Business Services

Recherche de preuves numériques

Thomas Duval <thomas.duval@orange.com>

version 09/01/2019

Table des matières

1 Introduction

L'objectif de ce TP est de vous faire travailler avec des outils d'investigation du monde libre via l'un des live-CD reconnus dans le monde du Forensics. Choisissez l'un des live-CD et démarrez le. Sur la clé USB, des preuves ont été positionnées dans le répertoire de travail « ~/proofs ».
Dans la suite du document, les commandes à taper sur le système sont écrites ainsi :

```
commandes <arguments> …
```

Les termes entre « <...> » sont des arguments qu'il vous faudra compléter, les trois points « ... » signifie que la commande n'est pas complète et que vous devez la compléter.

2 Sleuthkit

Entrez dans le répertoire « preuve1 »

```
cd preuves1
```

Vous devez rechercher les chaînes de caractères suivantes :

- first
- SECOND
- 1cross1
- 2cross2
- 3cross3
- 1slack1
- 2slack2
- 3slack3
- 2fragment sentence2
- 1fragment1
- deleted
- a?b\c*d$e#f[g^

Monter le fichier fat-img-kw.dd dans un répertoire de votre choix, le montage de fichier dans un répertoire s'effectue à l'aide de l'outil « mount » avec l'option « -o loop=... » :

```
mount  fat-img-kw.dd <répertoire> -o loop=/dev/loop0
```

Effectuer des recherches de chaînes de caractères sur les fichiers du répertoire :

```
grep <chaîne> <répertoire>/<nom de fichier>
```

Les fichiers sont binaires, vous ne pouvez pas effectuer une recherche ainsi, trouvez une autre méthode[1]...
Finalement, quelles sont les chaînes de caractères que l'on peut retrouver par cette méthode ?
Réponse :

Toutes les chaînes de caractères ne peuvent pas être trouvées via cette méthode, nous allons utilisé une autre manière. Plutôt que de rechercher des chaînes de caractère sur les fichiers du répertoire, vous pouvez directement effectuer des recherches sur le fichier fat-img-kw.dd. Quels sont les chaînes que l'on peut retrouver dans ce cas ?
Réponse :

Vous remarquerez que le fichier file5.dat est absent. Pour le retrouver, il va falloir utiliser l'outil "fls" de sleuthkit :

```
fls fat-img-kw.dd
```

Cet outil nous donne un numéro d'inode, trouvez cet inode et utilisez-le dans la commande suivante pour extraire le fichier file5.dat :

```
icat fat-img-kw.dd <numéro de l'inode> > file5.dat
```

Recherchez maintenant la chaîne de caractère « deleted » dans ce fichier.

Pour finir, remplissez le tableau suivant :

Chaînes de caractère	Nom du fichier contenant	Remarque

1 Essayez l'outil « strings »

	cette chaîne de caractère	
first		
SECOND		
1cross1		
2cross2		
3cross3		
1slack1		
2slack2		
3slack3		
2fragment sentence2		
1fragment1		
deleted		
a?b\c*d$e#f[g^		

3 Récupération d'images

Dans cet exemple vous allez analyser un fichier image et trois traces réseau. Allez dans le répertoire "~/proofs/preuves2"

Cette image vient à l'origine d'un challenge de la communauté DFRWS datant de 2005.

scénario :

La ville de la Nouvelle-Orléans a adopté une loi en 2004 où la possession de plus de 9 images uniques de rhinocéros est un crime grave. L'administrateur du réseau de l'Université de la Nouvelle-Orléans a récemment alerté la police lorsque son logiciel à détecter un traffic illégal de rhinocéros. Malheureusement, lors de la saisie, l'ordinateur n'avait pas de disque dur. Une clé USB a été imagée et une copie de l'image vous est donnée.

En plus de l'image de la clé USB , 3 traces de réseau sont également disponibles et ont été fournies par l'administrateur réseau et impliquent la machine avec le disque dur manquant. Le suspect, qui poursuit son doctorat à l'Université depuis 1972, est le principal utilisateur de cette machine.

Vos objectifs :

Récupérer au moins neuf images de rhinocéros qui seront des éléments de preuve et les inclure dans un bref rapport. Dans votre rapport, vous fournirez des réponses au maximum de questions :

Q1. Qui a donné à l'accusé un compte telnet / ftp ?

Q2. Quel est le nom d'utilisateur / mot de passe pour le compte ?

Q3. Quels transferts de fichiers pertinents apparaissent dans les traces de réseau ?

Q4. Qu'est-il arrivé au disque dur de l'ordinateur ? Où est-il maintenant ?

Q5. Qu'est-il arrivé à la clé USB ?

Q6. Quelles images sont récupérables à partir de l'image de la clé USB ?

Q7. Existe t'il des preuves qui permettent de relier les traces réseau à clé USB ? Si oui, lesquels ?

À vous !

Monter le fichier RHINOUSB.dd dans un répertoire. Est-ce qu'on retrouve des fichiers ?

