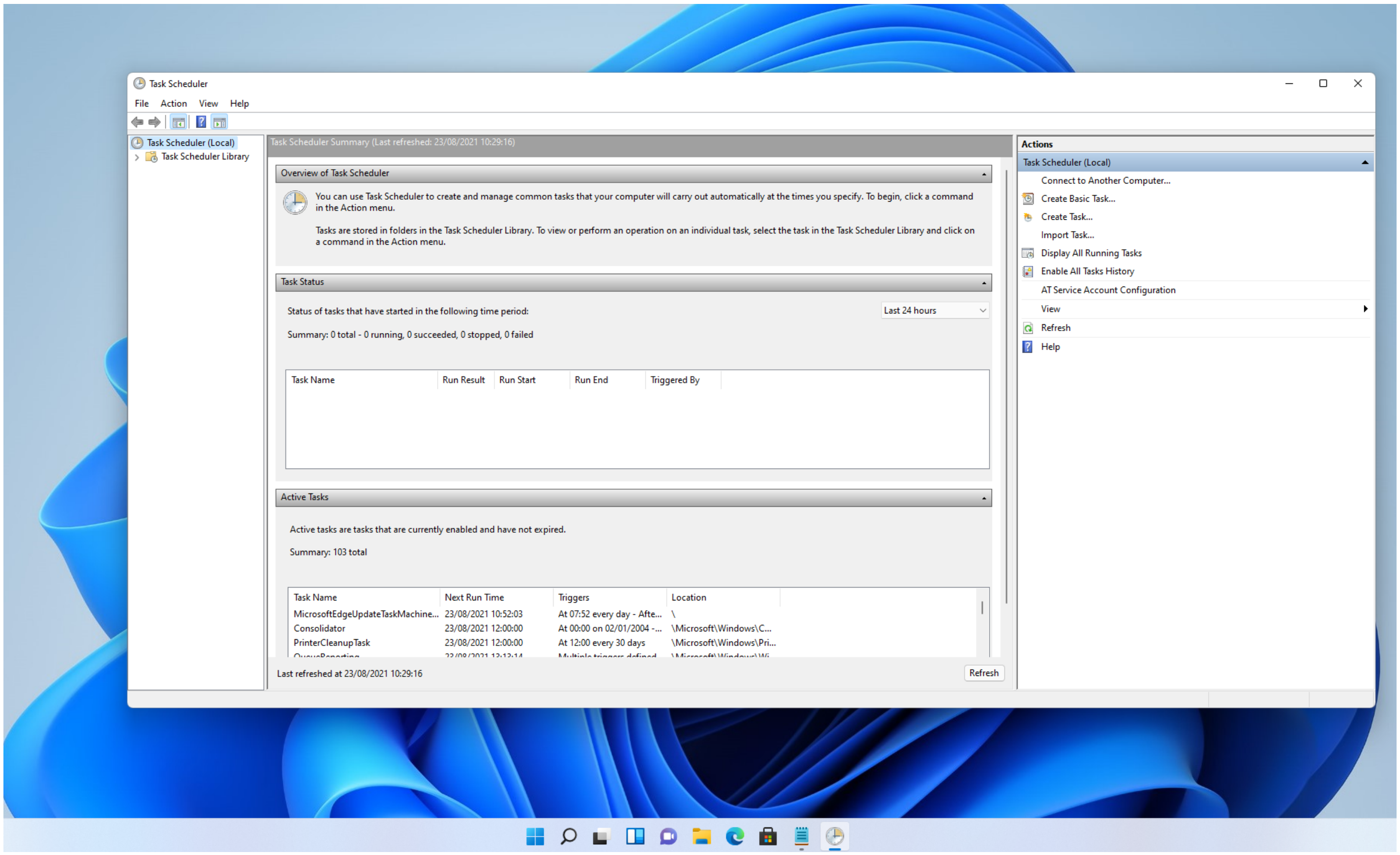
To set the initiator CHAP secret for use with mutual CHAP, click CHAP.

To set up the IPsec tunnel mode addresses for the initiator, click IPsec.

To generate a report of all connected targets and devices on the system, click Report.

```
PS C:\Windows\System32> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled
PS C:\Windows\System32> _
```

Task Scheduler



Task Scheduler Summary (Last refreshed: 23/08/2021 10:29:16)

You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

Tasks are stored in folders in the Task Scheduler Library. To view or perform an operation on an individual task, select the task in the Task Scheduler Library and click on a command in the Action menu.

