Memory forensic (Volatility)

Volatility est un outils permettant d'analyser les dumps de ram.

Installation

Pour l'installer il faut cloner le repo github : `git clone https://github.com/volatilityfoundation/volatility3.git`

Utilisation

Installer les dépendances :

- `pip3 install -r requirements.txt`

Vérfier l'installation :

- `python3 vol.py -h`

Commandes de base

Attention certaines commandes peuvent changer selon votre version de volatility, ces commandes fonctionnent avec volatility 3, mais peuvent changées entre temps.

Lister les procéssus actifs :

- `python3 vol.py -f <dump_memoire> windows.pslist`

ou selon la version

- `volatility --profile=Win10x64 -f <chemin_vers_le_dump> pslist`

Extraire un processus suspect :

- `python3 vol.py -f <dump_memoire> windows.dumpfiles --pid <PID>`

Lister tous les fichiers présents ou référencés en mémoire :

- `python3 vol.py -f <dump_memoire> filescan`

Extraire un fichier du dump :

- `python3 vol.py -f dump.raw windows.dumpfiles --physaddr <offset>`

Revision #7
Created 10 July 2025 06:48:18 by Bibi
Updated 10 July 2025 07:38:05 by Bibi