👨‍🎓 **Student name:** TEJEDA David, PEUGNET Thomas

🏛️ **Student class:** EFREI RS3 2025

📅 **Date:** 25/01/2024

Threats targeting the hybrid & cloud identity platform

Reconnaissance

All exercises and tasks must be done in the defined order. They build on each other, if you skip a step, you will no longer be able to continue.

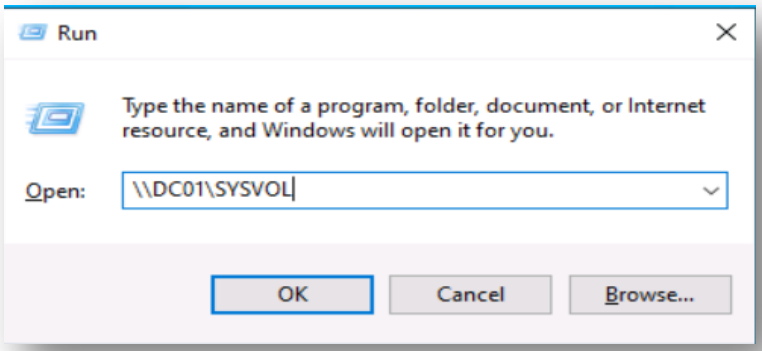
You mainly use two accounts:

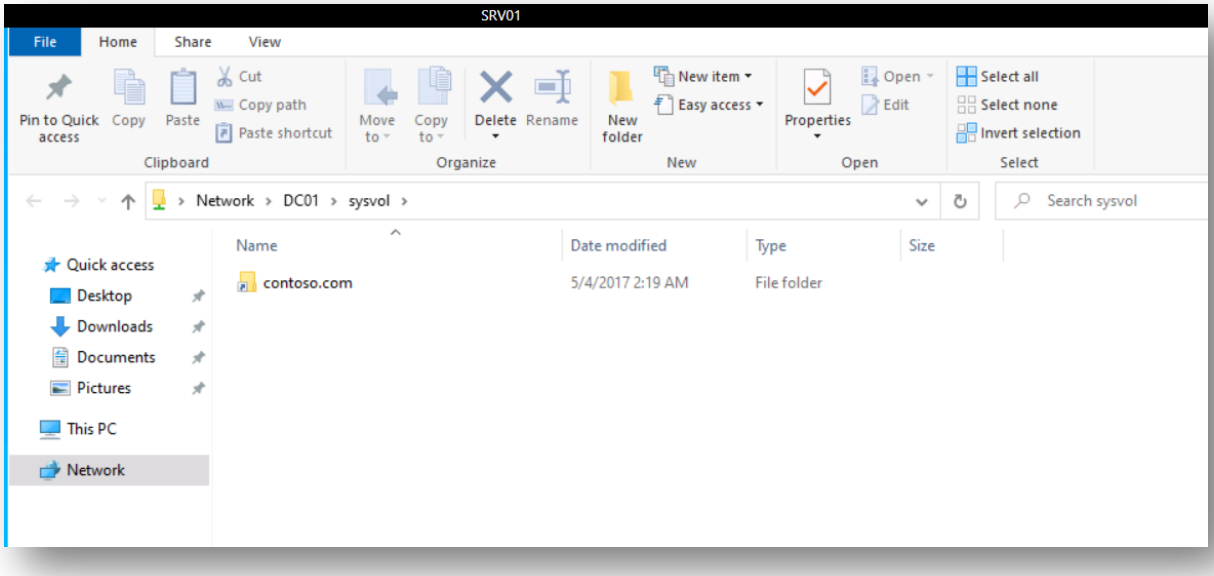
Red Team	Blue Team
Miss Red	Mister Blue
CONTOSO\red	CONTOSO\blue

CONTOSO\red is only a user of **CONTOSO\Domain Users** and does not have any privilege on the domain. However, she is a member of the local **Administrators** group on **CLI01**.

CONTOSO\blue is a domain privileged account member of the **Domain Admins** group.

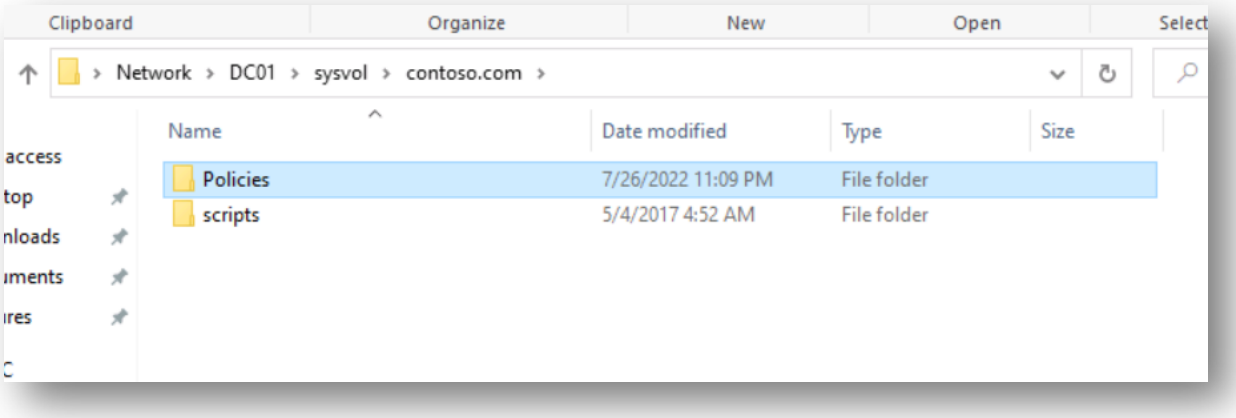
Module 2 – Lab 2 – Reconnaissance



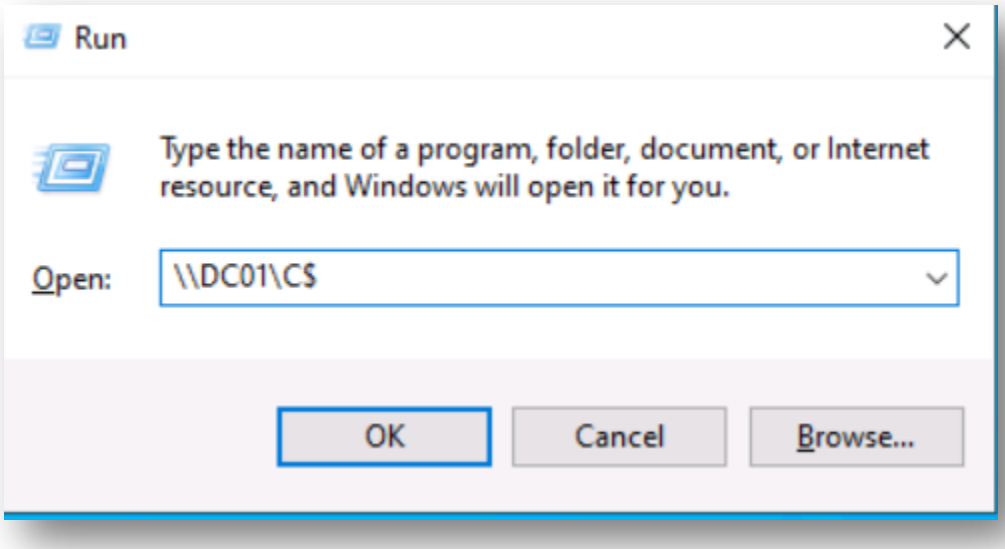


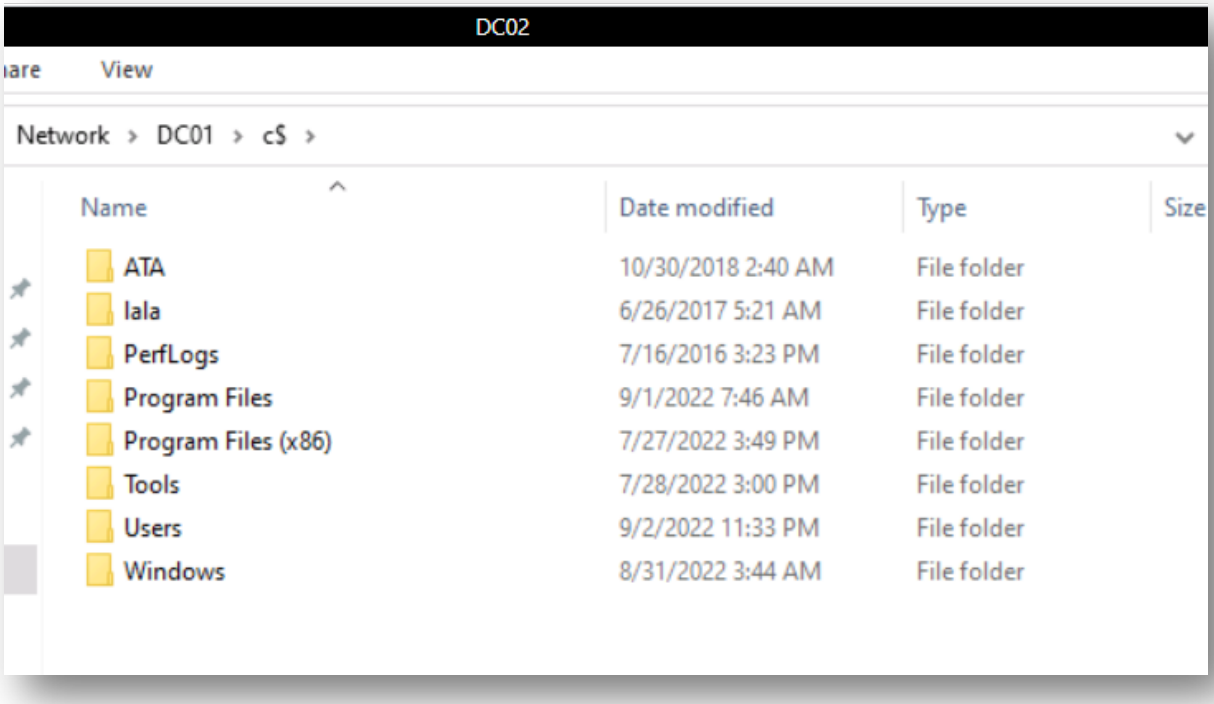
Exercise 1 - Prepare the environment

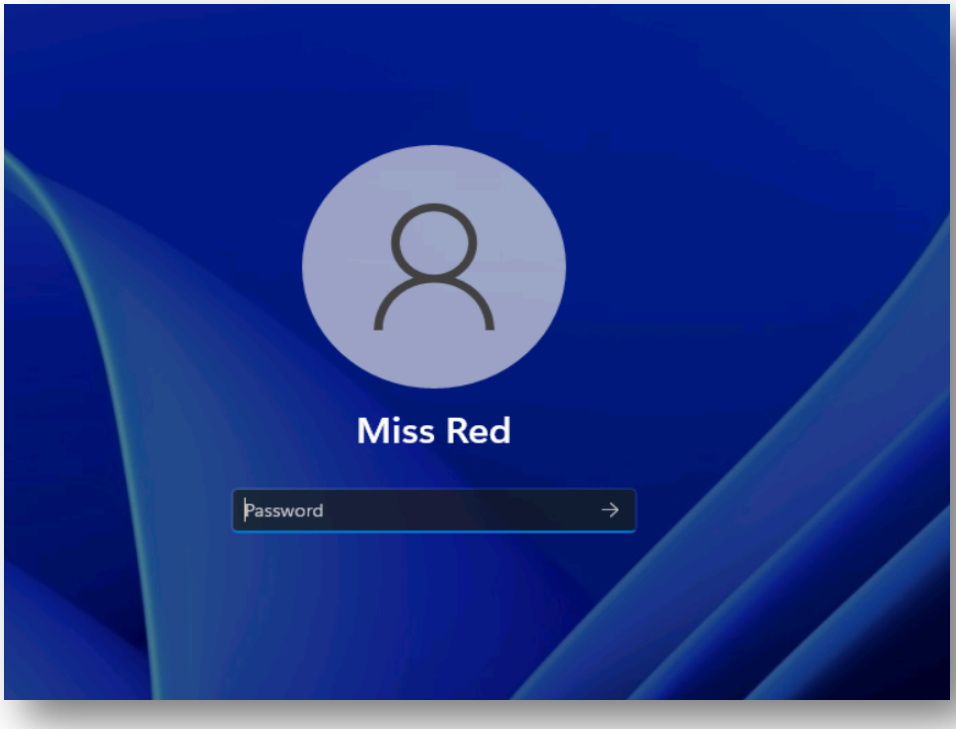
📝 What types of files can we find in this folder?

