

TP Forensics Sur Linux

ENSIAS, Université Mohammed V, Rabat

1 Introduction

Le forensique numérique est l'analyse d'un système informatique après incident. Elle consiste à acquérir, recouvrer, préserver, et présenter des informations traitées par le système d'information.

1.1 Dans quels cas on utilise l'analyse forensique ?

Une analyse forensique fait généralement suite à un incident : par exemple un serveur a été compromis et on souhaite déterminer les actions qui ont été effectuées sur les machines ainsi de collecter des preuves afin de pouvoir porter plainte. Néanmoins il existe encore de nombreux domaines qui utilisent l'analyse forensique :

- Analyse de malwares (surveillance du poste afin de déterminer les actions d'un malware).
- Récupération de données après sinistre.
- Test d'intrusion (récupération d'informations sensibles).
- Récupération de preuves en vue d'une plainte (intrusion, pédocriminalité, vol de données, etc.)

Pour cela, plusieurs techniques sont utilisées :

- Analyse des fichiers infectés.
- Analyse de la mémoire.
- Analyse des logs.
- Récupération de fichiers supprimés.
- Analyse du trafic réseau.
- etc ...

1.2 Les différentes approches

Il existe trois approches principales d'analyse forensique, à savoir le "dead" forensics (système éteint : analyse de disque), le "live" forensics (système allumé : analyse de la mémoire vive) et le "mixed" forensics (analyse de la mémoire vive et analyse du disque).

- A. **L'analyse à froid (le dead forensics)** : consiste à analyser un système éteint. Dans ce cas l'ensemble des données du système sera copié et analysé ultérieurement. C'est l'approche la plus complète mais nécessite plus de temps. L'analyse à froid permet de récupérer des informations sur :

- Les fichiers supprimés, l'espace libre du disque.
 - L'analyse de l'ensemble du système.
 - L'analyse du contenu du disque.
 - La détection des informations confidentielles.
 - etc ...
- B. **L'analyse à chaud (le live forensics)** : consiste à analyser l'état d'un système à un moment t . Dans ce cas, l'enquêteur récupère des informations issues de la mémoire vive :
- L'état du système.
 - Les informations liées à un processus.
 - La récupération des mots de passe dans la mémoire
 - etc ...
- C. **L'analyse mixte** : consiste à combiner les deux analyses précédentes : à froid et à chaud.

1.3 La méthodologie

L'analyse forensique exige une méthodologie pour collecter et préserver les preuves. Il est donc recommandé de suivre un guide des bonnes pratiques afin de ne pas altérer/modifier les données analysées. La méthodologie générale est la suivante :

- Sécuriser la preuve (le plus souvent en réalisant une image disque).
- Effectuer les étapes de pré-traitement.
- Lancer les recherches.
- Générer un rapport et faire l'extraction des éléments pertinents.

2 Cas Pratique sur Ubuntu 12.04

syslog est un daemon dédié à l'enregistrement des journaux (log) qui sont stockés souvent dans le répertoire `/var/log/`. Un journal log est un fichier texte dont les événements sont enregistrés, un par ligne. Tout logiciel écrit correctement utilise les journaux qu'il stocke sous différents emplacements :

- `/var/log`
- `/var/tmp`
- `/var/adm`
- `/tmp`
- `./nomdusoft/`
- `/usr/local/nomdusoft/`

2.1 Séance 1 : Formatage du disque

Formater les partitions

1. Lister les partitions en utilisant le gestionnaire de disque.
2. Combien de partitions sont répartie sur votre machine ?
3. Formater les partition en utilisant Utilitaire du disque :
 - Sélectionner la partition /dev/sdb (32 GB).
 - Formater le disque en utilisant Master Boot Record.
 - Créer une partition du type Ext4 avec la taille de 26 Go, Nommer la par **Backup**.
 - Monter le volume de la partition créée.
 - Supprimer la partition.
 - Formater le volume en type NTFS et nommer le **Backup**.
4. Lister les partitions en utilisant la commande fdisk.

Faire une Copie du Disque Il existe trois outils pour l'acquisition des données : dd, dcfldd et dc3dd.

1. dd est déjà installée sur Unix, sert pour la duplication ou la suppression des données d'un disque vers un autre. Créer une duplication de la partition /dev/sda dans une image qu'on place sur le bureau ddcopy.img
2. dcfldd (Defense Computer Forensics Lab) : est une fork de dd qui est plus rapide. Créer une copie de la partition /dev/sda et nommer la dcfcopy.img
3. dc3dd (Defence Cyber Crime Center)
 - Copier le disque /dev/sda vers le disque /dev/sdb en utilisant dc3dd command
 - Vérifier si le disque a été recopier par la commande fdisk.
 - Créer une image du disque /dev/sdc en image flashdrive.img. Placer l'image dans le bureau et changer ses permission pour qu'elle soit accessible.
 - Copier le disque /dev/sdc en image compressée.

2.2 Séance 2 : Fonction de Hachage et le data carving

Hashing : Vérifier l'intégrité des données les commandes md5sum, sha1sum et sha256sum sont déjà installés sur Unix.