Status of tasks that have started in the following time period: Last 24 hours

Summary: 0 total - 0 running, 0 succeeded, 0 stopped, 0 failed

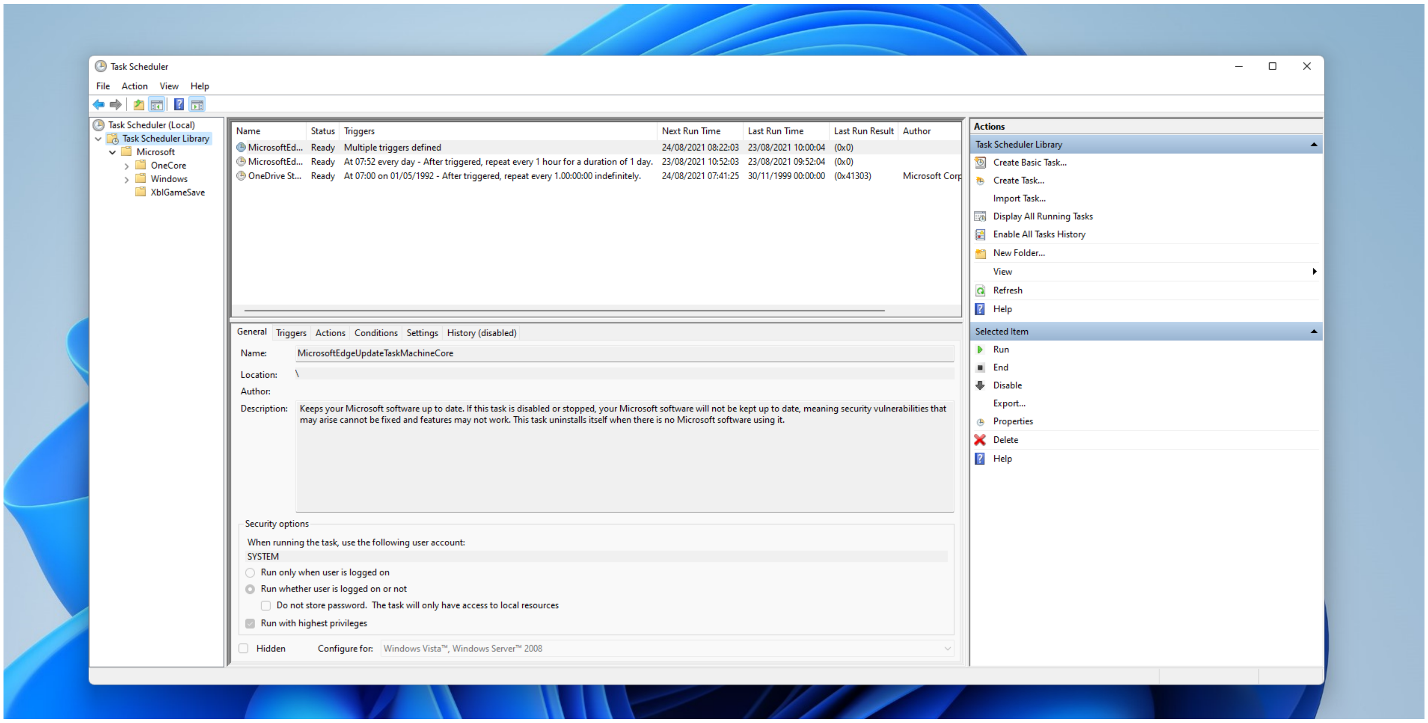
Task Name	Run Result	Run Start	Run End	Triggered By

Active tasks are tasks that are currently enabled and have not expired.

Summary: 103 total

Task Name	Next Run Time	Triggers	Location
MicrosoftEdgeUpdateTaskMachine...	23/08/2021 10:52:03	At 07:52 every day - Afte...	\
Consolidator	23/08/2021 12:00:00	At 00:00 on 02/01/2004 -...	\Microsoft\Windows\C...
PrinterCleanupTask	23/08/2021 12:00:00	At 12:00 every 30 days	\Microsoft\Windows\Pri...
QueueReporting	23/08/2021 12:13:14	Multiple triggers defined	\Microsoft\Windows\Wi...

Last refreshed at 23/08/2021 10:29:16



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author
MicrosoftEd...	Ready	Multiple triggers defined	24/08/2021 08:22:03	23/08/2021 10:00:04	(0x0)	
MicrosoftEd...	Ready	At 07:52 every day - After triggered, repeat every 1 hour for a duration of 1 day.	23/08/2021 10:52:03	23/08/2021 09:52:04	(0x0)	
OneDrive St...	Ready	At 07:00 on 01/05/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	24/08/2021 07:41:25	30/11/1999 00:00:00	(0x41303)	Microsoft Corp

General Triggers Actions Conditions Settings History (disabled)

Name: MicrosoftEdgeUpdateTaskMachineCore

Location: \

Author:

Description: Keeps your Microsoft software up to date. If this task is disabled or stopped, your Microsoft software will not be kept up to date, meaning security vulnerabilities that may arise cannot be fixed and features may not work. This task uninstalls itself when there is no Microsoft software using it.

Security options

When running the task, use the following user account:

