

**Introduction**

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

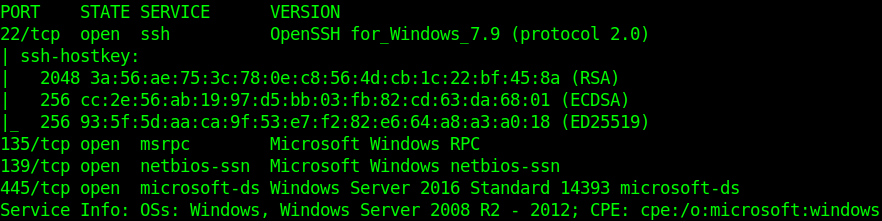
Compétences mises en œuvre :

* 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 |

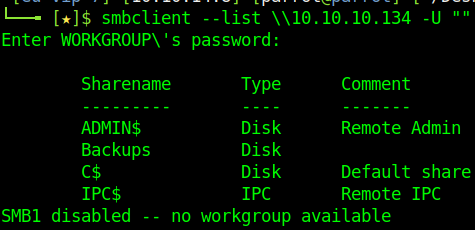


Plusieurs ports d’ouverts :

* **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** :

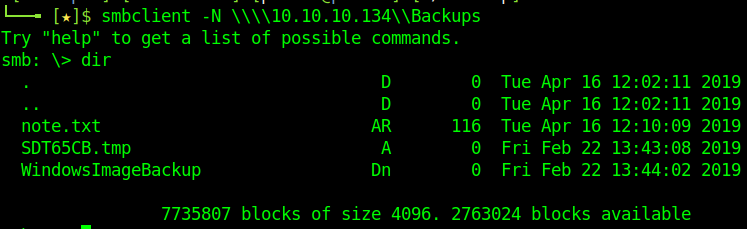
|  |
| --- |
| $ smbclient –list [\\10.10.10.134](file:///\\10.10.10.134) -u "" |



**Obtenir un accès utilisateur**

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

|  |
| --- |
| $ smbclient -N [\\\\10.10.10.134\\Backups](file:///\\\\10.10.10.134\\Backups)  Smb > dir |



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

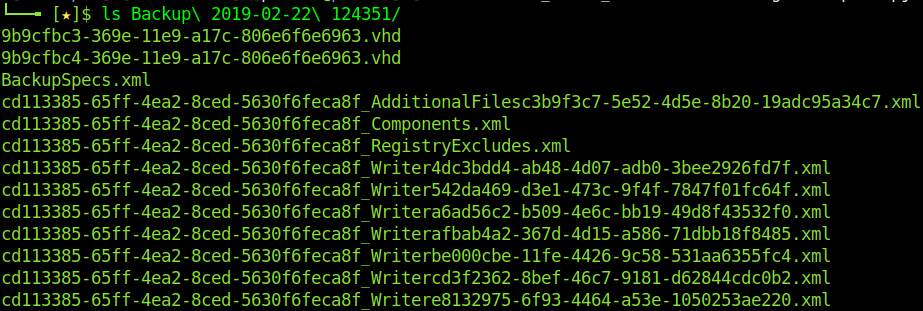
|  |
| --- |
| $ mkdir /mnt/bastion\_partage  $ mount -t cifs //10.10.10.134/Backups /mnt/bastion\_partage/ |

Le fichier **note.txt** contient :

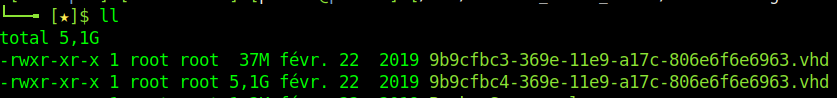


Le fichier **SDT65CB.tmp** ne contient rien.

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



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



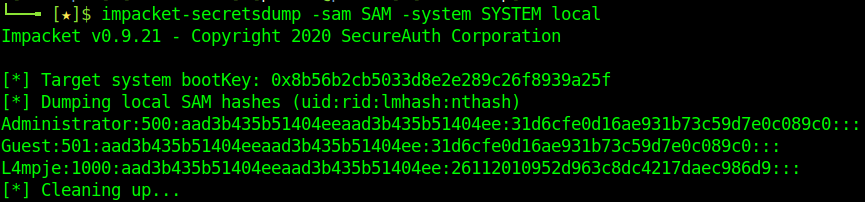
|  |
| --- |
| $ cp 9b9cfbc3-369e-lle9-a17c-806e6f6e6963.vhd ~/Desktop/image.vhd  $ guestmount –add image.vhd –ro –inspector -v /home/parrot/bastion/vhd |

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** :

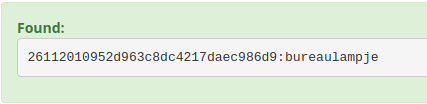
|  |
| --- |
| $ sudo cp vhd/Windows/System32/config/SAM ~/Desktop/SAM  $ sudo cp vhd/Windows/System32/config/SYSTEM ~/Desktop/SYSTEM |

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 |



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) :



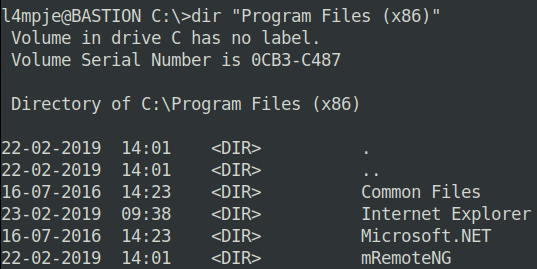
Nous allons nous connecter en **ssh** et lire le **user.txt** :



**Obtenir un accès administrateur**

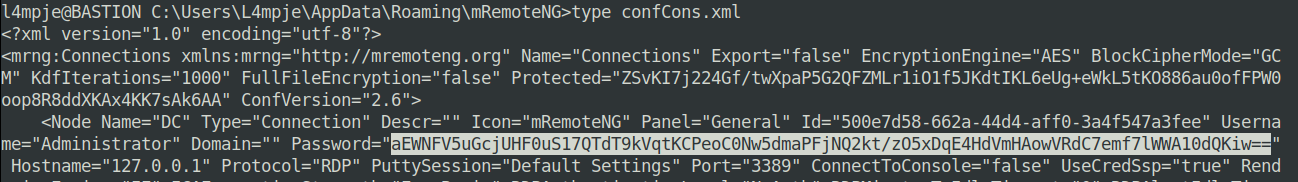
En faisant l’énumération de base, nous voyons un logiciel installé qui n’est pas commun :

|  |
| --- |
| C:\> dir "Program Files (x86)" |



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 |



|  |
| --- |
| $ python mremoteng\_decrypt.py -s <Hash> |



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