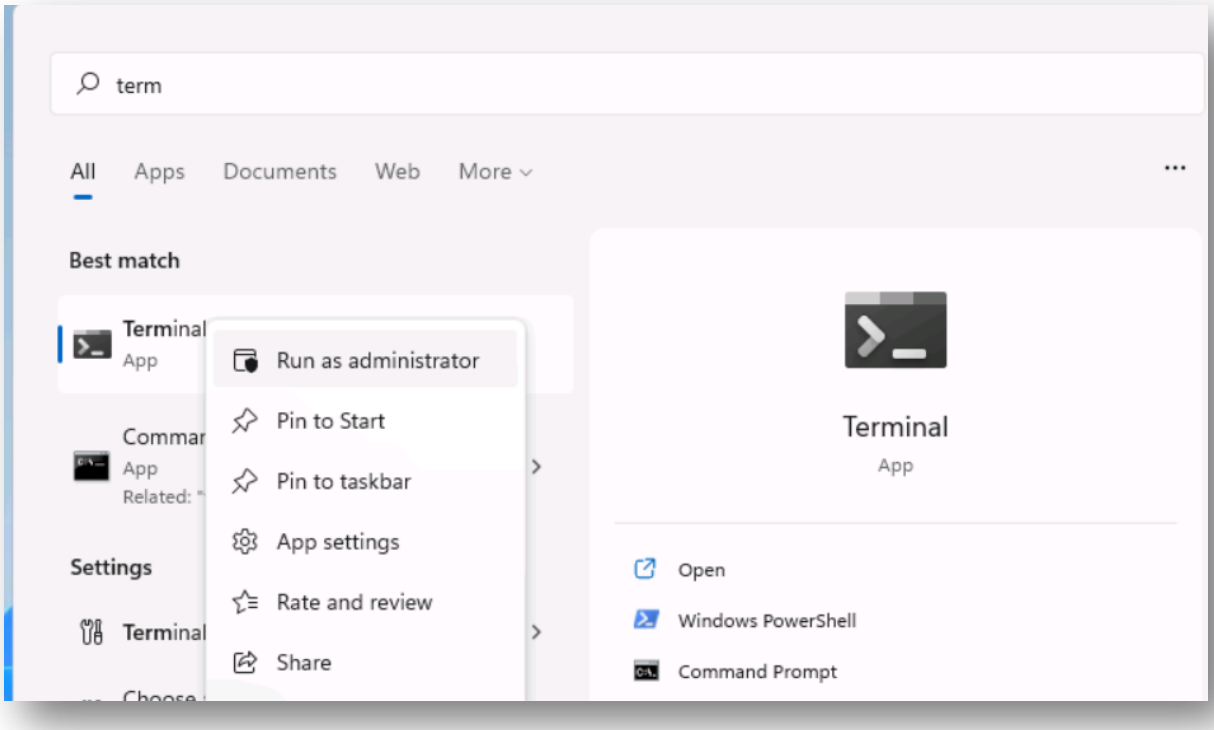


SYSVOL et Politiques de Groupe: Le dossier SYSVOL sur un contrôleur de domaine Windows inclut des fichiers de politique de groupe (GPO), qui sont utilisés pour centraliser la gestion des paramètres de configuration des ordinateurs et utilisateurs du domaine. Ces fichiers comprennent des modèles administratifs, des paramètres de sécurité, des scripts, et des fichiers de préférences. En plus, SYSVOL contient des scripts de connexion et de déconnexion qui sont exécutés lorsque les utilisateurs se connectent ou se déconnectent d'un ordinateur du domaine.




DC02
are
View
Network › DC01 › cS ›
Name
Date modified
Type
Size
ATA
10/30/2018 2:40 AM
File folder
lala
6/26/2017 5:21 AM
File folder
PerfLogs
7/16/2016 3:23 PM
File folder
Program Files
9/1/2022 7:46 AM
File folder
Program Files (x86)
7/27/2022 3:49 PM
File folder
Tools
7/28/2022 3:00 PM
File folder
Users
9/2/2022 11:33 PM
File folder
Windows
8/31/2022 3:44 AM
File folder

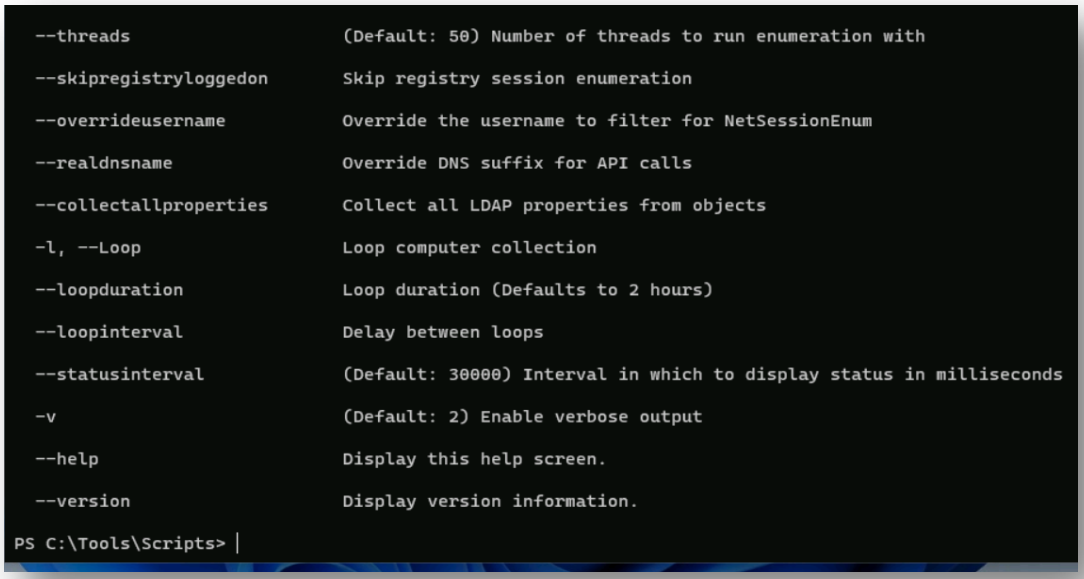

Miss Red
Password

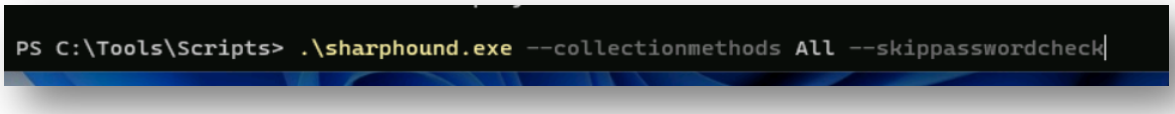

term
All
Apps
Documents
Web
More
Best match
Terminal
App
Run as administrator
Pin to Start
Pin to taskbar
App settings
Rate and review
Share
Settings
Terminal
Terminal
App
Open
Windows PowerShell
Command Prompt

Exercise 2 - Use BloodHound for recon

📝 Is is an alias for what PowerShell command?

- C’est un alias pour la commande dir.





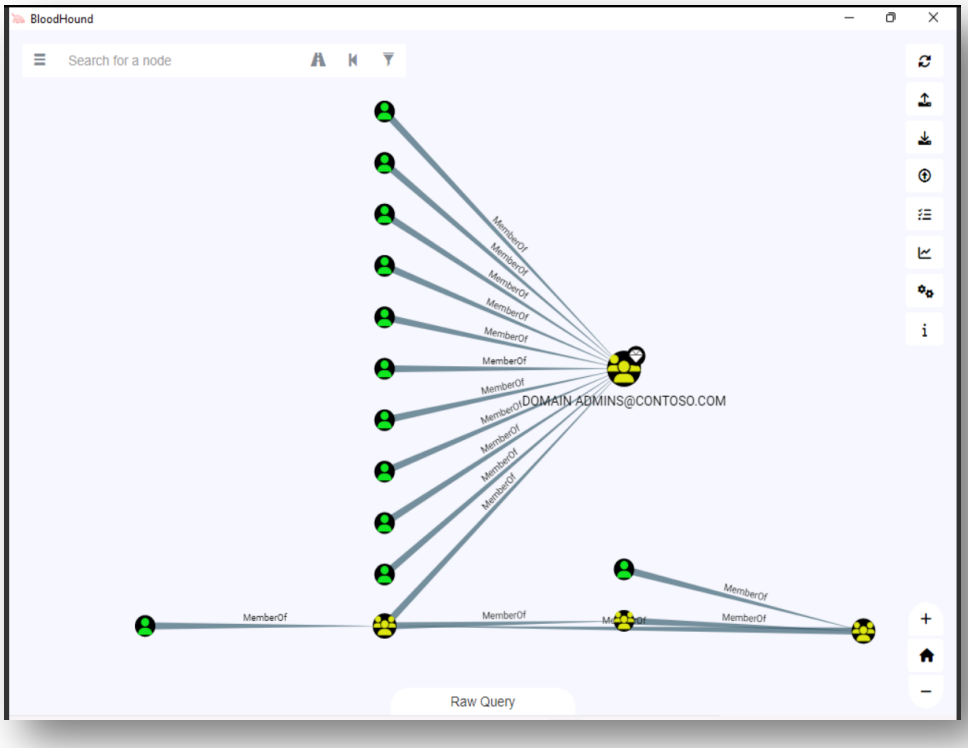
```
PS C:\Tools\Scripts> .\sharphound.exe --collectionmethods All --skippasswordcheck
2024-01-25T05:00:56.2505735-08:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of
 BloodHound
2024-01-25T05:00:56.4849494-08:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, S
ession, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-01-25T05:00:56.6099571-08:00|INFORMATION|Initializing SharpHound at 5:00 AM on 1/25/2024
2024-01-25T05:00:56.9849596-08:00|INFORMATION|Loaded cache with stats: 210 ID to type mappings.
 217 name to SID mappings.
 2 machine sid mappings.
 4 sid to domain mappings.
 0 global catalog mappings.
2024-01-25T05:00:57.0161970-08:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trus
ts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-01-25T05:00:57.7818219-08:00|INFORMATION|Beginning LDAP search for contoso.com
2024-01-25T05:00:58.0786950-08:00|INFORMATION|Producer has finished, closing LDAP channel
2024-01-25T05:00:58.0786950-08:00|INFORMATION|LDAP channel closed, waiting for consumers
2024-01-25T05:01:28.1575569-08:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 46 MB RAM
2024-01-25T05:01:42.7678660-08:00|INFORMATION|Consumers finished, closing output channel
Closing writers
2024-01-25T05:01:42.8303697-08:00|INFORMATION|Output channel closed, waiting for output task to complete
2024-01-25T05:01:42.8928671-08:00|INFORMATION|Status: 250 objects finished (+250 5.555555)/s -- Using 51 MB RA
M
2024-01-25T05:01:42.8928671-08:00|INFORMATION|Enumeration finished in 00:00:45.1164258
2024-01-25T05:01:43.0647430-08:00|INFORMATION|Saving cache with stats: 210 ID to type mappings.
 217 name to SID mappings.
 2 machine sid mappings.
 4 sid to domain mappings.
 0 global catalog mappings.
2024-01-25T05:01:43.0647430-08:00|INFORMATION|SharpHound Enumeration Completed at 5:01 AM on 1/25/2024! Happy
Graphing!
PS C:\Tools\Scripts>
```

```
PS C:\Tools\Scripts> Write-Output
                   > Write-Output "SRV01.contoso.com" | Out-File computers.lst
```