SYSTEM

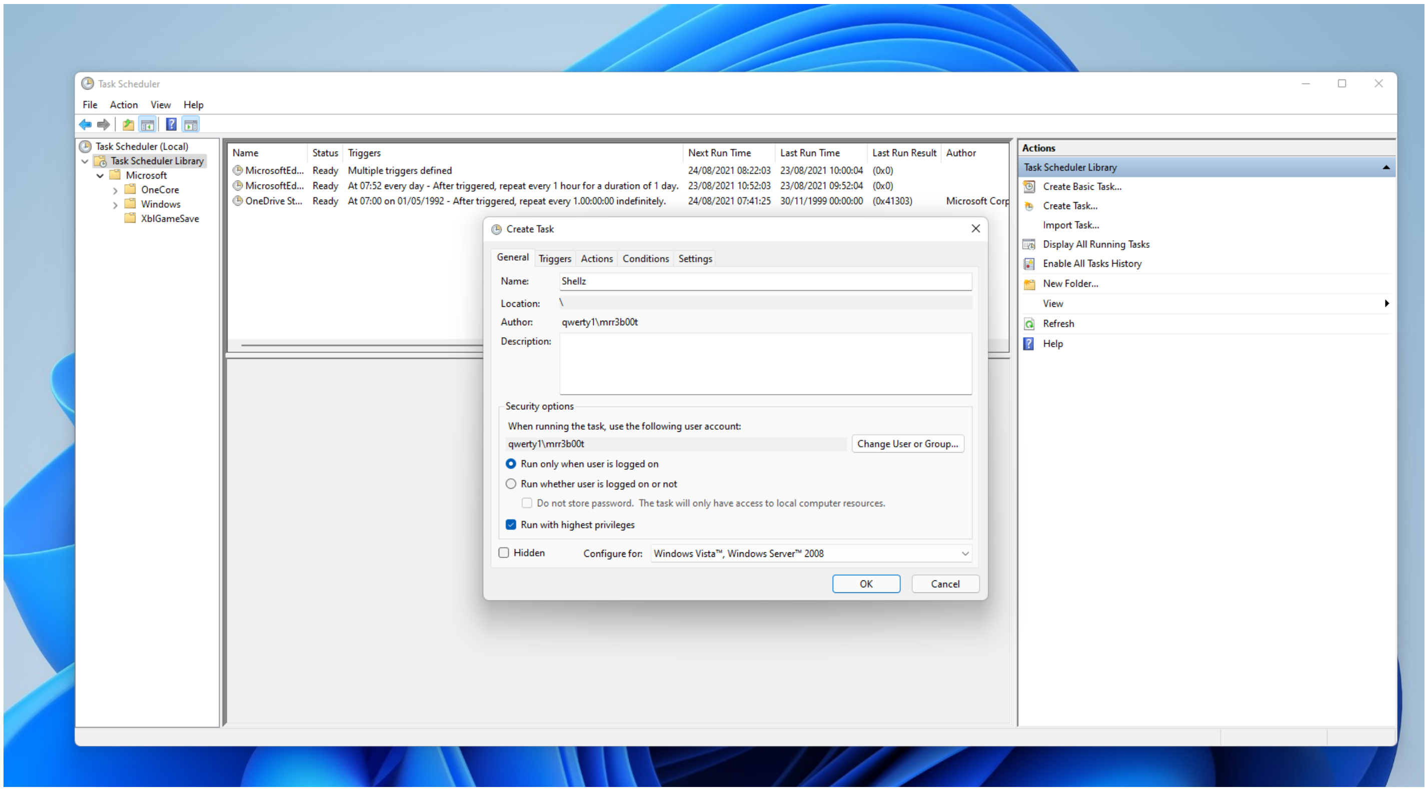
○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local resources

☑ Run with highest privileges

□ Hidden Configure for: Windows Vista™, Windows Server™ 2008



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author
MicrosoftEd...	Ready	Multiple triggers defined	24/08/2021 08:22:03	23/08/2021 10:00:04	(0x0)	
MicrosoftEd...	Ready	At 07:52 every day - After triggered, repeat every 1 hour for a duration of 1 day.	23/08/2021 10:52:03	23/08/2021 09:52:04	(0x0)	
OneDrive St...	Ready	At 07:00 on 01/05/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	24/08/2021 07:41:25	30/11/1999 00:00:00	(0x41303)	Microsoft Corp

Create Task

General Triggers Actions Conditions Settings

Name: Shellz

Location: \

Author: qwerty1\mrr3b00t

Description:

Security options

When running the task, use the following user account:

qwerty1\mrr3b00t Change User or Group...

● Run only when user is logged on

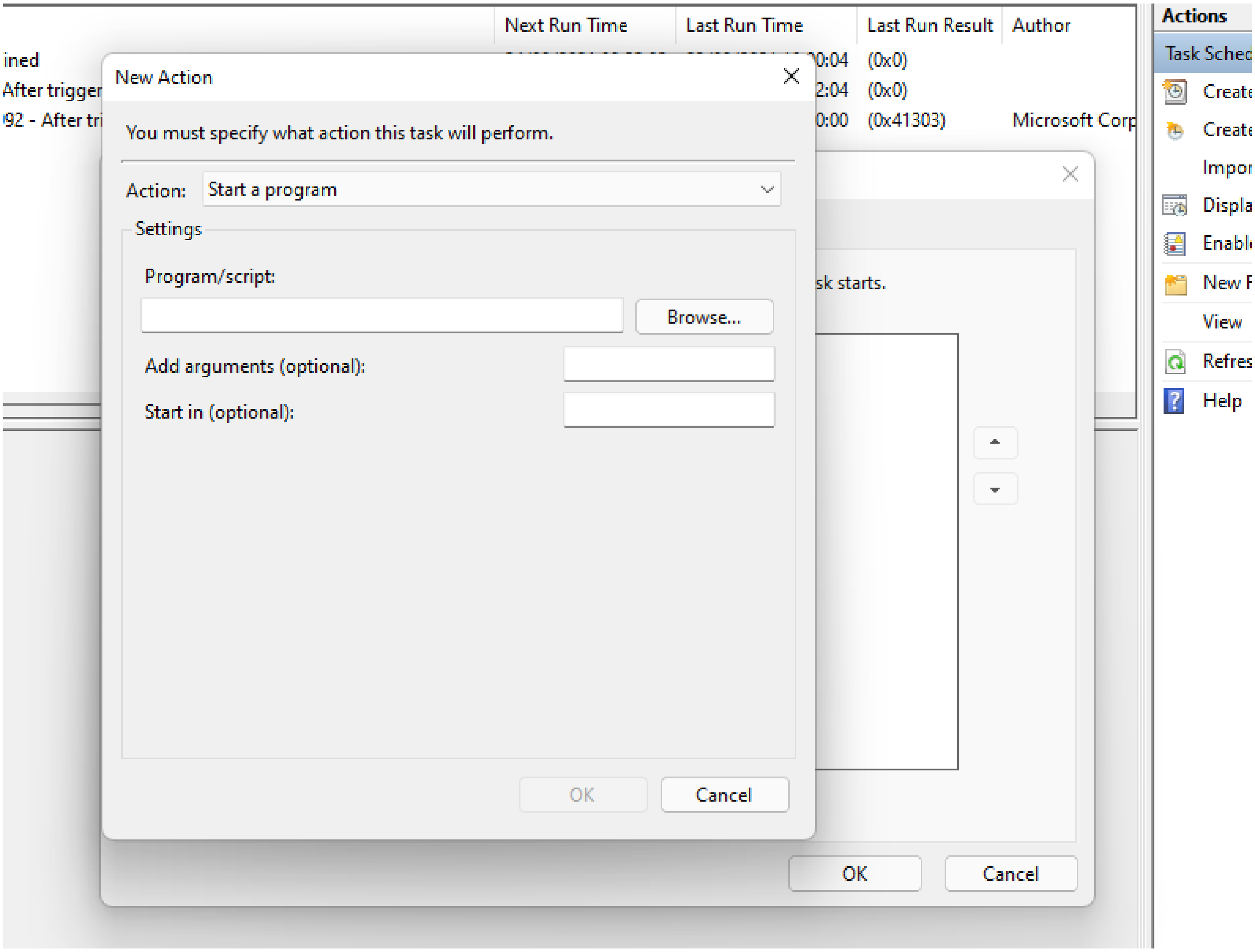
○ Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

