Computer forensics project

(Yves Le Bray)

Étude

Partant d'un disque dur dit formaté, ce projet consiste à démontrer qu'avec quelques outils d'analyse et une logique de récupération de données, qu'il est possible de récupérer une quantité importante (surtout données sensibles) d'information.

Ce rapport montre seulement la dangerosité des données formatées et est en aucun cas un résultat permettant de faire de la fouille de donnée de façon illégale.

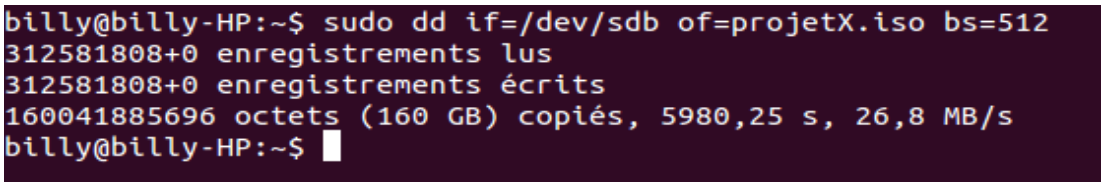
Acquisition des données

Copie du disque

Dans un premier temps je fais un ***fdisk*** pour déterminer le disque sur lequel je vais extraire les données.

```
billy@billy-HP:~$ sudo fdisk -l

Attention : identifiant de table de partitions GPT (GUID) détecté sur « /dev/sda
 » ! L'utilitaire fdisk ne prend pas GPT en charge. Utilisez GNU Parted.


Disk /dev/sda: 1000.2 GB, 1000204886016 bytes
255 têtes, 63 secteurs/piste, 121601 cylindres, total 1953525168 secteurs
Unités = secteurs de 1 * 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 4096 octets
taille d'E/S (minimale / optimale) : 4096 octets / 4096 octets
Identifiant de disque : 0x00000000

Périphérique Amorçage  Début         Fin      Blocs    Id. Système
/dev/sda1               1  1953525167   976762583+  ee  GPT
La partition 1 ne commence pas sur une frontière de cylindre physique.

Disk /dev/sdb: 160.0 GB, 160041885696 bytes
255 têtes, 63 secteurs/piste, 19457 cylindres, total 312581808 secteurs
Unités = secteurs de 1 * 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Identifiant de disque : 0x0994dd6e

Périphérique Amorçage  Début         Fin      Blocs    Id. Système
```

Le disque sera le volume sdb ; la copie se fera avec l'outil ***dd***.
Le but consiste à faire une copie bit à bit du disque sur un support différent afin de réaliser une analyse dite post-mortem par la suite.



Montage de l'image

Le but étant également de faire une analyse en évitant d'altérer les données originales sur le disque, il faut monter l'image disque comme suit :

sudo mount -o loop,ro /mnt/test

Il faut également penser à vérifier l'intégrité de l'image (Sha1sum)

Analyse du disque

Dans le cas de cette étude l'analyse consiste à extraire des données pertinentes tel que; l'identification du système d'exploitation, la récupération de données effacées ainsi que de données sensibles, l'analyse de logs...

Identification du système

Le logiciel ***autopsy*** m'a permis de déterminer le système d'exploitation utilisé.

FILE SYSTEM INFORMATION
File System Type: NTFS
Volume Serial Number: 0842E6CE42E6C014
OEM Name: NTFS
Version: Windows XP

Analyse de la base de registre

Le but ici est de reconstruire une partie de la partition d'origine afin d'en extraire le maximum de fichiers systèmes pouvant être intéressant.