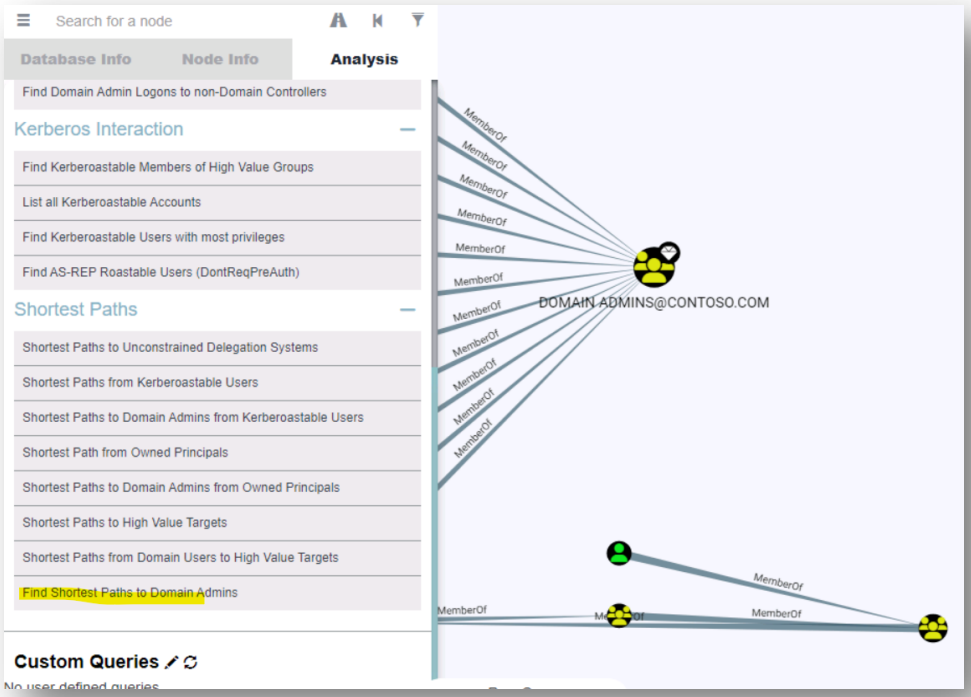
```
PS C:\Tools\Scripts> .\sharphound.exe --collectionmethods All --computerfile computers.lst --skippasswordcheck
2024-01-25T05:05:30.3251001-08:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of
 BloodHound
2024-01-25T05:05:30.4344838-08:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, S
ession, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-01-25T05:05:30.4657212-08:00|INFORMATION|Initializing SharpHound at 5:05 AM on 1/25/2024
2024-01-25T05:05:30.9032218-08:00|INFORMATION|Loaded cache with stats: 210 ID to type mappings.
 217 name to SID mappings.
 2 machine sid mappings.
 4 sid to domain mappings.
 0 global catalog mappings.
2024-01-25T05:05:30.9188489-08:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trus
ts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-01-25T05:05:31.1376022-08:00|INFORMATION|Producer has finished, closing LDAP channel
2024-01-25T05:05:31.1376022-08:00|INFORMATION|LDAP channel closed, waiting for consumers
2024-01-25T05:05:31.2625994-08:00|INFORMATION|Consumers finished, closing output channel
2024-01-25T05:05:31.2938473-08:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2024-01-25T05:05:31.3876507-08:00|INFORMATION|Status: 2 objects finished (+2 Infinity)/s -- Using 40 MB RAM
2024-01-25T05:05:31.3876507-08:00|INFORMATION|Enumeration finished in 00:00:00.2879884
2024-01-25T05:05:31.4500960-08:00|INFORMATION|Saving cache with stats: 210 ID to type mappings.
 217 name to SID mappings.
 2 machine sid mappings.
 4 sid to domain mappings.
 0 global catalog mappings.
2024-01-25T05:05:31.4500960-08:00|INFORMATION|SharpHound Enumeration Completed at 5:05 AM on 1/25/2024! Happy
Graphing!
```

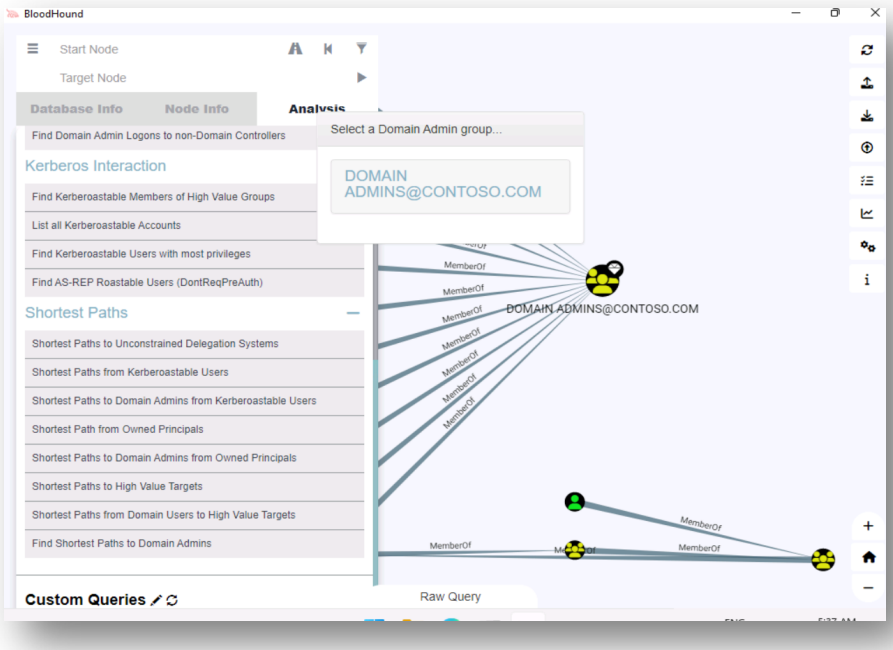
📝 How many zip files do you see?

```
PS C:\Tools\Scripts> dir *.zip


    Directory: C:\Tools\Scripts


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/25/2024   5:01 AM          27703 20240125050133_BloodHound.zip
-a----         1/25/2024   5:05 AM           1265 20240125050531_BloodHound.zip
```