□ Hidden Configure for: Windows Vista™, Windows Server™ 2008

OK Cancel



New Action

You must specify what action this task will perform.

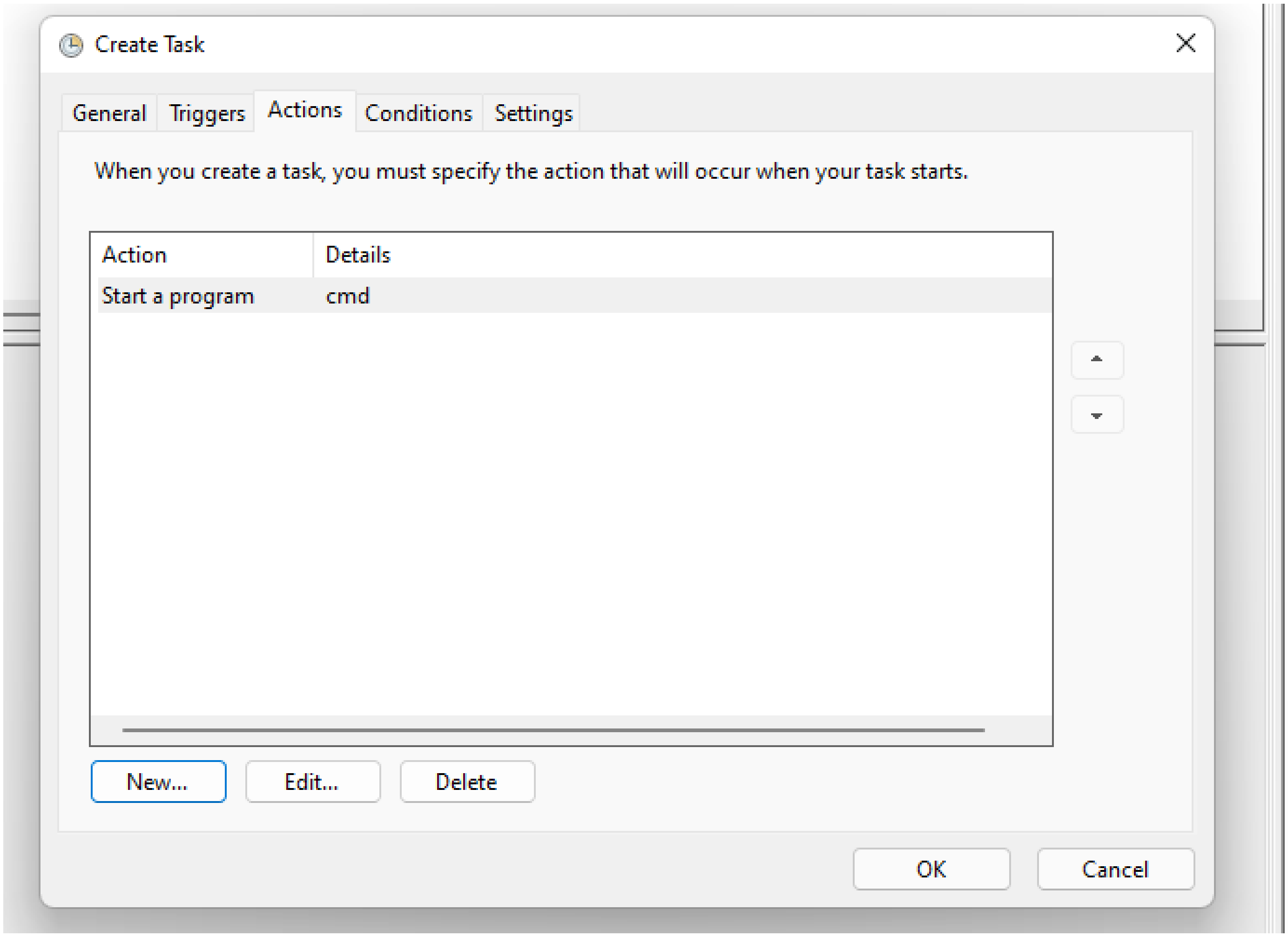
Action: Start a program

Settings

Program/script:

Add arguments (optional):

