Installation de logiciels additionnels

II – Installation des logiciels additionnel

Les logiciels

Bien que les logiciels que nous allons installer dans cette partie sont ou seront probablement installé par défaut dans les prochaines versions de Kali Linux, il est nécessaire de détailler leur installation à la main afin de savoir le faire en cas de problème.

Nous allons donc installer 3 Logiciels à savoir :

Volatility

Exiftool

FirefoxDecrypt

Le détail

Volatility *est un outils open source pour l'analyse de dump mémoire, c'est un framework écrit en Python. Il permet d'analyser les dumps mémoires de Windows/Mac/Linux/Android et le framework est disponible sur Windows/Mac/Linux. On peut aussi lui adjoindre une panoplie de plugins.*

ExifTool *est un logiciel gratuit et open-source permettant de lire, d'écrire et de manipuler des métadonnées d'image, audio, vidéo et PDF.*

Firefox Decrypt *est un outil pour extraire les mots de passe des profils de Mozilla Firefox™, Thunderbird®, SeaMonkey® et dérivés. Il peut être utilisé pour récupérer les mots de passe d'un profil protégé par un Master Password tant que ce dernier est connu. Si un profil n'est pas protégé*

par un mot de passe principal, les mots de passe sont affichés sans invite.

Mise à jour de Kali

Pour commencer sachez que cette étape peut sembler inutile mais elle permet au contraire de vous assurer de tous les temps être à jour. Comme ça tous les logiciels sont compatibles avec votre version. Pour la première commande :

```
sudo apt-get update && apt-get upgrade && apt-get dist-upgrade
```

Installation de Volatility

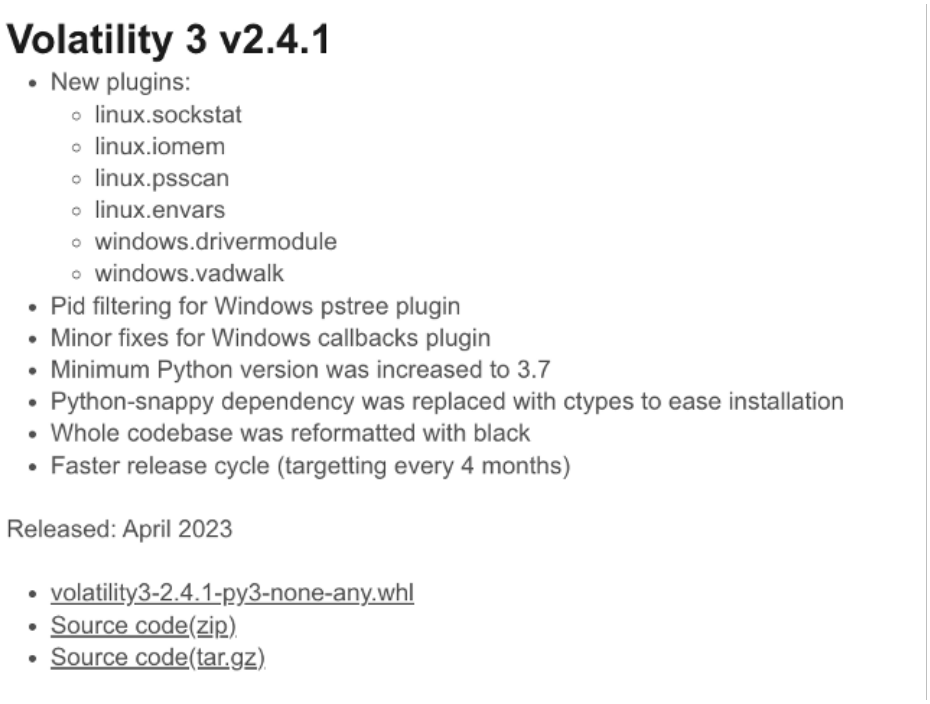
Dans un premier temps, il est nécessaire d'installer les paquets qui vont être nécessaire à l'installation de volatility.

```
sudo apt-get install python3


sudo apt-get install python3-pip build-essential python-setuptools
```

Une fois les paquets nécessaires installer, nous allons aller sur le site de volatility et télécharger le code source qui est nécessaire pour l'installation. Rendez-vous donc sur le site à cette adresse.

https://www.volatilityfoundation.org/releases-vol3. Télécharger la version dont vous avez besoin. Dans mon cas je vais prendre la dernière version actuelle à savoir la version Volatility 3 2.4.1.



Volatility 3 v2.4.1

- New plugins:
  - linux.sockstat
  - linux.iomem
  - linux.psscan
  - linux.envars
  - windows.drivermodule
  - windows.vadwalk
- Pid filtering for Windows pstree plugin
- Minor fixes for Windows callbacks plugin
- Minimum Python version was increased to 3.7
- Python-snappy dependency was replaced with ctypes to ease installation
- Whole codebase was reformatted with black
- Faster release cycle (targetting every 4 months)

Released: April 2023

- volatility3-2.4.1-py3-none-any.whl
- Source code(zip)
- Source code(tar.gz)

On se retrouve ensuite dans le dossier téléchargement ou le fichier de code source a été télécharger. On va maintenant décompresser l'archive précédemment télécharger. Pour ce faire on ouvre un terminal en mode root, on se rend dans le dossier Téléchargement.

```
cd /home/kali/Téléchargement/
```