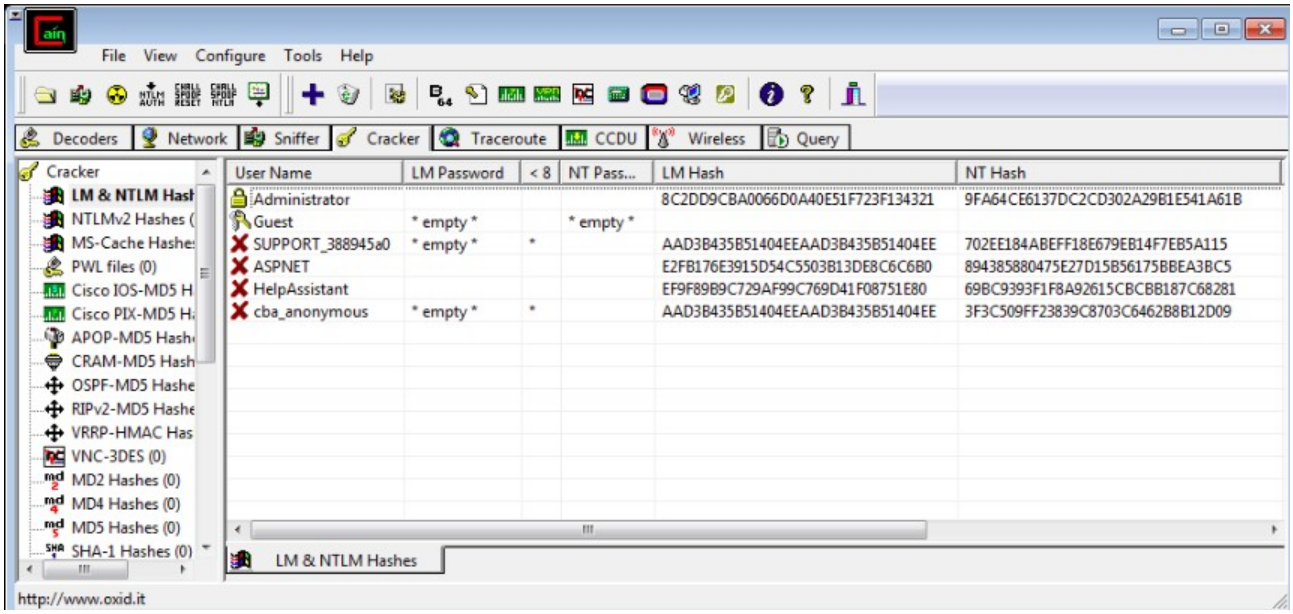
Pour ce faire j'ai récupérer les fichiers intéressant comme :
> **Netuser.dat** (ce fichier retourne entre autres le nom de l'utilisateur, son entreprise, les derniers fichiers ouverts, la liste des urls, les paramètres du proxy….)
> **Pam** (liste des utilisateurs du système)

Pour des raisons de confidentialité j'ai masqué les données propre à l'identification de l'utilisateur et de son entreprise dans le dossier analyse (masqué par XXXXXX)

J'ai utilisé le logiciel ***regripper*** pour lire les données de ces fichiers.

Je me suis servi de ces résultat pour rechercher des fichiers pertinents (comme les .pst d'outlook)

Par la suite j'ai utilisé le logiciel ***Caïn*** pour tenter un brute force de hash du mot de passe administrateur.
(vu le temps nécessaire au brute force (plusieurs jour) j'ai abandonné)



Récupération des fichiers effacés

J'ai utilisé ***Photorec*** pour récupérer des fichiers qui me paraissent pertinents (du type .doc, .pdf ,les fichiers de base de données …)

Les fichiers .pst (outlook) permettent de récupérer entre autres tout les mails échangés.
Pour ce faire j'ai converti les .pst avec ***readpst*** pour les lire avec thunderbird.

Ces fichiers permettent de récupérer énormément d'information, notamment les contacts de la victime ainsi qu'un nombre important d'informations contenues dans ces mails concernant la société.

Avec l'outil ***exiftool*** j'ai pu également extraire des méta-données de fichier (ex nom du propriétaire du fichiers, date de création….)

A venir (d'autres extraction de données)

Analyses des fichiers logs / événements

A venir

Analyse des traces de connexion Internet

J'ai pu également extraire les fichiers cookies de l'utilisateur contenus dans son dossier personnel.

Explication à venir

Conclusion

Il est évident vu les analyses faites sur ce disque que les données récupérées pourraient servir à un attaquant mal intentionné.

Cette étude démontre que le formatage simple d'un disque ne vaut rien en terme de destruction des données. Il faudrait réaliser des formatages beaucoup plus long comme la réécriture bit à bit de « blanc » en plusieurs passe pour minimiser la récupération de données par la suite.

Le plus simple serait la destruction physique du disque pour éviter toutes fuites par la suite.