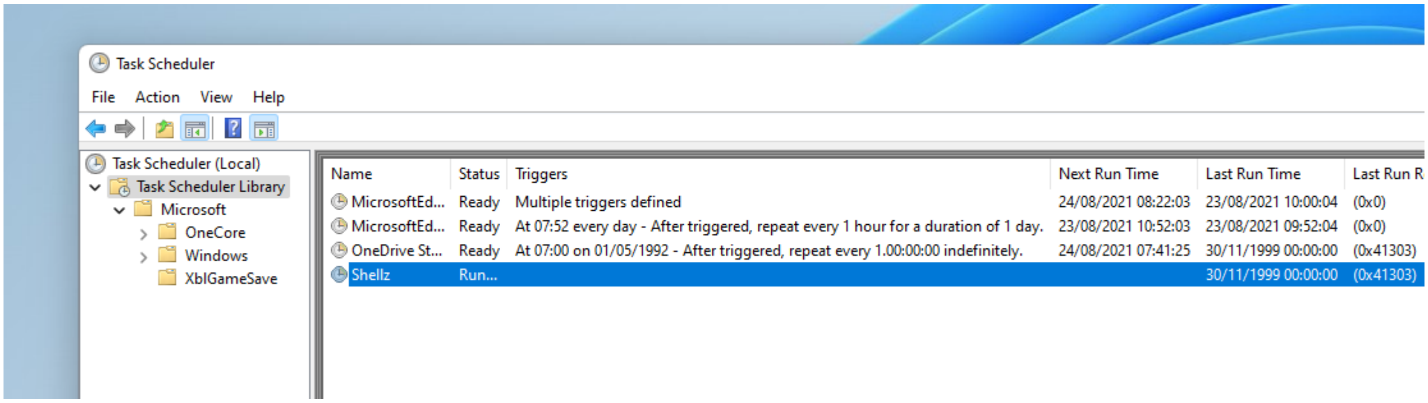
Start in (optional):



When you create a task, you must specify the action that will occur when your task starts.

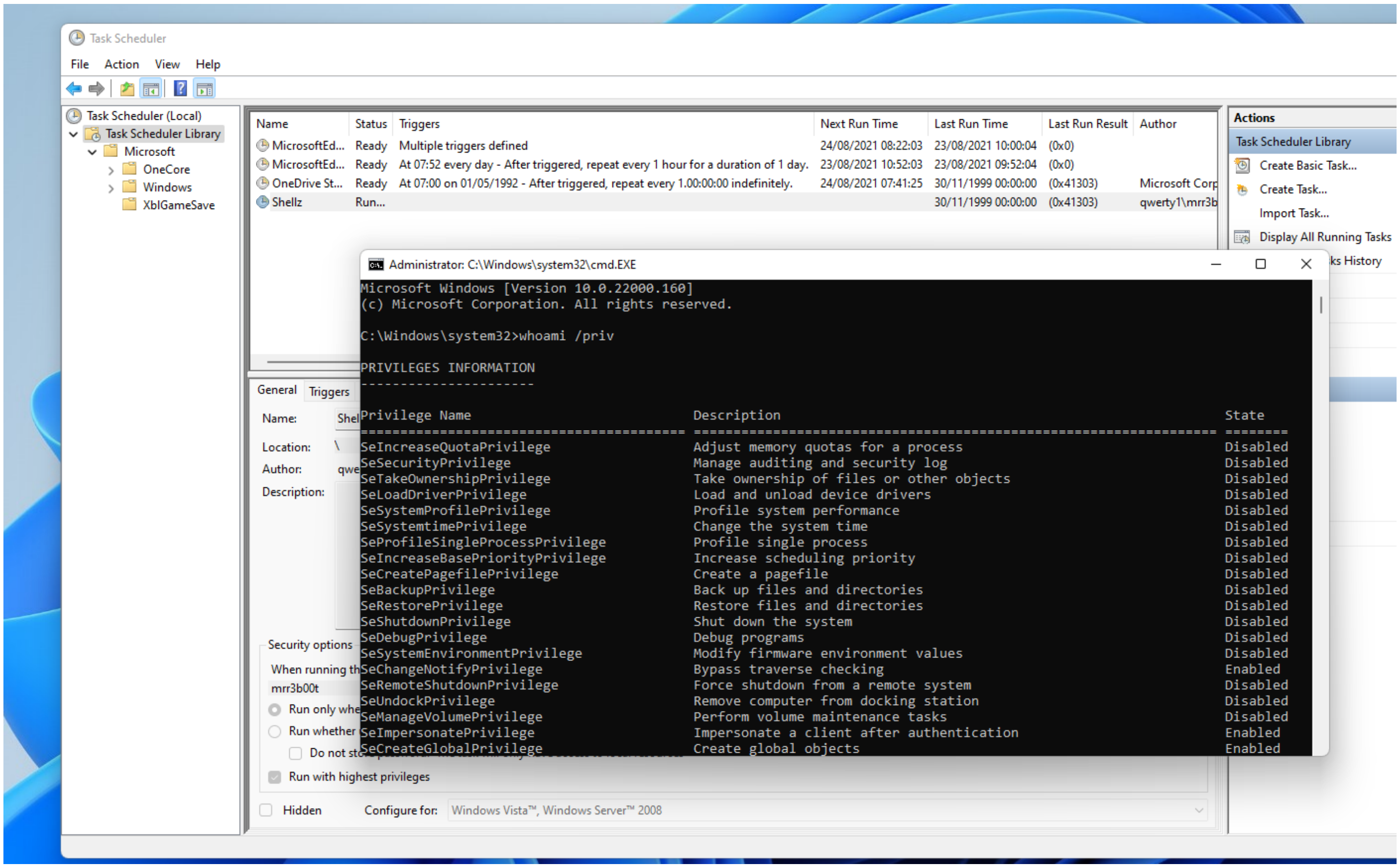
Action	Details
Start a program	cmd

Click OK



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run R
MicrosoftEd...	Ready	Multiple triggers defined	24/08/2021 08:22:03	23/08/2021 10:00:04	(0x0)
MicrosoftEd...	Ready	At 07:52 every day - After triggered, repeat every 1 hour for a duration of 1 day.	23/08/2021 10:52:03	23/08/2021 09:52:04	(0x0)
OneDrive St...	Ready	At 07:00 on 01/05/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	24/08/2021 07:41:25	30/11/1999 00:00:00	(0x41303)
Shellz	Run...			30/11/1999 00:00:00	(0x41303)

