Pentest - Windows RAM Extract and Analysis

Ce document présente la mise en oeuvre d'un dump de RAM sur une machine Windows, de son extraction et de son analyse. Il s'agit d'une étape de looting, on considèrera donc que nous avons déjà un accès administrateur à la machine à notre disposition.

Dump de RAM

Les outils permettant le dump de RAM sont généralement très simples à utiliser et ne présentent quasiment pas d'option. Il en existe un grand nombre.

Exemple : MagnetForensics DumpIt

https://www.magnetforensics.com/fr/resources/magnet-dumpit-pour-windows/

Le dump s'opère de manière extrêmement simple en lançant le binaire en tant qu'administrateur.

```
PS C:\Users\Administrateur\downloads> .\DumpIt.exe

  DumpIt 3.6.20230117 (X64) (Jan 17 2023)
  Copyright (C) 2007 - 2021, Matt Suiche (msuiche)
  Copyright (C) 2016 - 2021, Comae Technologies DMCC <https://www.comae.com>
  Copyright (c) 2022, Magnet Forensics, Inc. <https://www.magnetforensics.com/>
  All rights reserved.

  Thanks for using DumpIt! Always use Microsoft crash dumps!

    Destination path:           \??\C:\Users\Administrateur\downloads\WIN-43JJRDMS9FV-20

    Computer name:              WIN-43JJRDMS9FV


    --> Proceed with the acquisition ? [y/n] y
```

Si tout s'est bien passé, le dump doit faire la taille de la RAM disponible sur la machine. Il n'y a plus qu'à rapatrier le fichier de sortie sur la machine d'analyse.

```
      Length Name
      ------ ----
      630600 DumpIt.exe
  4294504448 WIN-43JJRDMS9FV-20230924-215540.dmp
```

Analyse du dump

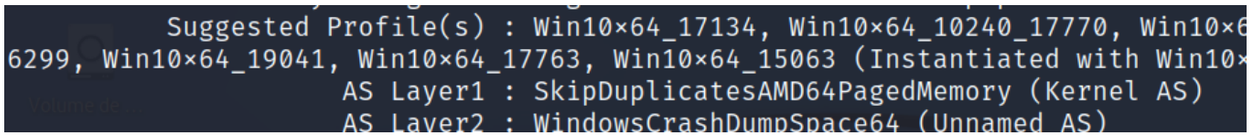
L'outil de base pour notre analyse sera le framework Volatility. Ce framework est généralement plutôt utilisé à des fins de Forensics mais répondra à notre besoin pour ce qui est de l'extraction de secrets dans la mémoire.

De manière assez rudimentaire, nous avons besoin d'une seule information (en plus du dump) pour avancer : le profil de la machine.

En effet, Volatility a besoin de savoir sur quel modèle se baser pour découper la mémoire et en extraire un maximum d'informations.

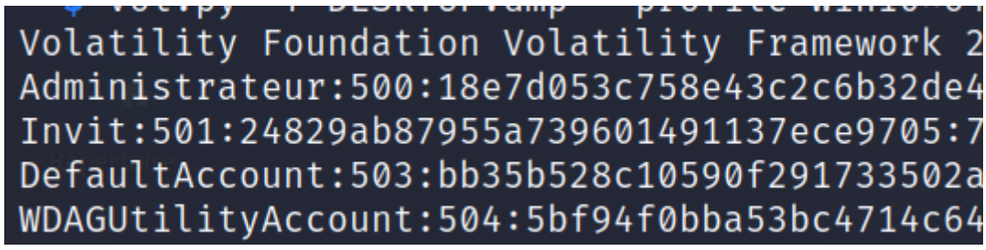
Pour déterminer ce profil :

```
vol.py -f fichier.dump imageinfo
```



Une fois que l'on aura celui-ci, il n'y a plus qu'à loot le dump :

```
vol.py -f fichier.dump --profile=Win10x64_17134 hashdump
```



Un hash NTLM étant assez faible, un coup dans une crackstation devrait sans trop de problème nous sortir le mot de passe initial.

Hash	Type	Result
ecce60725930	NTLM	passw0rd