Master 2 SeCReTS

TP Forensics - Extraction de malware

Première partie

Contexte

L'objectif de ce TP est de mettre en pratique les méthodes pour effectuer des analyses forensiques sur les sources de données pertinentes en cas d'incident de sécurité. Nous verrons comment mettre en évidence la présence d'informations intéressantes, et comment les extraire afin de procéder à des analyses plus poussées des codes malveillants trouvés.

Le TP aborde les différentes sources de données dans l'ordre suivant :

— Système de fichiers ;
— Fichiers ;
— Mémoire vive ;
— Réseau.

Nous allons avoir besoin d'installer plusieurs outils pour ce TP. Il s'agit essentiellement de :

— `sleuthkit`
— `testdisk`
— `hexedit`
— `volatility`
— `wireshark`
— `bro`

Deuxième partie

Analyse forensique sur un système de fichiers

1 Analyse d'une clé USB

Décompressez le fichier `disk1.img.bz2`. Il s'agit d'une extraction brute du contenu d'une clé USB. Nous allons déterminer ce que contient cette clé.

La première étape va être de monter le système de fichiers en lecture seule pour observer le contenu « visible ». Faites bien attention au montage à passer l'option pour être en lecture seule. Après avoir observé le contenu, démontez l'image.

Combien de fichiers avez-vous observé ?

La deuxième étape va être de retrouver les fichiers effacés. Deux outils sont classiquement utilisés pour cela, `sleuthkit` et `testdisk`.

Dans `sleuthkit`, les commandes intéressantes sont :

— fls, ils
— fcat, icat

Concernant `testdisk`, c'est un programme interactif donc vous pouvez vous laisser guider par les instructions.

Avez-vous trouvé plus de fichiers qu'à l'étape précédente ?

2 Analyse d'une partition ext4

Décompressez le fichier `disk2.img.bz2`. Il s'agit d'une copie d'un système de fichiers ext4. Commencez l'analyse avec les mêmes étapes que précédemment. Là encore, un contenu malicieux est présent mais dissimulé.

Combien de fichiers avez-vous observé ?

Pour essayer de trouver le contenu malicieux, nous allons observer les blocs de données non alloués du disque. Pour commencer, confirmez la présence d'un contenu malicieux à l'aide de la commande `strings`. *Pouvez-vous observer le contenu malveillant ?*

Pour aller plus loin, vous pouvez utiliser la commande `blkls` du `sleuthkit`.

Troisième partie
Analyse sur les captures réseau

Nous allons nous intéresser au fichier `victim.pcap`. Cette capture réseau assez volumineuse correspond à une session de mail/navigation d'une utilisatrice nommée Alice. Celle-ci a l'impression qu'elle s'est retrouvée sur un site malveillant.

Pour analyser ce fichier, nous allons utiliser les outils Wireshark et Bro.

3 Wireshark

Dans un premier temps, à l'aide de Wireshark, retrouvez les connexions d'Alice à son serveur de messagerie. Pour ce faire, vous pouvez utiliser la fonctions Statistiques de Wireshark, avec la liste des conversations. D'autres informations intéressantes peuvent venir des paquets DNS. Enfin lorsque vous trouvez une connexion TCP intéressante, vous pouvez utiliser la fonction de suivi du flux TCP pour observer l'intégralité des octets échangés dans les 2 sens.

Pour lire la capture avec Wireshark : `wireshark -r victim.pcap`

Astuce : concentrez-vous sur les protocoles de messagerie.

Retrouvez le mail reçu par Alice et le site visité suite à la lecture de ce mail.

4 Bro

Ensuite nous allons analyser la capture avec Bro pour observer les pages consultées par Alice sur le site référencé dans le mail. Utilisez l'adresse IP du site dans un filtre pour Bro, afin de vous concentrer sur les connexions TCP intéressantes. Cet outil produit différents fichiers décrivant ce qui a été observé dans la capture réseau.

Syntaxe : `bro -r <fichier pcap> -f '<filtre tcpdump>' <script bro>`

Pour extraire les fichiers avec Bro, vous pouvez utiliser le script `/usr/share/bro/policy/frameworks/files/extract-all-files.bro`. De nombreux autres scripts se trouvent dans le dossier `/usr/share/bro/policy`.

Utilisez bro pour extraire la page affichée par le site en question lors de la première requête.

Enfin, observez la seconde requête HTTP faite vers ce site, et notamment le contenu de l'URL consultée, et déterminez si Alice s'est fait voler son mot de passe (plus facile avec Wireshark).

Quatrième partie

Analyse sur la mémoire vive

Ici nous allons étudier le fichier `linuxdump.core.xz` que vous pouvez décompresser avec `unxz`. Ce fichier contient une extraction de la mémoire d'un système Linux lors d'une intrusion. L'outil que nous allons utiliser ici est Volatility.

Pour utiliser Volatility, vous devez récupérer un fichier de profil correspondant au système à analyser, ici Ubuntu 16.04.3 64 bits. Mettons que vous placer ce profil dans un dossier nommé `profiles`, la commande à lancer est la suivante : `volatility --plugins=profiles --profile=LinuxUbuntu16043x64 -f linuxdump.core <commande>`

Pour connaître la liste des commandes, vous pouvez faire `volatility --info`. Celles qui nous intéressent ont un préfixe `linux_`.

Essayez de mettre en évidence la liste des processus et des conenxions réseau.

Pour comprendre ce qui se passe, un second fichier est disponible, il s'agit d'une capture réseau nommée `linuxdump.pcap`. Ouvrez la capture avec Wireshark ou Tshark et analysez la chronologie des événements. Eventuellement, vous pouvez essayer de désassembler les octets échangés dans la première connexion avec un outil comme `ndisasm` ou `miasm`.

Que pouvez-vous dire sur le service qui a été piraté, et sur l'outil qui a été utilisé pour cela ?