Right click and run the task



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author
MicrosoftEd...	Ready	Multiple triggers defined	24/08/2021 08:22:03	23/08/2021 10:00:04	(0x0)	
MicrosoftEd...	Ready	At 07:52 every day - After triggered, repeat every 1 hour for a duration of 1 day.	23/08/2021 10:52:03	23/08/2021 09:52:04	(0x0)	
OneDrive St...	Ready	At 07:00 on 01/05/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	24/08/2021 07:41:25	30/11/1999 00:00:00	(0x41303)	Microsoft Corp
Shellz	Run...			30/11/1999 00:00:00	(0x41303)	qwerty1\mrr3b

Name: Shel
Location: \
Author: qwe
Description:

mrr3b00t

☑ Run with highest privileges

□ Hidden Configure for: Windows Vista™, Windows Server™ 2008

Administrator: C:\Windows\system32\cmd.EXE

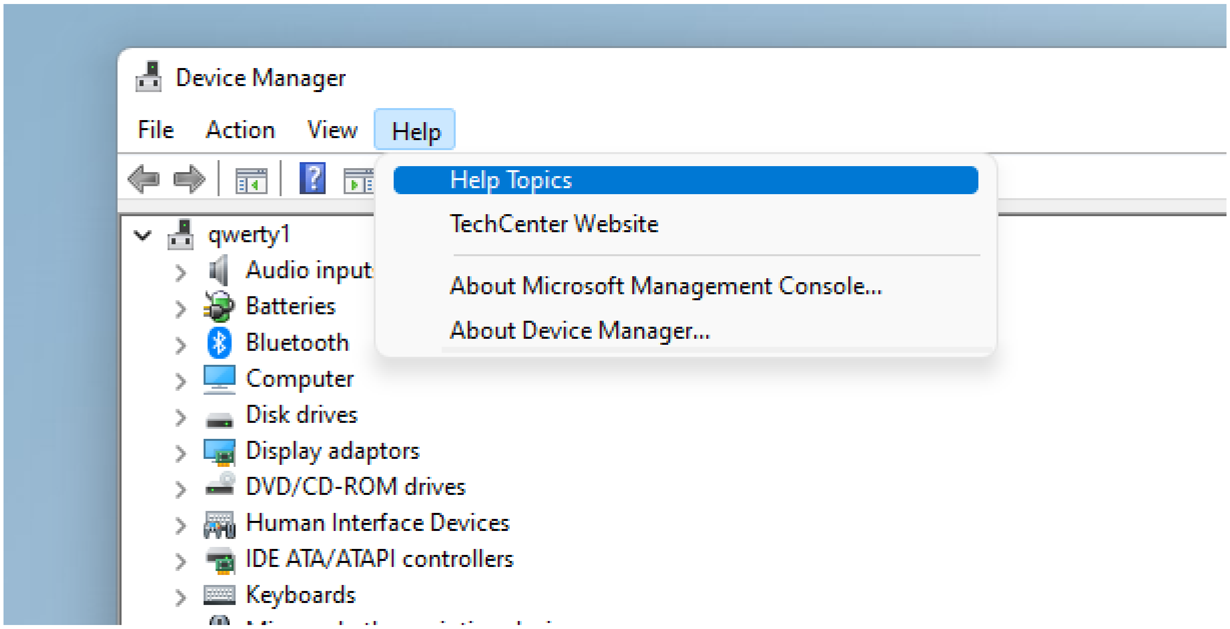
```
Microsoft Windows [Version 10.0.22000.160]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Disabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
```

MMC/Device Manager/Group Policy Editor etc.

