

**Introduction**

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

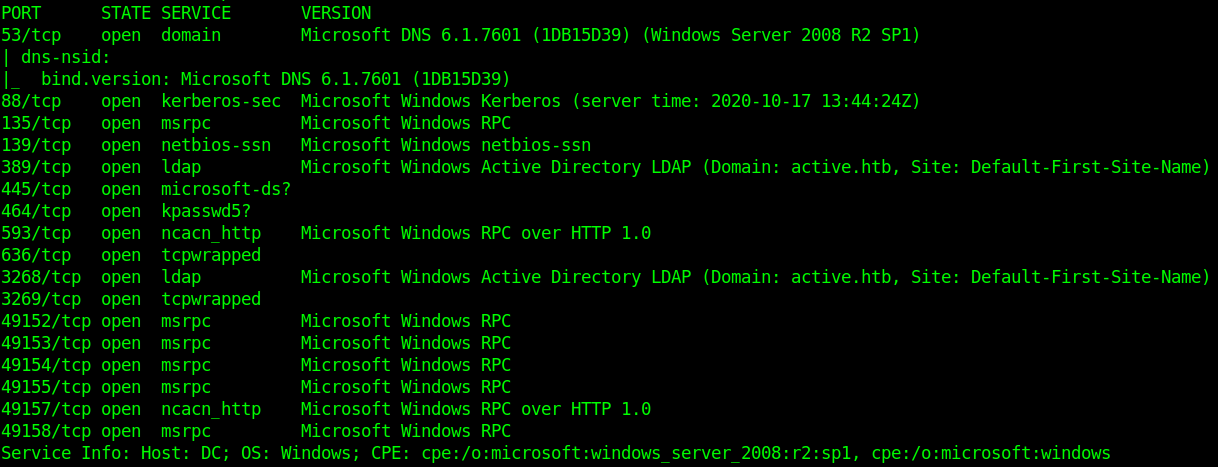
Compétences mises en œuvre :

* Enumération des ports et services d’un ordinateur distant.

**Enumération initiale**

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

|  |
| --- |
| $ nmap -T4 -A 10.10.10.100 |



Plusieurs ports d’ouverts :

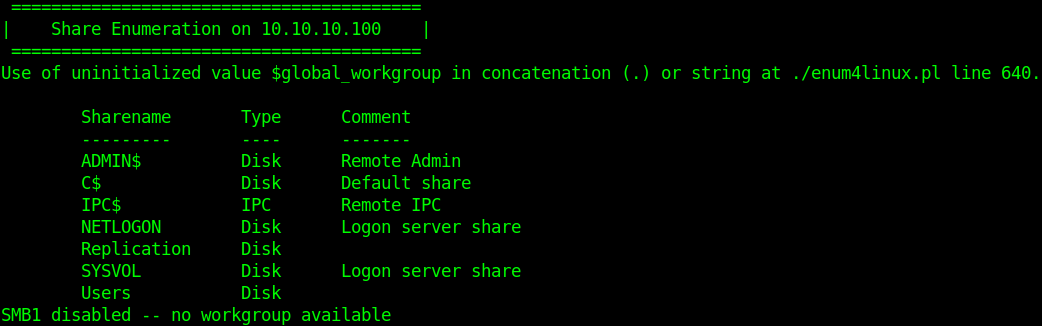
* **53** pour un service **DNS**.
* **88** pour un service **Kerberos**.
* **135** pour du **msrpc**, il permet les appels de procédures RPC.
* **139** pour du **netbios-ssn**, il permet la découverte et la connexion des voisins dans le réseau.
* **389** et **3268** pour un service d’annuaire (**Microsoft 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 :

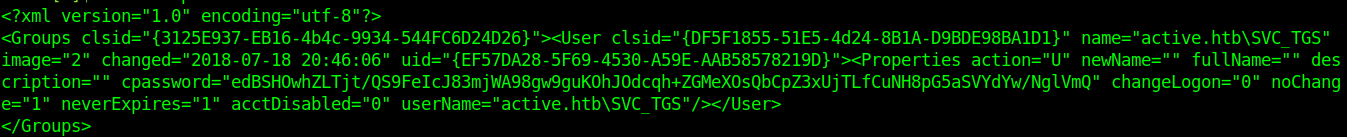
|  |
| --- |
| $ enum4linux 10.10.10.100 |



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

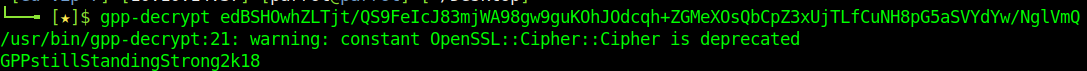
|  |
| --- |
| $ smbclient -N -U "" //10.10.10.100/Replication  \> cd active.htb  \> cd Policies  \> cd {31B2F340-016D-11D2-945F-00C04FB984F9}  \> cd MACHINE  \> cd Preferences  \> cd Groups  \> get Groups.xml |

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



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> |



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 |



**Obtenir un accès Administrateur**

Blaz