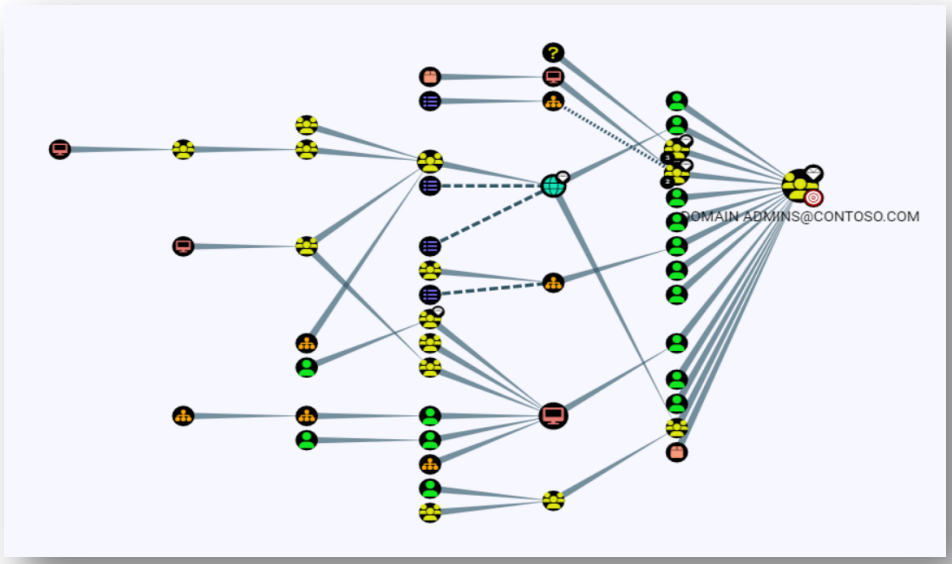


Module 2 – Lab 2 – Reconnaissance

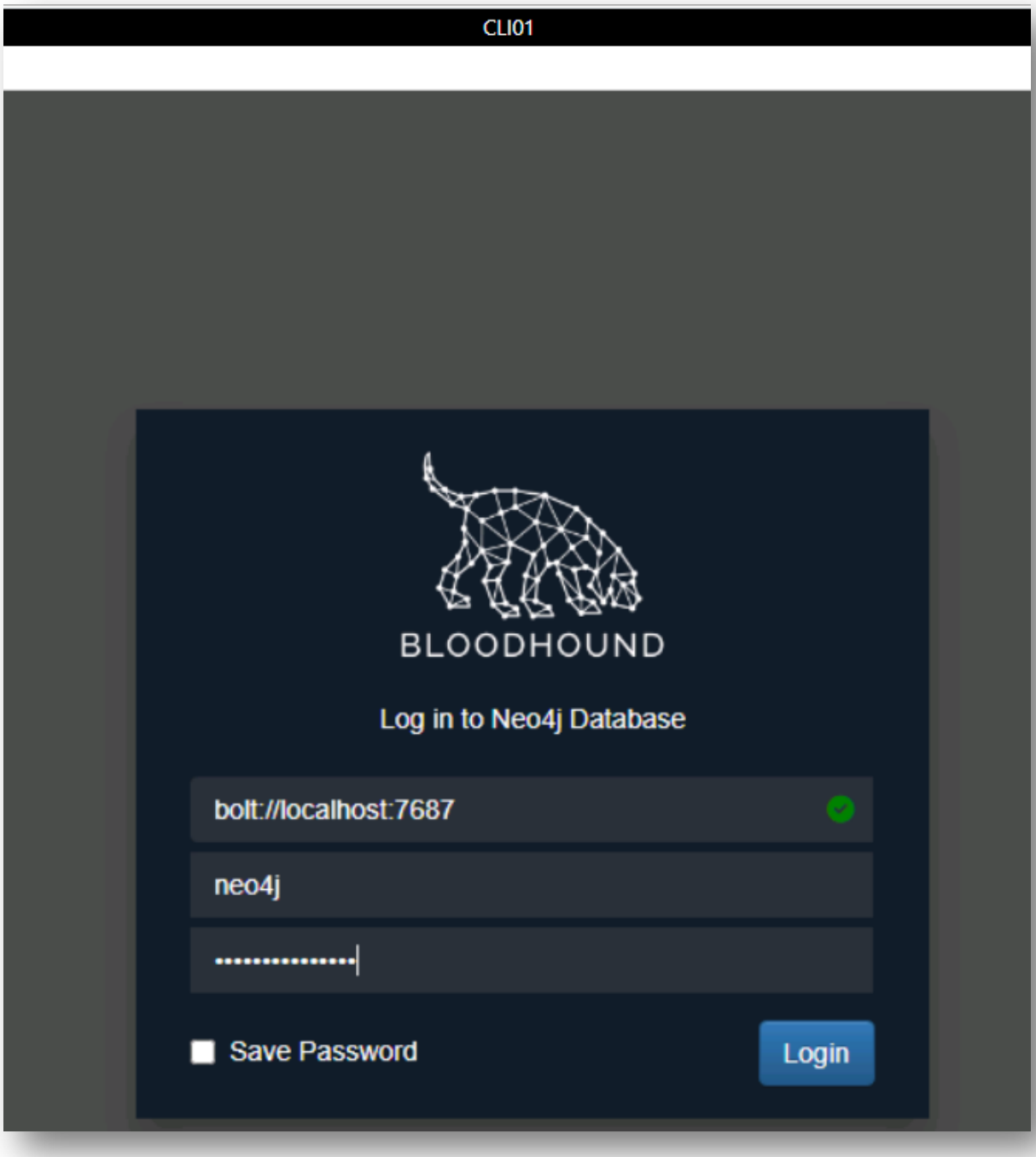




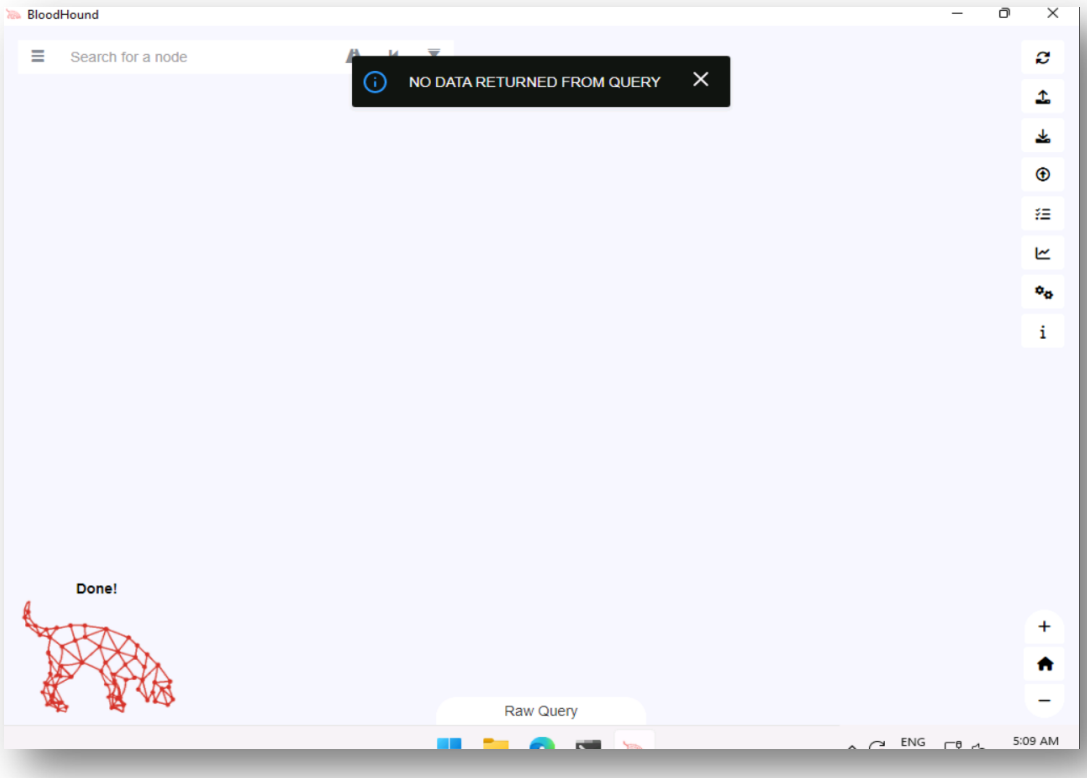
Module 2 – Lab 2 – Reconnaissance

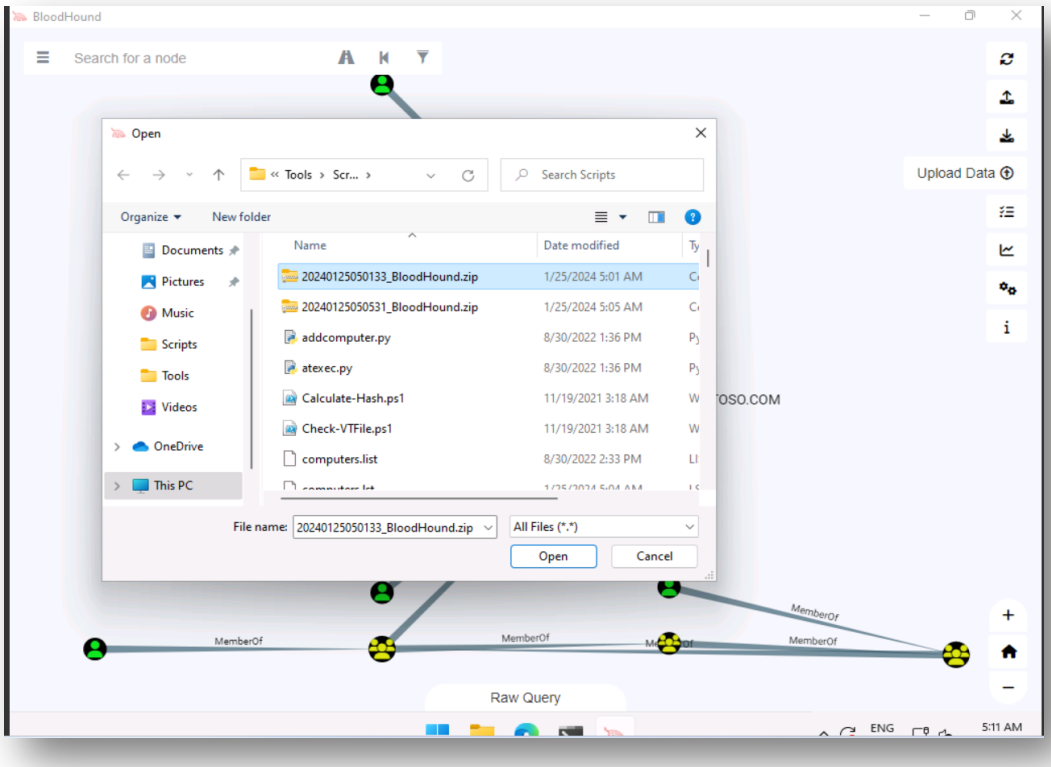


📝 Can you see who has a session and from where?