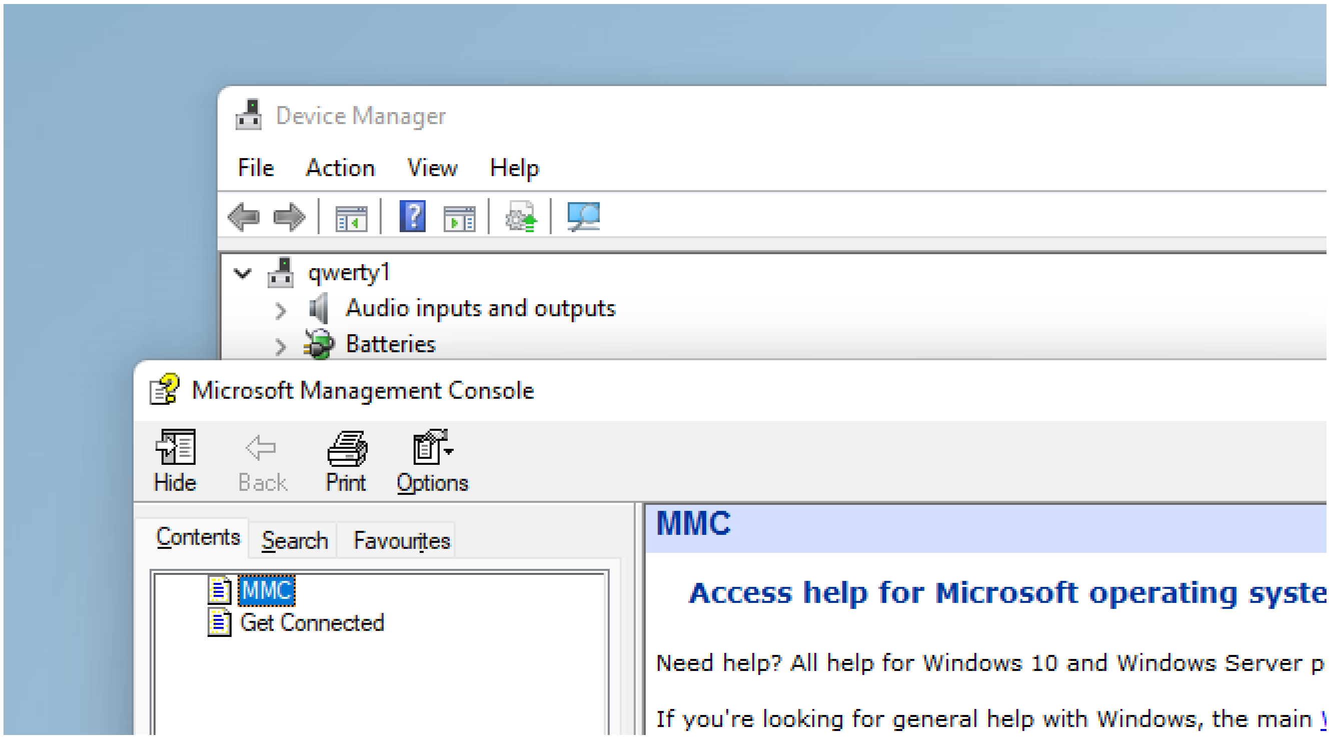
Run

mmc devmgmt.msc

Click Help



Help Topics



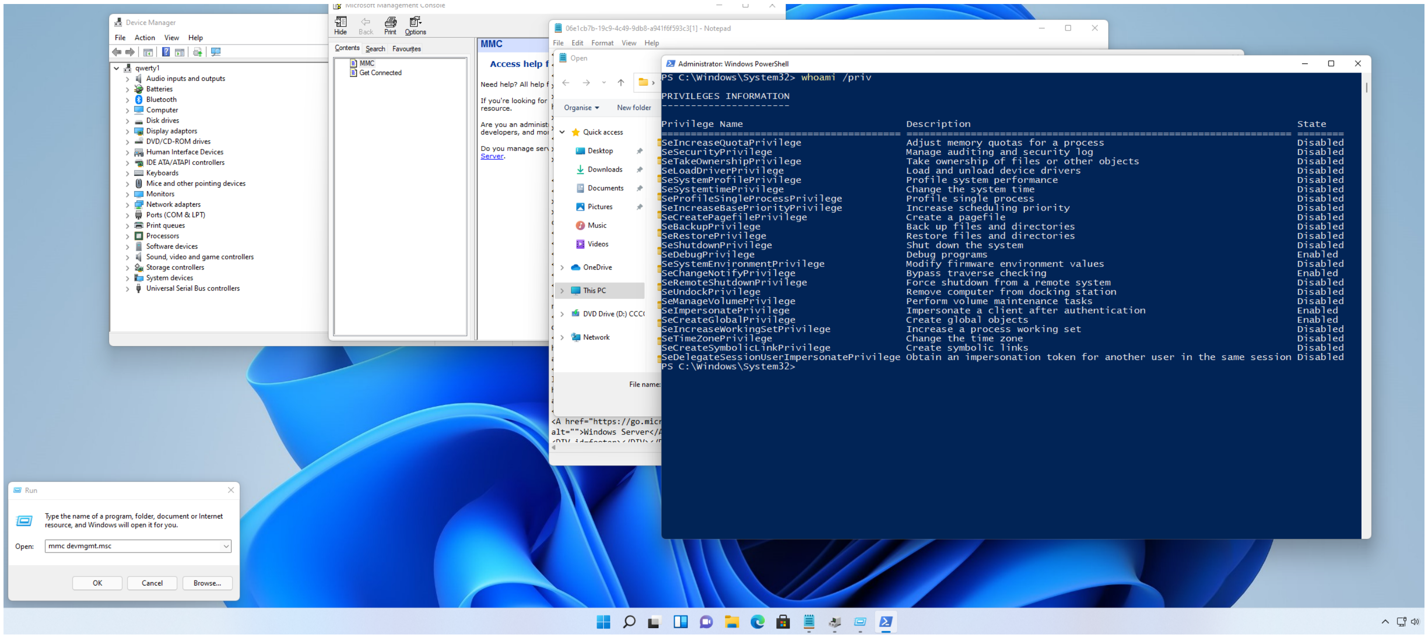
Access help for Microsoft operating syste

