TP Forensics Sur Linux

Fonction de Hachage et le data carving

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*.

Séance 4 : 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 hexadicimal : 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 Infor- mation Attribute).
   - Déterminer la longueur de l'attribue 0x10.
   - Extraire du hexedit les informations suivantes : la date et l'heur de créa- tion 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 créa- tion 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*.