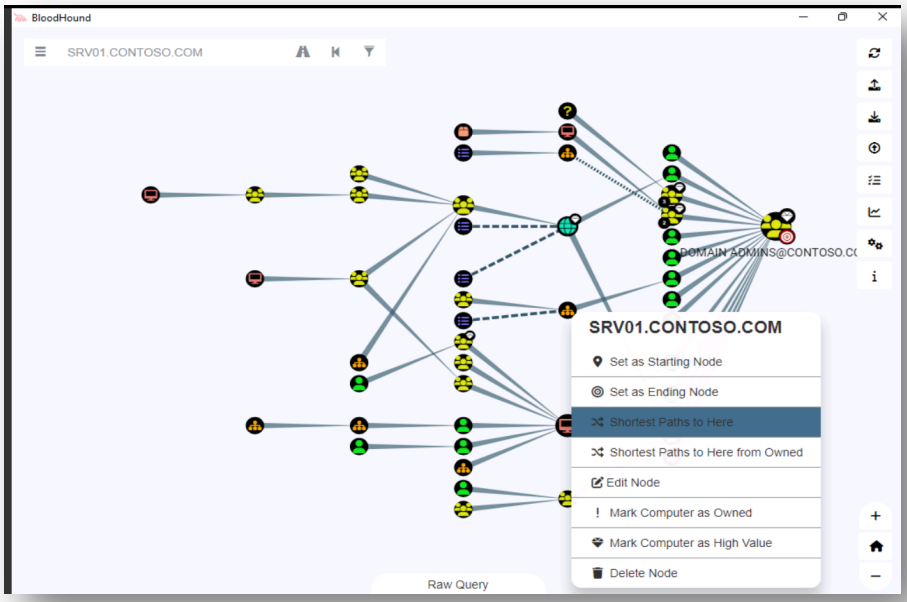


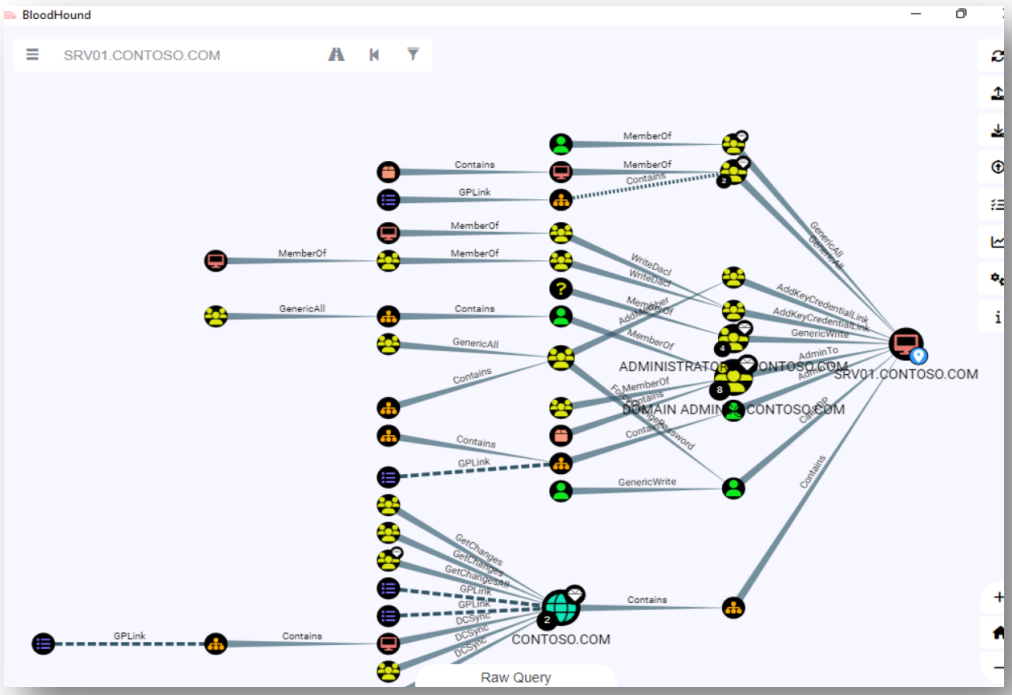
Module 2 – Lab 2 – Reconnaissance





Module 2 – Lab 2 – Reconnaissance

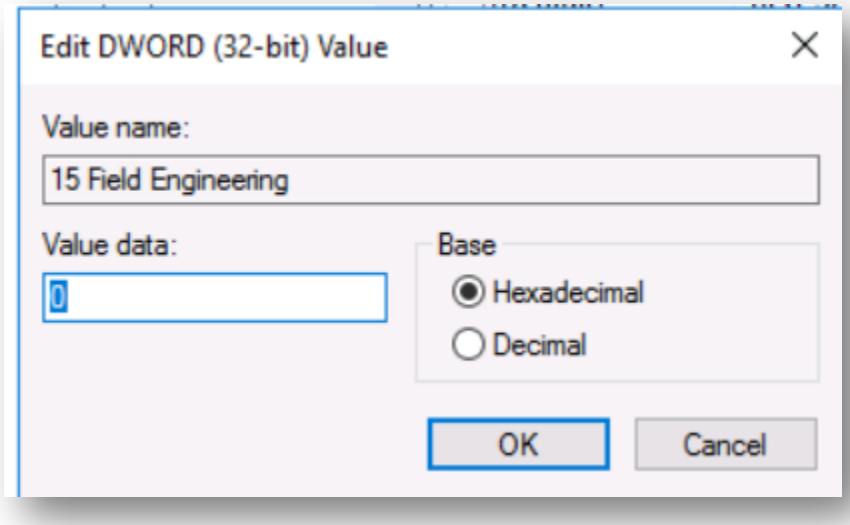


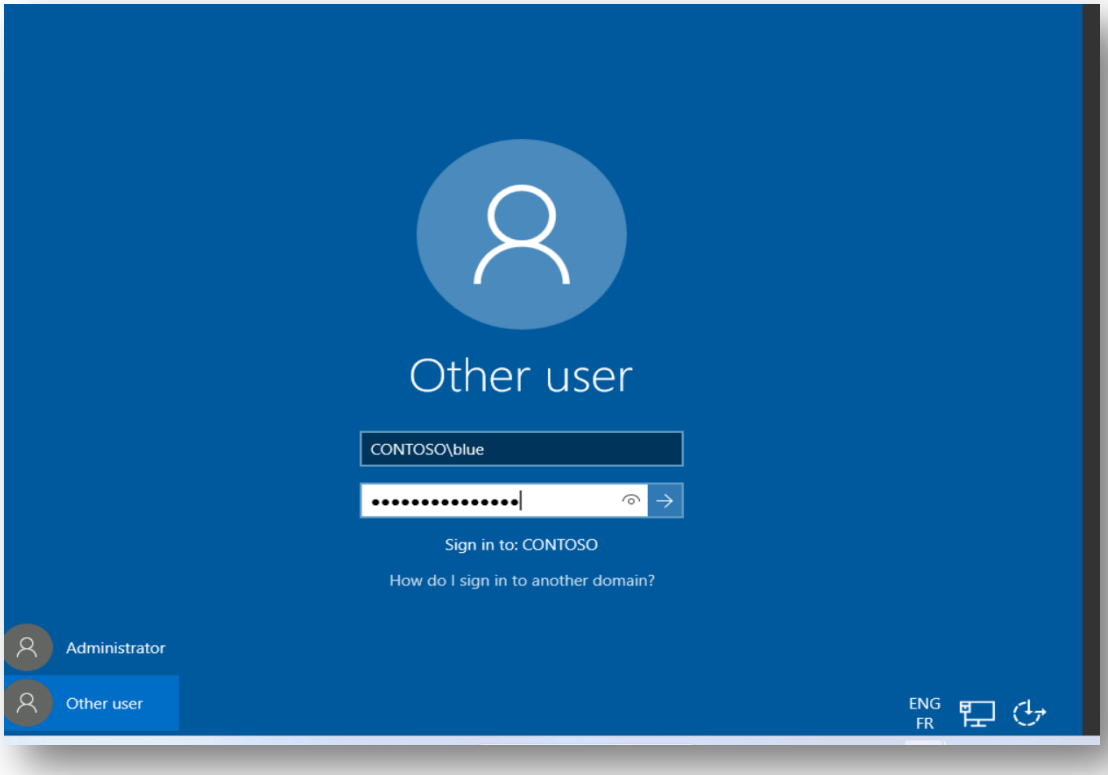


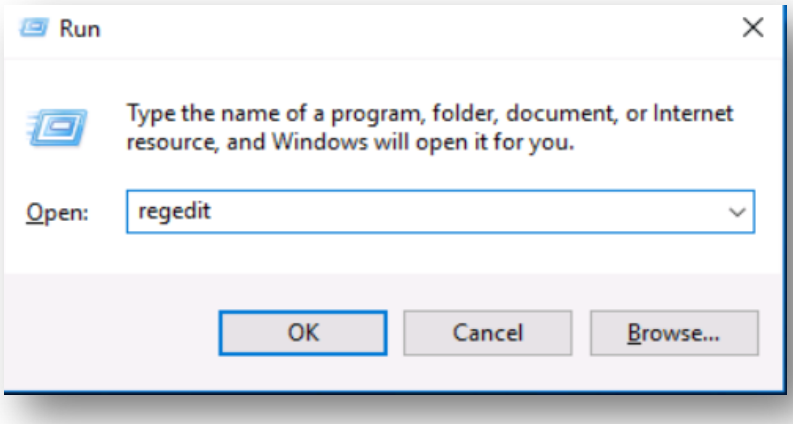
Exercise 3 - Enable LDAP logging

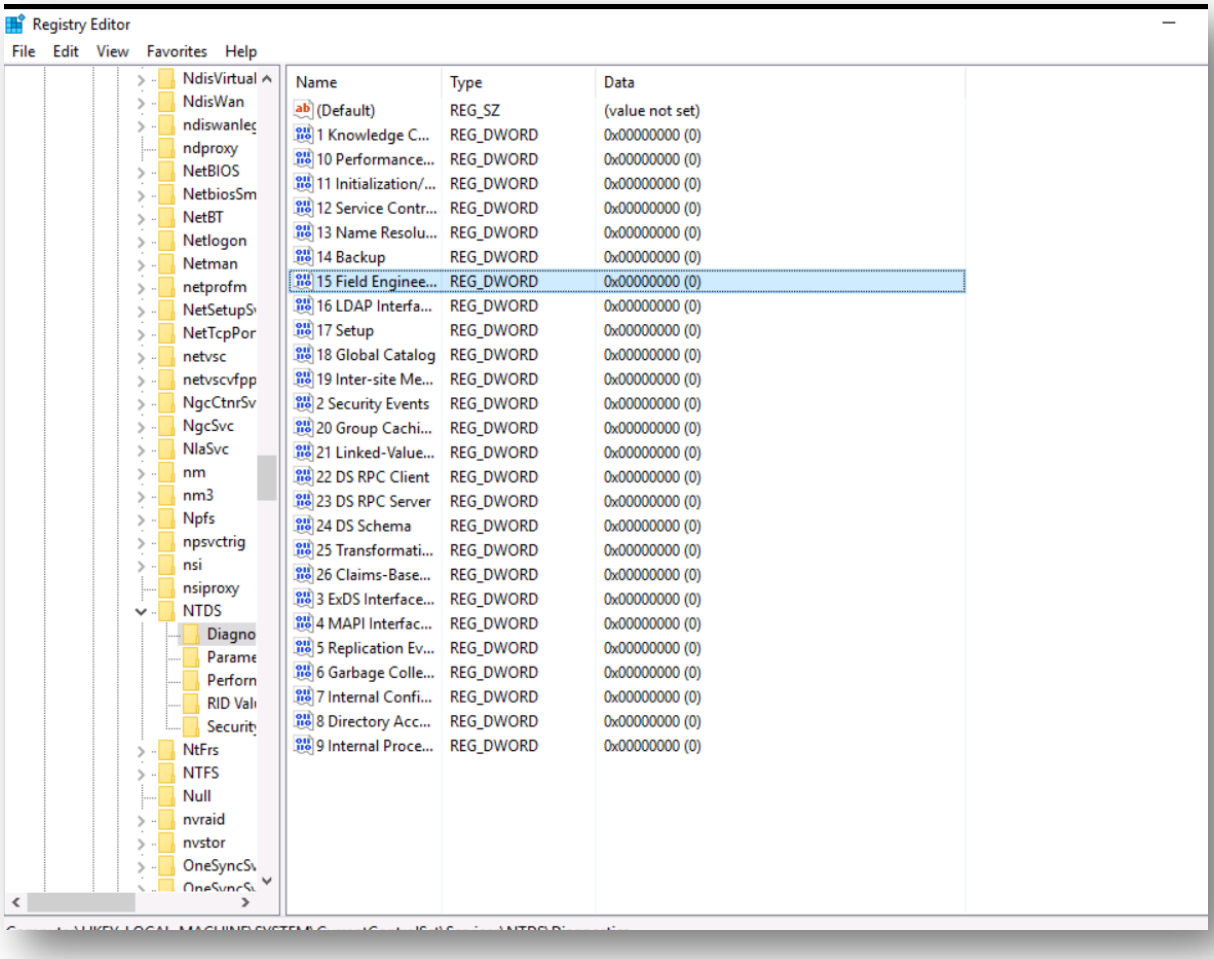
📝 What is the default value of all diagnostics configurations?

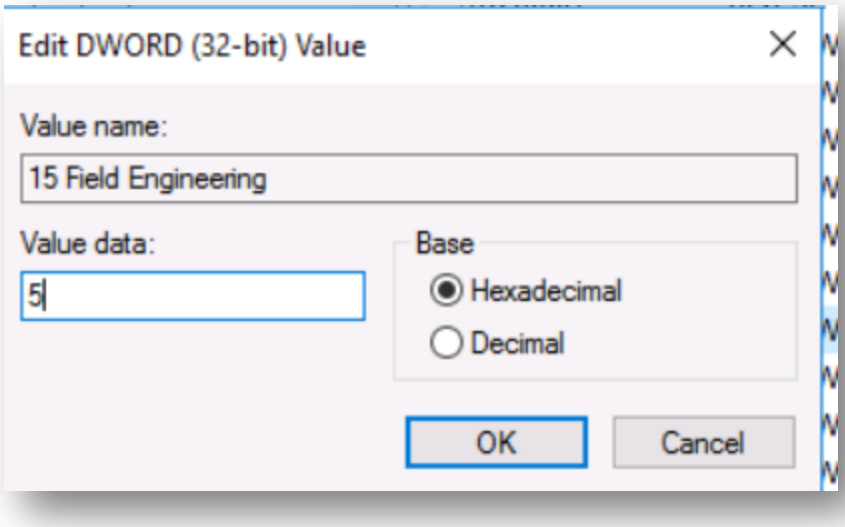
- Réponse sur la capture ci-dessous.