Need help? All help for Windows 10 and Windows Server p

If you're looking for general help with Windows, the main

Rick click and view source

Use the file open and then RIGHT CLICK + SHIFT to launch a shell

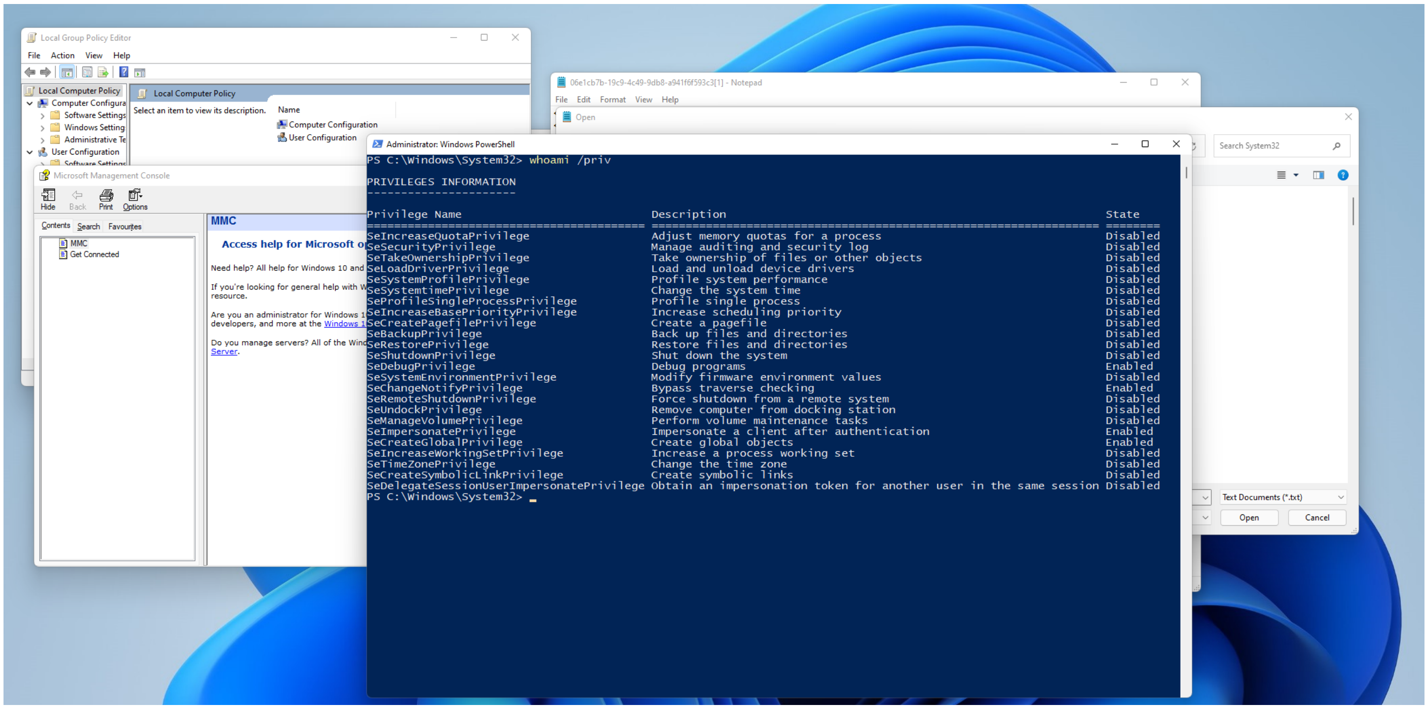

Device Manager
Microsoft Management Console
06e1cb7b-19c9-4c49-9db8-a941f6f593c3[1] - Notepad
Open
Administrator: Windows PowerShell
Run

Type the name of a program, folder, document or Internet resource, and Windows will open it for you.

Open: mmc devmgmt.msc

```
PS C:\Windows\System32> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled
PS C:\Windows\System32>
```

Shockingly you can run these with all kinds of the .msc consoles:


Local Group Policy Editor
Microsoft Management Console
06e1cb7b-19c9-4c49-9db8-a941f6f593c3[1] - Notepad
Open
Administrator: Windows PowerShell

```
PS C:\Windows\System32> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled
PS C:\Windows\System32> _
```

Here's using Group Policy Editor.

MORE

Ok so we get the gist of how to exploit this manually so what we need is a list of more binaries we can use:

- netplwiz.exe
- dcomcnfg.exe

- perfmon.exe
- compMgmtLauncher.exe
- eventvwr.exe

So there's lots of ways of doing this via binaries.

Summary

These might seem like they are not useful, but you can find position where these can be exploited. It's often the small things that make a difference, I've certainly been in positions where they techniques have helped before.

I recommend that people increase their UAC levels (do bear in the mind the user experience change though).

‹ Cyber Strategy Magic (https://www.pwndefend.com/2021/08/22/2036/)

Infection Monkey Overview (https://www.pwndefend.com/2021/08/26/infection-monkey-overview/) ›

blue team (https://www.pwndefend.com/tag/blue-team/) cybercrime (https://www.pwndefend.com/tag/cybercrime/) CyberSecurity (https://www.pwndefend.com/tag/cybersecurity/) education (https://www.pwndefend.com/tag/education/) guides (https://www.pwndefend.com/tag/guides/) Hacking (https://www.pwndefend.com/tag/hacking/) management (https://www.pwndefend.com/tag/management/) Risk (https://www.pwndefend.com/tag/risk/) Security (https://www.pwndefend.com/tag/security/)

Related articles

(https://www.pwndefend.com/2023/01/20/crackmapexec-mega-mega-cyber-pain/)

(https://www.pwndefend.com/2023/01/19/ransomware-shadow-copy/)

(https://www.pwndefend.com/2023/01/16/volume-spraying-office-365/)

Ransomware + Mega = Mega… (https://www.pwndefend.com/2023/01/20/ransomware-mega-mega-cyber-pain/)

Volume Shadow Copy (https://www.pwndefend.com/2023/01/19/volume-shadow-copy/)

Password Spraying Offic (https://www.pwndefend.com/2023/01/16/password-spraying-office-365/)

Leave a Reply

You must be **logged in (https://www.pwndefend.com/wp-login.php?redirect_to=https%3A%2F%2Fwww.pwndefend.com%2F2021%2F08%2F23%2Fwindows-11-privilege-escalation-via-uac-bypass-gui-based%2F)** to post a comment.