1. Créer un fichier file1.txt, recopier le puis renommer sa copie file2.txt.
2. Comparer les hashes des deux fichiers en utilisant md5sum, sha1sum, et sha256sum. Rediriger les résultats dans un fichier hash.txt. Qu'est ce que vous observez ?
3. Installer l'outil md5deep.
4. Comparer les hash des deux fichiers en utilisant md5deep, sha1deep, sha256deep, tigerdeep, et whirlpooldeep. Qu'est ce que vous observez ?
5. Afficher le temps de hachage pour la commande md5deep.

6. Créer le hash de la partition `/dev/sdc` et le hash de `flashdrive.img` en utilisant `md5deep`. Comparer les, qu'est ce que vous observez ?
7. Ajouter des espaces dans le fichier `ENSIAS/cookies.txt`
8. Refaire les hash et les comparer en utilisant `md5deep`. Qu'est ce que vous observez ?
9. Utiliser la commande `ssdeep` (fuzzy hash) pour comparer le pourcentage de similitude entre les deux hash (du disque et de l'image).

File Carving : Analyse Brute des données Une discipline consistant à retrouver des fichiers et des données, à partir d'un block uniforme RAW, en binaire, pouvant être chiffrés. Les outils les plus utilisés sont : Foremost, Scalpel, MagicRescue et Recoverjpeg.

– **File Carving par Foremost**

1. Installer Foremost et lister ses options en utilisant la commande *man*.
2. Récupérer à partir de l'image `flashDrive.img` les fichiers de type : gif, jpg, png et enregistrer les dans un dossier sur le bureau nommé : *FlashOutputForem*.
3. Ouvrez le dossier *audit.txt* Qu'est ce que vous observez ?
4. Retaper la même commande de la question 2, Qu'est ce que vous observez ? Pourquoi ?

– **File Carving par Scalpel**

1. Installer Scalpel et lister ses options en utilisant la commande *man*.
2. Décommenter les types gif, jpg, et png dans `/etc/scalpel/scalpel.conf`
3. Récupérer à partir de l'image `flashDrive.img` les fichiers de type : gif, jpg, png et enregistrer les dans un dossier sur le bureau nommé : *FlashOutputScal*
4. Récupérer les même types de fichiers à partir de la partition `/dev/sda`.

– **File Carving par MagicRescue**

1. Installer MagicRescue et lister ses options en utilisant la commande *man*.
2. Citer les *modes d'action* (recipe) dans le répertoire `/usr/share/magicrescue/recipes`
3. Créer un dossier *Output*
4. Récupérer à partir de l'image `flashDrive.img` les fichiers de type : jpeg et png et enregistrer les dans le dossier *Output*.

– **File Carving par Recoverjpeg**

1. Installer Recoverjpeg et lister ses options en utilisant la commande *man*.
2. Créer un dossier *Outputjpeg*
3. Récupérer les fichiers de type : jpeg à partir de la partition `/dev/sdc1`. Enregistrer les dans le dossier *Outputjpeg*.

2.3 Séance 3 : L'éditeur hexadécimal

Travail à Rendre

1. Qu'est-ce que le code Hexadécimal ?
2. Qu'est ce qu'un éditeur hexadécimal ?

3. Citer des éditeurs hexadécimal les plus utilisés sous ubuntu.
4. Convertir en décimal puis en binaire les code hexadécimal suivant : 3F, 5E, 20 et EB.
5. Convertir les mot suivant en hexadécimal : FindMe.txt et Find Me.txt.
6. Définir la forme Little Endian.
7. la partition NTFS est répartie sur trois parties : le secteur de boot NTFS, la MFT d'une partition NTFS et des données. Donner des définitions de chaque partie en présentant le type d'informations qu'elle contient.
8. Déterminer les valeurs hexadécimal des offsets liées aux attribues du MFT.

Recherche des attributs dans MFT : Master File Table

1. Installer Hexedit sur votre machine.
2. Créer deux Fichiers FindMe.txt et Find Me with space.txt dans la partition /dev/sdb1.
3. Convertir les noms des fichiers en hexadécimal
4. lancer l'outil hexedit sur la partition /dev/sdb1. Verifier que c'est la partition adéquate (NTFS).
5. Chercher dans la partie hexadécimal le fichier FindMe.txt.
6. Déterminer la longueur du l'entête du MFT.
7. Déterminer la taille de la MFT.
8. *Attribue standard 0x10*
 - Définir le début de l'attribue de l'information standard (Standar Information Attribute).
 - Déterminer la longueur de l'attribue 0x10.
 - Extraire du hexedit les informations suivantes : la date et l'heur de création du fichier, la date et l'heure de la dernière modification, la date et l'heure du dernier accès.
9. *Attribue du nom 0x30*
 - Déterminer la longueur de l'attribue 0x30.
 - Extraire du hexedit les informations suivantes : la date et l'heur de création du fichier, la date et l'heure de la dernière modification, la date et l'heure du dernier accès.
10. *Attribue d'identification d'objet 0x40*
 - Déterminer la taille de l'attribue 0x40.
 - Déterminer l'emplacement du GUID.
 - Trouver le GUID du fichier FindMe.txt
11. *Attribue de donnée 0x80*
 - Déterminer la taille de l'attribue 0x80.
 - Vérifier si les fichiers *FindMe.txt* et *Find Me with spaces.txt* sont de type *résident* ou *non-résident*.
 - Déterminer le début de chaque fichier.
 - Calculer les numéros des clusters (logiques ou virtuels) des données du fichier *Find Me with spaces.txt*.