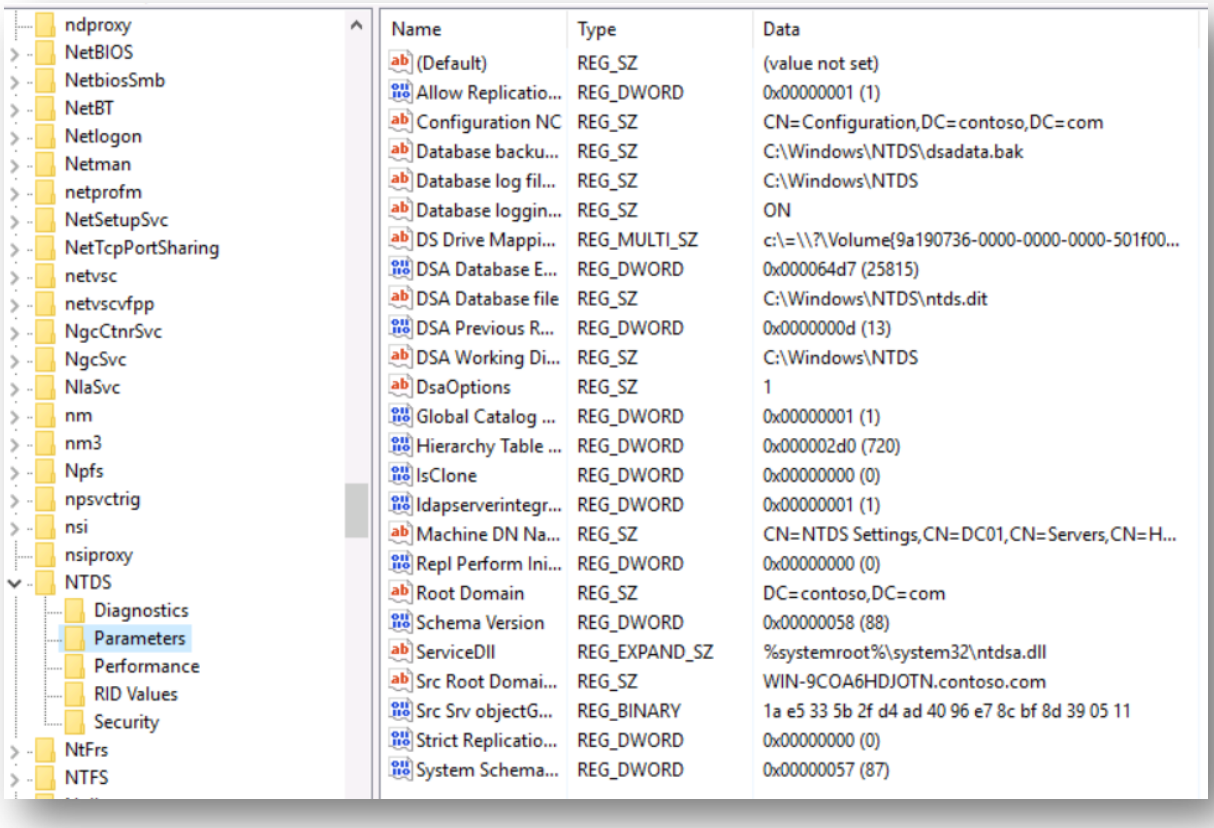


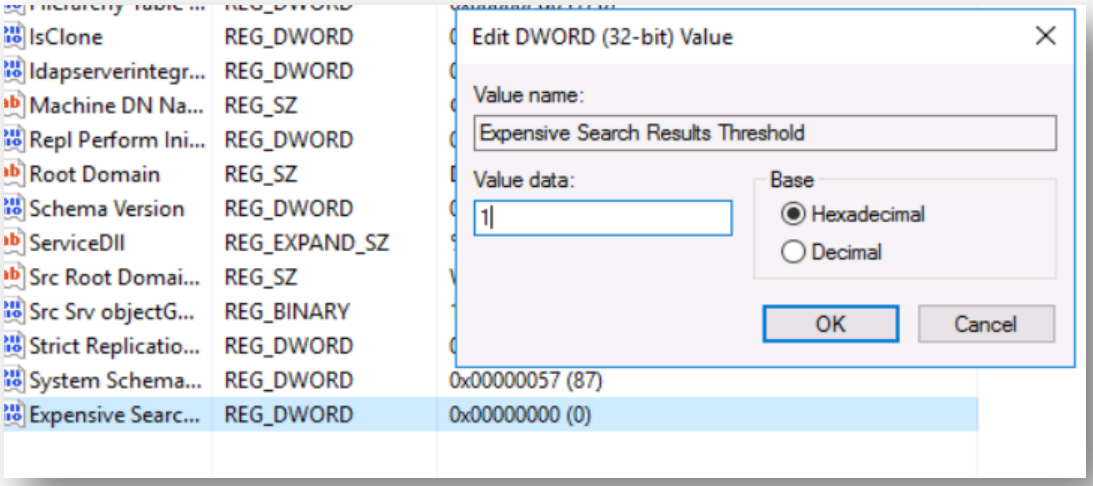


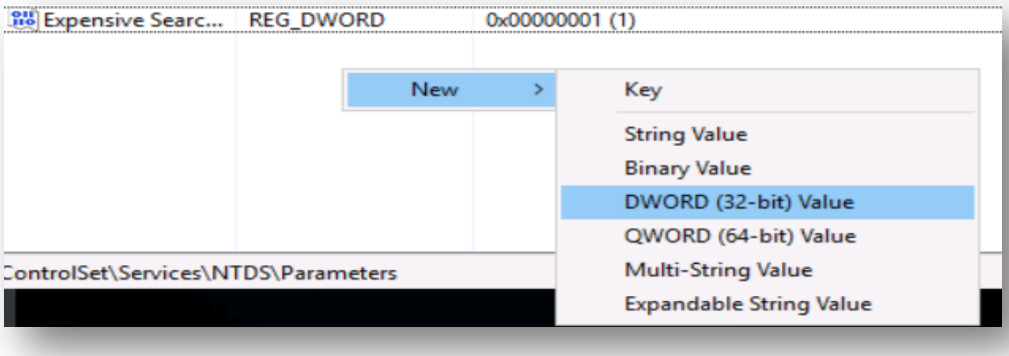

Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
regedit
OK
Cancel
Browse...

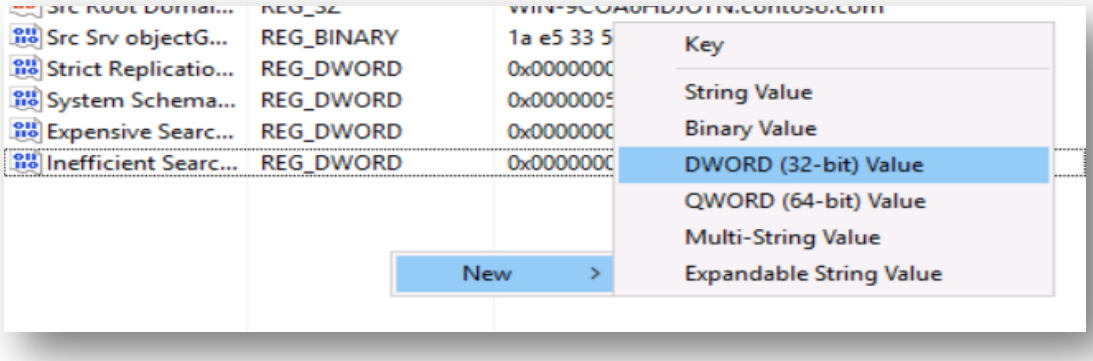

Registry Editor
File Edit View Favorites Help
NdisVirtual
NdisWan
ndiswanlegacy
ndproxy
NetBIOS
NetbiosSm
NetBT
Netlogon
Netman
netprofm
NetSetupSvc
NetTcpPor
netvsc
netvscvfpp
NgcCtnrSv
NgcSvc
NlaSvc
nm
nm3
Npfs
npsvctrig
nsi
nsiproxy
NTDS
Diagno
Parame
Perform
RID Val
Security
NtFrs
NTFS
Null
nvraid
nvstor
OneSyncSv
Name
Type
Data
(Default)
REG_SZ
(value not set)
1 Knowledge C...
10 Performance...
11 Initialization/...
12 Service Contr...
13 Name Resolu...
14 Backup
15 Field Enginee...
16 LDAP Interfa...
17 Setup
18 Global Catalog
19 Inter-site Me...
2 Security Events
20 Group Cachi...
21 Linked-Value...
22 DS RPC Client
23 DS RPC Server
24 DS Schema
25 Transformati...
26 Claims-Base...
3 ExDS Interface...
4 MAPI Interfac...
5 Replication Ev...
6 Garbage Colle...
7 Internal Confi...
8 Directory Acc...
9 Internal Proce...
REG_DWORD
0x00000000 (0)


Edit DWORD (32-bit) Value
Value name:
15 Field Engineering
Value data:
5
Base
Hexadecimal
Decimal
OK
Cancel

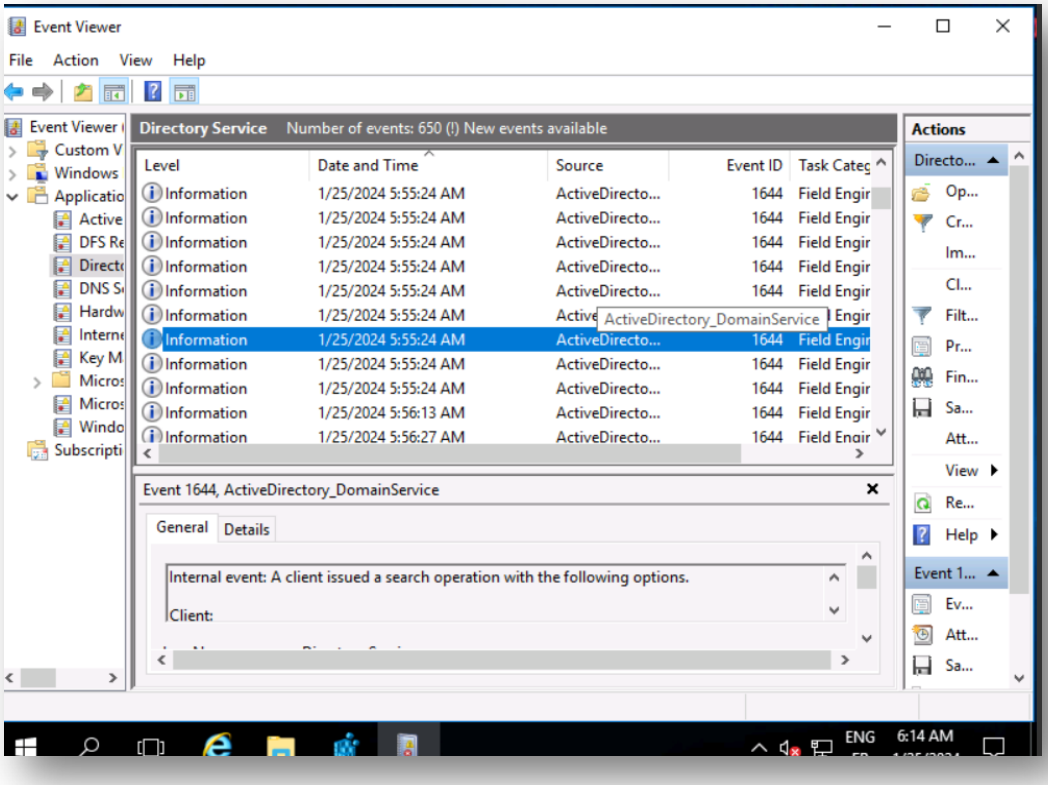

ndproxy
NetBIOS
NetbiosSmb
NetBT
Netlogon
Netman
netprofm
NetSetupSvc
NetTcpPortSharing
netvsc
netvscvfpp
NgcCtnrSvc
NgcSvc
NlaSvc
nm
nm3
Npfs
npsvctrig
nsi
nsiproxy
NTDS
Diagnostics
Parameters
Performance
RID Values
Security
NtFrs
NTFS
Name
Type
Data
(Default) REG_SZ (value not set)
Allow Replicatio... REG_DWORD 0x00000001 (1)
Configuration NC REG_SZ CN=Configuration,DC=contoso,DC=com
Database backu... REG_SZ C:\Windows\NTDS\dsadata.bak
Database log fil... REG_SZ C:\Windows\NTDS
Database loggin... REG_SZ ON
DS Drive Mappi... REG_MULTI_SZ c:\=\\?\Volume{9a190736-0000-0000-0000-501f00...
DSA Database E... REG_DWORD 0x000064d7 (25815)
DSA Database file REG_SZ C:\Windows\NTDS\ntds.dit
DSA Previous R... REG_DWORD 0x0000000d (13)
DSA Working Di... REG_SZ C:\Windows\NTDS
DsaOptions REG_SZ 1
Global Catalog ... REG_DWORD 0x00000001 (1)
Hierarchy Table ... REG_DWORD 0x000002d0 (720)
IsClone REG_DWORD 0x00000000 (0)
ldapserverintegr... REG_DWORD 0x00000001 (1)
Machine DN Na... REG_SZ CN=NTDS Settings,CN=DC01,CN=Servers,CN=H...
Repl Perform Ini... REG_DWORD 0x00000000 (0)
Root Domain REG_SZ DC=contoso,DC=com
Schema Version REG_DWORD 0x00000058 (88)
ServiceDll REG_EXPAND_SZ %systemroot%\system32\ntdsa.dll
Src Root Domai... REG_SZ WIN-9COA6HDJOTN.contoso.com
Src Srv objectG... REG_BINARY 1a e5 33 5b 2f d4 ad 40 96 e7 8c bf 8d 39 05 11
Strict Replicatio... REG_DWORD 0x00000000 (0)
System Schema... REG_DWORD 0x00000057 (87)