Réponse :

Effectuer une recherche avec Sleuthkit (outils fls). Est-ce qu'on retrouve des fichiers ?
Réponse :

Nous allons utiliser un outils de d'analyse par « carving » : Foremost, cet outil s'utilise de la façon suivante :

```
foremost -i <fichier input> -o <répertoire output>
```

Utilisez ce logiciel sur le fichier RHINOUSB.dd. Est-ce qu'on retrouve des fichiers ?
Réponse :

Analysez le fichier word que foremost a pu récupérer. Que contient-il ?

Réponse :

Vous êtes en mesure de répondre à la première question : "Qui a donné à l'accusé un compte telnet / ftp ?"[2]

Réponse :

Pour répondre à la question Q2, il va falloir regarder dans les traces réseau rhino*.log. Pour cela, nous allons utilisez l'outil "ngrep" qui utilise la syntaxe suivante :

```
ngrep -I <fichier input> <expression de filtrage>
```

Comme on recherche un login/password FTP, nous allons filtrer sur le port FTP :

```
ngrep -I rhino1.log port <numéro du port FTP>
```

Quels sont les login et mot de passe ?

Réponse :

Nous allons répondre maintenant à la question Q3. Pour cela, vous pouvez utiliser le même logiciel que précedemment. Quels fichiers peut-on trouver dans ces logs ?

Réponse :

On peut extaire les fichiers de ces logs réseau, pour cela, nous allons utiliser l'outil tcpxtract. À vous de trouver la syntaxe d'utilisation de ce logiciel. Quels fichiers peut-on récupérer ?

Réponse :

Même question avec l'outil tcpick.

Réponse :

Pour les questions Q4 et Q5, vous pouvez lire le fichier word récupéré plus haut.

Réponse :

Vous pouvez maintenant répondre facilement aux questions Q6 et Q7.

Réponse :

Pour effectivement trouver toutes les images de rhinocéros, il faut utiliser des logiciels de stéganographie, ce que je ne vous demande pas dans ce TP.

2 Aide : filtrez la sortie de la commande "strings" avec le mot "password"

4 Analyse de logs

Dans cet exemple vous allez devoir analyser un certain nombre de fichier de log. Allez dans le répertoire "~/proofs/preuves3"

Cette image vient à l'origine d'un challenge du "Honeynet Project" datant de 2010.

4.1 Challenge 5 of the Forensic Challenge 2010 - Log Mysteries

Challenge 5 - Log Mysteries - (provided by Raffael Marty from the Bay Area Chapter, Anton Chuvakin from the Hawaiian Chapter, Sebastien Tricaud from the French Chapter) takes you into the world of virtual systems and confusing log data. In this challenge, figure out what happened to a virtual server using all the logs from a possibly compromised server.

The questions are a more open ended than past challenges. To score highly, we recommend to answer the following way:

- Accuracy is highly encouraged to get the highest note
- You must explain tools you used and how
- If you use visualization tools such as afterglow, picviz, graphviz, gnuplot etc. explain why this was better (than other tools, than other visualization): such as good timeline representation etc.
- Outline HOW you found things

Submission deadline has passed. Results have been posted below. For any questions and inquiries, please contact forensicchallenge2010@honeynet.org.

Skill Level: Intermediate

Enjoy the challenge!

The Challenge:

Analyze the attached sanitized_log.zip and answer the following questions:

1. Was the system compromised and when? How do you know that for sure? (5pts)
2. If the was compromised, what was the method used? (5pts)
3. Can you locate how many attackers failed? If some succeeded, how many were they? How many stopped attacking after the first success? (5pts)
4. What happened after the brute force attack? (5pts)
5. Locate the authentication logs, was a bruteforce attack performed? if yes how many? (5pts)
6. What is the timeline of significant events? How certain are you of the timing? (5pts)
7. Anything else that looks suspicious in the logs? Any misconfigurations? Other issues? (5pts)
8. Was an automatic tool used to perform the attack? if yes which one? (5pts)
9. What can you say about the attacker's goals and methods? (5pts)

Bonus. What would you have done to avoid this attack? (5pts)

Répondez aux questions posées...

Réponse :

5 Trouver le chat

https://www.root-me.org/fr/Challenges/Forensic/Trouvez-le-chat

Énoncé

Le chat du président a été kidnappé par des indépendantistes. Un suspect a été interpellé par la gendarmerie. Il détenait sur lui une clef USB. Berthier, une nouvelle fois, à vous de jouer ! Essayez de faire parler cette clef et de trouver dans quelle ville est retenu ce chat !

La somme md5 de l'archive est edf2f1aaef605c308561888079e7f7f7. Entrez la ville en minuscule.

http://challenge01.root-me.org/forensic/ch9/ch9.gz

Réponse :

6 Command & Control Niveau 2

https://www.root-me.org/fr/Challenges/Forensic/Command-Control-niveau-2

Énoncé

Berthier, grâce à vous la machine a été identifiée, vous avez demandé un dump de la mémoire vive de la machine et vous aimeriez bien jeter un coup d'œil aux logs de l'antivirus. Malheureusement, vous n'avez pas pensé à noter le nom de cette machine. Heureusement ce n'est pas un problème, vous disposez du dump de memoire.

Le mot de passe de validation est le nom de la machine.

Le hash md5 du dump mémoire décompressé est e3a902d4d44e0f7bd9cb29865e0a15de

http://challenge01.root-me.org/forensic/ch2/ch2.tbz2

Réponse :