Une fois dans le dossier téléchargement on décompresse l'archive.

```
unzip volatility3-2.4.1.zip
```

Une fois décompresser, un dossier est créé. Nous allons maintenant le déplacer sur le bureau ou seront tous les outils de kali que je vais installer pour ce faire.

```
mv volatility3-2.4.1.zip /home/kali/Bureau/volatility
```

Une fois cela fait on peut se rendre sur le bureau pour voir si le fichier volatility est bien là. Vous allez donc voir que le fichier a un cadenas car il a été manipuler par le superutilisateur donc l'utilisateur Kali n'a pas les droits. Pour lui attribuer les droits, nous allons faire ceci.

```
chmod 777 /home/kali/Bureau/volatility
```

Une fois cette commande faites le cadenas disparait. On va donc pouvoir poursuivre l'installation de volatility.

Pour l'installation on va faire cette commande

```
python3 /home/kali/Bureau/volatility/setup.py install
```

Une fois la commande terminée, vous pouvez donc tester si volatility fonctionne bien.

```
cd /home/kali/Bureau/volatility


python3 vol.py
```

Normalement, la commande devrait afficher les options qui sont possible de faire avec volatility.

Installation de Exiftool

Pour commencer nous allons télécharger le logiciel. Pour ce faire faire cette commande

```
git clone https://github.com/exiftool/exiftool.git
```

Maintenant on peut retrouver sur le bureau le fichier exiftool avec le cadenas. Vous pouvez maintenant appliquer la méthode vue plus haut pour le faire disparaitre. On se rend donc dans le fichier précédemment télécharger avec la commande suivante.

```
cd exiftool
```

Maintenant on peut tester que le programme fonctionne en faisant la commande suivante

```
./exiftool
```

Vous allez donc voir une ligne s’afficher avec la manière donc il faut utiliser la commande.

Installation de Firefox Decrypt

De la même manière que exiftool, nous allons d’abord télécharger l’outil. Avec cette commande.

```
git clone https://github.com/unode/firefox_decrypt.git
```

Une fois la commande faite, nous allons faire la même chose en enlevant le cadenas au fichier télécharger. Nous pouvons maintenant exécuter l’outil de cette manière.

```
python firefox_decrypt.py
```

Des erreurs vont s’afficher mais c’est normal car aucun fichier de base de données Firefox a été spécifié.

Modifier la version de Python

Vérification

Dans un premier temps nous allons voir quelle version de python sont installer. Pour ce faire, cette commande.

```
update-alternatives --list python
```

Un message d’erreur doit donc apparaitre. Nous allons donc ajouter plusieurs alternative grâce au commandes suivante.

```
update-alternatives --install /usr/bin/python python /usr/bin/python2.7 1

update-alternatives --install /usr/bin/python python /usr/bin/python3.11 2
```

On peut donc revérifier si on a les versions alternatives de python d’installer avec cette commande qui doit donc retourner un résultat avec les version que vous avez choisi d’installer.

```
update-alternatives --list python
```

On peut donc avec cette commande choisir la version de python que l’on veut utiliser.

Sources : https://mk57blog.wordpress.com/2017/01/28/comment-modifier-la-version-par-defaut-de-python-sur-debian/

On va donc maintenant installer PIP pour la version 2.7 de python pour ce faire on commence par mettre a jour le système

```
sudo apt-get update
```

Puis on install les paquets nécessaire

```
curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py
```

Et enfin on exécuter le script télécharger

```
sudo python2 get-pip.py
```

Une fois fait tout est bon.

Installation de la suite Tinyscript

Contenu

Cette suite comprend 3 Outil :

- StegoLSB
- StegoPVD
- StegoPIT

Ces outils sont compliquer à installer. Il faut donc suivre la procédure au pied de la lettre.

Installation

Dans un premier temps nous allons télécharger les dépendance.

```
pip install tinyscript
```

Une fois cela fait, nous allons télécharger l’outil

```
wget https://gist.githubusercontent.com/dhondta/d2151c82dcd9a610a7380df1c6a0272c/raw/stegolsb.py && chmod +x stegolsb.py && sudo mv stegolsb.py /usr/bin/stegolsb
```

On peut aussi installer les deux autres outils une fois que le téléchargerment de celui-ci est fait.

```
wget https://gist.githubusercontent.com/dhondta/feaf4f5fb3ed8d1eb7515abe8cde4880/raw/stegopvd.py && chmod +x stegopvd.py && sudo mv stegopvd.py /usr/bin/stegopvd
```

Et enfin le dernier

```
wget https://gist.githubusercontent.com/dhondta/30abb35bb8ee86109d17437b11a1477a/raw/stegopit.py && chmod +x stegopit.py && sudo mv stegopit.py /usr/bin/stegopit
```

Une fois cela fait on peut donc se référer a la documentation des outils disponible a ces liens :

- https://gist.github.com/dhondta/d2151c82dcd9a610a7380df1c6a0272c
- https://gist.github.com/dhondta/feaf4f5fb3ed8d1eb7515abe8cde4880
- https://gist.github.com/dhondta/30abb35bb8ee86109d17437b11a1477a

---

Revision #2
Created 29 January 2025 18:45:39 by Admin
Updated 29 January 2025 19:01:25 by Admin