IsClone REG_DWORD
ldapserverintegr... REG_DWORD
Machine DN Na... REG_SZ
Repl Perform Ini... REG_DWORD
Root Domain REG_SZ
Schema Version REG_DWORD
ServiceDll REG_EXPAND_SZ
Src Root Domai... REG_SZ
Src Srv objectG... REG_BINARY
Strict Replicatio... REG_DWORD
System Schema... REG_DWORD 0x00000057 (87)
Expensive Searc... REG_DWORD 0x00000000 (0)
Edit DWORD (32-bit) Value
Value name:
Expensive Search Results Threshold
Value data:
1
Base
Hexadecimal
Decimal
OK
Cancel

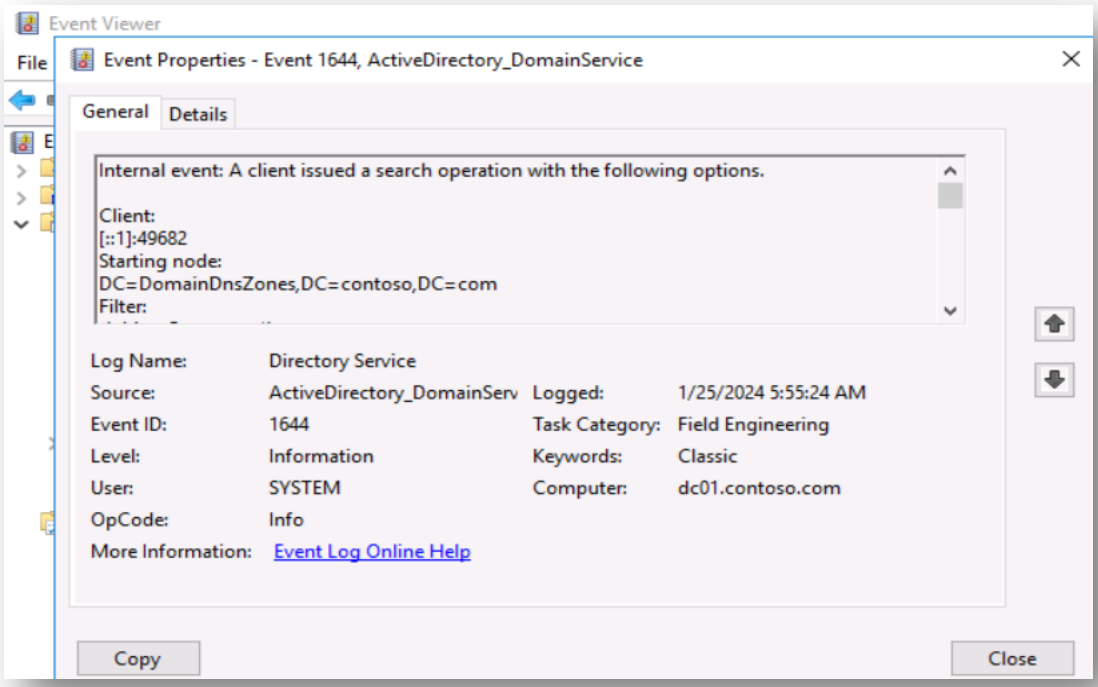

Expensive Searc... REG_DWORD 0x00000001 (1)
New
Key
String Value
Binary Value
DWORD (32-bit) Value
QWORD (64-bit) Value
Multi-String Value
Expandable String Value
ControlSet\Services\NTDS\Parameters


Src Srv objectG... REG_BINARY 1a e5 33 5
Strict Replicatio... REG_DWORD
System Schema... REG_DWORD
Expensive Searc... REG_DWORD
Inefficient Searc... REG_DWORD
New
Key
String Value
Binary Value
DWORD (32-bit) Value
QWORD (64-bit) Value
Multi-String Value
Expandable String Value

```
PS C:\Tools\Scripts> .\sharphound.exe --collectionmethods All
2024-01-25T06:08:00.2417400-08:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of
 BloodHound
2024-01-25T06:08:00.3667384-08:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, S
ession, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-01-25T06:08:00.3823636-08:00|INFORMATION|Initializing SharpHound at 6:08 AM on 1/25/2024
2024-01-25T06:08:01.9136922-08:00|INFORMATION|Loaded cache with stats: 210 ID to type mappings.
 217 name to SID mappings.
 2 machine sid mappings.
 4 sid to domain mappings.
 0 global catalog mappings.
2024-01-25T06:08:01.9136922-08:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trus
ts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-01-25T06:08:02.2261939-08:00|INFORMATION|Beginning LDAP search for contoso.com
2024-01-25T06:08:02.3198628-08:00|INFORMATION|Producer has finished, closing LDAP channel
2024-01-25T06:08:02.3198628-08:00|INFORMATION|LDAP channel closed, waiting for consumers
2024-01-25T06:08:32.2584381-08:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 46 MB RAM
2024-01-25T06:08:50.2276744-08:00|INFORMATION|Consumers finished, closing output channel
Closing writers
2024-01-25T06:08:50.2745429-08:00|INFORMATION|Output channel closed, waiting for output task to complete
2024-01-25T06:08:50.3526698-08:00|INFORMATION|Status: 250 objects finished (+250 5.208333)/s -- Using 50 MB RA
M
2024-01-25T06:08:50.3526698-08:00|INFORMATION|Enumeration finished in 00:00:48.1250726
2024-01-25T06:08:50.4151673-08:00|INFORMATION|Saving cache with stats: 210 ID to type mappings.
 217 name to SID mappings.
 2 machine sid mappings.
 4 sid to domain mappings.
 0 global catalog mappings.
2024-01-25T06:08:50.4151673-08:00|INFORMATION|SharpHound Enumeration Completed at 6:08 AM on 1/25/2024! Happy
Graphing!
PS C:\Tools\Scripts>
```

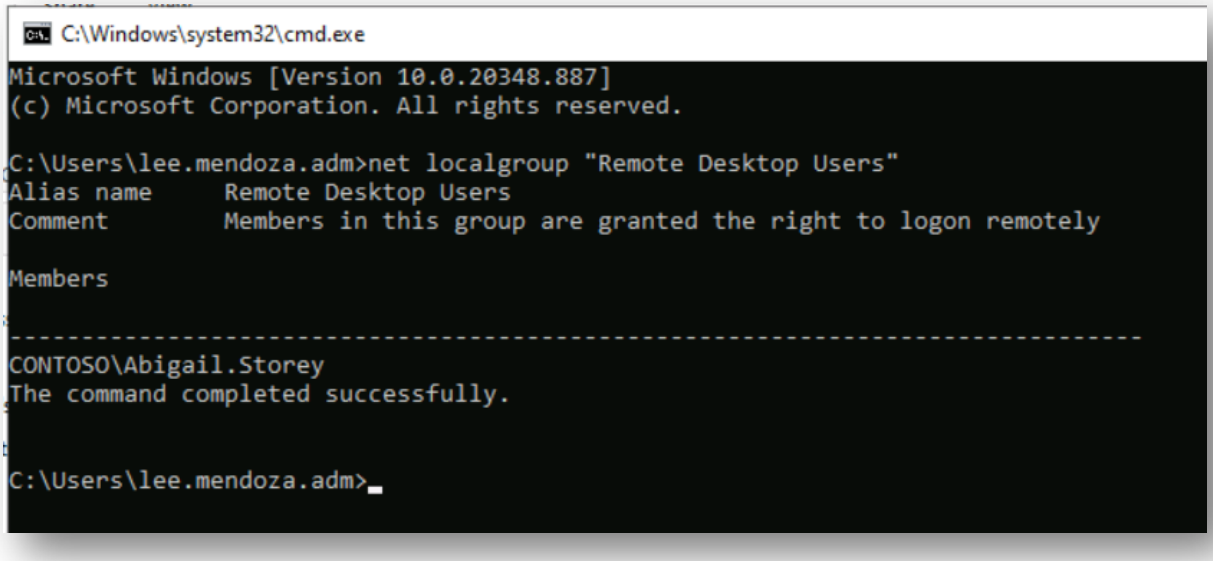


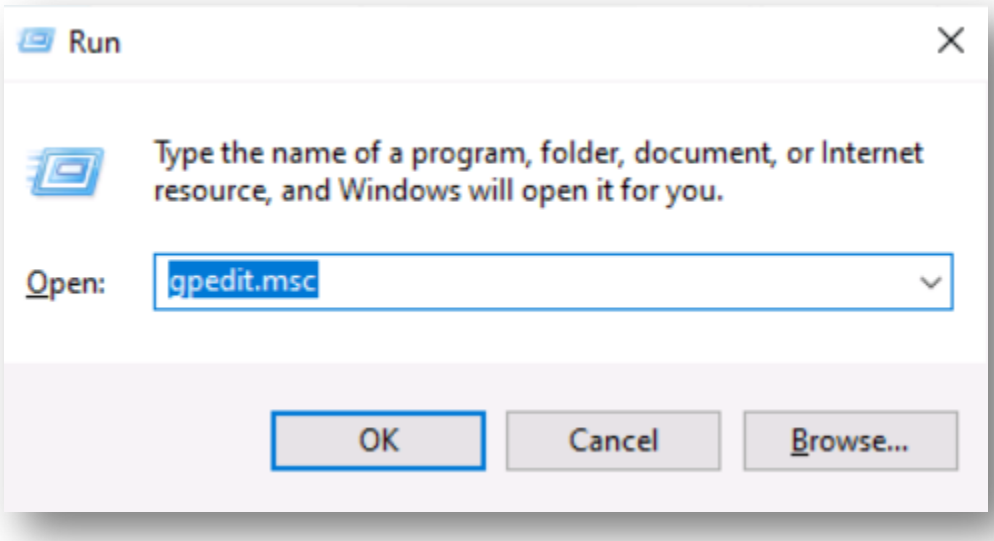
Module 2 – Lab 2 – Reconnaissance



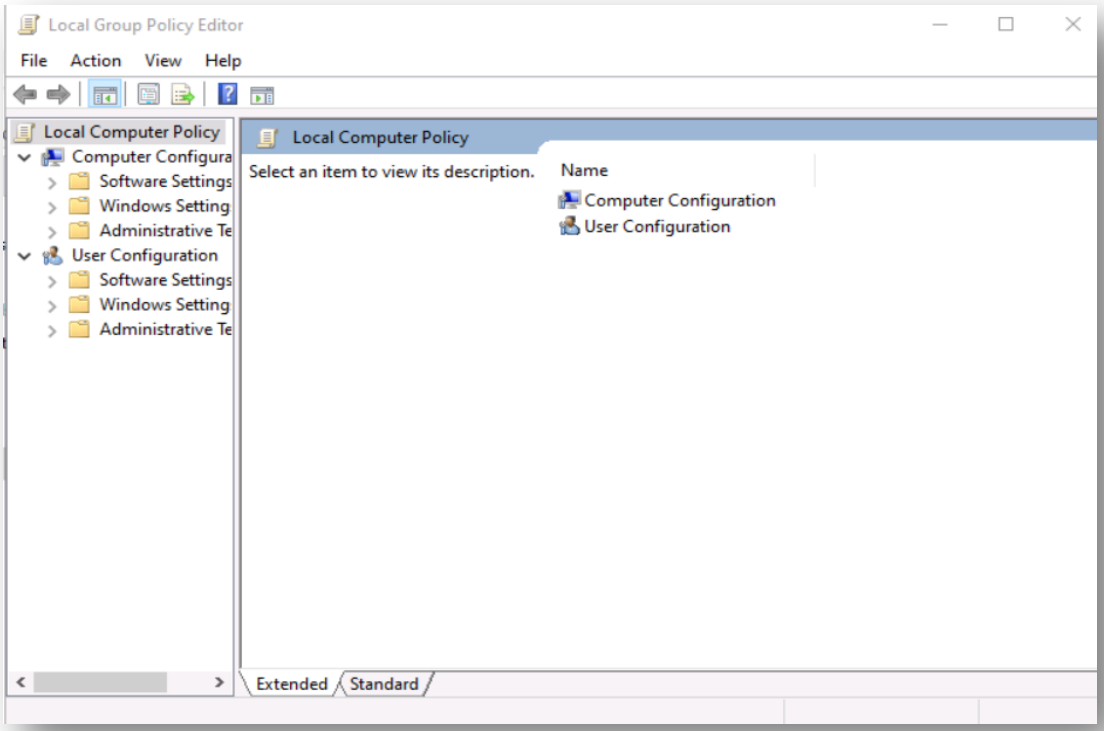
Exercise 4 - Restrict SAM-R enumeration on a member server

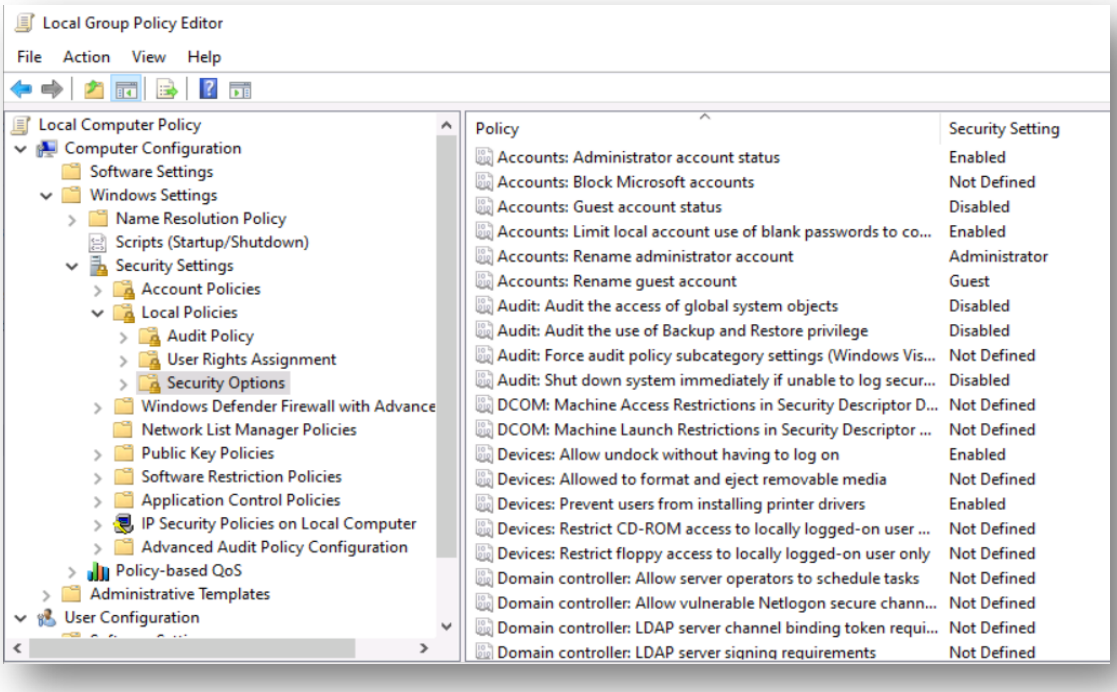
📝 Who is a member of the group?

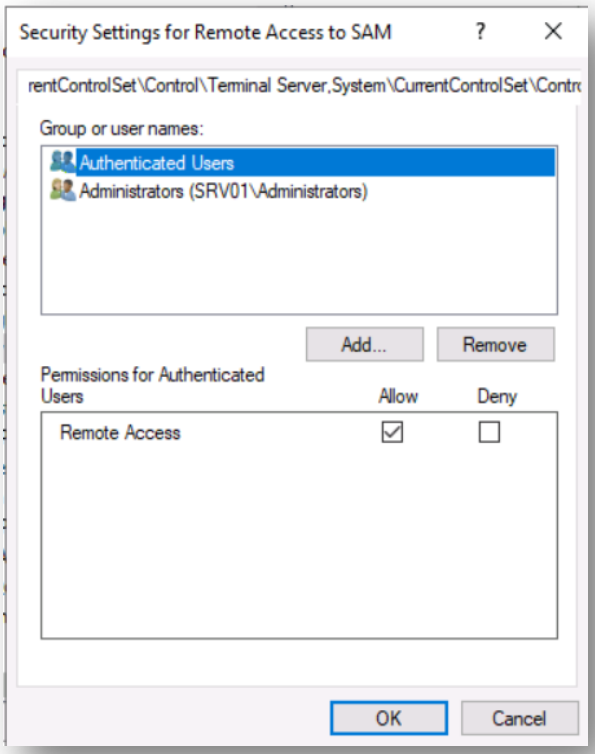


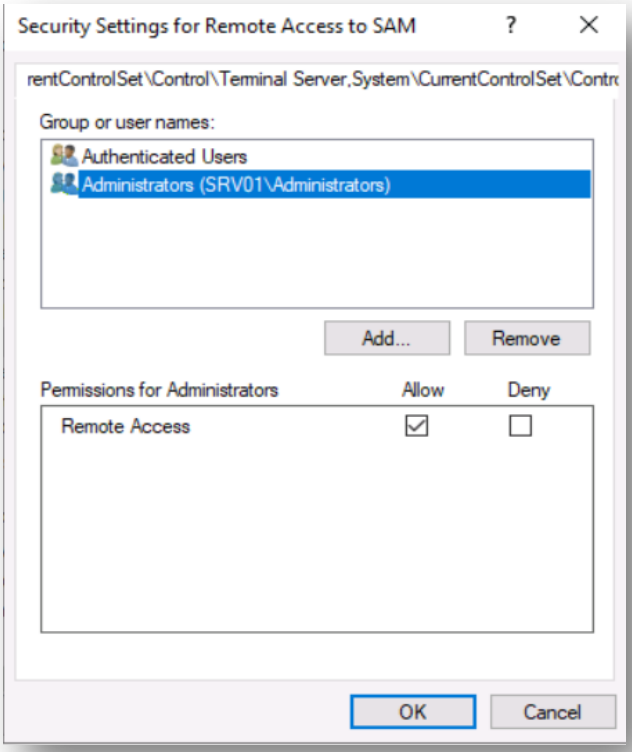


Module 2 – Lab 2 – Reconnaissance






Security Settings for Remote Access to SAM
rentControlSet\Control\Terminal Server,System\CurrentControlSet\Contro
Group or user names:
Authenticated Users
Administrators (SRV01\Administrators)
Add...
Remove
Permissions for Authenticated Users
Allow
Deny
Remote Access
OK
Cancel


Security Settings for Remote Access to SAM
rentControlSet\Control\Terminal Server,System\CurrentControlSet\Contro
Group or user names:
Authenticated Users
Administrators (SRV01\Administrators)
Add...
Remove
Permissions for Administrators
Allow
Deny
Remote Access
OK
Cancel

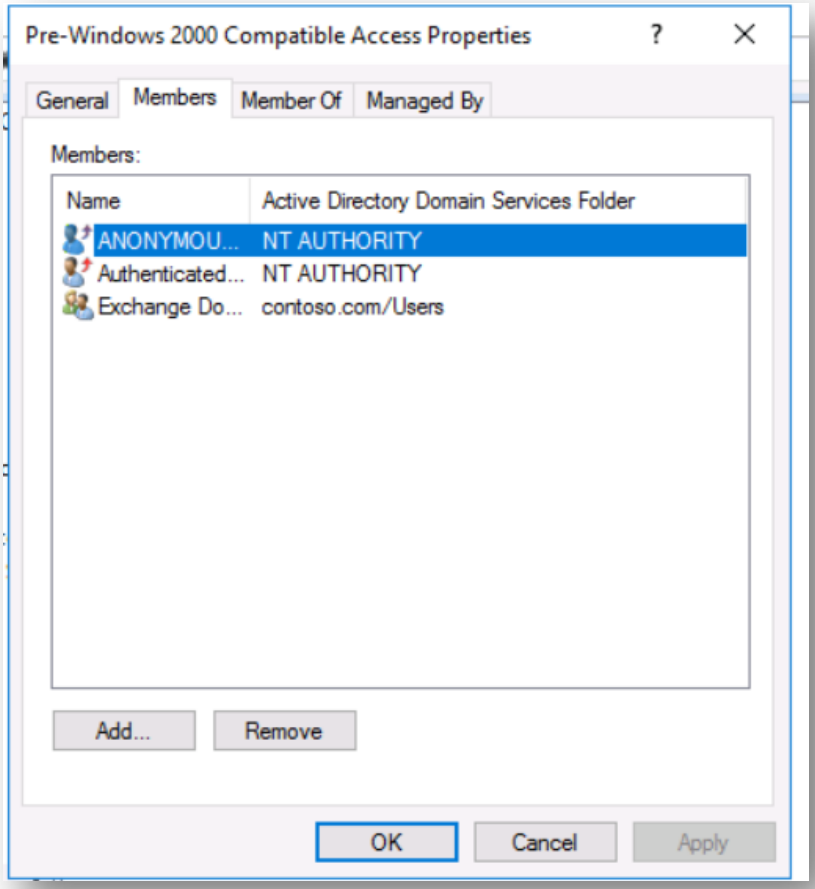
Module 2 – Lab 2 – Reconnaissance

📝 Why is using a group policy recommended to use a group policy for these settings?

L’utilisation d’une stratégie de groupe est recommandée pour ces paramètres car elle permet une configuration centralisée et cohérente des politiques des ordinateurs et des utilisateurs à travers un réseau, améliorant ainsi la sécurité et la gestion.

Exercise 5 - Enumerate domain users and group anonymously

📝 Who else is a member of this group in the lab?



📝 What is the error message?

```
Host script results:
| smb-enum-users:
|_  ERROR: Access denied while trying to enumerate users; except against Windows 2000, Guest or better is typi
cally required
Final times for host: srtt: 1000 rttvar: 3750  to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 07:04
Completed NSE at 07:04, 0.00s elapsed
Read from C:\Program Files (x86)\Nmap: nmap-mac-prefixes nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 5.48 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
PS C:\Users\red>
```

```
PS C:\Tools\Scripts> .\Invoke-NetSessionEnum.ps1 -Hostname DC01

Netapi32::NetSessionEnum Buffer Offset  --> 0x00000226F26D8AC0
Result-set contains 1 session(s)!

OriginatingHost DomainUser SessionTime IdleTime
--------------- ---------- ----------- --------
\\192.168.1.31  red                  0        0

Calling NetApiBufferFree, no memleaks here!
```

Exercise 6 - Restrict SMB enumeration [optional]

📝 Try to run the previous command without the "| Out-GridView -Title "SMB permissions". What is the difference?

📝 Do you still see connections?